主题：技术前沿、安全实践

交易技术前沿

2024年 第1期 总第55期

——网络安全专刊（第1期）

ITRDC 证券信息技术研究发展中心（上海）

上海证券交易所 SHANGHAI STOCK EXCHANGE

内部资料 免费交流
《准印证》编号沪(K)0671

内刊

2024年 第1期
总第 55 期

运营：
证券信息技术研究发展中心（上海）
网络安全实验室

主管、主办：
上海证券交易所

刊首语

近年来，以人工智能、大数据、云计算、区块链为代表的新兴技术与传统金融深度融合，在给证券行业发展提供巨大动力的同时，对证券行业网络和信息安全提出新的挑战。二十大以来,习近平总书记强调要深刻认识国家安全面临的复杂严峻形势，正确把握重大国家安全问题，加快推进国家安全体系和能力现代化，以新安全格局保障新发展格局，努力开创国家安全工作新局面。

作为证券期货业关键金融基础设施，上交所深入学习贯彻党中央决策精神，落实各项部署，加大对关键信息基础设施安全保护建设力度。在充分衔接上位要求、总结监管实践的基础上，不断强化组织及制度保障，提升组织效能，通过各项举措提升自身安全防护能力。为加强行业整体安全能力提升、促进行业安全共性问题的解决、构建行业良好安全合作生态、促进交流，2022年10月，经证监会科技监管局批准，上交所依托于证券信息技术研究发展中心（上海）成立了证券期货行业网络安全创新实验室（以下简称“实验室”）。实验室成立以来，在中国证券监督委员会科技监管司指导下，在上海证券交易所党委统筹和数字化专业委员会具体部署下，围绕监管支撑、行业助力和自我提升三大目标，坚持问题导向，重点就行业堵点、难点、痛点推进行业安全建设工作，举办了多场技术交流，组织行业开展课题研究，为促进行业安全交流、构建良好生态方面发挥积极作用。

由实验室主办的《交易技术前沿》-网络安全专刊聚集于安全领域,汇总提炼行业内安全思考、优秀实践、前沿技术、调研分析报告等四十多篇，促进了行业网络安全建设工作。希望能够打造品牌效应，汇聚分享行业网络安全建设成果，促进安全技术的推广和优秀安全创新应用解决方案的落地，也希望行业同仁一起参与实验室的后续建设和行业交流，为行业总体安全能力建设做出贡献。

证券期货行业网络安全创新实验室
2024.05.17

目录 安全实践

05 IPV6实践

06 安全建设

目录 技术前沿

07 安全架构

08 安全运营

09 密码技术

10 新技术应用

11 云原生

安全实践

01 安全思考

论“数字化”及“数字化转型”背景下企业信息安全建设路径

文丨侯亮、陈凯晖、赵黎、刘新亮、方莹莹

国泰君安证券股份有限公司

摘　要： 随着数字化转型逐渐进入深水区，已呈现多元融合、碎片化、复杂化发展等泛化趋势。企业需要及时调整网络安全战略定位及战略布局，从被动开展到需要打响“主动保卫战”，依托技术手段及技术工具，注重加快人才、流程、经验建设，为“业务数字化”夯实网络安全基石，最终实现与业务共同稳步发展。同时需要拓宽网络安全视角，积极探索内外交互联动方式及一体化合作发展的新型模式，最终真正实现网络安全“看得见、守得住、重沉淀、促发展、赢未来”，助力保障企业强劲竞争力。

关键字： 业务数字化、网络安全、主动保卫战

要让未来要发生的事情在今天思考，要让今天已做的事情成就未来。

背景

在十四五规划明确“加快数字化发展”在“加快发展现代产业体系、推动经济体系优化”目标中作为重要指导方针后，数字化浪潮便席卷而来。数字化转型对于企业来说不再是一道选择题，而是一道生存题。而网络安全防护工作却是作为数字化转型的前提基础和坚实保障，全面提升网络安全保障能力，切实为企业数字化转型保驾护航，推动高质量发展。

引言

“数字化”及“数字化转型”背景下的企业网络安全建设与推动发展，从技术的视角上看，数字化是IT（Information Technology）向DT（Data Technology）转化的过程。因此，就不得不提“三化”，即信息化、数字化、智能化，才能更好的理解在此背景下“企业网络安全”建设路径与重要意义。

信息化：信息化的本质是“连接”，既是将物理世界的信息和数据转换为“0与1”的二进制代码录入信息系统，以“数据”形式保存，将线下的流程和数据迁移到电脑上进行处理，以此提高效率、降低成本并提升可靠性。

信息化特点：人“主”机“辅”，即以人为主、以机器为辅。

数字化：数字化的本质是“生产力与生产关系的重构”，即是将许多复杂多变的信息转变为可以度量的数字、数据，再以这些数字、数据建立起适当的数字化模型，把它们转变为一系列二进制代码，引入计算机内部，进行统一处理，利用数字技术来改变原有商业模式并提供新的收入或新价值创造，这就是数字化的基本过程。

数字化特点：以“信息”转化为“数据”，再将数据转化成“可用”信息。

智能化：智能化的本质是“主次关系重构”，即是事物在计算机网络、大数据、物联网和人工智能等技术的支持下，所具有的能满足人的各种需求的属性。智能化是自动化技术当前和今后的发展动向之一，逐步具备类似于人类的感知能力、记忆和思维能力、学习能力、自适应能力和行为决策能力，在各种场景中，以人类的需求为中心，能动地感知外界事物，按照与人类思维模式相近的方式和给定的知识与规则，通过数据的处理和反馈，对随机性的外部环境做出决策并付诸行动。

智能化特点：机“主”人“辅”，即以机器为主、以人为辅。

正文

在数字化转型的过程中，不仅仅要把“关注点”放在人才、流程、组织、技术等上，要清晰清楚所在的公司“数字化”转型的目的、难点、阶段等。也要从全局观去了解人类在历史中所经历的四次科技变革，只有这样，才能更清晰清楚在本次的“数字化”时代的变革中，网络安全所处于的位置、分工、重要程度、方向，以及如何能更贴近“数字化”本身而做好网络安全工作本身，才能合理的分配资源、合理的设计规划、合理有序的推进网络安全工作。

从十八世纪六十年代至今，全人类经历了4次技术变革，每一次的技术变革都极大提高了生产力，改变了人与人、人

与物、物与物之间的纽带，也改变了世界的面貌，而本次技术变革的过程中，恰恰也是信息安全在全人类历史的长河中，开始产生广泛和深远影响的重要阶段，也逐步从“背后”走到了“舞台中央”。今天，信息安全已成为一个世界性的问题，“信息安全”已从起初的军事领域迅速地扩展到了数字化时代社会生活的方方面面，已关乎每一个人。信息安全问题所造成的影响和后果，轻则影响公民的正常生活、威胁企业生存发展，重则危及国家和社会的稳定与安全。信息技术的辐射性、衍生性，信息资源的共享性，信息传播的跨界性，通信网络手段的多样性等，决定了信息安全环境的开放性、复杂性。而在这么一个开放、复杂的环境中，信息安全注定是一个动态变化的过程，也永远将会是一种相对的安全。这个过程需要国际社会、国家、企业组织和公民共同努力，共同担责，不仅解决技术与产业问题，也要解决组织合作、法律法规、安全监管的问题。

第一次工业革命时期，瓦特改良蒸汽机，迅速在许多行业中使用，把人类带进了“蒸汽时代”，即是“蒸汽化”。

第二次工业革命时期，由于发电机和电动机的发明和使用，电力逐步取代了蒸汽，把人类带进了“电气时代”，即是“电气化”。

第三次工业革命时期，以物联网、云计算、大数据为核心的新一代信息技术把人类带进了“信息技术时代”，即是“信息化”。

第四次工业革命则是利用信息化技术促进产业变革的时代，以信息物理系统为基础，以生产高度数字化、网络化、机器自组织为标志。即是“智能化”。

无论是信息安全还是网络安全，亦或数据安全等，都要深刻的理解“安全”的基本含义，即是客观上不存在威胁，主观上不存在恐惧。即客体不担心其正常状态受到影响。可以把网络安全定义为：一个网络系统不受任何威胁与侵害，能正常地实现资源共享功能。要使网络能正常地实现资源共享功能，首先要保证网络的硬件、软件能正常运行，然后要保证数据信息交换的安全。

在了解了“数字化”及“数字化转型”的历史后，那么企业网络安全的建设与推进路径也就明朗了，即是15字方针，“看得清、守得住、当沉淀、促发展、赢未来”

看得清：看得清数字化资产的分布与暴露面，看得清业务场景的风险隐患，看得清“云网端数用边”安全形势，看得清宏观层面跨时间与空间的安全态势，看得清微观层面的攻击线索。抽象总结——“两体一道”，即是访问主体、访问通道、访问客体。

守得住：守得住数字化资产，守得住客户隐私数据，守得住商业秘密，守得住公司信誉。抽象总结——“四问”，即是外部客户访问、内部客户访问、运维管理访问、系统间访问。

当沉淀：沉淀安全分析规则、沉淀安全脚本、沉淀安全工具与平台、沉淀安全方法论、沉淀安全标准规范流程、沉淀自有安全人员。抽象即是——基础安全保护沉淀、身份与策略管控沉淀、检测响应与运营沉淀、源生安全集成沉淀。

促发展：促数据有序流通、促创新业务发展、促数字化转型。

赢未来：赢在业务创新，赢在数据开放，赢在数字化人才，赢在安全生态与安全文化，赢在未来。

数字化转型背景下企业网络安全建设的5个阶段

1. 第一个阶段，以资产和流量为视角，做看得清

资产层面，做好资产管理是安全运营最基础性的工作，是安全事件处置、漏洞补丁修复等流程能够顺利开展、精准定位的关键要素。这一阶段，开展多维度全方位的资产探查和测绘，实现资产价值管理和精细化管理。通过明确安全运营资产对象的重要性（包括终端、重要的服务器、核心的业务系统等），并针对资产的不同维度（如类型、IP、端口、组件、组件版本、是否对外发布）进行可视化的展示和维护，提取容易造成混淆或干扰的“噪音”资产（如正向代理、反向代理、扫描器、内部DNS、不规范的应用服务器），动态分析高敏感系统和集权平台（如VPN/OA/邮件/运维监控/堡垒机/财务系统）潜在风险。

流量层面，立体化覆盖边界流量（不限于互联网边界、安全域边界）、横向流量、重要服务器流量（不限于Web/DNS/Email/database服务器）等，精准区分内对外、外对内、内对内流量，充分运用SSL卸载以及加密流量分析引擎，根据规则匹配、语义分析、流量特征、关联分析等技术手段，快速识别漏洞、恶意软件，切实做到流量可见、风险可视。

2. 第二个阶段，以威胁狩猎和高效闭环为视角，做守得住

在看清安全形势的同时，需要一双火眼睛睛抓住高风险事件，并进行及时、恰当地处置，不断推动安全能力的持续提升，方能守得住。第二阶段，以威胁狩猎和高效闭环为视角，充分利用当前的安全资源，提升安全监测的有效性、安全响应的高效性，守住网络安全和数据安全。

威胁狩猎的首要任务是做好安全数据治理、建立威胁建模。安全数据治理，是对数据理解的过程，包含了数据采集-数据标准化-数据增强-数据分析-响应处置-复盘这个迭代过程中的数据治理部分。依据运营预期、需求、基础设施、预算、客观条件，明确采集范围、采集方式、采集格式、采集目的、数据接口管理、处置接口管理、预估存储大小、明确存储时间、数据源统一监控、变更管理等，明确前端数据源标准，明确数据模型。在贴合业务的场景下，建立威胁规则模型，基于攻防对抗、攻击模拟、历史安全事件、外部情报等，持续进行编排和优化，并利用各种验证框架提升威胁规则模型的有效性。在建立威胁规则模型的基础上，进一步开展数据强化分析，即威胁狩猎工作，利用各种方式区分正常与异常行为，例如分析影响范围和意图，加快事件调查和对根本原因的理解。

高效闭环，需要高效的事件闭环流程，一方面，结合业务

特点，制定自动化处置策略，如对业务时段、非业务时段制定不同封禁策略；另一方面，通过标准化的应急处置、通知预警、协同联动流程，辅以可视化的类工单系统进行事件的跟踪与管理，直至事件闭环。

3. 第三个阶段，以人和工具为视角，做当沉淀

看得清、守得住的最终目标是为了促发展、赢未来，而沉淀是其中必不可少的桥梁。小到沉淀一个安全分析规则、一个安全脚本，大到沉淀一套安全方法论、一套安全体系，都将给企业高质量创新发展注入新动力。

因为沉淀，才能培养高精专的自有人才，打造特色的自有安全团队；因为沉淀，才能将常态化运营和实战化经验相结合，转化为可以传承、共享的知识，通过不断地流动与迭代加以完善，形成公司级或者行业级标准、规范、最佳实践等，从赋能一个系统扩展到赋能多个系统，从赋能一个创新业务扩展到赋能多个创新业务，对各个团队、各个业务部门甚至整个行业产生积极的影响。

4. 第四个阶段，以促进数字化转型为视角，促发展

数字化转型是企业围绕“数据赋能业务”为核心进行全面布局并长期坚持的工作。数字化转型必须从技术、战略和人才的层面去思考，以技术赋能企业运营为起点，以战略重塑商业模式为核心，以人才打造组织能力为根本，实现这三个方面的有机结合。

有了安全技术、安全人才相关的沉淀，方能在各类创新业务飞速发展的当下，不会因为不熟悉的应用组件、多样的API接口、复杂的数据流动而心生恐惧，盲目阻断创新业务的上线；也不会因为缺少有效、可落地的安全管控，而发生数据安全泄露等事件。

总之，以促进数字化转型为视角，通过持续加深对业务安全的理解，建立健全数据安全规范体系，构建确保数据要素有序流通的基础能力，健全数据安全技术保障能力，谋求安全与业务共发展。

5. 第五个阶段，以共建安全开放生态为视角，赢未来

安全与创新是一个恒久的话题。只有快速适应未来安全形势的变化和细分安全能力的需求，为开放创新提供基础支撑，共建安全开放生态与安全文化，深度赋能业务发展与业务升级，企业才能在快速发展过程中树立行业地位、增强企业自身竞争力，赢在当下，且赢在未来。

企业数字化、数字化转型中网络安全建设六点建议

1. 企业网络安全建设是重大战略问题，是典型的“一把手”工程

“以安全保发展、以发展促安全”的要求，充分体现了马克思主义的辩证法，体现了科学的发展观。要解决数字化转型安全问题，需要企业从经营战略视角进行统一规划，建立系统性的安全防御机制，安全不再只是某个部门的工作范畴，更需要管理层战略关注，数字化时代，安全更成为“一把手”工程。

2. 加强“顶层设计”，提升体系化安全能力

要对安全体系建设进行统一的规划，制定安全体系框架，明确保障体系中所包含的内容。同时，还要制定统一的信息安全建设标准和管理规范，使得信息安全体系建设能够遵循一致的标准，管理能够遵循一致的规范。同步强调“统一规划建设、全面综合防御、技术管理并重、保障运营安全”，规划中要体现安全保障的重要性，利用多种安全保障机制，保障网络和信息系统的运行安全，在实战中保障业务的持续性和业务数据的安全性。

3. 善从外部借力，形成联动联合、互动互联

企业数字化转型过程中业务环境将更加开放，业务生态将更加复杂，这将对未来安全管理与保障带来巨大的挑战。未来“多云共存”“异构管理”等新安全挑战将成为企业数字化安全建设和发展面临的新常态，可以通过安全研究机构、产商等联合赋能，聚合企业数字化转型所需的安全能力，促进企业数字化相关安全系统形成一体化安全保障机制。探索安全管控赋能主动对接各系统安全态势感知及安全大数据支撑平台，实现相互交互联动，形成“一盘棋”的安全管理局面。

4. 加强人才培养，网络安全领域不拘一格降人才

数字化转型涉及的技术和场景众多，需要培养既懂网络安全技术，又了解数字化转型方法论，业务场景相关技术的复合型人才，才能更好地完成数字化转型下的网络安全相关工作，于企业而言，应逐步建立网络安全专业人才的招聘选拔培养任用机制，通过安排技术技能培训与考核，参与技能大赛和红蓝对抗演练等方式，实现人才队伍从信息安全等级保障，保护合规测评能力，向网络攻防专业技术能力及实践能力的“双轮驱动”提升。

5. 探索建设企业网络安全大数据中心

利用“实时、全样、精准”的安全大数据建立全程在线、跨厂商、全域覆盖、实时反馈的“企业网络与数据安全态势全景图”，全天候全方位监测预警网络安全威胁，提高对网络安全风险的感知、预警和防护能力，实现集约化、常态化的威胁发现和应急处置，实现“用数据感知、用数据决策、用数据管理”的网络安全治理新模式。

6. 把“网络安全”融入企业文化，助力企业“数字化转型”

企业文化是一个组织的核心价值观，体现在企业日常运行中的各个方面，是一个企业的基因。与传统企业内部笃信“领导经验”不同，一个数字化的企业上下皆以“数据”作为衡量决策及结果的唯一标准。要想让企业顺利完成“数字化转型”，需要在企业内部打造“网络安全”这样的文化，可以起到事半功倍的效果。

经过多年的信息化建设，企业进入到在线化、协同化、数字化、智能化的发展阶段，而数据是推动数字化、智能化的核心基础，数字化不仅带来企业运营效率提升、成本降低，更重

要的还是在于商业模式的变革与新价值创造。而前置条件便是网络安全、信息安全、数据安全。

结束语

一切企业不注重“网络安全”就谈数字化转型都是纸老虎。

一切企业不注重“数字化”就谈发展的都会被时代所抛弃。

企业安全建设一定要有战略思维、战略眼光，不能仅停留在“技术本身”，信息安全不是一个或几个部门的任务，而是数字化时代对于整个公司提出的新要求。在不同时期，对网络安全有过不同的称谓和解释，其内涵在不断深化，外延在不断扩展。而我们每一个人、每一个企业、每一个组织都需要重视并顺应“数字化转型”的趋势，并投身其中，为产业升级、建设数字中国贡献一份力量。

数据安全治理路径探索

文｜吕德旭

中金所技术公司

摘　要： 对证券期货行业而言，不断提升数据安全治理水平，在促进数据利用同时，保障数据安全，对促进数字经济发展具有重要意义。本文聚焦数据安全治理路径，提出从数据安全合规出发，待确认，结合机构或企业自身实际，选择合适数据安全治理框架，参考通行的技术标准，不断实践并迭代提升的思路。

关键字： 数据安全、数据安全治理、路径

背景

数据是做强做优做大数字经济的重要基础。2022年第2期《求是》杂志刊发了习近平总书记的重要文章《不断做强做优做大我国数字经济》，指出数字经济正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。在2023年2月印发的《数字中国建设整体布局规划》中指出要按照“2522”的整体框架进行布局，夯实数字基础设施和数据资源体系“两大基础”。

数据安全治理是建设“数字中国”的重要保障之一。在《数字中国建设整体布局规划》指出，要强化数字中国关键能力，一是构筑自立自强的数字技术创新体系。二是筑牢可信可控的数字安全屏障。在《数据安全法》指出：维护数据安全应建立健全数据安全治理体系，提高数据安全保障能力。

数据安全治理是一个长期化过程，需要选择适当的、可持续优化的路径。显而易见，在“数字中国”发展战略指引下，数据成为经济发展的重要驱动要素，也是企事业单位拥抱数字经济的必然选择。在证券期货行业的企事业单位，也必然要从自身实际出发，结合行业、企业特点，建立健全企业数据安全治理体系，提高数据安全保障能力，积极参与数字中国建设，为促进数字经济发展添砖加瓦。

数据安全治理基本要素

在证券期货行业，做好数据安全治理，有三个基本要素需要在先期进行考量。它们分别是合规、质量和成熟度。

合规

合规是根本性基础。

合规包含了法律法规层面、监管要求及本单位的制度层面合规。合规是做好数据安全治理基本依据，同时也是底线性要求。不能全面细致分析、理解并严格落实合规要求，在后续的实施环节就可能存在重大缺点和漏洞，甚至可能出现违法、违规的情况。

法律法规层面，涉及数据安全的包括《网络安全法》、《数据安全法》、《个人信息保护法》，《关键信息基础设施保护条例》等。

监管要求层面，证券期货行业需要严格遵循和落实证监会有关基本要求，同时根据不同情形，也需要遵循人民银行发布的有关要求。

企业内部制度，一般是在前两者基础上结合本单位实际制定，不做赘述。

如图1所示，证券期货行业机构在数据安全领域需要遵循的主要合规，其他未在图中列明的要求，建议各机构可自行梳理补充。

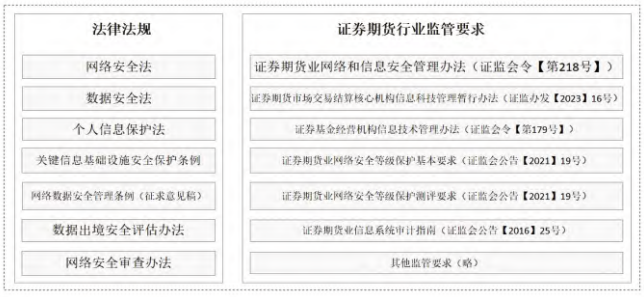


图1 与数据安全相关的主要合规要求（部分）

质量

数据质量是基本保障。

数据质量是数据治理中的重要环节，同时也是数据安全治理基本保障之一。数据质量低下，就可能造成很难理清数据资产、数据模型不统一、数据格式混乱等等问题，同时造成分类分级不准确，保护措施落实不到位等等问题。因此，数据安全治理中要确保数据质量的协同改进和提升。

数据质量一般需要较为规范、统一的数据模型，标准化的数据规范，同时需要持续的维护和更新。在证券期货行业，由于行业特定业务属性，还需要考量数据的跨机构访问、使用以及监管方对数据分析、审查等等需要，所以也需要遵循一定特定标准。

提高数据质量，除结合本企业的业务特点外，同时应关注两点，一是要遵循行业监管要求，例如《中国证监会数据管理办法（试行）》《中国证监会数据质量管理细则（试行）》，特别是后者中规定的数据质量评价指标，可以视为证券期货行业数据质量贯标的基本依据；二是要关注证券期货行业相关标准，例如证券期货业数据模型相关标准、证券期货业投资者权益相关数据的内容和格式相关标准（可在资本市场标准网查询和下载）。

图2 与数据质量相关的主要监管要求

除上述之外，较高的数据质量，可以为通过使用工具实现数据治理铺平道路，也可以进一步提升数据质量管理水平。从而为实现工具化、平台化的数据安全治理工作铺平道路。

成熟度

数据安全治理的成熟度是一个逐步提高的过程。

成熟度这个概念本身就说明了一种逐步迭代，不断改进和提升的过程。数据安全治理基本目标就是通过一系列的治理活动，不断提升数据安全能力成熟度。大家熟知的数据安全能力成熟度模型（Data Security Capability Maturity Mode，简称DSMM）于2019年8月30日正式发布《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019），为衡量一个组织的数据安全能力成熟度水平提供了可评判的基本依据。企业或组织通过这个衡量“标尺”，可以清晰的识别自身数据安全能力短板，从而有目的、有针对性的实施数据安全管理，补足短板，持续改进和提升数据安全能力。

数据安全治理思路

数据安全治理不是一蹴而就的，也不可能通过一次改进或治理活动就能够彻底解决所有问题，需要抓住重要的、迫切的关键性问题，反复迭代，持续改进。图3是本文主要讨论的一个数据安全治理路径，供参考。

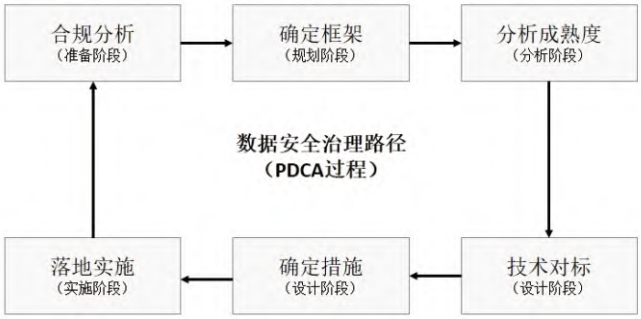


图3 数据安全治理路径

准备阶段——从确保合规出发

证券期货行业作为国家金融领域重要行业，一定要切实把握合规的重要性，将合规作为基本出发点。从确保合规出发提升数据治理能力，需要做好几项必要的工作：

1. 深入理解并严格遵守法律法规要求

最基本《网络安全法》、《数据安全法》、《个人信息保护法》要深入理解并遵守。结合本单位特点，如果是关键信息基础设施单位，还要遵守《关键信息基础设施保护条例》及相关要求。涉及可能存在国家核心数据、重要数据的，还应考虑遵守《网络安全审查办法》；涉及数据出境的，还应遵守《数据出境安全评估办法》等规章。证券期货行业机构还应遵循《证券期货业网络和信息安全管理办法》等要求。这些都是要结合企业自身特点进行汇总、整理，深入分析、理解并严格遵守和落实的。

2.将法律法规和监管要求科学融入自身数据安全管理相关制度

数据安全的落实离不开具体落实，而法律法规、监管要求通常要考虑通用性、普遍性，行业机构或企业就要结合自身特点，在法律法规、监管要求基础上进一步细化和完善，并科学融入到企业自身制度中。例如关键信息基础设施运营者，就应制定适合自身特点的有关关键信息基础设施相关的数据安全保护制度、规范、方案。而如证券公司、期货公司、基金公司的投资者客户众多，也需要结合自身特点，制定可覆盖

投资者个人信息保护的相关制度，从而为切实保障投资者个人信息安全奠定基础。

规划阶段——选择合适数据安全治理框架

在对数据安全合规充分认识的基础上。实施数据安全治理，应该选择一个适当数据安全治理框架。目前国内外有多种版本的数据安全治理框架，建议证券期货行业机构或企业结合自身实际和国情出发选择自身的治理框架。常见的数据安全治理框架主要有：

Gartner数据安全治理框架。Gartner最早提出数据安全治理理念，并认为数据安全治理不仅仅是一套用工具组合的产品级解决方案，而是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条。Gartner数据安全治理框架更加强调过程性，包含了五个过程：平衡业务需求与风险，识别、确定优先级和管理数据集生命周期，定义数据安全策略，实施安全产品，制定所有产品的政策。

微软数据安全治理框架DGPC。微软的治理框架更加侧重强调隐私、保密和合规，以更好实现数据安全风险控制。主要围绕“人员、流程、技术”三个核心能力领域的具体控制要求，同时强调与现有安全框架体系或标准协调合作。

中国软件评测中心网安中心数据安全治理框架（本文以下简称“软测框架”）。该框架更强调以“让数据使用更安全”为目的，通过组织构建、规范制度、技术支撑等要素共同完成数据安全建设的方法论。框架的核心内容主要由治理层、管理层、执行层和监督层四个层面组成。

应该说这些框架有自身的特点和重要价值，没有绝对的优劣可言，笔者更倾向于选择融合各家长处的方式，例如以软测框架为蓝本，把握治理过程理念，围绕“人、流程、技术”展开。除此之外，国内外还有一些安全机构或企业发布了数据安全治理框架，也可以作为参考框架标准。

分析阶段——评判成熟度水平，识别短板

数据治理涉及的方面很多，如何确定自身的短板和关键点，作为一段时期的切入点更加合适，建议将《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）作为基本的自评估（或外部评估）标准。

DSMM的架构由四个安全能力维度、七个安全过程维度、五个安全能力等级构成。四个安全能力维度：组织建设、制度流程、技术工具、人员能力；七个安全过程维度：数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、通用安全，共计30个过程域。五个安全能力等级：从低到高依次1至5级。

如前所述，已选取的数据安全治理框架，在执行DSMM自评估时，需要注意的是，不但要根据DSMM架构分析自身长处和不足，同时要与框架中的内容对应起来，这样就可以评判当前数据安全治理的关键要点在哪些方面。例如，可以将DSMM架构中的组织建设、制度流程与软测框架中的治理层、管理层内容对应起来。同时要注意，软测框架将技术和人员隐含在其中，需要审慎地将DSMM中技术工具、人员能力与软测框架中的有关内容对应。

此外，在DSMM评估基础上，一方面可以知道机构或企业自身数据安全能力水平；另一方面，可以明确数据安全治理框架有哪些薄弱环节，以便在下一步治理工作中进行改进。

为什么不选择在所有的工作开展前首先进行DSMM评估？笔者认为在缺乏明确的出发点和基本建设目标的情况下，直接进行DSMM评估不利于判断哪些环节更需要改进，同时也容易造成改进目标不明确，后续的工作可能变成“胡子眉毛一把抓”。

设计阶段——结合相关标准完善制度和措施

在上述评估基础上，需要有针对性地对已确定的治理框架的薄弱环节进行提升和改进。基本的建议有以下几点：

（1）制度层面要确保以合规为基础，结合自身实际制定。

（2）管理层面要把握的高效、协同，流程设计要综合考虑组织、人、技术协调，并尽可能简化。

（3）执行层面，要尽可能参考成熟的、有清晰指导意义的标准，例如在涉及数据生命周期的多个环节安全，可以参考主要标准包括：

· 涉及数据安全保护的，包括：《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）；《证券期货业数据安全管理与保护指引》（JR/T 0250—2022）；

· 涉及数据分类分级的，可以参考《金融数据安全 数据安全分级指南》（JRT 0197-2020）、《证券期货业数据分类分级指引》（JR/T 0158-2018）。

（4）保护措施选择层面，建议考虑技术与管理充分融合，避免技术手段看似先进，管理手段却落后的情形。建议尽可能多地考虑安全保护的逻辑性问题，避免看似有效的技术措施，在业务层面却丢失数据敏感性的保护。除严格落实强制规定外，还需要在技术措施的选择上兼顾数据使用便利性问题。这就是要结合特定场景来专门考虑的。

实施阶段——在落实环节持续改进并定期回顾，迭代提升成熟度

如前所述，在确定了框架、找到了薄弱环节、明确了制度和措施基础上，就需要严格的落实并持续改进了。

数据安全能力是在不断落实治理的过程中，持续改进的。这个过程中，一是要注重边实施、边改进，持续提升管理与安全技术措施；二是要注重使用必要的数据安全管理工具，不断利用自动化技术、AI工具等提升管理、监控水平和数据安全审计能力；三是要注重阶段性的回顾，关注成熟度提升的进展，寻找薄弱环节，确定下一个迭代的改进计划，这也是最重要的一点。

结束语

数据安全治理的根本目标是在保障安全的前提下，促进数据利用。由于数据自身存在的分散性、流动性、多变性等特点，为数据安全治理带来了很高的挑战，也不可能有通用的、普适性的方法或路径能够解决数据安全治理中的所有问题。

本文仅提供了一种数据安全治理路径思路，在具体实践中，建议机构或企业结合自身实际，选择合适的治理路径，通过不断持续改进，必然会逐步提升数据安全能力，不断促进机构或企业的数字化转型。

投资者个人信息保护制度下金融机构面对执法机关调查取证的问题思考

文丨徐正伟

国君集团资管公司

摘　要： 个人信息保护法的实质功能是一部个人信息处理活动行为规范法，个人信息保护的真正立法目的有两个：一个是“保护个人信息权益”，另一个是“促进个人信息合理利用”。《中华人民共和国个人信息保护法》与《网络安全法》、《数据安全法》等法律一起构成规范性、系统性、完整性的保护体系，共同为公民个人信息权益保护提供切实有力的法律保障。但当企业面临执法机关协查取证时，应当遵守法律法规配合执法机关，不随意扩大范围，保护投资者信息。

关键字： 投资者个人信息、金融数据、执法机关、协查取证

法律对侵害个人信息的处罚

根据《中华人民共和国刑法》第二百五十三条“【侵犯公民个人信息罪】违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。”

《个人信息保护法》规定的处罚标准为1-10万罚款，情节严重的为10-100万罚款。近两年以来，央行针对个人信息领域的违法行为已经出具了多份处罚，包含单位及个人。

序号	当事人名称	违法行为类型	处罚内容
1	鹏元征信有限公司	1.未经批准，擅自从事个人征信业务活动； 2.企业征信机构任命高级管理人员未及时备案。	没收违法所得19175499.29元，并处罚款62万元
2	华夏银行股份有限公司	违反信用信息采集、提供、查询及相关管理规定。	罚款486万元
3	兴业银行股份有限公司	违反信用信息采集、提供、查询及相关管理规定。	罚款5万元
4	浙商银行股份有限公司	违反信用信息采集、提供、查询及相关管理规定。	罚款65万元
5	李XX（时任浙商银行零售银行部信用卡部风险控制中心总经理）	对浙商银行以下违法违规行为负有责任：违反信用信息采集、提供、查询及相关管理规定。	罚款8万元
6	戴XX（时任浙商银行深圳分行零售银行部信用卡中心主管）	对浙商银行以下违法违规行为负有责任：违反信用信息采集、提供、查询及相关管理规定。	罚款1万元
7	连XX（时任浙商银行上海分行信用卡营销中心主管经理助理）	对浙商银行以下违法违规行为负有责任：违反信用信息采集、提供、查询及相关管理规定。	罚款0.5万元

图1 违法案例处罚情况

执法机关的权力及边界

随着互联网业务的蓬勃发展，犯罪分子将洗钱、电诈、赃款投资等应用到了传统的金融公司，购买基金、黄金、证券、信托等作为快速转移资金，分流资金，洗钱的手段。传统金融公司在流程，机制等方面反应能力弱于互联网公司，当取证整套流程走下来，犯罪分子可能已经将资金转走了。另外传统金融公司的人员基本都是从事内部相关的事务处理，当穿着制服的警察或其他执法机关人员亲临现场进行调查取证的时候，内部人员可能自乱阵脚不知道怎么应对。毕竟大多数人跟执法机关打交道的可能只有交警，对于公安、国安、检察、法院、军检、海关、中纪委等执法人员现场调查取证略显陌生。

早在1983年国家发布了《最高人民法院、中国人民银行关于查询冻结和扣划企业事业单位机关团体的银行存款的联合通知》（1983年12月20日（83）法研字第30号）该项已废止，1993年《中国人民银行、最高人民法院、最高人民检察院、公安部关于查询、冻结、扣划企业事业单位、机关、团体银行存款的通知》，2015年中国银监会联合最高人民检察院、公安部、国家安全部印发关于“《银行业金融机构协助人民检察院公安机关国家安全机关查询冻结工作规定》的通知（银监发〔2014〕53号）”，确定查、冻、扣权力及权限。

根据中国人民银行关于发布《金融机构协助查询、冻结、扣划工作管理规定》的通知(银发〔2002〕1号)法律法规，各机关的权限如下：

有权查询单位：公安、检察院、法院、税务、海关、安全机关、监察机关（包括军队监察机关）、军队保卫部门、监狱保卫部门、走私犯罪侦查机关、审计、证监会、反洗钱行政主管部

门、外汇管理机关、军队审计机构、公证机构、民政部、人力资源和社会保障部门、反垄断执法机构。

有权冻结单位：公安、检察院、法院、税务、海关、安全机关、监察机关（包括军队监察机关）、军队保卫部门、监狱保卫部门、走私犯罪侦查机关、审计、证监会、反洗钱行政主管部门。

有权扣划单位：法院、检察院、海关、税务、监察机关。

具有完整的查询、冻结、扣划存款权力的部门

1.人民法院。公、检、法部门在查、冻、扣方面的基本法律依据是《民事诉讼法》、《刑事诉讼法》，其中《民事诉讼法》第221条规定“被执行人未按执行通知履行法律文书确定的义务，人民法院有权向银行、信用合作社和其他有储蓄业务的单位查询被执行人的存款情况，有权冻结、扣划被执行人的存款。”这里，人民法院所获得的是在义务人不主动履行的情况下，为保证生效法律文书得以履行而采取的强制执行措施，这里的法律文书包括人民法院通过审判程序作出的判决和无强制执行权的行政机关的生效法律文书。

2.税务部门。有关法律法规对此作出了明确规定。《税收征收管理法》（2015年修订）第十七条从事生产、经营的纳税人应当按照国家有关规定，持税务登记证件，在银行或者其他金融机构开立基本存款帐户和其他存款帐户，并将其全部帐号向税务机关报告。银行和其他金融机构应当在从事生产、经营的纳税人的帐户中登录税务登记证件号码，并在税务登记证件中登录从事生产、经营的纳税人的帐户帐号。税务机关依法查询从事生产、经营的纳税人开立帐户的情况时，有关银行和其他金融机构应当予以协助。第三十八条税务机关有根据认为从事生产、经营的纳税人有逃避纳税义务行为的，可以在规定的纳税期之前，责令限期缴纳应纳税款；在限期内发现纳税人有明显的转移、隐匿其应纳税的商品、货物以及其他财产或者应纳税的收入的迹象的，税务机关可以责成纳税人提供纳税担保。如果纳税人不能提供纳税担保，经县以上税务局（分局）局长批准，税务机关可以采取下列税收保全措施：（一）书面通知纳税人开户银行或者其他金融机构冻结纳税人的金额相当于应纳税款的存款；（二）扣押、查封纳税人的价值相当于应纳税款的商品、货物或者其他财产。纳税人在前款规定的限期内缴纳税款的，税务机关必须立即解除税收保全措施；限期期满仍未缴纳税款的，经县以上税务局（分局）局长批准，税务机关可以书面通知纳税人开户银行或者其他金融机构从其冻结的存款中扣缴税款，或者依法拍卖或者变卖所扣押、查封的商品、货物或者其他财产，以拍卖或者变卖所得抵缴税款。个人及其所扶养家属维持生活必需的住房和用品，不在税收保全措施的范围之内。

安全、军队保卫部门、监狱、走私犯罪侦查机关、反洗钱行政主管部门只有查询和冻结存款的权力

《中华人民共和国刑事诉讼法》的规定查询、冻结犯罪嫌疑人、被告人的存款、汇款、债券、股票、基金份额等财产。有关单位和个人应当配合。

《中华人民共和国反恐怖主义法》第五十二条 公安机关调查恐怖活动嫌疑，经县级以上公安机关负责人批准，可以查询嫌疑人员的存款、汇款、债券、股票、基金份额等财产，可以采取查封、扣押、冻结措施。查封、扣押、冻结的期限不得超过二个月，情况复杂的，可以经上一级公安机关负责人批准延长一个月。

《银行业金融机构协助人民检察院公安机关国家安全机关查询冻结工作规定》第三条 本规定所称“协助查询、冻结”是指银行业金融机构依法协助人民检察院、公安机关、国家安全机关查询、冻结单位或个人在本机构的涉案存款、汇款等财产的行为。

《国家安全部、人民银行关于国家安全机关向银行查询、要求停止支付个人在银行的存款事项的通知》（一）国家安全机关因侦查案件，需要向银行查询与案件直接有关的个人存款时，必须向银行提出县级和县级以上国家安全机关正式查询公函，并提供存款人的有关线索，如存款人的姓名、存款日期、金额等情况；经银行县、市支行或分行区办一级核对，指定所属储蓄所提供资料。

《中国人民银行条法司关于对军队保卫部门查询、冻结有关储蓄存款问题的答复》一、根据《中华人民共和国刑事诉讼法》第225条及其他有关条款的规定，军队保卫部门只能对军队内部发生的刑事案件行使侦查权；在行使侦查权时，可以对犯罪嫌疑人的存款进行查询、冻结，但不能扣划。

有一特殊情况：《反洗钱法》第二十六条规定“经调查仍不能排除洗钱嫌疑的，应当立即向有管辖权的侦查机关报案。客户要求将调查所涉及的账户资金转往境外的，经国务院反洗钱行政主管部门负责人批准，可以采取临时冻结措施。”

只具查询权力的部门

1. 公证机构

根据《司法部 中国银行业监督管理委员会关于在办理继承公证过程中查询被继承人名下存款等事宜的通知》内容，公证机构在办理继承公证过程中需要核实被继承人银行存款情况的，各银行业金融机构应当予以协助。

2. 审计机关

根据《中华人民共和国审计法》规定，第三十七条 ……审计机关经县级以上人民政府审计机关负责人批准，有权查询被审计单位在金融机构的账户。

审计机关有证据证明被审计单位违反国家规定将公款转入其他单位、个人在金融机构账户的，经县级以上人民政府审计机关主要负责人批准，有权查询有关单位、个人在金融

机构与审计事项相关的存款。由于该《条例》属于国务院行政法规，符合《商业银行法》关于查询单位存款的规定，因此，审计机关也有权查询单位存款。另外，按照《审计署、中国人民银行关于＜审计署、中国人民银行关于审计机关在审计执法过程中查询被审计单位存款问题的通知>适用军队审计机关的通知》（审法发〔1999〕35号）的规定，军队审计机关也可以查询单位存款。

3. 外汇管理机关

根据《中华人民共和国外汇管理条例（2008修订）》规定，第三十三条外汇管理机关依法履行职责，有权采取下列措施：

▶进入涉嫌外汇违法行为发生场所调查取证；

▶询问有外汇收支或者外汇经营活动的机构和个人，要求其对与被调查外汇违法事件直接有关的事项作出说明；

▶查阅、复制与被调查外汇违法事件直接有关的交易单证等资料；

▶查阅、复制被调查外汇违法事件的当事人和直接有关的单位、个人的财务会计资料及相关文件，对可能被转移、隐匿或者毁损的文件和资料，可以予以封存；

▶经国务院外汇管理部门或者省级外汇管理机关负责人批准，查询被调查外汇违法事件的当事人和直接有关的单位、个人的账户，但个人储蓄存款账户除外；

▶对有证据证明已经或者可能转移、隐匿违法资金等涉案财产或者隐匿、伪造、毁损重要证据的，可以申请人民法院冻结或者查封。

4. 军队审计机构

《军队审计条例》2017年1月1日起施行。

第十六条军队审计机构办理审计事项，经本审计机构主要负责人批准，有权依照法定程序查询被审计单位、被审计领导干部所在单位在金融机构的账户、存款和有关人员的公务卡；有证据证明被审计单位、被审计领导干部所在单位以个人名义在金融机构存储公款的或者有证据证明被审计单位、被审计领导干部所在单位有资金非正常转入个人账户的，经本审计机构主要负责人批准，有权依照法定程序查询被审计单位、被审计领导干部所在单位以个人名义在金融机构的存款以及军队单位非正常转入相关个人账户的资金。

第十七条军队审计机构办理审计事项，对审计对象和有关人员转移、隐匿、篡改、毁弃有关资料，或者毁损、转移、隐匿违反规定取得的资产的行为，有权予以制止，并记录相关行为。必要时，经办理该审计事项的军队审计机构主要负责人批准，有权封存有关资料和违反规定取得的资产；对其中在金融机构的存款和有价证券，需要予以冻结的，按照有关规定办理。

有关单位和个人应当配合外汇管理机关的监督检查，如实说明有关情况并提供有关文件、资料，不得拒绝、阻碍和隐瞒。

企业配合执法及注意事项

当金融企业遇到权力机关现场调查取证应注意什么呢？首先明确一点，依据《中华人民共和国民事诉讼法》第六十七条人民法院有权向有关单位和个人调查取证，**有关单位和个人不得拒绝**。人民法院对有关单位和个人提出的证明文书，应当辨别真伪，审查确定其效力。《公安机关办理行政案件程序规定》公安部令第149号第二十八条需要向有关单位和个人调取证据的，**经公安机关办案部门负责人批准，开具调取证据通知书，明确调取的证据和提供时限**。被调取人应当在通知书上盖章或者签名，被调取人拒绝的，公安机关应当注明。必要时，公安机关应当采用录音、录像等方式固定证据内容及取证过程。

了解了执法机关的取证法律依据，下面就是根据法律依据配合执法机关的取证内容。

执法机关需要呈请的资料

1.《立案决定书》、《调证通知书》、执法人员的双人双证（工作证）。

2.经办案部门负责人同意，法制部门审核，报县级以上公安机关负责人批准。

3.《协助查询、冻结财产通知书》。

4.持通知书和工作证件，到银行或者其他金融机构查询、冻结犯罪嫌疑人的存款、汇款、债券、股票、基金。

5.冻结存款、汇款期限为6个月的，冻结债券、股票、基金份额等证券的期限为二年。需要延期的，按规定办理延长手续。

6.不需要继续冻结犯罪嫌疑人存款、汇款时，制作《解除冻结财产通知书》，通知银行或者其他金融机构执行。

行政执法案件调查取证规则

行政执法案件调查取证有一定的办案流程和规则，各单位应当了解，并予以识别程序有效性。

调查取证工作应当遵守以下规定：

（一）**执法人员不得少于两人**，向当事人或有关人员**出示有效执法证件**；

（二）应做到用语规范、举止文明；

（三）向当事人**告知执法依据**和当事人应有的权利义务，并保障当事人的合法权利；

（四）执法人员如与当事人有直接利害关系的，**应当回避**；

（五）**不得滥用职权**，干扰或影响有关单位和个人的正常生产经营活动；

（六）为有关单位和个人**保守商业秘密和个人隐私**。

金融机构需要配合的方面

1.认真学习法律法规了解执法机关权力和边界，配合执法机关办案，保护公民个人隐私。

2.认真按照法律法规要求，留存执法机关调证程序、文件和数据。

3.建立数据泄露和溯源机制，如果发现互联网数据有泄露能够及时追踪回溯。

4.做好执法机关调证记录的保存，以备执法机关监督监察使用。

金融机构应当注意的事项

1.冻结存款、汇款、债券、股票、基金的次数根据案件需要确定，每次期限不超过6个月。

2.冻结涉案账户的款项应与涉案金额相当。

3.犯罪嫌疑人的存款、汇款、债券、股票、基金已被冻结的，不得重复冻结，但可以轮候冻结。

4.对冻结的债券、股票、基金份额等财产，法院应告知有权申请出售。

5.仅提供与案件相关的信息，最小化处理数据。

6.可以拒绝律师单独上门调取证据。

7.与国家安全、国防安全、刑事侦查、起诉、审判和执行判决等直接相关的必须予以配合。

8.遇到异地办理检查、查询，查封、扣押或者冻结与案件有关的财物、文件的，应当请办案人员持相关的法律文书、办案协作函件和人民警察证，与协作地公安机关联系，协作地公安机关应当协助执行（这一点特别重要）。

9.做好工作留痕。

另：若有发现公安机关在取证过程中有违法违规行为可以打12389 和在网站进行投诉举报。

https://www.12389.gov.cn/

附录：【主要法律、法规依据】

依据一：

人民检察院、公安机关根据侦查犯罪的需要，可以依照规定查询、冻结犯罪嫌疑人的存款、汇款、债券、股票、基金份额等财产。有关单位和个人应当配合。

犯罪嫌疑人的存款、汇款、债券、股票、基金份额等财产已被冻结的，不得重复冻结。（《刑事诉讼法》第144条）

依据二：

对查封、扣押的财物、文件、邮件、电报或者冻结的存款、汇款、债券、股票、基金份额等财产，经查明确实与案件无关的，应当在三日以内解除查封、扣押、冻结，予以退还。（《刑事诉讼法》第145条）

依据三：

公安机关根据侦查犯罪的需要，可以依照规定查询、冻结犯罪嫌疑人的存款、汇款、证券交易结算资金、期货保证金等资金，债券、股票、基金份额和其他证券，以及股权、保单权益和其他投资权益等财产，并可以要求有关单位和个人配合。（《公安机关办理刑事案件程序规定》第237条）

依据四：

向金融机构等单位查询犯罪嫌疑人的存款、汇款、证券交易结算资金、期货保证金等资金，债券、股票、基金份额和其他证券，以及股权、保单权益和其他投资权益等财产，应当经县级以上公安机关负责人批准，制作协助查询财产通知书，通知金融机构等单位协助办理。（《公安机关办理刑事案件程序规定》第238条）

依据五：

需要冻结犯罪嫌疑人财产的，应当经县级以上公安机关负责人批准，制作协助冻结财产通知书，明确冻结财产的账户名称、账户号码、冻结数额、冻结期限、冻结范围以及是否及于孳息等事项，通知金融机构等单位协助办理。冻结股权、保单权益的，应当经设区的市一级以上公安机关负责人批准。冻结上市公司股权的，应当经省级以上公安机关负责人批准。（《公安机关办理刑事案件程序规定》第239条）

依据六：

犯罪嫌疑人的财产已被冻结的，不得重复冻结，但可以轮候冻结。（《公安机关办理刑事案件程序规定》第242条）

依据七：

冻结存款、汇款、证券交易结算资金、期货保证金等财产的期限为六个月。每次续冻期限最长不得超过六个月。对于重大、复杂案件，经设区的市一级以上公安机关负责人批准，冻结存款、汇款、证券交易结算资金、期货保证金等财产的期限可以为一年。每次续冻期限最长不得超过一年。（《公安机关办理刑事案件程序规定》第243条）

依据八：

对冻结的债券、股票、基金份额等财产，应当告知当事人或者其法定代理人、委托代理人有权申请出售。

权利人书面申请出售被冻结的债券、股票、基金份额等财产，不损害国家利益、被害人、其他权利人利益，不影响诉讼正常进行的，以及冻结的汇票、本票、支票的有效期即将届满的，经县级以上公安机关负责人批准，可以依法出售或者变现，所得价款应当继续冻结在其对应的银行账户中；没有对应的银行账户的，所得价款由公安机关在银行指定专门账户保管，并及时告知当事人或者其近亲属。（《公安机关办理刑事案件程序规定》第246条）

安全实践

02 研究调研报告

2022年证券期货业软件供应链安全调研分析报告

文丨证券期货业软件供应链安全指南研究课题组

关于报告

致谢

感谢对本报告予以数据支持的证券期货业机构，在报告调研阶段，为业界输出丰富的软件供应链安全建设经验。

报告由来

兴业证券积极参与证标委2022年度证券期货业标准研究工作，牵头承接《证券期货业软件供应链安全指南》研究与编制。行业广泛调研是编制此标准过程中的重要环节，调研结果可帮助课题组充分了解证券期货业软件供应链安全的真实现状和趋势情况、软件供应链安全相关技术的发展和应用情况，在此基础上提出符合证券期货业软件供应链安全管理特点的标准。

课题组成员

兴业证券、上交所技术公司、上海期货交易所、华泰证券、国泰君安证券、海通证券、东方证券、奇安信

致谢

感谢以下人员为《2022年证券期货业软件供应链安全调研分析报告》的编制付出的辛勤劳动。

王玥、吴佳伟、张涛、谢冉、陈凯晖、马冰、邬晓磊、庄飞、康乐、王彤。

前言

软件是证券期货业数字化转型的重要元素之一，随着新兴技术的快速发展，复杂的软件供应链带来了一系列的安全问题，软件供应链安全攻击事件持续高发，网络安全整体防护难度越来越大，软件供应链安全成为业界关注焦点。

证券期货业软件供应链安全指南研究课题组于2022年7月启动《证券期货业软件供应链安全调研分析报告》的编制工作。课题组旨在通过本次调研与分析，了解证券期货行业软件供应链安全的真实现状与发展趋势，输出符合证券期货业特点的软件供应链安全标准，指导和规范证券期货业软件供应链的安全管理和建设工作。

本次调研通过发放调研问卷、企业访谈等多种方式，面向证券期货业的信息化负责人、网络安全负责人开展覆盖基础软件供应链安全管理、安全开发、技术保障等环节的调研工作。

本次调研共收集到85份有效问卷，调研对象涵盖核心机构、券商、基金、期货、金融科技公司，给予报告充分的数据分析基础。

根据调研结果，课题组形成了《证券期货业软件供应链安全调研分析报告》，本报告由六个部分组成，第一部分为概述；第二部分为调研基础情况分析；第三部分为软件供应链安全管理现状分析；第四部分为软件供应链安全开发现状分析；第五部分为软件供应链安全技术保障现状分析；第六部分为软件供应链安全发展与总结。

软件供应链安全涉及上下游众多组织机构，需要国家、行业监管部门、行业机构、信息技术服务公司的共同努力，提高证券期货业软件供应链安全管理水平。

概述

调研背景

资本市场是现代金融体系的核心和基石，随着国内金融供给侧改革的深入与资本市场对外开放力度的加大，数字化转型正成为证券期货业机构增强核心竞争力的重要突破口，为行业创新发展带来重大发展机遇。

纵观过去三十年，证券期货业金融科技的发展伴随着资本市场从无到有。证券期货业始终坚持创新驱动发展，不断将自身业务与新兴技术融合，利用全面的数据和丰富的应用模型提供更智能化、数字化、精准化的专业服务。

伴随着证券期货业相关业务操作流程逐渐数字化、网格化、智能化，业务所依赖的软件应用已经成为金融科技的基础组件。业务规模的不断扩大、业务场景的不断增加，软件逻辑复杂、“混源”开发、外部供应商多、快速交付等特征凸显，由此导致软件供应链的安全隐患与风险愈发突出。

2020年12月发生的SolarWinds事件与2021年发生的Log4j2漏洞都属于典型的软件供应链安全事件，体现了软件供应链安全攻击门槛低、隐蔽性强、影响范围广三大特点。Log4j2漏洞影响了包括证券期货业在内的众多金融机构，直接关系到证券期货业关键基础设施和重要信息系统的安全运行，给行业敲响了警钟。

为加强证券期货业标准研究，支持行业各领域创新发展，证标委开展了2022年度证券期货业标准研究课题工作，由兴业证券牵头承接《证券期货业软件供应链安全指南》课题的研究工作。课题组旨在通过本次调研与分析，借由《证券期货业软件供应链安全调研分析报告》来反映行业软件供应链安全的真实现状与趋势、软件供应链安全相关技术的发展和应用情况，客观地展现软件供应链安全能力建设中遇到的阻碍和困难，分享软件供应链安全能力建设思路，协助证券期货业持续完善网络安全体系化建设，避免软件供应链安全风险对证券期货业乃至资本市场带来危害。

软件供应链安全定义

GB/T 36637-2018《信息安全技术 ICT供应链安全风险管理指南》给出了对ICT供应链的界定，即网络产品和服务的供应链，满足供应关系通过资源和过程将需方、供方相互连接的网链结构，可用于将ICT产品和服务提供给需方。

国标《信息安全技术 软件供应链安全要求-草案》中定义软件供应链为：贯穿软件产品和服务的全生存周期，从供需关系的建立、软件设计开发、产品交付获取、运维使用，直至软件产品废止或服务中止。软件供应链是基于供需关系，由相关方为完成软件供应任务进行的一系列活动（任务）过程中构成的网链关系。

软件供应链安全指软件供应链上软件设计与开发的各个阶段中来自本身的编码过程、工具、设备或供应链上游的代码、模块和服务的安全，以及软件交付渠道和使用安全的总和。

调研问卷在设计的过程中，基于软件供应链安全涉及上述的各个方面，设计了21个调研问题，给予报告充分的数据调研范围。

研究方法

结合定量分析与定性分析方法，课题组对调研资料进行归纳与概括，对数据进行分析与汇总，从而展现当前证券期货业软件供应链安全整体发展状态。

- 调研问卷
- 定向走访
- 资料整合
- 专家分析

重要发现

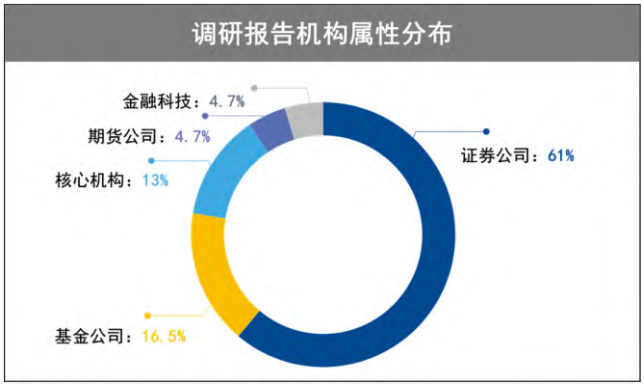
调研报告重要发现		
1.	调研基础情况分析	证券期货业软件应用以商业采购和联合开发为主，商采和联合开发的软件应用的占比超过 60%，自研软件占比较少。
2.		证券期货业软件应用的行业属性较明显，软件供应商存在共性。
3.		开源软件是证券行业软件开发过程中最基础的原材料，其代码自身的安全状况受到广泛关注。
4.	行业软件供应链安全管理现状分析	从安全管理角度看，64%的机构将软件供应链安全管理纳入本单位信息安全管理职能，由研发团队、运维团队、安全团队共同负责落地执行的相关工作。
5.		超过 94%的机构已制定软件供应链安全相关管理制度并不同程度的开展了软件供应链安全管理工作，仅个别机构暂未开展相关工作。
6.		外部软件供应商是软件供应链上的薄弱环节，是攻击者突破的重点。绝大部分机构在采购前与软件供应商制定了相关约束机制，仅个别机构暂未开展相关工作。
7.		46%的机构存在软件供应商远程接入的情况，所有机构都采取了安全管控措施。
8.	行业软件供应链安全开发现状分析	仅有 15%的机构自研软件的比例占全部软件的 50%-70%，以行业核心机构为主，包括少量的证券公司。
9.		软件开发过程中，仅有少量行业机构实践了软件安全开发生命周期（SDL）模型。
10.	行业软件供应链安全技术措施分析	绝大部分机构已具备软件供应链安全保障机制，以渗透测试与漏洞扫描为主，其次是主机 HIDS、威胁情报、源代码安全审计、开源软件漏洞检查。
11.		软件供应商数据泄露问题、软件供应链威胁情报、信创软件、软件供应链断供等问题同样备受行业机构所关注。

调研基础情况分析

本章节主要分析与探讨调研报告涉及的调研范围、调研机构属性等。

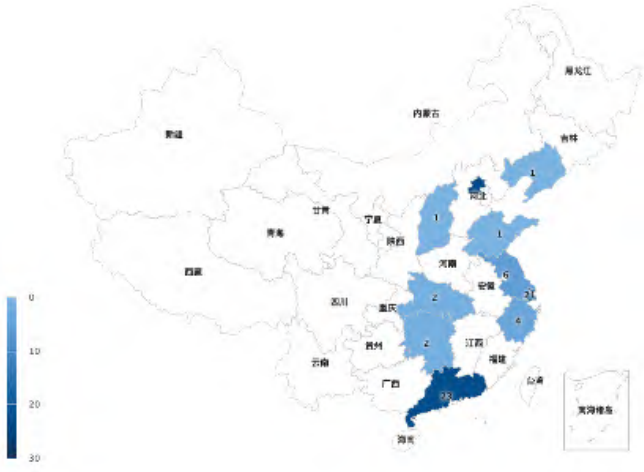
机构属性分布

本次调研总共涉及85份样本。从机构性质分布来看，本次调研证券公司占比最多，达61%，其次为基金公司和核心机构，分别占16%和13%。此外，期货公司、金融科技公司均有参与。调研总体的样本量较充分，机构类型全面。



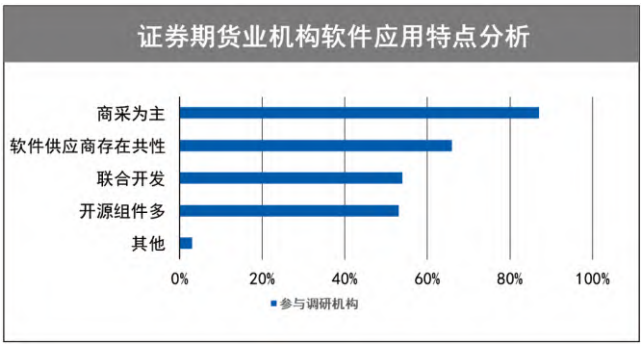
机构所在区域

本次参与调研的机构分布在10个省市自治区，其中，华北（以北京为主）、华南地区（以广东为主）、华东地区（以上海为主）样本量较多。



证券行业特点

本次调研中发现，证券期货业机构的软件应用以商业采购和联合开发为主，大部分机构商采和联合开发的软件应用的占比超过60%，自研软件占比较少。同时，由于行业软件应用的行业属性较明显，包括OA系统、邮件系统、集中交易系统等选取的软件供应商具备很强通用性。开源软件是证券行业软件开发最基础的原材料，其代码自身的安全状况受到广泛关注。



行业软件供应链安全管理现状分析

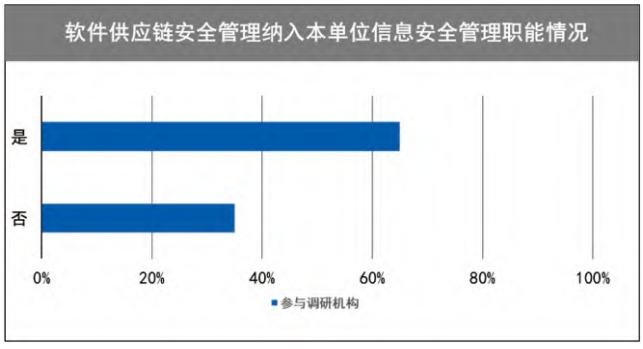
软件供应链涉及面广，安全风险类型多，安全问题引发的危害性大，需要从各机构的IT管理层加强对供应链安全的管理，多部门共同努力，不断提高和健全软件供应链安全管理保障体系。

本章节主要分析与探讨证券期货业机构目前对于软件供应链安全管理的现状。

组织机构

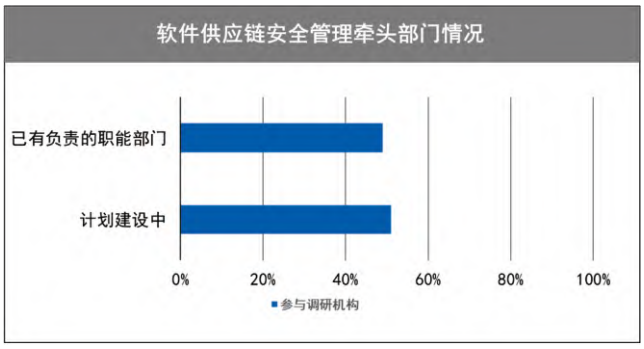
1.软件供应链安全管理情况

本次调研中已有65%的机构将软件供应链安全管理纳入本单位信息安全管理职能，开展供应链相关安全管理工作，这些机构以证券公司为主。35%的机构暂未落实软件供应链安全管理工作。



2.软件供应链安全管理牵头部门

通过对已经开展软件供应链安全管理工作的65%机构深入调研，结果显示其中已有49%的机构有专门负责软件供应链安全管理的职能部门，主要以信息技术中心牵头，51%的机构正计划建设相关职能部门。



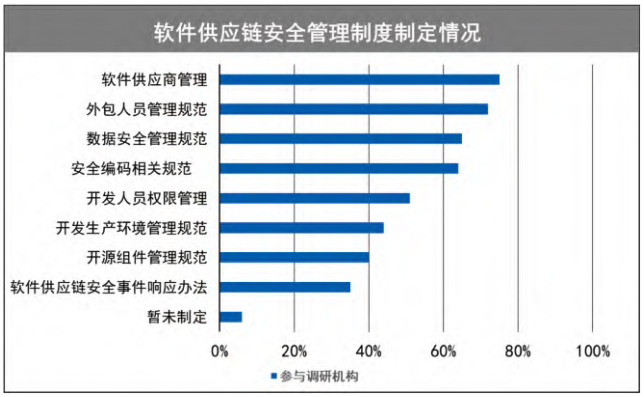
3.软件供应链安全管理执行部门

调研结果显示，软件供应链安全的执行部门多采用成立虚拟团队的方式，由研发团队、运维团队、安全团队共同负责落地执行的相关工作。部分机构的IT治理团队、采购部门、质量控制部门也会参与到具体的工作中。

管理制度

1.软件供应链安全管理制度

调研结果显示，超过94%的机构已制定软件供应链安全管理制度，各机构重点关注软件供应商管理、安全编码规范、开发人员权限、数据安全管理规范、外包人员管理规范，其次是开源组件管理、生产开发环境管理、安全事件应急响应。仅个别机构暂未制定软件供应链安全相关的管理制度。

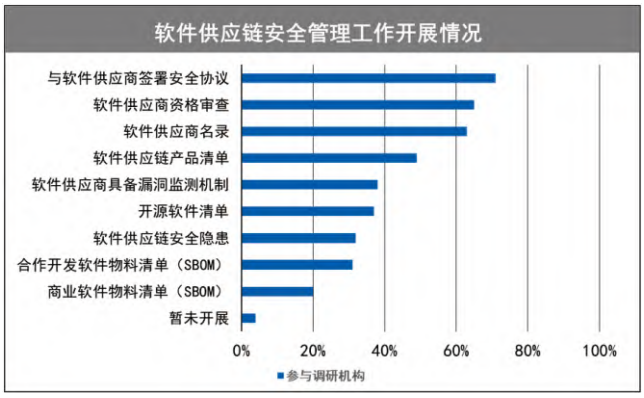


安全管理

1.软件供应链安全管理工作

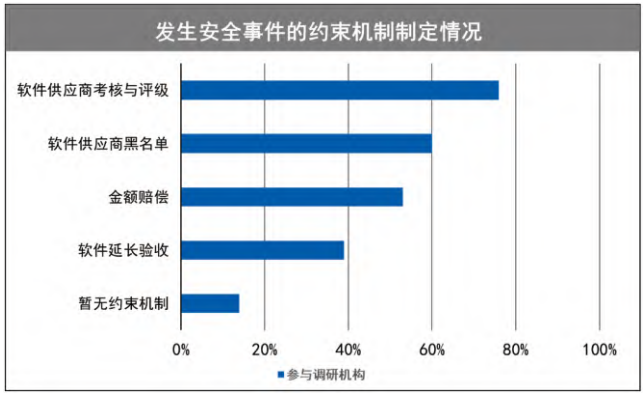
调研结果显示，超过95%的机构不同程度的开展了软件供应链安全管理工作。各机构重点关注于加强软件供应商的管理，制定本机构软件供应链名录、审核软件供应商资格审查、签署安全协议的机构超过60%。

软件应用的资产管理逐渐被关注，如建立软件产品清单、产品安全隐患清单、使用的开源软件清单、外包软件物料清单（SBOM）、商采软件物料清单（SBOM）等。同时近40%的机构要求软件供应商具备软件供应链漏洞监测机制。仅个别机构暂未开展软件供应链安全的管理工作。



2.安全事件约束机制

外部软件供应商提供的产品是软件供应链上的薄弱环节，是攻击者突破的重点，在采购商业软件与外包开发之前，应与软件供应链明确安全事件发生后的约束机制，明确供应商的安全责任和义务。调研结果显示，绝大部分机构在采购前与软件供应商制定相关约束机制，当软件供应商出现网络安全事件时及时采取措施。76%的机构与软件供应商制定考核与评级机制，60%的机构已形成内部的软件供应商黑名单机制，53%的机构与软件供应商制定赔偿机制。仅14%的机构未开展任何软件供应商约束机制方面的工作。

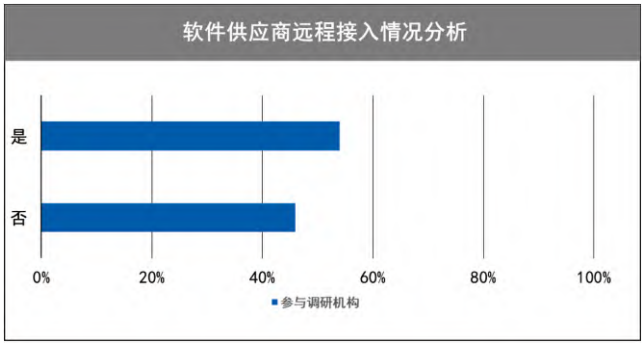


远程接入管理

目前很多软件供应商的网络安全建设相对滞后，历年网络安全攻防演习中发生过多起利用软件供应商远程接入通道攻击防守方成功的事件。

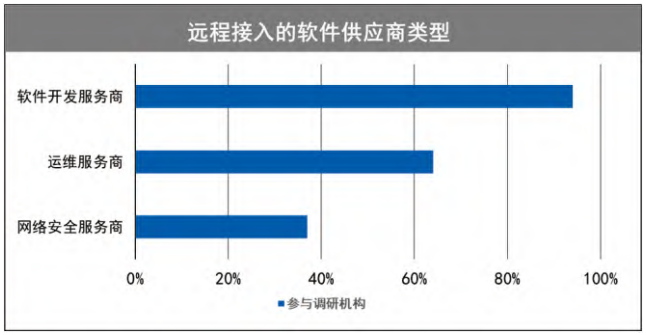
1.远程接入情况

调研结果显示，54%的存在提供远程接入通道给软件供应商的情况。本章后续调研分析将基于54%存在软件供应商远程接入的机构进行统计。



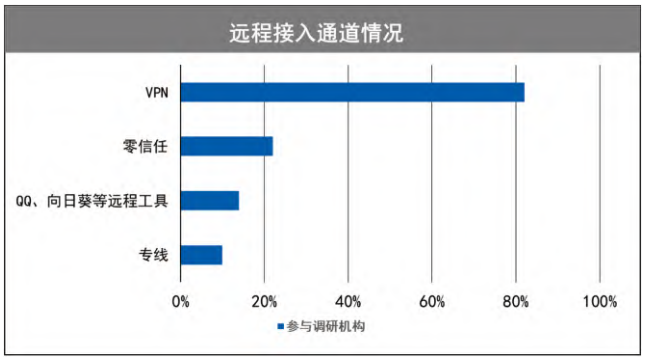
2.远程接入类型

调研结果显示，46%的机构存在软件供应商远程接入的情况，其中93%的机构有合作的外部软件开发服务商远程接入，63%的机构有合作的运维服务商远程接入，36%的机构有合作的网络安全服务商远程接入。



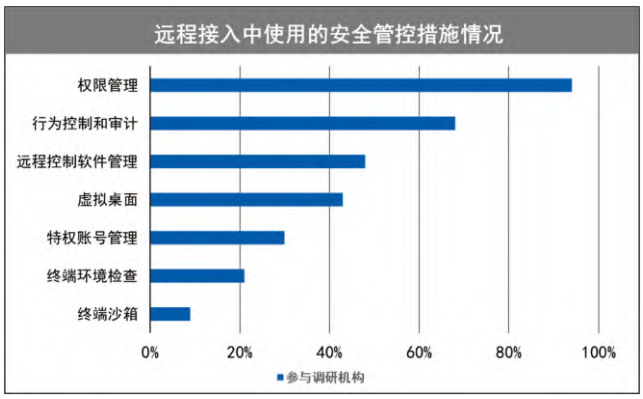
3.远程接入管理

调研结果显示，超过80%的外部软件供应商通过VPN的方式远程接入，21%的机构已采用零信任方式实现外部软件供应商远程接入，少数机构的外部软件供应商通过专线接入，个别机构提供QQ远程、向日葵等远程工具。



4.安全管控措施

调研结果显示，外部软件供应商远程接入各机构的过程中，所有机构都采取了安全管控措施，大部分机构采取多种措施结合的方式对外部软件供应商进行管理。其中超过87%的机构采取了人员权限管理、人员行为控制和审计方面的管控措施，48%的机构对远程控制软件（如TeamViewer、向日葵等）进行管控，30%的机构对特权账号进行管理，少部分机构采取终端环境检查、终端沙箱对接入终端进行强管控。



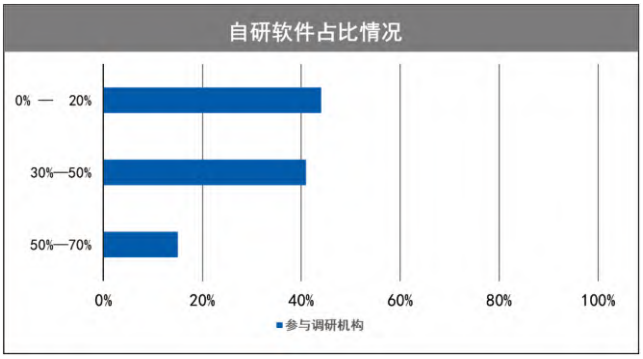
行业软件供应链安全开发现状分析

证券期货行业机构主要以外采商业软件、联合开发为主，部分软件自研的模式。软件开发阶段安全仍需关注，主要涉及软件产品的开发、集成、构建等环节。

本章节主要分析与探讨证券期货业机构目前对于自主开发的软件应用的安全现状。

自研软件情况

调研结果显示，仅约15%的机构自研软件的比例占全部软件的50%-70%，41%的机构自研软件的比例占全部软件的30%-50%，43%的机构自研软件的比例占全部软件的20%以下。

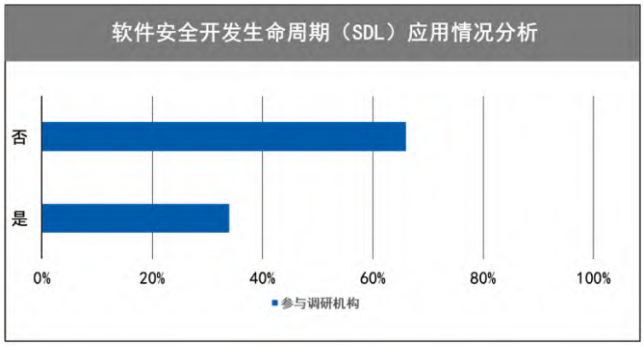


SDL应用情况

软件安全开发生命周期（SDL），是一个在帮助开发人员构建更安全的软件和解决安全合规要求的软件开发过程，旨在将安全集成在软件开发的每一个阶段，以减少软件中漏洞的数量并将安全缺陷降低到最小程度。

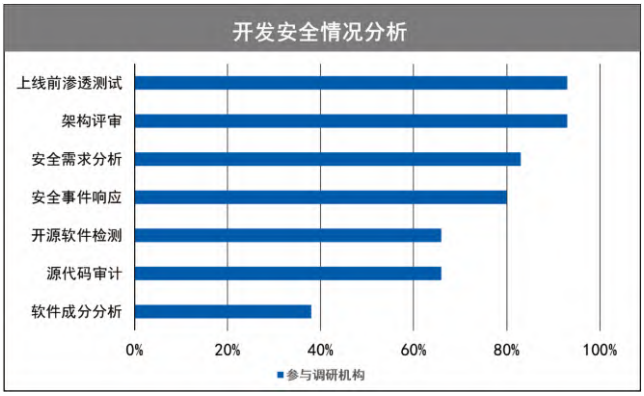
调研结果显示，仅有34%的机构在自研软件的开发过程中应用SDL模型，超过66%的机构暂未在软件开发的各个环

节中考虑安全活动。



开发安全情况

调研结果显示，软件研发的设计阶段，绝大部分机构开展安全需求分析、架构评审，仅有34%的机构通过威胁建模分析软件的安全威胁。软件研发的编码阶段，超过65%的机构采用源代码审计、开源组件检测等措施，37%的机构具备软件成分分析措施。软件上线之前，93%的机构对软件应用开展渗透测试。

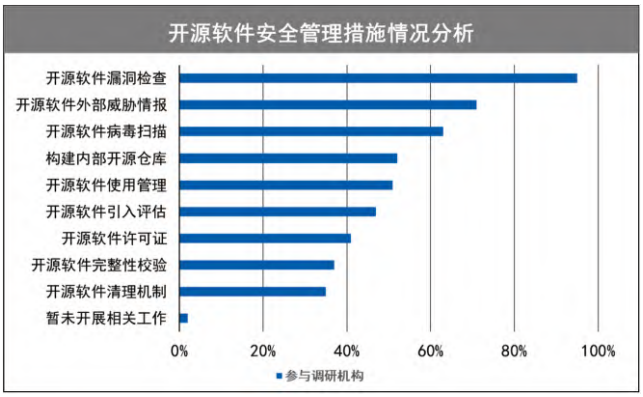


行业软件供应链安全技术措施分析

开源软件漏洞、供应链投毒、控制软件下发途径等问题是软件供应链安全问题增长的重要因素，需要加强全链条安全管控。本章节主要分析与探讨证券期货业机构目前使用的软件供应链安全技术措施的现状与不足。

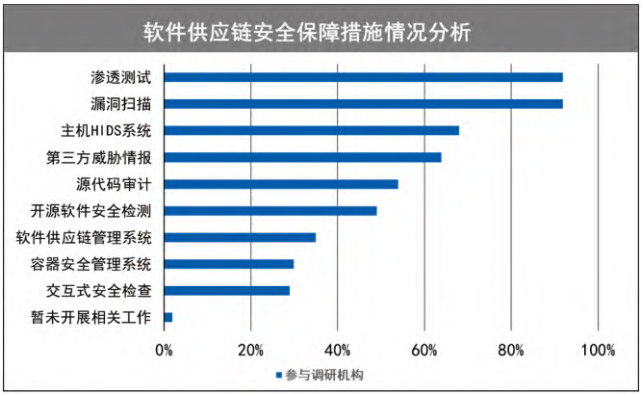
开源软件安全管理措施

开源软件安全风险是当前企业软件开发中亟待解决的首要问题，50%的机构已开展不同程度的开源软件安全管理工作。通过对各机构关注的开源软件风险管理的重点进行调研，从中发现各机构最重视的是开源软件漏洞检查、开源软件漏洞预警、开源软件病毒扫描三个方面的治理工作，分别有95%、71%、63%的关注度。另外开源软件引入来源、开源软件使用管理、内部开源软件仓库、开源软件引入评估、开源软件完整性校验、开源软件清理机制均是各机构关注的方面。

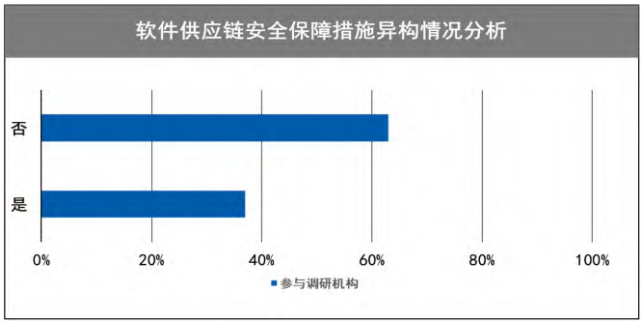


供应链安全保障措施

证券期货业对软件供应链安全高度重视，调研结果显示，98%的机构已开展软件供应链安全保障工作。其中传统的安全保障措施，渗透测试与漏洞扫描占比最高，达到92%。主机HIDS、威胁情报的使用均超过64%。源代码安全审计、开源组件安全检测的使用均超过50%。仅部分机构采取了交互式安全检查、容器安全管理平台、软件供应商管理平台作为安全保障措施。

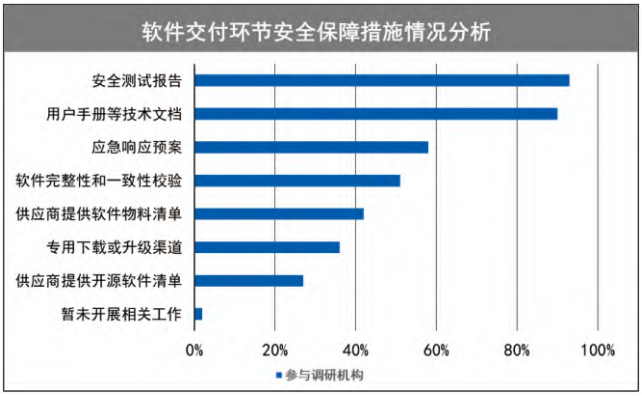


调研结果显示，37%的机构在软件供应链安全保障措施方面考虑异构部署，从而保障威胁检测的精准度和安全措施保障的高可用性。



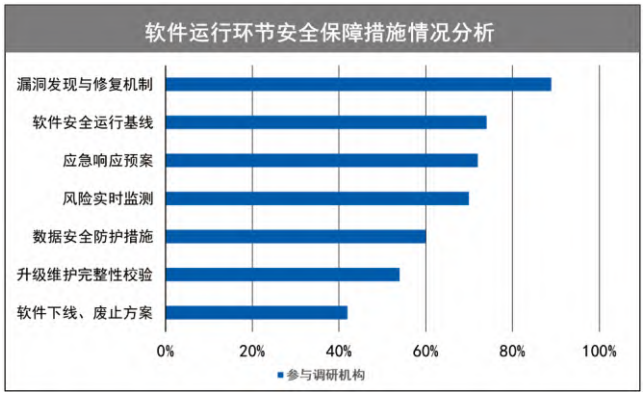
软件交付环节保障措施

调研结果显示，超过90%的机构要求软件供应商在交付软件应用之前提交软件安全测试报告、用户手册等技术文档。58%的机构要求软件供应商具备应急响应预案和相关措施。51%的机构在软件交付时进行完整性和一致性校验。42%的机构已形成或要求软件供应商提供软件物料清单。30%的机构具备专门的软件下载或升级渠道。仅27%的机构已形成或要求软件供应商提供开源软件物料清单。



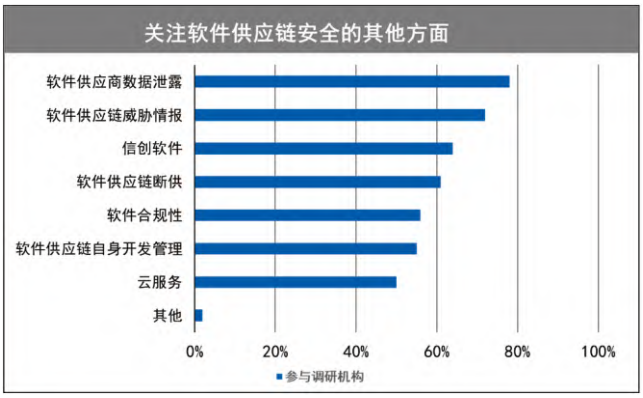
软件运行环节保障措施

调研结果显示，软件应用运行的过程中所有机构都应用了安全保障技术措施，超过75%的机构在漏洞发现与修复、软件安全运行配置基线、安全风险监控与防护、应急响应方面开展了相关工作。60%的机构具备数据安全相关措施。54%的机构在软件升级、维护时进行完整性校验。43%的机构具备软件下线、废止方案。



关注的其他方面

调研结果显示，在软件供应链安全的其他方面，超过70%的机构关注于软件供应商数据泄露问题、软件供应链威胁情报。超过60%的机构关注于信创软件、软件供应链断供问题。超过50%的机构关注于供应商自身的开发安全管理、软件合规、云服务。



行业软件供应链安全总结与建议

报告总结

通过调研分析，课题组看到证券期货行业绝大部分机构均不同程度的开展软件供应链安全相关工作，软件供应链安全的重要性已经逐步成为行业各方共识。安全管理方面，由多个职能部门共同负责落地执行的相关工作，制定软件供应链安全管理制度，着重加强对软件供应商、开发人员、数据安全、外包人员方面的管理。安全技术措施方面，几乎全部行业机构都已开展软件供应链安全保障工作，重点关注开源软件、软件应用运行过程的安全保障。

但另一方面课题组也看到，虽然大多数行业机构目前对于软件供应链安全已付诸相关行动，但覆盖范围尚且不够。安全管理方面，行业机构对软件供应链安全的管理高度不够，部分行业机构未将软件供应链安全管理纳入本单位信息安全管理职能，缺乏软件供应链安全管理牵头部门。软件应用的资产管理不足，缺乏对软件产品清单、产品安全隐患清单、软件物料清单（SBOM）等方面的管理。安全开发方面，自研软件的安全与开发割裂，对安全开发的认知不够。安全技术措施方面，大部分机构采用渗透测试、漏洞扫描等传统技术手段，开源组件、源代码、软件供应商等方面的技术手段不足，软件交付环节的保障措施不足。

行业安全建议

1.国家监管

建议国家和行业监管部门继续完善和制定软件供应链安全相关的政策、标准和实施指南，建立长效工作机制。建立国家级、行业级软件供应链安全风险分析平台，具备系统化、规模化的软件源代码缺陷和后门分析、软件漏洞分析、开源软件成分及风险分析等能力，及时发现和处置软件供应链安全风险。

2.行业机构

建议证券期货业行业机构从以下五方面加强软件供应链

安全管理工作：

⑴安全管理方面

建立供应链安全管理制度，落实供应链安全管理部门和安全责任人，加强对供应链安全管理资金、人员、权限等资源的保障。

⑵软件供应商管理方面

选择有实力、有能力、保障有力的供应商，防止由于政治、外交、贸易等非技术因素导致产品和服务供应中断。

在采购网络产品和服务时，应与供应商签订安全保密、安全约束机制等有关协议，协议内容应包括安全职责、保密内容、奖惩机制、有效期等；或者，要求供应商签署承诺书，明确供应商的安全责任和义务，由供应商承诺不非法获取用户数据、控制和操纵用户系统及设备，不利用用户对产品的依赖性谋取不正当利益。

要求厂商和供应商提供软件物料清单（SBOM），并与其签订安全责任协议，要求其对软件物料的安全性负责并提供后续的技术支持服务；对于运行重要业务的软件系统，应使用合适的检测工具验证厂商和供应商所提供的软件物料清单（SBOM）的正确性，确认软件的组成成分及安全风险状况；在软件系统日常运行过程中，应基于软件物料清单（SBOM）持续跟踪软件物料相关的威胁情报，及时采取安全措施，消减相关安全风险。

⑶软件供应链各类渠道方面

在软件供应链中，存在着各类软件代码、组件、补丁、成品由软件供应链的上游向下游转移的渠道。由于软件行业具有的互联网特性，许多关键渠道的运行依赖互联网，使得这些渠道的安全受到网络攻击的威胁，在被攻击后可以成为网络攻击向供应链下游扩散的渠道，同时渠道本身也有怀有恶意的可能性。这其中负责软件交付的集中式软件分发渠道直接影响大规模的用户，显得尤为重要。建议各机构加强针对软件供应链上的各类渠道设计安全防护措施，并使得软件供应商和用户能够识别具有恶意的渠道。

⑷安全检测方面

建议提升软件供应链安全技术检测能力。加强软件供应链安全生态协同管理机制。提升包含软件供应链各阶层的软件供应商和各类渠道在内的管理软件供应链风险的统一管理能力及技术手段。推动构建安全可靠的软件供应链可信组件资源平台，实现软件供应链资源的可控。采用专业工具和服务实现对软件产品的代码审查和缺陷检测，加强对新代码防护手段和技术的应用探索。提升对软件源代码的审计工具能力，加强软件安全性深度测试；针对开源最难进行的漏洞评估和验证，提升开源组件安全检测能力。

⑸应急响应方面

建立合理的设计框架和资产管理能力，对输入输出、网络传播等敏感过程的实时监控、对供应链各个环节的基础资产如APP、服务端软件进行盘点。安全团队也尽量多地对各个维度的行为和数据进行记录，对海量数据进行存储、分析、挖掘和关联，以便更好地发现并解决安全问题。

3.软件供应商

建议软件产品厂商提高安全责任意识，严控产品安全质量；建立清晰的软件供应链安全策略，明确相关的管理目标、工作流程、检查内容、责任部门等；严控上游，尤其重点管控开源软件的使用，建立开源软件资产台账，采用开源安全治理工具，持续监测和消减其安全风险；严控自主开发代码的质量，采用软件源代码安全分析工具，持续检测和修复软件源代码中的安全缺陷和漏洞；建立完善的产品漏洞响应机制，包括产品漏洞信息的收集、漏洞报告渠道的建立和维护、漏洞补丁的开发和发布、客户端漏洞应急响应和修复支持等。

课题组工作计划

为降低证券期货业软件供应链安全风险，并指导和规范证券期货业软件供应链的安全建设和管理工作，下一步课题组将站在证券期货行业角度，编写证券期货业软件供应链安全指南，通过该行业标准实现对证券期货业软件供应链安全管理规范化。

证券行业应用安全运营托管服务的可行性研究和总体实施建议

文｜李维春、刘亦翔、程度、刘敏杰

李维春 国投证券股份有限公司　　刘亦翔 国投证券股份有限公司
程　度 北京升鑫网络科技有限公司　　刘敏杰 深信服科技股份有限公司

摘　要： 新时代、新环境下网络安全工作面临巨大的挑战，在投入有限、人员流动频繁的前提下，如何有效地开展安全运营、保证各类安全控制措施的有效性，是行业机构面临的普遍问题，而安全运营托管是个可行的解决方案。本文针对安全运营托管的背景、行业机构的需求、安全运营托管的可行性进行了分析，并提出了整体的安全运营托管实施方案。

关键字： 安全运营托管现状、安全运营托管

课题背景及意义

近年来，以总体国家安全观为指导，国家网络安全工作顶层规划与总体布局不断完善，网络安全“四梁八柱”基本确立。相继出台了网络安全法、数据安全法、个人信息保护法、《关键信息基础设施安全保护条例》等网络安全法律法规，印发了《网络安全审查办法》《云计算服务安全评估办法》等部门规章和规范性文件，国家网络安全工作的政策体系框架基本形成。网络安全总体工作的政策保障在快速成形，本质上是我国数字化进程的加速推进，广大人民群众对网络安全、数据安全、个人信息安全的关注度与日俱增。

在这个大背景下，证券行业在数字化转型发展过程中所面临的网络安全风险将会持续扩大，存在局部网络安全风险向系统性社会风险转化和蔓延的问题。另外，证券行业机构的网络安全保障体系和能力的建设是国家安全体系和能力建设的重要组成部分。当前我国证券行业面临的网络安全问题有以下两点：

第一，安全建设水平差异较大。目前各单位的信息化水平差异较大，网络安全防护水平参差不齐。总体来说，受制于编制、资金、意识等条件的约束，网络安全水平层次不齐，缺乏一致、良好的网络安全基础设施，并且难以在短期内全面实现网络安全基础设施的改造升级。

第二，常态化网络安全感知和应急能力不足。网络安全的本质是对抗，证券行业单位在攻防两端对抗中处于“能力不对等”的处境。以国家大型实战攻防演习活动为例，绝大多数参与企业单位在演习期间，通过加大网络安全运营人员与设备的投入，并在演习期间采取特定的应对措施，在短时间内使其网络安全防御能力得到了全方位大幅度提升；但当攻防演习活动结束后，伴随着网络安全专家和临时租借的安全防护设施离场，安全防护水平又由战时的“铜墙铁壁”回到了平时的“焦头烂额”的基础防护水平，安全感知能力和应急反应速度无法与“战时”相提并论，无法做到24小时全天候对安全事件进行全面准确的监测和发现，并及时开展应急处理措施。

在这样的大背景下，如何更有效地、以更高投入产出比的方式开展安全建设和安全运营，是证券行业机构普遍面临的问题。

安全运营托管服务的可行性研究

安全运营托管服务简介

安全运营托管服务 (MSS，Managed security Service) 是将自身的网络安全托管给网络安全服务供应商的一种服务。此类服务的供应商是安全运营托管服务供应商 (MSSP，Managed Security Service Provider)，安全运营托管服务模式起源于 1990 年代中后期，当时互联网服务供应商向客户出售防火墙设备，并通过拨号连接管理客户的防火墙，并收取额外费用。目前企业通过采购安全运营托管服务，使用安全运营托管服务供应商构建的SOC（安全运营中心），企业可快速扩展自身的安全能力，实现预期的安全效果。

Gartner对安全运营托管服务的定义是：

· 7*24小时远程监控安全事件及相关安全数据源；

· 管理和控制安全相关的技术和产品；

· 远程的SOC服务，并不是通过驻场或者远程的一对一的

安全服务。

安全运营托管服务的核心服务内容是对安全事件的监控和安全事件的响应以及合规方面的报告。除此之外还可能包括以下方面的内容：

· 安全设备管理，如：防火墙、入侵检测系统（IPDS）、终端管理（EPP）、终端检测与响应（EDR）、安全应用网关（SWG）、安全邮件网关（SEG）等；

· 事件响应服务（包括远程服务和现场服务）；

· 漏洞评估和漏洞管理服务；

· 威胁情报服务；

一般认为，MSS会给甲方企业带来如下价值

1、降低安全运营成本

与大多数托管服务提供商一样，MSS可以带来规模经济效应，因此能够帮助企业降低安全运营工作的成本投入。同时，选择MSS可以将大部分安全预算由资本支出转化为运营支出，这可以为组织提供某些成本优势，并在预算编制过程中减少了变数。

2、提供不间断的安全服务和更强大的安全运营能力

大多数组织（尤其是中小型行业单位）都无力打造全天候运作的安全运营中心。但是由于具有规模效应，MSSP可以建立更完善的运维服务体系；MSSP通常可以更轻松地应对人员流动，保障服务的可靠性和稳定性。如果聘请一家成熟的MSSP，组织可以大幅提升许多方面的能力，例如在威胁检测和响应方面，企业可以更好地深入了解新旧威胁以及如何检测和防御这些威胁；MSSP处理过大量的安全警报和违规事件，因此它们往往更有经验，在处理突发性安全事件时往往会更加迅速；MSSP通常更积极地试用包括人工智能在内的新型安全工具和技术，这些创新工具和技术有可能带来更好的安全防护效果。

3、更准确了解和符合合规监管要求，更好的第三方证明

由于拥有更广泛的安全运营经验，许多MSSP能够更全面了解全球和国家层面的不同法规标准和监管要求，包括GDPR、HIPAA以及我国的网络安全法、数据安全法等。网络保险提供商、业务合作伙伴以及客户都会需要组织能够提供满足某些合规要求、落实网络安全标准的证明，MSSP代表了可靠、专业的第三方机构，它们可以帮助企业证实自己在安全保障方面的工作与能力。

4、提供更多的安全专家资源

MSSP通常更有能力雇佣网络安全人才，它们有广泛的合作伙伴和经济能力。考虑到目前网络安全人员的缺口巨大，通过与MSSP合作可能是组织获得所需安全专业人才的唯一途径。

行业现状调研分析

网络环境复杂性的增强，安全威胁攻击手段的提升使网络空间的攻防战愈发激烈，传统的人工应对方式已经完全不足以解决当前数量巨大、变化多端的威胁信息和夜以继日地攻击。通过人力完成对这些网络事件的应对，已经变得愈发困难。

目前行业内大部分中小证券威胁管理机制偏弱，且证券行业网络安全建设主流方案为部署大量的基于单点工作机制的网络安全防护产品。这些产品都是基于单点的工作机制，网络安全技术之间的整合度低、联动性不强，使得在应对网络安全威胁时不能高效率的处理事件，难以从海量的安全数据中有效发现和响应安全事件。在安全人员层面，行业内大多数中小证券正编安全人员偏少，只有1-2人，往往只能通过外包来解决安全威胁处置的需求，但由于外包人员能力有限、流动性大，正编人员较多的精力在指导外包人员成长，导致威胁管理领域投入精力有限，从而在威胁管理上效果也比较有限。

同时，我们发现在证券基金行业内大部分中小规模的经营机构采用的安全服务主要是通过人工定期进行交付，安全服务内容聚焦在传统安全服务，如漏洞扫描、基线核查、渗透测试等；并且常规安全服务缺乏有效的工具和流程支撑，对安全事件的感知局限于事后的处置和溯源加固，无法做到事前的主动发现和预警，也缺乏有效的安全事件应急预案和事件快速响应机制，在安全事件发生时无法做到主动发现和快速止损。

针对中小证券的安全运营托管模式，课题组在行业内开展了一次问卷调查，部分问题和数据摘录如下。

第3题：请问您所在公司，当前安全人员（正编）规模；如果有兼职或一人多岗情况，可按人员投入比例折算选择

选项	小计	比例
无专职安全人员	3	6.25%
1-3 人	22	45.83%
4-6 人	17	35.42%
7-10 人	3	6.25%
10-15 人	2	4.17%
16 人及以上	1	2.08%

第4题：请问您所在公司，常驻的安全服务（外包）人员规模

选项	小计	比例
无安全服务外包人员	26	54.17%
1-3 人	18	37.5%
4-6 人	2	4.17%
7-10 人	2	4.17%
10-15 人	0	0%
16 人及以上	0	0%

第7题：如果监管不明确反对安全服务托管，你会考虑将部分安全运营工作常态化地托管给“云服务商”吗？

云服务商的意思就是通过专家、系统工具，以远程形式完成安全服务，要么是专家远程开展工作，要么是把一部分安全数据交给非本地的系统、专家去处理。

选项	小计	比例
会	28	58.33%
不会	20	41.67%

第9题：为什么你觉得值得考虑“云服务商”的托管方式？

选项	小计	比例
招人太难了	16	57.14%
外包人员流动性大	14	50%
云托管方式性价比高	15	53.57%
其他	4	14.29%

受调查的单位有58%对安全运营托管服务持一半以上的开放态度，另外42%的受调查单位对安全运营托管服务的担心还是在于是否符合法律法规要求、数据安全风险是否可控、安全响应效率是否及时；如有手段可以较好地解决这些问题，证券行业采用安全运营托管服务的方式可以很好地提升安全运营的效率和质量。

证券行业应用安全运营托管服务的可行性研究

1. 必要性研究

数字化业务转型加快了企业发展的步伐，也滋生了更多的网络安全隐患。然而，由于许多企业缺乏所需的专业技能和资质能力，在开展网络安全建设时面对多种的安全挑战，同时还要面临着IT预算不断收紧等问题。

将企业安全建设和运营中的部分工作交给专业化服务公司，采用外包的模式，引入专业的MSSP，是企业网络安全建设的一种有效模式，而外包模式在整个IT行业都是一种常态。Forrester Research副总裁兼首席分析师Jeff Pollard表示：如果组织因为网络安全团队没有足够的时间、人才或能力来合理完成某些安全工作时，就应该尽快考虑并选择网络安全外包服务。此外，如果组织认为一些安全任务（比如评估内部威胁）不该由内部安全团队来处理，也可以考虑聘请安全托管服务来完成这些任务。

课题组在研究中发现，目前很少有组织会将整个安全建设和运营工作外包出去。大多数组织都在寻求混合模式：部分安全任务外包出去，部分留在内部自行管理。在混合模式下，内部安全主管、经理和高级专家通常处理战略性任务，而安全托管服务则更多负责执行等专业事务性任务。如果选择驻场的安全运营托管服务，则面临着如下挑战：

· 服务人员稳定性差：安全服务人员在甲方工作1-2年后，能力通常会获得较大的进步，现有的安全服务合同已经无法支撑其当下的期望，就会产生人员流动；研究发现行业内驻场安全服务人员平均服务周期为1.4年。

· 驻场安全运营服务人员教育成本高、有效利用率低：无论是有经验的安全服务人员，还是一名新手，在其进入甲方后通常都需要2-3个月的时间才能完全适应组织的文化、沟通方式、网络和系统架构等，留给其发挥价值的时间通常只有1年左右的时间。甲方人员需要耗费大量的时间精力在培训、管理驻场外包人员，导致真正花费在提升运营能力的时间精力极其有限。

· 高质量的服务人员数量少、招聘难度大：高素质、高质量的安全服务人员往往在服务商中承担更高层次的专家岗位，流动性低，导致甲方所需要的高质量的安全服务人员数量少、招聘难度大。甲方人员需要耗费大量的时间精力在人员招聘上，导致真正花费在提升运营能力的时间精力极其有限。

· 随着国家对资本市场的重视和不断投入，未来与国外资本市场的对接将是大势所趋，证券基金行业将很快进入需要7*24安全运行和保障的阶段，这对安全运营的挑战（包括人员编制、预算投入、响应支持、人员能力）将会显著提升。

· 安全工具繁多、人员缺少：随着安全体系建设要求的提高、攻防对抗激烈程度的加剧，安全运营所需的工具也逐渐增多，安全运营所需的人力数量也快速提升，然而由于上述安全运营服务人员的种种问题，放大了人员缺口矛盾。

结论：以上形势和挑战迫使甲方组织必须选择驻场安全运营服务之外的实施方案，安全运营托管服务是目前看来最佳的解决方案。

2. 合规性研究

（1）《网络安全法》《个人信息保护法》《数据安全法》合规性研究

出处	法条	法条内容
网络安全法	第十条	建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。
	第二十二条	网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。 网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。 网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

出处	法条	法条内容
网络安全法	第二十五条	网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。
	第四十二条	网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。 网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
	第四十五条	依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。
个人信息保护法	第五十一条	个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： （一）制定内部管理制度和操作规程； （二）对个人信息实行分类管理； （三）采取相应的加密、去标识化等安全技术措施； （四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训； （五）制定并组织实施个人信息安全事件应急预案； （六）法律、行政法规规定的其他措施。
	第五十五条	有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录： （一）处理敏感个人信息； （二）利用个人信息进行自动化决策； （三）委托处理个人信息、向其他个人信息处理者提
		供个人信息、公开个人信息； （四）向境外提供个人信息； （五）其他对个人权益有重大影响的个人信息处理活动。
	第五十九条	接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。
数据安全法	第二十七条	开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。
数据安全法	第二十九条	开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。
关键信息基础设施保护条例	第六条	运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。
	第十四条	运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。
	第十五条	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责： （一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划； （二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估； （三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件； （四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议； （五）组织网络安全教育、培训； （六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度； （七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理； （八）按照规定报告网络安全事件和重要事项。
	第三十条	网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。
	第三十一条	未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。
	第十九条	运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

通过对以上法条内容的研读，经咨询深圳市律师协会数据合规专业委员会，课题组认为

· 法无明文禁止即可为，金融行业的外包服务是常见的，禁止是不现实的。法律承认委托人和被委托人的法律关系，

外包人员是受托进行安全运营服务行为，法律对于受托人和委托人都规定了相应的法律责任，因此外包服务是符合法律要求的。

· 基于工作需要，如果安全服务外包人员必须接触甲方的信息、不接触不能完成业务，应遵循“最小必要”原则，同时做好防护、监测和风险处置措施，保障系统和数据安全，是被允许的。

· 关键信息基础设施的运营过程中可以采用网络安全运营托管服务。

· 关键信息基础设施的运营者在采购安全运营托管服务之前，应通过有关机构的安全审查；通过审查后，应与运营者签订保密协议、明确保密义务；应对关键岗位工作人员、外包人员进行背景审查。

(2)《证券基金经营机构信息技术管理办法(2021年修正)》合规性研究

法条	法条内容
第三十三条	证券基金经营机构应当记录经营数据和客户信息的使用情况，并持续监督信息技术服务机构等相关方落实保密协议的情况。 证券基金经营机构发现其他机构、个人违规存储或使用自身经营数据和客户信息的，应当排查数据泄露途径、评估影响范围，采取合理可行的整改措施，及时处置风险隐患，并按照中国证监会规定履行报告和调查处理职责。 证券基金经营机构发现信息技术服务机构等相关方违规存储或者使用自身经营数据和客户信息的，应当责令其立即改正并销毁已获取的经营数据和客户信息；信息技术服务机构等相关方拒绝配合整改的，证券基金经营机构应当立即停止与其合作，并采取措施维护自身及客户的合法权益。
第三十四条	证券基金经营机构应当建立健全数据安全管理制度，不得收集与服务无关的客户信息，不得购买或使用非法获取或来源不明的数据。在收集使用客户信息之前，证券基金经营机构应当公开收集、使用的规则和目的，并征得客户同意。 除法律法规和中国证监会另有规定外，证券基金经营机构不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供客户信息。

通过对以上法条内容的研读，我们认为

· 安全运营托管服务机构和服务人员在为证券基金经营机构提供安全服务的过程中，不可避免地会接触、访问到客户信息、经营信息，只要不存在违规截取、存储信息的行为，就属于合规。这里的“规”主要指各项法律法规，以及证券基金经营机构与安全运营托管服务机构之间的合同、协议。

· 对“除法律法规和中国证监会另有规定外，证券基金经营机构不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供客户信息”的解读，我们认为，只要安全运营托管服务机构的行为符合《网络安全法》《个人信息保护法》《数据安全法》等上位法的要求，就符合本条所述“法律法规”的要求。

· 安全运营托管服务机构遵照《信息技术管理办法》的要求提交备案，也满足行业监管的要求。

结论：我们认为只要安全运营托管服务机构对在服务过程中接触到客户信息、经营信息采取了合理的保护措施、监测措施、响应和处置措施，在安全运营托管服务过程中遵守与证券基金经营机构的合同、协议，就符合法律法规的要求。

风险及应对有效性分析

1. 信任风险

在安全运营托管服务过程中，信任风险包含两个内容，一是对服务机构的能力、资质的不信任，二是对服务机构的态度、意愿的不信任。针对这2类信任风险，我们认为可以采取如下多种措施

· 加强考核、利益引导；

· 建立服务机构、服务人员的黑名单和灰名单，或建立服务机构、服务人员的信用管理机制；

· 引入第三方进行检查、审计或认证；

· 提升MSSP对甲方单位服务内容的透明性；

· 落实对MSSP关键岗位、人员的背景审查。

2. 数据泄漏风险

在安全运营托管服务过程中，需要将证券基金经营机构的网络流量、可疑样本数据、人员操作日志传递给运营托管服务机构的安全分析系统，这其中不可避免地引发对数据泄漏风险的担忧。我们认为可采取如下措施

· 不将可能包含业务信息的网络全流量数据传递给运营托管服务商，仅传递NetFlow、五元组等行为、特征信息；或将网络全流量数据采集和分析能力部署在机构内部，仅将分析后的初步结果、威胁特征、可疑Payload传递给安全运营托管服务商；

· 在病毒样本分析、可疑附件分析、文件分析场景中，考虑到样本、日志中包含大量客户信息、经营信息的情况属于低概率事件，应允许传送可疑样本数据、日志数据，但要求运营托管服务机构明确对这类数据的保护措施，如租户隔离、存储分区、保留访问记录等；

· 运营托管服务机构定期接受第三方审计机构或认证机构或行业监管机构的监督和审查。

综上，我们认为在安全运营服务托管过程中面临的主要风险是可控的。

投资收益分析

一直以来，企业安全能力在安全需求和安全建设之间存在较大差距。企业既需要应对不断增长的安全威胁，同时又必须面对专业人才匮乏、防护经验缺失、安全预算有限的现实。尤其是在实战化趋势下，安全防护必须做到常态化运营，企业想要通过自身能力实现安全事件的持续监测、构建安全风险主动闭环处置能力难度很高。

正因如此，安全托管服务日益兴起，即“专业的事情交给专业的人来做”。安全托管服务颠覆了以往驻场式人工服务为主的服务模式（严格来说，这也是一种安全运营托管服务，本报告将这种模式描述为“本地托管”），让企业无需投入巨大资金和人力组建安全团队，通过远程托管的方式即可享受专业的安全服务和安全专家资源（本报告将这种模式描述为“云托管”，是本报告主要描述的安全运营托管服务模式）。

但值得注意的是，并非所有的安全托管服务方案都能很好地发挥效用。许多安全托管服务仅仅只做到了收集日志数据和发出海量警报，接近于设备托管，不仅没有起到简化流程、收敛攻击面和加固用户安全防护的作用，反而给企业安全团队带来了额外的投入。此外，即使是一个功能和服务完善的安全托管服务方案，也不一定适合所有行业，各行业用户在提出安全需求时总有一定的行业特殊安全需求，例如：证券行业对客户数据的保密性要求极高，但行业内大多数中小证券正编人员偏少，只有1-2人，只能通过托管来解决安全威胁处置的需求；但外包人员也因为流动性大的问题对安全事件的即时响应也存在一定的问题。如采用安全托管服务的方式将主要安全数据、告警分析和处置交给安全服务商进行托管，较大程度上可以解决招人难、外包人员流动大的问题，并且云托管的方式性价比也很高，可以节约很大的人工成本。

通过安全人员和安全产品的有效协同相互配合，可有效地协助客户提高组织整体网络安全的成熟度水平，进而促进和保障组织的业务发展，具有良好的经济和社会效益。

根据课题组的分析，目前国内有两种主流运营模式，一种是自建自运营加本地托管，一种是云托管式运营。

自建自运营就是证券基金经营机构在本地搭建安全运营平台，自己组建安全团队（也包括购买服务商的驻场人员），自己新建并打磨运营流程。成本投入方面比较固定，以3年建设周期计算，预计最低起步投入在110万左右，一般的投入在200万左右。

托管式运营则不需要自己购买安全运营平台和组建安全专家团队，而是复用安全厂商的安全运营平台和安全专家团队，也不用自己新建一整套的安全运营流程，而是复用安全服务商已经打磨成熟的安全运营流程，在此基础上，只需要完成和组织现有的业务流程的对接即可。成本投入方面可以做得比较灵活，以3年建设周期计算，最低预计投入24W左右就可以启动，可以根据业务需要灵活扩展。由于安全专家团队可以接触到丰富的场景、不同的业务需求，安全专家进入经验越丰富、人员越稳定的状态，并可以通过运营流程、规则、策略、知识库等复用在不同行业、企业的安全运营经验，可以帮助甲方在短时间内达到一个较好的安全运营水平。

根据课题组的调研，两种运营模式的效果方面，如果自建自运营加本地托管式运营能够招聘到安全能力达标、数量合格的人员，整体效果与托管式运营相差不大，不同之处在于托管式运营可以做到7*24监测和响应，在夜间响应方面会更有优势。如果自建自运营模式下无法招聘到足够安全能力和足够数量的人员，效果会有大概30%-40%的损耗；托管式运营则没有这方面的问题。

	自建自运营+本地托管式运营	云托管式运营
工具	自行购买安全运营平台	共享安全运营平台
人员	自己招聘 2-5 的专业安全人员或者购买驻场人员	共享厂商安全专家团队，人员能力强、稳定，7*24 小时持续保障业务安全
流程	需要新建并打磨一套运营流程：1、平台运营流程 2、问题闭环处置流程 3、评价机制等	实时监测、分析、研判、处置、加固的运营流程已经打磨成熟，直接对接即可，可快速标准化落地
3 年投入	平台建设费用 50-100W；驻场服务每人年 30w，1-2 人*3 年=90W 至 180W。则 3 年总投入月 140w-280w。	安全运营托管服务每年 8W 至 40W*3 年，则 3 年总投入 24W-120W
效果	白天平均响应时长<1H,夜间平均响应时长<8H，处置闭环率>90%	平均响应时长<1H，处置闭环率>90%

综上，我们认为在安全运营托管服务过程中采用基于远程专家服务、云上安全运营工具的安全运营托管服务，是投资收益比高的方式。

可行性研究结论

综上所述，课题组认为：在证券行业（含基金、期货）采用安全运营托管服务，尤其是基于远程专家服务、云上安全运营工具的安全运营托管服务，是合规的、风险可控的、投资收益比高的可行的实现方式，应予积极鼓励和支持，值得推广。

证券行业实施安全运营托管服务的总体建议

证券行业安全团队的特点

从本次课题组组织的调查来看，得到如下数据：

专职安全人数	安全外包人员规模	年安全服务投入规模	对 MSSP 的态度
专职安全人员规模为 1-3 人的公司（共 22 家）	8 家公司有 1-3 名安全外包 14 家公司没有安全外包	2 家公司年安全服务投入 500-1000 万 5 家公司年安全服务投入 300-500 万 15 家公司年安全服务<300 万	11 家支持 MSS 11 家不支持 MSS
专职安全人员规模为 4-6 人的公司（共 17 家）	1 家公司有 4-6 名安全外包 6 家公司有 1-3 名安全外包 10 家公司没有安全外包	3 家公司年安全服务投入 500-1000 万 8 家公司年安全服务投入 300-500 万 6 家公司年安全服务投入<300 万	14 家支持 MSS 3 家不支持 MSS

专职安全人数	安全外包人员规模	年安全服务投入规模	对 MSSP 的态度
专职安全人员规模超过 6 人的公司（共 6 家）	2 家公司有 7-10 名安全外包 1 家公司有 4-6 名安全外包 3 家公司有 1-3 名安全外包	2 家公司年安全服务投入 1000 万以上 3 家公司年安全服务投入 500-1000 万 1 家公司年安全服务投入 300-500 万	2 家支持 MSS 4 家不支持 MSS

从调查数据看到，证券基金经营机构的专职安全人员规模主要集中在1-3人（46%）、4-6人（35%）这两个区间内。证券基金经营机构安全团队（包括专职安全人员和安全外包人员）小、中、大规模的中位数分别为3、6、11.5。

从证券基金经营机构安全团队人员规模、投入规模来看，每年投入200万到安全运营托管服务并得到一个金融行业内70分水位的安全运营水平，是可行的。

安全运营有哪些工作内容

本节的目的主要在于识别安全运营的主要工作内容，为下一步分析、判断哪些工作内容可以交由MSSP奠定基础。

1. 识别与获取（Identify）

(1)资产数据管理：获取、优化资产数据的质量，以更好地提供服务；

(2)配置数据管理：获取、优化配置数据的质量，以更好地提供服务；

(3)漏洞和威胁情报的监测、获取、研究&外部关系管理：获取漏洞情报、威胁情报或外部事件、案例并对之进行研究；作为外部接口，获取其他外部渠道（如监管机构、上级单位、同行）输入的与我有关的情报、告警；通过扫描、数据分析等手段获得、验证与我有关的漏洞情报；

(4)安全数据的管理：获取、存储、优化安全运营所需要的告警、日志、流量等数据的质量，以更好地提供服务；

2. 检测与监测（Detect）

(1)健康度和覆盖率巡检：对安全设备、安全策略的健康度和覆盖率（包括但不限于安全设备的部署位置、安全系统运行健康度、安全基线的实现结果、安全设备的具体配置、安全Agent的部署范围等）等进行巡检，发现问题后进入（11）；

(2)管理告警和检测策略：设置和优化各类检测工具（如WAF、DLP、数据库审计、NTA、SIEM）的策略，以更好地达成检测的目标；检测的目标一般是发现威胁和异常，并输出告警；

3. 处置和恢复（Response & Recovery）

(1)漏洞和补丁管理：采取补丁、缓解措施等方法对漏洞进行处置直至达到预期效果；

(2)异常分析和处置：对告警进行分析、确定处置策略，执行处置直至达到预期效果；并在处置结束后进行复盘、输出改进建议并进入（11）。未来可能需要实现7*24告警监测、分析和处置；

4. 自我验证（Verify）

(1)安全策略有效性验证：采用工具和特定方法对现有的安全防护策略、检测策略的有效性进行检验，如发现异常则进行分析、确定处置措施并进入（11）；

(2)渗透测试、众测与红蓝对抗：采用不同强度的渗透测试手法对现有的安全防护策略、检测策略的有效性进行检验，如发现异常则进行分析、确定处置措施，并进入（11）；

5. 闭环和支撑（Loop）

(1)改进跟踪：对安全运营过程中发现的缺陷和差距进行改进，直至达到改进目标；形成安全运营的知识库；

(2)风险评估：对残余风险进行评估并纳入后续跟踪管理；对运营工作进行复盘、输出改进措施并进入（11）；

(3)流程、机制和工具管理（含运营工具的维护升级，自动化）：确定并优化安全运营的岗位、流程、考核评价机制；开发并优化安全运营的平台化和自动化工具；

(4)安全意识和安全技能培训：对安全运营人员进行安全意识和安全技能的培训；

(5)度量：对安全运营的过程和结果进行度量、分析，提出改进建议并进入（11）；

判断是否可以交付安全运营托管的要素

课题组认为，判断某一类型的安全运营工作是否可以依赖安全运营托管服务来实现的话，需要考虑如下要素。但具体衡量标准仍需甲方在实践中根据自身情况调整和把握。

1、是否法律法规、监管要求有明确的、书面的规范或指引

2、是否需要与甲方内部员工有频繁的互动、多种形式的信息往来

3、是否需要对甲方内部情况（比如网络架构、组织架构、人员特征和技能）非常熟悉

4、是否会导致客户信息、员工信息（统称个人信息）大量或高频被访问

5、是否会导致其他机密级及以上经营信息被大量或高频访问

6、完成动作所需专业技能要求的高低或学习成本的大小

7、完成动作所需人员是否容易获得，或获取成本在可承受范围之内

8、完成动作所需数据流量或带宽大小，存储的数据量大小

根据前期对行业内安全从业者的调研，对这8个要素的重视程度如下

选项	人数小计	比例
1、法律法规、监管要求有明确的、书面的规范或指引	23	82.14%
2、是否需要与甲方内部员工有频繁的互动、多种形式的信息往来	19	67.86%
3、是否需要对内部情况（比如网络架构、组织架构、人员特征和技能）要非常熟悉	17	60.71%
4、是否会导致客户信息、员工信息（统称个人信息）大量或高频被访问	21	75%
5、是否会导致其他机密级及以上内部信息被大量或高频访问	19	67.86%
6、完成动作所需专业技能要求高或学习成本的大小	13	46.43%
7、完成动作所需人员是否容易获得，或获取成本在可承受范围之内	12	42.86%
8、完成动作所需数据流量或带宽大小，存储的数据量大小	8	28.57%

如何实现安全运营托管

安全运营托管服务是一种通过共享安全专家团队的方式，便于各行业单位复用云端的安全服务专家人员的专业技术能力，以低成本、高可用、低风险的方式获得安全运营能力的交付模式，同时可以将安全专家的经验和知识库固化到云端运营平台，通过人机共智的方式协助甲方有序地开展安全工作，解决安全问题。

基于以上分析，在做好风险控制的前提上，课题组本着“能托管就不用自有人员，能云端就不用本地”的原则，对各项工作内容进行了如下分解。打钩就意味着本项工作更适合通过该类人员交付。

运营内容	自有人员	本地托管	云端托管
1 资产数据管理		√	
2 配置数据管理		√	
3 漏洞和威胁情报的监测、获取、研究			√
4 安全数据的管理		√	√
5 健康度和覆盖度的巡检			√
6 管理告警和检测策略		√	√
7 漏洞和补丁管理		√	
8 异常分析和处置	√		√
9 安全策略有效性验证	√		√
10 渗透测试、众测与红蓝对抗			√
11 改进跟踪	√		
12 风险评估	√		
13 流程、机制和工具	√		
14 安全意识和技能培训		√	√
15 度量	√		

对于以上表格的内容，课题组认为需要强调如下重要观点

1、在自有人员编制有限的情况下，应集中精力投入在异常分析和处置、差距分析和持续改进方面；同时应以度量为抓手，展现成果、暴露问题，这样既可以获得组织内的支持，又可以显著降低企业内部的安全风险；

2、资产、配置、漏洞、补丁的工作是安全运营的基础性工作，由于需要和公司内部人员有大量的沟通协作，需要对公司网络架构、系统运行情况比较熟悉，在自有人员编制有限的情况下，更适合交给驻场安全运营人员完成；

3、漏洞情况和威胁情报、渗透测试&众测&红蓝对抗，安全意识和技能提升，属于常见的、较成熟的云端交付模式；

4、安全数据的管理、健康度和覆盖率巡检、管理告警和检测策略、异常分析和处置、安全有效性验证都是更适合运用云端托管能力的工作内容。比如

(1)使用云端的日志和数据存储能力，可以显著降低甲方的数据管理压力和数据分析难度；

(2)由于行业内的安全设备、系统、工具的雷同性都较高，采用云端的健康度和覆盖率巡检服务、管理告警和检测策略服务，可以显著降低对人员的培训、监督、管理成本；

(3)采用异常分析和处置则更加能够集中使用云端的专家能力、知识库，显著弥补本地人员的能力不足，并可以通过云端的SIEM（安全信息和事件分析）、SOC（安全运营中心）、云沙箱、SOAR（安全编排和自动化响应工具）等工具实现自动化的响应和处置，减少安全建设成本，提升响应效率和质量，满足未来的7*24监测和响应需求，共享跨企业、跨行业的威胁情报。

5、后续可参考“云安全责任共担模型”，研究、输出“安全运营责任共担模型”，以便给业内同行提供更加可行的参考。

总结与展望

课题组在证券基金经营机构进行了安全运营托管的小范围试点和调研，试点表明，通过云服务的形式引入安全专家，并通过将证券基金经营机构本地的告警、流量分析、可疑样本分析、情报监测等安全运营任务通过安全运营托管服务实现，可以显著提升证券基金经营机构的安全运营效率和水平。

目前我国网络安全趋势正逐步地由传统被动防御模式转向主动治理的模式，企业正在努力建设纵深的安全运营体系。安全运营托管供应商拥有专业的人才及资源可以有效的缓解企业在安全运营建设过程中面临的人才成本。目前安全服务的规模扩张速度远超整体安全行业的平均增速。安全运营托管人才需求与日俱增、安全运营托管的自动化程度愈来愈高、行业标准日渐完善。

参考文献

1.《网络安全法》

2.《个人信息保护法》

3.《数据安全法》

4.《证券基金经营机构信息技术管理办法（2021年修正》

5.《信息安全技术 信息安全事件管理指南》(GB/T 20985-2007)

6.《信息安全技术 信息安全风险处理实施指南》(GB/T 33132-2016)

7.《信息安全技术 信息系统安全运维管理指南》(GB/T 36626-2018)

8.《信息安全技术 网络安全威胁信息格式规范》(GB/T 36643-2018)

9.Gartner自适应安全框架(Adaptive Security Architecture,ASA)

10.ATT&CK 模型(Adversarial Tactics, Techniques, and Common Knowledge)

11.《证券期货业信息安全运营管理指南》(征求意见稿)

安全实践

03 创新实践

SDWAN融合物联网 实现金融行业资产智能化管控

文丨王建国、徐渊、崔潇敏

山西证券股份有限公司

摘　要： 资产是企业日常运营的根本。在金融企业数字化转型的当下，资产管理须通过一系列系统、科学的方法，促进资产全生命周期内绩效、风险和成本的综合最优，最终实现企业的整体战略目标，其过程如何做到智能可视至关重要。

关键字： 物联网、金融、资产管理

金融行业资产管理面临的风险与挑战

2021年4月27日，《关键信息基础设施安全保护条例》经国务院第133次常务会议通过，自2021年9月1日起施行。2023年5月1日，《信息安全技术关键信息基础设施安全保护要求》开始正式实施。其中，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

目前，关键信息基础设施金融企业资产数量巨大，具有种类繁多，流转快、地点分散，使用周期长等特点，传统的管理方式常常会忽略资产的这些特性，仅以账面记录为基础进行事后统计，导致经常出现“有账无物”或“有物无账”的问题，这就造成了实物帐和财务账的信息不对等，大幅提升了企业的实际经营成本，甚至面临“资产流失”的法律风险。

金融企业资产管理面临的痛点主要包括：

1、账实不一致，资产报废时无法找到对应实物。

2、资产盘点费时费力，耗费大量人力却无法得到满意结果。

3、IP类资产数量多，入网慢，影响金融业务开通效率。

4、重要资产无法做到实时位置监控和异常情况联动报警。

智能资产管理解决方案

射频识别（RFID）技术的应用，为资产管理带来了便捷性，具有如下特性：

适用性：RFID技术依靠电磁波，并不需要连接双方的物理接触。这使得它能够无视尘、雾、塑料、纸张、木材以及各种障碍物建立连接，直接完成通信。

高效性：RFID系统的读写速度极快，一次典型的RFID传输过程通常不到100毫秒。高频段的RFID阅读器甚至可以同时识别、读取多个标签的内容，极大地提高了信息传输效率。

独一性：每个RFID标签都是独一无二的，通过RFID标签与产品的一一对应关系，可以清楚的跟踪每一件产品的后续流通情况。

简易性：RFID标签结构简单，识别速率高、所需读取设备简单。尤其是随着NFC技术在智能手机上逐渐普及，每个用户的手机都将成为最简单的RFID阅读器。

射频识别技术依据其标签的供电方式可分为无源RFID标签和有源RFID标签。

有源RFID标签识别距离较长（通常15米—30米），标签将资产信息传递给RFID读写器，RFID读写器可通过连接IP网络将数据实时传回资产管理系统。有源RFID标签的供电方式通常有外接电源和内置电池两种，外接电源的标签相对体积较大，不够便携，移动体验较差，且依赖外部电源，无法独立工作；内置电池使用寿命一般在3年—5年，寿命结束则需要进行批量更换,运维成本较高，通常用于关键性资产的管理。

无源RFID自身则无需供电，可通过手持阅读器等发出的高频/超高频的电磁波激励获取能量并完成数据的通信，且使用寿命通常在10年以上，经济实用，是一般性资产管理的首选；但无源RFID识别距离较短（通常1米-3米），由此手持阅读器可通过WIFI联接无线AP，从而将近距离读取的资产信息通过IP网络实时远程传送回资产管理系统。资产管理系统再与财务、安防、定位等系统的联动，达到设备管理分类科学、编码规范、标识统一，真正实现“账、卡、物”相符，提高设备管理的速度和准确性，使海量的不同种类设备管理真正落到实处。

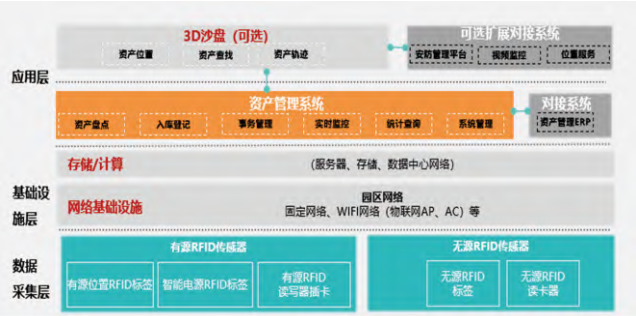


图1 RFID传感器架构

由此可见，不论是用于关键性资产的有源RFID标签还是用于一般性资产的无源RFID标签，都需要一个稳定可靠高效的IP网络提供RFID与WIFI融合接入，为了解决融合接入的问题，可采用无线物联AP的方案。该物联AP可将有源RFID的读写器以Mini PCIE插卡的形态插入到AP中，用一张物理网络提供RFID标签与WIFI终端的融合接入，并结合AP的无线网规地图，可获知到资产的位置信息，这样就避免了RFID物联专网的建设，降低了建网的成本，提升了资产管理网络开通的效率。

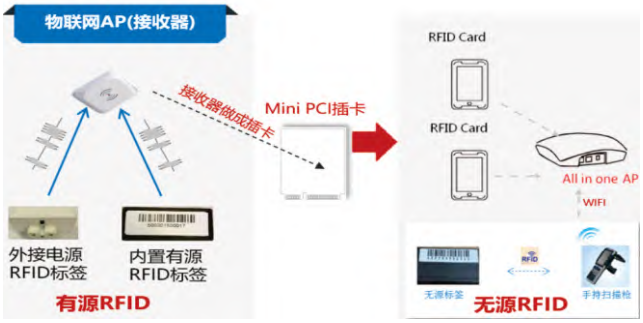


图2 RFID传感器区别

智能IP终端即插即用解决方案

金融行业随着数字化建设的推进，智能化、网联化的终端资产种类越来越多，数量越来越多，如：智能机器人，自助打印机、智慧屏、摄像头等；这类IP终端通常无专人值守，加上金融网点地理位置分散的特点，网络管理员无法做到进场为每个终端进行网络接入的配置工作，如何让这些智能化的IP终端安全高效的接入网络是提升金融业务开通效率的重要一环。

通常为这类无人值守的IP终端可泛称为IOT哑终端，采用ETH或者WIFI的方式接入网络，网络侧为了这些哑终端可采用更通用更便捷的方式入网，通常采用MAC认证的管控方式，但由此带来了两个问题：一是终端的MAC地址难采集，逐个手工抄录易出错，且需反复校对，效率低下；二是终端MAC地址易被仿冒，安全风险较大。

为解决上述的两个问题，山西证券股份有限公司（以下简称山西证券）部署了终端即插即用解决方案，如图所示：

图3 即插即用解决方案

终端即插即用解决方案基于终端智能识别引擎，在对现网业务零干扰的基础上，智能感知到所接入终端的MAC、IP、接入位置、终端类型，操作系统等多维度的信息，做到终端的可视、可控、可管，免MAC采集，管理员一键审批即可自动入网。

可视：网络智能感知终端流量特征，对已知终端采用指纹库匹配的方式，未知/新型终端采用AI聚类等方式，精确识别出终端的类别，厂商，型号，操作系统等信息。

可控：可根据终端不同的类型，OS，接入位置等信息，灵活制定终端访问网络的权限，自动开通网络，做到终端的即插即用。

可管：针对MAC易被仿冒的缺陷，网络可智能感知到终端类型的变更（如：该MAC地址对应的终端类型由打印机变成了PC），自动安全隔离，做到零仿冒，零私接，将安全风险降到最低。

SDWAN多分支高效互联，高可靠传输

山西证券于2021年开始针对不同分支机构的规模和业务特点，构建高性价比的高速SD-WAN互联通道，在节约了大量专线成本的同时，提升了集中管理效率。其中应用级智能选路方案保障了关键业务的体验；ZTP（Zero Touch Provisioning，零接触部署）开局方案，使各分支机构无需专业人员上门，利用USB、邮件等多种方式灵活开局，实现跨区域分支机构的分钟级上线。

同时，SDWAN方案解决了目前证券期货行业各分支机构通讯情况无法集中管理的困境，实现了通讯情况集中可视，全流程自动化管理，提升了运维效率。

在产业侧，充分验证了鲲鹏+欧拉和海思+VRP架构的稳定性，实现了SM3认证算法、SM4加密算法的双加密模式下通道的安全可靠。同时融合5G+IPv6技术重塑了证券期货业广大分支机构的广域网边缘基础设施，极大简化运维复杂度、减少故障定位时间，为分布式、跨地域的证券行业分支机构无人化运维提供了基础保障。

基于SDWAN＋WIFi6＋IoT技术的资产管理综合实践

在2021年构建高性价比的高速SDWAN多分支互联通道的基础上，2022年山西证券将SDWAN管控平台升级到LAN-WAN融合的一体式管控平台。该LAN-WAN融合解决方案实现了各分支机构的WIFi6无线AP与出口SDWAN路由器的统一纳管，IOT哑终端的即插即用，RFID标签与WIFI终端的融合接入,极大提升了业务开通，网络运维的效率，降低了建网成本。并且RFID终端以及IP终端的数据传输均由SDWAN数据隧道（SM4加密）传输到数据中心，解决了资产数据在互联网上传输的安全问题，结合AP的定位识别技术，可有效判断资产的位置，并实现资产在企业内部流转的可视化。

图4 资产盘点流程

SDWAN+WIFI6+IoT技术彻底改变了传统方式下固定资产管理工作繁忙、手段落后、信息迟滞、沟通困难的痛点。在办公室的方寸之中就能掌控全方位设备信息，实现了设备领用、盘点、巡检、运维保障、调拨、租赁、故障快速定位、网络快速开通等敏捷功能。通过后台对数据进行客观的统计分析，为企业领导层提供决策客观依据。

SDWAN+WIFi+IoT技术对金融数字化未来建设的展望

如今可穿戴设备、虚拟现实、物联网等技术已经悄然进入人们的生活中。借助物联网技术，智能办公模式加速形成，物联网自动化办公也逐渐成为一种趋势。当前，物联网的智能办公场景主要是会议室、休息室和办公室。通过将传感器、摄像头等监控传感设备与互联网实现高效连通，可以管理、控制办公室的多种设备，从而为员工工作提供便捷的环境。具体来讲，在办公室中，可以将窗帘、投影仪、空调等设备接入物联网系统中，在日常工作期间，员工可以根据实际需要，打开或者关闭相应的设备，以此来控制自己周围环境的温度、湿度等，有益于促进资源节约、降低能耗。

实际上将物联网技术应用于办公室后，使办公场所发生了许多变化。一方面，物联网让工作空间更加智能化。在节约能源、减少浪费、提高工作效率、个性化定制办公环境、提高工作场所安全性等方面，物联网的确起到了重要作用。另一方面，虽然物联网具有多种优势，但是其在实际落地中还存在一些问题。比如：成本问题。要想实现办公设备之间的智能连通，企业就需要安装相应的物联网设备，而这需要投入大量的资金。购买昂贵的物联网设备会成为一种负担。与此同时，接入物联网设备后，还会引发企业对于隐私数据是否安全的担忧。在当前隐私数据泄露事件频发的背景下，连入物联网后，是否会对企业的数据安全造成威胁，是需要重点考虑的问题。此外，物联网对稳定的电源和WiFi连接极度依赖，这就要求企业必须有比较完善的硬件设施和网络连接平台。只有具有稳定的运行环境，物联网设备才能及时准确的收集信息数据，并为管理人员进行相关决策时提供可以信赖的参考依据。

目前，在SDWAN+WIFi+IoT技术的推动下，高效化、智能化、自动化办公模式将加速形成，企业员工将进一步感受到科技给商业办公带来的便利。值得注意的是，为更好的服务企业，应该及时制定包括隐私政策在内的制度和规范。在实际操作过程中可以通过SDWAN+WIFi+IoT建立可靠和安全的网络基础设施。与此同时，只允许授权的物联网设备在办公室使用（如Mac地址绑定）、对员工进行适当的培训等措施，都可以促进智慧办公的高效运用，从而兼顾科技应用和网络安全。

SDWAN+WIFi+IOT的融合方案是山西证券在信创化道路上摸索出来的一套行之有效的资产综合管理解决办法。但该办法并不是唯一的，在解决互联网通道安全性的基础上，放置在互联网端的台账也可通过APP加密、区块链等技术来实现资产数据的安全性、保密性与完整性。这里也期待业内的各位同仁各抒己见，融合思想，并肩创新，找到符合金融行业各自实际情况的解决方案。

可编排网络安全架构研究及落地实践

文｜李家攀、何洲星、叶奔发

国投证券股份有限公司

摘　要： 在金融行业全面数字化转型的形势下，云计算、云原生、SDN等技术正在得到大力发展和推广使用，促使金融业网络及系统架构向软件定义、自动化、弹性扩展方向发展。随着新技术的发展和应用，新的安全风险层出不穷，来自外部和内部的信息安全风险不断增加，对金融系统的安全性提出了更高的要求。

通过优化现有互联网边界网络安全架构，形成可编排的新网络安全架构，新架构解决了原有架构网络流量无法按需分配、安全设备无法弹性伸缩、统一卸载SSL证书困难、网络及安全设备紧耦合以及无法支持业务系统灰度发布等问题。同时，也提升了SSL证书卸载的效率和统一管理能力，使得下游安全设备可以更好的消费卸载后的明文网络流量，更大程度上提升了安全检测和防护的能力。

关键字： 卸载SSL、智能编排、池化、解耦

前言

随着人工智能、大数据、区块链等新技术的兴起，券商业务迅速的互联网化，证券行业数字化转型日益深入，同时云原生等技术的大力发展和推广，促使金融业网络架构向软件定义、自动化、弹性扩展方向发展。与此同时，针对行业互联网系统的APT攻击、DDoS/CC攻击等也逐步体现出自动化、智能化的趋势。伴随着新业务、新技术的发展，新的安全威胁层出不穷，来自外部和内部的安全风险不断增加，对券商互联网边界安全性提出了更高的要求。

由于现有安全系统部署对于现有互联网边界网络架构依赖度很高，导致安全系统部署很难进行弹性伸缩，面对不断增加的HTTPS站点部署需求及流量快速增长带来的挑战，现有网络架构已不能满足和适应新增系统部署的需求，如何打破现有网络架构的约束，为安全系统提供更大的弹性，满足个性化、差异化、全面可视化的安全检测和防护需求成为了互联网边界安全需要重点思考的问题。

研究目标及内容

研究目标

(1) 网络流量编排：针对券商业务的特性，对互联网边界流量进行编排，将不同业务属性的流量进行定制化的分发，供后端的安全系统、网络系统及应用系统使用；

(2) SSL卸载：由前端系统统一卸载SSL，解决安全系统卸载SSL的重复性、性能不足问题，满足性能、架构方面的需求，解决安全系统无法处理加密流量的问题，最大化实现安全系统的价值；

(3) 证书统一管理：实现统一管理证书，避免证书文件泄露带来的安全风险，同时，也降低了管理成本；

(4) 安全系统池化，灵活扩展：现有网络架构及技术无法实现多台安全系统负载均衡模式，单系统运行的可用性风险较高，安全系统横向扩展的需求很大。通过将安全系统池化，使得安全系统可实现弹性扩展，同时，也可以更大程度上利用安全系统的容量；

(5) 助力业务系统灰度部署：借助流量编排，更好的助力业务系统实现灰度部署；

(6) 网络架构松耦合：将网络架构中安全、网络系统进行松耦合，对于网络、系统故障可以快速进行定位及处置。另外，可以更加灵活方便的在网络中添加或移除安全系统，在执行变更操作时降低上下游系统的依赖性。

1. 网络流量编排

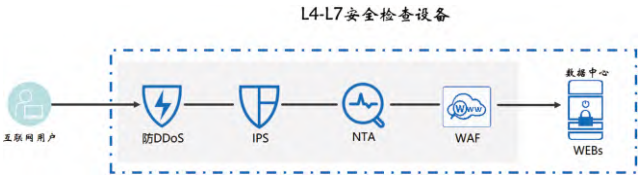


图1 传统互联网边界网络安全系统架构

在传统安全架构中，数据中心的安全防护主要是针对来访问自己核心业务系统的流量进行安全检查，以保证数据中心IT资产的安全。用户通常会在服务器前端串行部署ADS（防DDoS攻击）、IPS（入侵防御系统）/IDS（入侵检测系统）、NTA（网络流量安全分析）、WAF（Web应用防火墙）或旁路安全检测设备等。

众多的安全设备，采用二层或三层的接入方式，以糖葫芦串的形式一个挨一个的接入到用户网络中，为用户的数据中心构筑一道道防线，保障了数据中心IT应用资产的安全。

在以上传统网络安全架构中，由于设备串接部署，导致所有的流量必须流经所有的安全设备，但这是没有必要的，比如WAF只能检测HTTP流量，TCP流量和UDP流量WAF是无法检测的，而券商业务系统中有很大一部分流量如行情、交易等使用的是TCP私有协议，在实际应用中因网络流量识别及切分困难导致全协议流量都流经了WAF。这使得WAF设备消耗了不必要的性能，带来较大的IT资源浪费。同样，其他安全设备也存在类似的情况。

另外，由于所有的网络流量都流经所有的安全设备，对于某些不需要经过所有安全设备的流量来说，带来了不必要的时延，这也不符合券商行业追求低时延的行业特点，需要加以改进，以符合券商行业的业务要求。

希望能研究出一种流量编排技术，它能对流经安全设备的流量提前做判断，对于需要经过某种安全设备的流量，才转发到相应的安全设备进行安全防护；对于不需要某种安全设备的流量，不流经这路安全设备，以提高安全设备的有效利用率；同时减少不必要的设备转发，以减少转发时延。

2. 安全设备的高可用及弹性伸缩

在传统的组网架构中，一般安全设备以透明方式（二层部署）或是主备的方式部署于组网中。随着用户数据中心业务的发展或是应对突发流量，安全设备需要面临快速提升性能的问题。传统的做法是使用更高性能的设备进行替换，但是这样很难最大化实现安全资产的价值。同时在市场行情剧烈变化的情况下，突增的流量可能远远大于单台高性能安全设备的吞吐量，此时只能采取旁路安全设备而舍弃保护业务系统安全的做法，这种做法对业务系统的运行带来较大的安全风险。在传统的组网架构中，基本无法通过对安全设备进行弹性扩展来满足业务突增情况。

希望能研究出一种高可用技术，支持安全设备在各种组网模式下（二层组网、三层组网、TAP），支持安全设备的多活，而且能支持按性能比例进行业务分发，支持不同组网形式的安全设备高可用，同时可以支持安全设备的弹性扩展。

3. SSL卸载及证书统一管理

随着全球全站SSL应用推广，以及规避HTTP协议带来的安全风险，证券行业越来越多的Web站点通过HTTPS协议发布。随着SSL协议版本的不断更迭，目前最新的协议版本是2018年推出的TLS1.3。从SSL LABS的统计可以发现，用户对Web站点安全性的要求越来越高，采用高安全性的TLS协议的用户比例越来越多。因此，预计在未来2-3年，TLS 1.3及以上版本将成为主流。

以下为SSL LABS 统计的2022年9月份全球 TLS1.3使用情况：

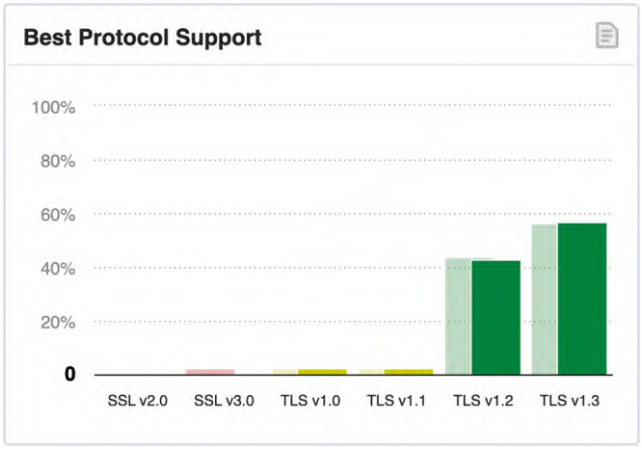


图2 2022年9月份全球 TLS1.3使用情况

TLS 1.3的快速发展带来了一个很大的挑战，就是PFS（完美前向安全）功能，TLS 1.3中将移除所有不支持PFS功能的加密套件。

PFS要求一个密钥只能访问由它所保护的数据。用来产生密钥的元素一次一换，不能再产生其他的密钥。一个密钥被破解，并不影响其他密钥的安全性。这样的密钥生成机制，导致以前的安全设备可以在Passive-TAP模式下就可以解密SSL流量的方式成为历史，所有安全设备必须inline部署，且加入到SSL整个安全协商过程中，在客户端与服务器端之间维系两个独立的SSL ID连接，才能解密SSL流量。因此，如何实现SSL可视化成为了编排设备的一个挑战。

同时为了提高证书的安全性，避免证书文件泄露带来的安全风险，需要将设备SSL证书做统一管理，提高证书的安全性。

4. 网络架构松耦合

在传统的网络架构中，所有的安全设备以糖葫芦串方式部署，形成了设备间的紧耦合，一旦串行链路中的某台设备出现问题，可导致整个网络链路的可用性受到影响。

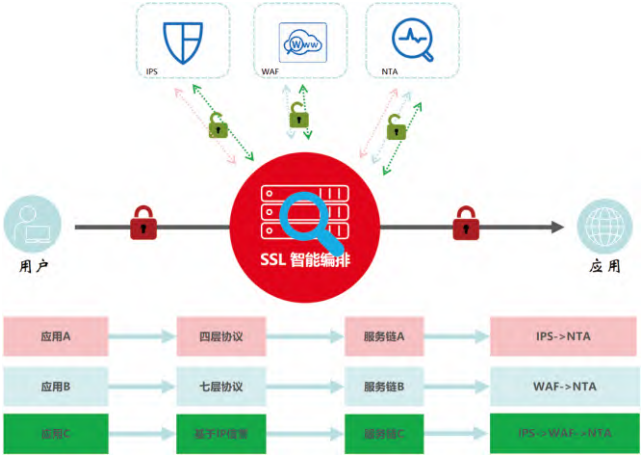


图3 服务编排组网方式

在上面的编排组网中，安全设备下挂于编排设备或是编排设备下面的二层交换机上，编排设备通过本身的负载均衡功能，对安全设备进行池化管理，实现安全设备的动态扩展，同时通过编排设备的健康检查能力，实时监测安全设备的可用性，如果安全设备出现故障，将不会向安全设备转发流量，实现安全设备与网络架构的松耦合。

5. 助力业务系统灰度部署

编排系统能帮助用户在需要测试新的安全设备或开展新的业务系统测试时，通过配置专用的测试服务链（需要经过哪些安全设备）和确定测试流量，让测试流量流经相应的测试系统，实现动态评估（灰度上线，即让一小部分流量经过新系统进行验证）。以往新业务功能上线都需要申请变更窗口期，窗口期内用户是无法访问业务的。现在则可以通过灰度的方式上线，即使业务在线状态下，也能轻松完成测试任务。这也是本次研究的内容。

关键技术及创新点

关键技术

1. 突破多种安全设备接入的可能

编排设备改变了原有的网络安全架构，安全设备不再串行接入到网络中，而是接入到编排设备下。编排支持多种安全设备的接入，所接入设备不限定品牌，只是与其接入方式相关。支持的设备包括：

· Web代理设备，如以网络代理服务器接入的安全设备；
· 三层设备，如以三层模式接入的防火墙设备；
· 二层设备，如以二层透明模式接入的IPS、WAF等设备；
· TAP 设备，如以TAP模式接入的只接受数据的IDS设备。

编排系统实现了丰富的部署场景：

（1）基于二层网络的入站方向

此场景主要用于流量进入数据中心的方向，对原有部署在数据中心保护其核心应用的安全设备进行SSL流量的编排。在用户不希望变更现有网络架构，而又想达到SSL安全流量的可视化和编排时使用。

编排通过二层透明模式部署在数据中心应用前端，无需改变现有网络架构。而其余安全设备，可以直接连接在编排物理端口，或通过交换机连接到编排设备。

（2）基于三层网络的入站方向

此场景主要用于流量进入数据中心的方向，此时编排作为反向代理模式接入网络。此接入方式的优点是可以在任何编排硬件平台支持，但缺点是需对现有网络架构进行改动。

（3）基于二层网络的出站方向

此场景主要应用在流量出数据中心的方向，用于对办公上网终端进行内容安全检查设备的SSL流量编排，如上网行为管理、Web Proxy、下一代防火墙等。此时编排以二层透明模式接入，无需改变现有网络架构。

（4）基于三层网络的出站方向

此场景主要应用在流量出数据中心的方向，此时编排以三层路由模式接入。此时客户端无需做其它修改，只需将网关指向编排设备，或保持原有网关，将原有网关的下一跳指向编排设备即可。

2. 实现流量协议识别和安全策略的自定义

用户业务种类多样，不同的业务采用的协议不同，安全防护级别不同，采用不同的安全策略，要流经不同的安全服务设备，平台需要根据不同的维度来区分流量，实现不同的流量采用不同的服务链来实现安全保护，平台可以根据以下条件及其组合来区分和引导流量：

· 流量的源IP地址位置信息(如国家、城市)
· 流量的源IP信誉度
· 流量的源IP地址网段
· 流量的源端口
· 匹配协议
· SSL检查
· URL匹配
· 编程语言：根据以上条件的“与”或者“或”的组合

安全策略，根据在条件中的定义来区分不同的流量，并指定其关联的服务链和动作，来决定对流量的调度操作。

创新点

1. 构建互联网边界网络安全弹性架构

通过编排设备，对接入安全设备形成一个安全设备资源区，安全设备不再串行接入到网络中，而是接入到编排设备下面，这种组网架构，为后续灵活扩展安全服务设备提供了便利：

· 安全设备接入具有了池化的能力，所有接入安全设备均为Active状态运行，安全设备无需配置为HA模式，由编排设备执行健康检查，并分配到策略指定的安全设备上；

· 所接入的安全设备具有了动态扩展的功能，随着所处理流量的增多，可随时在线扩展安全设备，即使新加安全设备性能与在线安全设备性能不同，新旧安全设备可以同时在线，处理业务流量，节省了投资；

· 如果有设备出现故障，编排设备通过健康检查得知后，将不再向其转发流量。如果整个安全组设备出现故障，此安全组将自动从动态服务链中Bypass，不会影响正常业务流量的转发；

在需要测试新的安全设备时，新的安全设备直接接入编排设备，不会影响业务系统的运行。在测试时，通过配置编排策略，让测试流量流经测试设备，实现动态评估（灰度上线），让用户无需申请停机窗口期，即使业务在线状态下，也能轻松完成测试任务。

2. 实践双模安全架构

采用流量编排系统中的服务链编排能力，可以针对安全设备运维和业务特点制定灵活的策略，进而实现双模安全架构。

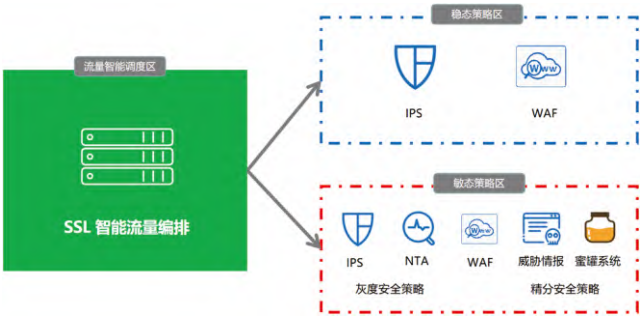


图4 双模网络安全架构

双模网络安全架构能够得以实现，主要依靠动态服务链。动态服务链可以用来定义流量在到达最终目的地的途中，将流经一个或多个安全服务组，动态服务链定义了用户希望流量采取的路径和顺序，在按所定义的顺序的安全设备处理完成后，流量最终回到流量编排设备。

在定义服务链之前，需要先定义接入的安全设备，包括WAF、IPS、NTA等，然后在服务链中指定流量经过设备的顺序，由此来灵活的编排安全流量。

公司在互联网边界部署了WAF、IPS和NTA三组安全设备，希望达到以下目的：

1）TCP/UDP流量依次经过NTA和IPS，且无需解密；

2）HTTP无需解密，依次经过WAF、IPS和NTA；

3）HTTPS流量解密后，依次经过WAF、IPS和NTA。

此时，只需定义两个安全服务链。第一条服务链为经过所有安全设备，第二条服务链为只经过NTA和IPS。在条件中定义区分TCP/UDP、HTTP和HTTPS流量，然后关联不同的服务链，并指定是否解密等动作即可。

通过以上方式可以简单便捷地实现稳态和敏态的安全策略。稳态区注重的是合规、稳定、可靠，而敏态区注重的是网络攻防对抗。

研究完成及落地实践情况

研究完成情况

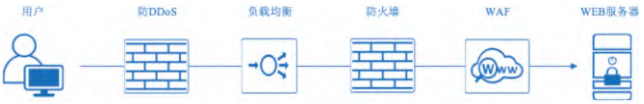


图5 原有互联网边界网络安全架构图

上图为原有互联网边界网络安全架构图，原有WAF、IPS等安全设备透明串行部署在网络中，网络架构存在较多不足。经过改造后，当前的互联网边界网络架构如下：

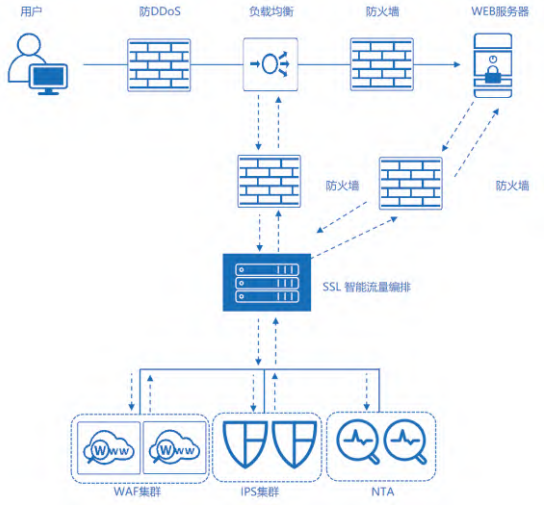


图6 改造后的互联网边界网络安全架构图

在新的网络架构中增加了两台流量编排设备，形成一个互联网安全设备资源区，由流量编排设备对其下挂的安全设备服务做流量编排。WAF、IPS等安全设备下挂到流量编排设备后面，由流量编排设备将安全设备作为一种服务对其进行流量编排。采用这种组网架构后，对WAF、IPS等安全设备进行了池化，提升了安全设备的处理能力，同时当这些安全设备发生故障时，编排设备可检测其存活状况并进行Bypass处理，减少对后端业务系统的影响，保障业务的连续性。

通过网络架构的挑战，实现了以下：

· 自定义服务链，根据业务需要，可以自由、合理分配业务路由；

· 安全设备运维变更过程中，不会对业务系统的可用性造成影响，对业务无感知；

· 将网络流量进行分类，对HTTP(S)、非HTTP(S)的网络流量识别和分发；

· 以前入站、主动出站访问均需要过WAF，调整后只有入站需要，对WAF设备的性能消耗大幅降低；

· 流量可视化，让其他安全设备可以看到明文流量，提升安全整体有效性；

· 安全设备池化，使网络架构与后端安全设备的品牌、性能无关，可根据需要进行弹性伸缩。

落地实践情况

目前此可编排网络安全架构已经进行了部署应用，运行情况满足预期。通过对原有网络架构的有效重构，将网络资源和安全资源服务进行统一池化、自动化编排管理，使得网络架构弹性可扩展，打破了原有架构的约束，解耦了网络资源、安全资源间的强关联，实现了网络和安全资源的价值最大化。同时，满足了支持业务系统的灵活发布需求。为安全检测和业务访问流量调度提供了更大的灵活性，满足了个性化、差异化、按需安全检测和业务流量编排的需求。

一种基于关口流量旁路劫持的威胁反制技术研究

文丨董小宇

上证所信息网络有限公司

摘　要： 随着网络技术的发展，企业面临来自各个方向的威胁和挑战，面对威胁，作为防守一方的企业受制于攻防的不对称性，难以对攻击行为做出有效反制和根本性溯源。为应对这一挑战，越来越多的公司采用蜜罐作为其反制手段，然而由于其先天特性，蜜罐只能采用被动方式诱捕，针对蜜罐之外的威胁却鞭长莫及。为丰富防守一方的溯源反制手段，本文提出了一种基于关口流量劫持的威胁反制方案，引入MITM、浏览器攻击等红队技术，来弥补蜜罐等工具在主动捕获威胁方面的缺陷。

关键字： 蓝队、溯源反制、流量劫持、蜜罐、对抗

概述

随着互联网技术的发展，越来越多的应用搬上互联网，企业在提升工作效率的同时，也面临着更多来自互联网的威胁和挑战。由于网络攻守的不对称特性，在面临网络攻击时，企业的防御存在两方面棘手之处：一是企业的互联网资产暴露了更多的攻击面，产生了更多的防守盲区，企业将疲于应对来自多个方向的嗅探和攻击，且针对盲区的攻击难以及时发现；二是由于网络的匿名性，即使发现攻击，对攻击开展溯源也很困难。针对第一点，越来越多的企业开始梳理资产、监测流量，能更快地发现威胁；对于第二点，行业在溯源反制方面应用最多的技术可能当属蜜罐，即通过模拟一个或多个易受攻击的主机或服务，吸引攻击者，捕获攻击流量与样本，进而发现网络威胁。复杂的蜜罐还能根据攻击者留下的蛛丝马迹开展一定程度的溯源反制。但是，大部分蜜罐产品仅能在蜜罐区发挥作用，针对发生在非蜜罐区网络的攻击则难以处置。本文在蜜罐的基础上，探讨一种新的防御思路——基于在关口处旁路牵引流量并劫持实现的威胁反制及溯源技术，以进一步提升企业在网络攻防中的反制能力。

企业网络是独立于公共互联网之外的区域网络，存在与互联网之间交互的固定接口。这些接口是连接企业网络与其他网络的重要节点，本文暂且将其称作“网络关口”，默认出入网络的流量均需要经过网络关口处设备的审计。当发生安全威胁事件，网络管理员通过终端安防设备、IDS、IPS等设备发现威胁流量后，常见的做法是及时隔离受影响的设备、阻断威胁流量，然而，这些常规手段往往会使攻击者意识到其攻击已暴露，聪明的行为攻击者为了保护留下的突破口、防止被管理员发现，会快速清理入侵痕迹，沉寂一段时间，在事件看似已风平浪静后，再度卷土重来。如果无法彻底清理攻击者留下的后门，无疑会给企业的网络安全埋下巨大隐患。

本文提供另一种反制和溯源的思路，在发现网络中发生了行为威胁时，不直接阻断，而是通过网络分流器等设备对攻击流量做牵引分流，引导流量进入事先准备好的诱捕网络或蜜罐网络，通过劫持等手段编辑流量，消弭流量中的敏感信息，注入攻击代码，再将流量重新注回网络，与攻击者或木马程序之间建立一条虚假连接，为取证溯源提供充足的时间。经关口设备回注的流量还可以打入数据水印，为将来的威胁溯源提供更多线索。

技术思路

该技术的整体实现思路为：在网络关口处布置网络分流器，用于牵引威胁流量至威胁反制区，对攻击流量做处理，或把流量引导入蜜罐进行诱捕，处理或诱捕后的流量再经过网络分流器汇聚，从关口设备重新路由回到互联网。涉及的设备部署整体架构如下图所示。

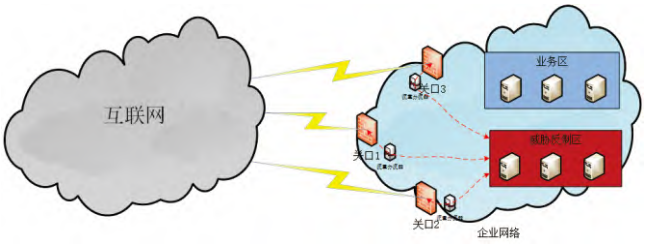


图1 设备部署整体架构图

以下内容将简述威胁反制的过程。

企业在网络关口处部署流量监测设备，当网络管理员发现异常流量时，使用网络流量分流器对异常流量做过滤分流，同时对关口处流量进行控制。针对不同类型的流量，可通过不同特征信息筛选恶意流量，将其牵引至威胁反制区。具体的特征和处理方式将在后文列举。

威胁反制区中包括处理流量的服务器或复杂交互式蜜罐网络，反制区的环境经过精心设计，与被攻击的环境相似。在收到分流的恶意流量后，处理流量的服务器快速分析数据包内容，根据请求包的内容，实时生成无害的响应包，修改校验值使其看起来与正常数据包无异。完成数据包伪造后，经过连接网络关口的线路，将数据包回注到原采集端口，通过网络关口处的路由交换设备返回互联网，与攻击者建立一条虚拟的连接。可通过实时控制回包的内容，来诱导攻击者的行为，在其请求一些特定内容时予以反制。处理流量的服务器还可以诱导攻击者主动进入蜜罐网络，实施诱捕。但使用蜜罐网络捕获威胁非本文重点，此处不做过多赘述。

威胁反制区通常建设在网络关口附近，以缓解处理流量过程中造成的延迟。将流量牵引服务器部署在关口附近，当企业网络存在多个出口时，也可通过网络专线将其他出口的流量汇聚至流量牵引服务器，由流量牵引服务器收集汇聚流量、对汇聚的流量做预处理。其网络连接关系如下图所示：

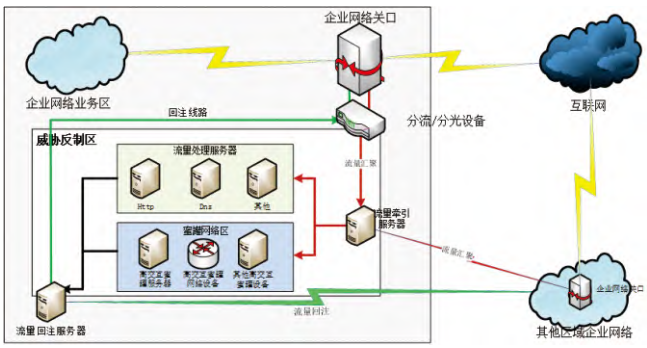


图2 威胁反制区服务器逻辑连接关系图

图中红色线条表示经过引流的威胁流量，绿色线条表示处理过的回注流量。当企业管理员借助IDS、IPS及其他设备发现威胁流量后，通过网络分流设备，将出、入网的威胁流量汇聚引导至流量牵引服务器，分析流量的五元组，将流量按照不同来源、不同协议做初步划分，根据预处理结果分别将其发送至流量处理服务器或蜜罐网络区，必要时可采取阻断措施，防止木马避开劫持、回连出网等情况；对于发送至蜜罐网络区的流量，通常按照蜜罐系统运行逻辑处理，此处不做赘述。

对于发送至流量处理服务器的流量数据，根据不同的网络协议采取不同的处理逻辑，如针对传输web内容的Http服务可在其流量中插入JS代码实现网页挂马；对于FTP、DNS、Telnet等明文协议可实时分析其明文内容，并返回具有诱导性（指引其向蜜罐网络移动等）或替换为恶意文件的数据；对于HTTPS、SSH等加密流量，可在配置证书后解包，之后进入对应明文协议流量的处理流程。对于攻击者回传的敏感数据流量，服务器在将其替换为虚假数据的同时，可在其中插入数据水印和流量水印等标记，以配合后续的威胁溯源工作。经流量处理服务器修改或专门构造过的数据包进入流量回注服务器进行最后的封装检查，通过补全五元组、重新计算校验和等方法使其成为网络中能够正常传输的流量，最后由回注服务器将流量重新注回网络链路。下图为解析DNS协议数据包示例。

```
DNS header information

  ID            : 0xb811
  Flags         : 0x8180
  Question      : 1
  Answer        : 3
  Author        : 5
  Addition      : 5

Queries

                : type A, class IN

Answers

                NAME, class IN, cname
                : type CNAME, class IN, cname
                com: type A, class IN, addr

Authoritive nameservers

                com: type NS, class IN, ns dns1.
                com: type NS, class IN, ns dns2
                com: type NS, class IN, ns dns5
                com: type NS, class IN, ns d
                com: type NS, class IN, ns dns6
```

图3 DNS协议报文解析

反制场景分析

与MITM攻击工作机制类似，本文提到的技术在攻击者与服务器或木马与回连服务器之间对攻击者相关的流量进行处理，一方面诱导攻击者进入事先准备好的陷阱或蜜罐网络，进而诱捕攻击者实现取证；另一方面处理木马回连流量，维持与回连服务器之间的虚假连接，为摸清木马通信机制，分析木马流量特征，排查后门隐患争取时间。以下提供简单示例来说明如何诱捕攻击者及如何建立木马与回连服务器之间的虚假连接。

攻击者对网站攻击场景

假设第一种情况，发现攻击者对网站实施恶意攻击行为，但尚未获取权限，此时攻击者会尝试一些特定的攻击行为，如扫描端口，爆破目录，翻找敏感文件，上传文件等，可根据其不同行为，采取不同的诱捕行动。如其执行端口扫描、爆破目录等操作时，网络管理员可控制生成错误的扫描或爆破结果，诱导攻击者产生错误判断，将其行动方向引导至蜜罐网络区实施诱捕。如其正在翻找敏感文件，可通过文件替换的

方式将其下载的敏感文件替换为能够执行代码的反控木马文件实现对攻击者的诱捕。当其上传文件时，将文件目录重定向或将文件另存至威胁反制区，一是更好地诱导攻击者向威胁反制区移动拓展，二是避免上传的文件对系统业务造成不必要的影响。

实际攻击过程中，有多个阶段攻击者需要下载文件，以便实现对受害者网络的深入控制并获取更多敏感数据。当攻击者下载可执行文件时，即是对攻击者实施反制的最佳阶段，如图所示为反制取证工具获取攻击者敏感信息。

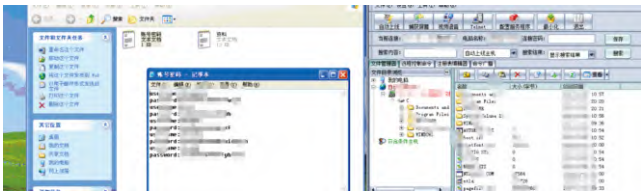


图4 利用反制工具获取攻击者敏感信息

以下对其中可能实施反制手段的阶段进行简要分析。

1、攻击通过VPN访问的网络

为方便员工在企业外部访问企业网络，越来越多的企业网络配置了VPN服务。VPN服务在为企业办公提供巨大便利的同时，也带来一定的安全隐患，当VPN存在漏洞或员工账密出现泄露时，往往能够使攻击者如入无人之境，对企业内部网络造成巨大威胁。为顺利实施攻击，攻击者往往需要对企业使用的VPN服务进行分析，当攻击者获取到员工泄露的账户时往往会下载客户端并进行登录尝试。在本文所属的反制技术中，一旦识别到攻击者从威胁反制区下载VPN客户端软件，即可将其替换为事先准备好的反制取证工具。当攻击者在自己的攻击机运行从“官网”下载的“VPN客户端”时，反制取证工具即可对攻击者的机器取证回传。

2、企图从攻陷节点中获取敏感信息

当攻击者对企业网络进行踩点或期望通过从被攻陷节点中获取敏感信息时，会收集网站或被攻陷节点的文件。获取到的敏感文件可以是多种形式，但是仅当敏感文件为office、pdf、rar或其他替换为可执行文件格式的文件时方可实现反制利用。针对office文件，可通过定制宏病毒实现取证，也可利用历史中出现的office漏洞、pdf漏洞进行利用取证。rar格式文件可以制作自解压形式的取证工具。可执行文件格式可直接投放反制取证工具或将取证作为一项功能内嵌在原文件中。

木马连接场景

假设第二种情况，攻击者已成功上传木马并已建立木马与回连服务器之间的连接。当流量不加密时可直接重定向木马的回连流量和回连服务器的响应流量至威胁反制区，通过伪造木马的回连请求和回连服务器响应回包建立两个虚连接，实现对木马和回连服务器的双向劫持。一方面通过建立与木马的虚连接，响应木马的心跳包，防止木马启动自毁程序；另一方面建立与回连服务器的虚连接，通过返回伪造的命令执行结果，将攻击者引导至蜜罐网络并最终实施诱捕。当流量加密无法破解时，网络管理员可预先移植木马文件至威胁反制区，并将响应木马的返回流量重定向至威胁反制区可实现木马与回连服务器之间的连接，通过威胁反制区蜜罐网络预先埋置的诱饵对攻击者实施溯源反制。

针对木马已上传的情况，企业还可利用木马主控端漏洞实现对主控端服务器的溯源反制。当前常见的webshell管理工具如蚁剑、哥斯拉、冰蝎等，常见的木马及C2工具如Cobalt Strike、MSF、Sliver等，其中蚁剑、Cobalt Strike均被爆出安全漏洞，当攻击者使用的版本存在安全漏洞时，便可实现对其攻击的反制。其他可利用场景如NPS代理漏洞溯源等。

除上述两种情况外，本文提到的技术结合浏览器攻击技术也可对攻击者实施反制。通过预先配置攻击载荷，可在攻击者访问威胁反制区构建的站点时对攻击者实施反制，以下为攻击者访问精心构造的web站点后的部分反制手段场景图示。

图5 获取攻击者浏览器指纹

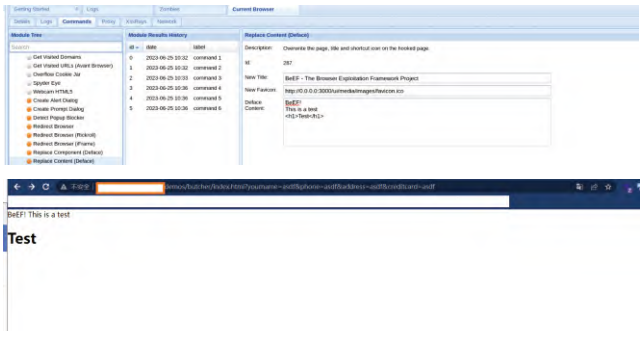


图6 实时修改攻击者访问的页面

DNS Query Record	IP Address	Created Time
0xb359.16.21?56c69742e20416c697175616d2063757273757320736365 6c65726973717565.zhe5wb.dnslog.cn	.58	2023-06-25 22:51:25
0xb359.5.21?73206e69736920766f6c7574706174206 56c6974207375736369706974206 17.zhe5wb.dnslog.cn	91.58	2023-06-25 22:51:21
0xb359.20.21?e756e63207669746165206 56e696d207068617265747261206 56c6569666 56e.zhe5wb.dnslog.cn	34	2023-06-25 22:51:04
0xb359.21.21.642e.zhe5wb.dnslog.cn	110	2023-06-25 22:51:04
0xb359.19.21?656e74657371756520757420 6163206f7263692e20496e20636f6e677565 206.zhe5wb.dnslog.cn	.30	2023-06-25 22:51:04
0xb359.20.21?e756e63207669746165206 56e696d207068617265747261206 56c6569666 56e.zhe5wb.dnslog.cn	.190	2023-06-25 22:51:03
0xb359.19.21?656e74657371756520757 6163206f7263692e20496e20636f6e67756 206.zhe5wb.dnslog.cn	54	2023-06-25 22:51:03
0xb359.19.21?656e74657371756520757 6163206f7263692e20496e20636f6e67756 206.zhe5wb.dnslog.cn	4	2023-06-25 22:51:03
0xb359.16.21?56c69742e20416c697175616d2063757273757320736365 6c65726973717565.zhe5wb.dnslog.cn	74	2023-06-25 22:51:02
0xb359.17.21?206469616d2061206672696e67696c6c612e204375726162697475720 6d6f6.zhe5wb.dnslog.cn	.82	2023-06-25 22:51:02

图7 通过DNS请求获取攻击者IP

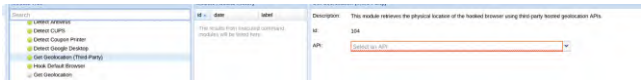


图8 通过第三方提供的API获取攻击者地理位置

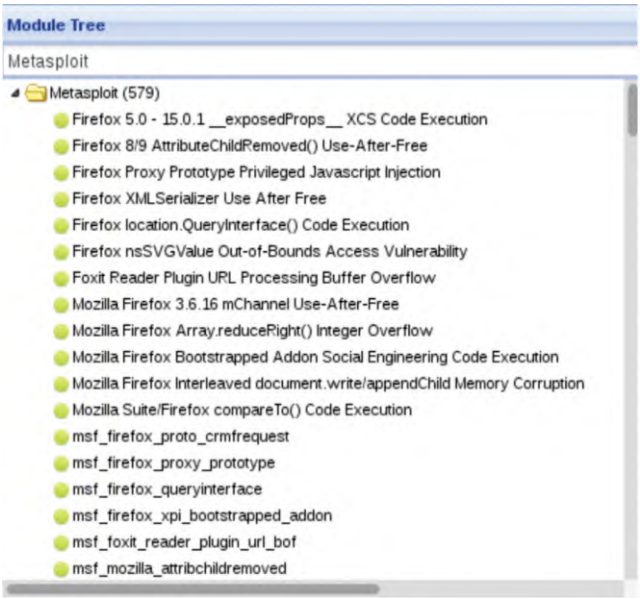


图9 联动metasploit攻击浏览器

根据攻击者自身攻击基础设施建设的复杂程度和反溯源意识的敏感程度，可在分析对方攻击流量的基础上配合执法部门利用掌握的漏洞来攻击其跳板服务器或C2服务器，若其在未经检查的情况下随意打开被替换成木马文件的“被窃取文件”时甚至能直接控制其计算机，实现对攻击者的根本性溯源和反制。企业在发现威胁并利用威胁反制系统处理流量的同时应快速排查受影响区域，可结合流量处理服务器的流量分析结果定位威胁，并从根源上彻底排查和清理攻击入口，消除隐患。流量处理服务器也可在对受感染机器取证的基础上优化流量生成规则，进一步迷惑攻击者，为溯源反制提供强有力的支撑。

除以上提到的反制手段，利用流量处理服务器对攻击响应流量做处理，可在一定范围内监控流量去向，为借助执法机构力量追踪溯源提供线索。流量处理服务器在对攻击响应包进行最后的封装前，通过流量水印技术对流量做标记，可以在数据包中插入特定的指纹，也可构造特定长度的数据包序列，当流量发出后可借助同样的流量分析技术在城域网、运营商骨干网等核心网络处分析捕获标记了水印的流量踪迹，进而实现流量跟踪。

困难和局限

以上提到了利用关口处旁路流量劫持的方法对攻击者实施反制的一些技术思路以及利用该技术对攻击者可能实施的一些反制示例。但是该技术在实际应用过程中也面临着一系列困难和局限，以下对此展开谈论。

首先在判断攻击者流量方面高度依赖外部系统和专家分析，当外部提供的攻击者流量出现误报时会对真正的客户造成影响。本文提到的技术仅对流量捕获及后续处理等内容做了讨论，但对于外部提供的攻击者流量的真伪无法做出判断，这就导致当外部系统或专家分析出现失误时，将直接影响到企业用户，由于反制手段存在一定的攻击性，严重时会对用户体验或企业声誉造成影响。针对此问题，需要企业加强外部合作，培养具备威胁溯源反制能力的专家，提高对威胁流量和威胁入侵的鉴别分析能力，在充分判断威胁事件的影响后确定是否采用反制措施以及如何实施反制，以防对正常用户业务造成不必要影响。

其次，利用该类技术对攻击者实施反制是否受法律保护目前并没有明确的规定。《网络安全法》第二十二条规定网络产品、服务的提供者不得设置恶意程序；第二十七条规定任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动，然而本文提到的部分反制技术具有攻击性，在实施过程中是否受法律保护尚存疑。针对此问题，企业应加强与执法部门的合作，在发生威胁事件后及时报警，在执法部门监督下开展后续工作。

此外由于要对攻击者实施溯源反制，在一定程度上需要反制者掌握一定的系统或浏览器漏洞，对企业安全团队的建设提出了更高的要求，不仅需要掌握防守技能，更需要一定的前沿攻击技术和漏洞挖掘能力，而目前大部分企业的安全团队尚不具备该类能力，需依赖外部专业团队协助。

最后一点也是最关键的一点，攻击者在攻击之前往往制

定周密的计划，建设完备的红队基础设施，尽管本文提到的攻击技术在一定程度上能够对反溯源意识薄弱的攻击者实施强有力的反制和打击，但是面对精通反溯源技术的攻击者时，仅仅依靠企业自身的力量往往难以获得好的效果。如攻击者在实施攻击时往往利用第三方或匿名方式获取的肉鸡发起攻击，即使通过反制手段获取肉鸡的权限，再深一步的溯源也难以进行；再有借助公共网络或加密技术构建通信隧道时，无法分析其通信内容，也就无法实施有效反制；还有攻击者在下载从受害目标处获取的文件后不在当前机器运行或打开，而是通过在网络隔离的沙箱中运行以防止反向钓鱼，那么反制者此前精心设计的陷阱就形同虚设，并且还会在技术高超的攻击者面前暴露意图，使得攻击者更加谨慎。面对此类攻击者，单纯依靠企业自身力量已无法应对，必须借助执法机构乃至国家安全机关的力量合力反制。

技术在落地实施过程中可能还面临其他一些困难，但总得来说主要体现在技术储备和法律合规两个方面。为解决这些难题需要企业一方面加强与外部安全公司的合作，提升自身安全队伍的取证溯源反制能力，另一方面要遵守法律法规，增强与国家相关部门的协作配合，积极打击网络违法犯罪活动。

总结

本文介绍了一种基于在关口处部署旁路设备，通过流量劫持、流量篡改等方式实现威胁反制的技术，为企业加强安全建设，提升威胁反制能力方面提供了一种不同的思路。随着网络安全技术的深入发展，企业安全建设在满足发现威胁、阻断威胁的基础上，如何在威胁发生后更好地保护企业资产、降低企业损失，也许提升威胁反制能力会是一个方向。尽管该技术在实际应用中可能还存在一定的困难和局限，但其仍然能够为企业溯源取证提供强有力的支撑。

安全实践

04 开源治理

开源软件安全管理思路探索与实践

文｜吴佳伟、钟蓉、李鹏、曹杰

兴业证券股份有限公司

摘　要： 当前各行业逐步进入数字化转型发展时期，数字经济规模越来越大，软件作为数字经济发展非常重要的基础设施，其技术和开发模式持续迭代更新。为提升软件开发效率和降低软件开发成本，开源软件得到广泛使用，但同时开源软件使用带来的安全问题也越来越突出，因开源软件安全问题发生的安全事件频频发生，如何有效开展开源软件安全管理工作已成为共同焦点。本文简要分析当前开源软件安全管理现状及痛点，简述兴业证券开源软件安全管理思路和相关具体应用实践，提升开源软件安全管理水平。

关键字： 开源软件、开发安全、软件供应链安全、开源治理

开源软件安全管理现状及痛点分析

开源软件现状分析

1.开源软件使用情况

开源软件是以源代码、文档等内容开放的模式来开发的软件，主要体现在软件开发的协同、软件成果的共享和软件功能的创新上。开源软件的使用无处不在，已经成为数字经济快速发展的重要力量，覆盖到操作系统、中间件、数据库、工具系统、SDK、组件、框架等不同系统。Gartner的调查显示，99%的组织在其信息系统中使用了开源软件；据信通院2022年全球开源生态研究报告统计，截至 2021 年 GitHub 托管仓库数量已达 2.61 亿，2021 年新增仓库组件6100 万个，增长率达 30.5%；2022年在物联网、网络安全、能源和清洁技术、计算机硬件和半导体行业的代码库中或多或少均使用了开源代码。

2.开源软件安全现状

开源软件安全形势十分严峻，根据CNCERT开源软件供应链安全风险研究报告，近6年开源组件仓库的漏洞数均大幅上涨；攻击者已把目光放在了开源软件上，利用开源代码漏洞，实现对软件供应链上游的攻击，达到规模化影响，如log4j漏洞影响了数百万个基于java的应用程序。

开源软件安全管理痛点分析

开源软件安全管理要达到预期效果面临较大挑战和痛点：

复杂度高：开源软件遍布各个系统中，且不同系统使用开源软件的种类、版本大概率不一样，极大增加了开源软件资产管理复杂度，开源软件资产不清晰，开源软件安全管理难于达到预期。

依赖性强：开源软件安全风险发现很多情况下依赖外部情报，安全风险整改依赖上游社区的更新升级，更新升级后系统的稳定性依赖开源软件更新后的可用性和兼容性，开源软件更新升级若不经过充分测试可能造成业务系统运行异常。

冲突性大：主要体现三个不一致，一是安全人员与研发人员价值目标不一致，安全人员希望要用安全可靠的开源软件，而研发人员希望快速找到一个能用、满足功能需求的开源软件；二是开源软件版本不一致，一种开源软件不同系统需使用的版本可能不一样，导致版本统一管理难；三是开源软件安全评估和准入流程不一致，研发和安全各一套。

开源软件安全管理探索

总体思路

为了更好解决开源软件安全管理痛点问题，提升开源软件安全管理能力，需先形成开源软件安全管理整体思路，依据整体思路开展具体工作。兴业证券整体思路如图1所示，明确了开源软件安全管理目标，即：开源软件资产管理清晰、安全管理标准统一、安全风险检测实时、安全风险响应及时；在目标确定后，基于开源软件准入、使用和退出三个阶段，建立开源软件安全管理机制和流程，并在各阶段持续性进行安全评估。在准入阶段引入安全评估的门槛和管理机制，在使用阶段定期开展漏洞检测、开源协议合规评估，能够实时监测到网络安全攻击行为，在退出阶段把不必要的开源软件进行淘汰，以免再次被系统使用引入安全风险。

图1 开源软件安全管理思路

开源软件准入

开源软件准入方面，自研系统和商采系统准入控制要求不一样。

1. 自研系统开源软件准入

建立开源软件制品库，统一开源软件来源，原则上制品库是各系统使用开源软件的唯一来源，限制各研发团队随意从互联网下载开源软件。若制品库中没有，研发团队提需求评估后方可进入制品库，另外对制品库中开源软件定期开展安全评估，及时修复制品库中开源软件安全风险。制定安全准入要求，设立门槛，高风险版本及不满足公司安全需求的开源软件不入库，且上线前安全检测中发现高风险的开源软件，需要重新评估是否将其从制品库中删除。持续对开发、测试人员开展安全意识培训，在开源软件准入要求上统一思想和达成一致。将开源软件准入规则标准化，建立标准化准入流程，并通过公司流程系统有效落地。

2. 商采系统开源软件准入

加强供应商安全管理，形成供应商清单，对供应商安全资质和安全服务能力进行评估，在采购中要求供应商落实安全要求，如要求供应商在软件开发过程中落实公司安全开发规范，在软件交付时要求供应商提供安全评估报告、SBOM清单等。

开源软件使用

开源软件上线运行使用后，需开展常态化安全风险检测、预警及响应。定期开展主动安全风险检测，建立多层次的安全检测体系，多层次体现在多种实施频率，多种检测工具，多种检测方式；建立实时监测预警安全系统，当发生安全攻击或漏洞利用攻击行为时，能够实时监测到并发出安全预警；及时响应处置安全风险，对内部主动检出的漏洞能够及时完成整改，对监测到攻击行为能够快速阻断，对外部获取的威胁情报能第一时间排查并定位资产，在过程中供应商的应急响应能力非常重要，商采系统安全风险的整改修复依托于供应商来完成。

开源软件退出

随着系统不断升级更新，不符合公司安全要求的开源软件需要从制品库中退出，需要退出的开源软件主要有三类：

多次出现重大安全漏洞的开源软件，如Struts2多次被报高危漏洞的开源软件，需限制新系统再使用，且从制品库中逐步退出，已使用的系统需进行逐步替换。

不再维护的开源软件，不再维护的开源软件已不提供更新修复补丁，若存在安全漏洞，系统运行的风险非常大，严重影响了系统运行稳定性。

使用频率很低的开源软件，为了降低管理成本，提升开源软件管理标准化水平，将有限安全资源解决主要矛盾，提高安全管理成效，制品库中维护开发常用的开源软件，将使用频率低的开源软件逐步被使用频率高的开源软件替代。

开源软件安全管理具体实践

兴业证券的开源软件安全管理能力建设正在持续推进中，当前主要基于软件开发生命周期来开展，如图2所示从软件的开发、交付和运行几个阶段来落实相应的安全控制措施。在项目立项、供应商准入时评估供应商安全服务能力，业务需求分析同时开展安全需求分析，软件开发过程中实施源代码审计、SCA和IDE编码环境实时安全检测，测试/交付环节开展IAST、上线前安全测试，运行后实施常态化安全漏洞检测和风险监控。为了更有效的落地各安全控制措施，兴业证券安全团队牵头技术管理、研发、测试和运维团队相关人员组成了虚拟组织协同推进开源软件安全管理工作。

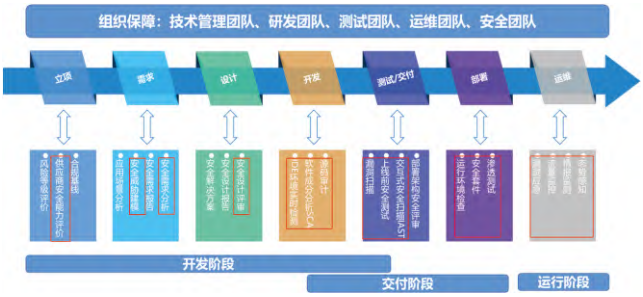


图2 兴业证券开源软件安全管理框架

实践场景1：自研系统中开源软件安全管控

自研系统开发环境位于公司内部网络，可灵活自主在开发流程中设置安全检测点对开源软件开展安全管控工作。如图3所示，在开源软件制品库管理方面，通过网络策略限制研发IDE仅可从公司内部制品库中获取开源组件，不可直接访问互联网仓库，由公司内部制品库统一升级更新，为避免因次生依赖给研发带来过大的编译压力，内部制品库在组件网关上仅拦截少量利用门槛极低的高风险组件。在开源软件安全检测方面，一是立项时在项目组宣贯上线组件要求并提供IDE客户端安全插件的使用手册，要求项目组在编码IDE环境

中对引入的第三方组件进行自检；二是在上线前设置安全红线，通过IAST、SCA等工具对引入的开源组件进行安全检测并同时采集系统引入组件的SBOM信息，便于开源组件上线运行后资产管理，当发现高风险漏洞时可及时定位相关开源组件。

图3 自研系统开源软件安全管控流程

实践场景2：外购成熟系统中开源软件安全管控

外购成熟系统的开发由供应商完成，厂商交付的系统在开发语言、系统格式及大小方面都存在较大的不可控性。如图4所示，对于常规的java字节码war/jar交付包，通过上传交付包本地检测或访问制品库地址远程检测方式完成字节码安全风险检测；对于较大容器镜像文件，向项目组提供二进制扫描命令行工具，在服务器上采集扫描所需的dockerfile等配置文件，再上传至安全检测引擎服务端进行安全扫描。

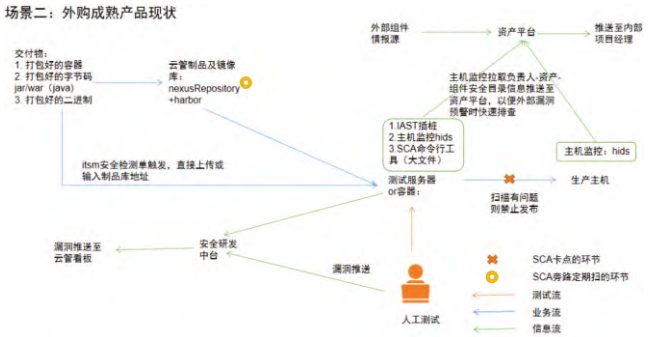


图4 外购成熟系统开源软件安全管控流程

总结与展望

开源软件是现在软件开发必备技术能力，但其带来的安全问题日趋严峻，开源软件安全管控迫在眉睫，需根据公司自身实际需求制定开源软件安全管控整体解决方案，统一安全管理标准和流程，从开源软件引入、使用和退出全生命周期落地安全控制措施，并持续开展风险评估。

开源软件安全管理是一项长期持续性工作，不同行业安全管控方式不一样，以商采为主传统行业优先要加强供应商管理；开源软件安全管理也是供应链安全治理重要部分，要上下游/供需方整个链条协同落实，同时在治理过程中需要将安全措施嵌入到业务、研发、运维流程中，形成大家认可一致的统一流程；行业级的开源软件威胁情报分享和平台化管理将是开源软件安全管理上升到更高层面的重要手段。

证券供应链开源组件治理探索实践

文｜刘宏、杜铁绳、马晓鹏、黄施宇、李晨、张华、朱嶷东

国金证券

摘　要： 纵览全局、横驱别骛，针对开源治理的繁难杂乱困境，国金证券以合规为方、流程为舱、制度为桨、工具为档，建立企业级开源软件台账，全面落地开源治理体系，转换开源软件风险治理主被动模式，解决供应链引入的开源组件问题，实现风险可知、可查、可控，达到安全合规双向协同赋能的目标。

关键字： 供应链管理、开源组件治理、安全合规、证券业

背景分析：内外发力双向驱动

外部监管与政策

近年来，人行、证监会、工信部等监管均对开源软件治理提出了要求和规范。

2021年10月27日，人民银行办公厅、证监会联合五部委发布的《关于规范金融业开源技术应用与发展的意见》（简称意见），整体从金融机构使用开源、金融机构自发开源、开源生态构建、标准体系与法律保障等4个方面提出了指导意见，并重点提出了金融机构在使用开源技术时应遵循“安全可控、合规使用、问题导向、开放创新”四大基本原则，以及“鼓励金融机构将开源技术应用作为提高核心技术自主可控能力的重要手段”。

2021年11月，工业和信息化部印发《“十四五”软件和信息技术服务业发展规划》提出深化开源技术应用，夯实开源基础设施，普及开源文化，完善开源治理机制和治理规则，加强开源国际合作，推动形成众研众用众创的开源软件生态。

内部需求分析

证券行业基于开源技术应用取得科技创新、业务赋能等积极成效的同时，也面临诸多风险。

1.开源漏洞引发的安全事件已引起业内关注。2021年发生的log4j2远程代码执行漏洞引发了重大风险。曾在72小时内受到84万次攻击，国内外知名企业受到经济损失，2018年某金融机构因开源软件Kafka漏洞问题被银保监会通报。

2.开源许可证带来的法律合规风险。2021年我国首例GPL许可证纠纷案在广东省宣判，标志着我国法律正式承认开源许可证的合法地位，应规范使用开源组件防范许可证带来的风险。

3.供应链中断可能影响业务开展。自主可控环境下需要对使用的开源软件进行监控，防止因为开源软件断供停服可能造成业务的中断。

开源治理难点

国金证券目前开源软件引入方式主要有两种：

(1)被动方式，采购的商业软件不开源被动的引入了开源软件；

(2)主动方式，开发团队主动引入一些组件提升研发效率。

这些引入带来了未知安全和合规风险。不同供应商使用的语言、版本不同，安全能力层次不齐；存在大量存量以及业务发展需要极速增长的增量开源软件，造成缺乏相应自动化工具，人工的方式进行资产梳理和管控难度大。

金融行业研究实践现状

中国人寿研发中心结合科技产品引用开源组件实际情况，聚焦突出问题，紧盯关键节点，按照“主动管控、消化存量、控制增量”的工作思路推进开源组件漏洞治理工作[1]。

海通证券从开源组件治理的开源团队设立、流程及制度设计、开源引入引出、开源检测及修复四个层面推荐，实现了良好的治理效果[2]。

北京银行采取了多种举措保证开源技术的安全可控性，在积极推广企业内部统一技术平台的同时，严格控制开源软件的引入，从多方面保证开源软件、代码使用的安全性和稳定性[3]。

另外在证标委推进下，证券行业多家券商联合开展供应链安全的行业标准起草，相信能够为行业的探索实践贡献更为强大的支持。

规划实施：统筹全局协同发展

现状分析

国金证券针对开源软件现状进行分析和总结，存在以下待完善点：

(1)开源治理制度规范不完善，在面对外部监管合规和内部合规，还需完善对自研、外包开发以及对外采购等相关环节的制度规范建设；

(2)软件成分分析工具缺失，面对大量存量和新增开源软件以及不同厂商，统计范围广、统计难度大，人工统计耗时长、数据不精确覆盖力度不够，需要软件成分分析（SCA）工具提升效率；

(3)缺少自动化安全检测流程,对于瀑布式及敏捷式开发模式，缺乏对开发流程中的开源软件引入、使用以及运维环节的自动化检测，无法对应用开发生命周期中的开源软件风险进行检测。

制定目标

国金证券开源治理目标为：

(1)落地开源治理制度及规范

根据国金证券现有开源治理情况，对比行业先进开源治理经验，建设开源治理组织，引入开源治理制度和规范，加强对开源软件风险管理。

(2)建成一体化开源软件检测和治理平台

结合现有开发模式对接软件成分分析工具，将开源安全治理技术的管理规则和流程固化到开发流程中，解决开发过程中新增开源软件问题，实现对开发过程中的开源软件敏捷化检测治理。

(3)满足行业监管和合规相关意见和要求

遵循《意见》满足监管合规和内部合规的原则，建立相应的合规检查项，定期对内部存在的漏洞风险和许可风险进行检查。

(4)达到行业开源治理成熟度标准（增强级）

参考行业成熟的《企业开源治理能力成熟度评估》，规范企业内部开源治理体系，提升开源软件治理能力，并进行相关评测认证，为证券行业开源治理标准和方向贡献微薄余力。

体系建设

国金证券开源治理的思路是先梳理再治理。第一步，参照开源软件治理能力成熟度模型，分析梳理企业当前的现状，包括组织机制、管理制度和风险管理（能力维度），以及开源软件从引入、使用到退出全生命周期管理（过程维度）；第二步根据差距分析结果，制定改进方案，通过完善流程制度、建设工具平台，从而提升公司整体可信开源治理能力水平。体系落地实践如表2-1所示：

现状调研	对国金证券开源软件管理现状进行全面了解和调研
差距分析	根据《开源治理能力成熟度模型》相关标准和资料，对现状调研结果进行差距分析，并提出差距追赶计划
方案制定	根据差距分析结果，制定相关方案和可行性计划，结合国金证券现状，提升相关开源治理能力
工具建设	结合现有国金证券开源治理工具现状，引入相应软件成分分析工具，对接现有开发流程，进行敏捷化检测
制度建设	根据企业现状、差距分析结果和现有治理策略，制定适用于国金证券的指引性规范
流程优化	根据现状，不断调整优化开源治理流程，增加各团队协作配合能力
持续改进	根据标准要求及目标，持续改进现有措施和方案，达到齐全完备的治理方案

表2-1 开源治理体系建设

工具建设

围绕源码SCA、二进制SCA和运行时SCA三个方向引入工具实现目标。

项目	源码 SCA	二进制 SCA	运行时 SCA
检测目的	检测使用的第三方组件，找到组件存在的安全漏洞及证书使用风险		
检测阶段	开发测试阶段	持续交付、持续集成阶段	应用运行阶段
检测对象	源码：开发过程产物，基于高阶语言来编写，写给人看，很方便分析其中语句的语义	二进制文件：开发最终产物，二进制是由流（指令流或字节流）构成的，是给计算机“看”的，不容易分析语句的语义	运行应用：在应用执行过程中，利用运行时插桩检测技术，检测应用真实运行加载的第三方组件
检测难度	难度小，源码文件包含信息完整，结果的可解释性与准确性较高	难度大，需要对提取常量字符串、部分类名称、函数名称等特征信息，再运用匹配算法进行相似度计算	容易，可通过运行时监控技术，检查程序运行时加载的第三方组件，可排除未执行加载冗余的组件，检测精度高
数据安全及便捷性	需要源代码，部分场景下客户无法提供，如供应商开发的软件	无需源码，上传包文件即可，数据安全风险小	无需源码，伴随应用执行，易于集成、监控、修复

表2-2 工具建设

SDLC能力一体化实践

在研发阶段的需求阶段，建立供应商和开源社区组件引入机制，对于使用的组件和各类工具包进行安全审查以明确可能存在的风险，建立黑白名单应用机制，将准入的组件清单纳入内部私有库，并根据安全情报动态调整，确保库内的组件库都是安全可靠的。同时在质量测试和安全测试阶段，应用引入的工具链进行二进制和源码级别的SCA分析，借助其他安全工具代码审计、IAST或DAST的安全扫描，实现组件已知漏洞和系统开发引入漏洞的闭环管理。

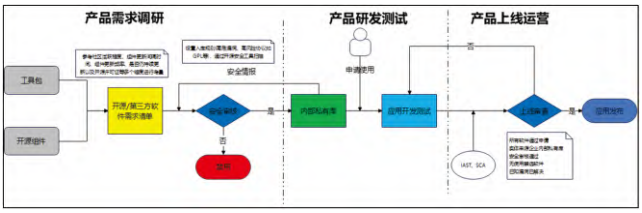


图2-3 SDLC能力一体化实践

实施难点与风险问题及团队分工

人员的问题是实施过程中的最大的难点和风险所在，一方面是外部专家包括咨询专家和第三方厂商对接专家的变动可能导致项目出现认知或资源偏差问题而无法保质保量交付内容达到预期效果，所以需要建立核心干系人的清单维护及人员管理工作，另一方面是内部人员的配合支持方面，供应链治理牵涉多个部门需要各个团队共同配合支持，建立相应的培训考核机制，通过培训宣贯及强制要求等措施，确保各条线职责明确、分工具体、理解到位、执行可靠，实现紧密配合，同时建立检查机制，对上线后出现的问题进行层层追责，明确风险源头所在，找到失效点。和内部第三方系统的对接需要从多方面考量，一是开源组件治理平台的成熟度和标准接口是否规范，是否能够匹配对接需求，对于不能提供标准接口的内部系统考量定制化开发的需求及排期问题，二是内部的一些系统如DevOps等平台的功能是否完善做好功能开发排期，以及对应的流程如何以比较恰当的方式做到最小化的干扰，避免影响现有流程的机制和效率。产品的误报问题，需要综合多方面因素进行调优和实践，将误报率和漏报率调整到比较均衡的状态，同时前期增加人工的审核环节可以加快调优进程。

风险类	风险项	触发点	造成的问题	解决方案
项目风险	咨询人员变动	项目进行中，相关开源安全咨询专家及厂商项目人员变动	核心成员的流动会影响项目进度，人员变动容易引起交接资源有误差，进而也影响任务进度	项目团队核心人员全程参与实施、记录项目文档，保证项目交付后相关技术和文档顺利移交
	人员意识不足	开发/运维/测试/PMO等条线人员对管理制度、流程、规范和要求理解存在偏差	制度流程建设未达到预期目标	运用平台固化制度，进行相关制度培训和考核，以及建立检查和追责机制。
	产品对接风险	与现有DevOps，Git以及JFrog制品仓库对接失败	对接缺失，短时间内无法实现项目目标	前期进行充分POC测试
产品风险	产品检测误报	检测中发生大量误报	误报太多无法进行治理修复	前期进行POC测试，要求厂商进行调优，减少误报，必要时人工复核
	产品数据风险	项目部署完成后，项目实施或产品运行过程中，存在人员失误或故意泄露重要信息数据	造成漏洞数据泄露风险	与每个项目人员签署正式的项目服务协议，项目实施过程中对项目内容、产品数据严格保密等相关违约责任的条款

实施后各主要相关部门的职责分工如下：

开发部门：了解相关开源组件引入和使用流程，对存量开源软件进行维护和升级。

研发管理部：制定和修正相关制度流程，推进工具平台化建设，及时推送通知相关开源软件情报信息，对相关制度和流程进行审查。

安全合规部：研发管理部协同安全和合规部督促相关开源问题的整改。

后续工作规划

1. 测评认证

根据外部咨询专家要求准备送审材料进行开源治理能力预评估，通过有权威背景的测评机构的开源治理能力成熟度测评认证，得到外部机构背书和认可，并根据测评意见进一步加强开源组件治理的丰富度和全面性。

2. 持续监测

对引入的评估模型持续监测和修正，对新增以及存量的

开源软件进行全面的盘点，对遇到的相关开源软件风险如漏洞、许可证以及合规等问题持续推进整改，保证开源组件的整个应用过程中的安全可靠性。

价值收益：体系完善安全赋能

建设组织、制度、流程及工具，全面落地开源治理体系

结合组织、制度、流程以及工具建设，实现对开源软件的引入、使用及运维安全可控，全面落地公司开源治理体系。

梳理开源软件，建立企业级开源软件台账

梳理公司开源软件资产，建立企业级开源软件台账。面对后续风险实现可查询、可定位、可修复。

落实《意见》要求，“安全”和“合规”双向并行

满足监管机构针对开源方面的要求，开源风险从被动应对到主动防御，更有效的控制开源风险。解决目前公司潜在的“安全”和“合规”问题。

为行业内可信开源的探索提供研究案例

在证券行业率先开展开源治理体系，在规避开源风险的同时，为行业内可信开源的问题开展研究和探索贡献微薄力量。

总结

本文在背景分析和现状梳理的基础上论述了供应链开源组件治理的必要性；通过难点解析、提升方向规划阐述了研究的可行性；在架构设计和落地实践层面提供了完整的供应链开源组件治理路径和方法模型体现了研究的落地性；最后在价值和收益方面释义供应链开源组件治理的价值体现，为行业开源组件治理提供了案例研究和探索方向。

参考文献

1.赵佳萌,路向宇,吉达勇等.开源组件漏洞治理实践与思考[J].金融电子化,2021,No.314(11):65-66.

2.周靖,马冰,王晓平等.开源组件治理的实践与思考[J].金融电子化,2022,No.317(02):29-30.

3.代铁.构筑开源管控体系 助力科技扬帆远航——北京银行开源技术安全可控性的探索和实践[J].金融电子化,2021,No.315(12):41-42.

4.纪守领,王琴应,陈安莹,赵彬彬,叶童,张旭鸿,吴敬征,李昀,尹建伟,武延军.开源软件供应链安全研究综述[J].软件学报,2023,34(03):1330-1364.

5.芦天亮,袁梦娇.开源软件供应链安全分析与防范对策[J].保密科学技术,2022(12):27-31.

安全实践

05 IPV6实践

海通证券IPv6安全演进与实践

文｜吴晨炜、马冰、王东

海通证券股份有限公司

摘　要： 随着IPv6网络规模不断扩大，承载的新应用不断涌现，IPv6流量对网络安全也带来新的挑战。顺应IPv6网络的演进：从“能用”到“好用”，最后实现“爱用”，不同阶段需要采取相对应的安全运营措施，从而保障IPv6演进阶段下的网络安全。本文归纳总结了IPv6规划中的演进路径对安全运营的影响，IPv6协议对网络安全新的挑战以及海通证券在新挑战下的安全运营实践。

关键字： IPv6、网络安全、安全运营、网络架构

IPv6行动计划整体安全观

我国IPv6推广历经两个阶段。一是2011年前，应对IP地址不足。二是2017年中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》，希望借助IPv6在新业务支撑与安全性上的变革，扭转网络安全的严峻形势。近日，工业和信息化部等八部门关于《推进IPv6技术演进和应用创新发展的实施意见》，提出到2025年底，IPv6技术演进和应用创新取得显著成效，网络技术创新能力明显增强，“IPv6+”等创新技术应用范围进一步扩大，重点行业“IPv6+”融合应用水平大幅提升，安全保障能力显著提升等方面明确了具体的发展目标。

攻击者可以利用IPv4缺乏地址可信验证机制的缺陷，随意发起网络攻击。IPv6增强可信与溯源能力，可以极大遏制网络资源被攻击者滥用，建设安全、可靠、便捷的网络基础设施。

IPv6对安全的影响分为三个方面：IPv6能解决的威胁问题、无法解决的问题、新引入的安全问题。同时，IPv6广泛使用后产生了新的业务场景，如SCTP、SRV6等新协议的使用，“东数西算”模式的支持，在业务链、APN、安全资源池广泛使用后带来的新的安全需求。新场景也对安全基础技术机制产生了影响，必须进行算法和原理上的创新，适应IPv6环境的新要求。

IPv6演进与对安全的影响

IPv6规划中的演进路径

Ipv6演进路径分为“能用、好用、爱用”三个阶段。

1.“能用阶段”：安全技术在传统场景下完成适配，合规可用

网络基础设施支持IPv6，满足IPv6网络环境下的安全功能要求。主要挑战包括：

· Anti-DDoS、防火墙、网络入侵检测/网络入侵防御、日志审计、态势感知等安全产品的IPv6 Ready协议适配与升级改造；

· 识别在IPv6下安全产品功能和使用的变化，进行适应性改造。

2.“好用阶段”：针对新领域新挑战，完成对应IPv6安全技术变革

安全功能和特性须适应物联网、5G、安全服务化、边缘计算等新业务场景，表现超越IPv4的安全竞争力。主要挑战包括：

· 针对IPv6下的SRv6等上层协议的应用与需求，开发新的安全特性；

· 针对IPv6安全方案端到端应用场景，识别身份认证、零信任、运营管理等领域的IPv6新挑战与需求。

3.“爱用阶段”：突破安全“根技术”，达到自主可控/安全治理目标

形成完善的IPv6安全生态，在关键产品、DNS等核心网络基础设施、关键技术上借助IPv6带来的技术变革机会，实现全面的自主可控与“根技术”突破，为国家数字化转型提供安全可信的产业数字化底座。

IPv6对网络安全的影响

1. IPv6协议族的变化

IPv6协议族在修正IPv4中的主要安全缺陷的同时，极大增强了协议自身安全性，变化主要包括：

· 地址变化：网络IP地址结构扩大，IPv6地址层次化清晰，地址类型新增任播，消除广播；

· 报文头变化：简化基本头信息，新增了扩展头信息，新增流标签；

· 协议栈变化：新增NDP协议，ICMP、DHCP协议演进为ICMPv6、DHCPv6。

对比维度	对比要素	IPv4	IPv6	影响分析
地址	长度	32bit	128bit	本质的改进，近似无限的空间
	结构	层次化不清晰	层次化清晰	汇聚地址构造，可赋予地址地域和机构标志
	生成方式	分配或配置	自动生成	自动配置通过加密地址生成方式(CGA)，与公钥绑定
	类型	单播多播广播	单播组播灵活	组播将是很普遍的通信方式，消除广播
报文头	基本头	复杂	流标签	基于流的路由、流量和业务的管理
	路由头 分片头	----	Hop，Route Dest，Frag	路由灵活，可用于流量牵引； 取消分片，消除攻击隐患
	安全头	----	AH， ESP	增强IPv6协议和基础设施自身安全性
	移动头	----	Mobility	移动内嵌
	其他头	----	HIP等	
关联协议	控制消息	ICMP	ICMPv6	解决广播放大攻击
	域名	DNS	DNSv6	增加了安全设计，防止DNS欺骗
	地址生成	DHCP	DHCPv6	增加IP地址管理中的设计安全性（CGA）
	地址映射	ARP	ND/SEND	有效防御各种Snoop攻击，实现地址验证等（CGA）
	组播	IGMP	MLD	

表1 IPv6和IPv4协议不同

2. IPv6自身安全能力增强

IPv6协议栈可提供地址可信与自身协议安全等增强的安全功能：

· IPv6地址长达128 位，海量地址空间扫描几乎不可能；通过CGA以及原地址验证技术，提供源地址检查技术手段；

· 可通过加密方式生成IPv6地址，支持隐私头；

· AH和ESP是IPv6的扩展头，IPsec用于保障安全；

· IPv6的DNS等相关协议增加安全设计，减少域名欺骗、网络钓鱼等攻击；

· IPv6下的NAT，对于需要隐藏真实地址的用户，可以使用IPv6 NPT协议隐藏内部IPv6地址。

3. IPv6对网络安全的有益效果

Ipv6协议栈对网络安全的有益效果包括：

· 攻击可溯源：地址层次化清晰，普遍采用GUA地址，无需NAT，网络追踪定位、攻击溯源更简单。

· 反黑客嗅探：扫描攻击难度大。

· 避免广播攻击：取消了广播地址，避免广播风暴和DDoS。

· 端到端的隧道机制: 扩展头AH、ESP实现报文传输的完整性、保密性提升

· 避免分片攻击：IPv6只允许端侧分片，避免中间安全设备的分片攻击。

4. IPv6带来的网络安全新挑战

IPv6协议栈对网络安全带来新的挑战：

· 资产管理：资产、漏洞管理难度增大，扫描探测在海量地址的场景失效。

· IPv4信誉库失效：基于IP地址的积累的威胁情报信息失效，海量的地址使黑白名单库的规格膨胀。

· 新增IPv6协议引入攻击： NDP等IPv6新协议仍然缺少认证机制,存在中间人攻击、地址伪造风险。

· IPv4-IPv6过渡机制：双栈机制、隧道机制、翻译机制引入新的安全风险。

· 新增的IPv6扩展头引入攻击：发送大量此类数据包消耗路由器等设备大量资源，造成DDOS攻击。

海通证券的IPv6实践

IPv6安全保障体系设计

1. IPv6对安全威胁的影响

从IPv6网络安全保障的角度，IPv6下的风险分成三类，一是IPv6下得到缓解或消除的安全威胁，包括地址空间增大影响的扫描类攻击、验证机制避免的欺骗类攻击、分片攻击等。二是继承IPv4的安全问题，包括海量IPv6地址的DDoS攻击、APT和应用层攻击IPv6流量的检测和还原、系统和协议栈漏洞利用攻击、海量地址带来的资产、漏洞和策略管理问题。三是IPv6新引入的安全问题，包括协议机制中的潜在缺陷、双栈机制引入的风险、工程实现上的漏洞。

2. IPv6对安全产品的影响

对产品实现的影响：产品对IPv6协议适配，支持全功能的IPv6协议栈和IPv4/IPv6双栈，处理IPv4和IPv6混合流量，实现难度和复杂度增加。

对安全基础技术的影响："资产扫描算法、黑白名单、威胁情报库、流量监测模型"等不再适用的安全机制，需改造算法。

威胁特征/情报库重建：新建IPv6威胁情报，需支持IPv6下的恶意文件还原、检测。

IPv6新场景与协议支持：支持IPv6、SRv6报文的采集、分析和检测；广域网需支持SRv6组网，带来业务编排和安全资

源池化新需求。

性能挑战：资产扫描和IP地址探测难度增大，IPv6地址解析性能消耗指数增长，安全功能消耗更多算力。

3. IPv6下的网络安全保障体系建设

IPv6安全保障体系设计，需特别关注上述继承风险、IPv6引入的新风险，以及IPv6网络对安全产品的影响。

海通证券的IPv6网络环境，由IPv6 Ready安全设备保障，符合“等保2.0”安全基线要求，包括：

产品	支持情况
防火墙+IPS/IDS	1、支持IPv6安全功能与策略，包括入侵检测、URL、AV、DNS过滤、带宽管理、NAT策略、IPSec6、SSL、DSVPN、L2TP、智能选路、NSH 2、网络特性（支持DNS、DHCP、动态路由、NSH） 3、高可靠性（支持双机、Iplink、BFD，跨DC集群）
Anti-DDoS	1、支持IPv4/IPv6双栈防御，流量检测、清洗和系统管理支持双栈管理 2、设备日志和策略下发支持IPv6 3、路由特性BGP Flowspec支持IPv6，MPLS LSP支持 IPv6 4、IP信誉、IP地理地址库支持IPv6
沙箱	1、支持通过IPv4与防火墙对接联动还原IPv6流量样本以及可视化展示 2、IPv6部署、沙箱IPv6流量还原
安全态势感知/运营管理系统	1、支持IPv6流量协议解析、安全日志对接、数据预处理、智能检索、威胁检测、底座（包括资产管理等基础能力）、安全管理（事件管理、智能检索、态势呈现）和安全响应（设备联动和响应编排） 2、IPv6威胁情报 3、管理面支持IPv6
上网行为管理	页面浏览控制，实时监控，应用控制部分支持，行为审计分析，核心功能均支持IPv6
漏洞扫描	基线核查等关键功能均支持IPv6
日志审计系统	支持IPv6环境安装、部署及访问、IPv6日志上报和解析
数据库审计	安装部署、协议审计、规则配置、统计报表均支持IPv6
WAF	访问控制和源IP解析等支持IPv6
堡垒机	整体支持基于IPv6的网络访问

表2 IPv6对网络安全设备影响

海通证券的IPv6网络安全保障体系由“威胁防御、内生可信、安全运营”三个体系所组成。各自对应了上表中的安全产品与技术。

4. 证券行业业务特点与IPv6组网模式

互联网服务区是金融/证券行业安全保障的重点，对外统一以B/S方式提供Web服务。互联网出口采用IPv6技术，无需使用NAT64、隧道等过渡技术，简化组网，避免了复杂的过渡技术引入的风险。

海通证券的IPv6组网示意图如下：

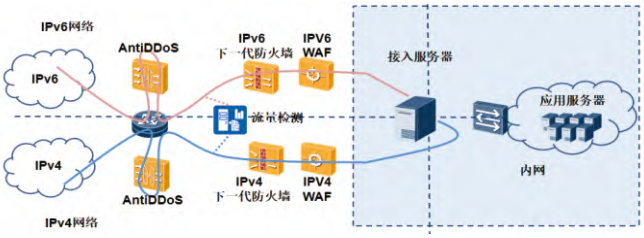


图1 互联网区域IPv6组网架构

海通证券的系统中独立设置了IPv4、IPv6两类对外访问接口，内部是经过IPv6改造的接入服务器，实现IPv6互联网业务接入至内网应用服务器。

Ipv6下的威胁防御能力建设

1. 典型组网下的威胁防御体系建设要求

IPv6安全保障体系要保证网络系统在各种风险下能够达到安全底线，需特别关注IPv6引入的新风险，以及IPv6网络规模化应用所带来的新的功能、性能需求。

海通证券威胁防御体系的目标是：在IPv4安全功能基础上，有效防御IPv6下的常见威胁，尽力而为地使系统不受外部攻击威胁影响。对IPv6威胁防御体系，参照“等保”功能基线要求，需要新增如下安全产品功能：

产品类型	主要功能
防火墙+IPS/IDS	基础网络功能、安全策略、入侵防御，反病毒，URL 过滤，内容过滤，AntiDDoS 等安全功能
接入网关	IPSec VPN、安全策略、GRE、策略路由等安全功能
Anti-DDoS	TCP、HTTP、DNS、UDP、ICMP、HTTPS、SIP 等攻击防御
日志审计系统	IPv6 环境部署及访问、接收解析识别 IPv6 格式日志
WAF	原有功能不变
沙箱	1、还原IPv6流量样本以及可视化 2、IPv6 部署和流量还原
堡垒机	基于IPv6的网络访问
安全态式感知/运营管理系统	1、IPV6流量协议解析、安全日志对接、数据预处理、智能检索、威胁检测、底座（包括资产管理等基础能力）、安全管理和安全响应（设备联动和响应编排） 2、IPv6威胁情报 3、管理面支持IPv6

表3 IPv6架构下网络安全设备功能

2. 防火墙/IPS/Anti-DDoS等IPv6网络安全设备功能与性能要求

(1) IPv6基本网络安全功能

IPv6下的网络安全设备功能涉及管理面、控制面和数据面的众多技术修改点。网元相关基础功能改造包括IPv6相关路由协议、ICMPv6识别过滤、IPv6下网桥、路由和混合工作模式、IPv6协议解析和过滤等，关键的网络安全功能改造如下：

安全功能	IPv6 影响	新的功能需求和改变
ACL/访问控制	五元组实施复杂 大部分流量被加密 上层分析可行性差	基于用户的 ACL，包括用户验证、针对用户的流量过滤规则
IDS/IDP	攻击流量被加密 新的攻击方式出现	匿名保密通信的解密 攻击流量与攻击者关联
SSL VPN	IPv6 自提供安全功能	传统功能可能消失 移动 IP 安全将是 SSL 的重点
IPsec VPN	IPv6 自身提供端到端安全 IKE 可能被替换	与地址绑定的密钥协商 IPsec 协议将采用扩展头
SIG/协议分析	部分流量从网络层加密	匿名保密通信的解密
AntiDDoS 功能	限制源地址欺骗 基于扫描的攻击将减少	源地址验证 基于正确地址的流量管理
终端安全	基本无影响	支持 IPv6 协议栈与事件采集

表4 IPv6网络安全设备功能与性能要求

(2)对IPv6新业务模式的支持

Ipv6网络中安全产品的服务化，可提高安全设备利用率，服务化改造需支持：

网络安全协同，基于SRv6业务链编排自动引流：通过网络控制器、安全控制器的协同，利用SRv6业务链技术，将流量按需动态引入安全资源池。

安全资源池化：通过防火墙多租户构建安全资源池，提供独立的IPS、AV、安全策略控制和防护能力。

安全业务自动发放：安全控制器实现安全防护策略下发。

(3)IPv6下的策略管理能力

IPv6地址空间大、长度长，安全设备难以再基于IP地址及五元组实现安全策略的配置管理。适应IPv6环境的改造方法包括适用于IPv4和IPv6业务流量共存的混合地址策略，可基于用户身份、网络域名和前后缀、网络应用、协议类型、协议标签、物理端口、流量方向、VLAN等非IP地址相关因子的安全策略，基于端口组、用户组、域名后缀组等特定实体分组的组策略，对接AD服务器、证书系统、域名系统的身份、标记识别的自动化策略，适用于多设备分布式部署场景的集中管理策略。

(4)IPv6下的网络安全设备性能要求

防火墙、Anti-DDoS等设备在实现双栈安全功能时，消耗IPv4业务的CPU、内存资源，导致IPv4会话表容量、新建速率、吞吐率等性能下降。根据IPv6协议特点评估，纯IPv6转发性能至少下降20%，双栈安全性能的下降随业务复杂性呈指数分布。

IPv6下防火墙、Anti-DDoS设备的性能指标要求如下：

· 硬件快转：IPv6报文硬件快转；

· IPv6转发高性能：大包100G/CPU，小包18G/CPU，会话新建80万/s/CPU，并发连接数4000万/CPU；

· DDoS防御高性能：NP硬件加速，单板小包防御100G，整机T级防御；

· CPU智能协同NP防御，毫秒级防御。

3. 对应用层安全设备WAF/DPI/日志管理/态势感知等设备的功能与性能要求

上述设备与网络协议不直接相关，安全功能无显著变化，只需支持IPv6协议栈分析，应用层安全能力（如协议识别、IPS、反病毒、URL过滤等）在IPv6网络中不受影响。

少部分网络协议在IPv6网络下变化，如DNS协议升级到DNSv6，对应的应用层安全检测一般通过产品软件版本升级来实现。

威胁分析与网络层协议弱相关，性能影响较小。

IPv6安全运营能力建设

基于IPDRR流程建设安全运营体系，充分利用系统内各产品安全能力，实现安全事件和异常的精准高效响应、处置。安全运营注重长期自动化能力建设，持续提高运营效率，降低人工要求和依赖。

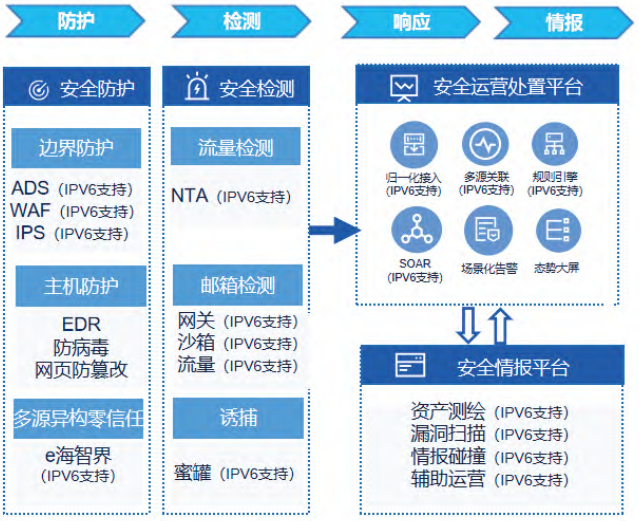


图2 IPv6安全运营架构

1. IPv6下对资产、分析处置等运营需求的挑战

· 海量地址探测

安全运营周期性进行资产测绘，以10Mb/s的速度进行资产扫描，遍历需5万年，挑战安全运营和攻击者。

· IPv6资产管理

IPv6规模部署，要求企业精细化管理CMDB，以精准有效的IPv6资产信息库、互联网资产实名率、收缩率等运营指标，实时管控企业的数字资产风险。

· 全网威胁发现

流量采集及分析需要支持IPv6、SRv6协议，覆盖全网IPv6区域，实现监测无盲区。

· 响应处置能力

IPv6地址空间和复杂度升级，无法纯人工完成地址封禁、事件调查等运营动作，同时日益丰富安全运营功能要求精准、快速、多平台协同的自动化响应和处置能力。

2. IPv6下对资产、分析处置等运营需求的对策

· 利用NDP协议：通过邻居节点的缓存表，发现本地网络主机；

· 利于DNS域名解析：通过域名反查工具，得到IPv6地址集；

· 通过日志分析：通过分析DPI、DNS、安全设备告警日志，得到活跃的IPv6地址；

· 网络安全分析能力：IPS、文件沙箱、旁路阻断产品，需支持IPv6报文解析及文件还原，发送IPv6重置报文，实现IPv6威胁检测和拦截；

· 编排响应技术：统一自动化编排防火墙、IPS、流量检测、DNS等设备安全能力，确保IPv6事件的精准、及时、标准化响应，并纳入处置案例库。

场景	SOAR编排效果
IPv6威胁情报感知	针对IP、DNS进行出网碰撞，基于CMDB定位资产
灵活IPv6地址域名封禁	实现多资源（IP/域名）多设备多策略封禁及解封
邮件响应	钓鱼邮件IOC封禁+自动提醒
运营赋能	针对告警进行IPv6情报、资产信息富化

表5 IPv6安全运营自动化编排

IPv6+金融骨干网的安全应用

IPv6不只是扩大了地址空间的IPv4，基于IPv6有一系列的新协议、新技术、新业务模式。SRv6是基于IPv6的新协议，在网络的端到端联通性、流量控制、网络可编程方面提供了IPv4下不可能提供的灵活功能：

· 基于对IP可达性的亲和性，使得不同网络域间连接更容易；

· 基于IPv6扩展头/SRH等可扩展性支持更多种类的封装，满足新业务的需求；

· 基于对IP亲和性和网络编程能力，实现IP承载网络与应用的融合，提升网络价值；

· 结合对更多地址空间的需求，进一步推广IPv6。

海通证券积极响应国家双千兆和IPv6+政策要求，促进公司金融服务创新，规划新一代基于IPv6+的金融骨干网，通过张江园区与南方中心SRv6骨干网切换，实现生产和测试各业务平面由当前IPv4 BGP协议切换到基于IPv6+的新技术SRv6的金融骨干网络，为整个骨干网SRv6打下基础。

图3 海通证券骨干网架构

1. 通过SRv6 EVPN实现不同业务安全隔离

海通证券金融骨干网络通过SRv6 EVPN为不同业务间提供逻辑隔离，保障业务安全：

海通张江数据中心：作为全功能主生产数据中心，提供云和非云业务部署环境，主要承载交易类、非交易类、办公管理类、互联网接入类、外联类、运维管理类等所有应用系统；另外规划了研发测试环境，承载开发测试业务；

东莞南方数据中心：作为异地灾备中心，提供云和非云业务部署环境，主要承载网上交易类、托管类、大数据类等应用系统；同时，作为交易所托管机房，就近接入深交所行情、交易线路，为托管客户提供极速行情交易服务；另外提供了研发测试环境；另外，作为集中交易等核心系统在异地实现应用级和数据级容灾备份，当中心故障，可切换至灾备中心接管服务；

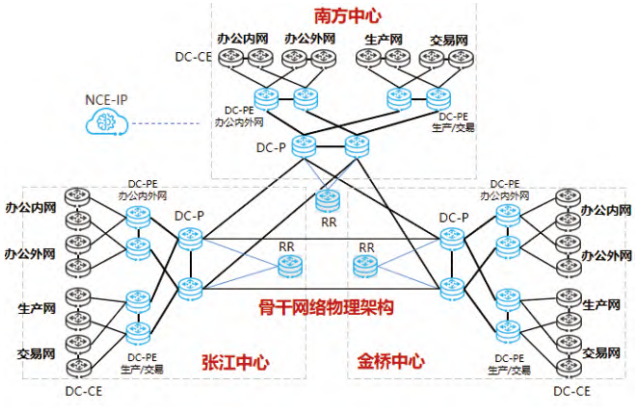


图4 海通证券SRv6骨干网架构

VPN规划原则：

· 按需部署原则：按需在对应的PE上部署VPN，办公内网/外网在对应DC-PE部署，生产/交易在对应DC-PE部署；

· 业务隔离原则：不同业务类型配置不同的VPN，实现业务间隔离；

· 安全隔离原则：不同业务类型配置不同的VPN，默认安全隔离；有互访要求推荐在防火墙跨VPN互访；

VPN的部署原则：

· 复用当前业务地址规划，不同VPN内路由不重叠；

· 根据现有业务部署四个独立的VPN，基于业务需求细化VPN规划；

· 多VPN场景下VPN路由默认隔离，有互访必要时通过推荐在防火墙上进行跨VPN互访；或者通过策略控制VPN间路由的导入；

· PE作为VPN业务的接入点（推荐子接口接入），P不需部署VPN，只做业务高速转发。

新建的IPv6骨干网实现PE与PE间的IPv4/IPv6私网业务业务互通，控制面通过EVPN传递VPNv4/VPNv6路由，转发面使用SRv6-Policy隧道承载。基于业务特征部署DSCP或者Color引流入不同的SRv6-Policy隧道。NCE控制器界面隧道路径流量可视，并根据带宽利用率，时延SLA进行路径调优。

总结

随着IPv6不断发展，在金融、科教、惠民等各领域进入实施部署的“深水区”，网络架构也将从早期的NAT形式至双出口模式，最终演变为单出口IPv4/IPv6双栈。安全运营在IPv6的趋势下，更重视自动化运营能力，通过自动化手段支撑互联网风险面的管理、威胁情报的赋能及安全事件的灵活响应，从而有效防范IPv6网络安全风险。

同时，SRv6凭借着软件定义网络、SRv6 Policy技术、智能化运维iFIT等技术在金融企业骨干网有大量实践，同时通过EVPN技术，实现了业务之间的逻辑隔离，保障了核心业务的安全带宽。

目前，我国IPv6网络“高速公路”已全面建成，至2025年底，将初步形成IPv6演进技术标准体系，形成以IPv6为核心的产业生态体系，打造超过1000个支持“IPv6+”技术能力的承载网络、企业/园区网络和数据中心；在每个重点行业打造20个以上应用标杆。海通证券的IPv6安全实践也需要不断演进，以满足IPv6下存在的新场景、新应用、新风险，从而充分发挥IPv6的价值。

证券行业IPv6网络规模部署的安全风险分析与应对

文丨宋士明、叶飞、姜玥

南京证券股份有限公司

摘　要： IPv6相比IPv4有诸多优势，能满足日益增长的互联网发展需求。为推动IPv6的广泛应用，我国正大力推进证券等金融行业IPv6规模部署，为行业数字化转型提供可持续的基础网络支撑，但也对网络和和信息安全带来了巨大挑战。本文从协议、设备、管理等方面，针对IPv6网络规模部署过程中可能面临的安全风险进行了分析，提出了相应的风险应对建议,为证券行业IPv6网络安全建设与健康发展提供参考。

关键字： IPv6、规模部署、安全风险、风险应对

前言

目前，我国正处于IPv6改造升级的关键时期，IPv6规模部署工作是网络强国战略的重要部分。根据国家IPv6发展监测平台数据显示，截止2023年4月，我国IPv6互联网活跃用户数量已达7.585亿，占我国互联网用户总数的71.08%。随着IPv6网络开始投入使用，针对IPv6网络的攻击数量急剧增加[1]，IPv6网络安全形势日益严峻。

在国家层面，2021年7月，中央网信办等部委发文明确要求持续提高金融服务机构面向公众服务的互联网应用系统IPv6支持能力，加强IPv6安全防护体系建设，强化复杂场景下IPv6安全保障能力；通过依托国家网络与信息安全信息通报机制，构建IPv6安全监测体系，提高IPv6安全态势感知、通报预警和应急响应能力。2021年11月，中央网信办等十二部发文指出要提高IPv6环境下漏洞监测发现与处置能力；推动IPv6网络安全产品和服务研发应用，探索在IPv6环境下新兴领域的网络安全技术、管理及机制创新。2023年4月，中央网信办等八部门发文明确指出要提升IPv6安全保障能力，强化IPv6网络安全防护，强化IPv6网络安全防护，推动IPv6安全应用。在国家大力推进IPv6规模部署的行动中，证券行业走在了前列。由于证券经营机构对网络安全稳定运行有极高的要求，在保障现有IPv4网络安全稳定运行的前提下，如何实现规模部署的IPv6网络安全稳定运行存在诸多挑战。

本文从IPv6安全风险分析，IPv6规模部署后面临的主要安全问题等入手，从技术和管理角度提出针对IPv6的安全部署建议，相关问题的探讨将有利于促进证券行业IPv6网络安全建设与健康发展。

IPv6的安全风险分析

IPv6协议的安全风险

IPv6与IPv4都是无连接的网络协议，使用相同的下层服务，并向上层提供相同的服务，从协议作用来看并无太大区别。但由于IPv6并不向后兼容IPv4，所以部署后会引入新的安全风险。下面将从IPv6与IPv4共有的安全风险、IPv6特有的安全风险、IPv6过渡机制的安全风险、对IPv6的安全误解等四个方面进行探讨。

1. IPv6与IPv4共有的安全风险

有多种攻击同时作用于IPv6与IPv4[2]，包括：(1)应用层攻击：如跨站脚本、SQL注入、DDoS等；(2)恶意设备：如恶意Wi-Fi接入点；(3)泛洪和所有基于流量的拒绝服务：比如RFC 6192中描述了一种使用非法IPv6流量攻击路由器控制平面的方法。此外，作为一个在实践中应用较少的网络协议，IPv6相关安全隐患还没有被发现和修复，且熟练维护IPv6网络的专业人才紧缺。

2. IPv6协议特有的安全风险

IPv6协议特有的安全风险主要包括其协议特点以及针对IPv6特有的攻击[3][4][5]，例如：(1)协议本身的安全特点。IPv6报文结构中引入的新字段（如流标签、RH0、路由头等）、IPv6协议族中引入的新协议（如邻居发现协议等）可能存在漏洞，被用于发起嗅探、DoS等攻击。此外，不同类型设备在实现IPv6协议栈时，可能存在因编码、实施造成的安全风险。(2) IPv6特有的攻击风险。如逐跳扩展头攻击、邻居发现协议攻击、DAD攻击、前缀欺骗攻击、MLD攻击、使用嵌入IPv4地址的IPv6地址绕过防护问题、不使用NAT导致的端到端透明性问题、将IPv6隐藏于IPv6隧道带来的绕过安全检查问题

等。

3. IPv6过渡机制可能引发的安全风险

在IPv4向IPv6过渡的过程中，“双栈”、“隧道”、“翻译”是三种可能采用的过渡方案，均可能带来新的安全风险[4][5]，如表1所示，下面将分别详细阐述。

过渡机制	安全影响	攻击风险	安全优势
双栈机制	网络和风险并存	因一种协议栈安全隐患引发的各类攻击等	无
隧道机制	内置安全功能缺失	仿冒、泛洪攻击等	无
翻译机制	未改变机制内生特性	地址池耗尽攻击等	已具备成熟的安全防护机制
			仅需针对翻译节点设备部署安全防护策略

表1 IPv4/IPv6过渡机制安全性对比分析

(1)双栈方案的安全风险

双栈部署的网络中同时运行着IPv4、IPv6两个逻辑通道，增加了设备/系统的暴露面，也意味着防火墙、IPS、WAF等安全防护节点需同时配置双栈策略，导致策略管理复杂度加倍，防护被打穿的机会增多。IPv4网络中，部分操作系统缺省启用了IPv6自动地址配置功能，使得IPv4网络中存在隐蔽的IPv6通道，由于该IPv6通道并没有进行防护配置，攻击者可以利用IPv6通道实施攻击，如图 1所示。此外，双栈系统的复杂性也会增加，导致网络安全防护节点性能消耗增多和故障率变高。

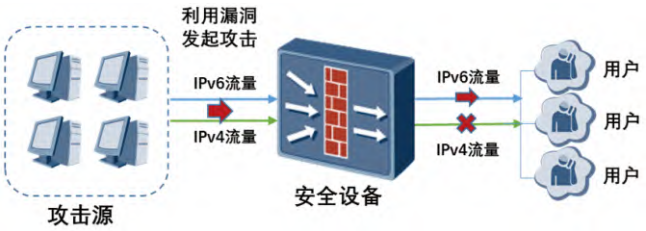


图1 双栈方案的安全风险

(2)隧道方案的安全风险

在隧道环境下，部分隧道方案仅要求隧道出入口节点对报文进行简单的封装和解封，缺乏内置认证、加密等安全功能，导致攻击者可能截取隧道报文，伪造用户地址并伪装成合法用户发起攻击。以IPv6 Over IPv4为例，存在攻击者可伪造内外层IP地址发起仿冒攻击等安全风险，如图 2所示。此外，由于部分隧道方案未采取对隧道封装内容的检查，攻击者可将IPv4流量承载在IPv6报文中，导致原来IPv4网络的攻击流量经由IPv6的“掩护”后穿越安全防护而造成威胁。

图2 隧道方案的安全风险

(3)翻译方案的安全风险

翻译方案也称协议转换，为IPv6网络节点与IPv4网络节点相互通信提供透明的路由。作为IPv6与IPv4互连节点，翻译节点易造成安全隐患，其面临地址池耗尽等常见DDoS攻击威胁，攻击者可通过伪造大量IPv6地址向翻译节点发起地址转换请求，消耗其地址池IPv4资源，同时导致合法用户无法获取IPv4地址，进而引发IPv4网络无法正常访问，导致网络瘫痪，如图 3所示。

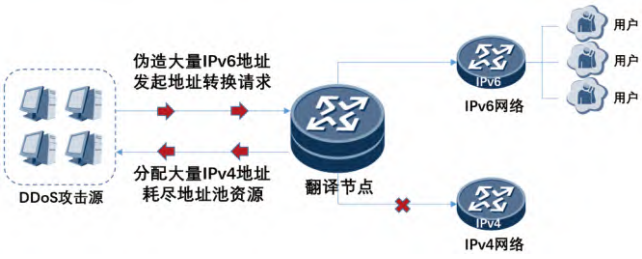


图3 翻译方案的安全风险

4. 关于IPv6协议的安全误解

关于IPv6协议的安全误解有很多，下面仅分析其中三个典型的[2]：

误解一是由于IPv6巨大的地址空间，无法通过枚举/64子网中所有的IPv6地址来进行网络扫描，因此黑客无法定位攻击目标。但RFC 5157描述了可用来寻找网络上潜在目标的替代技术，如枚举区域内所有的DNS名称；RFC 7707中也给出了有关IPv6网络探测的其他做法。

误解二是由于IPv6强制要求使用IPsec，因此它更安全。虽然最初的IPv6规范可能暗示了这一点，但RFC 6434明确指出并不强制性要求支持IPsec。如果企业内部的所有流量都被加密，那么不仅是恶意软件，那些依靠检测Payload的安全工具，如下一代防火墙、入侵防御系统、网络威胁分析等都会受到影响，实际上IPsec在IPv6中的用法与IPv4一致，如用于在非可信网络上建立VPN通道，或为某些特定应用预留。

误解三是由于IPv6不再有广播，因此在IPv6中不存在放大攻击（如SMURF）。这也是不对的，因为路由器和主机在转发或接收组播消息时，在某些情况下会产生ICMP错误或信息消息（见RFC 4443的2.4节）。因此，在IPv6网络中也必须像IPv4一样限制ICMPv6报文的生成和转发速率。

安全设备IPv6支持度亟待提升

随着IPv6在全球范围内的部署发展，主流网络厂商研发了大量的IPv6网络产品，产品类型丰富，根据《2021全球IPv6支持度白皮书》[6]，获得IPv6 Ready Logo测试认证的设备中，交换机和路由器等网络设备的型号已超过900个，几乎涵盖了绝大部分的网络产品，能够满足基本商用部署需求，而防火墙、IDS、WAF等安全设备获得IPv6 Ready Logo认证的占比相对较少。此外，启用IPv6将分别对网络层安全设备和应用层安全设备产生一定影响，如表2所示，下文将分别详细讨论[4]。

所在层	类别	影响设备	安全影响
网络层	访问控制	防火墙	缺少 NAT 防护，错误配置或忘记配置访问控制策略会导致按安全风险
	设备性能	安全设备	部分安全设备的处理能力明显降低，出现故障概率增加
	隧道	VPN、防火墙	存在虚假数据包跨越的可能
应用层	报文解析、规则匹配、漏洞扫描、日志记录	IDS、IPS、WAF、	影响对安全事件和漏洞的发现能力

表2 IPv6对安全设备的影响

1. 网络层安全设备

IPv6环境下所有设备均可使用全球单播地址，不需要使用NAT即可实现互通，天然缺少NAT形成的防护。因此，防火墙（或其他安全设备）的安全域划分与访问控制需要更加严格管理，一旦出现如“可以访问任意目标IP与端口”的错误配置将会造成更大风险。在IPv6与IPv4混合网络中，防火墙等网络层安全设备需要同时配置双栈安全策略，对设备的功能、性能的要求更高，出现单点故障的概率增加。此外，由于IPv6地址长度大于IPv4，原IPv4防火墙软件升级支持IPv6后，在硬件规格不变的情况下，防火墙会话表、地址簿容量等内部数据结构的条目数量可能减少，影响设备性能或安全防护能力。混合使用支持和不支持IPv6的设备也可能带来安全风险，如RFC 7359提及了一个不容易想到的情况[7]，远程访问VPN客户端可以操纵本地路由表，重定向所有或是指定目的地的流量到隧道，然而由于有些VPN客户端软件本身不支持IPv6或是未配置IPv6的分割隧道，这将导致它们无视IPv6路由表的存在，任由本应流经隧道的流量被操作系统通过本地IPv6转发至互联网，造成网络安全事件。

2. 应用层安全设备

WAF、IPS、IDS等应用层安全设备的IPv6报文解析能力、IPv6地址格式配置（如黑白名单等）功能可能不完善；包含安全功能的网络设备（如流量控制等）也可能存在类似风险。在IPv4环境下，系统漏洞扫描、WEB漏洞扫描等设备一般按照C段/B段地址进行扫描，目前主流的网络扫描设备可对外网或内网IPv4资产进行全面扫描。但IPv6地址长达128位，是IPv4的296倍，即使按IPv6默认的最小前缀划分区域（264个地址）进行扫描，也难以实施。上网日志留存系统在进行日志生成的过程中，需将Radius等设备的用户上网认证记录和防火墙NAT日志进行关联，可能存在不同系统间IPv4、IPv6匹配不一致的情况，导致日志缺失。

IPv6对安全管理的影响

当前，由于还缺少相配套的安全管理措施，IPv6网络部署实施将对现网的资产暴露面管理、域名解析管理、安全运营管理产生影响[4]，如表3所示。

类别	安全影响
资产暴露面管理	影响资产发现、资产指纹、基础威胁情报的获取
域名解析安全管理	影响 DNS 数据安全防护和 DNS 解析行为
安全运营管理	安全运营设备设备需提前进行 IPv6 改造，启用 IPv6 并支持双地址关联分析等

表3 IPv6对安全管理的影响

1. 资产暴露面安全管理

IPv4网络广泛使用NAT技术，所有节点隐藏在NAT节点后面。但使用IPv6后，如网络边界未能部署有效的安全设备及访问控制策略，则内网主机IPv6地址将裸露在互联网上，外网IPv6地址可以直接端到端连接访问内网IPv6地址，从而带来极大的安全风险[8]。由于当前互联网资产暴露面以“IP地址+端口”作为标识，IPv6网络规模部署后，对于资产暴露面探测、资产暴露面指纹获取、和基础威胁情报的获取及分析工作均将受到影响，如：（1）资产暴露面探测方面，目前的资产发现主要是通过扫描工具对IPv4地址段进行扫描，在IPv6环境下广泛的地址扫描已不可行，IPv6的规模部署对资产暴露面的远程探测能力提出了更高的要求；（2）资产暴露面指纹获取需要资产指纹扫描工具具备对IPv6的支持，部分设备与系统需改造升级；（3）IPv6威胁情报缺失。恶意IP地址及IP归属地是当前威胁情报分析中用到的最基本的情报，IPv4这类情报易得、准确率高。但目前现有的威胁情报库很少包括恶意IPv6情报，甚至存在地理位置归属不完善、定位不准确的现象。因此在IPv6规模部署过程中，IPv6威胁情报体系需要进一步加强建设。

2. DNS系统安全管理

由于IPv6地址较长，难以记忆，IPv6网络访问通常使用DNS域名解析，所以DNS系统对于IPv6网络安全运行的重要

性不言而喻。IPv6规模部署后，将对DNS安全防护、DNS解析行为等方面带来安全影响[8]，如：(1)应更加重视DNS系统的IPv6记录保护。DNS系统的IPv4记录的域名解析请求主要来自NAT设备的IP地址，而IPv6的DNS解析请求主要来自于用户设备的IPv6地址，DNS系统日志将保存大量用户真实IPv6源地址信息。入侵DNS获取DNS系统日志数据，将成为黑客获取用户真实IPv6地址的重要方式。一旦DNS系统日志被窃取，可能造成大量用户IPv6真实地址数据泄露。因此，预计未来在IPv6网络上，DNS系统将成为黑客的主要攻击目标，DNS安全防护的重点不仅是传统DDoS攻击，还要包括DNS系统自身安全和日志数据安全。(2)虽然目前主流操作系统都已支持IPv6的DNS解析，但解析行为有所区别。例如，对于不同操作系统，在优先使用IPv4还是IPv6发起DNS查询请求、优先查询A记录还是AAAA、记录查询得到2个记录时优先使用A记录还是AAAA发起连接、IPv6不可达时终端是否可以回退到使用IPv4等方面的行为有所不同。经过实际测试，微软的OS优先使用DNSv6，优先查询A记录（除XP）。苹果OS优先使用DNSv4，优先查询AAAA记录。全部OS优先使用IPv6（AAAA记录）发起网络连接。当IPv6不可达时，微软IE回退较慢，最长达70秒，用户体验差，苹果浏览器能够快速回退。为满足监管机构技术指标要求，应针对不同客户端进行IPv6 DNS解析的详细测试。

3. 安全运营管理

除基础网络和安全防护设备外，安全态势感知、SIEM、SOC、堡垒机、零信任网关、邮件安全网关、防毒墙、统一身份认证、欺骗防御系统等安全运营管理类系统，同样需针对IPv6环境进行改造优化。对于SIEM、SOC等具备日志收集功能的系统，特别需要注意是否具备IPv6地址日志收集解析以及对同一设备IPv4和IPv6双地址关联分析能力。此外，在IPv6规模部署过程中，网站安全监控、数据库安全审计、网络DLP等系统需及时升级支持IPv6，否则将存在业务系统提前改造而无法进行IPv6安全监管的风险。

IPv6安全风险应对

综合前文分析，IPv6的规模部署将会带来一定程度的新的安全风险。RFC 9099[9]从多个方面提出了通用的IPv6安全运营注意事项。证券经营机构需要从IPv6的安全规划、安全运营、专业人才队伍培养等多个方面加强建设，有效应对IPv6规模部署后带来的安全风险。典型的IPv6安全风险应对框架，如图4所示。

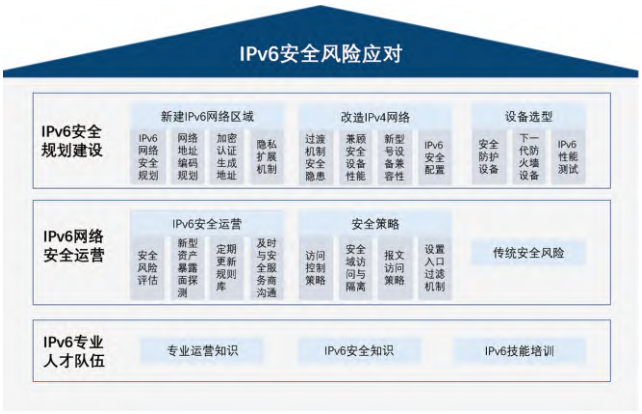


图4 Ipv6风险应对框架

做好IPv6安全规划建设

应结合相关网络系统的建设需要，全面梳理IPv6带来的安全风险，将IPv6安全方案包含在系统整体建设方案中。

1. 新建网络区域的IPv6安全规划

对于新建IPv6网络区域，证券经营机构应提前做好网络安全规划，制定具体实施方案和推进工作计划，明确涉及的关键产品、网络及业务范畴，按照优先级分步骤实施。统筹IPv6地址申请、分配等管理工作，严格落实IPv6网络地址编码规划方案。应充分利用IPv6逐级、层次化分配密码生成地址的方法，对生成地址进行加密认证，防止设备仿冒接入和中间人攻击，从而消除源地址欺骗和利用邻居发现协议攻击的隐患。针对IPv6网络没有地址转换而带来的内网结构及相关信息暴露问题，可利用IPv6新增的隐私扩展机制，隐藏真实的通信地址，防止关键信息暴露，确保网络安全。

2. 改造现有网络的IPv6安全方案

对于现有网络的IPv6改造，应深入了解各类IPv4/IPv6过渡方案可能带来的安全隐患，与设备厂商充分沟通，制定合理IPv6改造方案。如升级设备固件，应考虑升级后为兼容IPv6地址空间而可能带来的问题，如防火墙会话表容量、地址簿容量、新建连接速率、网络吞吐性能可能会出现不同程度的降低；如更新设备型号，应考虑新型号设备中新特性可能引入的兼容性问题。同时应做好相应IPv6安全配置，避免应错误配置引入安全风险。

3. IPv6安全设备选型

在设备选型方面，安全设备需支持纯IPv6（IPv6-Only）环境下、过渡期间IPv4/IPv6双栈部署等场景的功能需求，具体可参考人行科技司印发的“银科技〔2019〕33号文”《金融行业IPv6规模部署技术验证指标体系V1.0》中“IPv6自身安全”及“IPv6部署安全”两项。主要要求有：(1)下一代防火墙设备需要支持IPv4/IPv6双栈协议及过渡时期的常用隧道技术，同时其集成的应用层网关需支持IPv6解析，应用识别、病毒检测、入侵防御等功能所需的规则库应支持升级，以支持纯IPv6或IPv4/IPv6双栈场景；(2)在IPv4/IPv6双栈环境中，应充分考虑IPv4和IPv6两个逻辑通道的安全需求，安全设备应

具备对安全策略配置进行一致性检查等能力；(3)应进行IPv6性能测试，验证IPv6网络区域的二三层网络设备、负载均衡、防火墙、WAF等系统或设备的性能(CPU、内存、IO)不高于影响系统运行的阈值。此外，新设备上线前应采用行业IPv6安全基线进行配置，不得使用默认配置，避免带来安全隐患。

加强IPv6网络安全运营

1. IPv6日常运营要点

在日常网络安全运营工作中，证券经营机构需要从以下几个方面加强IPv6的网络安全运营，如：(1)对于IPv6环境下新业务上线，应严格开展IPv6安全评估，根据评估结果进行整改加固，未经评估不得上线；(2)构建安全态势感知和重点业务安全保障两方面能力，通过构建针对IPv6的安全态势感知、威胁情报分析能力，开展主动防御；(3)在运行阶段，开展周期性IPv6风险评估、监测和审计，确保IPv6安全能力始终符合国家及行业监管要求；(4)研究新型资产暴露面探测方式，以应对IPv6网络难以进行全量扫描的情况。(5)定期更新和优化IPS、WAF、安全态势感知、威胁情报平台等安全系统中的各类安全规则库和IOC库(如恶意攻击IPv6地址等)；(6)及时与安全服务商沟通需求，确保其具备针对IPv6的设备维保、漏洞挖掘和渗透测试能力，及时发现IPv6安全隐患，提升IPv6网络和系统安全能力；(7)应定期开展IPv6安全测试工作，及时发现设备及信息系统IPv6相关漏洞，避免设备“带病”入网。

2. IPv6安全策略配置

在安全策略方面[10]，由于IPv6协议与IPv4有所不同，尤其需要注意以下几个方面的风险应对，包括：(1)在防火墙、路由器、入侵检测和上网行为管理系统等安全设备上配置满足业务需要的访问控制策略，应关闭不必要的服务、禁止源路由，并实施单播反向路由查找技术，防止基于源地址欺骗的网络攻击行为；(2)根据实际需求，做好IPv6网络安全域的隔离与访问控制，采用恰当的网络过滤机制，实施IPv6网络接入许可。(3)需谨慎设置ICMPv6报文的访问策略，根据实际情况设置合适的安全措施，如配置ACL白名单，仅允许必须的ICMPv6等报文通过，接口关闭ICMPv6重定向、端口停止发送RA消息，关闭发送ICMP不可达信息，关闭源路由，防止Type 0 Routing Header攻击等，以免影响正常的服务和应用。(4)在防火墙上需设置扩展头检测规则，设置具有选择发送和重组到网络中间设备的分片的能力，并支持防范DDoS攻击，能识别、过滤Type0类型的路由扩展头报文；(5)在边界安全设备上启用入口过滤机制，以减少网络间的源地址伪造威胁，做好边界防护。

3. 传统安全风险防范

在传统安全风险方面[10]，IPv6继承了IPv4的一些应用层的安全风险，因此传统的IPv4网络安全技术和管理体系同样适用于IPv6。一要未雨绸缪，安装防病毒软件，在主机终端建立防护机制。二要筑牢防线，配备堡垒机、防火墙、IPS、WAF、上网行为管理器等网络安全防护系统，防止外部攻击，管控上网行为，严格实现内外网隔离。三要防止泄密与欺诈，使用数据加密和身份认证技术，确保数据完整可靠。四要选用有自主知识产权自主可控的软硬件系统，提高系统与设备自身的安全可靠性。五要提高人员安全意识，建章立制，合理分配权限，严防内部作案。六要做好IPv6相关应用的压力测试、渗透测试，开展安全攻防演练，全面评估IPv6系统的安全风险，及时修复系统漏洞，从根本上防范IPv6协议自身带来的风险。

培养IPv6专业人才队伍

在IPv6规模部署及运行过程中，证券经营机构面临的针对IPv6的最大安全风险可能就是缺乏专业的IPv6安全知识与技能。IPv6环境下引入了扩展头攻击、NDP攻击等安全新威胁，使现有IPv4安全知识和经验难以直接应用到IPv6环境中，给安全技术人员带来新的挑战，导致IPv6相关业务系统的运维存在安全隐患，大量防御薄弱的IPv6协议栈将成为攻击者实施网络攻击的新突破口。安全技术人员的IPv6知识储备不足，将导致无法充分认识和理解IPv6安全问题，很难有效应对IPv6安全威胁。如某日负载均衡设备无法正常探测IPv6业务端口，经排查，原因是防火墙默认阻断了ICMPv6协议的邻居发现报文所致。因此，培养IPv6专业人才队伍，加强技术人员的IPv6安全知识和技能培训，切实提升相关工作人员IPv6安全能力，是证券经营机构当务之急的一项重要工作。

结束语

IPv6将彻底改变原IPv4时代的网络形态，特别是纯IPv6网络将变得彻底扁平化。本文从IPv6协议本身、安全设备、安全管理等三个角度，分析了IPv6网络规模部署后可能带来的相关安全风险，并从规划建设、安全运营、人才培养等方面提出了相应的IPv6安全风险应对措施。证券经营机构只有坚持发展与安全并举，做到安全技术及管理与IPv6网络规模部署同步规划、同步建设、同步运行，才能打造出自主可控、安全可靠的IPv6网络。

参考文献

1.2021年上半年我国互联网网络安全监测数据分析报告[EB/OL]. 国家计算机网络应急技术处理协调中心.[2021.7].https://www.cert.org.cn/publish/main/upload/File/first-half%20%20year%20cyberseurity%20report%202021.pdf

2.K. Chittimaneni, T. Chown, L. Howard, et al. Enterprise IPv6 Deployment Guidelines[EB/OL]. IETF RFC 7381. [2014.10]; www.rfc-editor.org/rfc/rfc7381.txt

3.E. Davies, S. Krishnan and P. Savola. IPv6 Transition/Co-existence Security Considerations [EB/OL]. IETF RFC 4942.[2007.9]; www.rfc-editor.org/rfc/rfc4942.txt

4.IPv6安全白皮书[EB/OL].中国移动通信集团有限公司.[2018.12]. http://iot.10086.cn:81/Uploads/file/news/20181205/20181205173726_92618.pdf

5.筑牢下一代互联网安全防线—IPv6网络安全白皮书[EB/OL].中国信息通信研究院.[2019.9].http://www.caict.ac.cn/kxyj/qwfb/bps/201909/t20190918_211484.htm

6.2021全球IPv6支持度白皮书[EB/OL].下一代互联网国家工程中心.[2021.8]. https://www.ipv6ready.org.cn/public/download/ipv62.pdf

7.IPv6安全隐患的第一大来源[EB/OL].宋崟川.[2018.7].https://www.ipv6-cn.com/2018/07/10/IPv6-security-reflections-1.html

8.赵肃波.中国IPv6发展与网络安全挑战[J].信息安全研究,2019,5(3):261-272.

9.É. Vyncke, Chittimaneni, K., Kaeo, M., and E. Rey. Operational Security Considerations for IPv6 Networks[EB/OL]. IETF RFC 9099.[2021.8] ; www.rfc-editor.org/rfc/rfc9099.txt

10.何淑玲,陈世清.IPv6规模部署下网络安全风险防范[J].金融科技时代,2021,29(04):64-67.

安全实践

06 安全建设

国泰君安证券数据出境安全评估实践

文｜吴鑫涛、黄韦、俞枫

国泰君安证券股份有限公司

摘　要： 随着数据价值的提升，数据安全问题日益突出。我国相继出台《网络安全法》、《数据安全法》、《个人信息保护法》等一系列法规，规范了各行业数据安全管理。2022年9月，《数据出境安全评估办法》正式施行，确立了事前评估和持续监督相结合的原则。国泰君安证券率先通过国家网信办数据出境安全评估，成为全国首批通过该评估的证券公司之一，也是上海地区率先通过该评估的金融机构。这对提升国泰君安乃至金融行业数据出境安全治理水平具有重要意义，走出了行业在数据出境安全方面的实践之路。

关键字： 数据安全、数据出境安全评估、数据出境

引言

近年来，随着数据价值的不断提升，数据出境后遭到篡改、破坏、泄露、丢失、非法利用时有发生。国务院和国家相关管理部门不断出台相关法律，完善数据安全规范体系，《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》以及《关键信息基础设施安全保护条例》等一系列法律体系相继建立，要求各行业从业单位提高对于数据安全的重视程度，提高安全意识，定期进行数据安全检查，防微杜渐，避免数据安全问题发生。

2022年9月1日，《数据出境安全评估办法》（后简称“《评估办法》”）生效，正式确立网信部门主导的数据出境安全评估要求和门槛。根据《评估办法》，数据出境安全评估应当“坚持事前评估和持续监督相结合、风险自评估与安全评估相结合”的原则，即在数据出境安全评估的基础上设置“自评估”的前置要求。评估办法明确要求，在办法实施以前，已经开始的数据出境业务，必须在6个月内完成相应工作，报送相关资料。

国泰君安证券积极配合国家法律要求，适应行业特点，不断完善自身业务体系，提高公司的数据安全水平，率先完成自评估并获得通过，标志着数据出境安全治理在证券期货行业的率先落地。同时，该项目首次实现了证券经营机构与境外分支机构数据的合规出境，为经营一体化进程提供了有力支撑，也为证券期货持牌金融机构增添了全新的跨境服务创新驱动力。

金融行业数据出境趋势和影响

随着全球化和数字化的步伐不断加快，数据的跨境流通成为一种不可或缺的趋势。从全球范围看，数据流动对全球经济增长的贡献已经超过传统的国际贸易和投资，习近平总书记指出：“网络信息是跨国界流动的，信息流引领技术流、资金流、人才流。”如果数据不能自由跨境流动，跨国公司、跨境电商、全球供应链、全球服务外包等商业活动将难以有效开展，经济全球化下跨境数据已经成为新的生产要素。特别是在金融行业，这种趋势更加明显。在我国，随着金融市场的日益开放，数据的出境已经成为了金融市场双向开放的必然结果。数据跨境流动是金融高水平开放的重要内容，是实现金融强国不可回避的关键问题。中央金融工作会议提出，要着力推进金融高水平开放，确保国家金融和经济安全。为了更好地参与全球金融市场的竞争，我国金融行业必须在合规的前提下，推动数据跨境合规有序、高质量流转，提升金融服务的质量和效率，驱动金融行业高质量数字化转型。

数据跨境流通规模日益扩大，已成为提升数字经济发展质量，促进全球互联互通的重要途径。如何保障数据跨境安全、促进数据跨境有序流动，切实以安全保发展、以发展促安全，已成为国家和社会广泛关注和高度重视的问题。然而，数据出境的同时，也必然会带来一些风险和挑战。首先，数据安全和隐私保护问题是最关键的。数据跨境流通可能会导致数据泄露，增加金融机构和客户的风险。其次，数据跨境流通可能会带来法规合规的挑战，不同国家和地区的法律法规可能存在差异，金融机构需要处理好这些差异，避免违规。因此金融机构需要高度重视数据出境过程中数据安全问题。

数据出境流通对金融行业的影响深远。一方面，数据出境可以提高金融服务的效率和质量，加快金融创新的步伐。

数据是金融的基础要素，金融开放和合作需要数据跨境流通，促进跨境金融便利化。金融机构可以通过分析全球数据，预测市场趋势，为客户提供更好的金融产品和服务。另一方面，数据出境也对金融机构风险管理提出了新的要求。金融机构需要加强数据安全和隐私保护，确保合规，同时也需要利用新的技术，如区块链、隐私计算、大数据和人工智能等技术，提升风险管理的效能，完善数据跨境治理机制。

利用全球化的数据资源，提升我国金融市场的竞争力，必须要在合规和安全的基础上进行。数据跨境流通需要遵循我国和目标国家或地区的相关法律法规，特别是关于数据安全和隐私保护的法规。此外，数据出境的过程中，也需要防范可能出现的网络安全风险。

因此，我国金融机构在利用数据出境带来好处的同时，也需要重视和应对数据出境带来的风险和挑战。金融机构应该加强数据安全和隐私保护，提升数据出境的管理能力，确保数据出境的安全，以此来推动我国金融行业高质量发展和全球竞争力提升。

数据出境安全评估背景

评估背景

近年来，我国资本市场对外开放举措不断，多项改革持续推进，境内外市场加强互联互通，进一步推进资本市场双向开放，中国资本市场进一步与世界接轨。作为国内全面领先的综合金融服务商，国泰君安证券始终致力于为客户提供稳健全面的金融服务，积极探索“走出去”战略，在境外设立了以中国香港为中心的国泰君安国际控股等子公司，参与海外市场竞争，推动国际化业务，建立覆盖全球的业务网络和服务能力。为了提高数据保护能力、完善数据安全控制措施，公司积极履行国家相关法律法规要求，由国泰君安证券信息技术部牵头，联合数据平台运营部、法律合规部、数据中心等部门组成了数据出境安全评估联合工作组，在行业率先开展了数据出境安全评估工作，为行业探索数据出境安全评估方面的实践和经验。

评估场景

作为国内全面领先的综合金融服务商，国泰君安长期、持续为客户提供综合金融服务，积极推进国际化业务，在中国证监会批准下，开展合格境内机构投资者(Qualified Domestic Institutional Investors, QDII)、合格境外机构投资者(Qualified Foreign Institutional Investors, QFII)、人民币合格境外投资者(RMB Qualified Foreign Institutional Investors, RQFII)等业务，满足客户跨境交易需求，并建立了覆盖全球的业务网络和执行能力，努力建设成为中国资本市场全方位的领导者以及具有国际竞争力的现代投资银行。

为了更加高效的支持国泰君安集团国际化业务，实现集团境内外员工统一线上化、数字化管理，国泰君安证券建设了全连接电子公文系统。该系统包括了员工通讯录、工作签报、公司发文、印章申请、合同协议等功能，并面向集团全体员工开放。国泰君安国际位于中国香港，是国泰君安控股子公司，其员工可以访问上述母公司的全连接电子公文系统，并查看和浏览电子公文相关数据，包括公司员工通讯录信息、通知公告信息、公司发文信息、合同信息等。按照数据出境安全评估办法规定，虽然数据没有转移存储，但被境外机构、个人能够访问的也属于数据出境场景，同时上述电子公文系统涉及员工个人信息出境，且自公司成立以来，国泰君安累计处理自然人数据超一千万，符合《数据出境安全评估办法》第四条第二款情况，因此需要进行数据出境安全评估。

数据出境安全的全方位评估

数据出境工作需结合法律法规要求，证券期货业特点，明确不同阶段数据跨境合规管控要点，事前评估、事中监控、事后管理环环相扣，严格落实法律法规和监管要求。

事前评估

1.满足申报数据出境安全评估标准

数据出境前，证券期货业机构需对出境数据进行安全评估，厘清跨境整体情况，明确风险，促进数据跨境安全与流动。《数据出境安全评估办法》规定了跨境前评估的具体流程：(1)数据出境风险自评估(2)申报数据出境安全评估(3)网信办审核评估(4)重新评估和终止出境。金融机构需先开展数据出境风险自评估(可参考数据出境风险自评估报告模板)，详细说明出境活动整体情况，重点评估事项包括(1)数据出境的目的、范围、方式等的合法性、正当性、必要性；(2)数据的规模、范围、种类、敏感程度与风险；(3)接收方的责任义务以及保障数据安全的能力(4)数据被非法使用等的风险以及个人信息维权渠道的畅通度；(5)法律文件是否充分约定责任义务(6)其他影响事项。在自评估完成后，根据《数据出境安全评估办法》第四条，向境外输送重要数据或符合标准的机构提供个人信息时，需通过所在地省级网信部门向国家网信部门申报数据出境安全评估。最后由省级网信办查验材料完备性，国家网信部门进行审查，并出具评估结果。

2.未满足申报数据出境安全评估标准

对于未达到上述申报数据出境安全评估标准的情况，目前尚未给出明确的监管报备要求。涉及个人信息或敏感个人数据的情形，应先取得当事人同意书，做好留痕工作，先对数据进行形式审查，转移中或之后再实施实质性的审查。分类

分级等级与自评风险较高的数据，可根据数据安全需要，预先向行业监管机构报备，由相关单位审查后，再进行跨境传输工作。

事中监控

数据出境过程中，企业应对数据出境情况进行常态化持续风险监控：监督责任与义务的履行，保障数据传输的安全，管控数据权限，审查数据行为记录。

1.保障数据传输的安全

数据传输应采取国家标准规定的脱敏加密技术及遵守安全传输协议，并采取监控措施，保障数据传输的安全。在传输过程中，可通过部署监控设备和定期检查等手段，对数据传输过程进行监控，最大限度防范数据传输安全风险。

2.管控数据权限

数据接收者应对数据处理系统进行安全加固，严加把控数据权限，最小化数据访问范围。访问权限的审批应依据出境目的与约定用途，对权限所有者的允许访问范围应遵循最小化原则，仅允许访问与业务相关数据，防范数据泄漏风险。

3.审查数据行为记录

企业应保留数据发送日志以及出境中的数据行为日志，审查数据行为记录，防范数据窃取、篡改等风险。日志内容应记录所有访问敏感数据与重要数据的行为，包括但不限于账号、IP、时间、操作等，保证事故发生后可精确溯源。对日志应定期开展安全审计工作，对涉及敏感数据与重要数据的业务重点监测，鉴别行为是否异常。同时采取安全防护措施，防止日志记录被篡改。

事后管理

数据出境后的管理不可忽视，应遵循《评估办法》，落实目的完成后数据的销毁、超出目的范围数据的再评估、跨境数据的年度评价报告、违规行为的追责，完善事后管理流程。

数据安全能力的评估分类

数据安全能力评估是指对金融机构的数据安全能力进行评估和提升的过程。根据评估的对象和内容，数据安全能力评估分为以下几类：

1.技术能力评估

主要评估金融机构在数据安全技术方面的能力，包括数据加密、数据备份与恢复、网络安全、应用安全等方面的能力。

2.管理能力评估

主要评估金融机构在数据安全管理方面的能力，包括安全策略与规划、安全组织与管理、安全培训与教育等方面的能力。

3.应急响应能力评估

主要评估金融机构在数据安全事故应急响应方面的能力，包括预案编制与演练、紧急处置、事故调查与分析等方面的能力。

4.法律合规能力评估

主要评估金融机构在数据安全法律合规方面的能力，包括对相关法律法规的了解与遵守、隐私保护与合规、信息披露与报告等方面的能力。

5.外部威胁应对能力评估

主要评估金融机构在应对外部威胁方面的能力，包括网络攻击、网络钓鱼、勒索软件等方面的应对能力。

6.内部威胁应对能力评估

主要评估金融机构在应对内部威胁方面的能力，包括员工误操作、员工行为不端、内部恶意软件等方面的应对能力。

风险自评估报告

数据出境风险评估工作需要生成风险自评估报告，评估公司在数据出境过程中是否符合相关法律法规和监管要求。自评估报告主要包括自评估工作简述、出境活动整体情况、拟出境活动的风险自评估情况、出境活动风险自评估结论等四大部分。报告将详细记录自评估起止时间、自评估组织情况、实施过程和实施方式、自评估目的、自评估数据量和符合办法说明等内容。报告还将记录数据处理者基本情况、数据出境涉及业务和信息系统情况、拟出境数据情况、数据处理者数据安全保障能力情况、境外接收方情况、法律文件约定数据安全保护责任义务情况、数据处理者认为需要说明的其他情况等内容。报告将分析公司的合规性状况，包括数据分类和标识、访问控制、数据保护和监控等方面。风险自评估报告将帮助公司了解自身的合规性水平，并提供改进建议和建议的合规措施，以确保数据出境的合规性和法律遵循。

数据出境风险自评估工作还需要生成差异性分析报告，详细列出评估过程中发现的潜在安全风险和漏洞。报告将包括风险描述、影响程度、可能的威胁和建议的风险控制措施等。报告将帮助公司识别和理解数据出境中的安全风险，并提供针对性的建议和措施，以减轻或消除风险。

结果与报告将包括详细的分析和评估结果，以及针对性的建议和控制措施。我们将确保报告的准确性、完整性和可理解性，以便金融机构能够清晰了解数据出境安全评估的结果和建议。

数据安全保障能力要点

在申请出境安全评估时，根据网信办发布的《数据出境风险自评估报告（模板）》，要提交企业数据出境风险自评估报告，其中对企业数据安全保障能力进行了详细的列举（《数据出境安全评估申报指南（第一版）》附件四）：

（1）数据安全管理能力，包括管理组织体系和制度建设情况，全流程管理、分类分级、应急处置、风险评估、个人信息权益保护等制度及落实情况；

（2）数据安全技术能力，包括数据收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等；

（3）数据安全保障措施有效性证明，例如开展的数据安全风险评估、数据安全能力认证、数据安全检查测评、数据安全合规审计、网络安全等级保护测评等情况。

在评估过程中，国泰君安从数据的全生命周期出发，制定公司内部数据安全管理制度，健全完善数据分类分级、重要数据保护、风险评估、应急管理等重点管理机制。在标准规范方面，建立完善工信领域数据安全标准体系。具体执行的内容如下：

数据收集的过程中采用多种数据收集方法，包括主动收集和被动收集。主动收集包括调研问卷、面谈和会议记录等，被动收集包括日志记录、系统监控和数据备份等。

确保数据收集的合法性和合规性，遵循相关法律法规，以及保护客户隐私和数据安全的原则。国泰君安对收集到的数据进行分类和整理，以便进行进一步的分析和评估。根据数据的性质和敏感程度，采用安全等级标识进行分类，并确保每一类数据得到妥善处理和保护。并且国泰君安运用先进的数据分析工具和技术，如数据挖掘、机器学习和人工智能等，对收集到的数据进行深入分析和挖掘。这些工具和技术可以帮助发现潜在的数据安全风险、异常行为和潜在威胁，从而及时采取相应的安全措施和预防措施。通过对数据进行风险评估，识别和评估可能存在的数据安全风险和漏洞，包括数据泄露、篡改、非授权访问等。

基于风险评估的结果，国泰君安制定相应的风险控制措施，包括加强数据加密、访问权限管理、网络安全防护等，以最大程度地保障数据的安全性和可靠性。在数据收集和分析的过程中，国泰君安严格遵守数据隐私保护的原则和相关法律法规。确保客户的个人信息和敏感数据得到妥善保护，不被滥用和泄露。国泰君安采取措施对数据进行脱敏处理、匿名化处理等，以最大程度地降低数据泄露和隐私风险。

通过有效的数据收集与分析，国泰君安证券股份有限公司能够全面了解数据出境的风险和威胁，及时采取措施加强数据安全防护，保障数据的安全出境和传输。

成果与展望

国泰君安在数据出境安全评估实践的主要成果和影响

作为中国领先的金融机构之一，国泰君安高度重视数据出境安全。在保障数据安全和满足客户需求之间找到平衡，已经成为国泰君安迈向全球化的重要一步。

国泰君安在数据出境安全评估的实践中取得了显著的成果。国泰君安在数据出境安全方面高度重视，采取了多项措施加强数据安全保护，以最大程度降低潜在风险带来的影响。针对不可预见的情况，国泰君安制定了科学完备的应急预案，确保在紧急情况下能够迅速响应，做出妥善处理，从而保障数据的安全性和稳定性。

同时，国泰君安建立了一套完善的数据出境安全评估机制，包括数据分类、风险评估、数据加密和脱敏处理、以及后续的数据使用和存储管理。在此基础上，国泰君安出境活动符合法律法规和政策文件规定，采取了一系列安全措施以减轻风险的发生和影响，并制定了应急预案以及与境外接收方达成协议明确其应承担的责任和义务。国泰君安还考虑了可能出现的数据滥用风险和其他可能影响数据出境安全的因素，并采取了相应的措施应对。

2023年8月，国泰君安证券收到国家网信办正式通知，国泰君安申报的数据安全评估事项获批通过。国泰君安成为全国首批通过该评估的证券公司之一，也是上海地区率先通过该评估的金融机构。这对提升国泰君安乃至金融行业数据出境安全治理水平具有重要意义。国泰君安在数据出境安全实践的经验也被广泛推广于其他行业机构，对整个行业的数据安全管理产生了积极的影响。

未来数据出境安全工作建议

随着金融科技的发展，我们认为未来数据出境安全工作应有以下几方面的发展趋势和建议：

首先，需要加强技术研究和创新。积极探索技术手段，实现数据隐私保护和数据应用之间的平衡，应用区块链、隐私计算、人工智能等数字前沿技术，充分发挥新型数字技术在数据跨境流通全生命周期中的作用，在数据存储、传输等过程中采用良好的技术治理。例如，区块链技术可以确保数据的完整性和不可篡改性，隐私计算可以保护数据的隐私安全，实现“数据可用不出境”，人工智能可以进行风险预警和实时监控，这些都是未来需要进一步研究和应用的方向。

其次，建议加强监管科技的应用。通过利用大数据、云计算、人工智能等技术，实现对数据出境的实时监控和管理，提高数据跨境流动的透明度和可信度，提升监管效率和效果。

最后，建议构建更完善的数据出境安全管理制度。明确数据出境的标准和程序，强化数据的责任主体，保障数据出境的合规性和安全性。

未来数据出境安全工作展望

随着金融行业数据出境的趋势日益明显，我们相信通过加强技术研究和创新，以及应用监管科技，我们可以更好地管理和利用全球化的数据资源，实现金融服务的全球化和普惠化，为金融机构带来更多的业务机会和增长动力。

然而，与此同时，我们也需要对数据安全和隐私保护持续保持高度警惕，积极应对全球数据治理的新挑战。特别是在跨境数据流动日益频繁的背景下，如何确保数据出境的安全性和合规性，将会是我们面临的重要课题。对此，我们需要加强与全球的合作和交流，积极学习和借鉴国际上的成功经验和做法，不断提升数据安全管理和技术保障能力。

此次，国泰君安证券率先通过数据出境安全评估，证明了国泰君安证券对数据安全的高度重视以及对数据安全保护的专业技术能力。在未来，国泰君安将继续深入研究和探索数据出境安全评估的新模式和新技术，完善数据出境治理机制，提升数据出境保护能力，努力实现在满足全球业务需求的同时，保障数据安全和客户隐私的目标。我们相信，通过不断的技术创新和制度优化，可以更好地管理和利用全球数据资源，为金融行业的发展提供强大的支持和保障，同时也为全球客户提供更高效、更安全、更合规的金融服务。

基于安全能力有效性验证提升安全运营能力

文丨罗黎明、邓廷勋、乔喜慧

中国银河证券股份有限公司

摘　要： 本文重点阐述了安全能力有效性验证平台在银河证券的部署，以及在互联网边界、内网纵深防御等实际场景中的应用，相关验证结果表明安全能力有效性验证平台能够通过模拟各类攻击手法、工具等方式对企业安全防护体系进行安全验证，帮助企业从攻防对抗视角进一步提升安全保障和运营能力。

关键字： 安全防护、安全验证、安全运营、有效性

引言

国家和行业网络安全相关法律法规、行政规章的陆续施行，以及证券期货业数字化转型工作的持续深入开展，极大地推动了行业网络安全防护体系的发展与演进。同时，国内外严峻的网络安全形势，层出不穷的各类新型攻击方法、各类复杂攻击模式也对企业网络安全防护能力提出了更高的要求。

银河证券作为客户群体广泛、业务规模多样的重要证券经营机构，逐渐从侧重于设备运维与静态防护的传统安全模式，演变为以持续监测与动态防御为核心的主动安全与持续运营模式。在持续推进规范化、体系化安全能力建设的过程中，银河证券结合业界相关研究成果与先进实践，构建和部署了一套功能较为完备、场景比较丰富的安全能力有效性验证平台，实现了对各类安全防护措施的实时验证和持续监测，能够比较准确、动态和持续地评估公司安全整体防护能力，及时发现安全防护的薄弱环节并进行加固，提升了公司的安全防护能力和安全运营效率。

网络安全运营面临的挑战

证券行业作为关系国家金融稳定、支持实体经济发展、维护投资者合法权益的重要行业，极易成为各类网络攻击的主要目标。根据《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》以及《证券期货业网络和信息安全管理办法》等监管要求，银河证券近年来持续加强网络安全防护与运营能力建设。在开展相关工作的过程中，也遇到了一些困难和挑战，主要包括以下几个方面。

一是国内外勒索病毒、APT攻击、大规模数据泄露等网络安全攻击事件不断发生，新攻击发展演变快，安全形势不容乐观。防范各类新型攻击需要能够及时、快速地掌握和跟进各类攻击的威胁信息，并能够采取有效的方式对威胁信息及可采取的防护手段进行验证。

二是传统的被动式、静态化防御机制，缺少有效的脆弱性发现途径。传统安全防御多是基于部署各类安全设备和平台，所部署的安全机制和策略能否取得预期的防护效果也主要基于防御视角下的专家经验积累，缺少有效的验证、评估和反馈机制。

三是在大规模、跨区域、纵深防御的安全运营场景中，面对海量规模、分布广泛、架构异构的各类设备，如何通过工程化、自动化的方式对各类设备的防护措施进行验证，并根据验证结果对全局和细分安全策略等进行优化配置，达到协调一致的安全防护效果，是当前安全运营工作需要解决的重点难题。

基于上述背景，针对安全运营工作中存在的难点、痛点问题，银河证券充分参考和结合业界相关研究成果与先进实践，通过应用安全能力有效性验证技术，实现了对各类安全防护措施的有效验证和持续优化。

国内外研究现状

国外研究现状

2017年，Gartner在《面向威胁技术的成熟度曲线》(Hype Cycle for Threat-Facing Technologies)报告中首次提出了入侵与攻击模拟的概念，将其作为一类重要的新兴安全技术。Gartner在该报告中明确指出该框架“可供安全团队以一致的方式持续测试安全控制措施，贯穿从预防到检测（乃至响应）的整个过程”。

2021年，Gartner又在《2021年八大安全和风险管理趋势》(Top Security and Risk Trends for 2021)和《2021安全运营技术成熟度曲线》(Hype Cycle for Security Operations 2021)报告中，进一步强调了安全能力验证的必要性，Gartner预计安全能力验证将逐渐成为IT安全建设的重要技术手段，并在未来数年内被大量机构与企业广泛应用。

国外安全能力验证技术研究与应用发展较为迅速，一些新型专业安全公司以入侵与攻击模拟领域为核心业务领域，设计和实现了一系列方式多样、场景丰富的安全能力验证技术和产品，通过构造攻击场景的方式对已部署的安全措施进行验证。

国内研究现状

近年来，国家和证券行业对网络安全工作高度重视，监管部门对于网络安全防护有效性的要求不断提高。《信息安全技术 网络安全等级保护基本要求》(GB/T 22239—2019)、《证券期货业网络安全等级保护基本要求》(JR/T 0060—2021)、《信息安全技术 关键信息基础设施安全保护要求》(GB/T 39204—2022)等国家和行业标准中提出了对现有安全技术措施的有效性、安全配置与安全策略的一致性等内容定期进行全面安全检查的要求，针对关键信息基础设施还明确要求应采取模拟网络攻击方式，检测关键信息基础设施在面对实际网络攻击时的防护和响应能力。

在相关政策的持续驱动下，国内安全能力验证技术近年来发展迅速，技术研究和行业应用都存在较为广阔的研究和发展空间。目前国内的安全防护能力验证技术研究主要围绕几类重点场景，一是通过模拟实际攻击对已部署的安全防护措施的检测和防护效果进行验证，二是对防护策略在不同网络结构和不同网络区域的部署实施情况进行验证，三是对安全防护设备的攻击感知能力进行反向验证，从而更加全面、及时、准确地感知和验证安全攻击感知和防护水平。同时，安全能力验证平台化与自动化技术的应用研究也比较活跃，通过自动化部署攻击脚本，结合大量的专家经验与人工配置，能够更大规模、更大范围地实现快速、高效、准确、自动化的安全能力验证。

安全能力有效性验证应用实践与成效

银河证券基于自身安全运营需求，对国内外安全能力有效性验证前沿技术与先进实践，进行了全面系统的调研，并结合公司内部安全运营场景，部署实施了安全能力有效性验证平台，围绕互联网边界、内网纵深防御等重要场景，开展了多轮次的安全能力有效性测试与验证，基于验证结果对安全防护体系进行了持续优化，推动了公司安全防护体系与安全运营能力的不断提升。

总体框架

安全能力有效性验证平台采用分层设计，依次分为采集层、验证层和展示层，其中采集层的主要功能是各类安全日志信息的采集和初步解析处理；验证层是能力验证平台的核心模块，主要实现了验证场景管理、验证策略统一配置、验证任务调度和闭环管理以及资产信息管理等关键功能；展示层主要用于测试与验证结果的统计分析、集中呈现与可视化，帮助安全运营人员更加直观、准确地了解和衡量安全防护体系的有效性。

图1 平台总体框架

· 采集层：通过对接不同设备/平台的告警日志进行全自动解析，用于验证过程的自动化闭环分析。基于先进的攻击标识定位技术实现在海量日志中快速匹配所需要的日志信息，并进行自动化解析和验证结果判断输出。

· 验证层：通过分布在不同网络区域的有效性验证节点，对已部署的各类安全防护设备进行持续验证。实现对验证场景的自动化闭环执行，包括任务创建及调度、攻击模拟场景构造、执行过程判断、验证闭环等。

· 展示层：从防护措施分级、展示、验证结果获取、失效措施告警等维度，直观呈现有效性验证结果，并通过各类趋势

图表及统计分析数据等，准确地刻画当前安全防护能力态势。

部署实践

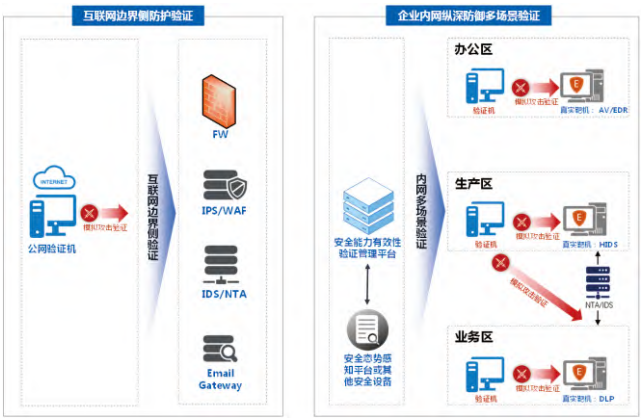


图2 内外部模拟攻击架构图

安全能力有效性验证管理平台统一部署在内网，验证机（执行攻击动作）和靶机（作为被攻击对象）根据验证方式和目标的不同，分别部署在不同网络区域中，且靶机上采取与业务环境等同的安全防护，但不部署真实业务与应用。通过验证机、靶机以及安全设备等的攻防交互，对安全防护规则和安全设备进行持续的无害化模拟攻击验证，形成自动化规则策略验证闭环。根据部署位置的不同，安全能力有效性验证的主要应用范围是互联网边界侧和内网纵深防御体系两大类验证场景：

· 互联网边界侧防护验证：通过内网的安全验证平台来管理部署在互联网上的验证机，对各类互联网暴露资产开展模拟攻击验证。通过OWASP Top通用漏洞防御检测场景（SQL注入、XSS、目录遍历等）、Apache Log4j远程代码执行漏洞及变种绕过检测场景、边界侧高危RCE漏洞利用防御检测场景等，对边界侧已部署的IDS、WAF等安全设备进行安全能力有效性验证。

· 企业内网纵深防御多场景验证：通过部署在内网的安全验证平台，构造不同的模拟攻击验证场景，对内网侧已部署的各类流量监测、主机安全、终端安全等纵深防御场景实施模拟攻击验证，基于流量侧和主机侧隧道转发和隐秘通信防御检测、内存马注入防御检测、反弹Shell防御检测、Webshell防御检测等场景，结合多种攻击手法和绕过方式，对内网已部署的安全防护措施进行持续验证和监测。

为准确匹配各类安全设备或系统的有效性验证结果，实现安全有效性平台的闭环验证，需要将有效性验证平台与安全态势感知平台或其他安全设备进行日志对接。实际部署过程中，采取为各类安全设备或系统添加特定标识的方式，并针对不同来源、不同格式的日志进行了统一解析和规范化处理。此外，在部署有效性验证平台的实际过程中，需提前针对有效性验证平台IP、端口等信息添加监测策略，避免因验证过程中的攻击行为而被安全设备误封禁，导致无法正常执行后续的验证操作。

互联网边界侧场景验证实践

互联网边界侧场景验证利用模拟攻击的方式在互联网侧对互联网边界资产的安全防护规则与策略进行验证。基于互联网暴露资产的URL或IP信息，定义模拟攻击验证指向，通过定制化攻击请求唯一标识技术、拦截返回代码、拦截返回页面、相似度匹配、日志快速匹配等不同方式，实现边界防护能力的快速闭环验证。

基于该场景下的验证，取得了比较良好的验证效果。例如通过OWASP Top通用漏洞防御检测场景（SQL注入、XSS、目录遍历等），对边界侧防护能力进行验证，整体防护能力较好，但发现域名X相比其他域名，对于某些特定SQL注入攻击载荷的攻击防护效果存在一定差距。基于本次验证结果，针对全量互联网侧域名的WAF防护策略进行了梳理，及时进行调整和优化，保证了互联网防护策略的一致性，有效提升了互联网边界侧的安全防护能力。

内网纵深防御场景验证实践

内网纵深防御场景验证利用模拟攻击的方式对内网安全防护规则与策略进行验证，包括流量侧安全验证、主机侧安全验证等场景。

1. 流量侧安全验证

内网纵深防御场景下的流量安全验证通过在内网已部署的验证机向靶机发起模拟攻击流量的方式，尝试构造不同类型的攻击，包括流量侧隧道转发和隐秘通信防御检测、SQL注入、WebLogic远程代码执行等攻击验证场景。对内网流量监测设备进行定制化攻击、变形绕过攻击等，检测安全能力防护的有效性，并与安全态势感知平台或其他安全设备日志进行直接对接，对验证结果进行自动化判断和输出。

实际验证工作中，通过配置定时任务、批量任务等方式，进行了多轮模拟攻击验证，发现某流量监测设备针对Webshell文件上传漏洞（Godzilla_vx.x.x_xx_xx.asp）告警率较低，经过对验证脚本的分析和情况复现，及时对流量监测设备针对该漏洞的检测规则进行了补充。

2. 主机侧安全验证

主机侧安全验证主要通过已部署的验证机向靶机发起真实的通信交互，模拟各类攻击行为，包括主机侧隧道转发和隐秘通信防御检测、内存马注入防御检测、反弹Shell防御检测、Webshell防御检测等场景。基于大量交互式攻击手法，对服务器主机进行模拟攻击，对主机HIDS、防病毒等主机侧安全防护设备和产品进行验证，判断其是否能够检测和阻断相关攻击，并对攻击行为进行告警。

通过对主机HIDS进行多轮次安全能力有效性验证，当前部署的HIDS产品对主机侧反弹Shell、Webshell、远控工具等的安全检测和防护能力良好，符合预期水平。针对验证发现的部分检测薄弱点，对HIDS的检测规则和防护策略进行差距分析和配置优化，提升了检测能力。

总结与思考

银河证券通过部署安全能力有效性验证平台，以攻击者视角对互联网边界、内网纵深防御等重要场景进行模拟攻击验证，帮助发现了一些运营过程中难以发现的薄弱点，在推动安全防护能力持续提升的同时，极大地提升了安全运营效率，降低了人工运营成本，取得了良好成效。

安全有效性验证平台在实际应用中仍存在一些待提升的环节，例如针对复杂攻击场景的验证模拟，多任务、大并发等特别场景下的任务调度效率还有待提高。在场景的覆盖度方面，当前传统网络安全防护的验证基本都已覆盖，但针对数据安全场景的有效性验证还有待进一步研究和落地实践。

后续，将结合安全运营实际需求，继续深入开展验证工作，围绕新型网络攻击、社会工程学攻击、数据安全等重点场景，对安全能力有效性验证平台进行持续优化，并加强与安全态势感知平台、威胁情报平台等的联动，助力安全运营能力的全面提升。

从实战攻防演练看中小券商安全建设

文｜焦翔、洪景城

甬兴证券有限公司

摘　要： 实战攻防演练从一开始的摸索阶段到现在遍地开花，极大的推动了国内多数企业的信息安全建设水平，大体量单位在不断提高安全建设水平的同时，中小体量企业也不应因资源问题而忽视安全建设，通过摸索、借鉴、合理的将资源最大化运用，安全建设提升一样能上出彩。

关键字： 资产、漏洞、外部安全、内部安全、开源

概述

随着国家政策及行业监管的推动，攻防实战演习已经成为一种常态化任务，大到国家，小到地市或券商内部，都在认真贯彻执行，通过持续的演练，“后门”、“漏洞”、“钓鱼”、“社工”等名词逐渐被大家所熟知，安全意识、防护能力都有了明显的提升，反应了实战化所带来的益处。对于中小券商，往往存在各种资源短缺问题，借助实战演练中发现的行业共性问题，并以此为安全建设切入点，合理分配资源去填补此类问题，从而实现较小的投入带来最大化收益。

中小券商安全建设面临的自身问题

对于中小券商，主要有以下两方面痛点。

资源缺失

人，目前多数中小券商安全人员还是以原有的运维、网络转岗担任或兼任，还处在安全团队建设最初级阶段，无法实际满足安全建设的需求，缺少能够以攻击者视角审视安全工作的专业人员。

资金，多数中小券商受限于业务发展及考核要求，安全建设往往以满足监管红线为主，在长期建设投入上，缺乏长线的资金支持，而安全建设往往不是一蹴而就，需要长期持续的投入。

推动落地难

企业发展往往以业务发展为导向，信息科技部门作为技术服务角色，以满足业务部门需求为主要目标，安全措施的落地，需要多个环节人员的配合，例如网络、主机、系统运维等，会带来业务效率的降低或业务系统上线延迟，同时由于大多数员工安全意识薄弱，存在不理解、不配合等情况，因此，日常安全工作推进过程中，会受到较大的阻力，如漏洞修复、安全加固类的工作，推进困难，下发的整改计划容易石沉大海。

中小券商实战攻防演练暴露出的共性问题

攻防演练作为一种模拟攻击和防御的实践活动，下面根据以往参与演练的经验，总结以下中小券商在实战攻防演练中的共性问题：

不知己-资产不清、信息不明

每次演练总结复盘阶段，总会发现部分失陷的资产是未知资产或停用未下线、已过维保期的资产，说明缺少对自身资产的梳理，没有完善的资产上线、下线全生命周期的管理流程。

不知彼-重边界、轻内部

多数企业存在错误观念，将边界防护作为首要目标，而轻视内部建设。但在实际攻击场景中，并不局限于针对互联网应用系统的攻击，随着社工攻击的盛行，再好的WAF也难以抵挡“简历.exe”的攻击。千里之堤溃于蚁穴，一封简单的钓鱼邮件、一个带宏病毒的文档亦或者携带恶意脚本的自解压压缩包，就能让攻击者打开城墙大门。

安全意识不足、弱口令永存

由于安全意识的缺失，内部弱口令/通用口令永远不会缺席，更无法防范社工攻击行为，在攻防演练中，除了通过字典破解、查看存放在桌面的密码本、抓取内存明文密码或密码hash、浏览器存储的各种凭证，还会通过发送大量钓鱼邮件、

软件等方式进行突破，特别是针对分支机构业务人员，假装客户发送带有木马程序的文件，几乎屡试不爽。

补丁欠缺

系统补丁缺失，是多数企业的共性问题，从系统分发开始，由于系统镜像没有及时更新，原有的镜像存在未修复补丁，后续的使用中也未对系统补丁进行修复，导致系统中存在各种常见的漏洞，如Linux的“脏牛”提权漏洞、Windows的Print Spooler代码执行等。

安全设备管理缺失

目前中小券商的安全建设中，已经按照监管要求完成了各种安全设备的上线，但因缺少专业人员或安全能力不足，缺少对安全设备的精细化管理，如未禁用非必要网络流量、策略设置为any、无法进行告警日志分析等，导致为黑客建立隐蔽的通信隧道、数据窃取等行为提供了便利。

中小券商初期信息安全建设建议

基于中小券商目前面临的自身问题，及实战攻防演练过程中发现的共性问题，建议中小券商在安全建设初期，将有限的资源集中去预防共性问题，只要彻底解决了此类问题，就能预防绝大多数黑客的攻击，自身的安全建设水平也将有很大提升。

资源梳理

1. 人员梳理

主要确定目前负责开展安全工作的人员，是否具备安全技能。

2. 产品梳理

梳理已有的安全资产，WAF、防火墙、IPS、IDS、防篡改、防病毒等。

3. 制度梳理

内部对资产上下线是否有严格的流程约束，上下线流程是否有足够严格、严谨的审批流程，是否存在绕过安全人员的情况。

4. 应用梳理

制定完善的表格字段，统计目前内外网存在的操作系统、数据库、Web应用的详细信息。关键字段，如下：

操作系统：系统版本、内核版本、IP地址、网络区域、责任人等。

数据库：数据库版本、IP地址、网络区域、责任人等。

Web应用：应用名称、内外网地址、端口、开发语言、中间件版本、第三方组件版本、后台开放情况、网络区域、责任人等。

5. 资金投入

从往年的投入中梳理目前每年投入的预期经费。

人员投入及管理

1. 专业人员投入

招聘至少一名具备安全技能的安全人员，很多工作的开展如果缺乏专业的人员，就需要采购外部服务来弥补，而这也将加大每年的预算，且实施效果难以保证。而有一名自己的安全人员，很多工作可以自行解决，这对于中小券商的安全投入上是非常划算的。

2. 安全意识提升

人员意识是安全建设中最大的薄弱点，人性是最大的安全漏洞，平时企业还涉及人员的流动，因此需要每年对全员进行安全意识普及。

边界安全

互联网边界，是安全防护仅次于安全意识的一环，防住边界，可以为内部的安全建设提供更多的缓冲时间。

1. 边界暴露资产管理

提升外部安全，最重要的一步为互联网暴露面梳理，APP、小程序、公众号、PC客户端、网站所有涉及的域名、IP、端口、应用系统。当这些信息能够按照特定的字段进行详细梳理后，就能对自己的互联网暴露面有充分的了解，当有新的漏洞暴露时，可以第一时间知道哪些系统受影响，及时联系负责人进行修复。同时，随着业务的扩展，该资产清单也需要不断更新。除此外，代码仓库、网盘、暗网等的信息泄漏问题也需要关注。解决这方面痛点，除了商业的安全服务外，部分还可以借助开源工具，辅助我们的工作。例如以下两个：

(1) 水泽：https://github.com/0x727/ShuiZe_0x727

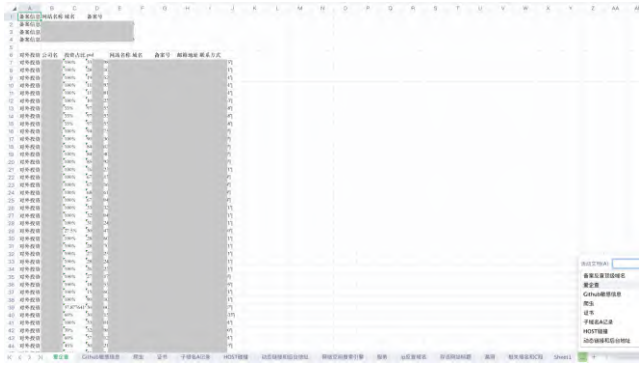


图1 水泽资产探测结果示意图

(2) 资产灯塔：https://github.com/TophantTechnology/ARL

图2 资产界面示意图

2. 安全设备管理

边界最主要产品为WAF、主机防护，需要有专人进行运营，例如每日巡检，发现异常告警及时分析，一方面防止防护策略配置错误，导致正常业务流量被阻拦，另一方面发现异常攻击行为，及时进行应急处置。

3. 漏洞发现

除了中证技术公司每月的漏洞扫描外，还应不定期/定期对互联网暴露的资产进行漏洞挖掘，覆盖漏洞扫描无法涉及的范围，例如逻辑类漏洞等。可以采取安全人员自测的形式，例如模拟实战攻击的形式，发现可能被利用的攻击路径。条件允许时，可考虑采购第三方代码审计服务，对重要信息系统代码安全性进行白盒审计。除了前面的主动型漏洞挖掘，还可以通过流量层面进行漏洞、风险发现，例如通过威胁狩猎服务发现当前网络环境下可能存在对异常流量，及早发现可能存在的被长期控制的主机以及被利用的漏洞。

内部安全

内部资产的梳理会略区别于互联网暴露面的梳理，因为还需要涉及员工PC、打印机等，尤其需要特别关注跨多网段设备，如跨多网段公共设备，打印机等设备漏洞容易被忽视，但往往就可以被作为跨网断跳板。以上这些往往需要桌面管理员提供相关的资产清单，同时借助网络准入平台进行统计。除此外，还有多个方面的建设方向可以做提升，又可以避免经费不足的问题。

1. 安全基线

根据等保要求，编写自动化脚本，对所有计划上线的机器进行安全加固，根据不同机器的业务场景，有些不适用的项目需要进行相应调整。初始口令可以相同密码，但是策略中应配置首次登录时强制要求修改密码。

2. 网络策略管理

在原有基础上，加强对icmp、dns流量的限制，对于有通过ping进行存活监测需求的，建议进行点对点的开放。对于测试环境应与生产、核心做好强隔离。

3. 补丁服务器

内部配置WSUS补丁服务器，自动拉取新的补丁。通过内部漏洞扫描来确定主机存在的漏洞，选择性从补丁服务器拉取补丁进行修复。

4. 下载源

由于近几年，开始出现通过上游投毒的方式，投放病毒，可搭建内部的下载源，例如yum源、软件仓库等。

5. 安全产品

主机防护、防病毒不能少，属于最基本的安全保障，但是这类产品告警量会很大，除了真正的安全告警外，还可能包含误报，例如有些业务程序需要对系统API的调用、敏感程序的调用，很容易造成安全设备告警和拦截，因此这类设备的运营，非常需要专业人员的分析。在资源有限的情况下，适当地在内部部署开源安全产品，也能对安全能力的提升有一定作用，例如开源蜜罐：

HFish(https://hfish.io/)

“Hfish是一款社区型免费蜜罐，侧重企业安全场景，从内网失陷检测、外网威胁感知、威胁情报生产三个场景出发，为用户提供可独立操作且实用的功能，通过安全、敏捷、可靠的中低交互蜜罐增加用户在失陷感知和威胁情报领域的能力。

HFish具有超过40种蜜罐环境、提供免费的云蜜网、可高度自定义的蜜饵能力、一键部署、跨平台多架构、国产操作系统和CPU支持、极低的性能要求、邮件/syslog/webhook/企业微信/钉钉/飞书告警等多项特性，帮助用户降低运维成本，提升运营效率。”

图3 安全态势图

内部漏洞扫描，除了采用外部购买的产品/服务，定期采用开源工具进行辅助也是不错的选择，例如：

Fscan (https://github.com/shadow1ng/fscan)

“一款内网综合扫描工具，方便一键自动化、全方位漏扫扫描。支持主机存活探测、端口扫描、常见服务的爆破、ms17010、redis批量写公钥、计划任务反弹shell、读取win网卡信息、web指纹识别、web漏洞扫描、netbios探测、域控识别等功能。”

通过探测可以将真实场景下，黑客关注的漏洞进行发掘，结合后期的漏洞修复，提高攻击者在内网环境下的攻击难度和时间成本，降低风险被发现的概率。

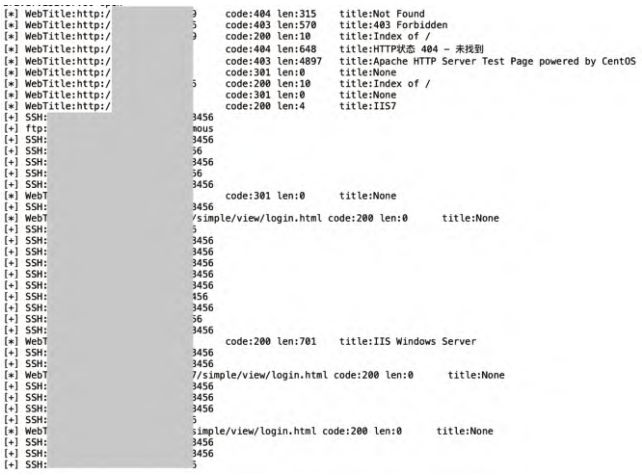


图4 Goby扫描过程示意图

Goby(https://gobies.org/)

“新一代网络安全技术，通过为目标建立完整的资产数据库，实现快速的安全应急。Goby只针对受影响的小范围进行漏洞应急，所以这种方式速度最快，对目标网络影响最小。”

相比于命令行工具，Goby可以分布式部署，即通过在不同网络环境部署节点，通过一个控制端来控制，可以实现例如在办公网就可以控制测试网对节点对测试网进行扫描。同时生态较好，有多种插件、可自定义POC、密码本等内容来优化扫描效果。具体还需自行探索。

图5 Goby扫描面板图

中小券商后期信息安全建设建议

通过初期的建设，安全能力已经具备一定雏形，后续的安全建设可围绕几个方向开展包括但不限于以下方向。

资产生命周期管理

从信息资产全生命周期治理的角度出发，将安全与管理流程打通，完成资产动态全流程管理。

建立健全应急响应机制

通常需要有足够的安全人员，或具备处置能力的人员来协同。内部具有应急响应机制、处置预案、职责分工，并进行日常复盘。

SOAR运用

建设后期，设备多、资产多导致告警多，这就需要能够采用自动化技术来减轻人工的负担，例如与WAF联动，对明显的扫描、漏洞利用等恶意攻击自动化封禁。

API安全

API安全非单纯的接口是否存在漏洞，还包含API的调用审计、风控，这就需要内部先做好数据分级分类，为API安全提供审计依据。

远程办公安全

传统VPN技术存在多种问题，例如审计方式粗旷，产品本身漏洞频出，可采用新的解决方案，例如“零信任”解决方案，提高审计颗粒度，同时能优化用户体验。

邮件网关

提升用户安全意识，能够抵挡部分钓鱼攻击，但邮件网关也尤为重要。本地部署的邮件服务器，前面部署邮件网关，对邮件内容进行安全检测。

除了上面这些，还有很多可以在后期提高安全水平的工作可以开展，例如开展定期邮件钓鱼检测、近源渗透、红队评估等，这取决于后期规划及安全投入水平。

自我检验

建设到一定水平后，在瓶颈期，自身安全弱点隐藏较深，可通过攻防演练对安全防护体系进行检验，发现建设的薄弱环节、可被利用的攻击路径，及时查缺补漏。

东吴证券
内部身份账号中心与权限管理实践

文｜华仁杰、朱健兵、沈嗣贤、刘国文

东吴证券

摘　要： 数字时代，安全更需先行！近年来，证券行业数字化转型步伐不断加速，一方面证券企业要面对全新的技术、业务场景、经济形态；同时又要紧随国家密集出台的各种安全法律法规政策与要求；另一方面企业旧有安全建设遗留下的安全隐患问题陆续凸显。传统以“网络为边界”的安全防护难以满足当前安全需求，如何在原有的安全防护基础上构建以“身份为中心”的新安全防护体系，从而突破上述三大安全困境，是当前东吴证券亟需思考的问题。本文旨在介绍东吴证券在传统身份安全及单点登录的基础上，结合零信任架构理念、UEBA等技术，构建以“身份为中心”动态访问控制的企业安全新架构，形成一套以用户集中管理、系统高效访问、权限有序变更、访问持续安全、审计全程贯穿的全新身份管理体系。

关键字： 身份安全、动态访问、零信任、统一身份与权限管控

前言

证券企业作为维护资本市场高质量发展的“中坚力量”之一，对中国经济社会发展有着重要作用与意义。一方面，国家政策积极鼓励金融证券行业加速迈向数字化发展；另一方面，基于行业的特殊性与重要性，其数字化发展更需建立在网络安全基础之上。

近年来，国家密集出台了《数据安全法》《个人信息保护法》《网络安全审查办法》《关键信息基础设施安全保护条例》等法律法规。为了有效落实上述相关要求，规范证券行业网络和信息安全管理，防范化解行业网络和信息安全风险，维护资本市场安全平稳高效运行，中国证监会于2023年正式发布了218号令《证券期货业网络和信息安全管理办法》，并将于2023年5月1日起正式实施。

与此同时，5G 互联网、物联网、云、大数据等新兴技术的高速发展与变革式创新，证券业务与技术加速融合，对网络安全和信息化日益依赖，增加了网络和信息安全管理的复杂度。而企业数字化智能化转型的提速，信息系统建设任务明显增加。传统基于公司内外网边界的安全防护在当下的新技术、新业务场景、新经济形态中陷入困局。寻找新的安全边界，并建立新的安全防护体系是当前证券企业网络安全防护的当务之急。

图1 传统安全边界面临的挑战

除了以上法律法规与技术发展带来的网络安全困境之外。东吴证券公司内部也存在业务安全、管理、体验、审计等痛点，具体如下：

1）管理问题：业务系统、用户越来越多，权限越来越复杂，IT管理工作随着用户入转调离的生命周期越来越繁重；

2）体验问题：从用户实际工作体验出发，随时随地远程访问权限范围内系统成为当下工作的刚需。而随着公司应用系统的不断扩增，多应用、多界面、多终端、多账号密码重复登录，严重影响工作效率及用户体验；

3）安全问题：账号管理工作的繁重导致僵尸账号风险难以规避。用户和系统的增加亦促使身份盗用、非授权访问、弱口令、权限滥用等风险上升。同时，在自主可控政策层面，也对金融自主可控适配工作提出了标准化要求；

4）审计问题：业务系统建设增加，没有统一可复用的用户管理系统，导致资源重复投入。而零散的用户管理给过程审计带来更大难度，难以做到实时有效的事前预警、事中审计

及事后责任追溯到人。

基于此，经过行业调研及技术测试，东吴证券与上海派拉软件联合开发，在传统身份安全及单点登录的基础上，结合零信任架构理念、UEBA等技术，以身份与访问控制管理新5A（认证Authentication、授权Authorization、管理Administration、审计Audit、分析Analytics）为核心，开展东吴证券内部数字身份账户中心与权限管理的实践，构建以“身份为中心”动态访问控制的企业安全架构，形成一套以用户集中管理、系统高效访问、权限有序变更、访问持续安全、审计全程贯穿的身份管理体系。

东吴证券内部用户数字身份中心与权限管理实践

基于可信身份动态管理构建新网络安全基石

身份作为网络安全的基石，如果没有身份安全，其他网络安全便都成了“空中楼阁”。尤其是在传统安全边界失效，以“身份为中心”的动态访问控制正在逐渐成为企业安全防护架构的主流。因此，东吴证券的数字身份中心一方面作为等保2.0网络安全防护技术架构中基础安全设施的重要组成部分，另一方面也是公司数字化转型中数字身份信息化管理的重要支撑。

整个数字身份中心以灵活、易用、安全、可持续为建设目标，以内部“身份账号”为建设基础。通过将集团内组织、人员、应用、数据等信息充分连接，形成集团级数字身份共享生态体系，打通应用账号的集中统一管理、系统的高效访问、应用单点登录、权限统一管控以及一体化全流程审计，真正基于可信身份构建安全动态访问控制管理，最终实现提高管理效率、加强信息安全、降低企业发展成本、满足政策合规等目标。

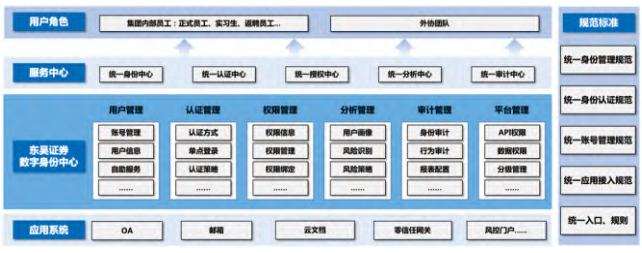


图2 东吴证券数字身份中心整体框架

1. 统一身份管理构建数字身份中心根基

数字身份中心建设的第一步，也是整个建设的根基，即完成公司现有用户数据的统一收集、清洗、聚合，消除重复账号、孤立账号等，从而构建统一的用户账号与管理中心。过程中，由于东吴证券内部存在一个用户的多个不同数据来源，为保障数字身份的权威可信与后续的有效管理，完成了数字身份权威主数据的确立。

整个数字身份中心建设过程中打破了现有的信息孤岛，融合各大业务系统，实现统一用户身份管理、应用单点登录、访问权限全生命周期控制以及一体化全流程的合规审计等。从而简化用户登录过程，提高办公效率；减轻管理员账号管理工作，减少人工误操作风险；提高企业信息安全水平，有效适应企业数字化发展与用户实际需求。

图3 数字身份基础建设框架

2. 管理策略实现自动化应用账号运维

传统的系统账号管理模式一般基于用户申请，比如员工入职时，系统管理员根据入职申请流程，在系统后台进行账号的手工创建；离职时，则根据离职流程进行账号的手工关闭。这种模式存在审批记录可能与系统中实际开通或关闭的情况不符，需依赖后续的审计与检查发现问题。

为此，东吴证券数字身份中心采取数字身份全生命周期一体化管理思路，先从上游权威数据源与用户的入转调离等人事变动触发流程，并与组织架构信息对接，将用户身份相关的组织、岗位、个人信息等数据统一汇聚到数字身份中心，进行集中管理。其次根据应用账号管理模式设置自动化供应策略，比如风控岗位的员工入职默认需有风控系统账号，系统会在用户入职流程完成后，自动开通对应岗位所需应用系统账号。同理，在离职时根据流程触发禁用账号的策略，从而形成基于管理策略的自动化应用账号全生命周期管理，保障账号管理安全合规的同时，加快业务响应速度。

图4 用户全生命周期身份自动化管理举例

3. 人工智能实现身份风险识别与控制

东吴证券数字身份中心一方面考虑到传统身份管理中统一认证、单点登录等基础应用场景，另一方面也兼顾了零信任架构中增强型身份管理对身份风险分析的要求。

风险分析能力的实现主要基于UEBA及人工智能技术。根据Gartner 对 UEBA 的定义，即提供画像并基于各种分析方法的异常检测，用打包分析来评估用户和其他实体（主机、应用程序、网络、数据库等），发现与用户或实体标准画像或行为相异常的活动所相关的潜在事件。

在数字身份中心实际应用场景中，UEBA主要用于检测用户在登录过程中的真实身份，防止用户账号被盗、身份冒领等黑客攻击及社会工程攻击。例如，当一个用户不小心点击了钓鱼邮件，泄漏了账号密码。攻击者拿到账号密码去访问系统时，处在异地登录或使用非常用设备登录时，就会自动触发升级认证，系统再次验证用户的手机验证码或动态口令才会放行，通过设置升级认证的动作将攻击者拒之门外。

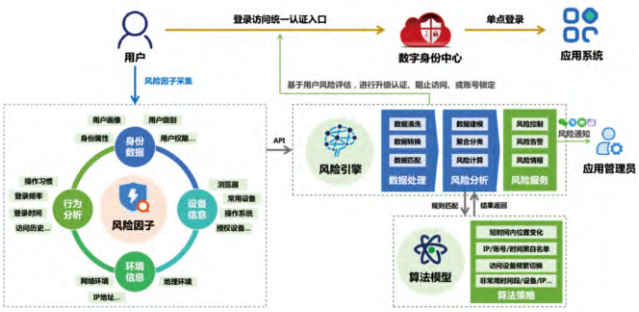


图5 UEBA风险识别及管控机制

而人工智能技术则会基于用户经常访问的时间、访问时使用的认证方式、经常使用的设备等画像结合算法模型，进行风险评估和控制。例如，黑客盗取账号密码后尝试登录，但该用户一直使用扫码登录，将立即触发风险机制。这一机制保障了事中的访问安全。

4. 统一标准规范保障可持续集成运营

平台的长期运营是投资收益回报的关键，根据Gartner对20+家大型企业实施完身份与访问控制管理后的统计，一般千人规模的企业在三年内的总投资收益率（ROI）可以达到300%。为了保障数字身份中心长期可持续地运营发展，数字身份中心平台形成了统一的身份数据规范、管控流程规范、安全技术标准规范。为后续其他类型的用户集成、新增应用系统的集成提供标准统一的规范，从而提高集成运营效率、减少建设成本。

例如，在用户及组织数据同步时，所有对外提供的API接口，均采用用户级别鉴权，最低为系统级别鉴权，携带数字身份中心颁发的JWT Token或Access Token进行安全校验；在应用系统单点登录集成时采用统一的OAuth2.0协议，确保技术层面的安全性。

图6 数字身份集成标准规范

基于RBAC授权管理模型实现应用权限细粒度管理

数字身份中心下一步规划将基于RBAC授权管理模型实现各应用系统的权限统一与细粒度管理，从而改善权限管理的分散、开通周期长、效率低、审批流程多等问题，实现一个权限管理中心，集中可控地管理所有业务系统权限。在权限统一分配管理之外，权限中心还具备权限审计、权限自动化供应，以及权限自助等场景实践。

图7 权限管理中心架构

整个权限中心与下游应用的对接主要采用RBAC的权限模型，即通过定义角色的权限，并对用户授予某个角色从而来控制用户的权限，实现用户和权限的逻辑分离（区别于ACL模型），极大方便了权限的管理。

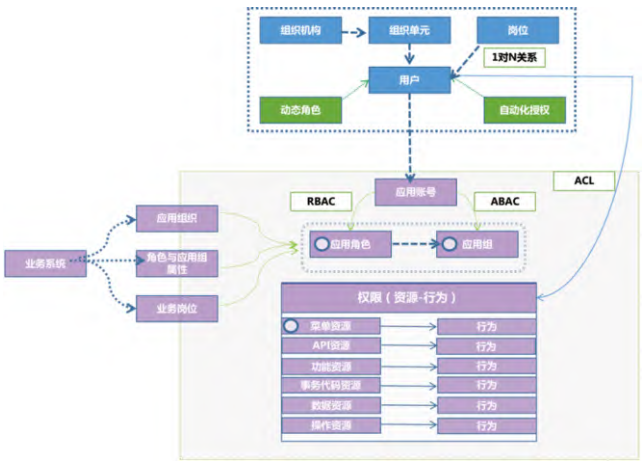


图8 业务系统一体化授权模型

数字身份中心在原有的身份同步基础上还将新增业务系统资源同步回收、业务系统角色同步、资源绑定、角色绑定等深度集成。在合规层面，考虑到部分角色存在权限互斥的场景，平台将进行互斥策略的定期检测及告警。在账号运维管理层面，数字身份中心在原有账号供应的基础上增加具体业务系统账号中权限的供应及回收。从而全面覆盖业务系统权限从开通到关闭的整个生命周期的细粒度管理。

全面适配的安全自主可控

金融类信息和数据涉及国家和居民安全，金融证券业在政策支持、自主驱动下，正在加速推进自主可控全栈式升级改造，包括从底层基础硬件、中间层基础软件到上层核心应用软件，以及在建设过程中发挥重要作用的网络安全、云平台、终端外设等环节。

作为东吴证券自主可控改造中间的重要一环，数字身份中心后续将在自主可控层面进行全方位适配，通过采用国产芯片、国产服务器操作系统、国产数据库等产品进行底层基础设施的全面切换，实现从基础设施至软件的全方位安全自主可控。

总结与展望

以“人”为中心的零信任安全架构逐渐成为主流

众所周知，网络安全最薄弱环节是“人”。网络攻防的本质就是人与人的对抗，人性的漏洞是网络空间治理的最大漏洞。正所谓“堡垒往往从内部瓦解”，传统的网络安全模型中处于内网可信的“人”成了威胁的来源。因此，没有绝对安全的网络，没有绝对的可信。

这正是零信任“从不信任、始终验证”的理念：不相信任何用户和角色，不论内网或外网，其信任的基础必须通过认证和授权得以建立，并对安全策略进行持续动态调整。零信任安全体系架构是一次由“网络中心化”向“身份中心化”转变，其本质是以“人”或“身份”为中心的动态访问控制。

身份是零信任的基石。作为零信任体系基础组件IAM（身份与访问控制管理），其重要性不言而喻。这也是本文中东吴证券内部身份账号中心与权限管理实践过程中，在构建新的安全防护边界时采取的基本思想。

未来，零信任中的IAM将更加敏捷、灵活且智能，不断适应各种新兴业务场景与新技术，并采取动态策略实现自主完善，不断调整以满足实际安全需求。而在数字化进程更深入的演进过程中，传统以“纵深防御+边界防御”为主的安全边界会进一步被打破，并彻底走向模糊化。基于“外网危险、内网安全”理念构建的安全防御体系将失效。以“人”为中心的零信任安全架构为代表的白环境分析手段将逐渐替代基于威胁特征“一刀切”的黑名单机制，成为主流。

混合架构下科技风险运营体系建设之轻量化“蓝军”探索

文｜郭孝军、饶滔、吴善鹏、蒋琼

中银国际证券股份有限公司

摘　要： 未知攻，焉知防，攻守相济的安全体系建设，是打造面向全科技流程的安全基座，是主动防御的关键所在。“蓝军”的内部建设需契合企业自身的需求，保障日益复杂的信息系统和逐渐增加的数字资产的安全。由于专职安全人员数量的限制，“蓝军”工作按照轻量化进行，具备“蓝军”任务的能力，并全面开展公司的“蓝军”相关任务，主要目标是尽可能多地主动发现企业安全风险，进而提高整体的安全防御能力。

关键字： 轻量化“蓝军” 网络安全、混合架构、科技风险运营

概述

近年来全球安全事故频发，国内外都极为重视网络安全。正如习总书记所强调：没有网络安全就没有国家安全。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，是把我国从网络大国建设为网络强国的关键。

未知攻焉知防，攻防无恒，安全无界。如今国内外都在如火如荼地开展国家网络安全实战演练，伴随实网演练的普及，企业安全攻防建设的重要性日益提升。对于安全建设，其最终目的还是用于面对真实的攻击、实网攻防演练，攻防对抗成为检验企业安全水位建设的重要指标之一。

为什么需要“蓝军”

根据Gartner的调查，97%的入侵行为发生在已经部署适当网络安全防护系统的公司，99%的攻击行为是使用已知并存在多年的攻击方式或者漏洞，95%的绕过安全防护设备的入侵攻击行为是因为错误的配置造成的。

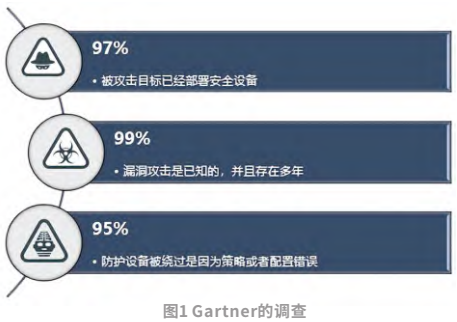


图1 Gartner的调查

由此可见，尽管企业部署了各类安全防护设备，但是如果没有持续升级或正确配置防护策略，这些安全防护设备依然无法发挥最大效果，无法有效防范安全入侵问题。因此，安全验证越来越被被业界所看重。普遍认可的安全运营架构中，按功能模块划分成四个模块：安全防护框架、安全运维框架、安全验证框架、安全度量框架。其中，安全验证框架主要功能是综合通过黑盒白盒验证措施，确保安全防护框架和安全运维框架的有效性。

图2 安全运营架构

安全验证框架解决安全有效性的问题，承担对安全防护和安全运维两个框架的功能验证。安全验证框架中企业安全的“蓝军”便是重要的组成部分，在和平时期，“蓝军”扮演着对手角色，利于及时发现、评估、修复、确认和改进安全防护和运维框架中的脆弱点。包括白盒检测（过程验证）和黑盒检测（结果验证）两部分。

“蓝军”建设，是传统安全建设工作的外延，“进攻是最好

的防守”，通过实战来强化组织的整体安全性，“蓝军”存在的价值可以体现为以下几点：

· 检验安全防护水平

随着企业所承载的业务高速发展，以及信息技术应用创新产业的发展，面对信息科技国产化，数字化转型，在银行业实行的全面风险管理体系中，已经把提升信息科技自主性、加快IT基础设施国产化替代进程，作为信息科技风险管理的一部分。网络安全威胁形势是不断动态变化的，混合架构下的科技风险运营，安全地基尚处于强度未知的状态。红蓝对抗可以检验企业安全防护体系：防护阻断、检测感知、响应溯源的能力，同时暴露防御脆弱点和业务风险盲点，从而针对性地优化和提升防护系统和消除业务风险，完成安全闭环。“蓝军”可以客观的用攻防实践来检验安全水平高低。

· 梳理风险盲点和攻防场景

像攻击者一样思考，不断积累并挖掘多样化的攻击面，对于每个攻击面梳理可能的攻击路径，将攻击路径根据杀伤链的各个环节，分离出关键场景。在暴露风险盲点的同时，“蓝军”团队一方面需要持续绘制出清晰的攻防场景地图，另一方面也可以为防御建设提供有价值的优先级和技术建议。

· 安全价值的体现

以攻促防，攻防相长。在攻防的过程中，可以考验出企业在安全防护能力以及安全事件的检测发现和应急能力。“蓝军”的攻击目标往往是企业的核心业务和数据，通过扮演了一个外部攻击者的角色，可以正面反映出安全投入的必要以及安全工作的价值。同时，只有持续暴露网络安全防护、监测和应急处置的缺陷并优化改进，才能更好地抵挡外部不断变换的攻击手法。

· 提升企业内部安全意识

对于企业而言，其自身真正发生安全事件可能相对低频，在业务层面极少有直接感知。若未发生事故，或者说面对网络攻击没有造成直接损失，很可能会给人带来安全防护足够完善、业务数据足够安全的错觉，甚至导致防护手段逐渐落后，安全流程越发陈旧，人员意识日益懈怠。一次攻防演练往往能让各方更加直观的感受到攻击现场，强化企业内部人员的安全意识。

需要什么样的“蓝军”

“蓝军”的概念，在军事领域早已有之。国内“蓝军”扮演假想敌（即敌方部队），与红军（我方正面部队）开展实战演习，帮助红军查缺补漏，提升作战能力。信息安全领域的红蓝对抗的概念也源自于此，通过开展攻击演习来全方位检验企业的安全稳健性和威胁监测及响应能力。与传统渗透测试相比，红蓝对抗中的“蓝军”演练更接近真实的攻击，一般包含在线业务、企业人员、合作方、供应商、办公环境、物理楼宇、数据中心等等多样化的攻击形式。红军作为企业防守方，通过安全加固、攻击监测、应急处置等手段来保障企业安全，而“蓝军”作为攻击方，以发现安全漏洞、获取业务权限或数据为目标，利用各种攻击手段，试图绕过红军层层防护，达成既定目标。

与互联网领域不同，证券行业是金融行业的重要组成，全世界针对金融的安全事件不断发生，安全变得极为重要。对于证券行业来说，更偏向于强合规、控风险，需要牢牢守住不发生系统性金融风险的底线，在此背景下，需要一支既了解公司业务，又能够以攻击视角持续渗透测试公司资产的内部攻击队伍，这样才会更容易了解到公司各项安全隐患，把风险消弭于萌芽之前。“蓝军”的建设既顺应了行业主管机构的要求，也是企业内部发展的需要。

轻量化“蓝军”建设的探索

“蓝军”的工作内容主要包括“渗透测试”和“红蓝对抗”，渗透测试尽量用较短的时间去挖掘尽可能多的安全漏洞，一般不太关注攻击行为是否被监测发现，即便被发现也不会立刻遭拦截，目的是帮助业务系统暴露和收敛更多风险。红蓝对抗更贴近真实攻击，侧重绕过防御体系，毫无声息达成获取业务权限或数据的目标，不求发现全部风险点，因为攻击动作越多被发现的概率越大，一旦被发现，红军就会把“蓝军”踢出战场，目的是检验在真实攻击中纵深防御能力、告警运营质量、应急处置能力，当然这过程中也会发现业务系统的一些安全漏洞。

混合架构下科技风险运营体系建设及安全管理中，需要“蓝军”来主动改善管理。攻防实战的本质是人与人之间的对抗，若辅以资源和环境的支持，将如虎添翼。一支有战斗力的自有“蓝军”团队并不是多大的奢望。但由于在安全管理上资源投入及专职安全人员数量的限制，所以对于“蓝军”的建设轻量化进行探索。

队伍建设

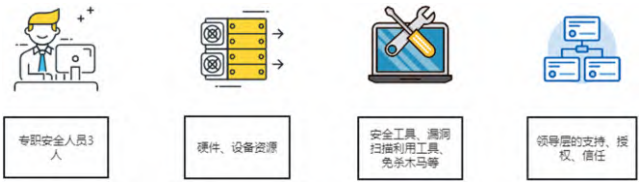


图3 轻量化“蓝军”队伍建设

人力：投入3名专职安全人员，分别做不同方向的安全研究、配合。

资源：性能足够，有管理员权限的工作电脑；一定的可支配资金，用于购买域名、vps、代理 ip 等蓝军测试辅助资源。

工具：包括安全工具、漏洞扫描器、漏洞利用工具、木马后

门等扫描工具、漏洞利用工具、木马程序、攻防知识库。

组织：对于组织而言，“蓝军”即“坏人”，进行相关的攻击行为需领导层的支持、授权和信任。

安全培训：借助集团的培训资源，深度参与各类“蓝军”技能培训：包括web安全、内网渗透、CTF竞赛、实战漏洞利用、钓鱼攻击等。

业务运营

队伍建设后，“蓝军”就可以发挥其锋锐的攻击特性了。在可控的前提下开展模拟攻击，首先通过多种手段获取立足点，在此基础上通过权限提升、信息发现和横向移动扩大控制权，最后达成数据收集、窃取和篡改破坏等目的。

图4 攻击业务开展

目标侦查：利用一系列侦查手段获取目标的资产、人员、环境等信息，为实施攻击提供基础信息支持，信息的全面性和准确性很大程度确定攻击的路径、战果和效率。比如通过DNS域传送漏洞、域名注册信息反查、域名枚举等手段获取域名资产信息，通过域名解析、网段扫描等手段获取IP资产信息，通过网站扫描、端口探测等手段获取程序指纹信息，通过在搜索引擎、网络空间搜索引擎、网盘、Github等平台检索以及社工欺骗等手段获取组织架构、员工信息、源代码、账户密码、常用软件、常上网站、安全防护策略、外包服务供应商等信息。

边界突破：根据收集到的目标信息，针对性制作攻击代码。如设计植入木马的文档,尝试对员工针对性钓鱼攻击；对于线上服务，可以通过自动化扫描、人工测试等手段对目标资产进行漏洞探测，发现可利用的漏洞。在目前公开的APT案例中，至少有80%是从攻击员工办公电脑入手，因为人是系统最大的漏洞，利用社会工程学的攻击成功率高，同时攻陷员工电脑后更容易摸清内部网络及扩大控制范围。

权限获取：利用各种手段将攻击载荷投递到目标，获取系统权限。比如利用命令注入、文件上传、SQL注入等漏洞直接远程攻击线上服务。利用邮件钓鱼、水坑攻击、网络劫持等方式入侵服务器、员工电脑、网络设备。利用系统弱点或配置不当等方式获取超级管理员级别权限，比如利用最新Windows/Linux内核提权漏洞，或者存在sudo权限的系统命令的情况下，“靠山吃山，靠水吃水”直接利用系统命令提权等。

横向移动：通过内网渗透攻击获取更多服务器权限和数据。一旦突破边界后进入内网，此时的攻击面就变成了内网，而内网应用数量远远大于互联网应用。从应用的安全要求和质量来看，由于安全开发、测试资源有限，公司内网应用的安全要求和质量远低于互联网应用。内网点多、面广、架构复杂、易攻难守。一般来说攻击者偏爱攻击拥有企业主机、网络、运维、数据相关管理权限的系统，比如说Windows域控、补丁服务器、邮箱系统、内部即时通讯工具、跳板机、运维运营平台、密码系统、代码管理平台等，一旦攻破这些系统就几乎能够控制全部机器，进而获取目标业务数据。

数据收集：搜集源代码、数据库、资产信息、技术方案、商业机密、邮件内容等攻击目标数据。对数据进行加密、压缩、分段处理，通过HTTP(S)/FTP/DNS/SMTP等网络协议主动对外传送、使用Web对外提供访问下载或业务API直接查询回显等方式将数据传输出网。

在攻击业务流程中，需要对攻击做好记录，比如攻击 IP、攻击行为，时间点等，方便攻击之后的复盘工作；攻击后要针对蓝军发现的安全问题落地有效的短期应对措施和长期解决方案，并持续跟进直到问题修复闭环。同时也需要考虑到风险管控，一旦“蓝军”人员真的从外网攻陷到内网，拿到了各种以前认为安全的机密数据或者有现金价值的数据，需要保证数据不外泄：所有数据只允许拿验证数据，不允许大量获取数据，保证“蓝军”不存储生产数据；操作可审计：采用瘦终端+堡垒机+云桌面，或者专用设备+录屏等方式，做到所有操作可审计，数据不落地到个人电脑。

运营过程中也需要“蓝军”有外部交流，为团队提供更高的外部视野、平台，给予团队不间断的成长机会。

总结

《孙子兵法 · 势篇》说道：“奇正之变，不可胜穷也。奇正相生，如循环之无端”。“蓝军”这支“奇”兵，不仅可以激励“正”军（“红军”）进行战略战术磨炼，提升其战斗技能，加强其预测真实战场情况、预判敌军战略战术的竞争能力，还可以与红军进行奇正转化，在需要的时候成为歼敌的主要力量。

基于“数据围栏”的终端安全建设思考

文｜孙一伟、崔毅然

上海证券有限责任公司

摘　要： 企业数据安全建设初期，权责划分、数据分类分级以及使用场景的梳理工作尚在起步中。作为此阶段中企业信息系统数据安全主要“责任人”的信息技术部门聚焦终端安全，通过层级防护模式、轻量化分类分级以及全链条的安全防护矩阵，降低企业内部信息系统的数据泄漏风险。

关键字： 数据围栏、数据分类、系统分级、全链条防护

前言

终端作为企业内部资源的使用端，具备访问和承载企业重要经营数据和用户个人信息的功能。随着办公场景多元化和远程办公常态化所导致的网络边界延伸，终端安全的定位已从最初的防病毒转变为抵御外部网络攻击的屏障，防范内部数据泄露的关卡。本文将结合笔者工作实践，探讨通过终端安全建设防范企业信息系统数据泄露的思路。

“To be, or not to be”

应用系统、网络边界，还是工作空间？

由设备、人员、场所和应用所构成的工作空间在实现企业员工多元化办公场景的同时，也成为终端安全建设中的保护对象。办公过程中，信息系统所承载的数据将流经应用系统、各级网络边界，最终到达用户的工作空间。下表为工作空间各元素的分类示例：

工作空间构成	类 别
设备	物理 PC、笔记本电脑、移动终端
人员	企业员工、客户经理、第三方人员
场所	固定场所（办公场所）、非固定场所
应用	B/S、C/S、APP、云桌面（含虚拟应用）

表1 工作空间元素分类

《证券基金经营机构信息技术管理办法》、《证券期货业网络和信息安全管理办法》、《证券期货业网络安全等级保护基本要求》等一系列外规对企业经营数据和客户信息提出了网络边界、计算环境等多方位的安全防护要求：

▶经营机构在本机构网络安全防护边界以外处理投资者个人信息的，应当采取数据脱敏、数据加密等措施，防范化解投资者个人信息在处理过程中的泄露风险；

▶证券基金经营机构应当完善网络隔离、用户认证、访问控制、数据加密、数据备份、数据销毁、日志记录、病毒防范和非法入侵检测等安全保障措施，保护经营数据和客户信息安全，防范信息泄露与损毁；

▶跨越边界的访问和数据流应通过边界设备提供的受控接口进行通信；

▶业务应用系统应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

▶证券基金经营机构应当记录经营数据和客户信息的使用情况。

近年来，随着公司对网络和信息安全工作重视度的不断提高，信息安全需求已逐步纳入到应用系统选型指标。而基于外规和最佳实践制定的应用系统安全功能开发规范则成为应用系统上线的安全评估标准之一。但作为一家业务主导、用以支撑业务的应用系统又是以商采为主的券商，在系统选型和上线过程中，对于应用系统本身安全功能缺失的情况，多以风险揭示或网络安全设备缓解为主要处置手段。

随着企业数字化转型，远程办公的常态化，企业的网络边界不断延伸，甚至逐渐模糊化。防火墙、IPS、WAF等传统的边界网络安全设备对于信息系统数据泄露风险缺乏有效的发现和控制机制。

工作空间的复杂多样，导致数据从可控区域流转至非可控区域，从网络安全防护边界内流转至防护边界外的场景增多。同时，如果把数据安全防护的压力全部集中到工作空间的话，对原本就不低的运维强度更是雪上加霜。

综上，对于降低信息系统数据泄露风险的措施，是对应用系统安全功能要求的强制执行?还是对边界网络安全设备进行补充?亦或全部由工作空间接管?成为数据安全保护措施实施者—信息技术部门首要考虑的问题。

数据分类分级，还是统一标准?

《证券基金经营机构信息技术管理办法》中规定“证券基金经营机构应当将经营及客户数据按照重要性和敏感性进行分类分级，并根据不同类别和级别作出差异化数据管理制度安排。”《证券期货业数据分类分级指引》为证券公司的数据分类分级工作提供了指导性原则；2022年起，监管机构的年度监督检查工作内容较历年增加了“数据分类信息、数据基础信息、公民个人信息、数据详细分类分级信息”项。由此看出，各级监管部门对于数据分类分级工作的重视程度不断提高。

基于数据分类分级有助于企业根据数据不同级别，确定数据在其生命周期的各个环节应采取的数据安全防护策略和管控措施，进而提高数据管理和安全防护水平，确保数据的完整性、保密性和可用性。

但现实情况，公司虽已开展数据分类分级标准制定工作，但因涉及繁多的数据资产梳理、多部门间的协作，此项工作呈现推进周期长，落地难度大的特征。同时，在数据安全管理工作开展初期，因企业内部权责划分不清晰，导致信息技术部门为避免监管罚单或规避数据泄露后的无限连带责任，而采取统一的强管控以实施信息系统数据安全保护。

数据安全防护措施的一刀切属于“用短期的解决方案来应对长期问题”。短期内不失为一种简单、粗暴，但见效快的方法，长远来看，必然会加大数据安全防护的投入成本，严重影响用户使用体验，同时也易在企业中形成“数据安全管理部门=信息技术部门“的观念。

基于数据分类分级标准的安全防护措施落地难，一刀切的粗犷式防护则不利于企业数据安全工作的持续开展。如何在”两难“之境寻求最佳平衡点，成为数据安全保护措施实施过程中的又一难题。

基础防护，还是数据生命周期防护?

经过多年的信息安全体系建设和等级保护工作的持续开展，企业在数据资产的传统环境--网络、主机、终端、应用、数据库、人员、组织等方面的建设基本完成，且已具备尚可的信息系统安全基础防护能力。虽然网络安全等级保护工作直接作用对象包括了数据资源，信息系统安全基础防护措施对静态数据也较为有效，但对动态数据的安全保护能力确实有限。

《证券基金经营机构信息技术管理办法》中规定“证券基金经营机构应当结合公司发展战略，建立全面、科学、有效的数据治理组织架构以及数据全生命周期管理机制，确保数据统一管理、持续可控和安全存储，切实履行数据安全及数据质量管理职责，不断提升数据使用价值”，《证券期货业数据安全管理与保护指引》也提出了“数据安全保护措施宜覆盖数据全生命周期”基本原则。

证券公司积累着大量的数据资产，且存在数据资产权责不一致、数据流转路径杂、流通渠道多等问题，因此一般会基于数据使用场景，让覆盖数据生命周期的安全防护能力有效落地。但在数据使用场景梳理过程中，企业却又面临着数据安全风险评估方法的选择、数据安全风险的识别，以及数据价值和数据风险间的平衡等难题。

建设思路

作为一家数据安全建设还处于初级阶段的企业，无论是人员能力和意识培养、权责划分，还是数据分类分级，数据使用场景梳理等工作均在起步中。此阶段，信息技术部门很大程度上仍旧会是公司信息系统数据安全的主要“责任人”。

缺乏话语权、投入成本有限、数据分类分级工作成效亟待提高，数据全生命周期的安全防护措施实施难以落地，以及数据泄露后的无限连带责任，让我们聚焦终端安全，通过“数据围栏”的防护模式，使用“数据分类+系统分级”的轻量级标准，构建全链条的安全防护矩阵，以降低企业内部信息系统的数据泄露风险。

数据围栏

多元化的办公场景下，应用系统、网络边界和工作空间是信息系统数据流动的必经之路。应用系统安全功能要求、边界网络安全设备和工作空间安全防护均各尽其职，层层防护拦截，降低信息系统数据泄露风险，最终形成“数据围栏”。

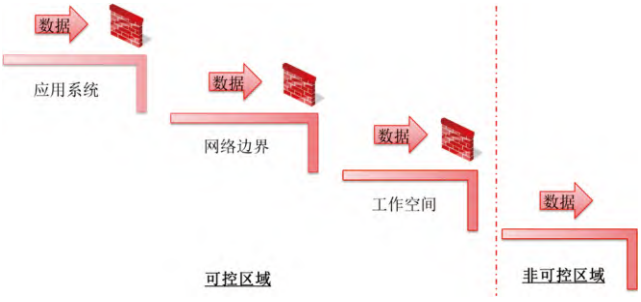


图1 数据围栏

应用系统层面，通过标识与认证、授权与访问控制、会话管理、数据安全、软件容错和异常管理、客户端安全、安全审计、互联网交互式服务等方面提出安全功能要求并进行了风险等级划分，强合规项具有系统上线的一票否决权。

网络边界层面，对于因应用系统安全功能缺失所产生的

数据泄露风险，在各级（互联网、办公网、业务网等）网络边界通过网络访问控制、安全防御设备拦截、流量监测和告警、内容审计等手段进行过滤。

当数据流转至用户工作空间后，则通过身份认证、外发文件和外设管控、水印、录屏、审批和审计等手段进行全链条防护。

在“数据围栏”的防护模式下，工作空间与应用系统安全功能要求、网络边界防护共同协作，为终端安全创造良好的先行条件，减小端点侧数据安全防护压力。通过该模式，将信息系统数据泄露风险尽可能在可控区域内得以控制，并对于流出围栏后的数据泄露具备一定追责或追溯能力。

数据分类，系统分级

在数据分类分级的基础上，数据安全管理将有的放矢地实施。但由于公司现行数据分类分级标准暂时无法产生太多实际效果，于是我们在终端侧采用了轻量级分类分级方法--数据分类、系统分级。

1.数据分类

《证券基金经营机构信息技术管理办法》中规定“具备完善的信息安全防护措施，能够保障经营数据和客户信息的安全、完整“，我们结合目前公司最迫切的数据保护需求，将数据分为三类：公司重要经营数据、客户个人信息和其他数据。

2.系统分级

在上述数据分类基础上，将企业对内提供服务的信息系统级别分为两级。示例如下：

数据分类	信息系统分级
公司重要经营数据	2
客户个人信息	2
其他数据	1

表2 信息系统分类分级

全链条防护

实现覆盖数据全生命周期的安全防护“路阻且长“，现有的信息系统基础防护能力对流动数据的安全防护效果不佳。我们针对不同的工作空间（办公场景）和信息系统级别，通过” 事前威慑、事中监控拦截、事后审计“在终端侧实施全链条的数据安全技术防护措施，最终达到“吓走一批人、警示一批人、处置一批人“的目的。全链条的安全防护矩阵示例如下：

工作空间	信息系统级别	事前威慑					事中监控拦截						事后审计			
		网络准入	身份认证		设备认证	数字水印	外发文件阻断	外设端口管控	恶意软件防范	防截屏	文件交互审批	上网行为管理	文件交互审计	截屏审计	录屏	数字水印
			人员	应用系统												
客户经理 移动终端 APP 非固定场所	2	√	√	√	√	√	√	X	√	√	X	N/A	X	√	X	√
员工 物理 PC 虚拟桌面 固定场所	2/1	√	√	√	√	√	√	√	√	X	√	√	√	X	X	√
员工 笔记本 C/S、B/S 非固定场所	1	√	√	√	√	X	X	X	√	X	X	N/A	X	X	X	X

表3 安全防护矩阵示例

信息安全建设至今，每个企业都会因为监管要求和自身安全需求，或多或少部署有一系列的安全产品。考虑目前投入成本有限，且长期来看，基于数据分类分级，覆盖数据全生命周期的安全防护措施对企业数据安全来说肯定最为有效手段。因此，现阶段我们没有采购额外产品，而是对现有安全措施进行整合，对于全链条中某阶段缺失的技术防护，会转由其他阶段的安全措施进行缓解。

此外，企业网络安全运营平台会对终端安全产品日志进行统一收集、分析，实现文件流跟踪、终端用户行为跟踪等场景。

总结和展望

无论是网络安全，还是数据安全视角出发，终端安全建设都存在终端环境复杂，安全产品有着填不完的坑，用户计算机知识水平参差不齐等情况，最终导致终端安全建设即“费人”也“废人”。要想摆脱当下困境，运维到运营，手工到自动化，都是信息安全团队必须做出的转变。

终端安全建设是管理、技术和运营的组合，同时也是一项平衡用户体验和安全要求的工程。看似能够缓解上述矛盾的零信任技术在终端侧的应用，现阶段到底只是增强型VPN，还是基于身份、设备、网络和应用的持续评估和动态调整，有待观望。

参考资料

1.《证券基金经营机构信息技术管理办法》
2.《证券期货业网络和信息安全管理办法》
3.《证券期货业网络安全等级保护基本要求》
4.《证券期货业网络安全等级保护测评要求》
5.《证券期货业数据分类分级指引》
6.《证券期货业数据安全管理与保护指引》
7.《金融数据安全 数据生命周期安全规范》
8.《数据安全治理白皮书》
9.《信息安全技术 数据安全能力成熟度模型》
10.《终端安全运营的实践和思考》欧阳昕
11.《终端安全的十年》zhenglei
12.《数据安全场景建设思路探索》兴业证券

金融企业CMDB建设实践

文｜陈建茂

行业机构

摘　要： 本文介绍了CMDB（Configuration Management Database）的概念、作用、优点以及构建CMDB的一个范例。CMDB是一个用于存储和管理IT基础设施中各种配置项（如服务器、网络设备、应用程序等）信息的数据库。它可以帮助组织实现IT系统的标准化和规范化，提高系统的可靠性和稳定性，降低运维成本，并增强IT系统的安全性。

关键字： CMDB、配置管理、IT基础设施、标准化、规范化、可靠性、稳定性、安全性、管理、维护

CMDB是什么

图1 某百科对CMDB的定义

上图是某百科对CMDB的定义，笔者认为存在明显的错误，经过反复思考和结合实践，笔者总结出以下三点内容，是否比某百科更好理解和更准确，由读者进行评价。

第一、CMDB是一个逻辑数据库，存储和管理需要管理的对象（专业术语叫配置项Configuration Item）和对象（CI）之间的关系。

第二、CMDB的内容要被使用，能发挥信息的价值。使用者可能是某个业务系统、可能是本人、可能是团队其他成员。

第三、CMDB必须有流程或机制来更新信息，保证信息的准确性。可以是自动的，也可以是人工的。

图2 关系树示意图

如果文字不好理解，笔者画了一张关系树，这张关系树包含系统台账、硬件台账、软件台账、数字证书台账、人员台账、供应商台账、应急联系人台账、合同台账、机房台账、机柜台账、IP地址台账等等管理对象。这些对象之间是存在关系的，例如应用系统分配多少台服务器、部署多少软件、使用多少张数字证书、等级保护是几级、软件供应商是哪家、是否有维保服务商、维护负责人是谁等等。这些全部要存储在CMDB中进行管理，对外提供服务接口用于数据查询和数据更新。

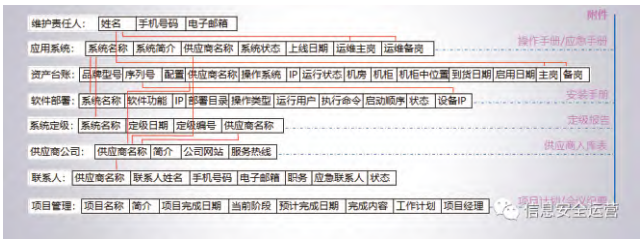


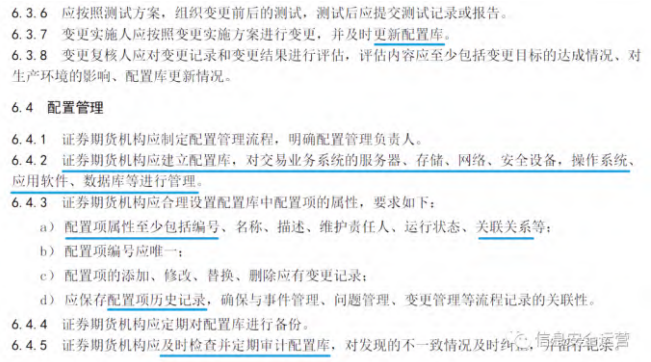
图3 数据表结构和关联关系示意图

如果关系树有点抽象，笔者给大家展示数据库中落地实施的数据表和关联。数据表就是台账，例如资产台账包括资产编号、品牌型号、序列号、硬件配置、操作系统、IP、到货日期、启用日期、运行状态等自有属性，机房、机柜、应用系统、部署软件、数字证书、主岗、备岗、供应商等外部属性通过关联进行建立。

为什么要建设CMDB

建设CMDB是外部监管机构的要求，也是内部团队协同工作的基础。

证监会2013年发布的《证券期货业信息系统运维管理规范》(现行有效)明确要求证券期货机构应建立配置库，对交易业务系统的服务器、存储、网络、安全设备、操作系统、应用软件、数据库等进行管理。



6.3.6 应按照测试方案，组织变更前后的测试，测试后应提交测试记录或报告。
6.3.7 变更实施人应按照变更实施方案进行变更，并及时更新配置库。
6.3.8 变更复核人应对变更记录和变更结果进行评估，评估内容应至少包括变更目标的达成情况、对生产环境的影响、配置库更新情况。

6.4 配置管理

6.4.1 证券期货机构应制定配置管理流程，明确配置管理负责人。
6.4.2 证券期货机构应建立配置库，对交易业务系统的服务器、存储、网络、安全设备，操作系统、应用软件、数据库等进行管理。
6.4.3 证券期货机构应合理设置配置库中配置项的属性，要求如下：
a）配置项属性至少包括编号、名称、描述、维护责任人、运行状态、关联关系等；
b）配置项编号应唯一；
c）配置项的添加、修改、替换、删除应有变更记录；
d）应保存配置项历史记录，确保与事件管理、问题管理、变更管理等流程记录的关联性。
6.4.4 证券期货机构应定期对配置库进行备份。
6.4.5 证券期货机构应及时检查并定期审计配置库，对发现的不一致情况及时纠正，与留存记录

图4 证券期货业信息系统运维管理规范的配置管理要求

金融企业随着规模的不断增长，信息系统数量和技术人员数量也不断增加，原有的电子表格台账存在无法关联、更新不及时、无变更记录、不支持高并发访问等短板，已无法满足团队高效协同工作的要求。很多工作需要应用系统管理员、存储系统管理员、基础架构管理员、网络安全管理员共同完成，CMDB就是团队高效协同工作的专家系统。

如何选择CMDB

目前除了自研CMDB外，采购商业软件和使用开源软件都是较好的选择。对于经济实力雄厚和对CMDB有着较高要求的金融企业，可以优先考虑商业软件；对于系统建设比较谨慎和技术人员爱好研究新技术的金融企业，可以优先考虑开源软件；对于无法投入数十万以上采购商业软件，又无技术人员研究开源软件，可以优先考虑外包方式（开源软件＋技术服务）。

如何建设CMDB

使用开源软件是建设CMDB的一种方式，笔者使用一台较低配置（4核8G内存60G硬盘）的虚拟机就完成CMDB的部署，部署时间小于2小时，内存增加至12G可作为办公系统支持30位人员的并发访问，增加服务器可实现高可用架构。

图5 开源CMDB版本信息

CMDBuild软件是由意大利团队维护的开源项目，初始版本发布于2006年，每年保持一次以上版本迭代。目前最新版本是3.4.1，发布于2022年9月30日，支持私有化部署，已支持全球32种操作语言，是被认可度较高的开源CMDB软件。在官方网站有应用软件、技术手册和说明手册等提供下载。

如何使用CMDB

CMDB的使用一定要场景化，实实在在地将CMDB用起来，发挥CMDB的价值。本次介绍3个场景，笔者实际已使用包括应用管理、运维管理、项目管理、基础架构管理、安全管理、资产管理、综合管理、供应商管理等的20多个场景。

资产台账管理

图6 资产台账管理界面

CMDB的发展源于资产管理，目前已涵盖技术管理的方方面面，具体管理内容取决于管理者的管理需求，本次介绍的第一场景从资产管理开始。

资产管理的基础功能是实现资产台账的线上化，将原来保存于电子表格的台账导入到系统中进行管理，这是高级资产管理的基础。在电子表格的时代，资产台账由资产管理员进行独立管理，记录在一张资产台账里，例如服务器功能这项是他无法管理好的，因为决定服务器功能的不是硬件，也不是操作系统，是应用软件，应用软件由应用系统管理员进行部署和管理的。使用CMDB能很好解决上述问题，将服务器信息的管理职责进行拆分，各自负责职责范围内的内容，真正实现团队的高效协同。

图7 资产台账卡片界面

资产管理员对服务器的资产编号、品牌型号、序列号、硬件配置、到货日期、启用日期、所在机房机柜位置、运行状态在“卡片”内进行维护，不涉及使用功能，详见以上截图。

主岗备岗可同时操作，数据修改立刻生效，可以避免主岗和备岗在信息方面存在差异。也能有效规避将不合适的责任分配给不具备权限的人员进行承担，更好地实现权责对等。

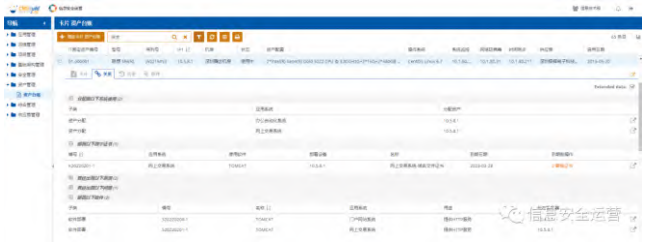


图8 资产台账与其他管理对象的关联展示界面

应用系统管理员专注于服务器的使用功能信息，动态形成“关系”，详见以上截图。

例如某系统被分配了服务器，应用系统管理员建立一下“系统名称”与“所分配的服务器”的关系。应用系统管理员部署了应用软件，填写软件部署信息，建立一下“应用软件”与“运行的服务器”的关系。应用系统管理员部署了数字证书，填写数字证书信息，建立一下“数字证书”与“运行的服务器”的关系。网络安全管理员发现了一个安全漏洞，填写漏洞管理信息，建立一下“漏洞信息”与“运行的服务器”的关系。

通过截图能清楚了解到此服务器分配给2个应用系统使用，使用一张数字证书，有效期到2023年3月28日，曾经出现2个系统漏洞，曾经出现1个技术问题，部署2套应用软件。这些都是通过关联的方式自动形成的，建立关系时自动添加，关系解除时自动消失。

特别说明：金融企业不会在一台服务器上同时运行交易类和非交易类的应用软件，也不会将交易类和非交易类的服务器放置在同一个DMZ中，分层分区是基本的安全管理原则，上述举例是希望向读者展示CMDB的功能。

CMDB系统的审计功能是非常重要的，在一定程度上保障了数据的准确性和更新的及时性，在“历史”中展示，详见以下截图。

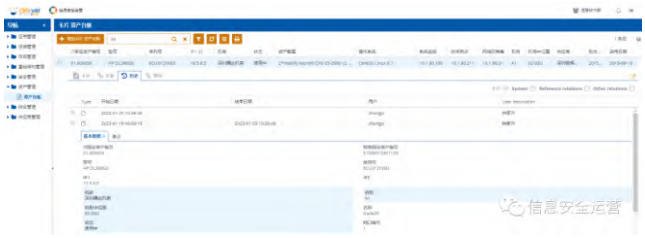


图9 资产台账全部历史记录界面

审计记录可以详细记载数据的全生命周期的变化，什么时候、由谁进行登记或修改、修改的最新内容都全部进行记录，这些记录是永久保存的，而且查看特别方便。

如果与部门的管理制度进行结合，要求系统管理员在更新CMDB后到OA流程中进行反馈，系统管理员就没有了偷懒的空间，因为审计信息将如实记录他的相关操作(操作内容和操作时点)。

“误改”是人工更新数据所绕不过的话题，如果有上述强大的审计功能，发现信息被误改是可以很容易纠正的，因为历史数据都在，可以实现秒级找回。如果是原来的电子表格台账，历史数据已被覆盖，修改时间也不知道，能否找回都是一个问题。

场景小结：基于CMDB，资产管理的职责被正确地进行拆分，资产管理员负责硬件管理，应用系统管理员负责功能管理，各自负责维护好职责范围内的内容，确保数据正确和更新及时。在管理实践中，需要规章制度明确更新CMDB的职责要求，在处理OA变更流程时如遇到资产信息变化需反馈更新CMDB的大致内容，确保CMDB资产数据得到更新，准确的CMDB资产数据才有价值，才能支撑技术管理工作。

应用系统管理

图10 应用系统管理界面

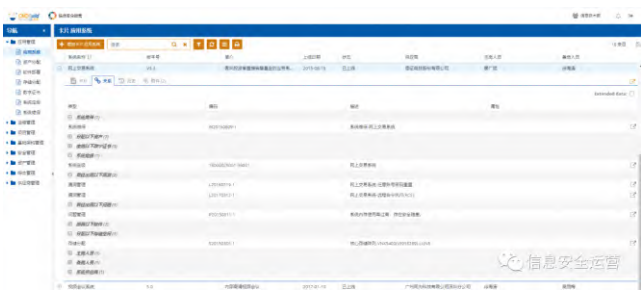


图11 应用系统与其他管理对象的关联展示界面

“应用系统”是技术管理的工作重点，技术部门的多数岗位都是围绕 “应用系统”开展工作的，现在介绍“应用系统管理”场景的使用，看看基于CMDB如何支撑团队进行高效协同工作。

如以上截图所示，通过“卡片+关系”的方式实现对应用系统的360度画像，真正全面了解应用系统才能管理好应用系统。

作为应用系统管理员，是否真的了解所管理的应用系统？如果说主岗了解，备岗是否同样了解？我们希望在应用系统信息方面，主岗和备岗能达到一致的水平。

“卡片”内的信息由应用系统管理员负责维护，应用系统管理员主岗也未必熟悉相关信息，例如无法给出系统“上线日期”的正确日期，原因是前任维护人员的交接资料里没有系统上线日期，借助维护“卡片”信息的机会可以对系统信息进行补正，是一劳永逸的工作。

“关系”内的信息由相关管理员负责维护，系统定级信息由安全管理员关联过来，存储信息由存储管理员关联过来，维保信息由合同管理员关联过来，漏洞信息由安全管理员关联过来，数字证书信息由应用管理员关联过来，问题信息由问题登记者关联过来，主岗备岗由负责主管指定并关联过来等等，关系解除时自动消失。

图12 附件展示界面

“附件”是每条信息都具备的属性，可以根据需要进行管理，例如在应用系统里可以上传“系统验收报告”、“系统功能测试报告”、“系统用户手册”等附件，需要时可以快速进行阅读和下载。

基于网络带宽和用户体验的考虑，笔者一般设置单个附件大小上限为30M，数量不限，基本能满足使用要求。

场景小结：通过使用CMDB，技术部门人员能比以前更加了解业务系统，知道业务系统的基础架构信息、系统管理员信息、安全信息、维保信息、供应商信息、联系人信息等等，当然这些信息是所有人员一起贡献、知晓和维护的，真实而且及时的，所有各岗位的技术人员能形成合力，消除潜在的风险隐患，共同保障应用系统的安全高效运行。

供应商管理

图13 供应商管理界面

“供应商管理”是技术管理的工作之一，在《证券期货业信息系统运维管理规范》明确要求证券期货机构应定期收集、更新供应商信息，组织对供应商的服务质量、合同履行情况、人员工作情况等内容进行评价，形成评价报告，并跟踪和记录供应商改进情况。

金融企业一般不会建设独立的供应商管理系统，或采购OA系统中的供应商管理模块，使用CMDB进行供应商管理是比较合适的解决方案。

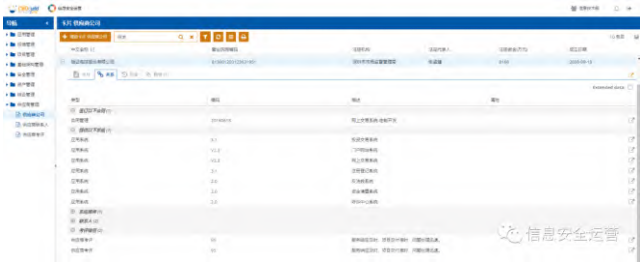


图14 供应商与其他管理对象的关联展示界面

“卡片”内的信息由初次引入供应商时进行登记，主要包括供应商的基本信息。在登记之前可以将供应商信息表格提交到部门领导进行审核，完成供应商入库审批，供应商信息表作为附件进行上传。

“关系”内的信息全部通过关联自动生成，可以动态展示与该供应商签订的合同信息、该供应商为本企业提供的应用系统清单、目前提供哪些系统维保、业务联系人、技术联系人、历年的考核评价信息等等。

场景小结：供应商是技术部门的合作伙伴，特别在应用系统出现异常时，技术人员必须立刻联系到供应商的技术联系人，如果技术人员把供应商公司和联系人信息集中维护，可以避免因联系不到人员而耽误异常情况的快速处理。

CMDB建设基础

建设CMDB是将原来分散在各个人员手中的电子表格和附件进行集中化、在线化管理，建设基础是信息的标准化和规范化，以下是一些举例和处理方法。

名词不统一

图15 对机房名称进行统一的举例

金融企业一般有多个物理或虚拟机房，在使用电子表格台账时，机房名称是任意录入的，例如深圳腾达机房有深圳腾达机房、深圳腾达3楼机房、深圳机房、深圳自建机房、深圳IDC、深圳市腾达机房、深圳生产机房、深圳主机房等等名称。建设CMDB时，统一确定为“深圳腾达机房”，在资产上架使用时，通过选择的方式确定所在机房名称，不允许输入机房名称。

类似的不统一还有应用系统名称不统一、机柜号不统一、各类状态不统一、各种等级不统一、操作系统名称不统一、供应商名称不统一、应用系统管理员不统一等等。

日期格式不统一

日期是重要的管理信息，在使用电子表格台账时，日期是任意录入的，在梳理历史信息发现很多类似2015/11/31、2013-06-a1、2016年5月等错误或无法确定日期的信息。建设CMDB时，使用“日期型”字段，导入导出时使用“yyyy-mm-dd”格式，对日期数据进行规范化，类似2015-02-29的信息将因校验不通过而无法使用。

类似的问题还有必填的信息出现缺失，在使用CMDB时，缺少必填的信息将无法进行提交。

未从使用角度管理数据

图16 对U位信息进行规范的差别展示

将数据在CMDB中进行管理的目的是为了使用，例如上图“机柜中位置”的数据，可以使用2-3U、5-6U、8-9U等数据，也可以使用02-03U、05-06U、08-09U等数据，但当我们对“机柜中位置”的数据进行排序时，差别就立即体现出来，使用02-03U的左图可以一目了然展示设备的上下位置关系和机柜剩余位置，右图就是乱七八糟。

由此可见，将原来电子台账的数据导入CMDB后，需要对数据进行管理，使数据更加符合使用需要，后续登记时按照新的要求进行填写。

CMDB建设难点

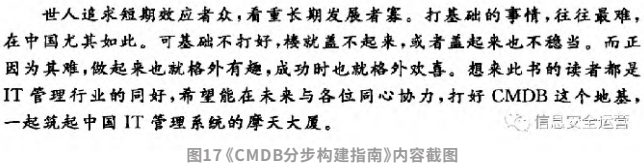

世人追求短期效应者众，看重长期发展者寡。打基础的事情，往往最难，在中国尤其如此。可基础不打好，楼就盖不起来，或者盖起来也不稳当。而正因为其难，做起来也就格外有趣，成功时也就格外欢喜。想来此书的读者都是IT管理行业的同好，希望能在未来与各位同心协力，打好CMDB这个地基，一起筑起中国IT管理系统的摩天大厦。

图17《CMDB分步构建指南》内容截图

以上截图来自《CMDB分步构建指南》书籍，“世人追求短期效应者众、看重长期发展者寡。打基础的事情，往往最难，在中国尤其如此。”在一定程度上体现CMDB建设的难度特别大。

如果是采购商业软件来建设CMDB，建议把项目按照“一把手”工程进行处理，最好以管理咨询项目进行切入，没有公司领导或部门负责人的支持注定会失败。如果是使用开源软件来建设CMDB，以满足资产管理、应用系统管理等场景化使用需求，可以立刻开始建设，基本没有难度，成功的概率很高。

补充说明

友好的用户界面

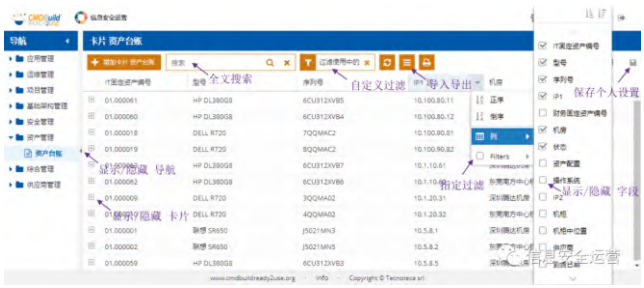


图18 CMDBuild用户界面和标注

相对其他开源CMDB软件，友好的用户界面是此款CMDB软件的亮点之一，功能布局非常合理，普通用户可以经过简单培训，甚至无需培训即可开始使用。

每个用户可以自定义用户界面，选择要显示的字段，拖拽

字段的左右位置，自定义多个过滤条件，可以选择一个过滤作为默认过滤，保存或清除个人设置。

支持全文搜索指定关键字，将包括关键字的条目全部列出，搜索速度非常快，基本都在1秒内完成搜索和条目列出。

全面的权限管理

图19 不同权限用户的用户界面

此款CMDB软件具备完善的权限管理功能，基于用户组进行设置权限，可以定义不同的导航菜单(如上图所示)，可以对不同的数据表定义添加、克隆、修改、删除、打印、导入、导出、附件、关系查看、历史记录查看的权限，可以在用户组之间进行切换。

由于审计信息是与条目进行高度绑定，在条目的“历史”中展示，条目的删除将导致审计信息的消失，管理实践中会把普通用户的删除权限不予分配，必要时由具有删除权限的用户进行删除操作。

强大的关联能力

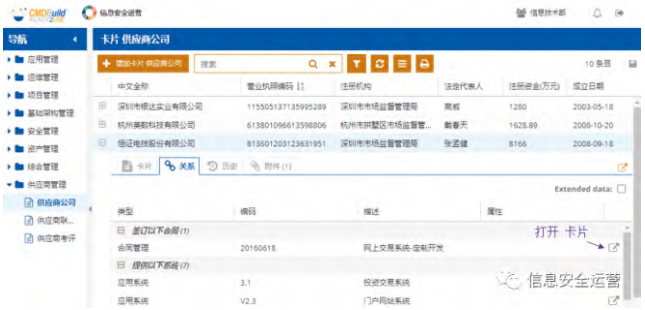


图20 实时关联信息展示界面和跳转功能

在介绍CMDB的定义时给大家展示过“关系树”，只要知道关系树中的一个节点信息，我们可以顺着关系找到需要的全部信息。

例如知道一个IP地址，可以关联出部署的软件、应用系统名称、系统管理员姓名、系统管理员手机号码、实体服务器、供应商公司、供应商技术人员姓名、技术人员手机号码等等，只需要在“关系”里不断打开卡片即可。

准确的数据底座

图21 电子邮箱收到通知邮件展示界面

经过一段时间的运行，CMDB中存储着准确的各种数据，这些数据可以给技术管理的很多系统使用，包括CMDB系统自身和其他各类业务系统，成为了技术管理的数据底座。

例如系统管理员前期已经维护了数字证书信息，笔者通过定制开发，读取数据库中的证书到期日期、证书名称、应用系统名称(关联获得)、系统管理员主岗和备岗的姓名(关联获得)、主岗和备岗的手机号码、电子邮箱(关联获得)，结合当天日期，计算出剩余有效期天数，在剩余有效期的90天、30天、15天、7天和3天向主岗和备岗发送通知电子邮件，同时抄送运维主管和笔者，向主岗和备岗发送手机提醒短信。

可以使用CMDB数据的包括监控系统、安全管理系统、流程管理系统、数据报送系统等等，详见各软件厂家的解决方案文档。

个人安全实验室

图22 个人安全实验室虚拟化主机界面

本文章展示的所有图片均来自笔者的个人安全实验室，由笔者根据分享的需要进行构建，并非金融企业信息，不涉及企业秘密。

CMDB是个筐

图23 一句非常经典的话

“CMDB是个筐，什么都可以往里装！”笔者认为包含两个意思：第一、CMDB是个筐，筐里装什么由管理者决定，需要充分发挥管理者的管理智慧，去定义场景并管理起来。第二、

如果您在技术管理时，有技术事项一直管理不好，CMDB会是最佳方案。

总结

CMDB是一个概念，不是一个固定的产品，企业可以根据自身需要建设多个CMDB，例如资产A-CMDB、安全S-CMDB、资源R-CMDB等等，只要达到笔者总结的三点内容就是好的CMDB。

CMDB系统是技术管理部门实现数字化转型的最佳实践之一，能够实现技术团队成员的高效协同、维护管理对象的动态关系、数据服务其他的业务系统、提升整体的技术管理水平，值得每一位技术管理者拥有。

企业研发环境安全管理实践探讨

文｜宋嘉

上海期货信息技术有限公司

摘　要： 数字时代，数据是企业发展的核心生产要素，也是驱动业务的关键，对于研发型企业而言，核心数据资产就是源代码，随着数字信息化的全面推进，面对来自外部和内部的安全风险，以及国家层面相关的政策法规的合规要求，传统的开发环境已经很难适应新时代的步伐，建设科学有效的防护体系，是研发型企业获得持续创新和市场竞争力的有力保障。

关键字： 研发环境、安全风险、防护体系

传统研发环境面临的一些问题

研发环境数据防泄密

传统PC的研发模式，项目开发中的源代码和技术文档等存放在本地硬盘，无法实现统一的存储管理，且开发人员可通过网络或存储介质拷贝等轻易带走各种项目成果，容易造成数据泄密的风险，数据的安全性得不到有效的保障。

外包人员安全管理

企业根据业务扩展的弹性需求，结合经营成本，一般都会聘请外包人员来解决人手不足的情况。由于外包人员存在很多不确定的因素，人员的稳定性、权限管理等，所以做好外包人员的安全管理，也是传统研发企业的难题。

研发环境的快速部署

传统PC+服务器虚拟化模式，软件研发测试的环境部署非常耗时，一般都需要依托运维部门逐台搭建开发测试环境，资源的回收重复利用率也低、不够灵活，影响软件研发测试效率和项目进度，同时运维成本高，无法统一管理。

研发环境配套安全管控

软件开发全生命周期过程中，如何确保依赖组件安全，如何确保使用的组件没有安全漏洞和法律风险，缺乏统一规范的管理。

远程开发的安全管理

针对不同场景的远程接入需求，如何确保研发人员远程接入研发环境，在兼顾数据安全的情况下完成开发、测试工作，尽可能减少对业务的影响。

分支机构研发环境协同管理

很多研发企业存在多分支机构研发中心，如何确保分支机构和母公司之间协同办公的便利性和安全性。

研发环境安全管理实践探讨

每家研发型企业的业务模式、研发模式、环境场景都是不同的，相对于安全的需求也是不同的，需要结合实际情况制定出一套符合自身企业的安全管理方案，但保护企业核心资产安全的出发点，大家应该都是一样的。在外部威胁和合规要求的驱动下，我们也是在一条以保护核心资产为基础、业务与安全相平衡的道路上不断的探索前进。

研发环境的安全管理，首先企业内部需要定一个基础的安全的原则，我们认为只要是能连通互联网的设备或者区域就是不安全的，结合国家合规层面数据安全法、数据分级分类指引、数据安全管理与保护指引等要求，通过分析企业内部不同的应用场景，数据的重要等级、业务的重要程度，融合安全纵深防御的理念。在基础安全架构层面划分了三个不同等级的安全域，分别为高敏区、中敏区、低敏区，综合安全和业务之间的平衡，定位了各区域的功能属性：

高敏区：属于高信息安全等级环境，以安全为优先，用于隔离保护公司具有重要意义的关键产品/项目/技术

中敏区：属于中信息安全等级环境，安全与效率平衡，用于隔离保护公司需要防护的产品/项目/技术

低敏区（办公区）：属于低信息安全等级环境，以效率为优先，用于企业日常办公和互联网业务需求

跨区域间的网络控制采用增强型逻辑隔离的方式，跨区域间的数据传输只能通过数据安全摆渡的方式，数据在跨区域间传输可结合业务实际情况、数据的重要等级设置对应的审批机制，其实可以理解为各区域间的数据传输用的就是带

审批功能的网闸，敏感数据跨区传输需要有脱敏的环节。高敏区和中敏区不能连通互联网，企业的研发基本都属于中敏区和小部分的高敏区，原则上核心业务不能使用外包，外包人员默认只能在中敏区开发环境，根据对应的访问权限，执行开发任务。如有特殊情况需经相关部门就合理性和必要性做相关的风险评估。

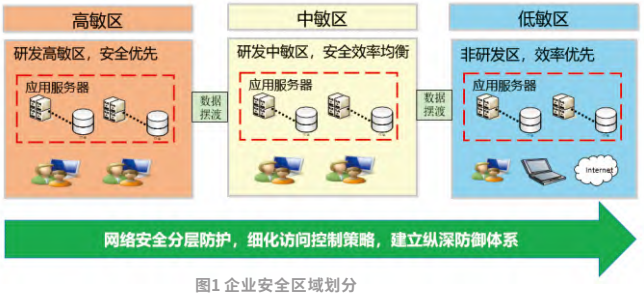


图1 企业安全区域划分

研发环境基础资源建设，通过在企业内部部署云桌面+云服务平台的方式，利用虚拟化计算、存储、网络的超融合技术和统一的云管理平台，构建安全稳定、易扩展、易管理的企业内部私有云。整个建设方案的特点，整体资源的高可用性，支持虚机故障自动迁移、多副本分布式存储确保数据的可靠性、基于SDN + 堆叠的网络高可用。建设方案的优势，平台的易扩展性，后续随着业务的变化，资源的扩充只需要增加服务器进相应的节点，但需要注意的是服务器的兼容性。资源的快速发放简化运维，当研发人员需要增加云桌面资源时，只需要通过云管理平台统一或批量下发即可，当研发人员申请服务器资源时，云管理平台可提供几种场景的资源供研发人员选择后快速部署发放，同时当资源不使用时，管理人员可以对资源做快速的回收处理，避免资源浪费。

通过云桌面的模式保障数据的不落地，所有的数据都是存储在企业内部私有云，同时通过云桌面外设管控，不允许通过存储介质等设备将数据拷出，所有跨区域间的数据传输都需要通过数据摆渡的模式，审批通过后才能进行数据传输，数据摆渡同时支持审计记录，方便后期溯源。研发人员可通过TC瘦终端或是笔记本的模式接入云桌面、同时云桌面支持桌面水印功能，威慑防止截屏。

在中敏区和高敏区里面，我们也会有对应研发的通用资源，通过登录云桌面就能访问的公共资源。但由于区域内研发人员，他们可能属于不同的部门、项目组，或是不同的产品线，对业务服务器的访问有不同的权限要求，这种情况之下，通过云平台基于租户的管理模式，自定义隔离不同部门、项目组或是产品线之间的网络通信。在高中低三区安全域隔离的情况下，每个单独区域内部进一步实现了微隔离。

软件研发过程中，难免需要用到外部的依赖组件，通过建设企业统一可信源的制品库，规范研发过程中依赖组件的安全性。防止下载的开源组件有漏洞，或是组件可能存在的法律风险。由于研发人员所属的区域是不能连互联网的，为了确保运维自动化和效率问题，通过办公区和高中敏区部署多级制品库的方式，办公区部署制品库源从指定的互联网源拉取数据，经制品安全扫描后，选择满足企业对开源组件漏洞安全和许可证合规性方面管控要求的产品后，通过对接区域间数据摆渡系统提供的安全API接口，传入企业研发环境。

在实际的工作场景中，总有一些离不开远程办公的场景，研发人员出差、项目代码应急查阅、疫情时期等特殊情况。目前是通过VPN+云桌面的方式，后续考虑通过零信任SDP+云桌面远程办公的模式接入，结合SPA单包敲门的机制、多因素的认证管控，资源权限最小化的原则，在满足不同场景远程接入的同时，保障数据的安全可控。

分支机构研发环境的协同管理，有时国内的分支机构需要和母公司接入同一组研发环境，目前我们是通过专线的方式，达到延申云桌面网络的效果，云桌面的网络传输是通过压缩的，所以带宽资源的消耗还是可以接受的，前提是云桌面虚机和测试环境之间不是两地部署。

从安全的角度来说，部署私有云配合区域管控的方式，通过统一各种操作系统、应用版本、安全基线等，实现了资产标准化的统一管理，同时也有效地收敛了风险暴露面，实现了数据不落地，安全管理的目标。

回顾与展望

在实践过程中我们也发现了很多后续待优化的方面，比如敏感数据传输通过DLP的赋能实现自动化，实际操作过程中，由于敏感数据的多样性，导致很难通过关键字或正则匹配、特征库等方式实现自动化的有效管控，跨区的数据传输还是依赖人工审核的方式，但人工审批还是存在一定的局限性，通过对摆渡数据的内容和描述，进行主观的判断，无法对通过技术手段刻意隐藏的数据做准确的判断。

云桌面水印的增强管控，云桌面数据虽然不落地，但还是可以通过拍照等方式留存，传统水印只是起到威慑的作用，相对于比较核心的数据，是否可以通过数字水印等方式加强水印的威慑性，在处理纠纷时可以提供有力的证据。

远程办公场景的安全性，虽然VPN可以通过终端检测，多因素认证等安全管控方式，但还是避免不了VPN接入时终端已经被远控的场景，虽然很多厂商目前支持VPN专网的模式，但业务场景多样化，需要满足很多特定的互联网需求，比如需要支持带通配符的域名等，而且安全管控措施需要满足各种信创终端的适配等。

整体研发环境的安全防护目前还是通过传统的终端管控、入侵检测，多因素的认证机制、安全域隔离的方式，来抵御相关的安全风险。随着最近几年零信任理念的逐渐成熟，后续可以在基于边界防御的基础上，增加一些零信任的防护能力，比如基于UEBA的持续信任评估能力，毕竟一个人的身份可以伪造，但一个人的行为拟态是很难伪装的。

浅谈社会工程学攻击的几种方式

文｜江旺、张双双

华泰证券股份有限公司

摘　要： 随着社会工程学攻击越来越成为攻防中一种不可忽视的攻击方式，其攻击方式多、攻击途径广的特点增加了防守方的防御难度，本文详细阐述了社会工程学的攻击方式和攻击途径，并以最为常见的钓鱼邮件攻击和IM投毒为例详细说明了防守方的防御策略与应对手段，对日常安全运营中应对社会工程学攻击有普遍的参考意义。

关键字： 社会工程学、钓鱼邮件、IM投毒、安全防御

概述

正如著名黑客凯文·米特尼克在《欺骗的艺术》中对社会工程学的定义："通过心理弱点、本能反应、好奇心、信任、贪婪等一些心理陷阱进行的诸如欺骗、伤害、信息盗取、利益谋取等对社会及人类带来危害的行为"。在计算机科学中，社会工程学指的是通过与人的合法交流，传递虚假消息来使其心理受到影响，做出某些动作或者是透露一些机密信息。这通常被认为是一种欺诈他人以收集信息、行骗和入侵计算机系统的行为。随着网络安全防护技术及安全防护产品应用的越来越成熟，诸如（WAF、IPS、IDS、EDR）等安全防护产品的大规模应用，很多常规的入侵手段越来越难。正面突破逐渐成为一种成本高、收益低的攻击途径。根据腾讯攻击队对日常攻防演练发布的数据可知，社会工程学（主要为钓鱼）在较少的时间成本下，可以拿到和正面突破差不多的分数，在这种情况下，更多的黑客将攻击手法转向了社会工程学攻击，同时利用社会工程学的攻击手段也日趋成熟，技术含量也越来越高。

社会工程学常见的攻击手段

计算机和网络都离不开人为的操作，在网络安全中，人是最薄弱的环节。如上文提到，通过对人性的分析和挖掘，利用人存在的一些固有弱点，就有可能达到事半功倍的效果。不管采用何种社会工程学攻击方式，其最后到人这一侧，其话术和套路大体都是相同的。主要分为以下几个方面：伪装欺诈、恐吓、反向社会工程学。

(1)伪装欺诈：主要伪装成客户、高管、求职者、朋友、同学、投资者等与受害人职业或关系较近的身份，骗取受害人信任，诱导受害人点击病毒文件等恶意样本。

(2)恐吓：攻击者常常以权威机构的身份出现，散布安全警告,系统风险之类的信息，使用危言耸听的伎俩恐吓欺骗计算机用户,并声称如果不按照他们的要求去做,会造成非常严重的危害或损失。

(3)反向社会工程学：反向社会工程学是指攻击者通过技术或者非技术的手段给网络或者计算机应用制造"问题"，使其公司员工深信不疑，诱使工作人员或网络管理人员透露攻击者需要获取的信息。

社会工程学常见的攻击途径

通过上节我们可知，黑客进行社会工程学攻击时经常进行伪装欺诈、恐吓等方式，社工以其途径多，门槛低等特点，越来越受到黑客的重视。结合目前网络环境中常见的社会工程学攻击方式，其主要的攻击途径有：利用IM即时通讯软件如：企微、QQ、钉钉等；钓鱼邮件攻击；虚假网站；近源攻击。在实际安全运营中，以钓鱼邮件、IM投毒最为频繁，接下来主要通过钓鱼邮件和IM投毒的攻击过程来详细讲述下社会工程学的攻击过程与防御手段。

钓鱼邮件攻击

Gartner研究报告指出：91%的APT攻击始于社交工程邮件，86%的加密勒索软件始于社交工程邮件。根据一份数据泄露报告指出：32%的违规行为涉及网络钓鱼，94%的恶意软件事件通过电子邮件传递。根据中国企业研究报告指出：40%的企业邮箱是正常邮件，意味这60%的企业邮件都是垃圾邮件，其中很大一部分可能为钓鱼邮件。

攻击者通常利用密码到期、发票、岗位薪资调整、财政补助等具有欺骗性的文字诱导受害者点击或者下载附件，从而达到窃取信息或远控的目的。其攻击方式也变得多种多样，通过日常安全运营可知，目前钓鱼邮件逐渐加密化、二维码化、图片化、精准化以及人工智能化。

IM投毒

随着IM作为对外沟通的渠道。其在防范社工钓鱼存在以下难点：

(1)应用范围广：微信、QQ、企业微信等IM软件、邮件在企业日常办公中承担重要支撑作用；对外沟通的重要渠道。

(2)检测难：IM软件协议私有，在协议层面无法还原，无法在网关和流量层面进行检测防范；同时装有IM软件的客户端遍布公司终端、自有终端。

(3)人的弱点：内部员工的安全意识参差不齐，面对针对性的话术诱骗容易落入圈套。

(4)处置难：无法快速定位失陷人员，很容易造成大面积失陷。

攻击者利用天时地利人和，在充分了解被害人的职位、工作内容、基本称呼和一些公开信息后进行有针对性的对话，一般的IM投毒主要伪装成客户、投诉者等，利用客服人员的工作性质，工作内容进行有针对性的话术欺骗，最终诱导受害者点击病毒文件，从而进行进一步的渗透。

社工攻击的响应与处置

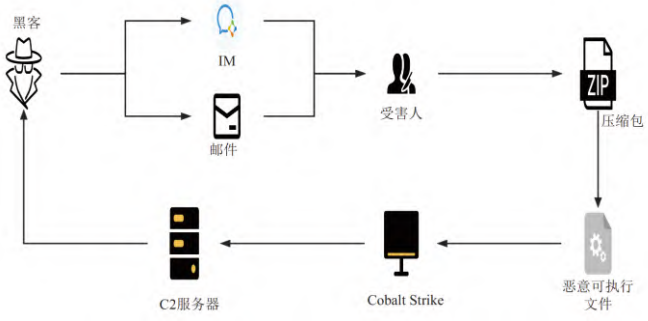


图1 社工钓鱼的攻击过程

一般的社工钓鱼流程如上图1所示，黑客通过IM、邮件等途径，利用欺诈、恐吓等手段，达到让受害人相信并下载恶意附件，执行病毒程序的目的。上面的例子可总结出，一般的钓鱼攻击过程分为三个阶段：

(1)投递阶段：攻击者通过向目标的 IM 即时通讯软件或者邮箱发送链接或者文件，诱导用户点击或下载文件执行。此阶段的主要特点是，攻击者利用人性弱点，进行社工突防，令人防不胜防。

(2)执行/内网横移阶段：当受害者运行了恶意程序后，恶意程序会在受害终端执行，建立持久化驻留，获取凭据，信息收集，横向移动等操作。此阶段的主要特点是，恶意程序为了能在系统中运行，通常都会经过免杀处理，从而逃避杀软的查杀。

(3)命令和控制(外联C2)：木马在受害终端运行后，为了获取终端敏感信息或建立进一步的恶意行为操作，木马会访问预先准备好的恶意地址，建立外联通信，从而实现远控。此阶段主要特点是，攻击者要实现窃取敏感数据等恶意操作，就需要外联。通常攻击者会采用一些隐匿加密通信技术进行外联通信。

针对上述两种常见的社工钓鱼方式，其防护手段也不尽相同，接下来结合防御示意图来简要叙述一下：

构建邮件纵深防御体系

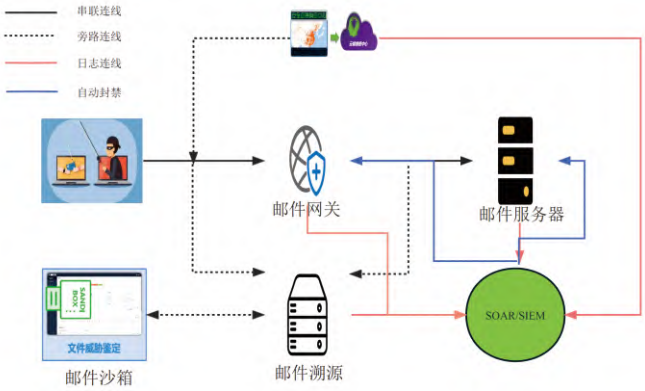


图2 邮件纵深防御示意图

如上图2所示，构建邮件纵深防御是解决邮件安全问题的一种思路，此防御体系可以总结为事前防御、事中防御、事后处置三个过程。

(1)事前防御：以加强人的安全意识为主，人是社会工程学的核心，任何攻击成功事件，都需要受害人的配合。所以一定频率的钓鱼演练和安全宣贯是社工防御必不可少的环节。情报的收集和获取也是事前防御的重点，购买情报服务或加入行业情报组织对于事前的社工防御也是重中之重，如果能先社工一步获取情报信息，提前建立起防御工事那么将极大减小被攻破的风险。

(2)事中防御：是整个纵深防御体系的关键环节，其中以邮件网关的防御能力为主，随着钓鱼邮件逐渐的加密化、二维码化、图片化甚至随着人工智能的兴起，钓鱼内容的生成也逐渐地智能化和精准化。邮件网关的能力也要随着技术的更新而不断的完善。其主要包括：SPF\RBL的检测能力、DDOS的防御能力、病毒邮件识别能力、垃圾邮件指纹分析能力、云情报联动能力、OCR识别能力、机器学习能力、Syslog日志推送能力、API功能对接能力。

(3)事后处置：对于透过邮件网关的钓鱼邮件，在用户点击威胁附件或链接之前，还有很短的一段时间，我们称之为邮件处理的黄金时间。如何在这段黄金时间如何在用户无感知的情况下快速删除邮件并封禁相关域名和IP，是思考邮件事后处置的基本出发点。我们通过SIEM（Security Information and EventManagement）接入各种邮件安全日志进行分析和告警，同时将确认无疑的告警发往SOAR（Security Orchestration Automation and

Response)进行自动化的编排和处置。其技术过程主要包括以下三点:1、邮件网关后流量接入邮件检测设备,包括邮件溯源系统、邮件M01联防系统、邮件沙箱等设备同时将这些设备检测的结果以syslog日志的形式传入SIEM;2、SIEM汇总来自旁路部署的各邮件安全设备的日志,同时还接入了邮件网关的日志、邮件服务器的登录日志等邮件相关日志,通过对邮件各种日志的汇总分析,分析出威胁严重的告警进而推送到SOAR;3、SOAR接收来自SIEM的威胁告警,包括邮件各维度的信息如发件人、收件人、主题等,通过打通SOAR对接邮件服务器的删除接口API和对接邮件网关的封禁接口API,同时编排应对各种场景的剧本,通过剧本来处置来自SIEM的告警。整个处置过程少于1分钟。

打造IM全流程处置体系

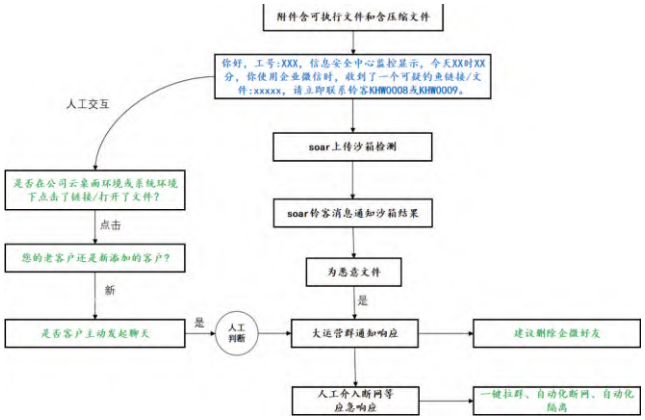


图3 IM社工处置示意图

如上图3所示,对于IM类投毒,进行IM的落地文件监控是至关重要的,尤其是可执行文件,一般木马程序都是通过可执行文件进行的。通过对文件的监控,把可疑文件放入沙箱进行自动化检测,如果发现有可疑文件,则通过IM进行通知检测结果,如果发现被受害人点击了威胁文件,则进行自动化断网,自动化隔离等一系列应急操作,通过对威胁文件的全流程监控,达到快速响应的效果。其过程主要分为以下几个方面:

(1)落地文件的监测,通过SIEM平台接入IM日志进行文件类型监控,主要针对于加密附件类与可执行文件类的检测。在此阶段通过分析判定该文件是否为恶意文件,如果为恶意文件则进行下一步操作。

(2)文件自动化检测,通过把威胁告警传给SOAR,SOAR接收来自威胁告警的详细信息,通过文件的ID调取IM的接口,下载文件传入文件沙箱,同时将文件沙箱的结果以IM的方式告知安全处置人员和受害人。

(3)威胁处置,安全人员收到来自SOAR的分析结果,则开始迅速响应,一般包括直接电话通知受害人,若受害人点击了威胁文件,则会触发自动化断网,和自动化隔离等操作。

(4)流程优化,对于经常收到IM投毒的客服人员或投顾人员,在进行社工安全的培训后可加入告警白名单,嵌入到整个自动化处置流程中,对于新增受害者则会重点关注,增加整个处置流程的效率。

总结

社会工程学的攻击虽然攻击手段、攻击途径多种多样,但是通过完善的安全防御体系,可以尽快发现并阻断其攻击,正如上文提到的防御体系,可以通过自动化的方式达到快速处理的目的。当然社会工程学的防御绝对不是孤立的,除上述的防御外,在日常安全运营中,我们也要和其他的防御系统有机的结合在一起,比如数据DLP、终端EDR、网络NTA、UEBA等设备,只有建立整体纵深的防御体系,才能保障我们日常运营的安全。

数据隔离与安全流转技术在异构终端上的应用探索

文｜甄明达、邬晓磊

东方证券股份有限公司

摘　要： 随着远程办公、移动办公等场景成为常态，基于互联网进行文件或数据传输给企业带来的安全风险正逐步显现。如何保障数据的收集、存储、加工、使用、流转等环节处于有效保护和合法利用的状态，成为企业安全的核心能力。本文从这个需求出发，结合当下企业内多类型终端异构的现状，进行数据隔离与数据安全流转的应用探索。

关键字： 数据隔离、零信任、安全流转、异构终端

研究背景

移动办公、远程办公、联合办公场景增多

随着5G、云计算、大数据、人工智能等新一代信息技术的快速发展，以及新冠疫情突发公共卫生事件的持续影响，国内移动办公需求显著提升，智能移动办公市场发展持续加速，再加上“智慧办公”等政府政策的支持，利用数字化信息技术进行移动办公、远程办公、联合办公已成为各大企业的共识。

虚拟桌面与终端沙箱

由于疫情期间存在较高的远程办公需求，虚拟桌面(VDI)的办公模式出现资源不足，扩容周期长，综合成本高等情况。为了在保持安全防护能力的情况下降低远程办公成本，我司引入终端沙箱模式以缓解VDI资源不足的情况。沙箱适配Windows，MacOS，信创OS等多类型终端，方便用户灵活使用。后疫情时代下，伴随着降本增效理念的推进，低成本的沙箱办公模式将可能覆盖更多的应用场景。

此外，VDI作为金融行业广泛使用的办公基础设施，在VDI的使用过程中员工的办公数据和VDI实例重度耦合，虽然实现了数据云端统一管理，但在整个运维过程中也发现了VDI数据备份依赖快照整个数据备份/恢复过程耗时长、无法提供文件级的个性化恢复的问题。当使用场景扩展至员工远程办公时出现了对于网络条件要求高、移动设备使用体验差等问题大大影响员工的办公效率。

数据存储缺乏安全属性

随着办公场景的多元化和安全管理边界的延伸，基于互联网进行文件传输的远程办公给企业带来的信息安全风险逐步暴露出来。

其中，最为明显的是，在传统办公场景中，由于设备单一、数据边界清晰、使用环境明确等因素，企业数据始终在可控的范围内流转。在移动和远程办公环境下，企业数据的载体已由传统的PC、笔记本转扩展到了智能移动设备、移动应用App上，企业数据的安全管理边界无限延伸。这种网络的泛化带来数据的全网全空间流动，传统的防御性安全手段难以奏效。

同时，在移动办公场景中，为确保业务运转，公司的客户资料、财务报表、研发材料甚至各部门的运营材料都可能需要在线上进行共享，由于缺少集中的数据管控措施，员工的复制和转发、移动设备的使用习惯不规范、移动设备丢失等行为均可能造成重要信息的泄露。

因此，数字时代，如何对企业数字资产进行安全管理，保障数据的收集、存储、加工、使用、流转等环节处于有效保护和合法利用的状态，成为企业经营的核心能力。

面临的问题

信创终端安全管控能力

随着信创终端在行业及券商的逐步推广，叠加远程办公等新型办公模式的引入，准入、DLP、防病毒等安全应用在信创设备的能力正在逐步补齐中。但整体上适配信创环境的安全能力，包括终端安全能力相较于传统架构还不够成熟，需要在实践中不断完善。

多终端场景的数据共享

传统模式下，数据存储在终端本地，即使同一用户多终端之间也无法很好进行数据共享使用，即使有企业网盘、共享存储等工具，使用体验也不佳，特别是在远程办公中，问题尤为明显。同时，多终端之间数据冗余的问题也会提升企业的数据存储成本。

多终端场景的数据管控

在传统办公模式下，企业数据以文件的形式储存在用户办公计算机中，文件和数据流动较少。这种场景下，企业对于文件和数据的管理相对容易。随着多终端办公、远程办公模式、私有设备办公等场景的引入，文件和数据势必会在同一用户或不同用户的多终端进行流转。在此背景下，有效的进行数据管控，防止数据和信息泄露，是比单终端场景更复杂更迫切的需求。

数据外泄溯源

员工个人设备通过VPN接入内网进行办公后，由于设备的多样性不可避免地会遇到如何应对终端设备截图、复制/粘贴、远程会议等数据外泄手段的问题，一但发生数据通过以上手段外泄如何对外泄数据进行溯源成为开放远程办公前需要解决的棘手问题。

解决方案

综上所述，随着信创终端投入使用、远程办公场景的扩展，传统的安全管理手段已经不能应对快速发展的多元复杂的办公场景。建设一套适应多类型终端（包括但不限于基于Windows终端，Windows VDI，MacOS终端，信创终端等）的办公安全基础平台，成为应对以上问题的一种有效方案。

基于内核级隔离打造可信沙箱容器

为了解决企业数据在终端上存储的问题，可采用操作系统内核级隔离技术打造了企业安全工作空间（可信沙箱容器）用来在终端上安全存储企业数据。操作系统提供了大量的驱动、服务、注册表（Windows）供应用系统使用，通过内核级沙箱对于这些启动、服务进行统一的虚拟、加固、隔离从而在终端上打造安全的数据隔离区和可信计算环境配合高性能SDP隧道，从而实现企业数据通过安全隧道传输至终端后存储于安全工作空间的加密虚拟磁盘内和本地文件系统完全隔离。

图1 可信沙箱容器架构

通过内核级隔离，存储于可信沙箱容器中的数据无法被容器外的app读取到、可信沙箱容器内部的应用如对磁盘进行写操作也会被可信沙箱容器重定向至可信沙箱容器专用的加密虚拟磁盘内进行保存通过整体的安全隔离保证企业数据在任意终端上不可被可信沙箱外的非授权应用读取到。通过在终端上严格的数据隔离，传统的复制/粘贴、截屏/录屏、蓝牙以及较新型的NFC近场通信、进程间通信、共享内存等手段均无法获取到可信沙箱容器内的企业数据保证企业数据在终端上的存储安全。

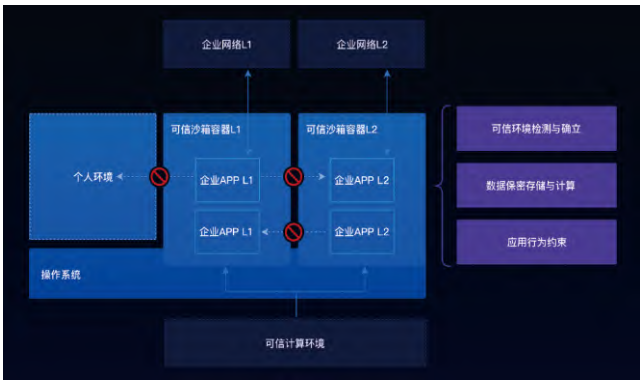


图2 可信沙箱容器数据保护模型

通过企业安全空间的打造在终端数据层保障了员工在配发的信创设备、个人设备上均可以安全存储企业数据。通过和零信任高性能安全隧道的融合，构建了支持远程办公的安全基础设施平台，支持员工安全远程办公。

建设细粒度网络访问控制

为了应对传统VPN权限与账号强关联无法判断根据终

端、网络、应用等环境状态控制访问权限的现状，基于软件定义边界的模型打造高性能接入隧道，实现了对远程接入时安全隧道的双向认证以及基于用户身份、设备风险情况、网络环境等多种客观环境构建自适应安全体系，对接入员工设备、网络风险进行持续性评估适时调整用户可访问的系统资源保证应用的访问安全。

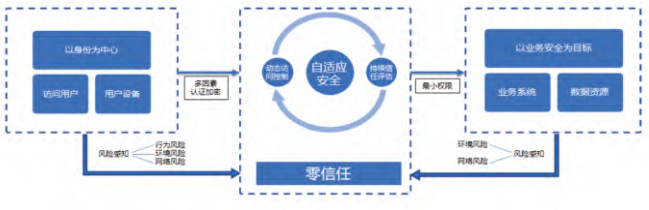


图3 零信任访问控制模型

通过高性能隧道的建设在网络接入层保障企业应用的安全访问，结合终端层企业安全工作空间、原数据中心安全基础设施构建了完整的“云-管-端”一体化远程安全办公平台在符合ZTNA（Zero Trust Network Access）标准的前提下额外构建了终端企业数据保护能力，保障员工远程办公场景下的企业数据安全。

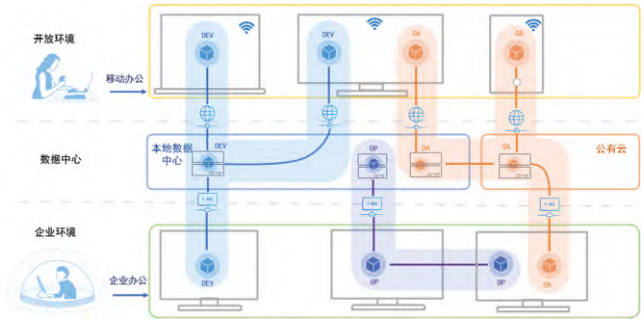


图4 “云-管-端”一体化数据保护模型

文件安全流转网关打造全终端员工数据湖

▶数据湖文件安全漫游

为了解决员工远程办公时利用各种智能设备安全、高效访问员工个人数据，采用新一代文件流转技术打造安全文件共享网关—Data+。Data+和安全工作空间客户端整合后分别为VDI、PC和智能移动设备提供专用客户端大大提高员工使用体验。

虚拟云桌面所有计算和数据均位于内网区域，安全文件流转网关客户端在云桌面自动登陆后客户端自动在VDI桌面挂载对应盘符的同时接管VDI常用的文件存储目录，例如Windows桌面的文档、下载、桌面；员工日常使用中对于文件的保存均通过文件网关同步至公司存储中，实现了类似Apple iCloud和微软OneDrive的效果。

信创设备、存量PC设备以及个人设备使用的安全工作空间客户端均整合Data+客户端保障员工从任意设备上登录均可以按需获取个人办公数据实现员工办公数据全终端安全漫游。

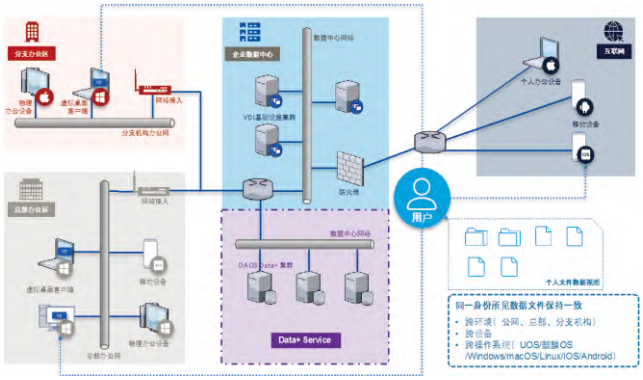


图5 全终端数据安全漫游模型

▶赋能VDI员工个人数据管理

同时Data+网关设计有非常灵活的备份机制，Data+可配置副本数量以及历史副本数，可以轻易做到文件级的数据恢复大大减轻员工数据恢复的复杂度和工作量。通过Data+网关的建设，建设了全终端一体化的员工数据安全同步机制并成功将VDI内的数据和用户实例进行解耦，在VDI进行快照备份时无须对员工数据进行备份大大减少了快照压力。

VDI纯快照备份方案						
VDI单用户快照容量（GB）	每集群快照数	单用户快照容量（TB）	用户数	快照总容量	文件存储容量（TB）	总容量（TB）
500	5	5	1000	5000	0	5000 *1
Data+融合VDI备份方案						
VDI单用户快照容量（GB）	每集群快照数	单用户快照容量（TB）	用户数	快照总容量	文件存储容量（TB）	总容量（TB）
30	5	0.3	1000	300	1410 *2	1710 *1

图6 1000用户每用户500GB容量备份对比

▶建立员工数据权限管控

员工通过管理存储于Data+的个人文件、数据的读写权限、分发范围、生存周期等权限；文件所有人配置分发范围后文件的接收人也不可超范围共享该文件。通过对源文件分发范围的管理，保障公司内的数据均可进行源头控制，保障数据不可被超范围使用。

通过Data+文件流转网关的建设，建立了完全私有化的“OneDrive”保障员工在任意时间任意地点安全、便捷地获取、使用、存储办公数据。

文件暗水印实现泄露溯源

随着信创办公设备、个人设备引入外加目前越来越频繁的线上会议，可通过规划建设安全智能暗水印能力对企业数据通过拍照、截屏、录屏等手段对外泄文件进行溯源。通过安全空间流转、外发、截图的文件均可调用水印网关自动加入暗水印，通过对泄漏文件暗水印的识别即可判断整个文件的流转过程以及最终泄漏人员。通过暗水印机制的建立，将使对于文件流转企业数据在信创终端、个人设备上的追述能力。通过对Data+归集的员工个人非结构化数据进行大数据分析，结合《证券期货业数据分类分级指引》和《证券期货业

数据安全管理与保护指引》的规范更好地对员工设备上的数据进行管理和保护。

总结与展望

随着信创设备、移动办公逐渐成为办公场景中的常态，传统的安全应用、安全手段逐渐暴露出无对应客户端、不适用于个人不同类型设备等新场景、新模式。通过打造企业安全工作空间为员工提供了全终端、全场景的安全办公服务基础设施平台，满足员工在任意网络区域、任意场景使用任意智能设备高效、安全办公的诉求。

通过企业安全工作空间的推广使用着力打造员工办公数据湖，通过数据湖的建设后续结合AI能力对数据文件进行分析、归类更进一步提高管理效率、办公效率。

证券行业零信任实践探索

文｜金文佳、朱毅、罗跃

国信证券股份有限公司

摘　要： 随着新型技术的发展，网络环境复杂度增加，传统VPN解决方案存在诸多弊端。零信任作为数字化转型战略的一部分，已上升到企业战略储备的阶段。本文依照证券行业网络特点，分析了所面临挑战、建设实践思路以及建设完成后对安全所带来的价值探讨，同时分享了整个建设过程中的经验和感受。

关键字： 零信任、面临挑战、建设思路、安全价值、建设经验

背景

近年来，“零信任”概念持续火热，随着国内外零信任相关标准规范、参考框架、成熟度模型的推出，零信任架构已经从概念走向了落地。各安全厂商都推出了零信任安全产品，从办公网零信任到生产网零信任，各大IT企业也广泛实践零信任安全架构，其已经上升到了企业战略储备的阶段。

所处的证券行业，长期以来发展出办公、生产两网物理隔离，总部与众多分支机构网络并存的网络基础架构。随着云计算、容器等新型技术的发展，各类公有云、私有云的实践落地进一步加深网络环境的复杂度。同时，深港两地国际化业务的开拓，更是引入跨境网络的X因素。在以上复杂的网络环境与用户群体中，如何实现用户高效安全的信息资源访问一直是重点课题。特别是疫情以来大量远程办公的新形势出现，越来越多的应用和数据需要交付给使用任意设备的员工或合作方。而传统VPN解决方案在访问便利性与安全性方面都存在着难以避免的缺陷。为满足办公与业务访问需求，在寻求提升访问接入安全性的同时，考虑架构可扩展性、易用性的改善，国信证券转型零信任架构，将零信任安全作为数字化转型战略的一部分，进行了大规模、多场景的零信任架构安全体系建设实践。本文就基于以上实践探索，提炼其中的行业共性要点予以分享。

建设挑战

实现零信任架构，需要打通现有的网络基础设施、基础服务平台、各安全资产，将各类应用层VPN替换为基于零信任架构的安全接入平台是其中的关键，往往也是第一步，会面临着诸多挑战。

用户规模大，业务连续性需保障

基于两网隔离的网络基础架构，不管是远程从互联网或是在公司办公网访问办公系统，普遍都需要接入VPN才能开展日常工作。访问的人员涉及总部员工、子公司员工、分支机构员工、外包人员等，接入用户基数大、身份多样、终端环境复杂、访问流量大。

在对VPN这条办公网络通道强依赖的现状下，新建零信任平台时如何做到网络平滑迁移、应用平滑过渡、业务无缝衔接，是一个非常大的挑战。一方面需要充分做好可用性设计，保障平台牢靠“可用”；另一方面也需要提升平台的易用性，让平台真正“好用”。

接入场景多，平台灵活性要求高

在员工接入场景方面，涉及远程办公、远程开发测试、远程运维、境外接入等多个业务场景，部分使用场景业务变化快，需要根据不同业务场景的接入特点，进行端到端的风险分析，对终端、身份、访问控制、应用转发模式、安全策略都进行相应的规则设计和调整，这是实现零信任安全的重要一环，其对平台配置管理的灵活性、时效性要求高。

个性化需求，大规模建设缺案例

为提升安全性和易用性，会衍生出适配企业实际环境的众多个性化需求，比如一站式接入多网络区域、单点登录集成、流量检测、安全处置联动等。很多个性化需求无法直接使

用成熟的零信任产品，需要与厂商有长期的产品打磨过程。在金融行业也缺少可直接参考的大规模建设案例，需要大量自主摸索设计，甚至试错。

建设思路

组织架构和IT基础设施的成熟度差异，决定了零信任架构安全体系的建设路径，在大规模、复杂接入场景中，难有“标准”的零信任建设方案。我们实践的建设思路，并不是把旧有的基础设施推倒重建，而是按照零信任架构的能力划分，充分利用现有网络、安全、身份基础设施，通过新建零信任平台进行基础设施的打通和能力联动，形成基于零信任架构的安全体系。

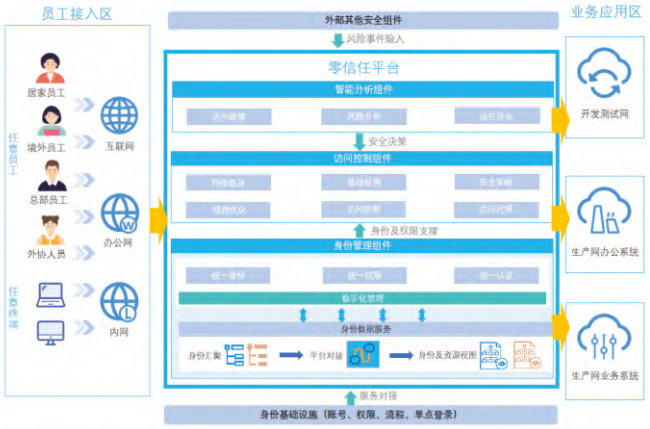


图1 零信任平台总体架构示例

如图示例所示，零信任平台为不同接入网络（互联网、办公网、内网）和不同业务网络（开发测试网、生产网）之间提供了跨网的业务安全访问通道。平台由身份管理、访问控制、智能分析三大组件构成。身份管理组件汇聚各类员工账号，完成权限管理、流程平台、单点登录等系统的对接，全面形成统一身份、统一权限的数字化管理能力，为员工提供统一认证的接入体验，是零信任平台的基石；访问控制组件为不同网络区域的业务应用进行服务隐藏、代理访问，对各类员工、终端进行全链路访问环节进行多层安全策略卡点和持续的访问控制，是零信任平台安全策略的落脚点；智能分析组件基于全链路日志，对身份、终端、应用访问进行可视化统计，同时收集外部风险事件进行关联分析，与安全运营体系联动进行风险响应处置，形成可扩展的安全能力。

价值探讨

安全的价值

零信任架构的建设对于我们的安全价值，首要体现在攻防对抗中。攻防对抗环境下，零信任仍然遵从经典安全建设的思路：纵深防御，持续监控。纵深防御措施包括：服务隐藏、终端基线、身份认证、访问控制；持续监控措施包括：终端环境采集、访问流量检测、UEBA分析。零信任架构带来以上安全机制的改变，不管对比根据网络地址ACL访问的内网环境，还是用户认证访问的VPN环境，都实现了安全的质变。在此，重点阐述可信进程（访问控制的一部分）、流量检测两个安全机制及其价值。

图2 零信任架构的安全价值

（1）可信进程

零信任平台接管并汇聚用户访问各类IT资源的通道，保障该通道的安全，成为攻防对抗的焦点。企图通过零信任通道进行内部网络攻击，首先需要突破的是零信任平台的服务隐藏，其次是身份认证。

可信进程的安全机制，就是用于在服务隐藏、身份认证都被突破后的攻防对抗场景。根据程序签名、进程名、进程文件hash等信息的组合建立可信进程白名单，使用白名单设置访问控制策略或者安全告警策略，对非白名单进程的网络访问进行阻拦或者告警。由此，可以保障通过零信任通道访问IT资源的发起进程都是安全可靠的。而网络攻击过程中的侦查跟踪、漏洞利用、命令控制阶段都必然使用大量专用渗透工具，这些工具尝试的网络连接都将被阻断并触发告警。

可信进程安全机制不但实时阻断渗透工具的网络连接，触发的安全告警也同时作为终端设备或者身份凭据被攻陷的线索，通过调查当前会话关联的设备信息、用户身份、访问记录，可以快速判断失陷情况，进行踢出会话、禁用设备、通知用户修改密码等有效处置。

可信进程其实是零信任“访问必经认证”理念的延续，其认证的是进程身份，使得攻击者即使拿到有效的零信任接入客户端、用户身份，也无法进一步进行渗透利用，甚至因此而暴露。

该安全机制的有效应用，实践关键包括：可信进程判定规

则、阻断或告警的处置选择。可信进程的判定规则，选择哪些进程属性、如何组合、松紧程度，都直接影响阻断的准确性、告警的有效率，另外规则的黑盒保密也能大大增强攻防对抗强度；阻断或告警的处置选择，直接阻断可以快速屏蔽安全风险，但是一旦误判会影响用户体验，只告警可以保护用户体验，但是从告警到定性处置期间会留有安全风险窗口。以上的这些选择都强依赖于实际应用环境，无法统一最佳实践。比如针对通用办公应用的访问，通信协议很纯粹，可信进程就可以制定得严格，只允许主流WEB浏览器访问，否则进行阻断；而对于测试环境的访问，访问资源与通信协议丰富多样，严格的可信进程判断与处置就可能难以为继。另外，多层次的信任等级以及不同资源区域差异化的信任与处置措施，能给可信进程安全机制更大的灵活度，提升实践效果。

(2)流量检测

在零信任平台里实现的流量检测，其安全监控能力可以等同理解为网络IDS，通过对零信任网络流量的直接检测，以特征匹配的规则去发现网络攻击行为与信息系统漏洞。核心能力本身仍是经典的安全技术能力，零信任平台将该能力整合，并提供施展能力的环境。

目前流量检测的应用场景多在互联网边界，而内网访问、VPN访问大多没有利用该安全能力。如此现状，一方面是“不为”，对网络位置、用户群体的信任，决策不为；另一方面是“不能为”，流量通道分散，不具备大量部署流量探针的条件，或者成本不允许，再加上无解的加密流量问题。而零信任打破对网络位置与用户身份的完全信任，本身又作为访问入口汇集所有信息资产的访问流量，同时还承担部分协议加解密的功能，为流量检测提供了有利的天然环境。

在我们零信任平台的安全监控中，流量检测是重要基础，其针对网络流量的特征匹配快速精准，与UEBA这种针对行为的模型匹配监控形成有层次的互补，辅之以终端环境采集能力，就能实现全面监控快速响应。

体验的价值

零信任平台带来安全架构变化的同时，也为我们带来了用户体验、管理灵活性上的提升。对员工，在从VPN切换到新的零信任平台后，不再需要多套账号多次认证，通过一次扫码即一站式接入，提升安全性的同时也大大提升了员工体验；对跨境访问，通过内置线路质量探测和选路的机制，保障了境外员工快速开展办公业务；对安全管理员来说，零信任平台将原来VPN分散的管理模式升级为统一管理，提升了管理效率，也降低了管理成本。

其他经验

如何保障可用性

由于零信任平台的建设，涉及到系统对接、定制开发、试用调整等，在根据业务场景、人员范围进行分阶段实施时，通常还伴随着新版本迭代、客户端升级、安全策略上线、应用发布调整等动作。在零信任与遗留VPN模式混合运行状态下，要保证业务连续性，在平台设计时就需要有技术手段来支撑分阶段的实施推广工作。而零信任平台作为统一接入的重要基础设施，也需要具备高级别的可用性保障。以下是我们大规模实施过程中总结的重点：

(1)所有配置需要支持灰度发布

▶配置的灰度：客户端升级、访问控制、安全检测、应用变更、操作系统等维度的策略配置，要做到能新旧配置并行运行，实时切换以及回退；

▶人员的灰度：可以按照人员、角色、用户组、部门、应用、网络等维度，进行灰度发布，稳定一段时间以后，再逐步扩大范围；

▶结果的灰度：对所有配置的执行结果，需要有多种方案，按照调测模式（不阻断业务）运行，通过相关数据评估策略是否符合预期，最后再正式启用，降低策略配置带来的可用性风险。

(2)统一管理

配置一站式统一管理，提升管理效率。零信任平台与网络基础架构、资源配置、安全管理等密切相关，部署和管理复杂性较高，我们在多个网络区域、部署了多套零信任接入节点，分别负责不同区域的业务代理。在管理上，所有区域的业务、策略都由统一的控制中心管理，并下发至指定网络区域的接入节点。

统一客户端版本，降低运维管理成本，提升问题解决效率。员工在境内外都需要通过零信任接入，涉及多条境内外运营商线路；在人员身份上，存在多套身份和双因素认证；同时要考虑客户端动态配置灾备数据中心，快速进行灾备切换。这些业务需求，都涉及客户端功能和配置逻辑，需要在设计时保证客户端功能的灵活性，从而保证版本的一致性，否则为不同场景交付不同客户端，不仅用户体验会变得糟糕，而且管理成本也会成倍增加。

(3)两地三中心

在高可用方面，进行零信任平台两地三中心部署的同时，也需要在零信任客户端的设计上考虑好诸如灾备线路发现变化、数据中心可用性检测、灾备切换时的用户引导等保障性功能，才能真正做好平台的高可用。

如何推广

零信任项目的实施最终将影响到企业大部分的员工，因此，得到普通员工的支持也是项目成功的关键。但实际上对于普通员工来讲，是没有动力主动从VPN切换到零信任客户端的。如何提升推广效率，我们提供两方面的思路：

（1）寻找提升用户体验的切入点

通过广泛收集VPN使用时员工反馈的易用性问题，在零信任的功能点中进行完善，比如我们通过将零信任客户端与单点登录的网页门户进行了对接，让员工从两次认证减少到一次认证。此功能就作为我们的推广切入点，让员工对新平台接受度更高，并吸引了不少员工自主安装推广，在内部收到了大量好评。

（2）利用内部宣传平台提高影响力

推广的过程，也是价值传递的过程。可以通过制作宣传视频、宣传海报、宣传手册、内部项目展演机会，进行多轮推广，增加平台曝光量，提升内部影响力，也让员工更好的理解平台价值。

另外还需要在平台功能上做好如人员覆盖度、客户端版本占比、策略命中率等数据，按照用户组、部门、终端等多维度进行数据汇总和展示，才能及时了解推广情况，保障推广目标的达成。

展望未来

零信任建设实践是一个持续演进的过程，替代原有的VPN访问通道是当前业内的主流切入点，未来进一步的拓展可以有三个明确的方向：接入场景、身份与权限、信任评估。

扩展更多的接入场景，完成人访问信息资源的全量覆盖。将零信任资源访问的安全保障能力迅速复制，同时统一各场景的访问体验与身份授权管理。比如原来在本地局域网通过网络ACL控制的内部访问通道，或者由于需要合作方协作而开放互联网访问的管理类应用，都可以通过接入零信任通道得到体验和安全的提升。

完善身份治理、权限管理等IAM能力。身份体系涉及认证与权限，特别是权限管理往往成为企业内部的顽疾，权限管理导致的用户体验糟糕、权限扩大、权限无法回收等问题屡见不鲜。零信任需要精准简约的权限管理，这就需要形成合理的身份体系与授权模型。

探索智能化的信任评估能力。零信任基础设施具有全访问链路的信息收集能力，利用收集的数据进行场景分析、建模，对访问的终端、账号、访问行为进行信任评估，以对传统安全能力进行多维补充。

技术前沿

07 安全架构

SASE架构下零信任技术落地和演进

文｜胡闽

杭州亿格云科技有限公司

摘　要： 本文结合安全技术发展的趋势以及数字化转型的业务驱动力，介绍了海外采用SASE架构落地零信任的缘由，通过分析海外领先厂商的零信任网络访问技术，并结合国内的情况，阐述了SASE架构下零信任技术如何落地和演进。

关键字： SASE、ZTNA、Fake DNS、身份认证、应用标记、终端拆流、传输协议、SD-WAN、安全网关、访问控制、应用隐身

概述

随着各行各业数字化转型的深入，大量企业积极采用云计算、大数据、物联网、移动互联网等新兴技术，促进IT建设不断向着“更好地连接客户”、“实现产业协同”、“提升生产效率”、“提高办公效率”等目标演进。在这样的背景下，业务系统变得越来越开放、IT 基础设施逐步混合云化、终端类型变得越来越多样、办公可以在任意位置进行。新技术带来新的生产力的同时，逐步瓦解了传统的物理网络安全边界，并且让开放协同、移动办公等新型办公场景成为常态。

新技术态势下的网络安全威胁和风险不断涌现、扩散，新办公场景叠加的安全风险也不容忽视。从外部威胁看，0day漏洞、社会工程学、APT等高级攻击手段层出不穷，黑客攻击手法也愈发专业化、隐蔽化，能轻松突破互联网边界进入内网，攻防对抗已经常态化；从内部威胁看，内部员工非授权访问业务系统，违规、有意的数据窃取，无意识的数据泄露等情况也愈演愈烈。

传统基于边界信任的网络安全模型在某种程度上假设或默认了内网的人和设备是值得信任的，认为安全就是构筑企业网络安全的护城河，因此将建设重点放在通过防火墙、WAF、IPS等边界安全产品/方案对企业网络边界进行重重防护。当黑客可以轻松突破互联网边界进入内网，当内部员工可以非授权访问业务系统获取到敏感数据，内网的人和设备都不再可信。传统基于边界信任模型的网络安全架构和解决方案已经难以满足数字化时代的安全防护需求，业务系统的网络安全及业务系统承载的数据安全都面临巨大的挑战。

零信任理念应运而生，秉持“永不信任、持续验证”的原则，重新构建访问控制的信任基础，确保身份可信、设备可信、应用可信和链路可信。

自从Google 2016年公开BeyondCorp之后，零信任从理念到落地迈出了一大步。

随后于2019年Gartner提出安全访问服务边缘（Secure Access Service Edge, SASE）的概念，这是一个基于云原生架构、融合网络和安全、分布式边缘覆盖、一体化安全集成、以身份为中心重构企业安全边界，适应数字化IT架构的全新安全体系。Gartner将零信任网络访问 (ZTNA) 作为SASE的核心组件之一，进一步的让所有企业相信并拥抱零信任。

在各行各业积极拥抱零信任理念的过程中，我们看到一个很有趣的现象，国内的绝大多数安全厂商都是基于传统点对点SDP架构落地零信任；而海外因为数字化和云化走的更快，几乎所有大型安全厂商都采用SASE/SSE落地零信任，这两年疫情催发的混合办公模式下的安全需求使得SASE/SSE在海外被迅速接受。统计数据显示，2022年《财富》500强公司中有超过40%（200多家）已采用SASE服务落地零信任；同时Gartner预估到2025年，70%实施基于客户端的零信任网络访问 (ZTNA) 的组织将为ZTNA选择安全服务边缘 (SSE) 提供商，而不是单独的ZTNA产品。

国际头部厂商之所以积极采用SASE/SSE来落地零信任，其核心出发点不是为了单单落地零信任网络访问，而是这样一套架构很容易支持安全一体化，可以解决传统办公安全碎片化的问题；同时安全网关支持分布式边缘部署，可以大幅度改善远程网络访问质量，提升用户体验，提高办公效率。

当前很多是以替换VPN 为切入点进行零信任网络访问（ZTNA）落地，但是实际上当零信任真正落地的时候，需要做到内外网完全一致的安全访问，这意味着所有的办公访问流量都要经过这张网络，这时候零信任网络访问（ZTNA）已经成为了办公基础设施，其工程化能力、零信任安全能力、端和网络稳定性、架构非侵入性、未来可拓展性等要素成为产品最核心的几个要素。

借助Gartner的报告，我们分析了Zscaler、Netskope等魔力象限领导者厂商、老牌厂商 Palo Alto Networks、初创公司Axis security、Twingate 几家，尝试来对这些海外零信任网络访问（ZTNA ）产品来进行技术还原，帮助企业的安全和IT负责人在做零信任内网访问技术选型时作一定的技术参考。

图1 2022 Gartner Magic Quadrant for Security Service Edge (Source: Gartner)

SASE架构下零信任技术落地

我们尝试从整个零信任网络访问（ZTNA）的流量路径来还原技术实现，如下图所示主要拆分为身份认证、应用标记、终端拆流、传输协议、云SD-WAN 网络、安全网关、访问控制、应用隐身这八个部分来进行技术分析。

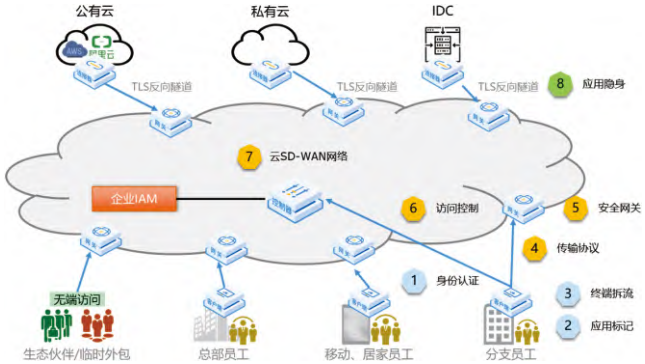


图2 SASE零信任网络访问架构

身份认证

一般而言SASE本身并不提供身份与访问管理功能，而是对接第三方的IAM系统来导入组织架构和身份信息，并进行身份认证。

也因此需要SASE支持各种各样的第三方身份源，比如Windows AD、Azure AD、LDAP等，在国内还需要支持大量企业在使用的钉钉、企微和飞书身份源。

身份认证使用的都是成熟技术，在此不展开讨论。

应用标记

零信任网络访问（ZTNA）相对VPN的一个主要变化是从过去的网络访问控制（Network Access Control）进化到应用访问控制（Application Access Control），而这个变化的关键点是如何在网络流量中区分出访问什么应用。VPN只能以IP来进行区分，其配置复杂度高，且在IP共享、网络重叠等场景不能精确标记应用。

我们调研的所有海外厂商，不管是Zscaler 还是Netskope、Axis Security都使用了Fake DNS技术来进行应用标记。技术原理其实还是比较简单的，提前保留一个大的私有网段（比如198.0.0.0/8），零信任客户端做DNS代理，在浏览器或APP 请求DNS的时候选择一个私有地址来进行标记返回，这样就构建了一个IP地址和域名的映射表，后续在TCP/IP报文中看到IP地址时，就可以根据映射表查询出请求的域名，并根据预设的策略进行流量转发。

以浏览器访问内网OA应用为例，其Fake DNS时序图如下图所示：

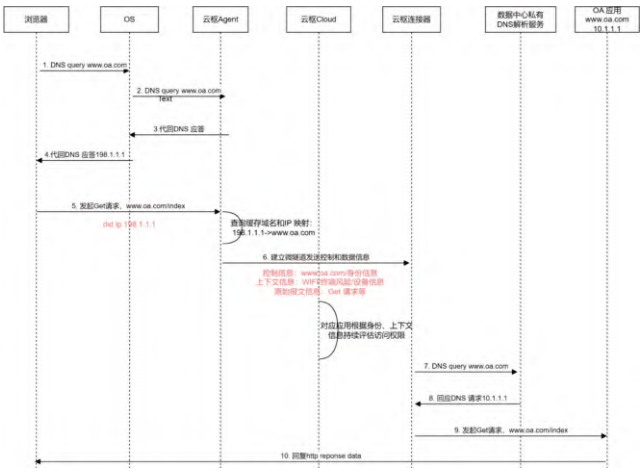


图3 Fake DNS 时序图

端上有两个本地代理，一个是DNS代理，一个是应用代理，DNS代理和控制器同步这个端有哪些应用权限，比如下发了*.oa.com，DNS代理一旦收到匹配这个泛域名的域名就会启动Fake DNS流程：

1、用户访问www.oa.com应用，首先会发起DNS请求报文；

2、DNS请求报文被DNS代理劫持进行虚假解析，直接返回一个198.1.1.1地址给到浏览器，同时记录下来www.oa.com 应用对应的IP地址是198.1.1.1；

3、浏览器认为198.1.1.1是www.oa.com 的真实地址，发送TCP 请求，TCP目的地址是198.1.1.1；

4、该报文被驱动劫持到应用代理，应用代理通过IP 198.1.1.1查询到实际访问的应用是www.oa.com；

5、应用代理封装隧道协议，协议控制报文里面携带这个流实际访问的应用是www.oa.com；

6、网关收到后，发现访问的应用是www.oa.com，经过相关应用访问控制策略，通过后转发到连接器；

7、连接器收到报文后，发现实际访问的应用是www.oa.com，这时候开始对DNS 真正进行解析，解析出目的地址是10.1.1.1；

8、连接器做代理转发报文到真实的应用。

使用Fake DNS进行应用标记的好处是显而易见的：

第一：简化应用配置。我们知道一个大型企业很难从一开始就梳理出公司的所有应用并且配置出精准访问控制策略。使用Fake DNS技术时，管理员可以在实施之初配置公司内网应用泛域名，从而把所有内网应用流量通过零信任网络转发，接着分析网络流量来自动发现和梳理应用，再根据用户访问应用的情况自动梳理访问权限基线并推荐访问控制策略，逐步达到零信任网络访问的效果。

第二：每个数据包过来的时候明确知道访问什么应用，配合专有传输协议和软件定义网络（SDN）技术可以做到网络零侵入（不需要改变原有DNS和路由）并实现多维动态访问控制，这部分可见后面的技术拆解。

终端拆流

如何将流量从端精细化的引流到云端，是整个零信任网络访问（ZTNA）的基础。VPN通常会创建一个虚拟网卡，通过默认路由将流量引流到虚拟网卡，进行隧道封装后发送给VPN服务器。为了缓解性能瓶颈并节省带宽，部分厂商支持了拆分隧道（Split tunneling），通常做法是通过下发精细路由只引流部分内网网段，控制粒度在IP网段粒度。基于路由模式的方案通常采用开源的TUN或TAP驱动，整体实现难度较低。

我们研究发现Gartner魔力象限头部的海外厂商并没有采用该方案，如Zscaler和Netskope都采用了基于Packet Filtering的引流方案。究其原因，是其对流量精细化拆分有了更高的要求，需要能精细化地控制哪些域名或端口走内网，哪些流量走互联网，甚至是哪些流量走加速链路。Packet Filtering方案通常采用NDIS或WFP过滤驱动获取用户流量，在过滤驱动层实现一套规则引擎，可以实现IP粒度、端口粒度、进程粒度拆流，配合Fake DNS，还可以实现域名和泛域名粒度的拆流。

采用基于Packet Filter方案的另一个优点是有更好的兼容性，因为其不在IP层同其他VPN客户端竞争，所以客户不会遇到路由冲突等兼容性问题。这在某些需要同时使用VPN和ZTNA方案场景下，可以给终端用户更好的网络体验。Packet Filtering方案实现难度相对路由模式要更高些，这也可能是初创公司没有广泛使用此方案的原因。

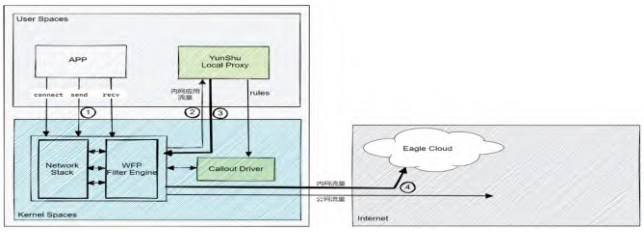


图4 包过滤方案原理图

基于WFP框架实现的网络过滤驱动，具备按规则进行流量拆分和流量重定向功能。用户配置的内网IP/端口/网段/域名/泛域名都会转换成协议+IP+端口的规则下发给WFP驱动模块，没有命中规则的流量会按照原路径继续转发，命中规则的内网流量，WFP驱动会将其重定向到本地监听的TCP/UDP端口。最终应用程序（如浏览器）仍会认为在同真正的应用服务器通信，实际上TCP/UDP连接已经被重定向到本地应用代理服务。

传输协议

过去许多 VPN 在 OSI 模型第 3 层（网络层）的 IPsec 协议上运行，该协议已经存在几十年，其设计之初的需求场景和今天的混合办公场景有了巨大的改变，当前很多VPN厂商或开发者也在进行协议的优化。而到了今天，零信任网络访问（ZTNA）最关键点就是传输协议需要是在应用程序层上运行，特别是QUIC/HTTP 3.0 的被广泛接受，UDP、多路复用等技术进一步使得应用协议兼具性能和灵活性。

我们分析了这几家海外厂商，发现在传输协议侧开始有了一定的技术区分，对于Zscaler、Netskope 这类新型领导者厂商，都是采用借鉴QUIC/HTTP 3.0的自研的应用传输协议，而 Palo Alto Networks 这类过去具备VPN 技术的厂商，我们看到的版本还是在延续过去的原有VPN 协议。

传输协议的作用一方面是提升网络的性能和稳定性，这块我们看到不管是wireguard 这类对VPN 优化的协议，还是基于QUIC 思路自研的应用传输协议对这块都有较好的提升。另一方面，零信任的有效实施依赖于对上下文信息的访问来进行精细访问控制，而这些上下文信息如果想做好实时的传递最好的方案就是通过自定义传输协议的控制报文进行传输，比如哪个进程发起的应用访问、在什么网络环境等，而这时候不管是传统VPN 协议还是wireguard新型VPN协议在灵活性上都相对比较弱。

云SD-WAN 网络

作为访问源与目的地之间的中间层，如何集成SD-WAN能力来对流量进行合理的调度？如何构建足够多的边缘节点。让流量以最小代价和最短的路径进行安全检测？如何将不同的安全能力灵活弹性的附加到离企业分支机构或者远程办公地点最近的PoP节点？以上是决定终端用户体验的重要因

素。

依托于AWS、Azure、GCP的云机房和一部分的自建数据中心，海外厂商构建了大量的POP节点，如Netskope宣称自己拥有50+ PoPs，Zscaler拥有150+ PoPs。同时各厂商也在整个网络的稳定性建设、延时优化、网络质量（DNS优化、远程传输加速、协议优化等）上做了大量工作，我们在海外场景测试其网络延时和丢包率后，得知相比于直接互联网访问或VPN访问有着明显的优势。从产品测试来看，基于云的SD-WAN 网络技术和端到端的加密技术在保证数据安全的前提下能较好的提升网络访问体验，这在混合办公场景下相对本地部署方案有一定的优势。

图5 Zscaler PoP分布

云SD-WAN网络就是构建在云厂商的虚拟网络之上，云厂商通过专线、CXP、多运营商联通等能力构建了一张全球的加速网络，我们在主要的云厂商上购买了标准的ECS + 网络互联服务，在其云虚拟网络等基础上构建了一张安全加速网络。

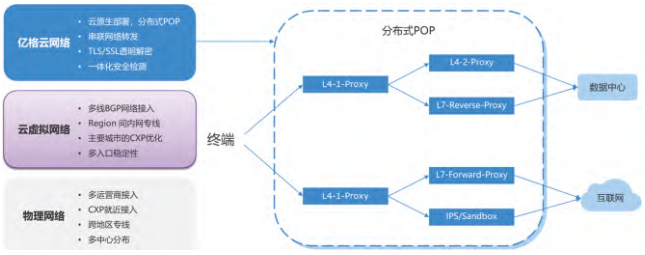


图6 云SD-WAN网络架构

安全网关是零信任网络访问（ZTNA）的核心组件之一，传统VPN 协议主要作用于4层，但是因为在传输协议层的瓶颈不能做到身份和应用上下文级别的访问控制，零信任网络访问（ZTNA）4层安全网关结合上述的Fake DNS 技术、自定义传输协议及身份认证等技术解决了应用访问上下文的信息传递和分析，可以做到基于身份和应用上下文的访问控制，这块基本能力的主要关键点其实在于Fake DNS和传输协议，不再深入阐述。

但是零信任网络访问（ZTNA）更进一步是需要加强在应用层的内容分析，基于应用内容的可视和可控得以在办公数据安全层面有技术创新来解决当前办公数据安全的一些痛点问题。我们分析了海外的相关公司，Netskope 是CASB 起家的所以其在SaaS 内网应用的访问控制侧有天然的技术积累，符合海外办公应用SaaS 化的趋势，但是其应用网关能力还在迭代中。Axis Security 作为初创公司一直在强调其在应用层的分析和控制能力，其开始之初构建的AgentLess 无端模式本身就是应用网关。Zscaler 目前在Agentless 应用网关场景，进一步了深入了应用安全能力，包括与WAF及欺骗防御的结合。

给人印象最深的其实是不管Zscaler 、Netskope、Axis security 一方面都在强化对应用的内容层面的分析和管控，CASB/SWG 不仅在互联网访问场景，同时在零信任网络访问（ZTNA ）场景也在不断的深化应用。另一方面部分厂商在架构的非侵入性上也有创新型演进，通过SDN 软件定义路由的能力结合 Fake DNS、自定义通信协议可以做到在不改变DNS（cname 模式）或路由的情况下实现7层应用安全网关透明转发，能透明解密HTTPS流量，该技术大大简化了零信任网络访问（ZTNA ）落地难度，可以做到对现有网络架构的零侵入，稳定性更好，这也是实施中最大的落地阻碍。

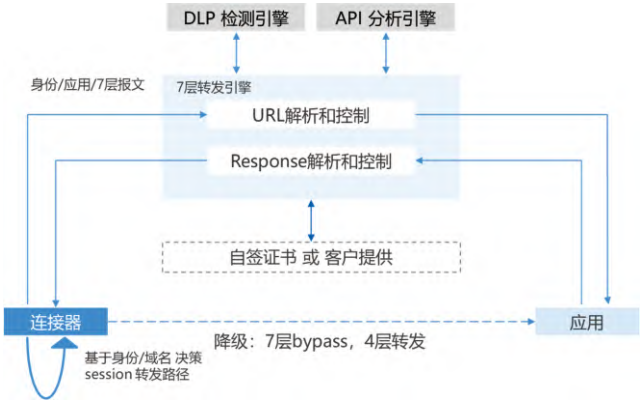


图7 对SDN 7层应用安全网关逻辑还原

访问控制

采用零信任网络访问替代VPN的核心原因之一就是能从基于网络的静态访问控制升级为基于身份和应用的多维动态访问控制。

零信任网络访问支持基于用户身份（组织架构、用户组、用户）、设备归属（例如公司设备、个人设备）、操作系统类型、网络区域（例如总部、分支或外部互联网）、终端安全风险、终端数据安全风险、访问时间及访问使用的应用程序等维度允许访问或禁止访问指定应用；进一步地可以支持对B/S应用进行7层URL级别精细化访问控制，决策条件包括用户、设备属性（公司设备、个人设备）、访问方式（有端访问、无端访问）、网络区域、应用URL，访问策略包括禁止访问、允许访问且允许下载文件、允许访问但禁止下载文件，降低高敏感资源被违规访问而导致的安全风险。

在零信任网络访问过程中，可以对终端进行动态评估、持续验证，当命中动态检测策略时，可以动态处置，以降低安全风险。

为了实现这样一个基于身份和应用的多维动态访问控制

机制，需要客户端、控制器、网关多个组件协同，如下图所示：

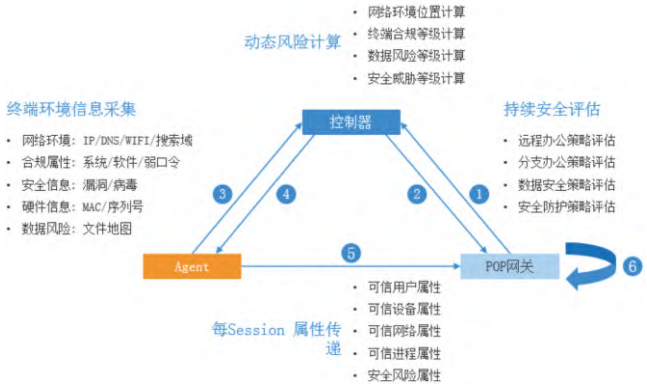


图8 零信任动态访问控制示意图

客户端需要实时采集终端环境信息，并且上报给控制器去计算风险，同时还要在每个会话的属性字段里传递这些设备上下文信息给网关，让网关基于控制器安全评估的结果来做动态的访问控制。

应用隐身

应用隐身是零信任网络访问（ZTNA）核心特性之一，零网络端口对外暴露在安全性上有很好的提高。不同于国内很多厂商在选择采用的SPA 单包敲门，海外几乎所有主流ZTNA厂商都选择了Connector反向连接的技术。该方案在企业内部部署一个轻量级Connector，通过反向TLS隧道的方式来连接安全网关。用户访问内网应用时，流量先经过高性能网关，再通过微隧道转发到Connector，Connector通过代理方式访问目标内网应用。由于连接是Connector主动发起的，因此Connector不需要在互联网上监听任何的端口，天然地实现了网络隐藏。

我们尝试分析了下海外和国内两种方案选择的背后原因，主要原因可能是因为海外云化进度更高，而国内可能本地化部署更多。但是再从技术上深度看一层，单包敲门方案还是相对比较复杂，NAT场景、UDP运营商限制、iptables性能限制都给其带来了性能和稳定性风险。而即使是本地化部署方案，轻量级Connector 会带来其他不同的技术优势，Connector方式由于不用开公网监听，且不需要变更内网路由，对企业已有网络拓扑、路由无任何变化，因此具备了极强的适应性。Connector除了连接企业内网和高性能网关之外，还可以进一步对流量进行安全监测和分析（如Connector可以通过SDN 技术结合七层应用网关实现WAF、API 安全、网络DLP等），企业可以根据应用的安全等级关联不同安全能力的Connector，在具备了高安全能力的同时，又可以灵活的有选择性的将一些视频、语音会议等大流量直接转发，避免了应用网关无谓的性能损耗。

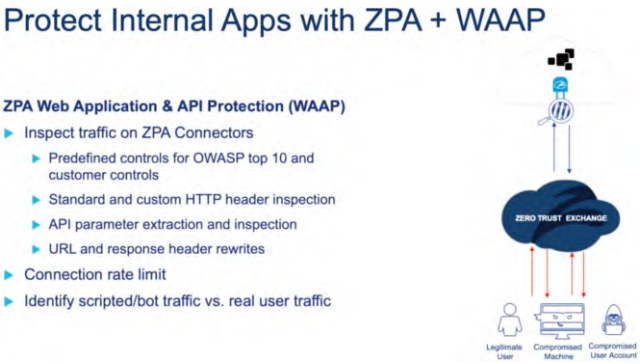


图9 Zscaler 发布的Connector 和 WAAP 的结合技术

SASE架构下零信任技术演进

如前所述，海外领先厂商普遍采用SASE架构落地零信任网络访问并不是单单为了零信任，核心目标其实是安全一体化，这里面零信任网络访问只是核心能力之一。

对于国际市场和中国市场，Gartner建议的SASE核心能力并不一样。

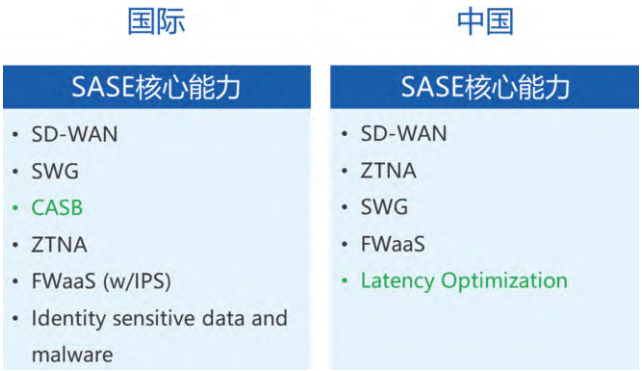


图10 Gartner建议的SASE核心能力

Gartner根据国际和国内不同的情况给出了自己的建议，比如CASB主要用于保护广泛使用的SaaS应用，如Microsoft 365、Salesforce等，但是由于国内SaaS并不成熟，因此在国内CASB也没有太多用武之地。

在我们的落地实践中，我们发现随着《数据安全法》、《个人信息保护法》等数据安全相关法律法规的发布，国内客户对数据防泄漏的需求非常强烈，同时我们也发现零信任结合传统的DLP技术之后，可以做到很多传统DLP做不到的功能和特性。

我们认为SASE架构下零信任技术的演进，将是以ZTNA作为SASE平台的基础功能，在此之上不断扩展新的安全能力，而这些新的安全能力绝不是孤零零的完全独立的安全能力，而是借助零信任网络访问技术实现所有安全能力全球策略统一管理、全场景安全水位一致、各安全能力联动联防的一体化安全效果。

总结

综前述所说，ZTNA在真正落地时将会承载所有的办公访问流量，并在每个员工的客户端上存在代理Agent，其已经变成了公司核心基础设施，这时候产品的工程化能力、零信任安全能力、端和网络稳定性、架构非侵入性、未来可拓展性等成为落地的核心关键要素。

我们希望通过有意义的技术交流，使得大家都认识到零信任产品不是仅仅依靠开源NGINX + OpenVPN 拼凑出来的，而是一个系统性的安全工程学设计和落地；而SASE也是落地零信任技术的最佳选择之一，尤其适合深度数字化转型、追求安全效果、办公效率和用户体验平衡的企业。

参考文献

1.Gartner 2022 Magic Quadrant for Security Service Edge

2.Gartner 2022 Strategic Roadmap for SASE Convergence

基于风险的安全架构研究与证券行业实践

文丨张晓兵

北京云科安信科技有限公司

摘　要： 数字资产是数字经济的基础生产资料，是社会发展的基石。数字资产是否安全，会从根本上影响数字经济发展的进程。证券行业，既是国家经济的排头兵，又是关键基础设施的核心单位，安全考量尤为重要。在这样的态势下，基于威胁的安全体系建设思想已经过时，未来需要基于风险来构建新的安全体系。

关键字： 数字经济、关健基础设施、风险驱动、风险模型、安全架构

概述

数字资产是数字经济的基础生产资料，是社会发展的基石。数字资产是否安全，会从根本上影响数字经济发展路径和结果。而数字资产最重要的属性是主权，在操作层面即为安全问题，安全能力的缺失会直接导致数字主权的瓦解。在数字主权维护范畴内，还有一个至关重要的概念：互联网化。美国是充分数字化的社会，但并没有充分互联网化；中国是充分互联网化的社会，但并没有充分数字化。互联网是风险的倍增器，互联网放大了中国由于安全能力不足导致的数字主权缺失的风险。

而对于证券行业来说，既是国家经济的排头兵，又是关键基础设施的核心单位，因此安全考量尤为重要。

在这样的态势下，基于威胁的安全体系建设思想已经过时，未来需要基于风险来构建新的安全体系。本文将从数字经济框架、风险评估、风险管理实践三个方面进行阐述。

数字经济框架下的安全再思考

数字经济发展现状

数字经济是以数字化的知识和信息作为关键生产要素，以数字技术为核心驱动力量，以现代信息网络为重要载体，通过数字技术与实体经济深度融合，不断提高经济社会的数字化、网络化、智能化水平，加速重构经济发展与治理模式的新型经济形态。具体包括四大部分：

一是数字产业化，即信息通信产业，具体包括电子信息制造业、电信业、软件和信息技术服务业、互联网行业等；**二是产业数字化，**即传统产业应用数字技术所带来的产出增加和效率提升部分，包括但不限于工业互联网、智能制造、车联网、平台经济等融合型新产业新模式新业态；**三是数字化治理，**包括但不限于多元治理，以“数字技术+治理”为典型特征的技管结合，以及数字化公共服务等；**四是数据价值化，**包括但不限于数据采集、数据标准、数据确权、数据标注、数据定价、数据交易、数据流转、数据保护等。

2022年，我国数字经济实现更高质量发展，进一步向做强、做优、做大的方向迈进，表现在：

一是数字经济进一步实现量的合理增长。2022 年，我国数字经济规模达到 50.2 万亿元，同比名义增长 10.3%，已连续 11 年显著高于同期 GDP 名义增速，数字经济占 GDP 比重达到 41.5%，这一比重相当于第二产业占国民经济的比重。

二是数字经济结构优化促进质的有效提升。2022 年，我国数字产业化规模达到 9.2 万亿元，产业数字化规模为 41 万亿元，占数字经济比重分别为 18.3%和 81.7%，数字经济的二八比例结构较为稳定。其中，三二一产数字经济渗透率分别为 44.7%、24.0%和 10.5%，同比分别提升 1.6、1.2 和 0.4 个百分点，二产渗透率增幅与三产渗透率增幅差距进一步缩小，形成服务业和工业数字化共同驱动发展格局。

三是数字经济全要素生产率进一步提升。总体看，我国数字经济全要素生产率从 2012 年的 1.66 上升至 2022 年的 1.75，数字经济生产率水平和同比增幅都显著高于整体国民经济生产效率，对国民经济生产效率提升起到支撑、拉动作用。分产业看，第一产业数字经济全要素生产率小幅上升，第二产业数字经济全要素生产率十年间整体呈现先升后降态势，第三产业数字经济全要素生产率大幅提升，成为驱动数字经济全要素生产率增长的关键力量。

四是数据生产要素价值进一步释放。数据产权、流通交易、收益分配、安全治理等基础制度加快建设，破解数据价值

释放过程中的系列难题。同时，数据要素市场建设进程加快，数据产业体系进一步健全，数据确权、定价、交易流通等市场化探索不断涌现。

数字经济框架下安全本质再思考

我们把安全单独拆出来看，可以大体划分为三个阶段：信息安全时代、网络安全时代和数字安全时代。

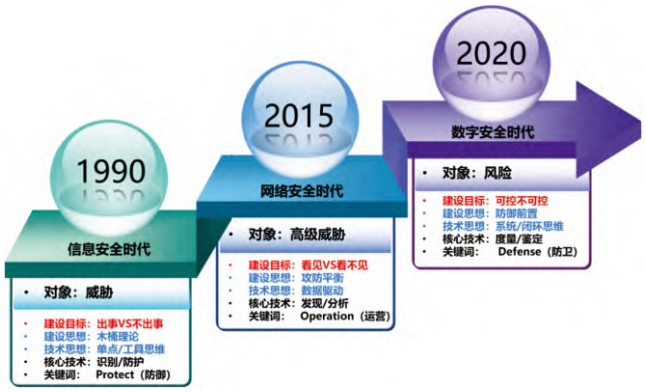


图1 安全发展的三个阶段

从1990年开始到2015年，这25年间我们可以把它称之为信息安全时代，这一时代主要的安全的对象就是“威胁”。这时候的整个的安全建设目标就是不出事，这个时代的建设思想就是木桶理论，技术思想就是单点和工具思维，所以这时候会出现各种反病毒、防火墙之类的产品，这时候的核心技术就是识别和防护技术，有一个关键词叫“protect”，翻译过来就是防御的意思。

从2015年到2020年这5年时间，我们把它称之为网络安全时代，这个时代的安全对象就是“高级威胁”，这个时候的建设目标就是以看见为主，建设思想就是攻防平衡，技术思想是数据驱动，即基于大数据技术来解决安全的问题，核心技术就是发现和分析技术。这时候有一个关键词叫“operation”，就是运营的意思。

从2020年到现在这几年，我们把它称之为数字安全时代，这个时代的主要核心的对象就从威胁变成了“风险”。这个时候的建设目标是可控。建设思想是基于防御前置的思想，技术思想就是用一种系统的和闭环的思维，核心技术就是度量和鉴定技术，这时候的关键词叫“defense”即防卫的意思。

在数字经济的框架下，我们要谈论的对象就要从原来的“威胁”变成“风险”。接下来，我们就要讲清楚威胁、风险、以及威胁与风险之间的关系。

威胁全景分析

虽然威胁最终都是由人产生的，但是我们对威胁本身特性进行研究，大致可以分成以下五类：恶意代码、黑客攻击、高级威胁、业务欺诈和内部威胁。

恶意代码 (Malware)	黑客攻击 (Hacker Attack)	高级威胁 (Advanced Threat)	业务欺诈 (Business Fraud)	内部威胁 (Internal Threat)
• 病毒 • 蠕虫 • 木马 • 后门 • 流氓软件 • 勒索软件	• 网站渗透（WEB） • 服务器入侵（二进制） • 黑产（挂马/暗链）	• 挖矿/流量木马 • 供应链攻击 • APT攻击	• 电信诈骗（2C） • 业务欺诈（2B）	• 渗透进来的攻击者 • 别有用心的内部人员
• 无目的性 • 终端安全	• 定向性 • 网关安全	• 高难度 • 大数据安全	• 经济性 • 应用安全	• 隐蔽性 • 身份/数据安全

图2 威胁分类

恶意代码就是我们常说的病毒，是一种由人编写的可以自动化感染和传播的程序，其中包括病毒、蠕虫、木马、后门、流氓软件、勒索软件等，它主要的特点就是无目的性。

第二种叫黑客攻击，就是我们常说的一些网站渗透的WEB攻击、服务器入侵的二进制攻击、黑产组织的挂马和暗链等，这类攻击的特点就是定向性。

第三种叫高级威胁，比如说我们常说的一些挖矿和流量木马、一些供应链攻击、APT攻击等，这类攻击的主要的特点就是高难度。

第四种叫业务欺诈，包括面向个人的电信诈骗和面向企业的业务欺诈，主要是从业务逻辑上进行一些攻击，它主要的特点就是经济性。

第五种叫内部威胁，包括一些渗透进来的攻击者和一些别有用心的内部员工，他们拥有更高的权限，这类威胁的主要的特点就是隐蔽性。

恶意代码防治主要依靠终端安全技术、黑客攻击防治主要依靠网关安全技术、高级威胁防治主要依靠大数据安全技术、业务欺诈防治主要依靠应用安全技术、内部威胁主要依靠身份/数据安全技术。

了解这些，能够为后面的行业实践提供有力的方案支撑。

威胁与风险的关系

我们接下来谈一谈威胁与风险的关系。

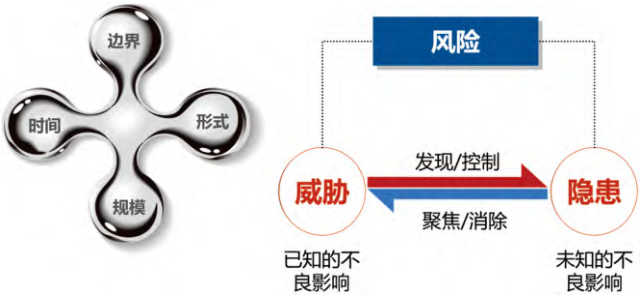


图3 威胁与风险关系

首先风险有四个不确定性。第一个就是它的边界不确定性、第二个就是它的时间不确定、第三个就是它的规模不确定、第四就是它的形式不确定。

我们可以把整个对企业的一些已知的不良的影响叫威胁，未知的不良影响叫隐患。我们主要做的事情就是要聚焦

威胁、控制隐患。

对于威胁，我们就是要采用各种相应的手段对威胁进行聚焦和消除，对于隐患，我们就是要发现它，并把它控制在可控的范围之内。

风险评估方法

风险是度量一个实体受到潜在环境或事件威胁的程度，它包含两个内容：一是已经发生的事件产生的不良影响；二是可能发生的事件所产生的潜在影响。

风险评估是识别、评估信息安全风险并确定其优先级的过程。评估风险需要仔细分析威胁和漏洞信息，以确定事件可能对组织产生不利影响的程度以及此类情况或事件发生的可能性。

下图为网络评估框架要素的关系模型：

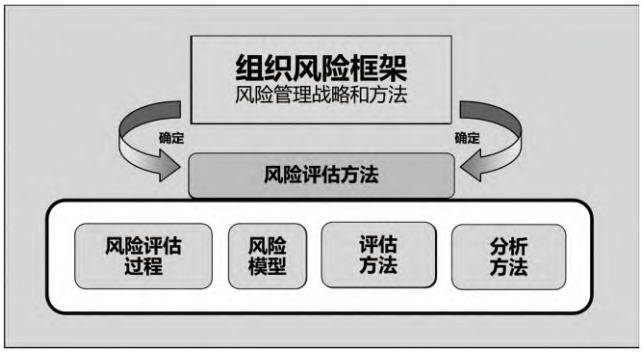


图4 风险评估框架要素关系

风险评估过程

整个风险评估过程分为四部分：风险框架、风险评估、风险响应与风险监测。

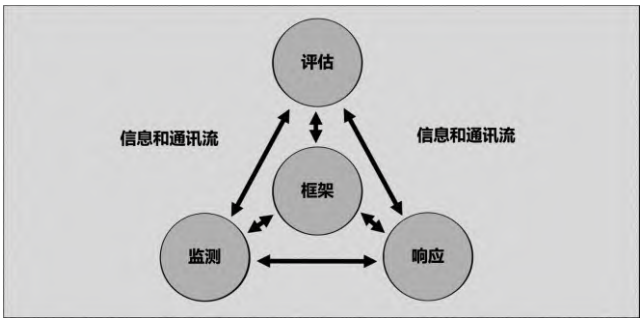


图5 风险评估过程

风险框架涉及组织如何界定风险或建立风险上下文，即描述基于风险的决策所处的环境。风险框架部分的目的是制定一项风险管理战略，解决组织打算如何评估风险、应对风险和监测风险的问题，使组织在做出投资和运营决策时，让风险感知边界清晰透明。

风险评估涉及组织如何在组织风险框架内评估风险。风险评估部分的目的是确定：一是对组织（即行动、资产或个人）的威胁或通过组织针对其他组织的威胁；二是组织内部和外部的脆弱性；三是考虑到利用漏洞进行威胁的可能性，可能发生的危害（即不利影响）；四是发生损害的可能性。最终结果是风险的确定（通常是伤害程度和伤害发生可能性的函数关系）。

风险响应是指一旦根据风险评估结果确定风险，组织如何应对风险。风险应对部分的目的是根据组织风险框架，在全组织范围内提供一致的风险应对措施：一是制定应对风险的替代行动方案；二是评估备选行动方案；三是确定符合组织风险承受能力的适当行动方案；四是根据选定的行动方案实施风险应对措施。

风险监测部分涉及组织如何随着时间的推移监控风险。风险监测部分的目的是：一是确定风险应对措施的持续有效性（与组织风险框架一致）；二是识别影响组织信息系统和系统运行环境的变化的风险；三是验证计划中的风险应对措施是否得到实施，以及为组织任务或业务目标制定的相关政策与标准、指导方针、操作流程等，是否满足可验证的信息安全要求。

风险模型

谈风险就要谈风险的关键要素，风险的关键要素就是威胁。威胁是指通过未经授权访问、销毁、披露或修改信息和拒绝服务，对组织运作和资产、个人、其他组织产生不利影响的任何情况或事件。

威胁事件是由威胁源引起的。威胁源的特征是：故意利用漏洞的意图和方法；意外利用漏洞的意图和方法。一般来说，威胁源的类型包括：恶意网络或物理攻击；操作实施的人为错误；组织控制资源（如硬件、软件、环境）的结构性故障；超出组织控制范围的自然和人为灾害、事故。

多个威胁源可能引发或导致同一威胁事件，例如，业务服务器可能因拒绝服务攻击、恶意系统管理员的故意行为、管理错误、硬件故障或电源故障而离线。

一个基于关键风险要素的通用风险模型如下图所示：

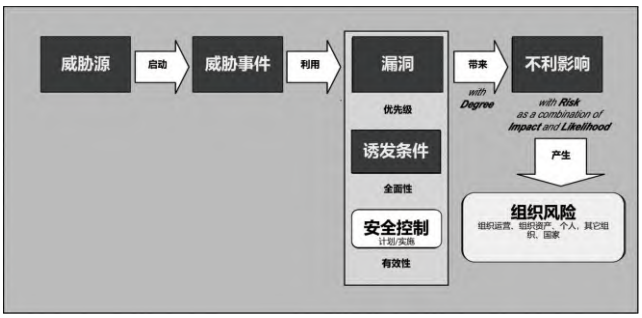


图6 基于关键风险要素的通用风险模型

在该模型框架中，有威胁源、威胁事件，漏洞、诱发条件、不利影响等5个关键要素。那么从威胁源启动产生威胁事件，然后利用漏洞，最终会带来不利的影响，从而产生组织风险。整个组织风险包括组织的运营、组织资产、个人、其他组织的风险。

要想规避企业风险，则要将企业的脆弱性通过优先级管理起来，然后全面发现诱发条件，最终才能产生有效的安全控制措施。该模型展示了整个组织的一个风险完整链条。

评估方法

风险及其影响因素可以通过多种方式进行评估，包括定量、定性或半定量。组织考虑的每种风险评估方法都有优点和缺点。可以根据组织业务需求，特别是根据组织对风险治理的态度选择首选方法。

定量评估通常采用一套基于数字逻辑的方法、原则来评估风险——其中值的含义和比例在评估上下文内外保持不变。这类评估能够有效地支持对风险对策或行动方针进行成本效益分析。然而，定量结果的含义可能并不总是明确的，可能需要解释，特别是解释评估结果的假设和约束。例如，组织通常会询问风险评估中获得的数字或结果是否可靠，或者所获得值的差异是否有意义。

此外，当主观决定被掺杂在定量评估中时，或者当值的确定存在重大不确定性时，量化的严谨性会大大降低。在某些情况下，定量评估的好处（就评估结果的严谨性、可重复性）可能被成本（就专家的时间和精力以及进行此类评估所需的工具）所抵消。

与定量评估相比，定性评估通常采用一套基于非数字类别或级别（例如，非常低、低、中、高、非常高）评估风险的方法、原则。这种类型的评估支持将风险结果显性传达给决策者。然而，在大多数情况下，定性评估中的数值范围相对较小，因此难以在报告的风险集合内确定相对优先次序或进行比较。此外，除非每个值都非常明确地定义或以有意义的例子为特征，否则依靠其个人经验的不同专家可能会产生明显不同的评估结果。通过注释评估值（例如，由于以下原因，该值很高）以及通过使用表格或其他明确定义的函数来组合定性值，可以提高定性评估的可重复性和再现性。

最后，半定量评估通常采用一套综合方法、原则来评估风险，半定量评估使用“区间值”和“量表”进行表达，其值和含义不需要其他的上下文。好处是可以同时提供定量和定性的评估结果。区间值（例如，0-15、16-35、36-70、71-85、86-100）或量表（例如，1-10）很容易转化为支持决策者可以理解的定性术语（例如，95分可以解释为非常高），同时还允许不同区间值中甚至同一区间值内的值之间的相对比较（例如，分别得分为70和71的风险之间的差异相对不明显，而得分为36和70的风险之间的差异相对明显等）。在决策过程中，该方法比纯粹的定量和定性评估都更好理解。此外，如果区间值组提供了足够的粒度，则结果之间的相对优先级比纯定性方法更加精准。与定量方法一样，当主观决定被掺杂在评估中时，或者当结果数值确定存在重大不确定性时，严谨性会大大降低。与在风险评估定性方法中使用的非数字类别或级别一样，每个区间值或量表范围都需要明确定义或用有意义的示例来表示。

分析方法

在风险评估起点、评估的详细程度以及如何处理类似威胁上下文导致的风险方面，分析方法有所不同。分析方法可以是：面向威胁、以资产/影响为导向或以脆弱性为导向。

面向威胁的办法从查明威胁来源和威胁事件开始，并侧重于发现威胁上下文;漏洞是在威胁的上下文中识别的，对于对抗性威胁，可以根据对手的意图识别影响。以资产/影响为导向的方法首先确定影响后果和关键资产，可以得出业务影响分析的结果，并识别可能导致这些影响的威胁源的威胁事件。

面向漏洞的方法从组织信息系统或系统运行环境中的一组诱发条件或可利用的漏洞开始，并确定可能造成这些漏洞的威胁事件以及漏洞的可能后果。每种分析方法都考虑到相同的风险因素，因此需要进行同一套风险评估活动，尽管顺序不同。风险评估起点的差异可能会使结果产生偏差，导致某些风险无法识别。因此，综合来看，用资产/影响分析方法补充面向漏洞的分析方法，可以提高分析的严谨性和有效性。

除了上述分析方法外，组织还可以应用更严格的分析技术（例如，基于图的分析）提供一种有效的方法来解释以下因素之间的多对多关系：威胁源和威胁事件（即单个威胁事件可能由多个威胁源引起，单个威胁源可能导致多个威胁事件）;威胁事件和漏洞（即单个威胁事件可以利用多个漏洞，单个漏洞可以被多个威胁事件利用）以及威胁事件和影响/资产（即单个威胁事件可能影响多个资产或具有多个影响，单个资产可能受到多个威胁事件的影响）。严格的分析方法还提供了一种办法，说明在评估风险的时间范围内，某一特定不利影响是否最多发生一次，或可能反复发生，这取决于影响的性质和各组织（包括业务程序或信息系统）如何从这种不利影响中恢复过来。

证券行业风险管理实践

证券行业面临的挑战

证券行业面临着外部网络新威胁、监管单位新要求、数字化转型新风险等三大挑战。

在外部网络新威胁方面，全球供应链攻击规模和影响不断升级;网络入侵事件与日俱增，高级可持续性攻击(APT攻击)呈多发态势;安全漏洞层出不穷，高危漏洞比例大幅增加，0day漏洞风险防不胜防。

在监管单位新要求方面，公安部、人民银行、银保监会等监管部门相继出台一系列网络安全监管制度；多家银行证券单位因违反相关条例被监管部门给予警告、罚款、责令整改等处罚；监管部门、各级政府部门纷纷组织开展攻防比赛、专项演练等专项工作。

在数字化转型新风险方面，一是新技术与银行业务的结合可能带来新风险（人工智能、物联网）；二是新技术应用带来新的安全问题（云计算、大数据）；三是新技术成为驱动网络安全防护数字化转型的重要组成部分（人工智能、区块链、量子计算）。

证券公司网络和信息安全三年提升计划

中国证券业协会，于2023年1月6日，颁布了“证券公司网络和信息安全三年提升计划（2023-2025）”

于1月6日开始向券商征求意见，指导2023年至2025年券商提升网络与信息安全工作的行动指南，券商可参照实施，并制定配套实施计划。鼓励有条件的公司2023-2025三个年度信息科技平均投入金额不少于上述三个年度平均净利润的8%或平均营业收入的6%。

从科技治理能力、科技投入机制、信息系统架构规划设计、研发测试效能与质量、系统运行保障能力和网络信息安全防护体系等六个方面明确提出提升方向和要求。并要求配备充足的信息科技和网络安全等专业人才，信息科技专业人员不低于公司员工总数的6%，网络和信息安全专业人员不低于信息科技专业人员的3%且不应少于4人。

在该计划中，提出了科技治理能力、科技投入机制、信息系统架构规划设计、系统研发测试管理能力、系统运行保障能力、网络和信息安全防护体系等六大方面的建设要求。

在科技治理能力方面，主要包括完善科技战略发展规划，健全科技治理架构，推动信息科技管理体系建设，增强合规风控内部审查，完善供应商管理机制等五方面具体要求。

在科技投入机制方面，主要包括加大科技资金投入，加强科技人才队伍建设等两方面具体要求。

在信息系统架构规划设计方面，主要包括建立及完善系统架构管理机制，建立及健全企业级应用架构，加强数据架构体系治理，推进技术架构转型升级，提高核心系统自主掌控能力等五方面具体要求。

在系统研发测试管理能力方面，主要包括建立及完善需求设计及分析机制，提升代码开发效率及安全，制定并落实信息系统代码审计规范，加强信息系统测试质量管控，提升第三方合作业务风险管控能力等五方面具体要求。

在系统运行保障能力方面，主要包括加强信息系统上下线管理，管控信息系统变更风险，提升信息系统故障发现能力，提高事件预警及处置效率，健全组织级应急响应管理机制，做好信息系统容量与性能管理，完善重要信息系统备份能力等七方面具体要求。

在网络和信息安全防护体系方面，主要包括深化漏洞全生命周期管控，提升安全攻击防控能力，加强网络安全态势感知和通报预警，加强数据安全管理体系建设，持续加强安全意识培训，做好安全全局性建设等八方面具体要求。

证券行业数字风险主动安全架构

为了应对日益增长的新的威胁和数字经济发展的要求，我们需要在证券行业里面去制定一个全新的安全架构以控制风险。

这个安全架构里必须考虑现在的一些安全建设基础和面向未来的一些新的安全构想，这样才能应对新兴的安全和新兴的威胁。

图7 数字经济主动安全架构

整个框架共分为数字世界风险防控体系、纵深防御体系、实战能力提升体系、系统运行保障体系、安全管理体系等五大部分的内容。

那么首先我们看到，中间的纵深防御体系里面，从下往上包括等级保护的要求、基础设施的安全、通信网络安全、计算环境安全、供应链安全、应用治理、和数据治理等七方面的内容。这方面内容主要是基于我们现在的等级保护条例和关键基础设施保护条例两个国家级的法律进行的设计。

实战能力提升体系主要是基于关基保护的最新要求，里面提出了攻击防控中心、安全运营中心、态势感知与通报预警中心等三大中心的设计。

最右边红色的部分是整个证券行业的安全管理体系，里面主要是一些制度保障的方面的内容，包括制度策略、管理人员、运维管理、检查评估、人才培养、建设管理、评估考核、监测预警等方面的内容。

系统运行保障体系主要是基于证券行业最新颁布的三年纲要里面提出的要求，里面包括统一告警平台的建设、一体化运维监控平台的建设、大数据智能化运维工具平台的建设、预案管理平台的建设、信息系统故障指挥与协同系统建设等。这五大平台的建设跟以往的平台建设不同，最大的变

化是将安全和IT相融合。

为了应对数字世界的风险我们还需要建立一个数字世界风险的管控体系，这里面主要包括数字风险测绘、互联网风险测绘、动态风险测绘、固定风险测绘、攻击者测绘、攻击面管理以及开源情报管理等。

通过这样五大方面的一个整体的安全架构，我们就可以把证券行业现在的安全建设以及面向未来的安全体系建设构成一个完整的安全体系，能够充分面对未来证券行业的安全新风险。

结论

随着数字经济的发展与安全新需求的出现，整个安全体系建设需要基于风险视角、行业视角、安全视角、IT建设视角进行综合考虑。传统的基于威胁构建安全体系的做法已经过。

因此，在数字经济的框架下，需要基于多个维度进行安全体系建设，并且需要兼顾行业的特性，本文中提出的“证券行业的数字风险主动安全架构”，能够以国家安全合规为准绳、以行业规划为框架、以风险为核，构建面向未来的数字经济框架下的新安全架构，对行业的安全发展，起到了很好的启发作用。

参考文献

1.中国信息通信研究院.中国数字经济发展研究报告(2023年).2023-04-27

2.NIST.NIST SP800-30 Rev.1.Guide for Conducting Risk Assessments（进行风险评估的指南）,2012-09-17

3.NIST.NIST SP800-39.Managing Information Security Risk: Organization, Mission, and Information System View（信息安全风险管理：组织、任务和信息系统视角）,2011-03-01

4.NIST.NIST SP800-37-r2.Risk Management Framework for Information Systems and Organizations（A System Life Cycle Approach for Security and Privacy）,2018-12

5.中国人民银行.中国人民银行关于印发《金融科技发展规划（2022-2025 年）》的通知

技术前沿

08 安全运营

攻与防视角下的安全运营技术探索

文｜尹振玺、杨昭华

北京长亭科技有限公司

摘　要： 网络安全中的实战攻防正在向更加无边界、无规则、无差别的方向演进。同时，随着网络环境、应用技术的更新迭代，如混合云、容器化、人工智能等的应用，网络攻击的途径、形式也在进化变得更敏捷、复杂、多态和智能，漏洞武器化速度也不断提速。在此般攻与防形式下，被动的护城河式防御模式已难以奏效，因此我们结合攻与防双重视角下进行安全运营技术的探索，寻找更高效的安全运营方法。

关键字： 网络安全、攻防技术、实战策略、安全运营

概述

无论是面对来自不法分子的安全威胁，还是实战攻防演练中自我安全运营能力的检验，从实战中积累了大量前沿经验，我们从攻击和防守的视角在实际安全建设工作中进行着安全运营技术探索。在本文将结合前沿的证券期货业安全运营建设及攻防实践，从分析攻击如何开展出发，阐述运营方如何利用攻击手法及技术提升自己的安全运营效果，再从安全运营实践阐述相应的防护建设技法落地。

常见攻击路径一窥究竟

对于大部分网络和信息安全从业人员来说，当在构建自身防护体系时，常会思考一个问题：“什么是攻防”？想要了解这个问题的答案，我们通过拆解攻击过程的主要阶段和分析三类常见的高危害入侵路径来一窥究竟。

无论是攻防演练还是真实的APT（高级持续性威胁）级别攻击团队，其攻击过程的主要阶段基本可归纳为如下过程：

图1 攻击过程的主要阶段拆解

这其中离不开三个核心要素

· 信息：实战攻防的第一生产力，贯穿攻击的整个生命周期，优秀的情报能力可以令准备和攻击事半功倍；

· 漏洞：撕开防线、扩大战果的重要武器，需要依靠信息进行精确制导；

· 工具：潜伏敌线、刺探情报的间谍：主要包括远控，搜集、密码窃取等前后渗透工具。

具体执行的过程包括如下步骤：

1.信息搜集：进行初始的入侵对象信息收集，并进行漏洞挖掘与储备；

2.初始入侵：通过前期收集的包括资产、漏洞、员工等信息，利用其中发现的薄弱环节突破防护边界；

3.站稳脚跟：突破边界后攻击者需能够长时间连接进内网才能进行下一步更深入的渗透，便会利用工具实现远程持续控制；

4.提升权限：初步突破边界往往拿到的是较初级的权限，其还要拿下更高级的权限才能看到更多可能的渗透路径；

5.内部信息收集：通过获取到的内网权限进一步搜集内网的系统和网络信息，寻找更多可利用的脆弱点；

6.横向移动：进而进行内部的横向渗透，拿下更多的主机或终端权限成为寻找最终目标的跳板；

7.流程循环：少量权限的获取常常不足以满足攻击者的“胃口”，其会在内网重复维持权限、提升权限、信息收集和横向移动的过程；

8.完成目标：最终找到既定的系统、主机或数据，达成攻击目的。

下面我们用3个实战的攻击路径进行详细解析来展现如上攻击过程的落地。

集约化管理系统一步到位

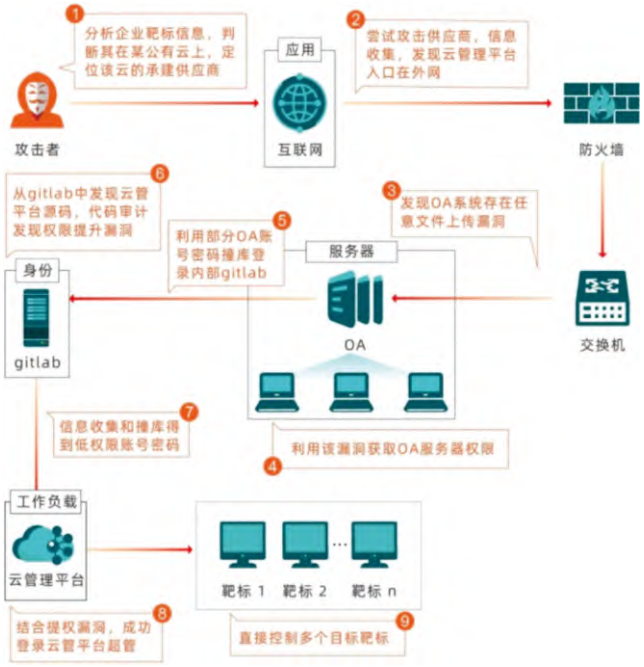


图2 HOTS技术架构图

如上图，攻击者在边界信息搜集中发现存在漏洞的OA系统，侵入后获取到云管理平台源码，经过代码审计发现的漏洞成功登录云管平台超级管理员账户，进而控制多个重要系统的服务器管理权限。

可以看到其中两个关键的集权系统，OA及云管平台，有着大量服务器信息和防护信息，一旦被攻破将导致大量敏感信息泄露或系统管理权限丢失，企业常见的类似系统还有堡垒机、域控制器、开发平台等。针对这些系统需要进行专项安全评估，包括已知、公开漏洞的检查，所在网络区域安全性，账号认证是否开启双因素等措施。

迂回渗透

如下图，攻击团队兵分两路：一支从正面突破进内网，但被企业发现后封锁了相应攻击路径；另一支迂回转向企业分、子公司系统脆弱点，成功进入到子公司内网，并摸索到与总公司核心区连通路径，最终成功进入总公司核心区域拿下重要系统权限。

可以看到，虽然很多企业在主要系统及网络的安全防护很充足，但却往往忽略掉一些周边网络区域的安全隐患。针对于此，需要做好网络架构安全分析，包括网络安全域划分、访问控制关系、攻击面评估、入侵防护评估等。

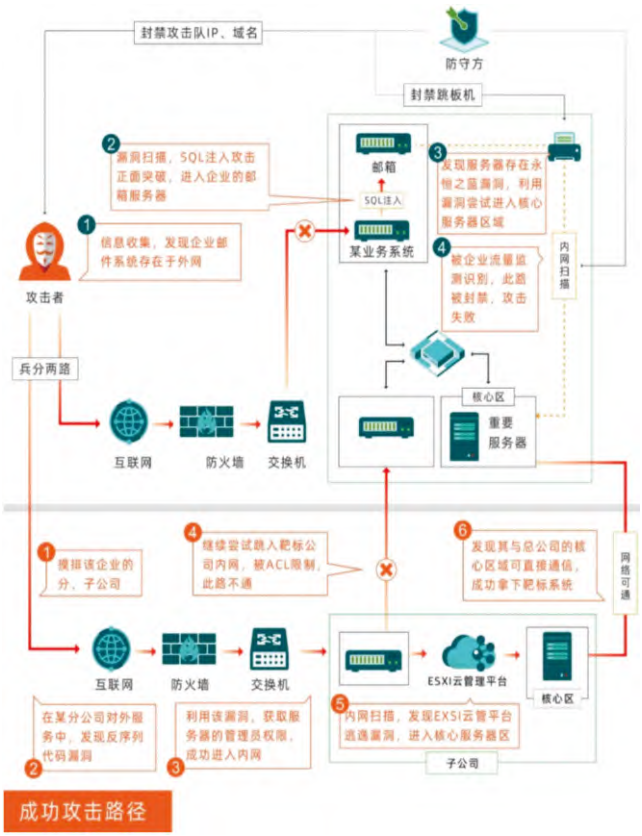


图3 迂回侧面找到有效攻击路径

网络或安全设备捷径

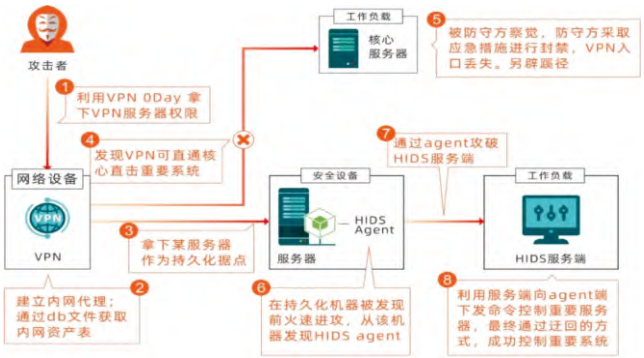


图4 通过网络或安全类设备实现批量控制

如上图，攻击者通过拿下VPN权限控制部分服务器，在被防守方应急响应后火速通过HIDS系统拿下其管理服务端进而控制重要系统。其中通过VPN和HIDS系统便捷地进入内网并迅速拿下权限。

针对此类网络或安全设备，需要针对其漏洞、安全机制、权限管控、弱口令、身份认证手段、自有的安全防护机制等进行针对性评估。

攻击手段提升运营效果

通过上面对入侵路径的示例解析，我们对实网攻击时的常见风险有了初步认识，下面我们系统性的分析近来较流行的攻击技战法，进而可借此思考对运营效果的提升。

五个攻击技战法解析

1.线上结合社工持续信息追踪

图5 线上搜索结合社工梳理目标信息

发起攻击前，尽可能多的搜集攻击目标信息，直击目标最脆弱的地方。

攻击者搜集关于目标组织的人员信息、组织架构、网络资产、技术框架及安全措施信息，为攻击决策提供支撑。搜集信息的种类包括但不限于分支机构、关联公司、外包公司、人员、网络、域名、帐户、邮箱等信息。

2.巧用漏洞和工具

基于攻击队伍的技术特长、擅长领域、漏洞储备、计算资源，以最快的速度找到目标的可入侵点。一般情况下，会先采用自动化工具进行第一波突破；若无果，再采用遍历攻击面的方式，逐个系统人工深入挖掘漏洞。

自动化工具是攻击者的倚天剑屠龙刀，可有效提升攻击效率，通过自动化工具结合人工操作来隐蔽行踪、攻其不备，持续进行信息搜集、扫描查点和漏洞利用工作。

3.利用网络或安全设备漏洞“擒王”

安全/运维/监控设备往往具备多系统的管理权限，这对攻击者寻找重要靶标系统无疑是绝对不会忽略的路径。此路径下大多从安全/运维管理设备的安全隐患入手，利用安全设备的漏洞进行攻击，且往往提前储备相关的0Day或1Day，供内网横纵向扩展；形式上常从Agent打到Server，再控制其他Agent的形式。

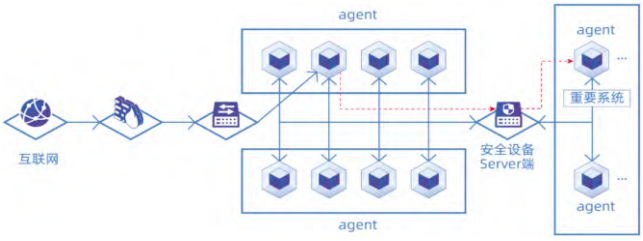


图6 从Agent控制Server，进而批量控制系统权限

4.供应链寻找切入点

随着企业系统越来越复杂、庞大，其供应链参与方及系统也相应增加，其中不难发现安全隐患作为入侵目标单位的跳板。寻找在供应链上的系统漏洞，大致为以下两类思路：

· 针对特定行业，常用特定软件或者系统进行一定储备和了解；

· 面对临时发现的第三方系统，可采取寻找源码，现场审计挖0Day的方式攻击。

5.社工欺骗

在众多社工攻击的手段中，钓鱼邮件是最为常见也最容易让人上钩的方式之一。最常见的社工手段有：

图7 常见的社工欺骗方式

实战攻防形式的检视方案落地实践

如上攻击技战法覆盖到了各类攻击场景，作为安全建设方，我们可以将“敌人”的手法/工具为己所用，在危险发生前自我进行检验，针对性的分析出运营工作的薄弱环节，提高“木桶”最短板。基于此思路，在某金融客户实践了基于攻击视角下的安全运营能力检视提升方案。

1.方案实践背景

某金融客户在大型攻防演练活动中参加防守工作，成为了攻击目标之一。然而此金融客户的安全体系建设历来以合规为基准，没有针对实战攻防进行过筹备，对防守保障的工作内容与流程缺乏清晰的思路，且演练前不足一月才着手准备，周期短、工作任务繁重。因此需要经验丰富、安全能力突出的厂商来协助开展防守准备工作，以应对高强度攻击态势。主要面对如下三方面挑战：

· 安全团队难以独立支撑重保整体工作：现有的应急响应流程无法满足实战场景需求，安全团队仅有4名人员，且大型攻防演练活动保障经验不足，难以在短时间独立推动整套实战防护方案落地。

· 内网缺乏流量安全检测手段：部分网络区域之间互相访问的业务流量和内网生产网流量缺乏相应的安全检测手段，无法检测异常行为，存在被攻击的风险。

· 安全日志无法集中管理分析：网络架构复杂，已部署的边界、内网和终端的各类安全产品数量较多，各类安全设备的告警日志无法集中管理和分析，安全体系也无法进行联动。

2.攻击视角落地战前准备

基于此，我们从攻击视角出发，在演练前进行多步准备工作：

1、资产梳理：明确资产属性，确定资产负责人，建立资产台账，确保漏洞排查修复及安全监测覆盖所有信息系统。发现近万个存活IP、1.5万以上开放端口，检测出数十个弱口令，并清理一百余个账号。

2、摸底评估：通过漏洞扫描、渗透测试和专项评估服务，发现系统存在的数十个高危漏洞和三百余个中低危漏洞，重点排查防护覆盖率和低成本攻击漏洞，并提供加固建议。

3、强化内网威胁检测能力：从攻防视角出发，对当前网络架构进行安全评估，梳理出3条此前未关注的攻击路径：

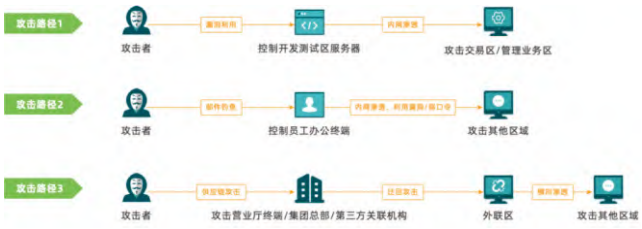


图8 梳理出3条攻击路径

基于以上对潜在攻击路径的分析，针对其安全技术体系的不足，制定针对性防御加固方案。

4、模拟演练：通过动态的攻防演练方式模拟实战场景，验证防护体系的有效性，针对发现的问题进行整改优化。

安全运营技法方案与实践

四个防守阻敌技法

攻击有其套路，防守方的运营工作同样也有其技术路线。在大量防护建设工作实践中结合对攻击的深刻理解整理了近来效果较显著的四个防守技战法：

1.常态化资产安全管理

资产是安全运营的基础支撑能力，合格的安全管理是建立在对于资产全面且精准掌握的基础之上，动态、周期性的资产监测以及及时的变更预警是非常必要的，保持对于资产部署分析、业务属性及应用上下游关系等清晰的认知，才能够将企业在互联网的暴露面进行持续收敛。

通过网络架构评估，明确整体网络安全域划分，梳理域间/域内访问控制关系，评估攻击面及入侵防护情况，最终实现网络隔离及攻击面收敛，则是对抗攻击的有效方式。

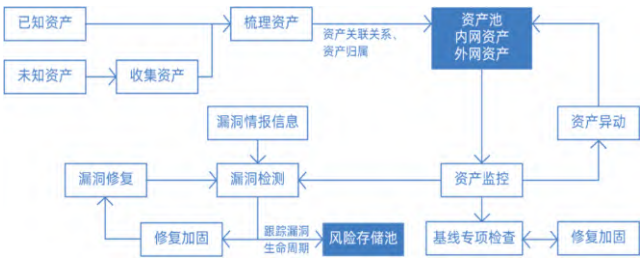


图9 常态化资产及风险收敛方式

2.内网威胁猎杀链

攻击者突破边界，进入内网后，将会有提权、横向移动等进一步操作，内网威胁需怎样捕获？

在攻防演练场景中，全流量分析、蜜罐和主机安全产品在常见攻击路径的关键节点上均能发挥重要作用，若三者能够联动打，可以实现“蜜-网-端”全面监测。

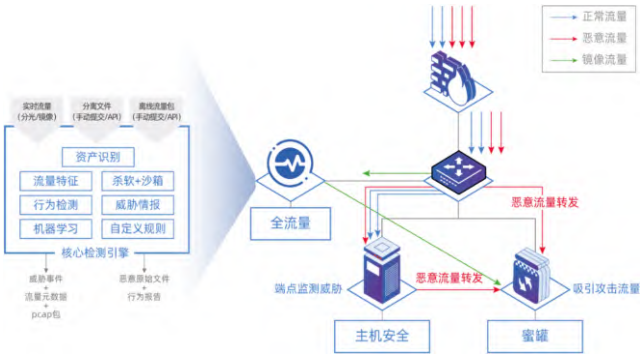


图10 内网“蜜-网-端”全面监测

3.自动化运营，以一敌百

自动化体系的搭建，通过将安全设备、日志管理设备等的日志进行汇总分析，并根据业务场景进行分析建模并对行为进行打分，联动防火墙/CDN等边界设备对问题IP进行秒级自动封禁，减轻人工分析成本，将有限的人员的注意力转移到更需要关注处理的事件中并降低响应时间。

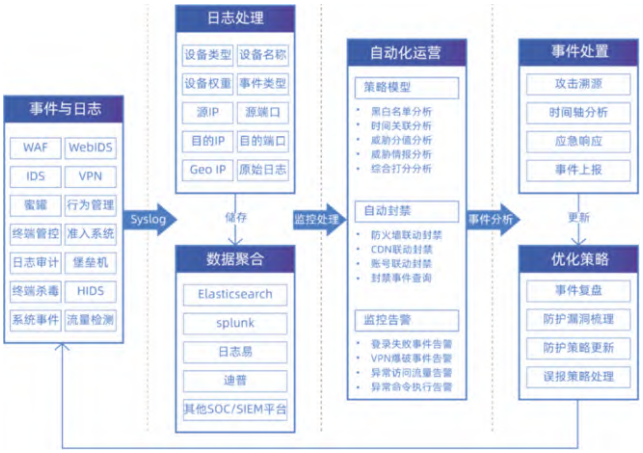


图11 日志自动化关联分析与处置流程搭建

4.扩大安全边界覆盖范围

边界防护是重中之重。多年攻防经验发现对边界防护的绕过仍大量存在，同时很多防守单位往往只将边界划分在企业网络出入口的位置，但向内对通信协议的不同层级没有对应的防护手段；向外对第三方、分子公司没有有效的管控措施。常见问题例如：

· 边界防护覆盖不全，如没有统一的流量入口、加密流量监控不到；

· 防护维度不够，高风险、重点资产防护不到位；

· 安全设备检测细粒度不够，没有贴合业务场景进行防护；

· 第三方、子公司、分支机构接入不设防。

在实战防护场景下，应将边界的防护范围扩大，筑牢边界防御体系，可采用如下措施：

图12 部分边界防护加强措施

安全运营建设实践

基于前述对攻击和防守的技战法分析，我们在某金融客户实践了检视提升方案后的安全运营建设工作。在进行网络架构与安全防护体系能力的综合评估后，发现当前安全能力体系仍然存在一些建设盲区，主要体现为以下两个方面：

(1)内网缺少流量检测能力：传统安全建设理念普遍认为，相比与互联网进行交互的外网系统，内网是安全的区域，因此在此前安全建设中，该金融客户并未部署流量监测设备，仅部署少量蜜罐和主机安全产品。而由于缺少对内网流量的监控，导致日常安全监测中，无法发现威胁在内网中的横向扩散行为，在应急响应处置中，也难以还原复现攻击过程，影响事件调查效率。

(2)安全设备碎片化，缺少统一管控平台：该金融客户在推进数字金融建设的同时，未曾忽视网络安全保障能力的同步提升，采购部署了包括防火墙、IPS、WAF等多台安全设备，形成了较为完善的边界防御体系。但设备众多、平台复杂、版本不一，分散的安全数据不仅对安全人员的分析能力要求极高，而且彼此告警之间难以验证，大大降低了威胁告警的可信度；且众多安全设备，依靠人工方式进行关联分析、协同处置，频繁的重复性工作，如IP封禁等占用运维人员宝贵精力；导致在面对高水平攻击防御时，无法切实有效的发挥安全设备和人员价值。

1.建设思路

通过分析该金融客户当前网络安全防护体系及实战防守要求，亟需快速完成内网流量检测和集中日志分析能力的提升，并通过简单流程的创建快速提升重复性工作的处置效率。

· 部署全流量监测设备，覆盖内网南北向的流量检测能力，补全纵深防御体系。

· 搭建安全分析管理平台，初步形成态势感知能力，为后续打造完整安全运营中心打下基础。

· 平台与服务相结合，保障、推动安全运营体系建设。

考虑到分析管理平台、全流量探针、以及众多安全设备构建形成的运营体系较为复杂，各类调优工作繁琐且专业性强。于是在平台建设的同时，通过引入安全服务支持的方式，针对性进行安全策略调优与模型调试工作，在确保产品发挥预期效果的同时，逐步推动安全运营体系建设。

2.建设落地

在该金融客户总部数据中心部署安全分析与管理平台和全流量分析预警系统，并在两个异地数据中心的关键节点各部署一台全流量探针。在完成设备部署后，将全流量探针、防火墙、WAF等安全设备的告警数据接入安全分析与管理平台，进行数据关联分析和告警聚合，并通过安全服务协助、平台定制优化等方式，初步建立IP自动化封禁流程。

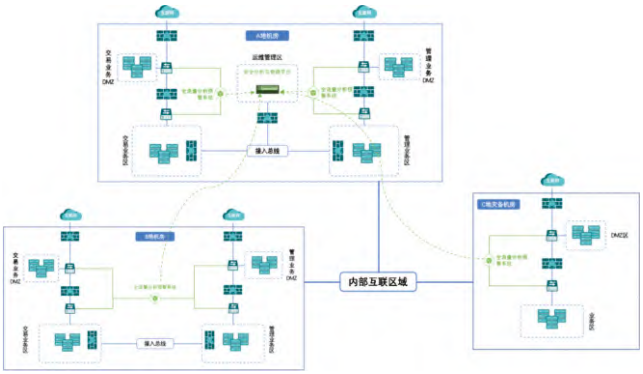


图13 整体建设部署示意图

加上攻击手段不断更新升级，传统方法存在检测能力不足，漏报误报严重的问题。基于深度学习预训练模型的攻击检测方法，深度理解攻击请求的上下文信息，从而提高攻击检测效率。

1.南北向流量检测：全流量探针采用旁路部署，接收网络关键节点的镜像流量，对流量中的网络会话和传输文件进行验证和分析，发现网络入侵行为，留存网络攻击行为数据，接入安全分析与管理平台并及时告警。补充威胁发现盲区，提升应急响应效率。

图14 全量接入流量实现攻击链关联分析

2.多源数据接入，形成安全数据中心：完成部署后，安全分析与管理平台接入各数据中心全流量探针的流量检测数据，以及防火墙、WAF等二十多台安全设备的日志告警等数据，对Syslog、FTP/SFTP、Kafka等方式采集来的数据进行泛化处理形成标准安全日志结构，便于集中展示与统一分析。

图15 多源数据进行事件聚合

3.大数据关联分析：基于标准化安全数据，利用安全分析与管理平台中的流式分析、离线周期分析等大数据分析引擎，通过可视化操作或SQL编程来定义分析模型进行告警数据的关联分析，贴合该金融客户业务模型个性化调整，输出高可信的风险告警。

图16 通过关联分析实现场景化能力

4.自动化处置：基于安全分析与管理平台的SOAR能力和丰富实战经验，在该金融客户通过设置多种封禁算法初步构建IP自动化封禁的剧本流程，解决值守期间人工封禁效率较低且存在空窗的问题，实现一定的自动化处置能力。

图17 自动化IP封禁流程

3.建设工作价值

通过前述方案落地动作，给该金融客户带来了如下的安全运营能力提升价值：

1.补充内网南北向流量检测能力，完成边-网-端纵深防御体系构建；

2.部署安全分析与管理平台，接入4大类20余台安全设备，显著提升安全数据信息的集中度；

3.基于平台大数据关联分析能力，可将日均约80万条的安全日志聚合为不到100条事件告警，有效提升告警可信度和处理效率；

4.初步构建IP自动化封禁等运营流程，协助在日常防守与实战眼里中自动封禁恶意IP，大幅降低安全运维压力。

总结

攻防实战下的实际安全运营能力正成为当下安全技术的演进方向，通过如上对攻和防两侧的技战法及实际落地经验分析，我们看到其中的两点在当前尤为关键，一个是对安全建设更精细化追求的度量方式，另一个则是云安全时代下的特点变化。

1.以攻量防

常说安全投入是无止境的，若要在安全预算和安全运营效果之间找到平衡，那么以攻击形式衡量安全防护效果形成风险覆盖率等指标，是最符合攻防根本的路线。以企业做安全防御的主要手段预防与检测响应为例，找到攻击威胁后再去应对缺乏前瞻性，应当实现安全风险防御的“步态左移”，需要量化步态与高频小跑来实现。这里涵盖了三个关键词：

· 转变：需转变防御思路，从传统事后防御转向“免疫式”的持续运营理念。安全能力、安全运营应强化日常运作，最好减少事后防御的动作，做到预防层面，以此达到降低风险覆盖率的效果。

· 高频：需进行高频且持续的安全指标监管，以降低风险暴露程度。面对复杂的资产情境、快速业务迭代和攻击面暴露，高频率和自动化的安全运营管理是有效应对多变攻击形式的必要手段。

· 量化：在攻击防御体系框架基础上，突出量化的指导、对比、迭代、进步。这包括对企业攻防能力成熟度的量化、交互式防御内在功力的量化、安全能力和运营能力的量化、安全运营健康度的量化等。

通过如上以攻量防、量化步态与高频小跑实践方法，推动安全防御向更高水平迈进。

2.云安全时代

上云，是无论证券期货行业还是其他金融行业企业都在讨论和探索的重点议题，混合云环境下的安全建设无疑是当下和未来网络安全工作的重点。随着企业数字化转型与业务上云的发展，会从单点能力的被动安全向纵深防御体系的主动安全演进。其中的网络安全建设变化会有如下特点：

1.基础架构将更加混合、异构和复杂；

2.随着业务向云上迁移，将有更多可利用的攻击路径；同时，攻击方式将更快、更频繁和自动化，复杂度和不可预测性也将进一步加剧；

3.安全将向一体化运营、云上托管的安全服务以及服务化按需调用等方向发展；

4.安全能力将融合于云基础设施和云产品组件之上，具备云原生的深度耦合、容器级的安全控制以及分布式和弹性高可用等原子化能力；

因此，我们需要开展更多的研究，以应对未来的安全挑战，同时探索新的安全防御策略和方法。

参考文献

1.长亭科技. 3条入侵路径详解，长亭防守实战经验打包. https://mp.weixin.qq.com/s/l5KCB_DjZaCzXqfQk_DdNw.

2.郭世超. 网络安全回归免疫疗法. https://mp.weixin.qq.com/s/DwFUZHGgndoxiz0UA3KE6Q.

3.长亭科技. 备战大型攻防演练，这一篇就够了. https://mp.weixin.qq.com/s/dWnm63hkmggpynrwyW4P7A

人机协同的智能安全运营时代

文｜傅奎

上海雾帜智能科技有限公司

摘　要： 我们已经进入了人机协同的智能安全运营时代，传统网络安全运营的很多方式、工具和理念将被被颠覆，安全人员必须尽快适应新的技术并思考如何用好新的技术。本文重点探讨的是，如何用好可编排的自动化技术（机器与机器）、基于大语言模型的AI能力（人与机器）和即将爆发的AR/VR技术（人与人），从而改变安全运营的现状，在未来的安全攻防战场为防守方赢得先机。同时我们也看到此类技术带来革命变化的同时，也引入了新的风险，值得我们思考。

关键字： 人工智能、ChatGPT、大语言模型、安全编排、自动化、SOAR、增强现实、虚拟现实、安全运营、人机协同

概述

在当前网络安全形势日益严峻的大环境下，各种多样化和快速演变的威胁正不断涌现。恶意攻击者正利用广泛应用的新兴技术，发起更高级别、更隐蔽的攻击，特别是针对企业的APT攻击、勒索软件和DDoS等手段层出不穷。随着物联网、云计算和移动互联网等技术的普及，攻击面急速扩大，导致企业面临的网络安全风险日益多样化。在这种情况下，企业不仅承受着巨大的安全防护压力，还需对各种技术风险和其他威胁作出迅速、有效的应对，通过整合技术、管理和人力资源来应对日益严重的网络威胁。

近来关于安全自动化、剧本编排、大语言模型、AR（增强现实）/VR（虚拟现实）等技术逐个涌现，不甘示弱的安全团队应主动拥抱新技术，改变思维方式，改进工作方法，提高工作质量，从而实现更加高水平和高质量的安全运营。以ChatGPT为代表的人工智能技术正在以惊人的速度发展，为无数行业带来了巨大的变革。可谓，我们已迈入了人与机器共同协作的新时代，如图1所示。在网络安全领域，我们同样已步入人与机器协同作战的智能安全运营时代。

图1：美军“自主协同作战飞机”（CCA）项项目

可编排的安全自动化加速系统联动

大中型企业每天需要面对成千上万的网络安全事件告警。现实情况是，安全团队的人员数量、技术水平和专业素养往往无法满足实时应对攻击的需求。在激烈的对抗和重重压力下，安全团队想要有效地开展安全运营，必须投入大量的时间、精力、资源和产品。团队成员的在岗状态、技术能力、操作熟练度、忠诚度，以及薪资成本、培训成本等都备受安全负责人、CISO甚至企业高层关注。

可编排的安全自动化的技术理念

过去，在面对相对较弱的攻击对抗中，企业可以通过增加人力和设备来解决问题，今天这种方式已不再适用。企业必须依靠自动化能力，特别是可编排的网络安全自动化，才能在面对海量事件告警和激烈的实战对抗中抢占先机。所谓的可编排安全自动化是指：将安全团队中个别专家的专业能力沉淀为固化的安全套路，然后将这些固化的套路转化为自动化方式，最后在自动化能力成熟的基础上实现可编程的安全自动化，如图2所示。

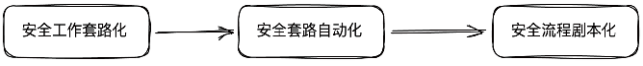


图2 可编排自动化的应用思维方式

换言之，安全团队成员只需关注安全事件运营的逻辑，而无需关注底层技术实践方法。在网络安全行业内，运用安全编排自动化能力通常是指SOAR（安全编排、自动化和响应）这一新兴技术，国内外已有相关的安全产品实现，并在实战过程中取得了良好的成果，如图2所示。

图3 n8n低代码平台实现的自动化编排

安全编排自动化的应用价值

安全运营实战场景下，往往因为人员不在岗、状态不佳、技能不足、系统不熟练等原因导致在实战过程中贻误战机。通过实战编排自动化安全能力，可以将安全团队中的专家经验沉淀成套路化的安全剧本，并且以自动化的方式进行执行，在下一次安全事件发生时可以重复开展高水平的应急处理。

当然，安全剧本编排不仅仅可以用于事件处理环节，在安全事件分析、上下文信息丰富、增强安全事件、调查安全取证计划、定时任务和自动报表统计等安全运营相关的各类环节都可以发挥作用。在实际运营过程中，可编排的安全自动化能够给企业客户带来的价值是显著的，包括：

· 放大安全能力：联动企业内部所有安全产品、网络设备、IT系统、SaaS服务，参与安全运营。激活所有安全能力——已购的安全产品再也不用因为无力运营而处于“吃灰”状态。

· 极速降本增效：实现分钟级秒级的事件响应，达到几十倍上百倍的效率提升。在单个事件平均处理时间缩短的同时，又提高了团队整体事件处理能力水平。单人单日可处理的安全事件数量可实现几十倍甚至上百倍的增长。

· 沉淀知识经验：利用可视化技术进行知识沉淀，将团队最高水平固化成标准套路和平均水平。即使人员更换，也无需担心代码不可读；图形化的剧本利于阅读和传承，本身就是知识经验。

· 提升运营水平：机器不会生病，也无需请假，支持7x24小时全天候运营，给不要说“996”。编排自动化有效降低了安全运营对人的过度依赖，将安全团队的运营水平始终保持在相对较高的水准上。

应对自动化要做的准备

可编排的安全自动化势必会全面改善安全团队的运营效率和水平。然而，在实践场景中充分落地自动化能力之前，还需要做好大量基础准备工作，包括：

· 提供可供编排的基础能力：完成网络安全基础能力的建设，为编排系统提供可调度的能力，例如防火墙、防病毒、SIEM、HIDS等产品。

· 形成较为标准的SOP：安全自动化就是将原本人工参与的SOP升级为自动化执行的剧本。这需要企业在安全场景运营过程中积累标准SOP。

· 改变思维方式和工作方式：将自动化理念深入到日常安全运营过程中，凡是人工做过两遍以上的工作，都可以考虑使用自动化方式去实现。

· 持续运营和积累：对已经剧本化的安全运营流程进行跟踪和优化，对未纳入自动化的工作场景进行思考，进行整体或部分地自动化尝试，逐步加大自动化覆盖的范围。

实现网络安全事件运营的全面自动化任重道远。国内主流安全产品在标准化和自动化方面尚有诸多不足，这要求安全编排自动化厂商支持更多基础安全产品能力，提炼更多安全剧本场景应用模板。同时，也需要市场上主流安全产品厂商提供更加开放的API接口和通讯协议，以便在未来为安全团队构建更加丰富的安全剧本提供技术支持。

大语言模型的AI能力重塑人机交互

过去几个月，ChatGPT领衔的"大语言模型（Large Language Model）"，让人工智能算法在全球范围内掀起波澜壮阔的关注浪潮。身处网络安全攻防战场的安全运营者们，绝不会错过这场狂欢，必须尽快搭上新技术的快车。技术本身介绍就不在这里赘述了，近半年关于ChatGPT的文章已经数不生数。

安全运营的日常工作涉及到人与人、人与机器的交互协作，存在众多痛点需求，现有技术手段难以让人满意。而ChatGPT这样的人工智能技术正好可以为我们带来改善和补充。

例说大模型处理非结构化数据

处理非结构化数据是安全团队日常工作中重要而阻力重重的课题，往往需要投入大量人力资源和时间成本，而人工处理质量却难以令人满意。诸如：批量处理一组杂乱无章的文本、在纷繁的文本中捕捉有价值的信息字段、对描述含糊的文本内容进行格式化输出等问题。而这些正是大语言模型的看家本领。

以ChatGPT为例，它能支持用自然语言描述的需求和文本作为输入，然后依据用户的意图快速、高质量地完成数据结构化处理。例如，把一组安全日志的原始数据交给ChatGPT进行格式化输出指定字段信息，就能得到一个可供下一个应用或系统直接使用的JSON结构。这样的过程不需要使用者具备任何编程能力，也不必手动逐个提取，如图4所示。

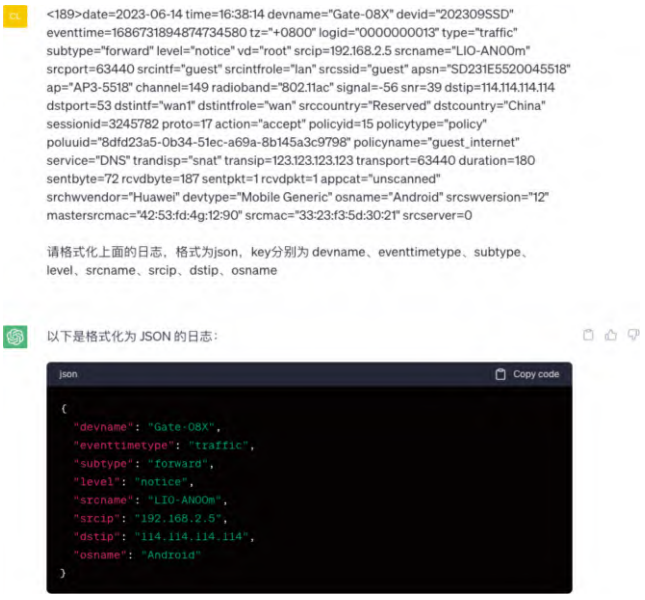


图4 通过ChatGPT对大段日志文本进行结构化输出

近乎完美的输出和几乎零等待的延迟，这样的人机交互，是过去几十年无数人类工程师梦寐以求的。接下来，它必将改变传统安全团队的工作方式和工作效率！

大模型在安全运营中的应用潜力

非结构化数据处理仅仅是大语言模型AI之花初绽的一瓣。实际上，在安全事件分析、威胁情报解读、安全事件响应策略制定、安全报告编写等环节，大模型都能协助现今的安全团队展开更为高效的安全运营。

· 弥补人类工程师的不足和优化工作流程：人工智能凭借着强大的处理能力，弥补人类工程师在处理大量复杂数据时容易出现的盲区。运用大语言模型，非结构化数据可被转化为结构化数据，简化分析过程，提升工作流程效率。

· 专业化文本输出：通过大模型对安全人员的调查报告进行重新编写和润色，可以快速将职场新手的报告提升到专家水准。

· 丰富的联想能力：经过海量数据积累的大模型，大模型掌握了全球范围内众多领域的最全面、最专业的素材，阅读了历史上发表过的几乎所有论文和专利。因此，在安全运营工作中，大模型能为网络安全工程师提供丰富的想象力支持，助力对抗恶意攻击。

· 自动化编程能力：安全和运维工作离不开Python、Go和Shell等编程语言。工程师为一个临时需求写代码往往伤透脑筋。而现在，提交给ChatGPT这样的大模型就能瞬间完成基础代码编写，稍加调整即可投入使用，大大减轻工作负担，提升工作质量和效率。

· 网络安全分析和决策支持中的智囊：通过使用大语言模型，安全团队可以更好地进行攻击模式分析、预测威胁走势，从而优化决策。针对已发生的安全事件，大模型可根据掌握的信息提出安全事件分析思路、应急响应流程和安全加固策略，减少对专家人员的过度依赖，毕竟这样的人才太稀缺！

AR/VR技术促进人与人之间的协同

VR/AR重新回到人们的视野——苹果公司近期发布的VR眼镜Apple Vision Pro，预示着VR/AR技术将对整个行业产生深远的影响。VR/AR技术也将为网络安全团队提供新的发展机遇，有望改善安全运营的效率和体验。

沉浸式安全互动与培训

主流的安全培训都是通过企业员工自学网络视频的方式完成。做得好一点的企业会组织人员线下集中培训。但未来大规模的线下人员聚集的机会会越来越少，在这样的背景下，通过AR/VR的方式开展安全人员培训则更容易产生好的效果。

借助AR/VR技术，人们可以跨过时空的界限聚集在一起参加集中的培训，并且通过高度可视化、动态和炫酷的效果，让网络安全培训更加直观、真实和有趣，以更好的效果提高人们对于网络安全风险的认知和理解度，便于他们更好地掌握安全技能和知识。

无边界的办公桌面

众所周知，办公场所最大的资源限制是“显示屏”，尤其是对那些要并行处理大量事务的一线人员来说，好的工作区展示能够大幅提升工作效率和工作心情。然而受限于物理空间，企业采购成本等等，现实办公区域内很难满足从业人员的这类需求。

随着AR/VR技术的逐步成熟，以及相关配套软件的丰富和成本的降低，人们已经看到了在物理空间拓展更多工作区的梦想即将实现。未来人们再不用担心桌面不够大，窗口被遮挡，工作不方便这样的问题了，如图5所示。

图5 以色列初创公司Sightful推出世界首台AR笔记本电脑——Spacetop

除了解决单人多桌面这一需求，使用者还可以随时和协

作的一个或多个远程同事共享办公桌面，共同查看文档，而无须像以前一样围在显示器边上。无边界的办公桌面将逐步成为IT及安全人员办公的必备利器。

不一样的应急演练和安全“会诊”

实战安全运营的应急响应中人们很难完美的期待团队成员人人在岗在线。每个工程师面前都会有几台电脑、几个桌面、不同的软件和菜单，很难完成便捷高效的信息分享和同步。

采用VR/AR技术可以极大地提高人机交互的效率，降低认知负担，改善体验。安全团队可以实现跨越时空的协作和无边界的办公桌面，甚至直接接管键盘鼠标。沉浸式的应急演练和实战协作，可以帮助团队成员更良好地互动，更深刻地理解安全。在办公室、家中、旅途中的所有人员可以像以往一样直接“面对面”开会，共同参与应急演练或者针对安全事件进行“会诊”，工作效率和质量大幅提高，完全颠覆传统安全团队协作方式。

跨越时空的安全服务

“术业有专攻，人力有极限”。今天稍具规模的甲方企业在安全产品或服务的采购合同中都有明确的针对乙方的应急响应服务SLA协议，例如我们经常提到所谓的“1小时或4小时到达现场”。实战攻防分秒必争，时间极其宝贵。未来人们完全可以减少甚至避免“人员奔赴”这个环节，安全专家可直接通过虚拟现实技术“现场”参与客户现场事件响应，提供专业技术支援。企业内部工程师可以和安全专家零距离沟通，在虚拟空间共享工作内容，从而跨越时空享受“专家上门”的安全服务。

总之，AR/VR技术对于网络安全领域来说是一种全新的变革和机遇。未来，人们可以利用这一技术手段，建立全息化的安全运营中心，实现实时响应和场景模拟，加强安全从业人员的沟通协作和技能培养。

新技术引入所带来的风险

虽然新技术在安全运营领域带来了诸多优势，但企业或政府机构引入新技术的同时也会给自身安全带来更大的风险和挑战；毕竟新兴的技术并不是完全成熟的，还可能存在一定的技术缺陷或难以适应快速变化的安全需求。

自动化的脆弱性与反自动化

自动化是一把双刃剑，它能加速安全事件响应并提升安全运营效率，但也存在一定的潜在风险。错误的输入信息可能导致自动化系统执行错误策略，软件Bug可能导致自动化流程失效，而过度依赖自动化可能导致人工操作水平下降。针对这些挑战，安全团队需要在使用创新技术的同时，通过设计合理的防御机制来降低风险，例如：

· 安全剧本编排过程中，对剧本节点的入参做充分的校验检查

· 对有操作风险的剧本节点，增加必要的人工审批和核验环节

· 对所有的写操作行为，设计反向操作功能，以在关键时刻使用剧本完成策略回撤

· 使用有严格权限控制的安全剧本编排系统，做好严格的角色划分

· 参照《SRE：Google运维解密》中的最佳实践，定期开展纯人工应急演练，保持一线人员的技能水平不会因为自动化代替而大幅下降

大模型应用的风险和现实难点

尽管大语言模型在人机交互层面开始全面颠覆传统技术，但也存在一定的风险，选择使用新技术时也应保持必要的谨慎，例如：

· 输出虚假或错误的信息：这类模型可能生成虚假或误导性的信息，可能带来不准确的回答和误导用户。在关键领域如核心业务业务系统操作，边界设备策略下发等环节，这样的风险尤为严重。

· 容易被黑产利用：恶意用户可能利用大型语言模型生成有害内容，如网络钓鱼、诈骗信息、网络暴力，进一步危害社交网络及社会环境。

· 数据安全与合规：用于训练模型的数据可能包含敏感信息，导致无意中泄漏个人隐私。使用模型过程中，将不得不发送内部数据到服务端，存在数据外发甚至出境的合规问题。

· 缺乏责任制度：目前，在大型语言模型产生问题时，很难界定责任归属，也就是我们日常所说的“谁来背锅”的问题。

此外，大模型在实际落地过程中还有一些现实难点：大模型与外部产品互动前，需要预先提供可供调用的标准接口。以微软Security Copilot和Blink Copilot为代表的安全副驾驶产品已经登上了历史的舞台。安全副驾驶能够通过自动化智能化的方式生成安全策略，并开展自动化应急处置。除了一方面需要大量的原始数据积累，更重要的是依赖于调度产品，对下游各种安全能力调度的支持。得益于主流安全产品开放性以及他们API的稳健性，国外人工智能与机器交互场景很容易实现安全能力的对接。然而在国内大量安全产品没有好的接口，甚至接口文档不完善，标准化能力不足，导致缺乏有效的技术联动，这还需要很长一段时间的积累。

虚拟现实将改变社会人文

虽然AR/VR技术在改善人类交互方面表现出巨大潜力，但在实际应用中也面临许多现实挑战与风险。除了硬件成本总提较高、技术成熟度有待提升以及软件生态需要持续完善等问题之外，长期使用AR/VR设备，将缩短人们在真实生活场景中的接触互动，可能导致社交隔阂。过度沉浸在虚拟世界中可能影响真实生活中的人际关系，因此平衡虚拟与现实之间的关系以确保AR/VR技术的健康应用是非常必要的。

总结

本文通过针对可编排安全自动化、基于大语言模型的AI能力和AR/VR技术等新兴技术，探讨了如何改变企业网络安全运营的现状，以及如何为此做好准备。随着技术日新月异，网络安全威胁越来越多元化，对企业网络安全防护提出了更高的要求。

可编排的安全自动化技术可以降低企业网络安全人员的负担，提高应急响应能力。基于大语言模型的AI技术，如ChatGPT等，给人机协同工作带来革命性变化，提高安全事件处理效率。同时，AR/VR技术有望为安全团队提供新的发展机遇，改善安全运营的效率和体验。

随着未来算力的增强和设备成本的下降，新技术将会以更快的速度进入我们的生活和工作场景，于此同时风险和挑战也随之增加。企业在引入新技术时，应始终关注潜在的风险，实现技术、管理和人力资源的有效整合。对于自动化技术，要注重风险防范和剧本节点的审查；大模型应用也存在一定的安全风险，如数据泄露、误导性输出等；AR/VR技术需要平衡虚拟与现实之间的关系，确保健康应用。

总的来说，企业要在网络安全攻防战场中取胜，必须积极拥抱新技术，转变思维方式，优化安全运营，同时防范新技术引入所带来的风险。未来已来，安全人请做好准备！

新背景、新趋势下的安全运营中心规划与实践

文｜袁明坤、张建盛

杭州安恒信息技术股份有限公司

摘　要： 网络攻击频发与网络安全要求日益严格的大背景下，如何确保安全防护效果与安全工作合规成为重要的议题，进行安全运营中心规划设计与实践能够充分发挥安全资源整体能力，确保各项安全工作合理、有序且标准化的开展，是整合繁杂的安全任务与发挥安全工作价值的最佳实践路径之一，也是在数字化转型大背景下发挥安全基石作用的重要保障。

关键字： 安全运营、运营平台、运营组织、运营场景、运营质量

概述

近几年，在外部网络安全监管要求与内部安全目标保障的双驱动下，各企业机构均搭建起较为完备的网络安全工具技术基础，安全管理体系各方面也逐渐完善，安全防护水平与管理能力得到了较大提升。但是，管理体系与技术体系之间的隔阂、安全工具割裂、安全数据分散、威胁风险处置不及时、安全管理成本过高等问题也随之而来，严重制约了安全治理水平与安全防护效果的持续提升，最终影响安全保障业务、响应合规等根本性目标的实现。

为此，各行业企业机构以自身安全需求为出发点，结合实际安全现状，研究并构建安全运营中心成为当前安全建设的重点内容。本文对当前网络安全运营现状与存在的问题进行剖析，立足网络安全运营目标，对安全运营中心架构与要素进行研究，并对运营中心的落地实践进行探索。

安全发展趋势视角的安全运营

长期以来，以等级保护等安全标准规范为核心导向的安全体系建设方式，在满足安全合规的前提下，在边界、流量、主机、服务等方面具备了初步的纵深防御与治理能力。但经过近几年各类攻防演练实战以及多样化攻击手法的演进的背景之下，以往整体技术偏静态的防护手段与安全措施，无法完全满足现有的安全防护强度需求。而以安全工具、服务人员、制度流程为核心的安全运营体系在实际演练与防护过程中，发挥了核心作用。

另外，数字化转型的逐步推进，使业务形态日益复杂多，网络与应用等基础支撑能力也随之在开放性、多样性方面发生了重大变化。新的变革必然带来新的风险，能否快速定位潜在风险威胁，能否构建与数字化转型相适应的安全运营服务能力，一方面是安全价值的体现问题，另一方面也事关数字化转型能否在充足的安全保障下顺利实施。

安全运营中心是网络安全发展过程的必经阶段，也是现实安全防护的需要，更是构建业务安全保障底座，确保业务战略实现的必要基础。

安全合规视角的安全运营

2017年6月1日起施行的《中华人民共和国网络安全法》，明确要求进行监测预警与应急处置，而这其中必然需要具备安全事件和风险的运营流程化支撑能力。在等级保护要求中强调的“一个中心、三重防护”，其中的安全管理中心部分，要求对安全体系各纬度进行统一化集中管理，并实现安全事件的识别、报警和分析。

另外在《关键信息基础设施安全保护要求》中分析识别等六个内容活动的要求中，必须依托安全运营体系的标准化、集约化、流程化的特点进行构建与运行，从而形成整体的关键信息基础设施保护能力。

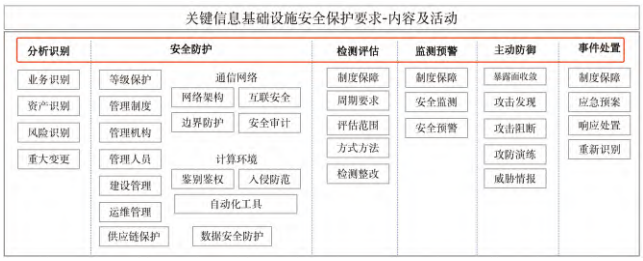


图1 关键信息技术设施安全保护要求内容与活动

安全运营中心建设需关注并解决的问题

安全运营本质上是面向安全结果与效果产出的，这就决定了安全运营中心建设不能简单以安全防护或安全治理视角进行技术性的构建，而是要将其定位成企业机构在安全领域里核心能力引擎，同时考虑业务侧对安全结果的需求、考虑安全管理的落实、考虑安全治理推进等等。基于此，在当前安全背景与安全趋势下，安全运营中心建设必须充分考虑以下几点：

（一）明确安全运营建设目标。安全运营涉及平台工具与服务等各方面，须考虑自身安全现状与防护目标的级别，匹配相适应的安全运营建设目标，将有限的安全资源进行针对性投入。

（二）安全高效协同性问题。将碎片化的安全数据与安全能力进行整合，发挥一体化安全效能。一方面降低安全管理成本，另一方面更是具备综合性分析能力，充分挖掘潜在安全攻击与风险。

（三）解决安全整体防护机制割裂问题。有设备、有人员、缺闭环、缺机制是当前安全工作的现状，安全运营须通过建立相关机制流程，实现人员的安全责任落实、安全运营过程闭环，将人与平台进行融合。

（四）安全能力由被动向主动转变。通过运营能力的构建与运营体系的运转，补充并形成网络安全整体主动防护能力，确保具备高水平安全对抗的能力。

（五）具备安全集中化决策支撑能力。运营中心除了具备安全风险与威胁层面的安全管控能力，应当能够体现整体安全态势、趋势，挖掘并呈现现有安全脆弱性与薄弱点，为安全建设、安全决策提供运营支撑。

（六）降本增效、提质减负。安全运营中心的建立在一定周期内应当是以有限的安全投入获取更高的安全效益，才更有利于推动安全运营水平的持续优化迭代，也符合更加广泛性的企业机构现状。

图2 新一代安全运营承载的任务与目标

安全运营中心规划设计

设计理念

安全管理纬度，安全运营中心的设计需满足由当前的事件驱动向数据驱动、管理驱动方向发展的要求，实现以管理促安全的目标，确保安全全局集中管理，在安全状态上由被动响应向主动运营演进。

网络安全是人与人的对抗，安全运营是安全对抗的主战场，运营中心和各项能力的搭建，也必须以实际运营相关人员为核心构建。对于安全决策者、安全责任人等运营管理者来讲，运营中心提供安全管理抓手、安全质量管控、安全战略制定、安全合规支撑等服务内容。对于运营岗位人员，运营中心提供能力与平台支持，完成运营动作，提高效率，提升安全技能水平。

图3 以人为中心的安全运营理念

运营中心整体架构

安全运营中心架构思路遵循一切工具皆服务，一切服务皆资源，一切资源皆运营的原则。以安全目标和安全需求为导向，以实际安全场景为基础，结合业务发展、IT演进、安全要求综合性要素，构建基于当前和面向未来的安全运营治理与防护体系。确保运营效果的有效衡量，现有安全资源的充分利用。

为实现安全运营事件驱动、数据驱动、管理驱动三步走规划，运营核心技术平台首先实现安全数据支撑能力，打破数据孤岛，进行多源异构数据接入，通过智能分析将安全大数据转变为运营小数据。其次，构建规模化安全运营支撑能力，针对各类安全场景、安全角色人员、成规模的资产等情况，解决响应、干预、处置过程的效率效能问题。最后构建体系化安全管理能力，为安全治理、防护等工作过程中提供快速决策、数据量化、安全质量衡量、安全成效评估、科学安全决策提供管理支撑。

为更好提供及时、有效的运营服务，采用在云地协同融合

方式，本地一体化运营平台与云端运营服务结合，能力下沉、运营上移、运营场景与需求全覆盖。通过安全咨询服务保障，将人、平台、流程进行符合运营逻辑的设计，同时对云端、本地；人员、工具之间的关联逻辑紧密耦合，发挥最大安全运营势能。

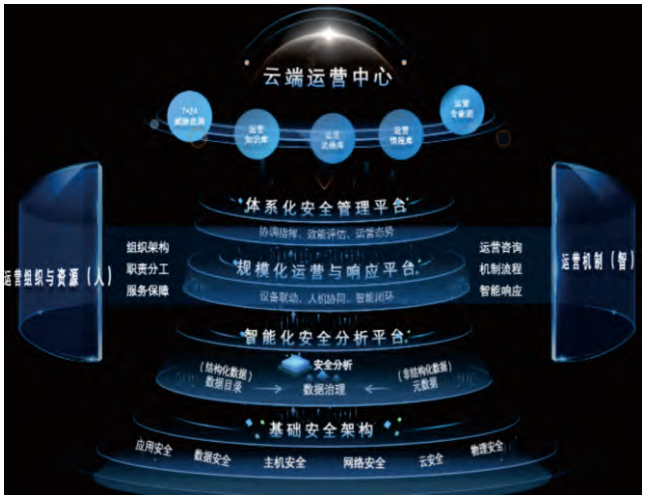


图4 运营中心技术架构示意图

分层解耦的一体化运营平台

在运营中心平台化建设方面，需要同步考虑人员角色的实际工作需求，实现人机有效互动协同的运营效果。从实际运营支撑角度，就需要将运营平台进行能力解耦，分为数据处理层、运营流程层、运营管理层，与安全监测分析、规模化安全运营、运营质量管理评估三部分核心运营工作相匹配。

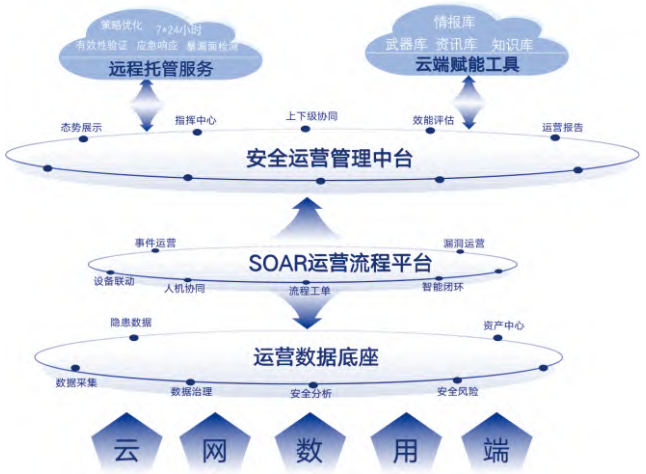


图5 平台分层解耦示意图

运营数据底座，汇聚全网安全数据、提高已知安全威胁检测的准确度并实现未知安全威胁的智能发现。

运营流程平台，整合人、过程和技术，实现自动化响应与定制化流程定义，大幅提升安全运营工作效率。

运营管理中台，对整体安全运营效率效能进行可视化管理，同时进行基于业务角度的安全管理工作，实现业务层面的工作职责划分与流程机制设计。

分工明确的运营组织架构

运营组织架构的设计以安全运营相关管理制度为依据，将技术部门、业务部门纳入运营管理组织范畴，同时将自有人员、外包等纳入运营体系之中，以安全场景设计运营组织结构，打破以往设备+人员一一对应的固化服务模式，确保运营岗位职责的明确。

同时，在运营组织中要设置运营经理相关职能岗位，进行日常运营团队管理，制定项目安全运营计划与任务分工，定期对工作进行总结、复盘，带领现场运营团队高质量完成客户下发的任务；并对整体网络安全态势进行分析与呈现，对特定目标遭受到网络攻击的态势进行分析。

在依据场景进行运营职责分工方面，可参照内部实际的需求进行弹性选取，一般包括监测、分析、处置、运维、合规、脆弱性管理等方面，在允许的情况下，可采用本地运营组织与远程服务结合的方式，满足运营工作开展的需要。

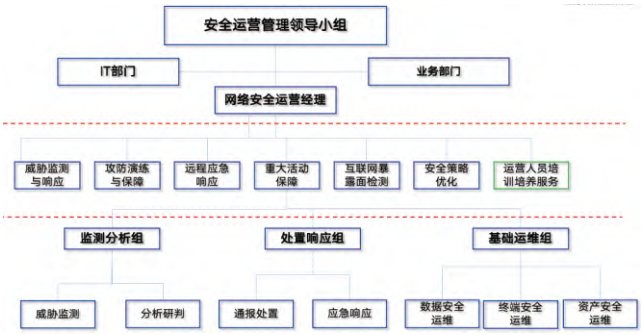


图6 运营组织架构分层示意图

规划化与场景化的运营流程设计

基于运营场景进行运营流程设计，是确保安全运营工作有序、标准化开展的基础。依托安全运营平台、运营组织结构，结合符合自身需求的运营场景进行运营流程设计，实现自动化、流程化的运营闭环管理。

图7 运营场景与运营流程设计

运营中心落地实践

安全运营中心搭建是个复杂的系统性工程，向下去兼容现有的安全现状与资源，向上兼顾安全运营目标与安全需求，进行阶段性运营中心建设目标与实际动作，确保运营能力的逐步形成。一般来讲，安全运营中心建设分为三个重要阶段：

强基整合阶段：以整体运营视角，进行局部落地达成基础运营效能呈现为目标，数据统一、工具集中、基础运行。包括基础运营平台搭建、人员组织架构设计、基础运营流程设计、现有运营资源情况调研等工作。

体系融合阶段：以完善丰富场景、运营服务化、处置自动化为建设目标，重点针对自动化流程工具搭建、安全策略优化、运营服务场景设计、增加感知与覆盖范围、运营指标设计探索进行运营能力设计。

量化赋能阶段：以安全验证、运营度量、效能管理的能力引入与运营结果呈现为目标，重点任务包括威胁情报引入、业务安全管理平台搭建、运营知识沉淀与转移、运营指标运转与量化等，实现运营工作的固化与优化，全面展现运营效益。

图8 运营体系落地实践规划

运营效果衡量与呈现

图9 运营指标线上化度量

为确保运营效果的可衡量与可量化，运营中心相关能力与成果，需要引入适当的运营评价体系与运营指标，一方面能够监控运营的效率，明确运营体系的短板和问题，为优化运营决策与安全建设指明相关方向。

运营指标设置可依据运营实际动作进行拆分，纳入平台能力、人员考核等方面，全面考核现有运营工作的同时，对现有安全运营成熟度进行整体评估。

总结与展望

网络安全重要性的不断提升与安全对抗程度的不断升级，一方面要确保安全合规符合性要求，另一方面也要确保安全工作不出事。充分整合现有安全基础能力，引入外部运营服务的支撑，构建符合自身安全防护要求的运营中心是各行业的必经之路，也是在数字化、数据化大背景下实现风险威胁快速发现到处置的基础。

随着业务场景的多样化发展，安全运营的覆盖范围势必不断延伸，逐渐形成以成熟的运营机制与开放性运营能力汇聚的运营中心，也是改变攻防不对称，保障业务稳定与安全的发展方向。

证券行业安全验证提升精细化安全运营能力创新实践

文｜聂君

北京知其安科技有限公司

摘　要： 金融行业网络安全的大力建设和快速发展得益于国家和行业相关法律、行政法规的陆续施行，以及数字化转型工作的持续深入开展。相对于早期被动防御，金融企业已经逐渐转变为以持续监测与动态防御为核心的主动安全与持续运营模式。为了提升安全防护能力和安全运营效率，金融企业需要构建完善的安全验证机制，通过平台部署的方式，实现对当前已部署的各类安全措施进行多维度、全场景的有效性验证。实时验证和持续监测各类安全防护措施，及时发现安全防护的薄弱环节并提供加固指导，从而提升企业的安全防护能力和安全运营效率。

关键字： 安全运营、金融行业、安全验证、防护失效

证券行业网络安全的重要性

证券行业在整个金融行业中具有重要地位。作为金融行业“三驾马车”之一，证券行业提供了一个有效的融资渠道，是证券交易、信息披露和信息价值交换的重要场所。各类IT信息系统作为业务的重要支撑，确保证券其在安全的前提下高效的开展经营业务至关重要。

首先，证券行业涉及大量的资金流动和交易，包括各类的敏感信息，如个人身份信息、资金交易记录等，一旦泄露或被攻击，将对客户和市场造成严重影响。网络安全能够确保交易过程中的信息不被泄露、篡改或破坏。

其次，证券交易平台是金融市场的重要基础设施，其安全稳定直接关系到金融市场的正常运转和投资者的资产安全。

再者，网络安全为证券行业的业务创新提供了有力支撑。在确保信息系统安全的前提下，证券公司可以更加放心地推进新技术和新业务的应用。如利用云计算、大数据和人工智能等技术提高交易效率、优化投资策略、提升客户服务等。网络安全不仅为业务创新提供了保障，也为证券公司带来了竞争优势。

证券行业安全运营现状与痛点

随着外部网络安全威胁的加剧，基于行业监管需要以及内生安全需求，各大券商通过近几年的持续建设和完善部署了一系列安全管控措施，包括各类安全设备、安全软件和安全工具，并在这些设备软件和攻击基础上，制定了一系列安全防护和检测规则进行7*24小时实时监控，并进行自动化和人工处置。通过构建起纵深防御的安全体系来应对日趋严峻的网络安全威胁。然而，在实际的安全运营中，仍然需要解决当前所面临的一些痛点：

威胁复杂严峻，攻击演变快速

攻防不断进化，每天都会涌现新的攻击和手法。如何跟踪和掌握这些威胁，将其反馈到实际的防御场景中，如何通过自动化和工程化手段验证和优化大规模、跨区域的防御策略，确保业务安全，是当前的紧急任务。

安全防护复杂，人工局限凸显

已部署的大量安全防护设备、软件和工具分布在不同的数据中心和网络架构中，但其可用性和连续性容易中断（很难发现），可能导致安全防护失效。尤其是流量检测类产品，告警多且误报也多，可能淹没真正的攻击告警事件。

常态化运营中，涉及多个端口、资产和测试/生产环境的联调测试，以及IT环境和系统的动态变化，可能导致已发布的安全策略失效。由于安全策略多且广泛，人工监控和掌握困难，导致安全防护效力偏离预期。例如，边界侧的不同WAF防护策略可能存在不一致和安全覆盖问题，这些问题很难通过人工方式发现。

安全防护脆弱，缺少验证机制

传统的防御基于已部署的各类安全设备和平台，实现被动的静态防御。需要高度依赖安全产品和厂商服务的专业性。为此，已部署的安全防护能力是否有效，是否能达到预期对于安全建设的效果反馈至关重要。长期以来安全运营团队

缺少一项机制，实现对已部署的安全防护能力进行全面的验证和评估。

从脆弱性角度分析，我们认为当下安全事件的发生是由两个因素叠加形成的。即：资产的脆弱性+安全防护体系的脆弱性。传统面向资产层面的漏洞扫描、渗透测试已然成熟，但面向安全防护体系的脆弱性，如何及时发现防护失效情况，量化和度量当前的安全防护能力是安全运营团队迫切的需要。

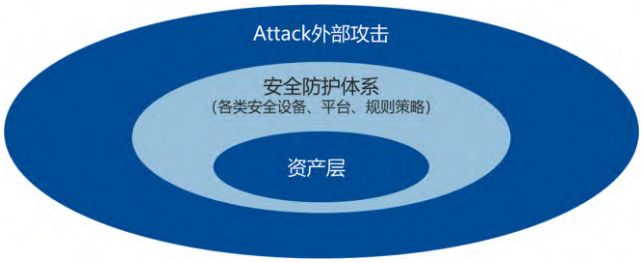


图1

面对当前已部署的各类防护措施和纷繁复杂的规则策略，安全管理和运营团队长期以来缺少抓手，对整体的安全防护体系进行掌握和度量。传统人工方式通过渗透攻击等手段进行验证，一方面需要有一定技能要求，另一方面存在覆盖面不全和效率低等问题，另外潜在的风险来自于人工攻击渗透所带来的职业道德风险，如何建立独立的旁路验证机制，如何对所有的验证执行过程可审计可追溯，如何实现自动化大规模的对防护体系进行验证评估是各个安全团队应该关注的。

国内外安全验证发展趋势

防御与攻击是相互博弈的，是一个动态平衡的过程。习近平总书记也提到，网络安全的本质在对抗，对抗的本质在攻防两端能力较量。只要涉及攻防，防守方都存在被攻击方成功入侵突破的可能。证券行业安全团队如何最快的速度发现入侵（告警），如何发现和检测是在哪个环节出现问题并立刻采取处置行为是至关重要。通过采用“持续性、常态化、自动化的自我攻击模拟验证”，基于攻击视角对当前安全建设进行全方面的从点至面的安全验证和评估。通过安全验证的手段，侧方位验证企业安全防御的有效性真正做到实战化的网络安全评估。

国外BAS向安全验证的发展和演变

▶2017年，Gartner在发布的《面向威胁技术的成熟度曲线》(Hype Cycle for Threat-Facing Technologies) 中首次出现BAS入侵与攻击模拟（Breach and Attack Simulation）概念，并将之归到了新兴技术行列。

▶2021及2022年，“Gartner在《2021年八大安全和风险管理趋势》、2021及2022《安全运营技术成熟度曲线》等报告中，连续提到BAS技术的必要性，将成为IT安全建设重要技术手段。”

▶2023年，Gartner最新的2023年网络安全趋势提到的9大趋势中，“Cybersecurity Validation网络安全验证”成为重要元素之一，从BAS技术框架的提出，到网络安全验证，真正落地实现了攻击模拟的落地化应用。

图2

国内安全验证的发展情况

目前国内对于安全验证技术和应用正处于高速发展阶段，从行业到应用都存在巨大的研究和发展空间。目前已经有部分比较先进的企业，注重正向建设的成果在实际攻击发生时的检测和防护效果、以及防护策略在各个网络位置的落实情况，已经开始进行反向验证体系的建设，旨在能够更加全面、及时、准确的了解到当前的安全防护装备对攻击的感知能力。但经过调查研究发现，当前阶段更多是以人工手动编写攻击脚本的方式进行验证，主要注重解决实际遇到的个例问题，较少实现平台化、体系化、自动化，存在实施效率不高、实施周期较长、验证规则编写与人员能力强相关等问题，且无法实现自动化的方式验证网络安全防护装备对于每一种的攻击手法或攻击方式的感知能力。目前国内已经涌现出少量在该领域专注的初创型企业，已开始大规模商业化部署和应用，实现快速迭代提升。

从法规政策的角度来看，国家及证券行业对网络安全问题的重视程度日益加深，监管部门也在持续提升对网络安全防护有效性的要求。诸如《证券期货业网络安全等级保护基本要求》、《信息安全技术 关键信息基础设施安全保护要求》以及《信息安全技术 信息安全风险评估方法》等监管规定，均强调了对现有安全技术措施的有效性、安全配置及安全策略一致性的定期全面核查，以评估关键信息基础设施在遭受实际网络攻击时的防御和应对能力。

安全验证实践要点与典型失效

安全验证实践要点

安全验证，从落地实践来说是基于BAS（入侵与攻击模拟）这项技术框架，打造出自适应的平台帮助在企业内部自行构造不同的模拟攻击验证场景，对企业纵深防御各个切片开展全面的模拟攻击验证，通过对攻击结果、攻击返回信息、告警日志信息等的汇集分析来评估整体防护的有效性。

基于对众多企业用户的研究和调研，我们认为安全验证在安全运营中应该具备和做到“四化三可”从而实现最佳落地实践。以自动化为核心，构建实战化、体系化、常态化的安全验证机制。通过在企业内部构造不同的模拟攻击验证场景对已部署的各类安全防护措施及规则策略开展模拟攻击验证形成可量化、可持续、可运营的：安全验证体系。

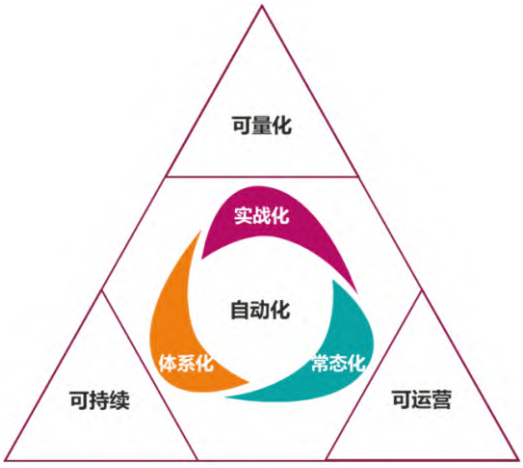


图3 安全验证在运营实践中的“四化三可”

· 实战化：真正以攻击者视角对当前已部署的各类安全防护措施模拟攻击验证，检验当前状态下各类防护能力的实际效力情况；

· 体系化：基于不同漏洞利用、攻击工具、攻击手法等实现对纵深防御不同场景下的安全防护验证，实现体系化的全局验证和掌握；

· 常态化：与安全运营高度融合，通过常态化的安全验证先于攻击者发现安全能力薄弱点，缩短问题存在时间窗，最终实现稳定、高水准的安全防护态势；

· 自动化：上述所有的实现，都应该基于平台以自动化的方式来实践，不需要额外的专人投入，通过自动化的方式实现攻击场景构建、任务调度、事件日志获取与分析评估，最终实现全自动化的验证和结果输出；

· 可量化：操作详情可回溯、可审计、可复测，所有验证数据可量化、可视化、可度量给出安全全貌，指导安全运营投入，让安全投入有的放矢，回报可见，安全建设资金高效利用可持续；

· 可持续：通过平台持续跟踪和更新，快速上线最新的、热点高危漏洞利用和攻击验证场景用例，及时对全局安全措施实现全覆盖的自动化持续验证，确保安全防护措施有效且处于稳定状态；

· 可运营：安全验证作为安全运营的重要组成，全流程具备可运营特性，基于各类攻击场景、防护措施、验证数据实现自身可运营的验证闭环。

典型防护失效案例

1. 管理与流程问题

1）域名管理不当导致防护被遗漏，互联网业务对外部入侵零感知

· 关键字：

流程失控、覆盖缺失、边界防护失效

· 失效点描述：

某企业通过互联网对外开展业务包括数百个URL。为了对这些业务边界进行防护，已部署IPS、WAF、NTA等网络安全设备构成了网络边界纵深防御体系。在开展验证的过程中，发现有30多个URL 并没有受到这些安全设备的保护。

· 原因分析：

该企业的域名有多个互联网出口，分别由不同的团队负责运维进行设备的配置，各团队间并未形成统一的互联网业务上线流程与配置要求。有些互联网业务发布时，直接开启了网络配置的变更，并未同步更改边界防护设备的配置。

· 整改措施：

i.对现有的互联网防护覆盖度进行排查，将未接入防护的互联网业务快速补防。

ii.将互联网出口进行统一纳管，强控所有互联网业务上线标准动作，包括上线前必须开展安全测试并完成重要漏洞修复，上线时强制要求接入防护措施。

iii.增加对域名与互联网接口的持续验证，对互联网出口资产的管理有效性进行监控。

· 其他常见原因：

i.域名新增或变更的过程中，并未同步修改安全设备的配置；

ii.域名解析规则配置错误，或部分解析节点未作覆盖。

2. 网络与系统架构问题

1）互联网加密流量未作证书卸载，网关设备不具备防护能力

· 关键字：

覆盖缺失、整改推动困难、边界防护失效

· 失效点描述：

某企业边界具有较完善的防护措施保护互联网业务，WAF防火墙也是串联在出口侧并开 启了阻断模式，但对其进行互联网业务防护覆盖度验证过程中，发现企业边界防护覆盖度非常低，仅有29%，大量业务处于不受保护的状态。

· 原因分析：

经分析，并未覆盖的业务大部分为加密流量，无法被

WAF保护是因为并未对流量进行证书卸载。该企业的WAF防火墙是后期部署的网关设备，在部署初期因无法与业务系统运营团队达成一致意见，并担心对业务造成影响，并未进行证书卸载。而之后企业也并未采取强制性系统架构标准，对证书加密事项进行统一要求，后续新上线业务系统的证书卸载工作推动也较难。

· 整改措施：

i.推动将加密流量证书卸载网关纳入整体架构标准并推动部署。

ii.将业务系统开发标准的流量加密算法作为基线要求，并对所有新系统及更新迭代的系统适用。

iii.推动现有系统的整改，以常态监控与量化指标评比晾晒，督促各业务系统的整改进度。

· 其他常见原因：

i.网关设备不支持业务系统采用的加密算法；

ii.证书发生变更并未做同步。

2）网络架构变更过程未同步协同，流量安全探针出现大量遗漏情况

· 关键字：

架构异常、变更协同、流量检测失效

· 失效点描述：

某大型企业中有多个互联网出口以及各个分子公司均部署有流量安全设备，总数超过50台。经过持续的模拟攻击验证后发现，其中有3台流量探针设备没有任何相关攻击流量日志产生，6台流量探针设备捕获到的相关攻击流量日志不足50%，流量检测能力存在较为明显的异常现象。

· 原因分析：

确认后发现，存在流量监测盲点的区域均进行过网络架构的调整，部分区域更换了新的交换机设备，而完成网络设备上线后并未同步调整流量配置为探针设备提供镜像流量。而安全运营人员被海量告警淹没，并未察觉到个别设备告警异常的情况。

· 整改措施：

i.调整网络配置使流量探针设备能够运转正常；

ii.将流量检测设备纳入基础设施标准设备范畴，在网络架构变更中同步考虑流量镜像的需求；

iii.以安全验证覆盖重要网络区域，作为日常监控安全能力状态的巡检工具。

· 其他常见原因：

i.路由策略、网络访问权限等的变化导致安全防护措施失效；

ii.在监测流量中存在加密流量且不具备解密条件。

3. 运营与操作问题

1）上线部署时采用最精简策略，边界 WAF 防火墙无法拦截初级攻击

· 关键字：

策略错误、运营不规范、边界防护失效

· 失效点描述：

某企业在互联网边界部署了 WAF 防火墙用于主动拦截各类 WEB 攻击，且所有的域名均已接入了该防火墙的防护范围内。但在实际的验证过程中，发现该企业 WAF 防火墙对于 SQL 注入、XSS 等初级且常见的攻击手法拦截率极低，而相同产品在其他客户是有较好的防护效果的，该企业的防护设备未能发挥其应有的能力。

· 原因分析：

回顾WAF上线时的过程，确认该企业部署设备时为了保障业务，精简了大量的策略规则。在后续的运营过程中，安全人员不具备对WAF调优的能力，也无法针对各个业务开展精细化运营。

· 整改措施：

i.推动策略调整变更动作，分批次对业务规则适用最基本的防护能力，对较初级的攻击行为进行阻拦；

ii.参考验证结果提供的用例，开展持续运营与规则优化，建立精细化策略调优的运营方法。

· 其他常见原因：

i.因业务稳定性问题时关闭了 WAF 的大部分策略，并非针对性进行策略调优；

ii.为应对紧急上线、故障等情况进行的临时应对处置，事后并未进行复盘及恢复；

iii.因人为操作失误导致的策略生效范围过大；

iv.设备升级过程中部分策略与规则变为默认关闭，运维人员并不知道需要重新打开。

2）版本升级后之前生效策略默认变为关闭，整个防护模块全部失效

· 关键字：

策略错误、运营不规范、主机防护失效

· 失效点描述：

某企业采用商业化主机防护解决方案对所有生产主机进行防护，且很明确相关软件已采购了恶意代码防护模块并开启了相关防护策略。但在实际验证过程中，发现相关防护软件对所有的恶意代码没有任何的检测与阻断能力。

· 原因分析：

通过查看防护软件的配置信息发现该企业缺失有恶意代码防护功能，但在策略设置中该模块处于关闭状态。经与相关人员核实，该策略部署时明确是启用的状态。但回顾运维操作日志，并未发现对该项策略调整的记录。在与厂商进行确认后，发现该模块在之前的一次版本升级中考虑到业务影响，被默认调整为关闭状态，而更新的调整信息未能及时同步，导致版本升级后很长一段时间整个该策略处于关闭的状态。

· 其他常见原因：

i.防护产品出现 bug 导致防护策略无法按预期生效；

ii.产品部署时实施工程师配置 / 操作不当，导致防护策略未生效。

4. 人员失误或意识问题

1）运维人员配置规则时出现错误，导致整个防护策略失效

· 关键字：

人员失误、运维流程、防护失效

· 失效点描述：

某企业有多套互联网边界的 WAF 防火墙分别对不同的互联网出口进行防护，且所有的设备是由安全团队设置了专人进行日常的巡检维护，在所有的巡检日志中并未发现设备的异常。但在实际验证结果中，发现其中一台设备处于毫无防护能力的状态，该互联网出口下所有业务都面临较大威胁。

· 原因分析：

经排查发现，失效设备上的策略规则中出现了一条错误规则，导致该规则以下所有的策略都无法正常生效。该设备的运维历经多人迭代且没有保留任何运维记录，已无法确认具体操作人员与原因。而运维人员的日常巡检关注的是性能状态，不会对所有的策略进行梳理确认。因运营人员日常关注的是日志集中的 SOC平台，业务无法关注到海量日志告警中该设备的日志告警异常。

· 整改措施：

i.删除异常策略，重新使防护策略生效；

ii.规范 WAF 运维规范，设置专人专用账号并留存所有运维操作记录；

iii.通过持续验证建立安全能力有效性的监控，及时发现各类原因导致的安全失效点。

· 其他常见原因：

i.因策略冲突导致配置失效而不知；

ii.人员恶意操作。

安全验证平台的关键技术及创新点

“安全验证平台”基于模拟攻击技术实践，模拟可能由黑客或攻击队实施的网络攻击，通过构造不同的模拟攻击验证场景，对已部署安全设备和策略开展持续性、有效性安全验证。通过在不同网络域单独部署验证机和靶机，实现无害化的开展持续的攻击验证，形成自动化规则策略验证闭环，实现安全防护、检测等安全设备的有效性验证，确保网络安全配置、安全设备、安全策略等按照预期运行。

关键技术

1. 引入自动化入侵与攻击模拟技术（BAS）

传统的风险评估技术侧重于识别系统、网络和应用程序漏洞，BAS方案可以更进一步。BAS是指通过主动验证+自动化的方式，利用攻击者的战术、技术和程序来模拟杀伤链的不同阶段，持续测试和验证现有网络整体的安全机制（包括各安全节点是否正常工作、安全策略与配置的有效性、检测/防护手段是否按预期运行等），对企业对抗外部威胁的能力进行量化评估，同时提供改进建议，推动企业安全体系走向成熟。

2016年笔者提出将安全验证框架作为安全运营四大框架之一，提出了白盒验证（过程验证）和黑盒验证（结果验证）的具体实现：安全验证框架主要功能是综合通过黑盒白盒验证措施，确保安全防护框架和安全运维框架有效性。安全度量框架主要功能是通过一系列安全度量指标，衡量评价安全运营质量水平，并针对性持续过程改进，实现质量的螺旋上升。由此形成了一套完整的安全验证方法论：以安全验证的技术和手段来验证安全有效性和安全的价值，早于Gartner提出安全验证概念7年。

2. 构建安全验证技术运营工具链

在企业信息安全建设初期，安全工作的主要内容是购买安全设备和部署安全管控系统并进行日常维护。从网络层、虚拟层、系统层到应用层、数据层、用户层部署了一系列安全设备或软件并确保其稳定运行，但发现安全状况并没有得到有效改善，安全问题频发，其根本原因是没有进行有效安全运营。如何建设企业有效的安全运营体系，则需要安全运营架构、工具、资源三合一的安全运营思路，从而构建安全验证技术运营工具链。

为确保安全运营架构能够灵活扩展，推荐按功能模块划分成四个模块：安全防护框架、安全运维框架、安全验证框架、安全度量框架。

基于攻击模拟技术的安全验证体系建设，模拟可能由犯罪分子实施的网络攻击，通过内置的攻击脚本及攻击行为，对安全设备和策略开展持续性、有效性安全验证，通过持续的验证，形成自动化规则策略验证闭环，实现安全防护、检测等安全设备的有效性验证，确保网络安全配置、安全设备、安全策略等按照预期运行。以此保障安全设备、规则和策略正常工作；通过全面的自动化攻击验证场景，结合渗透测试和红蓝对抗，开展攻击和防护体系持续对抗和能力升级，融合现有安全运营体系，建设以攻防实战为核心、具有持续验证能力的安全体系。新型漏洞和攻击手段具，能够在24小时内在企业内部进行自动化验证。

创新点

1. 理念先进，领先国外

2017年，Gartner在《面向威胁技术的成熟度曲线》(Hype Cycle for Threat-Facing Technologies)报告中首次提出了入侵与攻击模拟(BAS, Breach and Attack Simulation)的概念，将其作为一类重要的新兴安全技术。Gartner在该报告中明确指出该框架“可供安全团队以一致的方式持续测试安全控制措施，贯穿从预防到检测（乃至响应）的整个过程”。

2021年，Gartner又在《2021年八大安全和风险管理趋势》（Top Security and Risk Trends for 2021）和《2021安全运营技术成熟度曲线》（Hype Cycle for Security Operations 2021）报告中，进一步强调了安全能力验证的必要性，Gartner预计安全能力验证将逐渐成为IT安全建设的重要技术手段，并在未来数年内被大量机构与企业广泛应用。

2023年，Gartner在发布的网络安全趋势中，首次正式将“安全验证”列为趋势之一。

国外安全验证技术研究与应用发展较为迅速，一些新型专业安全公司以入侵与攻击模拟领域为核心业务领域，设计和实现了一系列方式多样、场景丰富的安全验证技术和产品，通过构造攻击场景的方式对已部署的安全措施进行验证。

将视野收回国内，我所在的某头部股份制银行则在2009年便开始建设SOC平台，2011年开始自建蓝军，在内部进行红蓝对抗，实现黑盒验证；2012年，该头部股份制银行网上银行首次实践网络安全验证技术，同时笔者有幸负责了国内最具创新力和科技能力的股份制银行的安全运营建设；2016年笔者公众号“君哥的体历”发表文章《金融行业企业安全运营之路》，系统性阐述了网络安全验证实践，2018年在个人著作《企业安全建设指南：金融行业安全架构与技术实践》中进一步完善了安全验证理念，并运用至今。2023年，Gartner在发布的网络安全趋势中，首次正式将“安全验证”列为趋势之一，这也意味着，我们在对安全验证的研究与实践上领先国外同行。

2. 适配行业安全防护体系

基于现有安全体系，以自动化全覆盖、验证闭环为原则，与安全策略验证措施相结合，设计了一套先进、完整的安全验证的框架。能够以统一的验证任务管理、安全验证场景配置、验证脚本管理为基础，利用分布式攻击验证引擎，持续对金融行业安全监测防护设备、运营响应流程等开展周期性、持续性验证，运用可视化技术，实时展现企业安全防护有效性状态，与攻防演练、红蓝对抗等攻防活动互为补充，提升企业安全防护水平。

3. 实现安全策略闭环验证

有效性验证系统采用服务端、验证机、靶机三部分分离技术、模拟攻击验证技术，实现灵活的模拟真实攻击者的方式进行安全验证；通过在不同网络域部署攻击机和靶机，开展持续的攻击验证，形成自动化规则策略验证闭环，实现安全防护、检测等安全设备的有效性验证，确保网络安全配置、安全设备、安全策略等按照预期运行。

4. 丰富的攻击验证能力

结合现有安全措施，多平台联动机制，通过与信息安全态势感知平台联动，同步安全设备资产信息、同步告警日志，接收系统验证结果，判断安全设备的防护有效性，实现自动化验证结果闭环；通过全面的自动化攻击验证场景，结合渗透测试和红蓝对抗，开展攻击和防护体系持续对抗和能力升级，融合现有安全运营体系，建设以攻防实战为核心、具有持续验证能力的安全体系。

5. 提升效率、数字化展示

通过自动化攻击验证能力替代现有安全策略的手工验证，在提升验证频率的同时节省人力，提升验证效率和效果，实时识别失效策略，确保安全防护体系实时有效；分析验证结果，形成防护有效性报告，量化安全防护能力和效果；结合网络及应用拓扑结构，可视化展示安全防护状态。

安全验证的未来发展

通过一段时间的验证与优化，安全验证平台从实战角度，以攻击者视角通过模拟攻击验证的方式确实帮助发现了很多人工运营很难发现的问题，通过自动化闭环的方式减少人员投入的同时具备更多有价值的验证数据产出，帮助掌握和量化度量整体的安全防护态势，对下一步安全建设提供了充分的指导依据。实现了安全运营的有效闭环，从攻防两端持续审视安全建设情况，让安全能力螺旋迭代加强。

Gartner最新的2023年网络安全趋势提到的9大趋势中，提出“到2026年，超过40%的组织，包括三分之二的中型企业，将依赖于统一的平台来运行网络安全验证评估。”安全验证，必将成为企业安全运营的利器。

网络安全验证工具，在将高度可重复和可预测的评估工作自动化方面，取得了快速进展，从而能够对攻击技术、安全控制和流程进行一致和定期的基准测试。基于实践需求预测未来网络安全验证的发展将覆盖更多领域：

1.安全有效性：通过红队活动评估现有安全控制可拦截和检测的程度，这一过程通常利用自动化攻击模拟实现。

2.安全一致性：自动化和定期审计，例如分析安全工具配置或重复攻击场景运行。检验真实的防护效力是否与预期一致。

3.事件响应效能：通过测量调查测试的攻击场景所需的时间来评估响应机制的及时性和有效性。

4.用户应对能力：通常通过培训实现，例如用户意识或桌面推演（沙盘推演）和模拟演练。也可基于安全验证（平台）的机制，实现安全意识演练，如钓鱼、社工等。

随着越来越多安全平台和工具的使用，企业组织需要逐步扩展其网络安全验证实践的范围。从基础的安全防护开始，逐步过渡到如数据安全治理、合规审计等方面，基于网络安全验证，一方面是对OT提到自动化运营技术的全面实践，同时在更大程度上推动和优化既有资源的最大化利用和挖掘。

技术前沿

09 密码技术

国密算法在证券行业联盟链中的应用

文｜王毛路、闫发腾

北京共识数信科技有限公司

摘　要： 本文旨在深入研究国密算法在证券行业联盟链中的应用，并重点探讨P7数字信封的作用。首先，我们将介绍国密算法的基本原理和特点，以及证券行业联盟链中的安全需求。接下来，我们将详细探讨国密改造后的P7数字信封在证券行业联盟链中的加密和解密过程，以及其在数据机密性和完整性保护方面的作用。此外，我们还将探讨国密算法在证券行业联盟链中的其他应用，如身份认证、密钥安全和数据验证等方面。最后，我们将通过实证研究和案例分析，验证国密算法在证券行业联盟链中的实际效果。

关键字： 联盟链、国密算法、证券行业、数字信封

项目背景

随着《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等法律法规的出台以及《中华人民共和国密码法》的实施，各行业都被要求进行密码国产化改造工作。证券期货行业作为金融体系的重要组成部分，其广泛的业务场景成为区块链技术应用的潜在市场。为了推进科技监管能力建设，促进证券业数字化转型，中国证券业协会于2021年1月建设并上线了名为"证券业联盟链"（简称证联链）的证券行业联盟链。证联链基于区块链技术，旨在利用区块链的可追溯性、不可篡改性和安全可信等特点，助力科技监管，推动数据共享和数据治理，构建证券行业的新型基础设施。

在证券行业联盟链中，密码学是基础，包括对称加密、非对称加密、单向散列算法和数字签名等。为了保护证券行业的信息安全，提升密码自主创新水平和供给能力，金融监管机构将推动证券期货行业进行国产密码改造工作，建立以国产密码为主要支撑的金融信息安全保障体系。在这一背景下，国密算法成为保障证券行业联盟链数据安全的核心技术之一。

国密算法在证券行业联盟链中的应用，重点研究国密算法及其密钥管理技术，并制定行业标准，推进国产密码技术在行业中的应用。目标是提升行业数据应用的安全性和可靠性，并为证券期货行业提供一套完整的基于国密算法的行业联盟链应用方案。关注安全高效的密钥管理技术和共识协议的执行效率，以提高数据应用的安全性和可靠性。通过推动加密算法在证券期货行业中的广泛应用和推广，为行业数据应用的安全和可信建设做出积极贡献。促进国产密码技术在行业中的广泛应用。这将提升证券行业数据应用的安全性和可靠性，推动行业的数字化转型。

国密算法在证券行业联盟链的应用实践

证券行业联盟链的安全需求

证券行业联盟链作为金融市场的重要组成部分，面临着众多的安全需求。以下是证券行业联盟链中的安全需求：

数据保密性：证券行业联盟链涉及大量的敏感数据，包括交易信息、客户资料、账户余额等。这些数据在传输和存储过程中必须得到严格的保密，以防止未经授权的访问和信息泄露。数据保密性是确保联盟链参与方和客户信任的基础。

数据完整性：在证券交易过程中，数据的完整性至关重要。任何对数据的篡改或损坏都可能导致交易的错误或丧失客户的信任。因此，联盟链系统需要确保数据在传输和存储过程中的完整性，以防止数据被恶意篡改。

身份认证和访问控制：证券行业联盟链中的参与方涉及多个角色，如证券交易所、券商、投资者等。因此，确保每个参与方的身份真实性和权限合法性是至关重要的。合理的身份认证和访问控制机制可以防止未经授权的访问和恶意操作，保障系统的安全性和稳定性。

抗攻击能力：金融领域一直是黑客和恶意攻击者的重点目标。证券行业联盟链作为一个金融基础设施，需要具备足够的抗攻击能力，以抵御各种网络攻击、数据泄露、恶意软件和社会工程等威胁。只有保持高度的安全性，才能确保交易的可靠性和系统的稳定运行。

在解决证券期货行业中加密算法及关键技术应用方面的主要问题，其中包括以下几个方面：

1.国密算法在行业联盟链中的选择与应用：针对证券期货行业的数据加密需求，研究不同类型的加密算法，包括对称加密算法、非对称加密算法、哈希算法等，并根据具体应用场景选择合适的算法进行应用。

2.国密算法在联盟链证书管理体系中的应用：研究如何在保证数据安全性的前提下，实现国密算法标准的多级证书的签发、验证、重置、撤销、导出及托管的能力，覆盖证书的全生命周期。

3.国密算法在大文件分布式存储相关技术中的应用：探索国密算法在证券期行业中的P7数据信封技术及大文件分布式存储技术标准与规范，确保文件加密的可用性、安全性，并明确其算法的应用机制。

4.国密证书在多种跨链方式的结合：研究采用国密算法构建跨链互信及认证机制。

5.国密算法与智能合约的结合：研究联盟链与应用层对接时，区块链智能合约及配套接口的国密应用方法。

6.国密算法与数据隐私共享的结合：研究基于国密算法的链上数据隐私保护方案设计，利用不同类型的国密算法与隐私保护技术结合实现链上数据的隐私保护。

“证联链”整体架构

依托“证联链”进行构建的系统，技术架构整体上分为三个层次：业务层、数据层、适配层。

图1 证联链技术架构

业务层：主要指具备业务逻辑处理功能，能对业务数据进行生成、处理及存储等操作的系统；

数据层：主要包括数据标准及规范，用于规范数据格式，确保业务数据传输及处理过程中的高效性、正确性；

适配层：主要指“证联链”服务网络，包括区块链节点、“IPFS”节点，实现区块链网络及“IPFS”网络的接入及数据的加密/解密处理。

业务层生成的业务数据经数据层处理转化为标准的结构化数据，再经过数据的加密处理接入适配层，并经过区块链及“IPFS”节点完成数据传输。

区块链数据交互说明

区块链数据交互是基于“证联链”节点通过区块链监听服务获取“证联链”链上数据。“证联链”基于Fabric1.4为底层建构，基于Fabric SDK实现区块监听服务，具体逻辑如下：

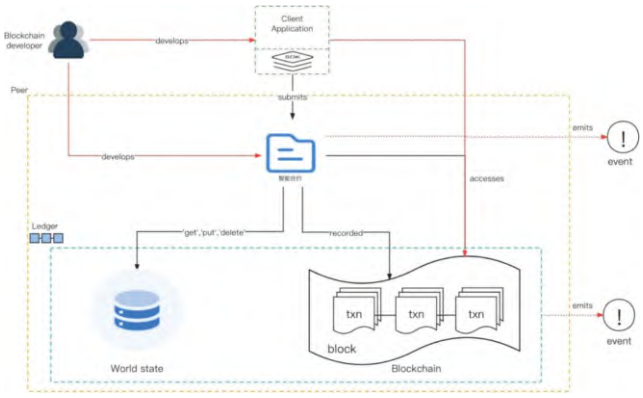


图2 区块监听逻辑图

客户端（Fabric SDK）与Peer节点通过gRPC进行通讯：

1.Fabric SDK提供了BlockEvent，可以用来监控被添加到账本上的区块，区块链每产生一个区块，Fabric SDK都会接收到通知。

2.BlockEvent事件有2 种类型：

1）Filtered：事件订阅时默认的类型，指获取的信息“不全”；

2）非Filtered：指可以获取完整的区块、交易、链码事件信息；

3.注册事件需要使用EventClient，并可以指定事件订阅Option，3个Option的介绍如下：

Option	描述
WithBlockEvents()	事件为非“filtered”，会向调用 Fabric SDK 的客户端发送完整的区块，可以获得订阅事件完整的信息。
WithSeekType	可以指定从某个区块高度获取事件
WithBlockNum	指定区块高度

4.客户端(Fabric SDK) 中通过实现一个 Dispatcher 将应用中的事件注册请求转换为事件订阅请求并通过 DeliverClient 发送给 Peer 节点，Peer 节点中的 DeliverServer 接收订阅请求，调用 deliverBlocks 进入循环，从 Ledger 读取区块并生成事件，最后发送给客户端，客户端中的 Dispatcher 又将其转换为应用订阅的事件响应，如下图所示：

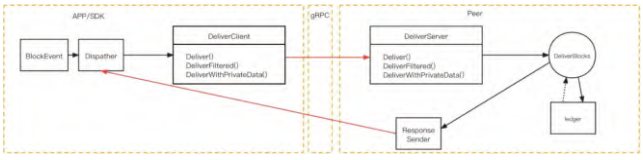


图3 客户端订阅事件响应过程

5.向“证联链”节点报送数据需调用链上智能合约进行数据校验。

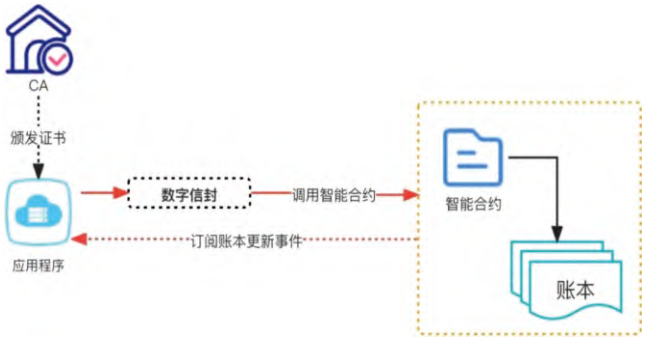


图4 数据报送流程

依据证监会《证券期货业密码应用与创新发展实施方案(2018-2022年)》要求，“证联链”全面采用国密算法，证券公司需对Fabric SDK和区块链底层进行国密化改造，涉及到的改造点包括：

1.基于Fabric 1.4.2版本进行改造；

2.摘要算法需为国密SM3算法；

3.签名验签算法需为国密SM2算法；

4.需支持验证“证联链”提供的国密数字证书，作为节点身份准入控制；

5.需使用基于国密算法的TLS加密通讯。

基于商密体系的证联链建设主要包括以下方面的内容：①基于商密体系的身份认证机制；②基于商密体系的密钥安全措施；③基于商密体系的信息安全指南；④基于商密体系的数据验证方法；⑤基于商密体系的隐私保护等级；⑥基于商密体系的数据存储规范；⑦基于商密体系的硬件支持系统。作为面向广泛国内证券期货行业领域服务的证联链的重点是在安全性层面需要确保对商密系列算法的支持。目前Hash 算法广泛应用于区块链工作量证明中，每个具有创新性的区块链项目中均有各自不同的实现，属于区块链中比较核心和基础的技术。主流公有链中的主要非对称加密算法主要采用 RSA 算法，下面主要论证这两种算法的商密替代性。为了保障商用密码的安全性，国家密码管理局商用密码管理办公室制定了一系列密码标准，包括SM1(SCB2)、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法（ZUC） 等等。其中，SM1、SM4、SM7、祖冲之密码(ZUC)是对称算法；SM2、SM9是非对称算法；SM3 是哈希算法。目前，这些算法已广泛应用于各个领域中，期待有一天会有采用商密算法的区块链应用出现。其中 SM1、SM7 算法不公开，调用该算法时，需要通过加密芯片的接口进行调用。

采用商密体系中 SM3 作为证联链的摘要算法区块链可以用于登记和发行数字化资产、积分等，并以点对点的方式进行转账、支付和交易。由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序不可能完全一致。因此区块链系统需要设计一种机制对在差不多时间内发生的事务的先后顺序进行共识，这种对一个时间窗口内的事务的先后顺序达成共识的算法被称为“共识机制”。现有的共识机制包括 Pow、Pos 和 DPos 等，其中 Pow 是相对安全最高的公链共识算法。现有的比特币即采用 Pow 共识算法芯片，在比特币系统中，矿工为了挖掘新的 Block(数据区块)必须进行并完成工作量证明过程。矿工计算每个数据区块头部信息的 SHA256 值 (HASH 值的一种)，如果比前一个数据区块的 SHA256 值小，那么P2P网络便接受这个新的数据区块。目前比特币已经吸引了全球大部分的算力，其它再用 Pow 共识机制的区块链应用很难获得相同的算力来保障安全。在对国内外各类共识机制和共识算法芯片进行调研的基础上，研究了 SM3 共识算法，算法流程如图 1 所示。SM3 密码摘要算法是国家密码管理局商用密码管理办公室 2010 年公布的中国商用密码杂凑算法标准，SM3 算法是在SHA256 基础上改进实现的算法，采用 MerkleDamgard 结构，消息分组长度为 512 位，摘要值长度为 256 位。此算法对输入长度小于 2 的 64次方的比特消息，经过填充和迭代压缩，生成长度为 256 比特的杂凑值，其中使用了异或，模，模加，移位，与，或，非运算，由填充，迭代过程，消息扩展和压缩函数所构成。SM3 密码杂凑算法的压缩函数与 SHA256 的压缩函数具有相似的结构，但是 SM3 算法的压缩函数的结构和消息拓展过程的设计都更加复杂，压缩函数的每一轮都使用 2 个消息字，消息拓展过程的每一轮都使用 5 个消息字等。基于 SM3 共识算法芯片保证更高的安全性，与此同时，由于 SM3 算法与 SHA256 算法结构相似，可以与 HASH256芯片使用统一的处理模型，只是针对各运算单元分别进行重构设计，有效地节约资源。SM3密码杂凑（哈希、散列）算法适用于商用密码应用中的数字签名和验证，消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。

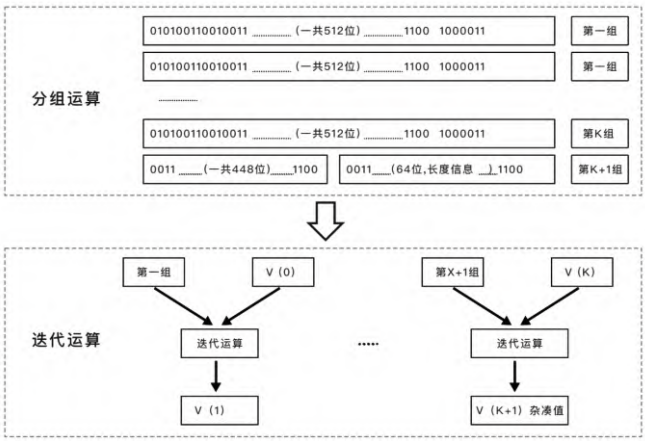


图5 Sm3算法流程

证联链使用 SM3 杂凑算法进行摘要计算，由于 SM3 是在 SHA-256 基础上改进实现的一种算法，因此虽然 SM3 算法的压缩函数与 SHA-256 的压缩函数具有相似的结构 ，但是 SM3 算法的设计更加复杂，安全性也相对较高。

采用商密体系中 SM2 作为证联链的数字签名算法

传统区块链采用多重签名技术，这是为了更好的保障交

易双方的权益，多重签名交易的地址可以有多个相关联的私钥，最常见的是2/3 的组合，所谓 2/3 指的是多重签名交易的地址可以有三个相关联的私钥，交易者需要其中的两个才能完成一笔转账。多重签名技术所能带来的最大好处即保证了交易的安全性，交易的多方均可以看到资金的安全存储，只有双方均同意才可以转移资金，保证了交易各方的权益。但现有的多重签名交易不一定安全，当前多数情况下多重签名钱包以客户端网页应用出现，如果攻击者控制了交易平台的服务器，他们就有能力向用户输送错误的网页应用，这种多重签名方案并没有提供多重签名应有的安全保证，方案提供者在协议中扮演了客户端和服务器两个角色。

在对国内外区块链技术和区块链交易方法进行调研的基础上，研究确定了基于商密体系中 SM2 的多重签名交易方法。SM2 算法由国家密码管理局 2010 年 12 月 17 日发布，称为椭圆曲线算法，算法加解密流程如图 2 所示。SM2算法的安全性基于数学难题“离散对数问题”，使用 SM2 算法进行数字签名时，所要求的密钥长度比以往 RSA 要短。基于 SM2 算法的多重签名交易方法不仅使得用户和交易平台需要记忆和存储密钥更加便捷，验证速率加快，同时保证交易不受单方影响，即保证买卖双方的权益的同时使得平台也无法挪用交易资金，且外部不能通过攻击服务器来危险公链中经济安全。

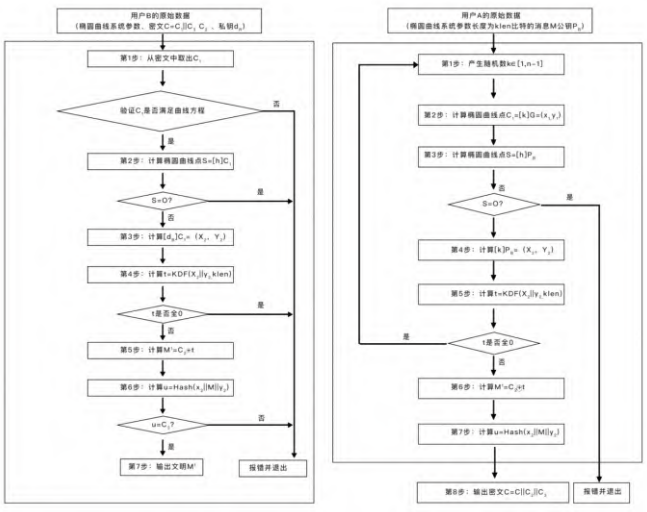


图6 Sm2加解密流程

证联链使用 SM2 椭圆曲线算法进行区块链公私钥密钥对的生成与签名验证，使得本身的计算复杂度达到了完全指数级，并且与传统区块链中所使用的 RSA 相比，同样的安全性能下所需的公钥位数更少，密钥的生成速度与加解密速度相较于 RSA 算法也快百倍以上。SM2 算法在很多方面都优于 RSA 算法（RSA 发展得早，应用普遍，SM2 领先也很自然），与 RSA 安全性对比如表 1 所示。

密钥安全性对比		
RSA 密钥强度（长度）	SM2 密钥强度（长度）	破解所需时间（年）
521 比特	106 比特	104（已破解）
768 比特	132 比特	108（已破解）
1024 比特	160 比特	1011
2048 比特	210 比特	1020
速度对比		
算法	签名速度	验签速度
1024RSA	2792 次/秒	51224 次/秒
2048RSA	455 次/秒	15122 次/秒
256SM2	4095 次/秒	871 次/秒

表1 SM2与RSA安全性对比

链上公私钥密钥对所使用的椭圆曲线非对称加密算法为SM2，区块链分布式账本记账中所使用的哈希杂凑算法则为SM3。通过我国自主知识产权的加密手段，实现了链上数据安全的有效保障。因此，证联链可以作为数据交换系统内置的安全保障机制，作为第三方安全认证平台的重要功能，在提供数据信息交换传输加密保障的同时，对数据本身进行提供认证、授权、防篡改、可溯源等高安全保障。基于商密体系的证联链整合共享交换应用中提供标记上链，通过数据标记的存证保全，就能够对各个节点的数据交换总量、当前运行状态、传输线路状态、数据交换进程状态、交换服务状态等进行有效监控溯源，并且还能在指定时间内按照进入 / 转出、目的地 / 来源地、数据量大小等项目对具体数据交换包进行查询和统计；通过对数据状态（例如等待交换、正在交换、交换完毕、回执收到、处理中断等）的监控，追踪某一个指定数据的状态。

P7数字信封在证券行业联盟链中的应用

P7数字信封是一种国际通用的加密标准，在证券行业联盟链中，通过对P7数字信封进行国密化改造，可以为数据安全提供重要保障。

国密化改造后的P7数字信封技术在证券行业联盟链中具有广泛的应用前景。它通过结合国密算法，对P7数字信封进行增强和改进，使其能够更好地满足证券行业的安全需求。

国密化改造后的P7数字信封技术提供了更高级别的加密算法。国密算法以其安全性和高效性而著称，通过将国际通用的P7数字信封与国密算法相结合，加密算法的安全性得到了进一步提升。这使得证券行业联盟链中的交易数据能够更可靠地加密，有效地防止未经授权的访问和数据泄露。

国密化改造后的P7数字信封技术还提供了更强大的数字签名功能。数字签名是验证数据在传输过程中是否被篡改的重要手段，确保数据的完整性和可信性。通过国密化改造，P7数字信封技术能够采用更安全的国密签名算法，为证券行业联盟链中的数据传输提供更可靠的保护。

国密化改造后的P7数字信封技术还具备高效性和兼容性

的优势。它能够在证券行业联盟链的各个节点间快速、安全地传输加密数据，并且与现有的证券行业系统和标准兼容。这使得证券行业的参与者能够更加便捷地采用和应用国密化改造后的P7数字信封技术，提升整体的数据安全水平。

国密算法在证券行业联盟链中的应用案例

国密算法在证券行业联盟链中有广泛的应用。它可以提供加密通信、数字签名、密钥管理、数据加密和解密，以及安全审计等功能，从而有效地增强联盟链系统的安全性和可靠性。国密算法的应用可以帮助证券行业实现安全的交易和合规的运营，促进行业的发展和创新。

加密通信：证券行业联盟链中的参与方需要进行安全的通信，以保证信息的机密性和完整性。国密算法提供了高效、安全的加密算法，可以用于加密联盟链参与方之间的通信。参与方可以使用国密算法中的对称加密算法，如SM1、SM4，来加密通信内容，以防止信息被窃听和篡改。

数字签名：在证券交易中，参与方需要对交易数据进行签名，以确保交易的真实性和不可否认性。国密算法提供了强大的数字签名算法，如SM2。通过使用SM2算法，参与方可以生成和验证数字签名，以确保交易数据的完整性和可信度。

密钥管理：密钥管理是证券行业联盟链中的关键任务之一。国密算法提供了一套完整的密钥管理机制，包括密钥生成、分发、存储和更新等功能。通过使用国密算法的密钥管理机制，参与方可以安全地生成和管理加密算法所需的密钥，确保密钥的安全性和合规性。

数据加密和解密：证券行业联盟链中的数据需要进行加密存储和传输，以保证数据的保密性和完整性。国密算法提供了高效、安全的数据加密算法，如SM4。参与方可以使用SM4算法对数据进行加密，同时使用对应的解密算法进行解密操作。这样可以有效地保护数据免受未经授权的访问和篡改。

安全审计：证券行业联盟链中的交易和操作需要进行安全审计，以确保系统的合规性和安全性。国密算法提供了安全审计机制，可以对交易和操作进行记录和审计，以便进行后续的安全分析和溯源。通过安全审计，可以发现潜在的安全风险和漏洞，并及时采取措施进行修复和改进。

主要创新

本研究的主要创新点包括：

1. 行业特定场景国密算法应用解决方案：针对证券期货行业特定需求，研究并选择最合适的国密加密算法，提供行业特定场景的加密解决方案。

2. 制定行业密码应用标准接口：通过研究行业密码应用的标准化需求，制定适用于证券期货行业的密码应用标准接口，促进加密算法的一致性和互操作性，降低系统集成和应用开发的复杂度。

3. 构建安全可靠的数据传输与共享机制：结合区块链、IPFS、数字信封等技术，构建安全可靠的数据传输和共享机制，确保数据在跨系统和跨组织间的传输和存储过程中的安全性、完整性和可追溯性。

4. 国密算法与数据隐私保护的结合：研究并设计出基于国密算法的链上数据隐私保护方案，有效保护联盟链中的数据隐私。

5. 国密算法与区块链快速检索的结合：研究并设计出在区块链上基于国密算法的关键字快速检索方案，提升联盟链检索效能。

6. 推进国密算法在行业区块链技术中的标准化工作：通过实验和验证，推动现行国密算法的标准化工作，为行业区块链技术应用提供统一的技术规范。

结论/总结

证联链以国家密码管理局要求的SM2、SM3和SM4等国产密码算法为基础，遵从算法的规范、格式要求、协议规范以及算法标准提供算法服务。证联链对通讯数据进行加密和签名保护，利用数字信封等技术手段保障敏感数据在交互双方的存储和传输过程的安全可控。系统中主要在密钥生命周期管理、哈希散列管理、签名验证管理、加解密功能等方面进行商用密码改造：

1）密钥生命周期管理

非对称加密算法采用国家密码管理局认可的SM2算法，正确地传递参数，即可正确地使用SM2算法库，以API函数方式提供给各层调用执行，SM2算法主要用于对数据的加密、解密和对身份信息的签名、验签等。

2）哈希散列管理

哈希算法采用国家密码管理局认可的SM3算法。SM3算法主要是对大量的数据进行摘要，将重要私密数据进行杂凑后，配合SM2使用。

3）签名验证管理

签名验签工作存在于整个交易过程中，涉及中间的每个节点，整个生命周期中，客户端、背书节点、排序节点、提交节点都参与了签名或者验签工作。证联链采用国家密码管理局认可的SM2算法提供签名验签功能。

4）加解密功能

证联链使用国家密码管理局认可的SM2算法提供非对称加解密功能，使用国家密码管理局认可的SM4算法提供对称加解密功能。

5）BCCSP

BCCSP全称是区块链密码服务提供者，用来提供区块链相关的算法标准和实现。BCCSP模块为区块链的上层模块提供密码学服务，它包含的具体功能有：对称加密和非对称加

密的密钥生成、导入、导出，数字签名和验证，对称加密和解密、摘要计算。

国密算法在证券行业联盟链中的应用进行了研究和探讨。通过对国密算法和P7数字信封技术的概述，我们了解到国密算法在加密通信、数字签名、密钥管理和数据保护等方面具有重要的优势。在证券行业联盟链中，国密算法可以为数据安全性、可信度和可靠性提供有效保障。

通过分析证券行业联盟链的安全需求，我们认识到证券行业面临的安全挑战和隐患，并发现国密算法在解决这些问题上具备独特优势。国密算法可以有效保护交易数据的机密性、完整性和可用性，确保联盟链中各参与方的安全交互和数据共享。

然而，国密算法的应用仍然面临一些挑战，如标准与互操作性、安全性与保护、性能与效率以及国际合作与交流等方面。为了克服这些挑战，需要进一步研究和改进国密算法，制定国际化的加密算法标准，并加强与国际组织和其他国家的合作与交流。

尽管存在挑战，国密算法在证券行业联盟链中的应用仍具有巨大的潜力和发展空间。通过不断改进和创新，国密算法可以为证券行业的数字化转型和创新发展提供可靠的安全支持。

共建共享、协作共赢的合作态度，协会与证券期货经营机构等共同承担证联链服务行业的职能，共同建设基于证联链的金融科技应用，共同拓展共识、共信、共生数字证券业务，共同打造服务监管自律、服务行业高质量发展、服务市场规范发展的高水平联盟链，携手构建符合证券行业特点的创新型区块链基础设施。

商用密码在证券期货业个人信息保护探索

文丨白小勇

北京炼石网络技术有限公司

摘　要： 金融事关发展全局，证券期货业个人信息安全管理刻不容缓。证券期货业的特点是数据规模大、数据价值高、数据应用场景复杂，客户个人信息、交易、行情、资讯等海量数据在其业务系统中高速流转，其业务持续性和安全性决定着整个交易系统的运转。同时，证券期货业务场景所具有的特殊性与复杂性，也使得监管侧对数据与个人信息安全和系统自主可控性要求更为严格。商用密码作为数据安全防护的核心手段，可为证券期货业个人信息保护重新定义虚拟的“防护边界”，在不影响业务要求的数据流动和共享的情况下，实现证券期货业个人信息安全实战化防护。

关键字： 证券期货业、个人信息保护、商用密码、数据安全、实战化防护

引言

随着数字化建设的不断演进，证券期货业高度依赖网络与信息系统，业务系统承载着海量金融用户个人信息，这使得数据安全问题日益凸显，加强数据安全建设迫在眉睫。在全面了解证券期货业网络与信息系统安全状况的基础上，不影响业务要求的数据流动和共享，设计出基于商用密码技术的数据安全保护方案，才能有效保障用户个人信息安全。

证券期货业务系统个人信息安全分析

个人信息安全面临挑战

随着大数据、云计算、区块链和人工智能等新技术应用的不断深入，证券期货业务与技术加速融合，各类业务活动日益依赖网络安全和信息化，信息化系统对证券期货业务的支撑作用日益突出，数据成为新的价值资源的同时，也增加了数据和个人信息安全管理的复杂度。证券期货市场是一个典型的以信息为主导的市场，我国中小投资者数量近1.77亿，投资者个人信息往往涉及金融账户信息、投资能力信息等敏感内容，这些信息一旦泄露往往会导致极大的经济损失，进而影响经济和社会稳定[1]。合法适度的用户个人信息收集、流动等，可以有效促进证券期货业的商业发展、预防金融犯罪。但必须正视的是，实践中已经出现的越来越多的用户个人信息被泄露、滥用和盗用的情况。

1. 个人信息安全威胁分析

证券期货业信息系统内部存储的大量包含了用户等个人信息的敏感数据，而这些数据在整个生命周期中都面临安全风险。风险主要来自以下几个方面：

(1) 存储数据的威胁

攻击者可从服务端入手，窃取集中存储的数据（包括数据库中的结构化数据以及文件系统中的非结构化数据），在内部没有安全防护措施的情况下，风险极大。

(2) 数据防篡改威胁

数据在分发过程中，攻击者可能截取数据并篡改内容后，再发给数据的接收方，而数据接收方无法识别文件是否被篡改，文件的内容是否还是数据发送方的原意，存在接收错误信息的风险。

(3) 应用内面临威胁

攻击者可以从数据库或者文件服务器直接窃取敏感数据。

(4) 上云的泄露威胁

上云已经成为目前证券期货业数字化转型的主要内容之一，但每个上云用户都会担心敏感数据上传到云端的安全问题，云设施无法由用户物理掌控，数据存在泄露的风险。

(5) 访问控制被绕过

数据在服务端可直接窃取，绕过访问控制也可以将数据进行窃取，同时审计置信度较低，这既会带来数据泄露的威胁，也是对安全机制本身的破坏。

2. 个人信息安全建设难题

如何实现在用户个人信息流动的同时，做好安全保护工作，是金融期货业亟待解决的问题。已建成的应用系统往往缺失个人信息安全保护的能力，需要补充和增强。在个人信息安全改造方面，主要需解决以下难题：

(1) 系统不能大变动，全面改造增强安全无望

证券期货业信息化建设往往已经投入巨额资金，并且已经上线运行为客户和业务部门提供在线服务。如果以开发改造的方式，为其信息化系统增强和补充安全能力，特别是加入密码能力，要从应用底层架构入手，就需要继续投入大量人力物力，而且需要较长周期。同时，对在线运行的应用系统进行改造切换会带来运营风险，造成间接业务损失。

⑵积累数据量巨大，安全建设如何无碍效率

证券期货业务系统中掌握着大量国内外客户的姓名、手机号、证件号等个人信息，数据量以亿条计，而且每时每刻都在高速流转，采用密码技术对证券期货业应用系统的数据进行安全保护时，不能影响到数据的流转效率，从而影响到相关金融投资业务的正常开展。因此，对所采用密码的性能提出了很高的要求。

⑶数据库品牌多样，增加数据安全保护难度

在不同阶段建设的应用系统，或者直接采购的成套应用系统产品，带来机构内部多个品牌数据库并存的情况，而且相同品牌的数据库的版本也不统一，要针对每个品牌和版本的数据库进行个人信息安全保护，就需要落地的方案能够支持每一种数据库，而每个品牌、每个版本的数据库都进行各自的安全保护，从成本和后期维护工作量上，对于证券金融机构来说往往是难以接受的。

⑷开发技术不统一，使得密码技术落地更难

各个时期建设的应用系统由不同的开发商供应，所使用的应用开发技术不统一，比如有JAVA、.NET、PHP等技术，要实现个人信息安全防护，就要对接不同的开发技术，实现密码技术与应用系统的结合，从而实现为应用系统中的数据提供安全防护。

用户信息安全实战需求

针对以上分析，为有效化解针对包括用户个人信息在内的敏感数据面临的安全风险，并有效应对用户信息安全建设中的诸多挑战，证券期货业在个人信息安全防护工作中存在以下具体需求：

1. 对敏感数据加密

为加强针对数据资产的保护，防范数据被窃取的威胁，维护机构和企业的声誉和利益，需要使用密码技术对数据进行安全保护。

2. 策略集中易管控

对于分布于各个应用系统中的敏感数据，在进行安全保护过程中所各自执行的安全策略，需要进行集中管控。平台要能够集中设置多个应用的加解密策略，并能够设置按照时间限制的管控策略。

3. 应用免开发改造

通过应用开发改造的方式来实现数据和个人信息安全防护，需要投入大量的工作，而且已经上线运行的系统经过安全底层的改造，会影响到正常业务的开展。因此，理想的状态是应用系统免改造的方案周期短、风险低。

4. 加解密须高性能

数据在共享中，大数据量的高速流转。因此，需要平台具备高性能的加解密能力。

5. 服务具备高可用

为保持证券期货服务业务的持续不间断，为各个应用系统提供数据和个人信息安全服务的平台需要具备高可用的特性。

6. 兼容各种数据库

在改造中，不可能针对每个数据库都要实现一种专门的方案，需要一种方案无关数据库品牌和版本，并以统一方式实现数据库中的数据安全，而其中的数据既包含传统的基于SQL 的数据库，如 Oracle、SQL Server、MySQL 等，也要支持 New Sql 的新型数据库，如 MongoDB。

7. 统一管理可扩展

数据来源于各种业务应用系统的采集和产生，并在各个应用系统和业务部门之间流转，建设的数据加解密平台能够统一管理各个信息系统的安全功能，并且随着信息化的发展，对于新建设的系统也能够纳入统一平台管理的范围内。

8. 建密码防护体系

通过顶层规划，面向证券期货信息化建设的全局，构建个人信息安全密码防护体系，建设数据加解密及去标识化服务平台，持续为证券期货服务业务的运营保驾护航。

9. 使用密码须合规

采用密码技术实现个人信息安全的同时，证券期货机构需要遵循国家密码管理局对于密码应用合规性方面的要求，使得实施方案能够通过由国密局认可的密评机构的密码安全性评测。

个人信息保护合规需求

自2018年欧盟《通用数据保护条例（General Data Protection Regulations）》（“GDPR”）正式生效实施以来，合规和风险的驱动使得数据保护的重要性日益受到重视，人们更加清晰地认识到数据能够产生的价值和可能带来的危害。

个人信息作为数据资源的重要组成部分，应该受到严格保护。个人信息处理者掌握着控制信息的主动权，只有规范个人信息处理行为，才能保障个人信息权益。实际调研证实，以往作为信息处理者的企业，在保护个人信息方面重视不够，投入不足，安全建设滞后于业务功能建设。出现个人信息安全事件后，企业责任不清晰。

1. 法律明确数据保护的必要性

在数字中国建设的顶层战略规划下，防范证券数据安全风险，全面保障用户个人信息安全，这一工作任务日益艰巨且迫切。近年来，我国陆续出台个人信息保护相关法律及其配套政策规章对数据安全和个人信息保护建设提出明确要

求。

《网络安全法》《密码法》《数据安全法》和《个人信息保护法》为保障数据安全夯实了法律基础。2021年正式施行的《数据安全法》、《个人信息保护法》，就“数据安全保护义务”“个人信息处理规则”“个人信息跨境提供的规则”“个人在个人信息处理活动中的权利”“个人信息处理者的义务”“履行个人信息保护职责的部门”，以及相关各方的“法律责任”做出了明确界定。两法统筹私人主体和公权力机关的义务与责任，兼顾个人信息保护与利用，为个人信息保护工作提供了清晰的法律依据[2][3]。个人信息安全建设已经由“或有”变为“刚需”，个人信息处理者应依照法律法规相关要求，采取技术措施，加强个人信息保护，使个人信息在安全的前提下，可以被有效开发利用。

聚焦重要数据和个人信息保护，基于以上“四法”进一步延伸出“四例”，分别为《关键信息基础设施安全保护条例》《网络安全等级保护条例（征求意见稿）》《商用密码管理条例》《网络数据安全管理条例（征求意见稿）》，在技术和管理等方面对数据合规提出明确指引和要求。可以预见，后续各级单位和各行各业也将不断完善各级法律法规和政策制度，推动统一公平、竞争有序、成熟完备的数据经济市场发展。

2. 行业监管督促数据安全保护

针对证券期货业个人信息安全保护和监管，我国积极制定出台相关的行业规范和要求指南，促进商用密码技术健康发展。

2022年底，证监会发布《证券期货业数据安全管理与保护指引》，从数据安全管理基本原则、组织架构、制度、技术等方面提供指引，规范行业机构开展数据安全管理和保护工作，提升行业数据安全管理水平。

2023年1月，中证协下发《证券公司网络和信息安全三年提升计划（2023—2025）》征求意见稿，提出33项重点工作，明确：加强数据安全管理体系建设，在2023年底前建立个人信息保护制度体系，在明确数据权责的基础上，对数据进行分类分级，并以数据全生命周期安全防护要求为重点，构建目标明确、职责清晰、层次分明、落地性强的制度规范。

2023年3月，证监会发布《证券期货业网络和信息安全管理办法》，对网络和信息安全管理提出规范要求，并结合违法违规的具体情形，规定相应罚则。数据安全和个人信息保护方面，《办法》明确要求建立健全投资者个人信息保护体系和管理机制；明确安全信息发布和行业数据备份中心相关要求；要求核心机构和经营机构在本机构网络安全防护边界以外处理投资者个人信息的，应当采取数据脱敏、数据加密等措施，防范化解投资者个人信息在处理过程中的泄露风险。

密码安全一体化新防护思路

个人信息安全需兼顾内外威胁

总体上看，证券期货业个人信息安全面临的风险主要来自两方面。一是外部威胁与对抗的持续升级，黑客可以利用网络漏洞，远程窃取数据库中的敏感数据，同时，新兴技术演进也带来了不可预知的安全风险；二是来自内部的安全风险，机构和企业内部工作人员有工作之便，存在无意泄露或出于商业目的，有意倒卖包括用户个人信息在内的敏感数据的可能，即传统安全体系存在的固有问题。

数据安全乃至网络安全的本质，始终是攻击者和防御者之间的战斗，证券期货业因为拥有海量高价值的数据和用户信息，将会成为攻击者和防御者的重要战场。未来存在大量不确定性，证券期货业将会持续面临新的、不断演化的数据安全威胁与挑战。

网络与数据并重安全防护思路

传统的数据防护主流思路是应对式防御，通常是系统遭受了攻击后，根据攻击情况采取行动，即“以网络为中心”的数据安全，主要是保护被传统物理网络多层包围的数据，包括且不限于：传统杀毒软件、基于特征库入侵检测、病毒查杀、访问控制、数据加密等手段，这种防护体系仅适用于保护静态数据，“滞后于攻击手段”的弊端明显。直接针对数据本身进行主动式防护，通过加密和去标识化等技术为需要保护的数据穿上“防弹衣”，能够更有效增强对数据本身的防护能力，即“以数据为中心”采取措施，是实现数据安全的最直接有效的手段。以网络为中心的安全体系是保证数据安全的前提和基石，而以数据为中心的安全，是以数据为抓手实施安全保护。因此，网络与数据并重的安全建设成为大势所趋（见图1）。

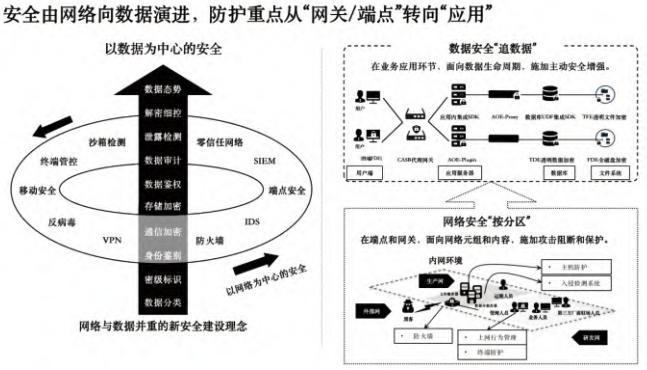


图1 网络与数据并重的安全建设思路框架部署示意图

以密码为核心构建防护体系

密码是数据安全的基石

密码技术是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务[4]。

密码是网络安全的杀手锏技术和核心支撑，是保护网络与信息安全的重要手段[5]，是网络信任的基石。利用密码在安全认证、加密保护、信任传递等方面的重要作用，能够有效消除或控制潜在的“安全危机”，实现被动防御向积极防御的战略转变。密码在网络安全防护中具有保底作用，是最后一道防线。密码技术可以实现当前OSI网络安全架构的“鉴别、访问控制、机密性、完整性、抗抵赖”等5种基本安全服务。

在以数据为中心的主动式数据安全防护体系中，密码技术提供了重要价值。比如：识别方面，密码可以为数据识别提供身份安全能力，为接口通道实现安全加密；防护方面，数据加密技术本身就是在开放式信道中，构建了强制的防护措施，并结合身份实现访问控制。检测、响应、恢复和反制方面，密码也能够为其分别提供身份鉴别、数据保护、水印追溯等不同能力。

安全技术从应对到主动

证券期货业目前的数据防护主流思路仍然是应对式防御，“应对式防御”的弊端比较明显，在应对拟人化以及精密化的攻击时，很容易被攻击者快速发现漏洞，并针对薄弱点进行精准攻击，难以适应时代发展，难于达到数据安全和个人信息保护的目的。

互联网难以避免的各种先天缺陷和日趋复杂的应用，以及网络广泛脆弱性成为常态。“找漏洞、打补丁、防病毒等被动式防御、局部式治理、增量式修复，已不能适应多变的网络安全形势。网络安全日益强调全域安全，强信任、强安全、强可控、强防护成为必然要求，必须以规范使用国家认可的密码技术为基础，以系统性、整体性和协同性为原则，构建以密码为基石的网络空间新安全[6]。”

从防御角度看，网络漏洞在所难免，“应对式防御”难以从根本上解决问题，必须更新思路，聚焦于核心保护目标“数据”，采取基于密码的系列技术手段，建立主动式防护机制才是解决问题的有效办法。

2019年12月1日起正式实行的等级保护2.0标准，在1.0的标准基础上，更加注重主动防御，建立事前、事中、事后全流程的安全可信、动态感知和全面审计，一方面实现对金融证券业务系统、基础信息网络的等级保护，一方面实现对云计算、大数据、物联网、移动互联网等新兴技术下的等级保护对象的全覆盖。

安全产品从外挂到内嵌

边界往往是数据安全防护的焦点。从安全能力来看，个人信息在流动过程中没有边界，通过将数据放在一个安全增强点上进行加密，人为塑造一个数据边界，然后在解密点上再结合用户身份进行脱敏等访问控制，将数据安全防护从游离于业务的“外挂式”，提升到融合业务的“内嵌式”，从而构建出“防绕过”的访问控制、高置信度的访问审计，并基于此打造新一代安全产品，不仅能实现保护个人信息不受外部攻击，也能防范内部业务人员的越权访问，实现降低重标识风险，兼顾个人信息的安全性和有用性。

安全机制从单点到纵深

在数据安全防护过程中，不存在一招制敌的战法。只有建立防御纵深，凭借先发优势、面向失效的设计、环环相扣的递进式设防，才能铸造出有效的防护网。

1. 建立先发优势

为了对抗体系化的攻击，防御体系的设计应用好“先发优势”，针对威胁行为模式，提前布置好层层防线，综合利用多种手段，实现各个维度防御手段的纵深覆盖，让进攻者在防守者布局的环境中“挣扎”。

2. 面向失效设计

面向失效的设计原则是指，任何东西都可能失效，且随时失效。需要考虑如前一道防御失效了，如何补上后手。面向失效设计的整体思路是：从传统静态、被动的方式转向积极体系化的防御纵深模式。分析进攻者的进入路径，打造多样化多层次递进式的防御“后手”。

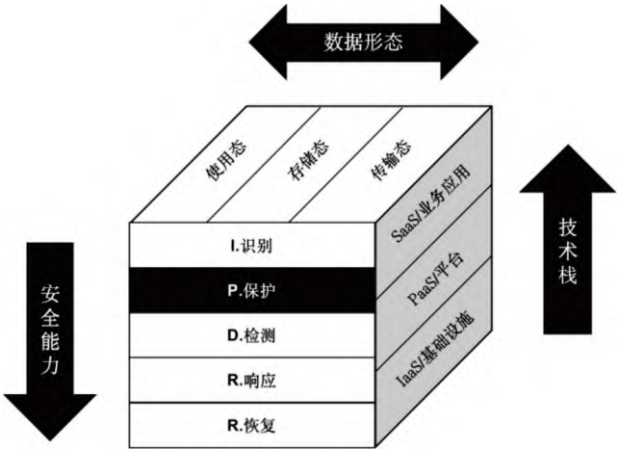


图2 面向失效的数据安全纵深防御新战法

基于面向失效的防御理念，从几个重要维度层层切入，当一种保护手段失效，设计好后手应对，综合利用多种手段，打造纵深协同。如图2，这里选择三个比较重要的维度，一是安全能力维度（I.识别、P.防护、D.检测、R.响应、R.恢复、C.反制），二是数据形态维度（使用态、存储态和传输态等），三是技术栈维度（SaaS/业务应用、Paas/平台、IaaS/基础设施），这三

个维度之间关系是独立的、正交的，三者叠加可构建有效的数据纵深防御体系。

3. 安全纵深防御

“纵深防御”是一种应该体现在数据安全防御体系设计各个方面的基本原则，而不是一种“可以独立堆叠形成的解决方案”。

⑴ 多层堆叠不等于防御纵深

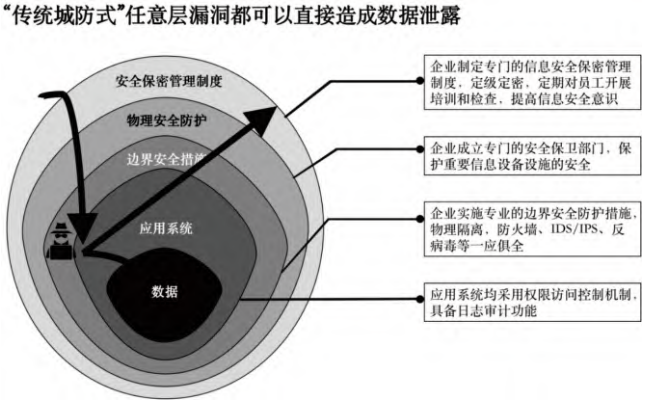


图3 “传统城防式”数据安全防护架构图

传统的安全防护是城防式的（见图3），为了保护核心数据，在多个层面进行控制和防御。实际上任意层漏洞都可能直接造成数据的泄漏，导致之前建设的所有的安全手段就会瞬间瓦解。

多组件系统实现“模块纵深”防御覆盖时，必须实现可信可靠、环环相扣的组件间安全交互机制，才能确保构建的是纵深防御。结合业务流程设置多道防线，有助于阻断攻击获利环节。密文信息的解密环节可重点防护，信息系统在加密等防御保护措施基础上，对解密操作等行为重点监控，可能给攻击获利环节造成难度，甚至形成威慑。

⑵ 从多个维度分别构建数据纵深防御

①从安全能力构建数据防御纵深

“IPDRRC”体现了数据保护的时间顺序，基于时间维度，可以有机结合多种安全机制。识别是一切数据保护的前提，在数据识别、分类分级和身份识别的前提下，针对数据安全威胁的事前防护、事中检测和响应、事后恢复和追溯反制等多种安全机制，环环相扣，协同联动，可以有效构建出面向失效的纵深防御机制。

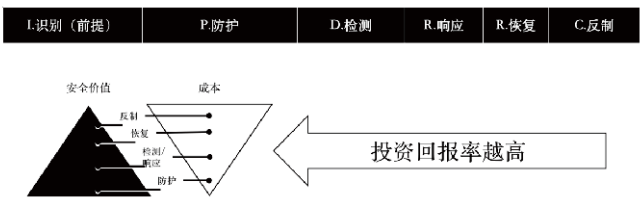


图4 从安全能力构建数据防御纵深的投资回报率分布图

从当前证券期货业的数据安全和个人信息保护建设重点看，如图4越靠近“事前防护”，投资回报率越高，如果仅依靠检测/响应、恢复以及反制等环节，损失已经发生，可能会因此付出更高成本。

②从数据形态构建数据防御纵深

数据状态大致可以分成传输态、存储态和使用态，而身份鉴别及信任体系则是对数据访问的补充或者前提，基于“数据三态”可延伸出数据全生命周期。围绕数据形态，可以构建多种安全机制有机结合的防御纵深。结合20种密码应用模式（见图5），采用IPDRRC中数据防护段的密码技术，可以进行数据形态维度的纵深防御构建。

图5 20种常见密码应用模式一览

在信息系统中，数据在传输、存储、使用等不同形态之间的转化，在此过程中，可以利用多种安全技术构建协同联动的纵深防御机制。

③从技术栈构建数据防御纵深

信息系统的技术栈体现了空间维度，这也可以作为数据保护的纵深。沿着数据流转路径，在典型B/S三层信息系统架构（终端侧、应用侧、基础设施侧）的多个数据处理流转点，总结出适用技术栈不同层次的数据保护技术。综合IPDRRC中数据防护段的密码技术、数据存储态和典型信息系统的技术栈分层，可以从技术栈维度构建数据防御纵深。

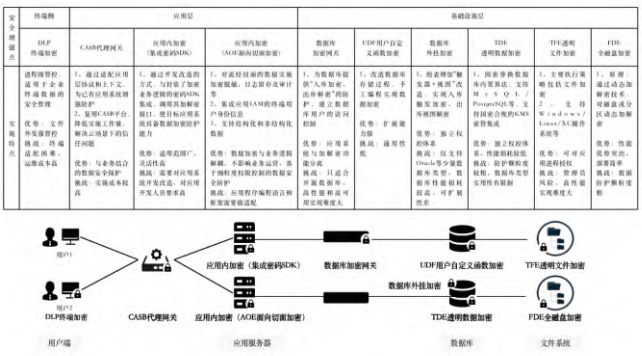


图6 覆盖不同技术栈的数据存储加密技术

如图6列举了10种数据存储加密技术，在应用场景以及性能优势方面各有侧重：DLP终端加密技术侧重于企业PC端的数据安全防护；CASB代理网关、应用内加密（集成密码SDK）、应用内加密（AOE面向切面加密）侧重于企业应用服务器端的数据安全防护；数据库加密网关、数据库外挂加密、

TDE透明数据加密、UDF用户自定义函数加密则侧重于数据库端的数据安全防护；TFE透明文件加密、FDE全磁盘加密则侧重于文件系统数据安全防护。其中，覆盖全量数据的FDE技术可作为基础设施层安全标配。针对特别重要的数据，再叠加AOE等技术实施细粒度加密保护，两者的结合可以面向技术栈构建出数据防护纵深。

综上所述，从安全能力、数据形态、技术栈等多个不同维度上，有机结合多种安全技术构建纵深防御机制，可以形成兼顾实战和合规、协同联动体系化的数据安全和个人信息保护新战法。

个人信息安全体系建设落地

数字化转型升级为证券期货业提高效率，降低成本提供了极大助力，也对机构和企业的管理支撑系统提出了更高要求，需要进一步提升管理系统运作效率、提高业务透明度、加强业务管控。然而，在个人信息安全体系实际建设落地中，由于证券期货业业务特性，导致项目实施痛点重重，如待保护的数据量达到亿级，且数据存在形式多、访问人员众多、存储分散、易传播；开发改造应用叠加数据安全，周期长、难度大、风险高；信息系统环境复杂，涉及字段类型多、数据库种类多，涉及分库分表、存储过程、模糊查询等使用场景；加解密过程不可影响或中断正常业务的运行；需要满足合规要求，同步提升机构和企业安全运维管理能力。

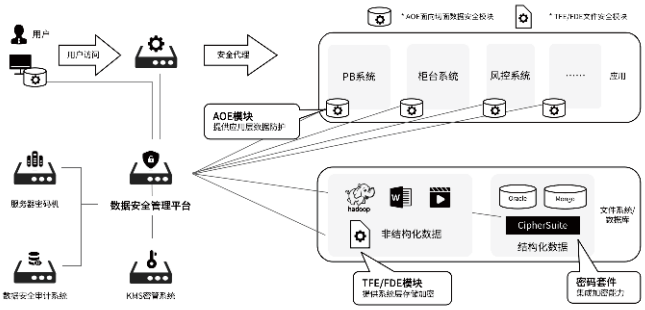


图7 部署模式：统一平台下的多控制点，对数据精准识别和保护

基于上述密码安全防护一体化思路，炼石打造满足金融行业安全建设实战需求方案，该方案已经在副部级金融央企、大型金融保险服务集团、全球前三大信用卡组织、商业银行等多个大型金融机构落地，实战化防护金融重要数据与个人信息安全。依托自主研发的AOE加密模块、TFE透明文件加密模块，打造免开发改造应用的数据保护、高性能密码产品，面向复杂应用系统，快速实施密码安全一体化的全面数据保护。方案通过构建高覆盖率的安全增强点组合，无需开发改造应用代码，实现批量系统的应用数据加密需求，重构数据防护边界，强化企业自身“免疫力”，为证券期货业客户和员工个人信息安全提供强力保障。同时，充分考虑国家法律法规、行业规范等政策需求，个人隐私数据保护、商用密码信息系统密码应用规范要求，全面保障数据和业务的安全运营。基于纵深防御体系建设落地的基本思路，具体来说，需要落地实现以下基本功能，以保障用户个人信息安全。

保障业务性能与安全兼备

用户信息在证券期货业务系统中流转，在实现数据的高效流转的同时，也带来安全挑战。传统的磁盘存储加密技术虽然对业务性能影响不大，但颗粒度较粗，很难有效保护数据。客户端侧的加解密技术，会给客户使用造成不便，同时影响数据的高效流转。分级隔离技术虽然能够有效管控数据风险，却会间接影响数据的共享。

要兼顾数据流转与安全防护，最好的方法是将加密等数据安全能力融合到业务流程中，可以根据证券期货实际的业务场景，制定针对性的数据安全保护方案；同时，机构和企业需要采用高性能的密码技术，将安全机制与用户的现有流程无缝对接，在不改变用户的操作习惯，不伤害用户粘性，不影响数据的流转性能的前提下，实现两者之间的动态平衡。

兼顾多形态数据安全防护

证券期货业的海量价值数据，不仅仅包括传统数据库中的结构化数据，同时涵盖了文档、图片、视频、音频等大量高价值的非结构化数据。想要构建覆盖结构化与非结构化数据的纵深防御，可以采用AOE面向切面技术与TFE透明文件加密等多种加密技术结合，通过优势互补的方式，实现数据的全方位保护。

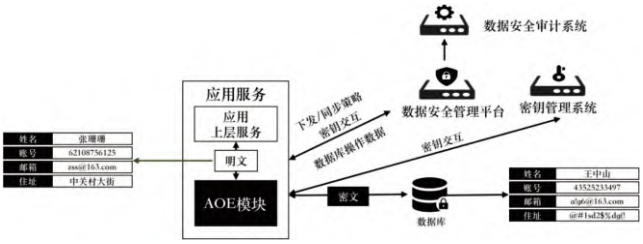


图8 AOE面向切面加密技术原理

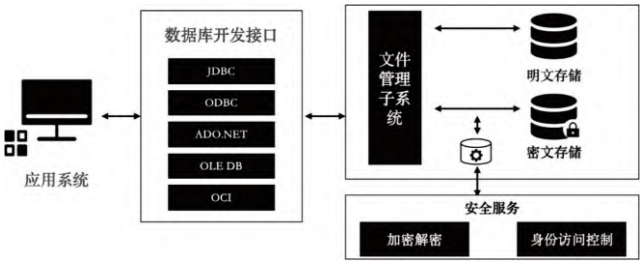


图9 TFE透明文件加密技术原理

对于结构化数据，可以采用AOE面向切面加密技术（如图8），其实现原理是将数据安全插件部署在应用服务中间件，并结合旁路部署的数据安全管理平台、密钥管理系统，通过

拦截入库SQL，将数据加密后存入数据库；对于非结构化数据（如图9），可以采用TFE透明文件加密技术，其实现原理是在操作系统的文件管理子系统上部署加密插件来实现数据加密，并基于用户态与内核态交付，实现“逐文件逐密钥”加密。

应用安全技术不影响业务运行

证券期货业务涉及的数据量往往非常庞大，在安全保护实现的过程中，如果影响到业务系统的正常运转，将会导致大量用户的权益受到损害。传统技术路线一般会基于密码机硬件设备提供SDK对金融投资业务系统进行密码整改，一方面给信息系统的应用开发人员增加了负担，一方面也带来了较大的业务风险。

基于AOE面向切面加密技术的特性，结合TFE透明文件加密等安全技术，证券期货业可实现整体安全方案的免开发改造敏捷实施，使安全与业务系统在技术上解耦，在能力上融合交织，最终实现批量化快速部署实施。在确保方案安全可靠的前提下，可以实现方案在多场景、多地域下的快速复制，从而能够实现安全能力的快速升级迭代，以更好地适应新技术下的安全挑战。

建立数据访问防绕过机制

很多数据泄露事件源于重要数据在数据库或备份的过程中被盗取，访问控制被不法分子利用网络或权限漏洞绕过，从而获取到海量价值数据。证券期货业在构建个人信息安全防御体系的过程中，有必要考虑建立基于数据安全的防绕过机制。

在密码技术的基础上，将访问控制、审计等多种安全技术相结合，通过部署独立性的数据访问审计，使每条日志都支持追溯到具体业务用户，并可以为审计日志提供完整性保护，从而实现数据泄露后可追溯源头，形成“以加密技术为核心，融合数据识别、防护、检测/响应、追溯等多种安全技术”的个人信息安全保护体系，解决了访问控制容易被不法分子轻易绕过的问题。

结语

本文分析了当前证券期货业在用户个人信息保护工作中所面临的挑战，结合国家的相关法律法规、前沿的数据安全防护理念以及高性能商用密码技术，针对证券期货业提出“网络”与“数据”并重的安全建设思路，设计出多维度、多种安全技术有机组合的纵深防御战法，以期为证券期货业加强包括用户个人信息在内的敏感数据安全防护提供参考。

参考文献

1.证券期货业网络安全新规发布https://legal.zgswcn.com/article/202303/202303281111531054.html

2.中华人民共和国数据安全法[J].中华人民共和国全国人民代表大会常务委员会公报，2021(05):951-956。

3.中华人民共和国个人信息保护法[J].中华人民共和国全国人民代表大会常务委员会公报，2021(06):1117-1125。

4.中华人民共和国密码法[J].中华人民共和国全国人民代表大会常务委员会公报，2019(06):912-916。

5.白小勇.合规与实战推动密码产业发展[J].信息安全与通信保密,2021(01):92-98。

6.霍炜.构筑以密码为基石的智能时代新安全[J].网络空间安全,2018,9(05):23-26+31。

证券行业加密业务安全风险监测与防御技术研究

文丨闫伯龙、马冰、江旺

闫伯龙 北京观成科技有限公司
马　冰 海通证券股份有限公司
江　旺 华泰证券股份有限公司

摘　要： 为解决证券行业加密流量威胁问题、加密流量中的应用风险问题，对若干证券行业的实际流量内容进行调研分析，分析了证券行业加密流量面临的合规性风险和加密协议及证书本身存在的风险、以及可能存在的外部加密流量威胁，并提出防御策略和措施。

关键字： 证券加密业务、加密应用、加密流量、商用密码安全评估、加密风险、加密威胁、监测防御

概述

数据爆发式增长的DT(Data technology)时代，加密技术是数据传输的重要保护手段。随着互联网和企业内部流量场景的加密化趋势快速增长，证券行业也面临着更加迫切的加密需求。证券行业涉及的加密业务种类繁多，因此如何实现有效的安全运维、风险监控和威胁检测成为亟待解决的问题。

据谷歌透明度报告统计，94%的谷歌浏览器流量为加密流量 。据观成科技评估，企业内部加密流量占比也达到80%。证券行业性质特殊，涉及国家金融安全、客户个人隐私和财产安全，加密需求相比其他业务场景更突出、更急迫，因此证券行业流量加密化的趋势更加明显和普遍。证券行业业务繁杂，包涵用户鉴权业务、交易结算业务和资产管理业务等，涉及的加密应用众多，这些加密应用产生大量不同加密协议、不同加密算法的加密流量。

从政策和法规层面考察，为保障国家商业机密安全和数据安全，国家制定和颁布了一系列政策法规，包括《网络安全法》、《密码法》等。具体到金融行业，2022年11月25日，中国人民银行正式发布《金融行业信息系统商用密码应用》系列金融行业标准，包括《金融行业信息系统商用密码应用 基本要求》（JR/T 0255—2022）、《金融行业信息系统商用密码应用 测评要求》（JR/T 0256—2022）和《金融行业信息系统商用密码应用 测评过程指南》（JR/T 0257—2022）三项金融行业标准。上述法律、行业标准针对证券行业加密应用的密码使用、加密传输等进行了详细规范，并对网络安全等级保护、商用密码安全评估提出了落实和监管要求。

考虑到网络安全的对抗特性，安全风险管理与防御技术必将与相应的攻击技术交替攀升。因此除等保、密评等固化要求外，证券行业必须考虑自身业务中存在的其他加密风险，避免因此类额外风险带来的系统和业务完整性、机密性、可用性、可控性及不可否认性破坏，做到防患于未然。除此之外，伴随证券业务加密化增多的趋势，各种使用加密流量进行攻击、窃密和远程控制的恶意威胁也逐年递增。根据知名零信任厂商Zscaler历年统计，截至2022年，超过85%的网络攻击行为采用的是加密方式，同比2021年增长20% 。常见境外APT组织攻击绝大多数已经转向加密方式传递信息，攻防演练场景中常用的扫描暴破、漏洞利用、远程控制和代理转发等工具也大量使用各种加密协议进行加密。除传统明文检测能力外，针对加密流量构建加密威胁检测能力，也成为证券行业亟待解决的问题之一。

在本文中，我们建议对证券行业的加密业务进行梳理，明确各类加密协议、加密算法、加密数据格式以及业务特点。在此基础上，评估其合规加密风险和其他加密风险，并开展风险监控与缓解工作。同时，针对恶意加密威胁，需要分析恶意加密流量的特点，并根据证券行业业务特点构建对应加密威胁检测防线，以确保证券业务的安全、稳定运行。后续章节将深入探讨上述问题，并提供进一步的研究建议。

证券行业加密业务调研

为调研掌握证券行业现有加密流量概况，观成科技联合华泰证券、海通证券，以部分业务流量作为分析样本，数据分析情况如下：

整体概况

数据采集时间为2023年6月12日，共采集5000万帧。其中IP帧49999774帧，非IP帧226帧，非IP帧包含ARP(23帧)、LLC(130帧)、LLDP(42帧)和SLOW(31帧)等链路协议。IP帧中约97.36%为TCP协议，UDP占2.57%，另外有ICMP、OSPF、VRRP等协议，占比极小。以数据量统计，TCP协议占比为98.82%，UDP占比为1.17%。IP帧数、字节数情况表如下所示：

	帧数	帧占比	字节数	字节占比
TCP	48681233	0.9736	34436707242	0.9882
UDP	1284076	0.0257	406686111	0.0117
ICMP	33661	0.0007	3639112	0.0001
VRRP	427		29036	
DATA	297		415916	
OSPF	68		12128	
IPv6	12		1320	

表1 IP协议分布情况

值得注意的是，有297帧，共415916字节不明数据，需要进一步研究其数据性质。

协议分布调研

1. TCP协议分布

样本流量中TCP协议承载公开标准协议65个，约占TCP协议总帧数的52.14%，总数据量的33.55%。占比较高的15项协议分类为远程登录协议、数据库协议、数据传输协议、设备管理协议和加密传输协议。头部15个协议仅有两个非加密协议，其他均为加密或部分加密。这也印证了上文中关于加密流量占比较大的描述。TCP协议占比详表如下所示：

协议分类	是否加密	是否公开	帧数	帧数占比	字节数	字节数占比
远程登录协议 1	加密	公开	2391610	0.0692	2456785189	0.0871
远程登录协议 2	非加密	公开	446883	0.0129	532311318	0.0189
数据库协议 1	加密	公开	3481310	0.1007	2475663785	0.0878
数据库协议 2	非加密	公开	559267	0.0162	114377784	0.0041
数据库协议 3	加密	公开	191650	0.0055	103952272	0.0037
数据库协议 4	加密	公开	26468	0.0008	42768779	0.0015
数据传输协议 1	加密	私有	16538724	0.4786	18736990575	0.6645
数据传输协议 2	部分加密	公开	945624	0.0274	1094982178	0.0388
数据传输协议 3	部分加密	公开	2339032	0.0677	602260401	0.0214
数据传输协议 4	加密	公开	346668	0.0100	370138495	0.0131
数据传输协议 5	加密	公开	47693	0.0014	81127769	0.0029
数据传输协议 6	加密	公开	38484	0.0011	65762207	0.0023
数据传输协议 7	部分加密	公开	12696	0.0004	3914871	0.0001
设备管理协议	加密	公开	886602	0.0257	415129083	0.0147
加密传输协议	加密	公开	490871	0.0142	540042450	0.0192

表2 TCP协议分布情况

以HTTP协议为例，经过统计发现，正常承载文字、图像和媒体业务的HTTP协议流量只占HTTP总流量的48%，有2.33%的HTTP载荷无法识别格式，可能是HTTP隧道利用。剩余约50%的HTTP流量，实际上是作为隧道承载其他协议，常见协议有SSL、POP、HTTP等，其中绝大部分是SSL加密流量。

	帧数	帧占比	字节数	字节占比	加密	隧道
xml	12788	0.0356	8211195	0.0264	明文	否
data-text-lines	69078	0.1924	43678546	0.1405	明文	否
json	89893	0.2503	52643156	0.1694	明文	否
mime_multipart	10105	0.0281	17730592	0.0570	明文	否
image-gif	463	0.0013	428971	0.0014	明文	否
media	12666	0.0353	18704150	0.0602	明文	否
text	14	0.0000	36970	0.0001	明文	否
image-jfif	1618	0.0045	2043793	0.0066	明文	否
png	1775	0.0049	2164800	0.0070	明文	否
data	8060	0.0224	7228925	0.0233	部分加密	可能
pop	427	0.0012	507488	0.0016	明文	是
smpp	2	0.0000	1560	0.0000	明文	是
dcerpc	43	0.0001	112327	0.0004	加密	是
ocsp	6	0.0000	3470	0.0000	明文	是
ssl	150368	0.4187	157140541	0.5056	加密	是
http	1798	0.0050	183815	0.0006	明文	是

表3 HTTP协议应用分布情况

除公开标准协议外，在样本流量的TCP通信中，占据最大比重的是私有协议流量，约占总数据量的66.45%，总帧数的47.86%。考虑到样本流量中绝大多数是TCP流量，这也意味着约三分之二的流量是各种业务、应用所产生的私有协议数据，这些数据是哪些应用产生的，数据如何加密、是否有加密风险和安全风险，都有待梳理研究。

2. UDP协议分布

样本流量中UDP占比较少，仅占总数据量的2.57%。UDP流量中公开标准协议有15个，按分类统计头部协议包含通信控制协议、数据库协议、数据传输协议、设备管理协议、域名解析协议和其他功能性协议，其他协议占比均不超过UDP协议总数据量的1%。除公开标准协议外，69.70%的UDP流量无法识别上层协议，应为各类证券业务所产生的私有协议数据，其中部分数据可能加密。UDP协议占比详表如下所示：

协议分类	是否加密	是否公开	帧数	帧数占比	字节数	字节数占比
域名解析协议	非加密	公开	69290	0.0540	9905862	0.0244
通信控制协议 1	非加密	公开	14908	0.0116	8545155	0.0210
通信控制协议 2	加密	公开	23088	0.0180	3138349	0.0077
通信控制协议 3	非加密	公开	62		21572	
数据库协议	非加密	公开	635	0.0005	184896	0.0005
数据传输协议 1	部分加密	私有	722429	0.5626	283466768	0.6970
数据传输协议 2	部分加密	公开	404736	0.3152	88121811	0.2167
数据传输协议 3	非加密	公开	18372	0.0143	9967145	0.0245
数据传输协议 4	非加密	公开	2244	0.0017	660034	0.0016
数据传输协议 5	非加密	公开	2181	0.0017	233367	0.0006
数据传输协议 6	非加密	公开	755	0.0006	67502	0.0002
数据传输协议 7	非加密	公开	5		450	
设备管理协议	非加密	公开	6		588	
其他协议 1	非加密	公开	23310	0.0182	2236992	0.0055
其他协议 2	非加密	公开	457	0.0004	32598	0.0001
其他协议 3	非加密	公开	2		390	

表4 UDP协议分布情况

综合上述针对TCP、UDP两大传输层协议的分析可知，样本流量具有如下两个显著特点：

· 在公开标准协议中，加密协议数据量占比超过70%；

· 近三分之二的流量为私有协议数据，其中包括私有加密流量。按照50%的私有协议数据被加密估算，业务流量中加密流量占总数据量约60%。

TLS协议加密流量调研

1. 应用分析

样本流量中TLS协议数据约为540M字节，共27824次加密会话，涉及Server Name Indicator共61个，其中大多数为公开网页。因此判断样本流量中的TLS协议数据为互联网浏览或操作系统、软件升级流量。在TLS协议数据中，我们识别了一系列加密资产，如企业邮箱服务、云计算平台、云开发平台和统一数平台等，同时也发现了一系列与证券行业相关的应用信息，如各类证券分析应用、证券交易应用、证券信息平台等。

2. 风险分析

本次调研针对TLS流量风险也进行了初步评估，评估重点主要放在TLS证书和TLS协议规范方面，针对入联和出联两种情况进行评估。

综合入联与出联TLS协议两类流量分析，目前业务流量中TLS协议数据存在的主要风险包括：

· 使用自签名证书：无法验证身份，可能面临中间人攻击；

· 证书链校验失败：无法验证身份，浏览器告警；

· 证书过期：无法验证身份，浏览器告警；

· 证书即将过期：如果不及时更新则证书将会失效；

· 证书SAN与客户端SNI不匹配：证书颁发或服务器配置错误；

· 客户端支持弱密码套件：使用较老SSL库，需要更新；

· 服务端选择弱密码套件：数据加密强度弱，可被快速破译；

· 客户端SNI泄露服务端IP：信息泄露风险；

· 加密套件与证书不匹配：TLS协议实现或服务器配置错误。

从数据量上看，入联流量中，涉及自身资产的风险流量占比较大，约为47%，外联流量异常较少，约为7%。这种分布差异与企业内部网络服务器配置不规范、证书不规范等因素相关。通过风险评估，我们也初步识别了内部网络中存在的各类加密风险，为下一步规避风险工作打下良好基础。

调研小结

本次调研针对两家证券公司部分业务流量进行分析，初步厘清了内网加密与非加密流量协议类型、占比情况，并针对TLS协议加密流量应用和风险情况进行了初步分析。经过调研，我们有如下认识：

证券行业业务流量加密化趋势明显。在所调研的流量中，存在大量标准加密协议数据和私有协议加密数据。梳理清楚其中不明或未知加密流量格式、性质和业务归属，对于实现加密流量安全运维管控至关重要。

证券行业业务流量中存在一定加密风险。这些风险可能是因为内部应用研发实现失误、加密服务配置错误以及加密基础设施更新不及时等因素引起，如不及时排查解决，将会造成数据泄露、被破译等严重后果，需要引起足够重视。

证券行业加密业务面临的安全风险及应对策略

合规加密风险

在证券行业中，加密应用和加密服务的安全合规性评估至关重要。随着密码“一法三规一条例”（《密码法》、《国务院办公厅关于印 发国家政务信息化项目建设管理办法的通知》、《贯彻落实网络安全等 级保护制度和关键信息 基础设施安全保护制度的指导意见》、《关键信息基础设施安 全保护条例（征求意见稿）》、《商用密码管理条例》）以及国标GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》的出台，促进了密码产业及技术的发展，商用密码技术不断推陈出新，其普及、推广与应用也随之增长。密码使用的合规性、正确性、有效性成为了国家及企业关注的重点。《密码法》第二十七条规定法律、行政法规和国家有关规定要求使用商

用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估（密评）是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。

加密应用方面，商用密码评估主要涉及客户隐私加密、交易数据加密、财务数据加密等方面的评估，确保核心业务加密合规。加密服务方面，商用密码评估主要涉及以下几点：

· 通信协议评估：需要规范使用符合密码评估要求的安全通信协议，以保证业务通信过程中的安全性。

· 加密算法评估：需要选择足够强的加密算法对数据进行加密。如是否按照相关法规和规范使用国密算法等。

· 访问控制和审安全审计评估：需要建立完善的访问控制机制，对员工和客户的访问进行严格控制，并记录访问日志和操作记录，以便对安全事件进行审计和追溯。商用密码评估需要对访问控制和审计机制的可靠性和安全性进行评估，确保访问控制和审计的有效性和完整性。

根据相关标准逐条映射，可归纳出密码评估需求对应加密资产的评估点和评估方法，部分评估项如下图所示：

异常类型	协议	规则描述	规则详情	测评指标	应用要求	网络和通信安全	设备和计算安全	应用和数据安全
证书	通用	证书过期		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
证书	通用	自签名证书		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
证书	通用	证书RSA公钥长度小于2048bit		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
证书	通用	证书RSA公钥指数小于256		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
证书	通用	证书RSA公钥末位为0		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
证书	通用	证书采用未定义签名算法		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
证书	通用	证书采用未定义加密算法		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
证书	通用	证书采用非国密签名算法		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
证书	通用	证书采用非国密加密算法		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
身份	通用	证书链校验不通过		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
协议	ISAKMP	使用IKEv1		通信数据完整性	宜	8.2.b)	8.3.c)	8.4.f)
协议	ISAKMP	IKEv1使用野蛮模式		通信过程中重要数据的机密性	应	8.2.c)	8.3.d)	8.4.d)
协议	AH	使用AH传输数据		通信过程中重要数据的机密性	应	8.2.c)	8.3.d)	8.4.d)
协议	ESP	载荷未加密	载荷随机性差	通信过程中重要数据的机密性	应	8.2.c)	8.3.d)	8.4.d)
协议	SSL	TLS版本过低	使用SSL 2.0、	密码技术	应	8.2	8.3	8.4
协议	SSL	TLS版本未定义	使用未定义的协	密码技术	应	8.2	8.3	8.4
协议	TCP/UDP	自定义加密		密码技术	应	8.2	8.3	8.4
算法		采用弱加密算法	DES、RC4	通信过程中重要数据的机密性	应	8.2.c)	8.3.d)	8.4.d)
算法		采用弱公钥算法	RSA（不足2048	身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
算法		支持弱加密算法	DES、RC4	通信过程中重要数据的机密性	应	8.2.c)	8.3.d)	8.4.d)
算法		支持弱公钥算法	RSA（不足2048	身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
算法		采用非国密加密算法		通信过程中重要数据的机密性	应	8.2.c)	8.3.d)	8.4.d)
算法		采用非国密摘要算法		通信数据完整性	宜	8.2.b)	8.3.c)	8.4.f)
算法		采用非国密公钥算法		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)
算法		支持非国密加密算法		通信过程中重要数据的机密性	应	8.2.c)	8.3.d)	8.4.d)
算法		支持非国密摘要算法		通信数据完整性	宜	8.2.b)	8.3.c)	8.4.f)
算法		支持非国密公钥算法		身份鉴别	应	8.2.a)	8.3.a)	8.4.a)

图1 密码安全评估方法

如果商用密码评估结果表明存在不符合项，证券公司需要及时采取措施进行修复，以保证客户和公司的数据安全。此外，商用密码评估结果也可以帮助证券公司选择更加安全和可靠的加密技术和服务，有效保障业务正常运转。

其他加密风险

如前所述，除等保、密评等固化要求外，证券行业必须考虑自身业务中存在的其他加密风险，避免因此类额外风险带来的系统和业务完整性、机密性、可用性、可控性及不可否认性破坏，做到防患于未然。这类额外加密风险主要来自如下3个方面。

1. 加密证书安全风险

加密证书是PKI体系最重要的一环，用于保护数据安全和隐私。证书通常由数字证书机构颁发，用于验证证书持有者的身份并授权他们访问受保护的资源。加密证书的安全风险主要包括以下几个方面：

· 有效性风险：是指服务端或客户端证书有效性异常，包括证书已经过期、尚未生效、即将过期和有效期过长等风险。

· 信任链风险：是指证书颁发过程中的异常，包括证书链校验失败、证书自签名、叶子证书可颁发等风险。

· 机密性风险：是指用于身份验证的公钥算法或签名算法存在异常，包括使用RSA、DSA或ECC算法的密钥过短、使用MD5、SHA1等已被证明存在弱点的摘要算法等。在需要使用国密证书的场景下，如果证书未采用国密算法，也将产生异常。此外，各类加密算法参数必须正确，如RSA公钥模数必须是大质数乘积等，否则将产生异常。

· 完整性风险：是指用于验证的身份信息和证书扩展等信息完整。如证书使用者通用名、国家、州、城市、部门等信息如果为空，则表示证书信息不完整。必要的证书扩展如密钥用法(Key Usage)扩展也不能缺失。

· 一致性风险：是指证书信息与使用场景存在不一致的异常。如某些协议场景下，要求证书具备数字签名功能，但是在对应的证书密钥用法列表中，并不包含数字签名(Digital Signature)用法，此时将产生异常。

2. 加密协议安全风险

TLS、SSH、RDP以及网络层的IPSec等加密协议，大致分为密钥协商和加密会话两大阶段。加密协议安全风险主要考察密钥协商阶段客户端与服务端协商行为，针对其中的异常点进行监控，识别加密协议安全风险。以TLS协议举例，主要包括如下几个方面：

· 机密性风险：主要包括客户端支持或服务端选择无加密套件、无认证套件和已知存在弱点的弱加密、弱摘要套件。在一些安全性要求较高的场合，还可以检测是否使用支持前向加密的加密套件。除加密套件外，TLS随机数在协议运行中发挥关键作用，如果多次会话中客户端或服务端出现随机数重用、主对方随机数相同和主对方短暂私钥重用等情况，也说明协议运行出现异常。在使用国密的场景下，需要对加密套件是否是国密算法进行检查。

· 一致性风险：主要包括根据协议规范不应该出现的协商交互。如在RSA密钥交换中出现Server Key Exchange消息，或者在ECDHE交换中未出现Server Key Exchange消息，就表明协商过程出现异常，有可能是服务端配置错误或TLS协议遭到篡改。另外，各类TLS扩展的协商中，如客户端提供ALPN扩展，但服务端并未在客户端支持的应用层协议中选取，也表明协商过程出现异常。

· 可用性风险：主要包括使用已知存在风险的协议版本等。如使用过低的TLS版本，使用未定义的协议版本，或者在协商过程中支持或使用已被证明存在缺陷的压缩等。

3. 加密通联安全风险

加密通联风险是指加密业务通联行为可能存在的安全风

险。加密通联风险与业务强相关，主要包含如下几个方面：

· 时间风险：时间风险是指与业务相关的加密通联发生的时间异常。如非交易时段产生加密的交易业务通联，证明交易系统存在异常等。

· 协议风险：协议风险是指与业务相关的加密通联出现不应出现的协议。如本应密传的业务出现明文协议，表明加密业务遭到破坏或篡改等。

· 目标风险：目标风险是指与业务相关的访问者或被访问者出现异常。如不应主动外联境外的加密资产发生境外访问，或本地服务被境外地址访问登录等。

· 流量风险：流量风险是指正常加密业务数据量出现极大变化。如加密服务下载量激增，如果是外部访问，则表明可能存在信息泄露风险，如果是内部访问，可能是内部安全风险等。

加密业务安全风险监测防御策略

加密业务安全风险危害严重，为了防范这类风险，关键是做到未雨绸缪，防患于未然。应从如下4个方面着手进行监测与防御：

· 尽快厘清自有加密资产、加密业务，包含标准加密协议和私有加密协议数据，做到对自己的加密流量了如指掌，才可能做到全面的风险识别。

· 根据自身加密资产和加密业务特点进行风险梳理，合规加密风险方面，根据国家相应法律、规定进行排查，其他加密风险方面，从加密证书、加密协议和加密通联三方面进行综合考察。针对业务中的私有加密协议，应对加密数据、加密算法等进行分析，识别其中的风险点。

· 根据第二步梳理的各类风险点，制定缓解措施并有效执行。

· 综合利用规则、基线、人工智能等技术，持续监控流量中可能新出现的加密业务安全风险。

证券行业加密业务面临的加密威胁及应对策略

加密攻击概述

证券行业企业面临的加密攻击威胁在网络攻击的多个阶段都有体现，攻击者在初始信息搜集、初始打点、横向移动、命中靶标等各个阶段，均会使用不同的加密通信手段隐藏攻击行为。

· 信息搜集阶段，攻击者通过互联网搜索引擎对域名和资产进行调查外，还会通过主动探测来收集开放在互联网上的系统服务和API接口信息，对于企业边界产生入联流量，例如针对HTTPS服务进行探测的加密流量。

· 初始打点阶段，攻击者可能通过对员工的社工钓鱼，以及对暴露资产的暴力破解、漏洞利用等方式攻陷某一台主机。这一阶段，站在企业视角会面临多种入联加密流量威胁，例如针对资产的SSH、RDP暴力破解和针对HTTPS站点的漏洞利用都会产生加密流量。

· 横向移动阶段，在建立初始据点后，大多数的情况初始据点权限不够或只是作为内网跳板，此时攻击者会进行横向移动持续获取权限。这个过程产生的加密流量可能包括：首先，横向移动技术本身涉及的信息搜集、渗透突破过程，会涉及SSH、RDP扫描暴破、漏洞利用等加密流量；其次，在横向移动的过程中，攻击者不可避免的要维持一条或多条内外连接通道，这类通道可能通过加密反弹木马、部署Webshell提供，也可以通过加密反弹Shell、加密代理转发等实现。

· 窃密控制阶段，攻击者拿下目标机器权限并成功窃取数据进行回传，会通过TLS木马回连、代理转发、隐蔽隧道等加密流量进行命令与控制、窃密回传等恶意行为。

入联加密攻击及防御策略

在渗透和后渗透阶段可能遇到不同的入联加密攻击：

· 在渗透过程中，加密流量多来自对暴露在互联网上资产的扫描探测与暴力破解，例如HTTPS扫描、漏洞攻击、SSH和RDP用户口令暴力破解等。

· 在后渗透阶段，获取shell后，会进行一系列持久化预置的动作，例如上传Webshell、正向代理等后门。

这些问题的本质都是对Web服务等业务主机不合常规的访问，所涉及的加密协议以HTTPS为主。针对入联加密攻击行为，通常有两种防御策略：一种是通过串联解密设备将访问Web服务的入联HTTPS流量解密后，还原载荷中的HTTP流量，再经过WAF、IDS等传统明文检测设备进行规则检测；另一种是不解密，直接经过旁路部署的加密流量检测设备，结合人工智能、指纹、流行为等技术，识别隐藏在加密流量中的恶意攻击行为。

入联加密攻击在渗透阶段和后渗透阶段会有不同形式的体现。

在渗透过程中，加密流量多来自对暴露在互联网上资产的扫描探测与暴力破解，例如HTTPS扫描、漏洞攻击、SSH和RDP用户口令暴力破解等。在渗透阶段获取shell后，会进行一系列持久化预置的动作，例如上传Webshell、正向代理等后门。这些问题的本质都是对Web服务等业务主机不合常规的访问，所涉及的加密协议以HTTPS为主。

针对HTTPS服务的扫描探测、漏洞攻击、Webshell连接等攻击行为，通常有两种防御策略：一种是通过串联解密设备将访问Web服务的入联HTTPS流量解密后，还原载荷中的HTTP流量，再经过WAF、IDS等传统明文检测设备进行规则检测；另一种是不解密，直接经过旁路部署的加密流量检测设备识别隐藏在加密流量中的恶意流行为。

在不具备解密条件时，可以通过对每一组IP对加密载荷在一个时间区间内时间与空间分布的特性，结合特定数学模

型进行验证，初步判断这些流量在行为特征上是否可能存在漏洞扫描、暴力破解等攻击行为。进一步对目标为Web服务的多条TLS流中存在的多次会话进行切割比对，从流量的时空特征的角度入手来对会话做区分，分出哪些是以传输、响应指令为主的流量，哪些是正常的访问浏览。最后，把认为不正常的这类流量再在现有的知识库中做对比以识别出真正的Webshell、正向代理类流量及其相关信息，如：事先搜集、研究、整理得到的工具静态特征、协议指纹进行二次判断，确定此次是否为攻击与攻击使用工具的具体的家族信息。

横向移动加密攻击及防御策略

横向移动阶段，主要为已经进入内网后针对内网资产加密服务的扫描探测，与入联阶段大部分相同，防御策略类似，但是由于内网渗透使用的工具与外网渗透有所不同，并且内网中的网络环境更为复杂，很可能有许多行为与扫描暴破类似的正常业务流量，所以要在防御筛查时更加严格，避免产生大量误报。

出联威胁加密攻击及防御策略

出联威胁主要涉及到两大类攻击者常用的命令与控制、窃密回传通道：远控木马加密通信和隐蔽隧道通信。

· 远控木马会使用HTTPS协议加密外联，将恶意流量混在出网的大量正常HTTPS流量中，从而逃避检测，还会利用代理转发、CDN、域前置等技术进一步隐藏其控制端基础设施。

· 另一大类是加密隐蔽隧道外联，指的是依托于不以加密通信为设计目的的常见标准协议之上，并自行设计加密方式通信的技术。如：利用DNS、ICMP、HTTP和一些特殊端口的TCP/UDP等会被防火墙放行的内对外流量中建立隐蔽隧道出网。

对出联加密通信木马的防御与检测通常可以借助人工智能技术以及限定域指纹、多流行为模型、加密威胁情报等辅助方法有机结合进行出联加密流量检测和预警。对于TCP、UDP、HTTP这类隐蔽隧道，可以通过针对自行设计的加密隧道流量载荷中，必定存在自定义结构的弱点，来设计一类一法对其做出检测和发现。

结论

证券行业的业务性质特殊，加密业务相较其他行业更加复杂和多变，因此证券行业对于加密业务的安全风险和威胁检测需求比其他行业更加迫切。在保护这些关键数据安全传输的过程中，证券行业必须应对加密风险监控和加密威胁检测的挑战。

为了应对这些挑战，有必要对资产和流量中不同类型的加密业务进行梳理，了解其各自的特点与应用场景。在此基础上，实现对合规加密类和其他加密风险的有效识别与防护。面对可能涉及证券行业加密业务的各类攻击场景，如攻防演练场景、APT对抗场景等，证券行业需建立一个覆盖入联、横向、出联全阶段的加密流量综合检测体系。

综上所述，我们需要针对证券行业的加密业务进行识别、监控和检测予以充分重视。通过全面梳理加密业务、建立完整的风险监控与威胁检测体系，以防范各类安全风险和安全威胁，有力提高数字化时代下的证券行业网络安全防护能力。

参考文献

1.Zscaler加密攻击报告（2022年）ThreatLabz State of Encrypted Attacks 2022 Report https://www.zscaler.com/blogs/security-research/2022-encrypted-attacks-report

2.谷歌透明度报告 Google Transparency Report https://transparencyreport.google.com

技术前沿

10 新技术应用

ChatGPT在网络安全领域的应用前景探索

文｜孟鑫

奇安信科技集团股份有限公司

摘　要： ChatGPT掀起了人工智能的新一轮变革，受到了多行业、多学科的广泛关注，也为网络安全领域带来的新的挑战和机遇，众多安全企业开展了相关探索和实践。目前，ChatGPT在网络安全领域的研究仍处于起步探索阶段。本文从ChatGPT给网络安全领域带来的可能威胁以及如何赋能网络安全防御能力升级两个方面，对ChatGPT在网络安全的应用研究进行了归纳总结。

关键字： ChatGPT、网络安全、双刃剑、威胁、防御

ChatGPT的发展概述

2010年之后，随着大数据、云计算、互联网、物联网等信息技术的发展，以深度神经网络为代表的人工智能技术飞速发展，大幅跨越了科学与应用之间的技术鸿沟，诸如图像分类、语音识别、知识问答、人机对弈、无人驾驶等人工智能技术实现了重大的技术突破，迎来爆发式增长的新高潮。

近年来，提出了预训练语言模型（Pre-training Language Model，PLM），即在大规模语料库中进行预训练，PLM在各种自然语言处理任务中展现出强大的能力，当训练参数规模超过一定量级时（GPT-3拥有1750亿参数），不仅能显著改善模型的性能，同时还会显示出在小规模模型中不具备的上下文学习能力，由此诞生了大型语言模型（Large Language Model,LLM）。

自GPT系列模型问世以来一直遵循相同的基本工作模式，采用的是基于casual掩码的解码器结构。第一代的GPT（generative pre-training）利用大量无标记数据预训练语言模型，通过Transformor的编码器学习上下文信息，通过Transformor的解码器生成下一个词，GPT-2和GPT-3模型在第一代基础上进一步扩大了训练数据集和参数规模，GPT-2的参数规模为15亿。GPT-3则达到了1750亿个参数，GPT-3虽然在多项任务重取得了很好地效果，但仍面临着会生成无用或虚假信息的问题。

为此OpenAI公司使用了人类反馈强化学习等微调技术对GPT-3模型进行了调整，并推出了ChatGPT模型，并在2022年11月正式推出，并迅速火爆全网，作为一种大型语言模型技术，展现出了巨大的语言理解和文本生成能力，以及上下文学习的特殊能力。因其具有强大的语料库、更高的计算能力、更加通用的预训练、更强的适应性和更高的准确性，被看做是一场新的生产力革命，受到了各行各业的广发关注。

成为网络安全产业创新赛道

以ChatGPT为代表的通用大语言模型同样可以应用于网络安全领域，并有望重新定义网络安全时代。通过对近5年创新沙盒发展和变化的分析，除云安全、数据安全、软件供应链安全、身份安全四个热门赛道热度持续外，智能应用和自动化异军突起，成为2023年的创新技术热点，随着ChatGPT的火爆，国内外众多安全企业开始投身于以ChatGPT为代表的大模型技术在网络安全领域的应用研究。

2023年（智能与自动化）			2022年（云原生安全）			2021年（数据安全）			2020年（供应链安全）			2019年（云安全）		
公司名称	国家	技术领域	公司名称	国家	技术领域	公司名称	国家	技术领域	公司名称	国家	技术领域	公司名称	国家	技术领域
AnChain AI	美国	数据DSPM	Araali Networks	美国	云原生安全（威胁管理）	Abnormal	美国	邮件安全	AppOmi	美国	云安全（SaaS）	ArKose Labs	美国	身份与访问安全（身份滥用）
Astrix	以色列	云身份安全	BastionZero.Inc	美国	身份与访问安全（零信任）	Apiiro	以色列	软件供应链安全（代码安全）	BluBracket	美国	软件供应链安全（代码安全）	Axonius	美国	网络安全资产管理
Dazz	美国	安全自动化	Cado Security	美国	云原生安全（数字取证与取证）	Axis Security	美国	身份与访问安全（零信任）	Elevate Security	美国	安全意识教育	Capsule8	美国	云安全（容器安全）
Endor Labs	美国	软件供应链安全管理	Cycode	以色列	软件供应链安全（代码安全）	Cape Privacy	美国	数据安全（隐私计算）	ForALLSecurity	美国	软件供应链安全（代码安全）	CloudKnox Security	美国	身份与访问安全（IDaaS）
HiddenLayer	美国	AI/ML网络防御	Dasera	美国	数据治理与运维（DataGovOps）	Deduce	美国	身份与访问安全（零信任）	INKY Technology	美国	邮件安全	DisruptOps	美国	云安全（云管理平台）
Pangea	美国	云安全平台及服务	Lightspin	以色列	云原生安全（云安全平台（CNAPP）	Open Raven	美国	数据安全（数据治理）	Obsidian Security	美国	云安全（SaaS应用安全）	Duality	美国	数据安全（数据应用）
Relyance AI	美国	数据数据安全与隐私安全	Neosec	美国	API安全（XDR）	Satori	以色列	数据安全（隐私合规）	SECURITI.ai	美国	数据安全（数据治理）	Eclypsium	美国	硬件及固件威胁预防
SafeBase	美国	可信通道平台	Sevco Security	美国	云原生安全（资产管理）	Strata	美国	身份与访问安全（IDaaS）	Sqreen	美国	软件供应链安全（开发安全）	Salt Security	美国	云安全（API保护）
Valence Security	以色列	安全自动化	Talon Cyber Security	以色列	安全浏览器	Wabbi	美国	软件供应链安全（开发安全）	Tala Security	美国	数据安全（隐私保护）	ShiftLeft	美国	软件供应链安全（开发安全）
Aama	法国	数据应用与隐私安全	Torq	以色列	安全运营（无代码自动化平台）	WIZ	以色列	云安全（无代理云安全平台）	Vulcan Cyber	以色列	云安全（漏洞管理和修复）	WireWheel	法国	数据安全（隐私计算）

图1 创新沙盒2019-2023年十强赛道分析

一方面，以ChatGPT为代表的生成式人工智能的应用也隐藏着众多潜在网络安全风险，可能构成严重的网络安全威胁。网络攻击者已开始使用ChatGPT来生成钓鱼邮件、恶意软件和其他网络攻击工具，代表着日益复杂的网络攻击能力在危险演化上又向前迈进了一步。

另一方面，作为一款强大的人工智能工具，ChatGPT也可以成为网络防御者的强大武器，提升网络安全领域的整体势能。人工智能可以被广泛应用于安全防御的各个环节，提升安全大数据的分析能力、威胁的发现能力、响应处置效率。可以预见，随着人工智能的不断发展，网络安全将从传统的人与人的对抗，演绎成人与机器的对抗，网络安全不仅是产品、

工具和平台间的互联互通，更是人员、工具、机器、自动化、人工智能等在内的创造和组合,以最高的效率实现最佳结果。

加深网络攻击的危险化程度

作为一种生成式人工智能，ChatGPT不仅能够替代人类完成部分重复性工作，同时能够通过自我学习产生新的内容，例如文本生成、内容创作、代码编写等。攻击者可以利用人工智能的语义理解和代码生成能力，生成基于文本的钓鱼邮件，开发基于编码的恶意软件，进行漏洞的挖掘和利用，实施自动化的网络攻击，使网络安全威胁形势愈加严峻。

开展网络钓鱼攻击

人是网络安全中最薄弱的环节。ChatGPT作为由OpenAI训练的大型语言模型，能够生成可用于多种用途的文本。其中一种用途是在社会工程攻击领域。社会工程攻击是一种依靠心理操纵来诱骗人们泄露敏感信息或执行某些操作的策略。这可以通过各种方式完成，比如网络钓鱼攻击。

由于ChatGPT擅长模仿人类书写对话并产生创新内容，使其可能成为强大的网络钓鱼工具。目前钓鱼邮件主要分为普通网络钓鱼和鱼叉式网络钓鱼，普通网络钓鱼的规模大，但由于形式通用易被发现。鱼叉式网络钓鱼利用社会工程，针对性地制定诱饵，规模小但成功率高。借助ChatGPT，攻击者可以更为简单、低成本地构造更具欺骗性、诱骗性的钓鱼邮件，如包含组织热点，可能关注的事件的邮件，驱使被攻击者点击钓鱼邮件。ChatGPT可以助力攻击者构建自动化的钓鱼系统，生成鱼叉式网络钓鱼邮件，提高攻击成功率。

用于恶意软件开发

ChatGPT还可以被攻击者用于恶意软件开发，生成恶意的攻击代码。ChatGPT本身会设置被恶意利用的规则，但攻击者仍能绕开和规避ChatGPT为防止滥用而设置的规则。例如，网络攻击者可以利用ChatGPT创建远程访问木马、信息窃取器，攻击者不需要具备太多的编程能力，只要向ChatGPT简单描述所需的功能，就可以得到相应的恶意代码。攻击者借助人工智能的代码编写能力，可以更简单低成本地发起网络攻击。

攻击者还可以利用暗网上或开源库中的恶意代码对ChatGPT进行模型训练，生成可逃避病毒检测的恶意代码的不同变体，或使用ChatGPT创建恶意软件配置文件并设置命令和控制系统。

潜在漏洞挖掘利用

ChatGPT可以用于代码分析和缺陷发现，发现输入代码中可能存在的缺陷漏洞，并针对性地生成攻击代码，攻击者可以快速实施攻击。相较于传统的漏洞发现工具，ChatGPT具有更大的数据输入作为安全知识库，同时具备更好的上下文理解能力，能给深入分析代码间的逻辑，发现漏洞并生产漏洞利用代码。

隐含数据泄露风险

国内的类ChatGPT架构远未到成熟阶段，不可避免的存在AI漏洞，容易被攻击者利用，对数据进行污染，加入伪装数据或者恶意样本，即所谓的“数据投毒”，造成算法模型结果的错误，进而导致巨大的数据安全隐患。

从数据安全与个人隐私的角度来看，ChatGPT与各种用户进行交互，交互信息可能被用于进一步训练ChatGPT，可能会产生敏感信息、个人信息、商业机密在未经数据主体同意的情况下被共享的风险。

企业在应用ChatGPT模型训练时，也需要输入大量数据进行迭代训练，输入数据如果包含有机密信息，也可能造成敏感数据泄漏的风险。

推动网络安全防御能力升级

ChatGPT同样被用于安全防御能力的提升，人工智能和机器学习技术可以大幅度提升对威胁情报和安全数据的分析能力，流量和日志的安全检测能力，安全事件的自动化调查、分析、研判能力，以提升安全运营效率。安全企业可以将这些能力应用于终端安全、数据安全、安全运营和攻防对抗等领域，可以帮助安全企业开发更多基于行为而非规则的安全工具，赋能安全产品，以发现更多的高级威胁，助力网络安全防御能力升级。

提升威胁情报分析能力

作为一种生成式人工智能，ChatGPT具有极强的文本生成、上下文学习和知识理解的能力，通过将ChatGPT与威胁情报等安全大数据深度融合，可以极大地提高为威胁情报的分析能力，有助于安全企业从海量威胁情报中挖掘有效信息，提高情报的有效性和准确性，从而增强预测能力，提高威胁发现能力。

1.提高对威胁情报上下文信息的分析能力

时效性和上下文信息是影响威胁情报实际应用效果的两个重要属性，人工智能和机器学习技术的发展，改变了依靠人工获取和处理威胁情报的传统，通过算法和模型自动化地处理和分析大量的文本、语音和图像等数据，自动识别数据中的关键信息，深度理解上下文信息，威胁情报分析和处理

的速度和准确度得到了提高，进一步增强了威胁情报的时效性和有效性。

2.提高对非结构化情报数据的处理能力

人工智能处理威胁情报时，往往只能处理结构化数据，而无法处理非结构化数据，这就导致了信息不全面，从而产生漏报。以ChatGPT为代表的大语言模型具备千亿级的训练参数，结合安全企业自身积累的大量安全大数据，可以对模型进行不断优化，提升对威胁情报中非结构化数据的处理能力，大幅度减少漏报误报可能性。

3.在ALPHA 威胁分析平台中的应用

人工智能技术已应用于威胁情报生产运营流程的各个环节，也应用于威胁情报中心推出的多款安全产品中，其中，ALPHA 威胁分析平台的“威胁图谱分析”模块尤为典型。

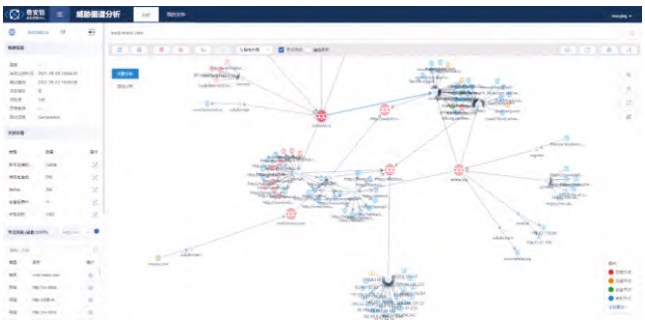


图2 ALPHA 威胁分析平台的“威胁图谱分析”模块

知识图谱是结构化的语义知识库，通过将各种实体、概念和关系以图形化的方式表达出来，从而构建出一个涵盖了丰富知识的结构化数据集。知识图谱的构建需要大量的数据积累和处理，人工智能技术可以通过自然语言处理、机器学习、图像识别等技术，对非结构化数据进行分析和处理，将其中的实体、概念和关系与知识图谱中的实体、概念和关系进行关联，将海量的数据转化为可用的知识图谱。

ALPHA威胁分析平台——威胁图谱分析，是一款面向安全运营分析人员的可视化威胁分析工具，是知识图谱的高级可视化呈现，通过构建知识层级的威胁情报查询系统，针对某个单一的威胁实体，提供基于该实体的基本属性、关联关系、关联节点属性的结果数据集。威胁图谱分析支持对IP、URL、Hash、Domain、Email 等多类型数据实体的单个查询及批量查询，采用多种人工智能领域优化算法，自动化进行快速、精准的数据解析匹配，分析各类实体之间的关联关系和各种行为之间的因果依赖关系，基于威胁发现能力模型，展示数据实体间的关联关系，并提供多方位下钻查询、拓线溯源能力。该功能模块可以实现攻击者溯源及画像，使得安全运营人员快速、高效地提取高价值威胁情报、挖掘异常行为、提升安全响应效率。

提升威胁攻击检测能力

ChatGPT在检测和响应网络攻击方面发挥着关键作用有助于提升威胁检测能力，消除威胁信号中的一些噪音，从海量告警中提取有效信息，提高网络防御能力和防御决策的自动化。

1. 网络钓鱼检测

ChatGPT可以被攻击者创造钓鱼邮件，同样可以从大型语言模型中学习，帮助组织识别和标记钓鱼邮件，结合企业部署的各类钓鱼邮件防护设备及时阻断钓鱼邮件的投递，从而显著降低网络钓鱼活动成功的机会。安全企业同样可以利用 ChatGPT 来训练网络钓鱼检测系统，以识别与这些攻击相关的模式和语言。以便提高网络钓鱼检测系统的效率和有效性。

2.漏洞发现处置

ChatGPT具有的逻辑推理能力，能够深入理解代码间的逻辑，可以协助网络安全专业人员识别未知的漏洞。基于ChatGPT的生成创作能力，并还使用知识信息推理来提高软件和系统的安全性，给出更有效的安全控制建议，或改进当前的安全措施和实践。

将ChatGPT应用于漏洞检测或漏洞管理类工具中，可以对网络漏洞进行扫描和评估，发现企业使用软件和系统中的新漏洞，预测漏洞被利用的可能性和影响范围，并给出漏洞修复建议，随着人工智能的不断发展还可能实现漏洞检测和修复的自动化和/或半自动化，以及基于风险的优先级。从而提高漏洞发现的准确率和漏洞修复效率。这对于面临资源限制的IT和安全团队来说，将是非常有吸引力的应用。

3.流量威胁检测

传统攻击检测手段主要采用规则和机器学习的方法达到了一定的检出率，但由于缺乏对代码上下文语义的理解，加上攻击手段不断更新升级，传统方法存在检测能力不足，漏报误报严重的问题。基于深度学习预训练模型的攻击检测方法，深度理解攻击请求的上下文信息，从而提高攻击检测效率。

赋能多种安全运营过程

近年来，受限于告警量多、处置效率低、人员工作量大等问题，安全运营领域有些停滞不前，安全运营人员面对众多安全设备产生的海量告警，从中找出有效数据，进行分析整合，判定攻击的真实性，再通过人工或安全编排和自动化响应工具进行处置，处置完成后还需要进行复验工作，安全运营人员往往不堪重负。

以ChatGPT为代表的生成式人工智能可以实现一些安全分析和自动化处置工作，简化安全团队的工作，并将自动化运营将从传统的机械式自动化，引入智能自动化、认知自动化。

1.日志解析

日志解析是包括SOC、SIEM、安全管理平台在内的关键能力，不同厂商不同设备的日志格式和字段语义存在较大差

异，传统的解决方式是采用基于规则和知识库的方式将各种日志解析规则固化形成知识库内置在平台内。生成式人工智能的语义理解能力可以对新的日志类型进行理解和分析，提升安全运营类设备对未知日志类型的解析能力。

2.事件分析

ChatGPT在安全事件分析方面展示出其独特的优势，ChatGPT从安全信息和事件管理(SIEM)工具或安全运营平台中获取数据，进行快速地处理，生成安全事件的分析，创建有关安全事件的清晰画面，形成分析报告，协助安全团队做出更好的安全决策。

ChatGPT 可以提供告警和安全事件的见解和处置建议，并提供安全威胁情报知识的标注，协助安全研判人员进行事件研判。在已有安全知识无法对事件进行分析时，分析研判人员可以与ChatGPT进行连续对话，主动提供更多的告警上下文情境信息，或者在ChatGPT 的指引下获取并提供更多情境信息，以得到更精确的信息。

3.自动化响应

安全事件响应是安全运营工作的核心工作。安全人员在面对各种设备产生的海量告警时面临着告警疲惫、处置效率低、经验难以固化等问题，SOAR安全编排与自动化响应工具应运而生，目前国内外主流SOAR产品通常包含作战室功能，并配以Chatbot，以聊天机器人的方式和安全分析人员进行互动，进行事件响应处置。

随着ChatGPT等高级AI加持的聊天机器人出现，结合SOAR技术，未来安全事件响应的工作效率可能会出现大的提升。例如：在处置环节，ChatGPT已经可以根据处置工程师的要求产生处置脚本，再进行人工调整，能够显著减轻处置人员的工作压力。可以预期，未来一些基本的安全响应脚本初稿的撰写工作可以交给ChatGPT或者类似的AI机器人去做，处置工程师可以在脚本初稿的基础上加以完善并转为SOAR剧本，情报查询、资产排查、漏洞确认、补丁修复和验证，以及影响性评估都可以通过剧本自动化的完成。

4.编写处置报告

在报告环节，ChatGPT可以根据整个研判和处置过程中产生的各类信息，以及安全分析人员输入的上下文信息，快速生成事件分析处置报告，减轻安全分析人员的工作量。

ChatGPT等高级AI驱动的聊天机器人目前还无法完全取代安全分析人员和威胁研判人员，更多是提供辅助决策与操作支持。相信随着持续高强度的人机会话互动，再借助更大规模、更专业的语料库训练，ChatGPT会不断强化自己的能力。

总结

以ChatGPT为代表的生成式人工智能正在各个领域掀起巨大变革，ChatGPT已成为网络安全领域的双刃剑，不仅可以被攻击者用于网络攻击，还可能存在开源模型被攻击、数据泄露等风险。但技术本身并无善恶，利用好以ChatGPT为代表的人工智能工具，以人工智能对抗人工智能，推动企业网络安全防御能力升级，提升威胁情报的分析能力、攻击检测能力，赋能安全运营过程，帮助安全人员提高效率，从繁琐的重复性工作中解放出来，才能发挥人和机器的更大价值。

参考文献

1.张弛,翁方宸,张玉清.ChatGPT在网络安全领域的应用、现状与趋势[J].信息安全研究,2023,9(06):500-509.

2.刘胡君,薛宇.ChatGPT——网络空间安全的“双刃剑”[J].军事文摘,2023(11):33-36.

3.张宇.威胁情报与人工智能的碰撞融合效应.[J].网安26号院,2023(29):35-38.

4.叶蓬.重新定义安全运营“平台”——从RSAC2023看安全运营技术发展趋势.[J].网安26号院,2023(29):21-27.

5.朱孟垚,李兴华.ChatGPT安全威胁研究[J].信息安全研究,2023,9(06):533-542.

6.叶蓬.ChatGPT提升安全运营：表现超预期，展示强大能力.[J].网安26号院,2023(27):20-23.

7.张少波.ChatGPT暗藏敏感数据泄露风险，政企如何才能规避.[J].网安26号院,2023(27):24-27.

FIDO无口令认证技术发展及应用

文｜庞南、朱晶晶

北京指掌易科技有限公司

摘　要： 网络应用服务的用户身份认证严重依赖账号/口令认证机制，其固有安全缺陷是用户信息保护和应用数据保护的严重威胁，无法适应当前网络安全发展态势，以FIDO为代表的无口令认证技术发展迅速，已经基本具备取代口令认证机制的应用基础条件。本文主要针对口令认证机制的安全缺陷，典型无口令认证技术FIDO规范的发展、原理、应用情况，以及无口令认证技术在证券行业的落地应用前景等内容进行论述。

关键字： 口令（Password）、无口令认证（Passwordless Authentication）、FIDO（Fast ID Online）、公钥密码（Public Key Cryptography）、数字签名（Digital Signature）、生物特征（Biometrics）、零信任网络访问（ZeroTrust Network Access）

概述

无口令身份认证（Passwordless Authentication），也被称为免密认证，是近年来面向网络身份验证的新解决方案，旨在消除网络应用服务对传统静态密码认证的依赖，该技术综合利用了生物特征识别和密码认证技术，来替代账号/口令认证机制，实现了认证信息的控制权完全属于用户，网络应用服务无需存储用户认证信息，既减少了用户认证信息暴露而提高了安全性，又确保了用户隐私信息保护，同时避免了维护支持成本的增加。

网络应用服务运营因为广泛使用账号/口令认证来完成用户身份认证，仍在普遍面临弱口令账号、以及社工钓鱼、社工库撞库等方式导致身份冒用、越权访问、数据泄露等一系列安全风险，而且针对口令认证的攻击是攻击者展开攻击链的最有效手段之一，彻底改变当前网络应用服务用户认证过于依赖口令认证的现状势在必行，以FIDO规范为代表的无口令认证技术，提供了现实可行的技术选择。

证券行业经过多年信息化和数字化建设，不仅运营着数量众多的关键业务应用服务，而且建设了相当规模的“以身份为中心”的ZTNA零信任网络访问控制设施，无论是从降低业务运营安全风险考虑，还是从提升零信任控制设施的核心安全能力考虑，关注和研究无口令认证技术，对证券行业机构都具有重要意义。

FIDO无口令认证技术发展及应用

口令认证广泛使用及安全性增强

在数字世界里，信任不会凭空产生，而身份认证是构建信任的关键环节。账号/口令方式的身份认证最早于20世纪60年代应用于控制大型计算机上本地文件的访问权限，历经20世纪90年代以来的互联网飞速发展，目前仍然是互联网世界保护用户信息安全的最主要技术手段之一。

同时，正是因为账号/口令认证技术仍被广泛应用，该技术自身存在的易被爆破猜测、易被撞库获取、易被钓鱼窃取等安全缺陷，以及提高口令安全策略强度（例如提高口令复杂度和强制定期修改等），所带来的维护和支持成本上升，都使得该技术已经无法适应当前网络空间安全威胁的发展态势。

北美最大的电信运营商Verizon在《2021年数据泄露调查报告》中统计披露，Web应用服务发生的数据泄露事件中，有89%是由认证信息滥用所导致的，攻击者可以通过暴力破解或钓鱼窃取等方式非法获得账号认证信息，继而实现身份冒用并导致数据泄露，这其中的根本原因是相当大部分Web应用服务都在采用账号/口令认证技术来完成用户身份认证。

业界对账号/口令认证技术的固有安全缺陷有清楚的认识，从2000年以来，陆续提出了很多基于口令认证机制，增强安全性的技术方案，其主要改进方向就是大力推动多因素认证MFA（Multi-Factor Authentication）。

业界将种类众多的身份认证技术总结归纳为三种类型，即1）基于用户所知（Know），如口令；2）基于用户所有（Have），如数字证书；3）基于用户所是（Are），如生物特征识

别。MFA多因素认证是使用以上三类认证技术中的至少两类来联合完成身份认证，该技术也被称为强身份认证（Strong Authentication）。

MFA的价值主要在于安全性的提升，降低认证信息被滥用的安全风险。例如微软公司与安全企业RSA公司合作开发了一种名为SecurID的“硬件设备+验证码”的双因素认证技术。除此之外，其它数量众多的OTP（One Time Password）动态口令认证、PKI（Public Key Infrastructure）数字证书认证、指纹/人脸生物特征认证技术和方案也纷纷涌现，这些身份认证的新方法，都无法广泛推广并取代账号/口令认证，通常作为口令认证基础之上的可选第二因素增强认证技术使用。口令认证的地位不仅没有被撼动，反而得到了更广泛的应用，用户平均拥有的账号口令数量，仍然处于持续增长的趋势之中，由此造成的安全隐患并未得到实质性改善。

FIDO无口令认证技术

无口令认证，是当前身份认证技术发展的一个趋势，通过对“所知”、“所有”、“所是”三类身份认证技术中的后两类技术的联合使用，彻底抛弃对“所知”类技术的依赖，摆脱对口令认证的依赖，从而规避“所知”类认证技术的伴生风险，提高身份认证机制的安全性。

具体而言，目前典型的无口令认证技术是联合使用“所有”和“所是”技术的双因素认证技术，将用户登录应用服务的认证过程分离为两个步骤，首先是客户端设备本地对用户真实身份的验证，使用的是本地生物特征识别技术，通过本地设备的指纹或人脸等认证方式，确保用户身份真实性，并获得本地私钥的合法使用授权来完成数字签名，属于“所是”类技术的应用；然后是服务端对客户端身份的验证，依托于公钥密码体制的数字签名验签技术，客户端必须使用所拥有的唯一私钥才能完成数字签名操作，属于“所有”类技术的应用。

无口令认证技术发展，在国际上，基本是FIDO（Fast IDentity Online）联盟推动的技术规范主导的局面，在国内，则是FIDO、IIFAA、SOTER等三个主要技术和生态体系共存的局面，三者的基本原理类似，以下仅针对FIDO规范的发展、原理、应用情况进行阐述。

1. FIDO规范发展

FIDO联盟成立于2012年，创始成员包括Paypal、联想等企业，FIDO联盟是一个开放的行业协会，联盟的使命是促进身份认证（Authentication）和设备证明（Attestation）标准的开发、使用和遵守，帮助世界减少对口令认证的过度依赖。目前FIDO联盟成员超过300家企业和政府机构，其中包括了Google、Microsoft、Intel、Apple、Amazon、Cisco、Visa、Paypal、Samsung，以及联想、飞天诚信、阿里巴巴、华为、OPPO等国内外知名企业。

FIDO联盟自成立开始，持续致力于推进具备更优安全性、易用性、隐私保护、成本等综合特性的身份认证技术标准的制定和推广使用，回顾FIDO身份认证规范的发展，可以划分为两个阶段：FIDO1.0（2014年至2019年）和FIDO2.0（2019年至今），其中包括了FIDO U2F、FIDO UAF、FIDO2等三套开放的身份认证规范。

FIDO1.0规范包括U2F和UAF两套技术规范，仅仅是行业联盟制定的技术规范，如果特定的互联网应用想实施符合规范的技术方案，都需要自行完成技术升级改造，由此带来的投入成本一定程度上限制了该规范的推广普及，该规范的推广情况与FIDO联盟在世界范围内消除口令依赖的愿景之间仍然均在巨大的差距。

FIDO联盟在2019年发布了FIDO2规范，开启了FIDO2.0阶段，与之前FIDO1.0规范最显著的区别在于，FIDO2规范的核心内容中包含了万维网联盟（W3C）发布的Web认证推荐标准Webauthn（Web身份认证），由于获得了W3C推荐标准的加持，主流浏览器厂商需要遵循W3C的标准，而主流浏览器厂商通常又是终端操作系统平台厂商，这使得FIDO2得到了更广泛的终端平台软件兼容支持，大幅简化了众多B/S架构的互联网应用部署FIDO2的终端侧技术改造工作，为FIDO2的大范围快速推广铺平了道路。

2. FIDO规范原理

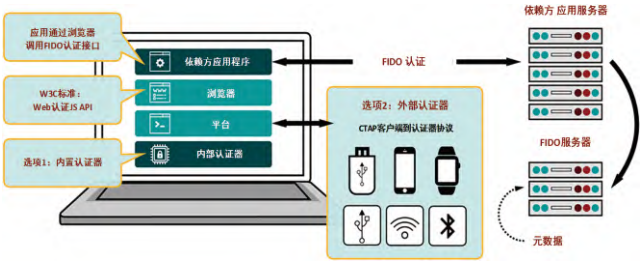
FIDO1.0标准发布于2014年，包括了两套技术规范，分别为：

· FIDO U2F（FIDO Universal 2nd Factor），即FIDO通用第二因素规范，该协议在“账号/口令”认证基础上，增加了由可物理交互硬件设备实现的、基于数字签名的双因子身份认证机制，有助于增强身份认证的安全强度。U2F也被称为CTAP1（Client to Authenticator Protocol）协议。

· FIDO UAF，即FIDO通用认证框架，该协议与U2F相似之处在于仍然基于公钥密码体制的数字签名技术实现身份认证，不同之处是依托用户侧终端设备的生物特征认证完成签名密钥使用授权。

对比而言，U2F仍然是依托口令认证机制的增强第二因素认证，属于口令增强技术，只能用于改善口令认证的安全性。而UAF自身已经是生物特征结合公钥密码的双因素认证，可以完全摒弃脱离账号/口令认证机制，属于真正意义上的无口令认证技术。

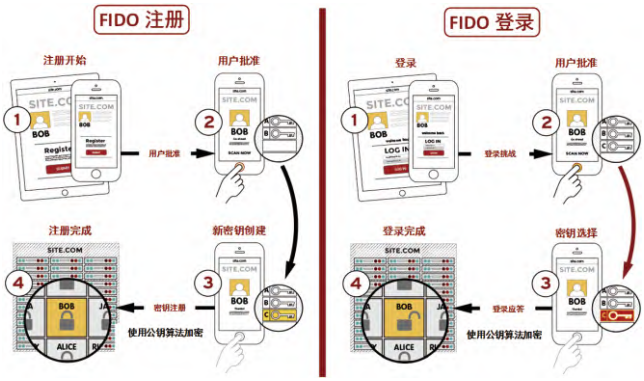
FIDO2由W3C的Webauthn协议和FIDO联盟的CTAP2协议两部分组成，其中Webauthn，即 Web Authentication，是由W3C制定发布的web认证推荐标准，定义了一组标准的Web API，内置在平台和浏览器中以支持FIDO无口令认证，它提供了一个创建和管理公钥凭证的接口，标准化了浏览器与认证器之间的通信交互。CTAP2为升级后的客户端到认证器协议，允许认证器同时作为身份验证的第一和第二因素，可以为用户提供无口令身份验证体验，或者在需要额外保护时提供双因素和多因素身份验证体验。



FIDO规范的工作过程分为用户注册和用户认证两阶段：

· 用户注册阶段，终端在生物特征识别保障下，在认证器中产生后续用于对应服务登录认证的公私密钥对，其中私钥在认证器中安全保存，将公钥提供给服务端与用户账号进行关联，并完成注册。认证器可以使用PC终端内部认证器，也可以使用移动终端、硬件安全密钥作为外部认证器。

· 用户认证阶段，终端在生物特征识别保障下，获得与服务对应私钥的使用授权，对服务端提供的登录挑战消息在认证器内完成数字签名，作为应答消息反馈给服务端，服务端使用用户账号关联的公钥完成签名验证，验证通过则允许用户成功登录。



FIDO认证协议的发展，提供了从增强双因素认证到无口令认证的技术选择，特别是FIDO2开放标准的推出，以及微软、谷歌、苹果等公司的操作系统和浏览器对FIDO2的全面兼容支持，让服务商为用户提供跨平台的、安全、易用的无口令身份认证成为可能，互联网世界摆脱对账号/口令认证机制的过度依赖这一技术变革更接近于实现。

FIDO无口令认证技术应用情况

1. 国际应用情况

包括微软、谷歌、苹果在内的国际主要IT和互联网厂商，增强和替换口令认证的实践活动可以分为四个阶段：

· 终端设备本地无口令登录认证

· 自有生态内的服务账号无口令登录认证

· 对符合FIDO规范的硬件安全密钥（Passkey）的使用支持

· 跨生态、跨平台的应用无口令登录认证

微软的Windows系统占据主要的PC终端市场份额，而且在Azure云端为大量用户提供Office365、Outlook、Skype等一系列SaaS服务，用户需要登录微软账户访问服务，为改善用户登录系统和服务的安全性，微软大力推进无口令认证技术的落地应用，形成了包括Windows Hello、Microsoft Authenticator APP、以及FIDO硬件安全密钥在内的无口令认证体系，微软的无口令认证实践关键动作包括：

· 从Windows10开始提供Windows Hello用于增强Windows系统登录安全性，Window Hello提供设备本地认证器的PIN、指纹、人脸等认证方式，用户无需输入口令就能完成设备登录。另外Windows Hello通过FIDO2认证，可作为终端内置认证器使用；

· 自Windows10的1809版本开始，Windows操作系统和Edge浏览器兼容支持FIDO2无口令认证；

· 提供面向安卓/iOS用户的Microsoft Authenticator APP，将移动终端作为认证器使用；

· 兼容支持符合FIDO规范的硬件安全密钥Passkey。

谷歌的安卓系统、Chrome浏览器、以及Gmail、Youtube等旗下服务，同样拥有大量用户，谷歌也在大力推进无口令认证在自有生态内的应用，关键时间动作包括：

· 安卓系统支持本地指纹、人脸等方式的屏幕解锁认证方式；

· 谷歌账号先是支持FIDO U2F的增强用户认证，目前已经支持FIDO2无口令认证；

· 安卓操作系统7.0及以后版本兼容支持FIDO，并且通过了FIDO2认证，安卓手机可以自身作为认证器，支持网站/应用的FIDO2无口令登录认证；

· 支持通过USB、NFC、BLE等通信方式使用其它符合FIDO规范的硬件安全密钥，支持应用登录的增强身份认证或无口令认证；

· Chrome浏览器76及以后版本兼容支持FIDO2，Web服务可以借助Chrome浏览器这一能力，实现用户无口令登录认证。

苹果的iOS、ipadOS和MacOS在移动端和PC端同样拥有大量用户，Safari浏览器、iCloud服务也被广泛使用，但苹果只是在FIDO2标准发布后，才在2020年正式加入FIDO联盟。苹果在推进无口令认证落地应用的关键动作包括：

· iOS、ipadOS和MacOS支持TouchID、FaceID等方式的本地生物特征识别认证方式；

· AppleID的登录认证增强方式，从2021年钥匙串技术，到2022年的通行密钥（Passkeys）技术，从IOS16.3、Macos13.2开始，为AppleID的登录，增加物理安全密钥的支持，提供增强的第二因素认证保护；

另外，国外还有Yubico这样的硬件安全密钥厂商，为无口令认证使用场景提供符合FIDO规范的漫游认证器产品，被广泛使用。

以上我们可以看到，各大厂商的无口令认证实践，主要集中于各自生态内的终端和服务范围，随着FIDO2包含W3C

Web认证推荐标准，以及苹果加入FIDO联盟，这一情况发生了显著变化，2022年世界密码日，苹果、谷歌、微软联合承诺支持FIDO无口令认证，承诺在一年内对各自产品进行改造，Windows、MacOS、安卓、IOS等主流操作系统，以及Chrome、Edge、Safari等主流浏览器都实现了对FIDO2的支持，为互联网网站/应用推动实现跨平台、跨终端的用户无口令登录认证提供了有力支撑。

2. 国内应用情况

FIDO联盟在2016年成立中国工作组，旨在推动FIDO技术本土化落地，促进FIDO标准在国内乃至全球产业链发展，以及推动国内新型在线身份认证体系升级，该工作组目前由国民认证、飞天诚信、以及华为等FIDO联盟成员的技术专家负责工作推进。

FIDO规范在中国国内落地方向主要集中在U2F和UAF。从落地行业看，虽然FIDO技术本身不具有行业倾向性，但因为中国在移动支付、互金等新兴金融领域的发展势头迅猛，且监管力度强，天然对更安全、易用的身份认证技术的需求强劲，所以FIDO的技术落地主要集中于金融行业，并逐渐向非金融领域推进。

国民认证的前身是联想集团在线认证事业部，联想集团是FIDO联盟董事会成员单位，主要业务是为主流互联网服务商、政府、企业、金融机构、硬件制造商、生物认证技术商提供完整的身份认证解决方案。技术特点是将身份认证手段（如生物识别技术、PIN码等）与身份认证协议解耦合，通过非对称性的公私钥体制来完成对用户的身份鉴别。

飞天诚信是FIDO联盟董事会成员单位，主要产品方案包括了符合FIDO规范的多款硬件安全密钥和FTFIDO无密码在线快速身份认证平台，其中ePass硬件安全密钥通过了苹果认证，被用于AppleID的增强登录保护，FTFIDO无密码在线快速身份认证平台提供对FIDO2协议的支持，并在多家金融机构成功落地。

CFCA中国金融认证中心是FIDO联盟协理会员单位，CFCA推出的FIDO+方案，结合了FIDO技术和数字证书电子认证技术，用户可以通过人脸识别、指纹识别等方式实现免密登陆和免密交易，拥有便捷性的同时，实现高安全性，并保障司法取证。方案应用于手机银行、第三方支付、理财消费等互联网金融和政府机构领域。

FIDO无口令认证技术在证券行业应用前景

证券行业机构运营着大量的面向外部用户和面向内部员工使用的关键应用服务，同时实现了广泛的业务移动化，用户可以使用PC终端和移动终端实现便捷访问，这些应用服务比较普遍仍在使用账号/口令认证来完成用户身份真实性鉴别，或者仅针对部分重要用户提供了基于口令认证的双因素认证实现安全性增强。

另外，近年来证券行业机构也开始变革升级其安全框架，其中一项重要内容就是建设ZTNA零信任网络访问控制设施，包括了IAM、SDP等具体控制措施，零信任理念的核心是以身份为中心，持续验证，从不信任，也将身份认证核心安全能力的重要性提升到更高高度，口令认证或增强口令认证成为制约ZTNA设施发挥保护效能的短板隐患。

本质上讲，所有涉及到账号/口令认证的场景，都存在无口令认证技术应用的需要，无论是面向外部用户，还是面向内部员工，无口令认证技术都可以实现对口令认证机制的取代，从而大幅度提升身份认证安全性。但是，考虑稳妥验证新技术成熟度，降低对用户使用体验影响程度的考虑，证券行业机构先从内部网络应用服务场景进行无口令认证技术的探索建设，是更可行、现实的选择。

例如，对现有IAM统一身份认证系统进行技术改造，使其支持无口令认证能力，并针对内部办公应用系统开展无口令认证试点建设，积累建设和运营经验，未来适当条件下，再考虑向外部用户使用的关键业务应用进行后续推广。

结论

以FIDO规范为代表的无口令认证技术，随着操作系统、浏览器等基础平台软件的兼容支持，以及用户终端设备生物特征识别能力的广泛普及，已经趋于成熟，在网络应用服务的用户身份认证环节取代具有安全缺陷但仍广泛使用的口令认证机制，已经具备实际应用条件。

证券行业机构研究和使用无口令认证技术，来降低关键业务应用运营的整体安全风险，并改善现有ZTNA控制设施的核心安全能力，为有力支撑持续的数字化转型具有重要意义。

参考文献

1. FIDO规范，FIDO Specifications，Download Authentication Specifications - FIDO Alliance

2. W3C，Web Authentication 推荐标准，Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org)

3. 微软安全，无口令保护白皮书，RE2KEup (microsoft.com)

IAST在证券行业的落地实践探索

文｜庞伊良

北京基调网络股份有限公司

摘　要： 随着监管与业务双重压力的不断增长，证券行业企业面临着越来越大的业务安全压力。为了弥补开发实践中安全能力的欠缺、提前发现安全威胁、降低漏洞修复成本，证券行业企业必须探索建设DevSecOps流程，推动安全左移。IAST作为一款结合了黑盒与白盒优点的新型安全测试工具，可以有效帮助证券甲方企业补足在DevSecOps流程中敏捷开发的能力。

关键字： IAST、灰盒、证券、DevSecOps、应用安全、开发安全

证券行业安全风险与压力逐年升高

IDC在《中国数字化转型市场预测，2021-2026：通过应用场景践行数字化优先策略》中预测，未来五年是数字化发展的黄金时期，企业在应用硬件、软件和服务上的投入将快速增长。证券行业作为金融行业的代表，是数字化转型浪潮中的领航员，在应用开发、应用安全方面面临着更多机遇与更大的挑战。

图1 IDC《中国数字化转型市场预测，2021-2026：通过应用场景践行数字化优先策略》

伴随着数字化浪潮而来的，还有日益严重的应用安全问题，金融行业的网络安全风险不断累积，证券行业网络安全防护也面临着前所未有的威胁与挑战。在2022年国家信息安全漏洞共享平台CNVD公布的漏洞趋势中，应用漏洞几乎始终占据70%以上的占比。应用安全问题不仅带来了个人隐私泄露风险，影响企业经营，在金融这样与国计民生息息相关的行业中，会直接影响社会经济正常运转。

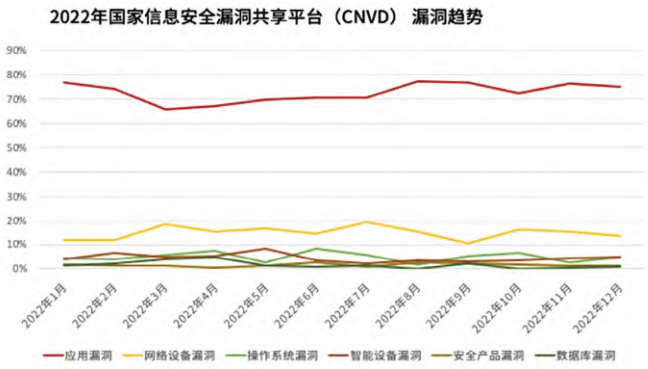


图2 2022年国家信息安全漏洞共享平台（CNVD）漏洞趋势

以XSS、SQL注入、敏感信息泄露、未授权访问、弱口令、远程代码执行、任意文件读取、逻辑漏洞等为代表的Web安全漏洞依旧是最多发的漏洞类型。应用系统上线后漏洞修复往往要耗费较长时间和较高的成本。

保障业务连续性无疑是证券行业进行网络安全建设时的首要目标。面对如此多发的应用安全漏洞，仅仅依靠应用上线后的各种安全防护设备显然是不合理也不可行的。为了推动数字化转型过程中企业同步建设完善网络安全体系，国家与监管机构在保障网络安全方面对企业的要求越来越高。除了与业务直接相关的漏洞压力之外，证券企业也同时要面临巨大的监管压力。

2023年6月9日，中国证券业协会（中证协）正式印发《证券公司网络和信息安全三年提升计划（2023-2025）》，提出建立科学合理的科技投入机制，要求行业合理加大科技资金投入。鼓励有条件的公司2023-2025三个年度信息科技平均投入金额不少于上述三个年度平均净利润的8%或平均营业收入的6%。一些省份如江苏省也发布了省级的金融管理办

法，要求将IT建设投入的5%以上投入在网络安全领域。

《三年提升计划》明确要求证券公司健全网络和信息安全防护体系，深化漏洞全生命周期管控。要求使用白盒检测、黑盒检测、灰盒检测和人工渗透相结合的技术手段，检测代码安全缺陷和引入的第三方组件漏洞，提升安全风险检测的全面性、准确性和效率，实现漏洞通报、修复的闭环管理，确保变更上线前已知风险全面收敛。

在实际的业务运行过程中，越来越多的证券行业企业发现原有的软件开发与安全测试流程过于复杂，工作繁琐，且对于人工投入要求较高，很难适应业务的敏捷快速迭代开发模式。为了弥补开发实践中安全能力的欠缺、提前发现安全威胁、降低漏洞修复成本，证券行业企业必须探索建设DevSecOps流程，推动安全左移。

《三年提升计划》中提及的白盒、黑盒、SCA等能力，均是DevSecOps流程中典型、常见且较为成熟的能力，但计划中还提及了灰盒检测能力，是目前大家较为陌生的工具。

灰盒IAST在安全建设中的应用

灰盒IAST（Interactive Application Security Testing，交互式应用程序安全测试）是一款适用于开发与测试阶段的应用安全测试工具，可以完美适配敏捷开发和DevSecOps流程，让开发人员和测试人员在执行功能测试时，实时、动态、同步进行漏洞检测，精确确定漏洞所在代码行，在无感知的情况下完成安全测试，帮助企业在应用上线前进行应用安全测试，提前发现安全漏洞，降低漏洞修复成本。

IAST在应用和API中可以实现自动化识别和诊断软件漏洞，通过在程序运行过程中使用插桩技术（Instrumented）收集、监控Web应用程序运行时的函数执行、数据传输，并与服务端（server）进行实时交互，根据这些信息来判断程序是否存在漏洞与安全风险，高效、准确地识别安全缺陷及漏洞。

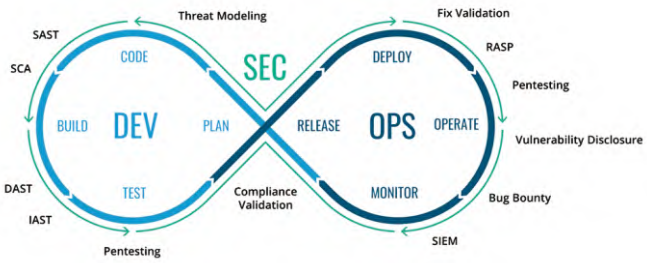


图3 DevSecOps安全开发全流程各阶段常用安全工具

它对来自客户端产生的请求和响应进行分析，检测结果准确，这点类似于DAST；而它能够监控数据流信息，通过污点分析产生告警，检测结果全面，又类似于SAST，是一款结合了黑盒与白盒优势的新工具。

灰盒IAST的部署与使用效果受企业是否已经建立完整的DevSecOps流程影响很大，目前，IAST在互联网等信息化水平较高的行业中应用效果较好，在证券等金融行业中的应用则仍然存在一些挑战。

IAST在证券行业的落地实践方案

头部的大型证券企业内部基本都拥有完整的安全评估与漏洞管理、修复流程，自身具备较强的安全实力。部分企业通过自研SDL全流程赋能平台，可以集成威胁建模、自动化测试等功能，实现自动化基于场景的轻量级威胁建模能力，可支持从外部接入源代码分析、AST等工具和渗透测试服务。想要在证券行业DevSecOps流程中融入IAST，接入SDL全流程赋能平台，需要解决几个关键问题：

1、Agent节点全量覆盖的同时保持稳定性；

2、绝不能产生脏数据影响业务；

3、确保检测结果的准确性，误报率、漏报率低；

4、能够与其他安全工具良好协作。

我们以某头部大型证券企业为例，探索IAST在证券行业的落地实践过程。该证券行业客户体量庞大，资产、应用、数据众多，应用上线前依赖人工渗透测试寻找安全隐患，并且为了确保上线业务的安全性，还需要多人渗透并进行交叉验证。人工投入大、人员能力要求高，效率难以满足业务的敏捷快速迭代开发。通过接入灰盒IAST，最终实现应用上线前的漏洞自动化检测与发现，把人从重复性劳动中解放出来。

图4 IAST接入某证券行业企业自研SDL全流程赋能平台

图5 在证券行业中接入IAST实现自动化漏洞发现实施过程思路

Agent自动化全量部署的同时，保持极高的稳定性

接入自动化IAST的第一步是插桩，想要在如此庞大的体量中使用IAST进行全量覆盖，需要部署过万个节点，Agent的部署是其中的重点也是难点。通过采用数据采集与扫描引擎分离的独特架构，Agent端只负责采集数据，所有运算分析，包括核心的sca组件收集、hook点字节码转化、调用链收集、主动验证、API梳理等核心操作均在server端完成，从资源的需求上有效地降低了占用。

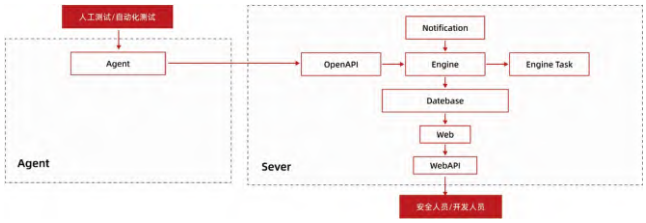


图6 数据采集与扫描引擎分离独特架构

任何的插桩行为都可能对性能和资源消耗产生一定影响，上万个节点的插桩更是对IAST性能优化的挑战。这要求IAST提供多维度的熔断降级策略，分级延迟加载Agent，并提供细粒度的Agent管理。这让IAST在支持数万个节点的部署与上万个节点并发的同时，仍能保持生产级别的Agent稳定性。

对脏数据零容忍

对于头部证券的业务部门来说，脏数据是无法接受的。上万个节点的并发检测如何能不产生任何脏数据?IAST给出的解决方案是被动插桩模式。被动插桩模式不会主动发送payload，对来自客户端的请求响应进行污点传播数据流监控，根据是否经过无害化处理判断是否存在漏洞。只需要业务测试（手动或自动）来触发安全测试，通过测试流量即可实时的进行漏洞检测，并不会影响同时运行的其他测试活动，在此过程中不会产生脏数据。

图7 被动插桩模式

检测结果准确，漏报、误报低

实现规模化IAST插桩检测后，检测的准确性是另一个关键问题。IAST作为结合了SAST与DAST部分优势特性的工具，本就已经具备了检测结果准确、误报漏报少的优势。如何在80分的基础上更进一步，做到90分甚至95分?我们发现在测试验收阶段加入安全度量指标，实现IAST检查结果的展示与处理是一个可行性很高的思路。

这里提供一个建议：将静态安全扫描、制品安全扫描、IAST扫描结果作为安全度量指标，按照应用-单元-版本号等关键字段管理扫描结果。将指标统计数据、中高危风险概要和全量详细信息指标数据汇总用于展示和门禁管控，可有效帮助梳理IAST的检测结果。

与其他安全工具联动以实现更大价值

在与客户自研的SDL全流程赋能平台对接的过程中我们发现，该平台作为一个SDL全流程赋能平台，接入了包括IAST、DAST等多种单点安全工具，各个单点安全工具均在应用安全测试中拥有着各自的独特价值。IAST产品的特点决定了它可以提供更高的测试准确性，可详细地标注漏洞在应用程序代码中的确切位置，帮助开发人员修复。但同时IAST也存在一定的限制，对于部分复杂的漏洞场景，由于漏洞检测不依赖真实的漏洞 Payload，所以在验证漏洞的可利用性时，可能会存在一定难度。

目前，各单点工具之间仍然是独立工作，难以协同。如今，如同木桶效应中各块木板的长短一般，相较于追求某个单点安全工具的极致性能，探寻安全能力和安全数据之间联通的可能性或许是一个更具性价比也更高效可行的安全建设路径。在拥有可以满足核心安全需求的单点安全能力的条件下，通过联通性与安全效能的叠加性可以获得更大的经济收益与安全保障效果。

理想很丰满，但现实很骨感。即使是SDL全流程赋能平台可以提供完整SDL能力，要实现各个单点工具之间的联动仍然是十分困难的，需要耗费极大的人力与时间。因此，我们开始思考如何通过IAST直接与其他应用安全测试工具结合起来，以更方便地验证漏洞，从而进一步降低漏洞修复工作的难度。

目前，有且仅有洞态IAST已经实现了与黑盒DAST工具的一体化联动，黑盒工具可根据以下架构在实现请求头修改和数据同步之后对漏洞数据进行关联。

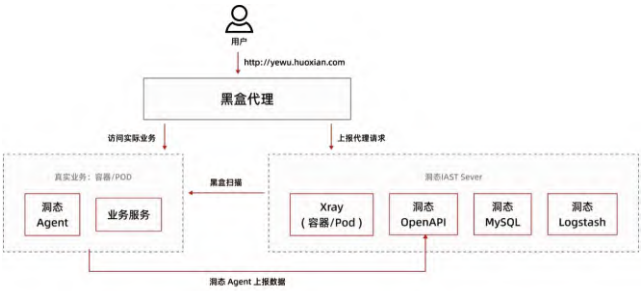


图8 洞态IAST与黑盒DAST一体化联动架构

有了IAST成功接入SDL全流程赋能平台的经验，且洞态IAST已实现与黑盒联动，相信在未来，单点工具之间、工具与平台之间互相联动协作，数据互通，必将帮助甲方更好地推进信息安全建设。

能落地，才有意义

安全部门的首要目标是保障业务连续，免受安全风险与威胁，安全产品与安全能力不能落地就没有意义。安全团队如何与开发、业务部门协作，是技术、产品、人员之外一个隐性的影响因素，特别是在IAST这种由安全部门采购，研发部门使用的安全工具，其中的影响表现得尤其明显。安全产品拥有良好的落地能力，高效、准确地发现与修复漏洞的过程提高了安全部门的价值，也间接推动了安全部门与其他部门的沟通合作，这对于甲方安全部门在内部推动整体安全建设是大有裨益的。

经过多年数字化转型的建设，证券行业信息化水平普遍较高，大多已经建立了较为完备的DevSecOps流程，在如今业务与监管的双重压力下，证券甲方企业需要补足在DevSecOps流程中各个节点的安全能力，更需要能落地、能联动的、好用、易用的人性化安全产品。

注：2024年1月北京基调网络股份有限公司已经完成对洞态IAST及其安全团队的收购，文中所述“洞态IAST”已经升级为“安云IAST”。

LLM为静态代码分析带来了什么

文｜束骏亮

上海蜚语信息科技有限公司

摘　要： 静态程序分析技术主要目的是从软件代码中寻找潜在的Bug与安全漏洞。自其诞生来，静态分析技术就存在分析结果不精确、误报率较高、使用门槛高、漏洞治理难以闭环等缺点。近年符号执行、形式化验证等前沿程序分析技术在工程领域实现了落地，改善了静态分析技术在分析精度方面的弱点。但是其使用门槛高、漏洞治理难以形成闭环缺陷仍然没有得到很好的解决。随着ChatGPT的发布，GPT等大模型所展现出来对于文本语言和代码的理解与生成能力，让技术人员看到了改善静态分析技术的使用门槛高和漏洞治理难以闭环等缺陷的希望。本文回顾了静态分析技术近年来的技术发展路径与其在现代研发场景下的落地应用，并对大型语言模型技术在静态分析场景下的应用前景进行了论证与展望。

关键字： 软件安全、静态代码分析、生成式人工智能、大型语言模型

概述

静态程序分析技术是一项伴随软件研发行业成长的基础支撑性技术，其主要目的是从软件代码中寻找潜在的Bug与安全漏洞，帮助研发人员提升软件的质量与安全性。自其诞生来，静态分析技术就存在分析结果不精确、误报率较高、使用门槛高、漏洞治理难以闭环等缺点。随着近十年技术的发展，符号执行、形式化验证等前沿程序分析技术在工程领域实现了落地，静态分析技术在分析精度方面有了大幅度提升。但是其使用门槛高、漏洞治理难以形成闭环缺陷仍然没有得到很好的解决。

2022年底，OpenAI发布了最新的大型语言模型GPT-3.5，其衍生应用ChatGPT引领了人工智能领域新一轮的技术浪潮。GPT系列大模型所展现出来对于文本语言和代码的理解与生成能力，让技术人员看到了改善静态分析技术的使用门槛高和漏洞治理难以闭环等缺陷的希望。

本文回顾了静态分析技术近年来的技术发展路径与其在现代研发场景下的落地应用，并对大型语言模型技术在静态分析场景下的应用前景进行了论证与展望。

静态分析技术的现代应用场景

自从静态分析技术诞生以来，就受制于计算复杂度的限制。由于现代程序的功能与逻辑越来越复杂，一般我们很难在静态分析的场景下完全还原出程序的所有行为。这个在计算复杂性理论里已经被证明过，在有限的多项式时间内穷举一个程序的所有可能状态是一个NP（Non deterministic Ploynomial，即非确定性多项式问题）困难问题。因此困扰静态分析的难题是分析的准确性比较低，这个也是从业人员这几十年以来一直努力去优化解决的方向。

虽然我们不能100%还原程序的行为，经过这么多年技术的发展，研究人员通过平衡分析的目标、准确性和完备性，仍然为静态分析技术找到了一些能够解决的比较好的问题，这其中的一部分被市场证明了具备比较好的应用价值，形成了成熟的落地场景。从所解决的问题来看，目前静态程序分析技术主要应用场景大致有以下几类：

代码风格分析

针对代码风格的分析技术相对来说比较简单，因为风格的检查往往不会涉及到上下的语义信息，主要是对代码进行语法检查。因此，对于代码风格的分析不需要引入复杂的程序分析技术，很多开源工具都可以完成的比较好。另外，由于对于代码风格的定义和要求往往因企业而异，业界也不存在统一的第三方标准，大部分有相关需求的企业往往参考大厂的成型代码风格（如Google的一系列code style）再进行调整，然后选择合适的开源工具来搭建自动化分析能力（如与Google C++ Style配套的cpplint、SonarQube等等）。

代码质量分析

针对代码质量的分析需求主要集中嵌入式研发领域，众所周知，由于所使用的场景较为底层，嵌入式软件对于代码运行的稳定性有着非常高的要求。同时，由于嵌入式硬件在算力、存储、内存等方面的限制，嵌入式软件对于运行效率、内存占用、代码体积都有着比较苛刻要求。在这样几方面需

求的影响下，嵌入式软件对于软件代码质量的要求要显著高于其他领域。并且在嵌入式研发领域大家所使用的又是C/C++这类语法复杂、比较容易写出BUG的编程语言，能够对代码进行自动化质量检查的静态分析工具成为了该领域必备的研发支撑软件。

针对嵌入式领域C/C++代码的质量分析工具目前已经被广泛的应用在物联网、军工、航空航天、能源电力、医疗器械、轨道交通等行业，很多行业已经形成了比较权威的代码质量标准和规范，比如ISO26262、DO-178B/C、IEC62304、EN50128、GJB8114、MISRA-C/C++等。

对于代码质量的分析，从技术上来说要难于代码风格检查，部分代码质量规则会涉及到代码的上下文语义信息。同时由于已经形成众多权威的代码质量规范，软件研发企业往往对相关工具的检测完备性有着较高的要求。因此在该场景下，一般会选择成熟的商业化工具。由于过去中国在相关领域的研发从业者较少，这些产品绝大部分来自国外，比如QAC、Klocwork、Coverity等。

代码安全分析

代码安全分析是另一个商业化比较成功的静态分析技术落地场景，也就是我们大家熟知的SAST(Static Application Security Testing)或是白盒分析类工具。由于代码质量分析的需求比较集中在嵌入式开发领域，并且随着开发工具链和硬件的进步，大部分行业的软件研发从业人员如今并不会面对太多代码质量方面的困扰。反而随着网络安全产业的发展和网络安全攻击事件的日趋频繁，对于安全漏洞或是相关代码缺陷的分析成为了静态分析技术的另一个主要应用场景。当然这背后离不开这么些年来静态分析技术本身的进步，毕竟安全漏洞从分析难度来说要远高于代码质量问题。近年来，随着DevSecOps理念的推广和漏洞治理难度的不断增加，安全左移成为了安全行业的热点方向之一。本来只是作为漏洞治理生态一环的SAST工具迎来的新的发展机遇，很可能会成为未来软件漏洞治理的主流手段之一。

由于不同编程语言的安全漏洞从代码形态上来说存在着比较大的差异，SAST工具往往也因为擅长分析语言的不同而具备不同的差异化竞争优势。对于偏底层的C/C++类语言来说，安全漏洞的形成往往是源于代码对于内存的错误操作，攻击者通过组合多个代码缺陷能够获取部分内存区域的读写权限，从而获得劫持程序运行逻辑的能力，进而实现提权等攻击行为。因此对于C/C++类语言来说，代码安全分析的重点就在于如何发现代码中与内存、指针相关的代码BUG，比如空指针解引用、UAF、double free、数组越界、栈/堆溢出等等。由于这些代码BUG即使没有形成可利用的漏洞，也会严重影响程序运行的稳定性。因此在代码质量分析的场景下，这些BUG类型也具备非常重要的意义，针对C/C++语言的代码质量分析和代码安全分析需求在这里存在一定的重叠，部分工具也具备解决两方面问题的能力。由于C/C++语言从编译到语法都比较复杂，针对C/C++的静态代码分析技术也是比较困难的一部分，仅有少部分的工具具备成熟的C/C++代码安全分析能力，比如Coverity、PolySpace、Infer、CSA等等。

虽然在2022年重新夺回了TIOBE年度编程语言的江湖地位，C/C++在国内的使用普及度仍与Java相去甚远。对于Java的分析能力依旧是在国内市场考察一款静态分析工具成熟度的重要指标。与C/C++不同，由于Java的主要应用场景是在服务器侧，针对Java的静态分析工具主要关注如何在代码中寻找与攻防相关的代码漏洞，比如XSS、各种注入、命令执行、路径穿越、密码学误用等等。这些代码漏洞往往具备比较复杂的上下文场景，触发条件也受到程序状态的影响，同时由于Java语言的灵活性，不同项目所使用的各类库也不尽相同，传统的静态分析工具在面对这类问题时往往存在比较高的误报率与漏报率，需要使用者付出比较多的精力进行二次开发和调优才能达到相对比较好的效果。从检测安全漏洞的角度来看，SAST与其他几类开发安全产品(DAST、IAST等)的能力产生了重叠，不过正如上文所说，由于静态分析与动态测试技术各有所长，在大部分的场景下这些不同类型的测试分析工具是互补的关系。由于应用场景更加普遍，因此针对Java的静态分析工具相对可选择空间较多，比如Fortify、Checkmarx、Sonarqube、FindSecBug、CodeQL等等。

其他场景

除了上述几类成熟场景外，静态分析技术也在软件成分分析、数据安全、隐私合规等场景下有着良好的应用。

静态分析技术的落地困境

从产品侧来看，现有的静态分析类产品均存在较大的提升空间，目前主流的静态分析产品距离开发人员心目中的样子仍然有比较大的距离。

目前国内常见静态分析类产品还是以国外厂商为主，开源的Sonarqube，Infer和CodeQL等，商用的Coverity，Fortify和Checkmarx等。国内厂商还在努力缩小和国际一流产品的差距。

然而即使以国际一流产品为参考，他们在国内的场景落地仍然存在相当的不足，主要体现在以下几个方面：

使用成本高

目前的主流静态分析类产品还是被设计为一种专业人士使用的高门槛工具，常见的开源工具和商业化产品均具备比

较强大的自定义能力。丰富的自定义配置能力也意味着若想发挥出工具的真实效果，需要用户投入较多的人力和时间成本进行运营优化，在厂商无法提供有力技术支持的情况下，这对于大部分的国内用户显得有些难以做到。太高的使用成本是阻碍静态分类工具打开市场的第一道门槛。

分析精度不足

虽然静态分析技术在近二十年间有了长足的发展，但是很少有厂家能够将这些在论文中大放异彩的前沿技术落地在商业化的产品中，现实世界的软件代码和benchmark往往有着天壤之别。此外，随着分析技术不断的进步，人们对于静态分析技术的期望也在不断提升。简单的问题早已被解决，无论是影响程序稳定的恶性BUG还是影响程序安全的高危漏洞，在现实世界软件代码中隐藏的越来越深，软件架构越来越复杂。传统工具的分析能力无法应对这些复杂的代码场景，过高的误报率导致用户的使用成本大幅提升。能否解决现代化软件架构下的分析精度问题，已经成为用户评估此类产品的首要指标。

漏洞治理难以闭环

静态分析工具的终极目标是帮助开发人员减少代码中潜在的Bug与安全问题。然而目前几乎所有的静态分析工具都将目光聚焦在发现问题这一点上。从业务场景来说，发现问题仅仅是解决问题的第一步。在静态工具发现问题后，用户往往需要花费大量的时间进行漏洞的理解、漏洞真实性的判断以及最终完成漏洞的修复。在这个过程中还需要寻求运维、研发、安全部门其他同事的协作。整体的漏洞治理成本高昂，难以闭环。

AIGC为静态分析技术带来了什么

在上一章中我们提到了漏洞治理难以闭环是现阶段阻碍静态分析工具走向更广阔应用场景的关键问题。不解决这个问题，静态分析工具就只能是安全/测试部门手中的专业工具，难以被普通开发者使用。也就无法实现在研发流程中持续、高效、低成本的解决Bug与漏洞问题。

在过去，技术人员在这方面有过很多尝试，比如通过收集Github上的fix code来实现修复建议推荐，但是效果都不理想。随着以GPT为代表的大型语言模型技术的发展，解决这些问题变得不再遥不可及。

2022年底，OpenAI发布了其最新一代的大型语言模型GPT-3.5及衍生应用ChatGPT。ChatGPT一问世就引发了科技届的狂热讨论。其展现出来的文本理解、生成与对话能力远超过去任何一种人工智能技术，并且ChatGPT还表现了相当亮眼的代码理解与生成能力。而ChatGPT的出现也促进了全球范围内的LLM(Large Language Models，大型语言模型)基础设施的发展，为技术人员在各垂直领域落地LLM能力提供了诸多便利。静态分析技术作为一种以代码文本为主要处理对象的技术，天然能够与NLP技术进行融合。ChatGPT及后续GPT-4模型在代码理解与生成方面的能力，对于静态分析工具的演化有着关键作用。

为了探索LLM在静态代码分析场景下的落地可行性，我们进行了一系列的实验。最终得出如下结论：

从目前GPT-4的能力来看，基于LLM (Large Language Models，大型语言模型) 的代码分析技术，无法成为替代传统程序分析技术栈的新技术路径。但是LLM所带来的全新能力，能够大幅度提升现有SAST工具的水平。

接下来我们从两方面来详细的拆解这个结论。

LLM大型语言模型的代码分析能力

本文不对GPT-4模型本身进行过多介绍，感兴趣的读者可以自行查阅相关资料。推荐有时间的读者阅读微软研究院发表的154页的论文，

基于现有的LLM演示和ChatGPT等应用表现出来的能力，看似GPT能像人一样去“阅读”代码，给出对代码上下文语法、语义的“理解”，做一些“推理判断”，然后用自然的语言把这些结论展示出来，并且能够持续的和用户进行交互。甚至我们在测试中发现它还能识别开源代码片段的来源，具备一定的SCA能力。从这个角度上来看，GPT的确涌现了很多之前其他模型所不具备的能力，表现是很惊艳的。

但是在惊艳之后，我们更多的是希望从生产应用场景的角度来探寻用LLM大型语言模型进行代码分析任务可行性。大炮能打蚊子并不代表你一定要用大炮来打蚊子，更多时候你需要的只是一个20块的电蚊拍。经过一段时间的研究和测试，我们有以下发现：

1. 工程落地难度

由于大型语言模型的稀缺性，所有相关方案都无法回避落地问题。从现实商业场景来说，有很多问题需要解决，包括了代码传输时的数据安全问题、API的可连接性、面对海量代码时的经济成本、本地化的可行性等等。

2. 分析复杂代码的能力

基于微软论文里给出的信息，目前的自回归模型在数学/推理任务中缺少规划能力（planning)，这使得这类模型即使面对稍微复杂一点的推理问题也很容易失败。然而推理能力是代码分析场景所必须要具备的能力，否则就难以做到精确分析。在我们的测试中，GPT-4模型能够很好的解决简单的代码分析任务，然而一旦测试用例中出现了变量、控制流相关的推理逻辑，GPT-4模型就会出现误判。对于部分场景，可以通过一系列人为的引导逐步推出正确的结论，但是从工程上来说效果仍然很差。感兴趣的同学可以用OWASP Java

Benchmark来试试。

3. 输入限制

目前的GPT-4模型给出了32000 tokens的输入上限。在面对真实软件项目时，这样的输入窗口太小，只能够进行代码片段的分析。即使通过embedding向量化，可用性也很有限。此外，由于输入窗口上限是由模型本身决定的，这就意味着难以通过工程的方法后期进行扩充。

4. 分析效率

GPT-4是基于逐单词预测的模式来生成回答，分析时间基本是由需要输出的文本量决定。从现在的使用体验上来看，给出结果的效率太低，有几个数量级的缺口。人为缩短输出内容的长度可以做一些加速，但是又会遇到之前说的推理不完全的情况。所以直接使用LLM来做分析，效率会是一个很难逾越的瓶颈。

5. LLM大型语言模型的可预测性、可解释性、可控制性

大模型的不可控制是另一个难以解决的问题。这里说的不可控制是指在生产应用场景下，一个分析工具所必须具备的可维护能力。我们都知道GPT-4在分析代码的时候经常会出现误判，其实误判并不可怕，所有的分析工具都会有漏报误报。最关键的问题是，当出现漏报误报时，用户无法针对性的对错误的结果进行修正，错误永远会出现。即使重新训练模型，也很可能无法实现想要的修正，只能期待什么时候这个大模型再一次进化，涌现出新的能力。这就导致整个工具的使用处于一种不可控的状态。这对于追求精确、高效、规划的代码分析任务来说，是难以接受的。

上面我们提到的这些问题，有些可以通过工程实践来缓解，有些可能只有等GPT-5、GPT-6出现才知道能不能解决。至少从GPT-4的表现和相关的文献材料来看，我们觉得利用LLM大型语言模型来进行代码分析任务，不是一个更优的选择。

LLM大型语言模型对静态分析任务的辅助作用

基于上述的实验与论证，我们发现LLM并不能替代现有的静态分析技术。那静态分析工具是否能从LLM的大发展中获得其他的好处呢?答案是肯定的。

在上文中我们已经阐述了一直以来困扰静态分析产品的两个难题：分析精度和使用门槛。由于计算理论的限制，我们在静态分析的场景下无法做到对程序运行状态的完全还原，也就导致了静态分析技术总是存在着漏报和误报。误报意味着额外的工作量，这也是很多开发人员不愿意使用这类工具的主要原因。研究人员经过了数十年的努力，一直在努力提升程序分析技术的精确度，但是时至今日，仍然有非常多的技术难点。随着软件研发的规模化和复杂化，这些问题变得愈发难以解决，比如数据断流、函数摘要、复杂控制流的约束求解、跨模块/应用分析等等。

现在GPT-4的出现，为这些快要走入死胡同的难题带来了一线曙光。我们团队从2018年就开始探索AI技术和程序分析技术融合可能性，2019年我们在RAID发表了名为NLP-EYE: Detecting Memory Corruptions via Semantic-Aware Memory Operation Function Identification 的论文，探讨了NLP技术如何能够帮助我们识别更多的危险函数。2022年我们在S&P发表了名为Goshawk: Hunting Memory Corruptions via Structure-Aware and Object-Centric Memory Operation Synopsis 的论文，通过引入更成熟的AI技术，在Linux内核、OpenSSL等多个开源项目中发现了上百个内存破坏型BUG。

除了分析精度，使用门槛过高也是阻碍代码分析工具普及的一大原因。由于分析能力的不足，过去的分析工具提供了复杂的配置接口来帮助提升特定场景下的使用效果，使用起来非常复杂。对于分析结果的解读，同样也有很高的技术门槛，往往是做开发的不懂安全，搞安全的不懂代码，能真正形成闭环让工具辅助开发提升效率的用户很少。而这些涉及到人机交互、答疑解释的场景正是LLM最为擅长的。

LLM大型语言模型所展示的想象空间是巨大的，同时又处在高速的进化中。与其担心哪一天被替代，不如尽早拥抱新时代。

互联网业务安全中机器流量识别与对抗

文｜雷冲

瑞数信息技术（上海）有限公司

摘　要： 本文探讨在金融及证券行业数字化大环境下，对于越来越多的互联网恶意流量，恶意机器人流量的识别与防护技-AntiBot。利用动态对抗技术，结合多层次防护框架，逐渐精准预测各类未知与新型攻击，达到最佳的Bot防护效果。采用“动态安全”为核心技术，以Bot 防护为核心功能，结合智能威胁检测技术、行为分析技术，将威胁提前止于攻击的漏洞探测和踩点阶段，实现AntiBot，确保应用安全和业务安全的最佳实践。

关键字： 恶意机器人流量、识别与防护、动态对抗技术、智能威胁检测技术

背景介绍

《证券公司网络和信息安全三年提升计划（2023-2025）》提出了6大提升重点任务，其中针对“强化系统研发测试管理能力”，“夯实系统运行保障能力”，以及“健全网络和信息安全防护体系” 等技术能力要求方面多次强调业务应用安全，主动防御能力，互联网安全保障等。

就互联网安全威胁而言，根据国内专业网络安全专业分析组织的分析显示，随着数字化不断推进，公有云、私有云、混合云等云计算机技术的广泛应用，来自互联网的攻击威胁已经从2017年前的以重点针对AA级券商和C级券商为目标攻击威胁，演变为覆盖所有券商乃至关联企业的无差别攻击。助长这些恶意行为的技术之一便是互联网中恶意机器流量。因此，需要有效的互联网机器流量识别与对抗 --Antibot。

互联网业务安全中恶意机器流量的威胁分析

恶意机器流量

所谓Bot，是Robot（机器人）的简称，一般指无形的虚拟机器人，也可以看作是自动完成某项任务的智能软件。Bot流量，指在互联网上对 Web网站、APP应用、API接口通过工具脚本、爬虫程序或模拟器等非人工手动操作访问的自动化程序流量。

在数字技术高速发展的催化下，企业的数字化转型加速，网络空间的流量呈现爆发式增长。据腾讯安全《Bot管理白皮书》统计数据显示，2022年上半年Bot流量约占整体互联网流量的60%，平均每月达到110亿+；在而其中具备恶意攻击性的Bot流量占比则高达46%，恶意Bot流量的危害亟须重视。恶意Bot流量增长趋势迅猛，攻击目标从业务资源型Bot逐步切换为针对业务内容的API型Bot，随着Bot技术的不断迭代，Bot技术被更多地使用在网络攻击上。

Bot流量的好坏由其意图及行为决定，如搜索引擎、统计和广告程序等正常流量能提升网站排名，进行网站监控提升用户体验的Bot被称为良好Bot流量；而利用代理或秒拨IP、手机群控等手段来实现信息数据爬取、薅羊毛、外挂作弊等恶意攻击行为的Bot则是恶意Bot流量。

Anti-bot机器人是指为了防止恶意机器流量（Bot）对网站进行攻击或滥用而采取的一种技术手段。Anti-bot机器人的作用是通过识别和区分人类用户和机器人，阻止机器人对网站进行自动化操作，保护网站的正常运行和用户的信息安全。

自动化攻击

自动化攻击是指利用自动化脚本或工具模拟正常人的行为来实现网络攻击的一种方式。通过借助自动化工具，过去劳动密集型、高智商、高成本的网络攻击，将不再是高级黑客的专属，普通网络罪犯也可以在短时间内以高效、隐蔽的方式对利用网站漏洞进行攻击。

网络攻击在基于AI的对抗学习、自动化工具的应用下找到了新的转型模式，依靠自动化形成更为拟人化和精密化的网络攻击趋势。这类机器人模拟真人的行为会更聪明，更大胆，也更难以追踪，更难以区别于真人的行为。

频繁的数据外泄事件后，身份信息被暴露、贩卖。而网络罪犯可以结合自动化脚本或者工具，轻松利用这些被曝光的个人数据，在短时间内对数百个不同的网站不断进行登录验证，试图盗用账号，乃至发起进一步攻击并从中获利。

对抗自动化工具需要多维度治理：从数据维度来看，需保护核心资产数据信息不受Bot侵害；从业务维度来看，需防护Bot对平台业务稳定性造成影响；从安全维度来看，需保护基

础设置不受扫描器侵害。依托客户端风险识别、安全情报、智能分析，可帮助构筑多层次体系化检测响应防线。

机器流量识别与对抗技术研究

动态安全防护系统Anti-bot采用多种技术手段来辨别人类用户和机器人。其中包括基于行为分析的方法，例如分析用户的鼠标移动轨迹、点击模式等；基于人机交互的方法，例如要求用户进行点击、拖动或输入验证码等；以及基于机器学习和人工智能的方法，通过建立模型来判断用户的真实性。

目前，恶意Bot流量的识别主要通过以下几种方式：

(1) 限制源IP的请求频率：通过定义访问频率阈值，能有针对性地对访问频率过高的Bot流量进行过滤。虽然限制源IP的频率实现起来比较简单，且操作方便，但是如何合理设置频率阈值是需要解决的问题，并且当正常流量突增时，要及时、准确地调整阈值，否则会严重影响业务。

(2) 设备指纹技术：Bot程序可以通过修改各项属性绕过设备指纹验证，对于同一出口设备，会产生误判情况。设备指纹更精细，可达到的防护效果更好，但是防护成本较高。

(3) 基于业务访问链路行为分析：通过Referer字段表示请求的来源位置，对用户访问业务链路的先后顺序进行校验，对于需要明确访问顺序的，如果用户跳过中间步骤则判定为异常访问。但并不是所有请求中都含有Referer信息，此时需要通过探针对请求进行探测监控，但是当业务比较复杂时，不具备普遍性。

为了有效应对恶意机器人，Anti-bot在上述技术之上还可以增加人机交互的要求，例如使用图形验证码、滑动验证码等，要求用户进行人类特有的操作，从而区分机器人。其次，可以使用行为分析技术来识别恶意机器人的行为模式，例如识别自动化的点击、快速填写表单等操作。此外，还可以利用机器学习和人工智能算法，建立模型来判断用户的真实性，提高识别准确率。

但是，随着自动化攻击与安全防护之间对抗的不断升级，提供各类对抗服务的黑灰产组织也越来越多，各类服务例如代理IP服务、图形验证码识别、短信验证码代收、群控设备池、账号提供商等等，可以轻易获取。大部分自动化攻击防护手段被轻松穿透，与此同时又催生了更具拟人特点的全新自动化攻击，这些恶意自动化攻击会通过使用模拟器、伪造浏览器环境、UA、分布式IP等手段给系统安全带来极大威胁。此外，自动化攻击的免费、简单、高效的三大特性，更使自动化攻击呈现愈演愈烈的态势，不断让企业的传统网络安全防线频频失守。Forrester报告显示，由于当前的Waf方案无法处理更广泛的应用程序攻击，特别是由机器人驱动的自动化攻击，已经让企业用户苦不堪言。

机器流量识别与对抗相关技术知识介绍

综上可知，自动化攻击全面升级的新时代，对防火墙防御能力也提出了更高的要求。现有的方法存在成本高、准确性和普适性低等缺陷。因此，我们需要更加有效的自适应Bot机器人流量识别和防护方法。基于访问流量的自适应学习引擎进行深度分析，精确识别恶意Bot流量、合规Bot流量及其他正常流量；结合实时的流量分析特征、业务场景和服务器状态指标，动态生成各类型业务场景防护策略。在精确识别恶意流量的同时有效降低误拦截概率，同时也降低用户使用成本及部署门槛。

动态安全防护系统Anti-bot以一系列“动态”技术为核心，提供应用和业务层面的威胁感知和防御，对黑客和不法分子隐蔽自己，甄别伪装和假冒正常行为的已知和未知自动化攻击，提供企业和个人安全的业务服务，保护企业和个人数据；同时，其“动态验证”技术，可以有效识别客户端是“工具还是人”，针对模拟合法操作的工具行为进行阻拦或者软拦截，为建立新的动态安全防护能力，满足合规要求。

动态安全防护系统Anti-bot的整体架构如下图所示，共分为展示层、功能层、处理层，每个层面分别发挥不同的作用。基本的安全防护能力通过功能层四个动态模块实现，定制化的业务威胁与分析工作，则通过数据处理层和展示层完成。

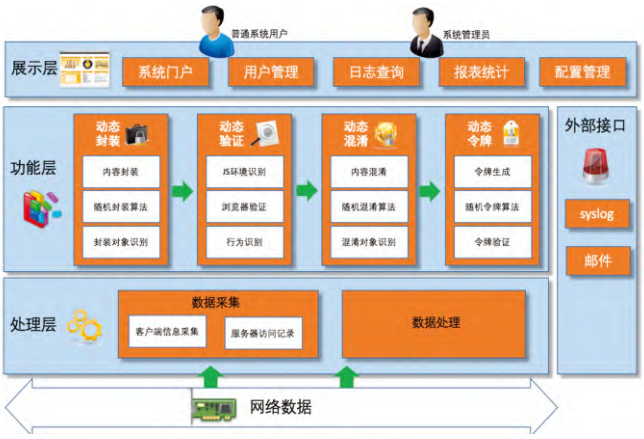


图1 动态安全防护系统架构

(1) 处理层：主要功能包括数据收集、数据解析。通过相关网络配置实现网络流量牵引，识别防护流量将非防护流量直接进行转发，并将防护流量转发至设备引擎；对HTTP以及HTTPS应用层协议解析，并将解析出来的数据（包括请求头部信息，请求参数信息，请求路径信息等）进行存储，供后续模块使用。

(2) 功能层：功能层是系统最核心的组件，即动态防护模块，以“动态技术”为核心包含网页动态封装、动态验证、动态令牌、动态混淆，通过对服务器网页代码对持续动态变换，增

加服务器行为对“不可预测性”；提供面向业务层的主动防御，有效甄别伪装和假冒正常行为的已知和未知自动化攻击。

(3)展现层：提供用户可视化界面，实现用户管理、日志查询、报表统计和配置管理功能。用户管理提供用户创建、用户权限管理、密码管理等功能；日志查询提供图形化查询系统操作日志、审计日志和安全访问日志；报表统计提供图形化展示报表功能，包括告警和定制化报表，配置管理提供站点配置、策略管理等功能，通过界面进行策略调整以及动态修改防护站点相关配置。

动态安全防护系统Anti-bot的设计原理，就是通过对网页代码的持续动态变化，实现对网页敏感内容的隐藏，防止攻击者对网页代码进行深入分析。动态安全防护的核心是对工具的识别，再结合用户行为分析，实现对各种自动化攻击的拦截。

· 动态技术其根本的原理就是判定是“人”的操作还是“工具”操作，识别拦截工具请求

· 动态技术并不依赖“访问频率”，“集中的IP来源”来判断是否为工具

· 动态技术不管这个工具是什么名字，在业务逻辑的哪个环节，模拟了哪类浏览器、是否不断更换工具和改变IP，它判断是否为“工具”，同时，对于高级工具，需要结合行为分析进行识别和阻拦。

动态安全防护系统Anti-bot通过对网页底层代码的持续变化，在网页中插入JavaScript代码，实现对自动化工具的识别；为了保证插入JS代码的安全性，系统通过动态变化技术让用户访问每次看到的代码算法和内容都不同，从而无法预测服务器的行为，进一步做代码分析或者逆向。

“动态技术”的实现源自于四大创新专利技术：动态封装、动态验证、动态混淆和动态令牌。这些专利的应用可以有效的对抗包括自动化攻击和交易欺诈等在内的各种恶意行为，撞库攻击只是一种攻击行为。

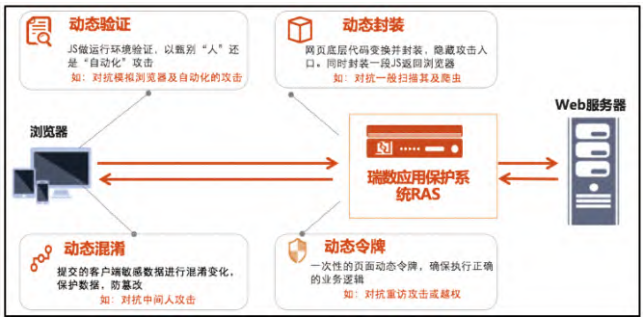


图2 4大核心“动态技术”

1.动态令牌 --为用户端可以合法访问的URL地址分配的一次性“通行证识别码”。用户端每个请求附带的令牌都需要通过服务器端的校验，从而防止违规访问等恶意行为。

2.动态封装 -- 对网站返回内容的底层代码进行封装，将可能被攻击的敏感位置，例如URL、表单和Cookie等转化成攻击者难以读懂的内容，并且每次封装的算法互不相同，从而隐藏了攻击的入口，使攻击者无法预测服务器的行为。

3.动态验证 -- 通过对客户端与服务器的动态双向验证，严密检查运行环境、浏览器指纹、疑似攻击行为等因素，防止恶意终端访问。而且每次验证都会随机选取检测的项目与数量，以增加应用的不可预测性，大幅提高了攻击成本。

4.动态混淆 -- 对网页上敏感的传输数据进行动态混淆，将敏感的用户名和密码等信息全部混淆掉，防止通过中间人攻击等行为进行伪造请求、恶意代码注入、窃听或篡改交易内容。从而有效避免网页挂马、中间人攻击（MITM或MITB）、SQL注入攻击、越权访问等攻击行为。

Antibot动态安全系统利用动态防护技术对恶意机器流量进行：

1.运行环境监测 -- 对包括PhantomJS和Web Driver在内的所有流行自动化工具进行检测，从而针对性的阻止自动化扫描和入侵。

2.浏览器指纹采集 -- 对客户端浏览器的语言、插件、时区信息等指纹特征进行检测，防止模拟浏览器行为的攻击模式。

3.用户行为检测 -- 对用户的操作行为进行检测和分析，包括检测鼠标的点击、鼠标的移动、触摸屏点击、按键行为等特征，从而更有效地防止自动化工具的扫描和入侵。

进而，Antibot动态安全系统通过大数据分析能力，结合业务威胁的特征，对流量进行实时监控。全方位透视自动化攻击的类型、工具、目标和来源。并对攻击者进行画像，建立IP 信誉库、指纹信誉库和账号信誉库，作为威胁情报进行响应拦截，形成安全联防，让攻击者无所遁形。

通过独有的动态技术在前后端采集超过上百个字段，并确保每个字段（特别是终端指纹）的准确性和可靠性，不会被逆向和篡改。通过采集到的信息，多维度判断，在客户端访问还没有到达业务系统前， 就实现人机识别，将整个风控体现延伸到客户端，实现风控前置。

Antibot动态安全系统覆盖 OWASP 定义的全部 21 种自动化威胁的产品。有效识别互联网恶意机器流量，防护互联网业务安全风险，

· 防止站点内容被抓取、转载、刷票、薅羊毛、短信接口滥刷等带来的业务运营风险。

· 防止黑客利用恶意Bot程序进行自动化的撞库攻击、漏洞嗅探、CC攻击等恶意攻击行为。

· 降低大量恶意的爬虫Bot程序流量占用站点资源，造成服务器的高负载，从而影响正常用户的访问速度与体验。

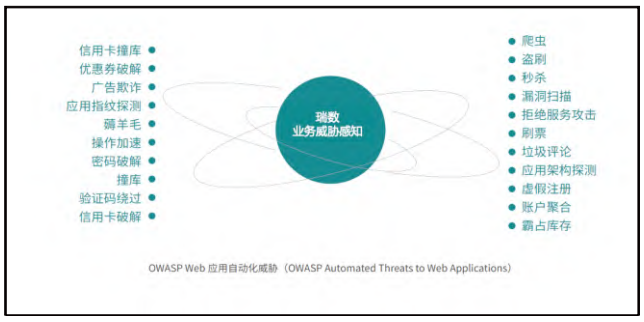


图3 OWASP Web应用自动化威胁Top20

机器流量识别与对抗建设案例、建设方案介绍

某金融证券公司项目案例详情

由于全球人工智能热，部分金融公司开始尝试将AI技术引入客户服务、业务处理等活动中。然而，在体验并接入互联网人工智能的同时，自动化流量以及自动化API数据交互使得互联网业务安全防护的难度进一步增加。

某证券积极探索大语言模型在基础问题解答、客户需求识别、内部效率提升方面的能力的同时在其特定领域开放域模型，比如服务陪伴、知识回答、特定任务处理等业务系统中采用动态安全防护系统Anti-bot对互联网自动化流量进行精确识别与对抗

防护效果

· 黑产团伙识别

对异常来源IP进行深入分析，利用流量自学习能力发现异常IP有很明显的聚类效应，大部分的异常IP都集中在：61.151.*.*、61.129.*.*、101.89.*.*、101.91.*.*这几个网段，明显来自于同一个攻击团伙。攻击者为了绕过防护系统，一直在不停的变换动态IP，且每个IP的访问量几乎不超过1000次，但仍被Antibot动态安全系统系统所识别。

· 短信接口滥用防护

监测到攻击IP：221.**.**.** 通过简单脚本对短信接口持续不断进行轰炸。该IP持续对这个短信接口发起post请求，请求量已接近20万次。且该IP对该路径的访问全被RAS检测为NO_COOKIE_KEY，说明这个IP是通过简单脚本对短信接口持续不断进行轰炸。

· API异常访问防护

访问量最多的API路径已经高达100万次，访问API最多的IP访问量超过10万次；目前API访问主要面临着流量变化异常、简单脚本访问等威胁。访问来源地址主要分布，以N市为主，也有一部分其他来源访问，如H市等。

价值

· 保障业务安全，对抗黑产团伙，对业务的有效投放提供技术保障；

· 对已知和未知的自动化攻击，及各种利用自动化工具发起的恶意行为做到及时、高效拦截，保护业务系统的稳定运行，防止业务受到CC攻击；

· API保护：针对API接口，防止其被滥用并用于谋取利益，监控API的访问行为，针对高频情况等进行防护，防止高频情况等造成的API性能瓶颈。

图4 短信接口滥用检测与防护

某期货交易所项目案例详情

作为全国五家期货交易所之一，隶属于中国证券监督管理委员会垂直管理。是为期货合约集中竞价交易提供场所、设施及相关服务。其拥有快捷、高效、安全、可靠的计算机交易系统。高性能的实时撮合系统分布于全国主要城市的远程交易终端，功能完善的结算、交割、风险监测、信息发布和会员服务系统从技术上确保期货交易的安全运行。为了进一步强化互联网业务安全防护，其将主要互联网业务系统，业务服务平台以及新开发的APP，微信小程序等纳入Antibot动态安全系统。

防护效果

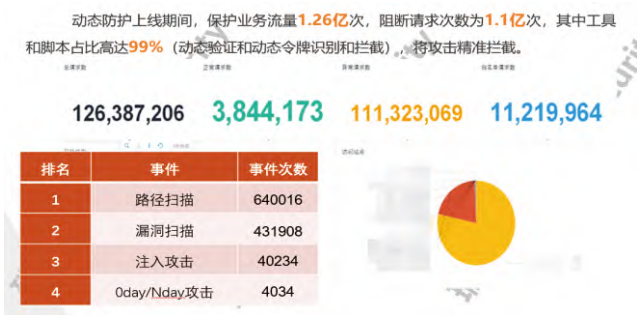


图5 权益侵占防护效果

· 高危业务账号发现

图6 权益侵占分析

· 非法工具识别

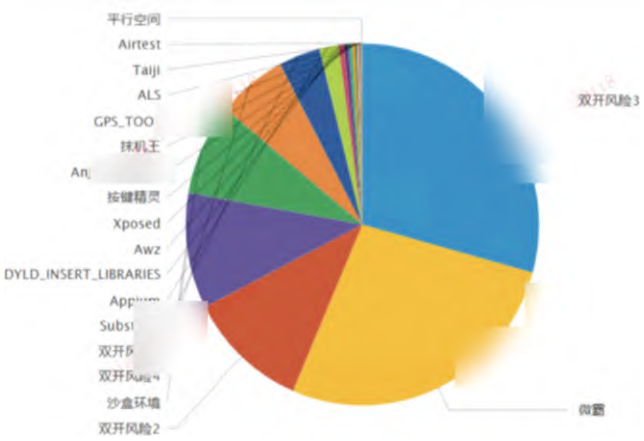


图7 非法攻击检测与识别

措施与价值

动态安全防护系统Anti-bot对系统登录账号进行安全控制监测，增加动态挑战，在人机识别是增加DOM元素干扰，拖动，变形，汉字拼音，识别指定图标，点击图标等；并且进行随机组合，或按百分比动态组合挑战。

丰富敏感账号安全监测与管理，并且与门户系统蜜罐联动。通过动态安全系统对使用弱口令的用户，可以直接拦截，或者返回特定页面，让其修改密码后再进行登录。

利用动态安全防护系统Anti-bot中的动态验证能力，通过Cookie，IP，指纹等组合方式进行限频，避免攻击者通过更换IP，清空Cookie等方式绕过防护；并且增加时间窗口，访问速率多维度限制。

从而，对已知和未知的自动化攻击，及各种利用自动化工具发起的恶意行为做到及时、高效拦截，保护业务系统的稳定运行。

内网拓扑可视化及管控技术

文丨程度

青藤云安全

摘　要： 微隔离技术通过内网拓扑可视化和流量管控，应对内网安全所面临的渗透威胁和管理挑战。微隔离有软件定义网络、虚拟化层防火墙和主机探针（Agent-based）三种实现路线，其中Agent-based路线具有异构环境统管和分布式网络管控的优势。Agent-based技术架构由探针、计算引擎和控制台构成，提供三大核心能力：网络拓扑可视化、流量信息采集、东西向流量管控。本文通过一个实践案例来说明和体现微隔离对内网安全的重要价值。

关键字： 微隔离、内网拓扑可视化、东西向流量管控、流量采集

内网安全面临严峻威胁和管理挑战

在当今数字化时代，企业面临着日益复杂和多样化的网络安全威胁。云计算和移动设备的普及增加了网络边界的复杂性和模糊性，使传统的边界防护措施疲于应对更复杂的安全攻击手段。比如边界防护难以防止内部员工或恶意攻击者通过获取合法访问权限，绕过边界防护设施，直接访问企业内部网络。

随着近几年攻防对抗演习、安全建设工作和行业安全交流的大力推行，越来越多的行业单位和机构已经认识到传统边界防护的薄弱，将安全治理工作的重心转移到内网安全领域。由于内部网络远比边界网络的情况更加复杂，安全管理员面对理解门槛和运营难度更高的内网安全问题时，难以开展工作。在实际管理工作过程中出现的挑战主要体现在以下几个方面：

欠缺对业务的深入理解而难以梳理安全建设思路

随着整个证券期货行业数字化转型的推进，传统的柜台业务已发展为完全的线上服务或线上线下双线共存的业务形态，带来大量的软件应用开发和部署，数据中心里业务系统的数量爆发性地增长，安全管理对象激增。与此同时，网络空间规划不合理的弊病在数据中心规模化的过程中一并暴露，导致安全管理问题更加复杂。而安全管理人员关于新系统的业务重要性、敏感性、复杂程度、内在通信逻辑、对外暴露面等各个方面的理解却未能一同增长，难以梳理安全管理工作的分类和优先级，安全建设的推进因而迟滞。

难以发现内网异常行为并有效处置

内网攻击具有隐蔽性和内部知识的特点，攻击者往往可以利用已存在的合法访问权限，在内部网络中进行活动，从而隐匿其攻击行为。内网攻击行为通常是低调和渐进式的，攻击者往往会在长时间内悄悄地进行活动，以避免被发现。他们可能利用合法的身份、弱密码和漏洞来持续地渗透、侦察和利用内部系统。这种渐进性的攻击行为使得难以及时发现攻击迹象，从而降低了处置的效果。另外，内网攻击行为具有高度的变化性，攻击者可以使用多种技术和工具来隐藏其攻击行为，例如横向移动、欺骗、隐蔽通信等。这使得传统的安全监控和检测系统难以有效应对。对于大型组织而言，内部网络通常庞大而复杂，更是让防护工作难以开展。

许多组织已经采用诸如HIDS之类的主机安全产品来守护内网安全，对这类渗透攻击的识别的确做出了积极贡献，但这类产品主要用于事中发现，缺少事前防护和事后处置的能力。而EDR这类带有主动防御能力的产品不能友好适配业务服务器的特性，其提供的自动处置能力对业务连续性可能造成负面影响。安全管理员缺少能有效、高效处置已知威胁的手段。

业务部署形态各异和业务迁移让管理策略难以统一且不可持续

由于业务系统的上线时期、功能作用不同，其部署的形态可能有所区别。传统的选择是将应用部署在虚拟机或物理服务器上，随着云计算、大数据的普及，大量应用系统已采用云化部署的方式。在证券期货行业内还不乏采用了更先进的容器化部署方案的组织，业务系统被拆分为众多细小的微服务，物理位置变得愈发分散。在大型网络中心内，混合部署环境是常态，不同业务环境的安防和运维内容不同，安全策略需要针对性地适配。而且随着业务云化、容器化的加深，安全策略需要随着业务部署形态的改变而调整，这对于安全管理员而言无疑是巨大的负担。

微隔离技术介绍

应对内网防护挑战的一个有效工具是微隔离。

自Gartner在2015年提出微隔离以来，对其核心能力的要求聚焦在东西向流量的隔离上（当然对南北向隔离也能发挥作用），一是有别于防火墙的隔离作用，二是满足云计算环境中的真实需求。微隔离顾名思义是细粒度更小的网络隔离技术，能够应对传统环境、虚拟化环境、混合云环境、容器环境下对于东西向流量隔离的需求，重点用于阻止攻击者进入企业数据中心网络内部后的横向平移。微隔离平台从以下几个方面解决内网流量管控的问题：

1)直观展示业务访问关系，帮助梳理安全构建工作：以多视角拓扑图展现工作负载之间、业务系统之间的访问关系，提供统计和分析数据，辅助梳理业务应用的暴露面、访问基线和管理优先级；

2)细粒度管控访问，提供异常访问处置能力：按业务系统、组件角色等多维度标签对工作负载进行分组管理，基于标签可配置工作负载、业务应用之间的隔离策略，填补区域内管控的空白。对偏离访问基线的异常流量进行告警和记录，可从网络侧对攻击事件进行处置，隔绝失陷工作负载的网络，切断恶意连接；

3)统一策略应对异构部署架构，自适应策略降低运维负担：提供可统一用于纳管对象的策略，计算引擎实现策略转换对接异构的底层环境，将管理员的工作重心从环境适配牵引到业务层面。随着环境变化自动调整策略，保证策略作用的一致性和稳定性，减少人工参与。

从系统架构的角度来看，微隔离技术可以通过三种方式实现：软件定义网络（SDN）、虚拟层防火墙、基于主机探针。

图1 三种微隔离实现方式

（一）软件定义网络路线

随着SDN的引入，基础设施技术也得到了改进，使得组织能够选择在微隔离中部署和使用SDN控制器。这种选择可以通过与SDN控制器API对接的第三方安全工具实现，也可以通过直接进行SDN编程来实现。这一方法对那些在网络工程中投资于SDN，并希望从单一供应商获取SDN技术的组织尤为有吸引力。

然而，这套基于基础设施技术的实现方案更适合相对静态的私有云部署，而无法有效保护有可移动性、可扩展性的工作负载，比如基于动态混合云环境的工作负载。这种类型的微隔离可能会引入阻塞点，降低网络性能，使网络工程复杂化。

（二）虚拟化层防火墙路线

在VMware的NSX中模拟了SDN控制器的功能，可以实现虚拟化层面的微隔离。对于大规模使用VMware的组织非常适用，能保持用户一致的使用习惯和操作流程。然而，这也局限于特定的虚拟化平台，不适合那些同时使用混合云和虚拟化技术的组织，无法跨环境提供保护。

（三）基于主机探针路线

让控制端驻于工作负载上，直接使用主机防火墙，利用其成熟、灵活、完备的访问控制能力，最大程度发挥已有资源的效能。将安全策略与管控对象在物理层面直接绑定，保证了策略可随着工作负载的移动而迁移，对于动态环境的适配是最佳选择。而且探针可兼容适配不同类型的工作负载，轻松适配异构环境。

相较于其他技术路线，基于主机探针的技术实现相对复杂，需要解决大量探针管理、策略分发、动态调整等问题。但其带来的收益也更为可观。

Agent-based技术架构

在三种技术形态之中，基于Agent的实现方案占据主流位置，是国内外厂商的首选。其整体架构包含主机探针、计算引擎和控制台。

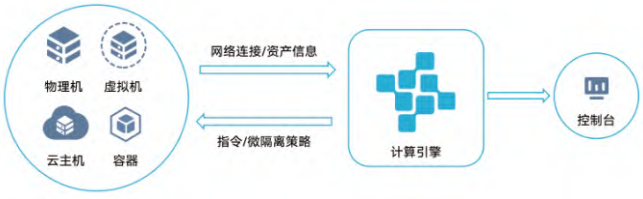


图2 Agent-based微隔离技术架构

1)轻量的主机探针可一键安装在物理服务器、虚拟机、云主机和容器上，在混合的IT环境中也可直接适配，管理员无需关注底层部署架构，只用关注业务逻辑。主机探针以低资源消耗的状态持续采集网络流量数据，接收管控中心的指令并向主机防火墙写入网络策略，以及实时监控异常访问。

2)计算引擎负责策略计算以及可视化渲染。将标签形式定义的策略转换成IP、端口、协议的形式写入主机防火墙中；在工作负载的IP、标签发生变化后，自适应调整防火墙策略以满足相适应的流量管控要求。计算流量数据在拓扑图里的展示逻辑，以及与策略的适配性，为业务梳理提供依据。

3)控制台在web端呈现。以易读直观的方式呈现业务访问关系和网络策略，提供策略配置和管理能力，让管理员高效简便地管控网络访问。

相较于另外两种技术路线，Agent-based架构主要具备

两个方面的优势：1）支持混合异构环境下工作负载的统一管控，用形式一致的网络策略进行管理，极大减轻策略运维负担；2）分布式网络管控能力，不存在唯一的网络堵点，流量处理效率高，对通信效果的影响可忽略不计。

网络拓扑可视化

数据中心业务流量的可视化展示对于管理员深入理解业务，为后续流量管控提供依据有重要意义。

框架设计

网络拓扑图涉及流量数据存储、数据加工、前端渲染等各环节，模块框架如下图所示：

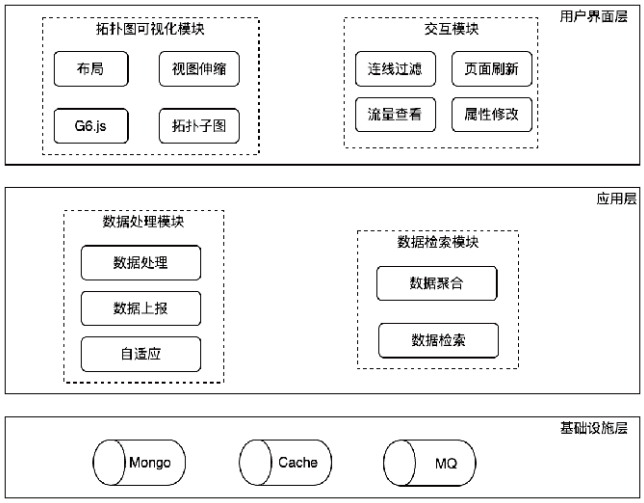


图3 网络拓扑可视化技术架构

· 用户界面层

用户界面层分为拓扑图可视化模块和交互模块。拓扑图可视化模块将从后端获取到的数据，利用可视化库如G6.js及前端框架如React渲染成带有节点（物理机、虚拟机、容器）以及节点之间连线（TCP/UDP访问）的拓扑图，支持视图切换、子图钻取、画布缩放等功能。交互模块负责数据展示、数据过滤、工作负载属性修改等与后端数据交互的功能。

· 应用层

应用层主要进行数据处理和检索，为用户界面层提供数据和API。数据处理模块负责对探针上报的数据在存储之前进行处理，包括策略匹配、聚合等，以及在策略变更时，自适应更新存量数据的策略匹配情况。数据检索模块为用户界面层的交互操作提供API和逻辑实现，如流量数据过滤、视图变换、信息展示等。

· 基础设施层

基础设施层通过引入数据库及缓存、消息队列等中间件，实现系统各功能模块的解耦，提供数据复用能力，同时提高系统响应效率。

（二）重难点问题和解决思路

数据中心工作负载数量可能非常庞大，导致拓扑图需渲染大量节点和连线，给系统内部的数据存储、检索和传输，以及前端浏览器的性能都造成巨大的压力。如何有效应对大规模数据，给管理员提供流畅的使用体验，是需要重点解决的问题。

· 存储优化

在数据库选择方面，要考虑高性能、可扩展的数据库。比如MongoDB。MongoDB是一个功能强大、灵活且易于使用的数据库管理系统，适用于各种类型的应用程序，尤其适合需要处理大量非结构化数据和需要高可用性、可扩展性的场景，其在数据分片方面的优良特性，让检索效率更高。若使用传统的MySQL存储，则会存在查询效率低下、分库分表实现复杂等问题。

而在数据结构方面，为了减轻存储压力，应对数据进行适当的聚合，比如源IP、目的IP、目的端口、协议、进程等五元组相同的流量数据被聚合在同一条记录上并计数。同时建立合适的索引，进一步提高查询效率。

· 处理优化

为降低系统内部的网络访问开销，可使用分布式内存缓存，如Guava Cache + Redis。Guava Cache是一个功能丰富且易于使用的缓存库，它能够帮助开发人员简化内存缓存的管理和使用，并提供灵活的配置选项和并发支持，以提升应用程序的性能和响应速度。Redis的发布/订阅模式提供了一种简单而强大的消息通信机制，具有实时性、扩展性和解耦性的优势。二者结合保证在高可用环境下各节点内存数据一致。

· 渲染优化

在UI层可以通过特殊的技巧来优化性能表现。

1）通过减少非必要图元的渲染来提升性能。拓扑图由各类图元构成，图元可以是节点、连线或标签等。在执行界面交互时，展示关键图元并隐藏其他图元，可降低性能压力。比如拖拽画布时，只显示节点图元而隐藏连线图元。

2）通过视图的设计，将拓扑图拆分成若干子拓扑图的组合，子拓扑图内部的细节需下钻之后展示，以此减少同一界面中图元的数量。

3）为避免数量过大导致页面卡顿不可用，可对渲染数量做边界限制，并引导使用者进行筛选以降低渲染数量。

流量信息采集

主机探针将工作负载的出入站流量上报至计算引擎，用于流量可视化和策略计算。区别于流量型分析产品，微隔离关注的是访问关系，即IP、端口、协议、进程等信息，并不解析

数据包内容。当前主流的流量采集方式有如下几种。

· **网络连接快照**

对于一个工作负载，固定时间间隔使用 Netlink 从内核获取当前NetWork NameSpace的网络连接信息，生成快照。前后两次快照的差异代表在这段时间内产生的新连接。这种方式实现简单，但缺点是数据精度不高，如果采样频率过低，采样间隔之间的流量会丢失。

· **PCAP抓包**

PCAP (Packet Capture) 是一种网络数据包捕获技术，用于在计算机网络中捕获、分析和存储网络数据包。具有实时、灵活、安全等诸多优点，缺点是抓包粒度只能到主机端口，不能抓取进程信息。需要再根据端口关联与监听端口绑定的进程，来获取进程数据。

· **NFLOG**

NFLOG（Netfilter Logging）是一个Linux内核功能，它允许用户空间程序捕获和处理网络数据包。NFLOG通常与Netfilter（Linux防火墙框架）一起使用，用于在数据包经过网络堆栈时将特定的数据包流量传递到用户空间程序进行进一步处理。在Netfilter的链表中写入NFLOG规则，将满足指定条件的流量记录成日志信息，再读取并向服务端上传日志数据，实现流量采集效果。其弊端同样是无法直接获取进程信息，需要通过其他途径关联。

· ETW

ETW（Event Tracing for Windows）是一种在Windows操作系统中实现高性能事件日志记录和跟踪的机制。它提供了一种可靠的方式来收集和分析系统和应用程序生成的事件数据，以帮助开发人员进行故障排除、性能分析和系统监控。ETW机制基于事件提供者（Event Provider）和事件消费者（Event Consumer）的模型。事件提供者是生成事件数据的组件，可以是操作系统、应用程序、驱动程序或其他软件组件。事件消费者则是收集和处理事件数据的组件，可以是日志记录器、跟踪工具、分析工具或自定义应用程序。网络连接事件是ETW支持的众多事件类型中的一种，可用于微隔离平台的流量数据输入。

东西向流量管控

数据中心内部东西向流量隔离采用覆盖（Overlay）模式，以基于IP的基础网络技术为主，在对基础网络不做大规模修改的条件下，实现微隔离在网络上的承载，并与其他网络业务分离。

主机防火墙

基于主机探针的微隔离平台并不提供软件防火墙，而是借助主机防火墙实现网络控制效果，下面介绍两个主流系统平台的防火墙。

· **iptables**

iptables是Linux系统上的一个强大的防火墙工具，可以通过配置iptables规则来控制网络流量的传输和访问。通过在iptables“四表五链”中设置不同规则来实现不同的访问控制效果，如放行、拦截、转发、包修改等。所谓四表指的是：raw、mangle、nat、filter，五链指的是 PREROUTING，INPUT，FORWARD，OUTPUT，POSTROUTING链。

· **WFP**

Windows Filtering Platform（WFP）是Windows操作系统中的一个网络包过滤框架。它提供了一种在操作系统级别进行网络流量过滤和检测的机制，通过其提供的API向防火墙内核写入控制策略，实现对网络流量的细粒度管控。

流量管控技术要点

· **基于工作负载身份的策略形式**

在云化和容器化普遍的现代数据中心里，工作负载的IP不再是一个稳定属性，以IP为直接管理媒介的传统访问控制方式采用静态策略，当工作负载扩容、缩容或漂移的时候，原有的策略不再适用新的业务环境，由人工调整运维策略负担巨大，难以持续管理。微隔离平台在IP之上增加一层Overlay，暴露给使用者的是标签、分组等代表工作负载身份的属性，基于这些属性配置的策略经计算引擎转换成防火墙可识别的IP形式策略。这样的做法带来两方面好处：

1）由于使用自然语言描述的标签，策略含义容易理解；

2）工作负载业务性质发生改变后，调整标签、分组即可继承控制策略，显著降低运营成本。

当然，这样一层转换设计对系统的计算能力提出了高要求，策略转换的稳定性、效率要有严格保障。

· **策略自动生成**

为了进一步减轻对存量业务的策略构建以及后续运营的负担，系统应当具备根据所采集的流量批量、快速、自动生成策略的能力。首先，应能将访问行为一致的流量聚合在一起，对原始流量数据进行归纳压缩，如应用服务器对数据库集群各节点的多条访问流量，可聚合为应用服务器访问数据库集群这一条访问关系。然后，系统能根据聚合流量推荐合适的策略形式并最终生成策略，免去管理员手动配置策略参数的繁冗工作。

· **策略模拟测试**

不完整的策略可能导致业务故障，因此在策略真正生效之前应当有模拟测试阶段。系统将流量与策略进行匹配比对，对偏离策略的流量进行标记，而不对其进行拦截，管理员由此调整策略以确保完美贴合业务要求。直到策略调校完善后再真正以阻断效果运行。

· **策略自适应**

策略自适应指的是通过对工作负载IP、标签、分组等属性

的持续监控，当属性发生变化时可自动计算相适应的新策略，及时调整防火墙管控行为。主要场景有：

1）由于网络运维的需要或容器漂移现象导致工作负载IP发生变化，主机探针通过定时获取系统IP或监听IP变更事件，发现IP变化并将其上报给计算引擎，后者向相关工作负载重新下发新的策略。

2）虚机迁移或集群扩缩容，系统根据工作负载标签的变化计算新的策略，实现策略的及时调整。

· 规则冲突检测及兼容适配

微隔离平台一般以接管主机防火墙的模式运行，防火墙中已存在的规则将被执行优先级更高的微隔离策略屏蔽，这样的做法将防火墙管理权限集中收回到微隔离平台，达到统一管理及防止私自篡改的目的。但这样的模式也可能导致原本用于特殊业务目的的规则失效，反而影响业务，比如对流量进行转发的特殊规则被屏蔽后导致流量无法正常转发。因此系统应能检测防火墙中已有的规则并分析是否可能和微隔离策略有冲突隐患，这一特性可能依赖识别规则库，效果取决于规则库的丰富程度。

但也不乏需要在保证原有规则发挥作用的前提下执行微隔离管控逻辑的情况，系统应额外提供防火墙兼容模式，通过调整规则的优先级或写入位置来实现规则共存。典型的场景是运行Kubernetes（k8s）的宿主机，其防火墙被k8s规则重度占用，缺少兼容模式将无法在保证容器正常通信的同时管控宿主机的网络服务。

落地实践案例

在业界已有不少微隔离实践方案，帮助企业单位清扫了业务不可视的障碍，建立起可靠的内网防护围栏。下面以某证券单位的实践过程和效果为例，深入了解内网拓扑可视化和控制技术产生的重要价值。

项目实施需求

实施对象包含生产及测试环境共近1万台主机，涉及虚拟化平台、云平台、本地数据中心，涵盖Linux和Windows主流操作系统。在部署微隔离平台之前，内网隔离手段主要依靠防火墙，实现区域间隔离，隔离粒度粗，同属一个网络区域的业务系统和工作负载之间没有做任何隔离控制。安全管理员希望实现细粒度的管控效果，对工作负载和业务系统级别的流量进行限制。

实施过程

1. 资产梳理

在评估实施方案阶段，发现资产管理混乱，不清楚工作负载所属业务系统，缺少基本的先验知识会导致后续策略配置受阻。所以优先梳理工作负载所属的业务系统，通过流量数据定位有紧密联系的工作负载，通过和运维部门、业务部门的协作明确归属关系，在微隔离平台中对工作负载按照业务部门、安全等级、业务系统等多层级进行分组。

2. 流量学习及暴露面分析

所有工作负载经过3周的流量学习，工作负载之间的访问关系绘制基本稳定。基于流量学习的结果主要完成两方面的分析：定位互联网暴露系统、定位空闲端口。从流量方向可找到与互联网直接相连的业务系统，优先对这部分系统进行管控。筛选出存在无流量端口的工作负载，核实这部分资产是否有风险敞口过大的问题，可通过策略屏蔽不应开放的端口。

3. 策略配置

基于主动学习到的IP、端口、协议等信息，协同业务部门对采集到的访问关系进行核对，判断是否符合正常的业务要求。基于工作负载的分组、标签配置访问控制策略，定义受信的访问基线。由于管理对象数量庞大，分阶段完成策略配置，第一阶段仅对存在高危攻击风险的端口进行管控，在后续阶段逐步完善所有业务端口的策略配置。

4. 测试及阻断

以告警模式运行策略，对偏离基线的访问进行告警反馈，优化调整策略以保证完整贴合业务流量。在这个阶段流量不被阻断，以防不完整的策略影响业务连续性。经过1个月的模拟测试，将策略切换至阻断状态，真正对流量进行受信管控。

5. 策略运营

建立业务变更和上下线的线下申报流程，审批通过后，在业务系统发生变更之前调整策略，再实施变更，以保证流量管控效果和业务访问要求的同步。

实施效果总结

通过在混合环境下实施细粒度的微隔离管控，结合流量可视化能力完成资产从无序到有序的梳理、对内网隔离工作划分执行优先级，配置系统级别、工作负载级别、端口级别的细粒度策略，有效阻断横向移动路径，提升纵深防御能力。

身份安全检测技术的发展与应用

文｜李帅臻

北京中安网星科技有限责任公司

摘　要： 随着IT基础架构的云化和复杂化，传统的边界安全模型变得越来越模糊，身份已成为企业防护的新边界。传统的安全产品无法有效应对新的威胁。因此，保护IAM、AD、PAM等身份基础设施成为当务之急，ITDR的出现，正是从这个身份维度深入解决这个传统的安全检测盲区中存在的潜在风险，本文将深入浅出分析ITDR技术的发展与应用。

关键字： 身份安全、网络新边界、身份防护、防护盲区、ITDR

概述

网络安全是当今信息时代中至关重要的一个议题。随着科技的迅猛发展，网络已经成为我们生活的重要组成部分，无论是个人、企业还是国家，都依赖于网络进行信息传输和交流。然而，网络的普及也带来了一系列的安全隐患和风险。因此，保护网络安全成为了当务之急。首先，网络安全对于个人而言至关重要。我们的个人信息、财务数据、社交媒体账号等都储存在网络上，一旦这些信息落入不法分子之手，就可能导致严重的个人隐私泄露和财务损失。其次，对于企业而言，网络安全是商业成功的关键之一。企业的核心竞争力常常依赖于创新的技术和商业机密。如果这些重要信息遭到窃取或篡改，企业将面临严重的经济损失。网络攻击者可能利用恶意软件、网络钓鱼等手段，入侵企业的网络系统，获取关键信息，甚至制造瘫痪性的攻击，这将对企业的运营造成严重影响。此外，国家安全也紧密依赖于网络安全。现代社会的重要基础设施，如电力、交通、通信等，都与网络紧密相连。

随着当下整个IT基础架构逐渐云化及复杂化，身份成为了企业防护的新边界。过去的IT架构相对简单，传统的安全防护模型是以边界设计为核心，安全信任级别跟位置是强关联的。边界设计的网络安全方法是先连接，后信任，在网络边界验证用户身份，如果用户被认定为是可信任的，就能访问该网络内的数据和资源。过去的很长一段时间内，企业通过对各类边界层层防护拥有了强大的纵深防护能力，但如今IT架构的云化和复杂化，身份本身成为了企业新的边界，传统边界类的防护方案开始捉襟见肘，无法防护新IT架构下新场景的威胁。承载企业身份相关的身份基础设施逐渐成为主要的攻击对象，如IAM、AD、PAM、4A等。这些身份基础设施通常具有保存密码多、控制节点多、网络权限广的特点，对攻击者而言是核心的攻击对象，对企业而言则需要重点防护，而过去网络安全市场并没有针对用户身份的针对性的安全防护产品或解决方案，这也是当前网络安全面临的新挑战。

身份安全威胁检测与响应（ITDR）

2022年7月，在Gartner发布的《2022安全运营技术成熟度曲线》报告当中，一项新的技术被正式提出——身份威胁检测和响应（Identity Threat Detection and Response,ITDR），该技术此前多次出现在Gartner发布的安全趋势报告当中，即对身份安全在未来安全领域的价值认可。

图1 Gartner2022安全运营技术成熟度曲线

在Gartner《2022安全运营技术成熟度曲线》报告中，ITDR被列为新兴技术，其效益等级为高，目标受众有着5%至20%的市场渗透率，这代表着Gartner对这项技术应用价值的潜在认可。从技术成熟度上来看，ITDR技术本身成熟度较高，Gartner预期未来2-5年即可达到主流应用。

报告中Gartner对ITDR技术的正式定义为：身份威胁检测和响应（ITDR）包括保护身份基础架构免受恶意攻击的工具和流程。他们可以发现和检测威胁、评估策略、响应威胁、调查潜在攻击并根据需要恢复正常操作。

对于ITDR技术的重要性，Gartner解释为随着身份变得越来越重要，攻击者越来越多地将目标对准身份基础设施本身，组织必须更加专注于保护其IAM基础设施。只有经过授权

的用户、设备和服务才能访问您的系统，ITDR技术将为身份和访问管理（IAM）部署增加额外的安全层。

也就是说，Gartner定义ITDR这一全新技术，寄希望于解决双重趋势推动的核心问题——身份安全。双重趋势之一是安全边界的转变，之二是围绕着这一安全边界（身份）展开的攻击已经非常普遍，且缺乏专业的威胁检测和响应流程。

身份是网络新边界

在网络安全中，身份是指用于区分其他个体的一种标识。它可以用于标识一个人，也可以用于标识一个机器、一个物体，甚至一个虚拟的东西（如进程、会话过程等）。因此，网络环境下的身份是在一定范围内用于标识事、物、人的字符串。攻击者越来越多地使用凭据填充、网络钓鱼和其他身份攻击来瞄准云服务和基础设施。根据 Verizon 的年度“数据泄露调查报告”，估计 2021 年 85% 的 Web 应用程序攻击使用窃取的凭据，而微软估计 70% 的攻击始于网络钓鱼，这是另一种以身份为中心的攻击。

过去我们对安全边界可以由防火墙来定义，到Web2.0时代出现了Web应用防火墙。随着IT基础设施和应用向云、大、物、移转变，以及攻防技术的演变，身份已然成为新的边界。

其中前者其实非常好理解，如我们远程办公、移动应用，绝大多数的调用的都是云端程序，而非本地应用。从攻防技术角度来看，过去政府网站最常见的攻击是页面篡改，现在进入数字时代，更多的是以窃取政务数据为主，同时整个的攻击链路也在发生转变。

与过去攻击过程不同的点在于，当下攻击者一旦获取到一个用户的凭据，即可从外网使用该凭据登录VPN等系统，轻松突破网络边界，在复杂的攻击链路当中，身份将是一个核心的链路点，更是关键的检测点与阻断点。攻击链路中身份是核心要素，趋势定义了身份安全的重要性，就需要有相对应的安全技术解决这一风险。

由此看来，Gartner定义ITDR技术，可以理解为基于身份的“防火墙”产品，将围绕着企业的身份基础设施，实施全面的基于身份攻击的检测和响应。

图2 万物互联的核心是身份

身份防御是现有网络安全体系的防护盲区

纵观网络安全的发展历程，IT架构的变革长期驱动网络安全行业，IT架构变革会带来新的威胁挑战。回顾15年前的IT架构，单一且刚需，比如曾经的网络边界防火墙。到后面发展到Web2.0时代，用户与互联网开始产生大量交互，此时web应用防护（WAF）开始成为标配。如今我们进入云原生时代，企业的边界愈加模糊、复杂。其中身份作为企业联接万物的控制点，仍旧贯穿所有的业务场景，身份成为了企业的新边界。在可预见的趋势中，身份威胁检测一定是当下及未来的必然产物。

攻击技术的变化是攻击事件的核心，诸如BlackHat这样的会议中身份类攻击逐渐成为讨论趋势，当下身份已经贯穿整个攻击链路， 从信息探测的身份钓鱼，到过程中基于身份的横向权限拓展，到攻击结束后的身份后门维持充斥在攻击的各个环节，如此我们能够看到身份类攻击是当下最新的攻击向量、攻击趋势。

当前针对身份的攻击愈演愈烈，即使如此企业面对身份攻击仍显得力不从心，在这个过程中存在多方面的痛点：

▶外部身份威胁

企业外部的身份连接信息成为攻击者验证的猎物，常常采集企业对外暴露的身份信息分析后针对其进行攻击。

▶内部身份威胁

身份是一个人在数字世界的映射，一旦内部出现心怀恶意的内鬼或疏忽大意的员工必然会出现失陷账号与失陷主机导致的各种内部威胁； 身份凭据滥用，账号管理松散，密钥管理混乱极易引发安全问题。

▶身份设施割裂无法集中监控

对于企业内部而言，不同的供应商使用独立的认证源，企业无法做到统一身份基础设施，如企业的公有云、私有云、本地办公设施等身份源存在必然的割裂；集团子企业使用不同的身份源；部分产品无法对接企业身份源，未来这一情况也无法得到根本的改善。这造成企业内部统一认证身份设施割裂，内部多个身份源无法统一观察与监控，且存在大量独立的认证源存在监控死角，仅仅依靠身份设施自身的安全监控能力是无法满足企业管控需要的，企业如果要进行安全分析与身份溯源往往力不从心。

▶身份威胁监控能力不足，安全团队人员不足或能力有限

身份威胁监控能力不足，安全团队人员不足或能力有限，深陷不对称的“安全战争”之中。传统的安全威胁是以漏洞为基础，漏洞总是由攻击者掌握，而防守者掌握并加入到企业防护体系中的周期往往是以月记的，这常常会陷入到攻防不对称的状态中。

因此通过对攻击者行为的预测就显得格外重要，身份检测就是这样一个范式，可以预测攻击者行为。但企业身份威

胁安全监控缺乏监控维度与规则，企业被攻击之后无法快速溯源，无法回答身份的调用过程是如何扭转的。

为了顺应新的IT架构变革，更好地应对云时代的到来，近几年来企业开始应用身份认证和管理类方案，如IAM、IGA、IDaaS和 PAM等，此类方案主要侧重于授权和身份验证，确保合适的人可以访问他们需要的文件和应用资源，但却疏忽了身份威胁检测和响应的能力，同时这些设施本身也带来了巨大的攻击风险。

伴随着身份认证管理方案的普及，越来越多的攻击者将攻击目标转向具有高攻击价值的身份基础设施。攻击者通过窃取身份设施中的合法身份进行利用，在内网中横向移动而不被发现，也能使用身份设施中访问权限来窃取更有价值的数据，例如员工和企业的敏感个人信息或财务信息等。

而目前所有的安全防护设备及解决方案中，均为通过流量、日志分析等方式，根据现成的漏洞利用规则、攻击特征等进行防御来自互联网的攻击，但是身份攻击在大多数时候均为利用正确的用户凭据进行攻击，而这种攻击在常规的安全设备中，均被视为正常的通信特征，对于传统的网络安全体系，身份攻击正是其中的监测盲区所在，ITDR正是为了解决这样的监测盲区，通过全流程追踪用户身份的活动，判断其异常行为，发现未知的攻击威胁。

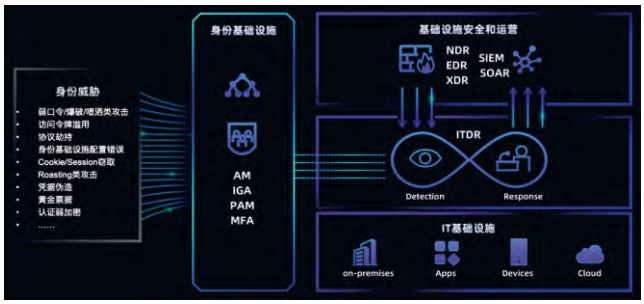


图3 ITDR作用关系示意图

身份防护对于网络攻击可见性大于任何一种安全防御手段

从攻击的角度来看攻击者的攻击过程抽象出来看可以观察到三个必须的步骤，即找到目标、寻找合法凭据、最后登录目标。即便是我们经典之一漏洞永恒之蓝漏洞也是需要指定一个指定目标之后通过远程溢出或其他方式获取到目标计算机的最高权限后登录，通过获取到的计算机权限后再继续通过重复同样的攻击方式继续攻击。我们从这样的视角发现，凭据、登录等关键词都与身份相关。

从防御方的视角我们也抽象到宏观来观察，网络安全的核心三大支柱分别为资产、身份、权限，与资产相关的有漏洞管理、配置管理等；与身份相关的主要是认证与信任；与权限相关的主要是权限访问控制。实际上我们今天的安全产品大部分都在解决这里面的单个或多个问题。身份和权限在整个检测与防护当中扮演着非常重要的角色。

试想一个场景，如果一起攻击事件发生，攻击者均使用正常的用户凭据进行登录认证，窃取企业数据，但是现有的防护方案或杀毒软件无法基于来源用户身份的上下文来共享用户信息进行报告，那么将永远无法得知攻击事件的发生。

如果我们没有对敏感资产的访问进行追踪，也就永远无法知道一个身份对敏感数据的访问是否合适。在目前的整个防御体系中对于资产的防护企业已经做到了较高的水平，但是对于身份与权限的管理还处在较低的水平，那身份相关的威胁具体有哪些?我们又能如何解决这些威胁?ITDR身份威胁检测与响应就是我们的答案。

目前身份威胁大致分为信息收集、权限获取、凭据窃取、横向移动、权限维持五大类，对应的也有ATT&CK的对应TTP。覆盖范围包括凭据、token、账户密码等等。

ITDR能够在事前通过分析物理世界的人与数字世界的身份映射帮助企业掌控全局身份安全，了解企业员工拥有多少数字身份并能够关注每个数字身份的细节。更有身份基线、弱口令等核查功能辅助减少身份攻击面。那么在事前的加固完成之后仅仅能保证当前的时间点的安全问题，对于未来我们在使用的过程中可能会引入新的风险，同时我们需要针对当前攻击者对企业攻击的态势进行感知。那么ITDR就需要在事中有更强大的能力。

ITDR能够在事中通过规则与学习引擎解决检测问题，对于常见不合理登录与访问行为能够快速分析告警。ITDR不仅仅停留在识别恶意行为的规则上，更通过机器学习与身份行为引擎来分析异常行为；针对身份攻击特征优化机器学习模型，动态分析异常指标、时序异常、模式异常、序列异常等问题，为身份提供实时强大的安全防护。

同时ITDR引入了身份欺骗的能力，通过创建、写入、监控的方式来识别身份凭据的活动进而发现攻击行为。相较于已有的蜜罐方案他的资源消耗少、部署周期短、有效性与可靠性也更高，这也是ITDR系统的一个亮点所在。

通过结合机器学习、图计算等技术进行结合，可以从正常、复杂的身份活动中，精准定位可疑的身份活动，从而发现其中潜在的安全威胁。

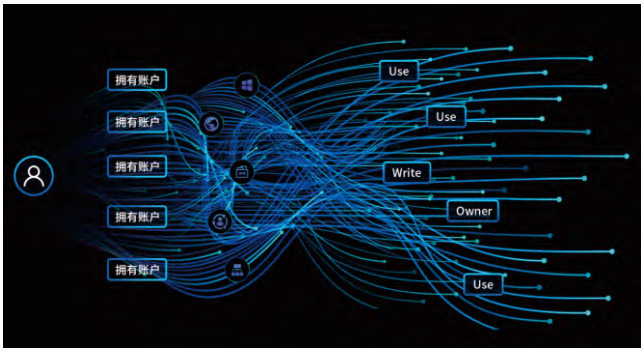


图4 用户权限梳理示意图

身份防护在中国的发展前景

ITDR技术在国外发展还是比较迅速的，ITDR的赛道发展也是以国际厂商为主，涌现了一波独角兽公司，从Gartner的《2022安全运营技术成熟度曲线》报告给出的供应厂商为例：Illusive、Microsoft、Netwrix、Quest、Semperis、SentinelOne（Attivo Networks）、Silverfort、SpecterOps、Tenable，可见领域为清一色的国际厂商。

国内ITDR发展还属于起步阶段，中国ITDR企业要尽快实现在企业中的身份安全落地，必须去结合国内企业安全现状去思考实际解决方案，过去企业侧已有的身份基础设施，包括生产网用堡垒机，办公网用AD，隔离网用云桌面，内部虚拟化用vCenter等，这些土壤足够支撑ITDR方向企业现阶段的发展；随着零信任的落地浪潮，身份厂商的快速发展，企业的身份设施同样会更加多样化，会让ITDR有可预期的大展拳脚的机会。

从市场来看，身份设施是企业侧最基础的管理工具，几乎不存在没有身份管理设施的企业，现在网络安全覆盖的万余家企业一般都是已经部署了AD域、堡垒机、4A中的一种或几种设施作为传统的身份管理。现在更多的应用对接产生了更多的身份场景，衍生出IAM、IDAAS这些新兴的身份设施。
终端、流量、身份形成了贯穿公司内行为的三层，终端检测相应形成了EDR，流量检测响应形成了NDR，而基于身份检测相应的ITDR则会成为未来身份这一层最重要的安全产品。未来无论是零信任方案还是XDR方案都绕不开ITDR的支持。

纵然国内ITDR这一技术领域尚属起步阶段，但可以预见的是，未来随着ITDR技术热度的兴起，注定会有更多安全企业躬身入局，以自身的能力积累切入这一市场，从身份的视角探索检测与响应类技术的更多可能性，共同推动ITDR产品在多个行业的落地。而伴随着市场的逐渐成熟，ITDR技术也必将迎来更广阔的发展空间。

虚假网络信息的识别技术与证券行业网络安全应用的研究

文丨刘广坤

北京天际友盟信息技术有限公司

摘　要： 传播虚假信息可能会实现传播者的经济甚至是政治上的价值，证券行业由于其巨大的金融价值更容易成为攻击者的目标。本文介绍了利用群体情报对虚假网络信息进行识别的技术。利用群体情报检测的技术涉及社交环境、群体知识、群体行为的应用，以推断信息可信度。本文所介绍的利用群体情报对虚假网络信息进行检测的模型假设当用户被认为是可信时，该用户发表的信息被归类为可信信息，对该信息的回复、认可将被认为是可信的。该模型分为两个步骤，第一步：检测用户可信度，第二步,信息的可信度评价。

关键字： 虚假网络信息、群体情报、机器学习、模糊语言决策、可信度

概述

传播虚假信息可能会实现传播者的经济甚至是政治上的价值，因此制造和传播虚假信息、未经验证传播虚假信息在互联网上频频发生，证券行业由于其巨大的金融价值更容易成为攻击者的目标。本文介绍了利用群体情报对虚假网络信息进行识别的技术。

利用群体情报检测的技术涉及社交环境、群体知识、群体行为的应用，以推断信息可信度,本文所介绍的利用群体情报对虚假网络信息进行检测的模型假设当用户被认为是可信时，该用户发表的信息被归类为可信信息，对该信息的回复、认可将被认为是可信的。该模型分为两个步骤，第一步：检测用户可信度，第二步,信息的可信度评价。

背景

互联网的应用使得信息的传播更加地便捷，然而传播虚假信息可能会实现传播者的经济甚至是政治上的价值，因此制造和传播虚假信息、未经验证传播虚假信息在互联网上频频发生。虽然很多国家都采用了实名制，但由于个人信息保护、跨域法律等各种因素的影响，使得互联网上传播虚假信息所获得的收益与相应惩罚不平衡，所以仅仅依靠法律无法阻止互联网混杂着大量的虚假信息传播。这些虚假信息包括伪造的web网站、新闻等，其形式通常以文章、图片以及其他的多媒体等独立或组合形态出现。

例如：COVID-19的出现不仅仅给人们带来了线下的伤害，网络犯罪分子利用COVID-19危机不断尝试欺骗，以实现其经济的或者其他目的。让我们看一则案例：某网站以帮助其进行 COVID-19 研究作为吸引注意力的点，号召人们捐献自己的计算力或转发捐献的链接进行宣传，但事实的真相却是该网站利用人们的善良在志愿者的电脑上植入供窃取信息的恶意软件或者进行其他恶意行为。 很显然，该网站利用了虚假信息进行网络犯罪活动。

证券行业由于交易所产生的巨大价值，因此更加容易成为犯罪分子的目标，例如，根据我国最高人民检察院的公告：

· 唐某博等人操纵证券市场案：2012年5月至2013年1月间，唐某博伙同唐某子、唐某琦使用本人及其控制的数十个他人证券账户，不以成交为目的，采取频繁申报后撤单或者大额申报后撤单的方式，诱导其他证券投资者进行与虚假申报方向相同的交易，违法所得金额共计2581万余元。

· 欣某股份有限公司、温某乙、刘某胜欺诈发行股票、违规披露重要信息案：该公司实际控制人温某乙与财务总监刘某胜虚构2011年至2013年6月间的收回应收款项情况，在首次公开发行股票并在创业板上市申请文件和招股说明书中记载了上述重大虚假内容，骗取了股票发行核准，公开发行股票募集资金2.57亿元。

仿冒网站则是另一种形式的虚假网络信息。以英国国家网络安全中心（NCSC）公开的2021年仿冒网站处置数据为例，英国金融市场行为监管局高居前三位之一，而这并不是全部潜在存活的仿冒网站。

Government brand	Number of attacks (URLs)
National Lottery	511
Financial Conduct Authority	459
Bank of England	392
Ministry of Justice	370
British Broadcasting Corporation	123
Metropolitan Police	44
Department for Exiting the European Union (Brexit)	43
HM Treasury	37
National Crime Agency	25
Prudential Regulation Authority	18

互联网具有巨大的数据产生量、传播速度快等特征，使得人工对从众多信息中识别出虚假信息进成为不可能完成的任务，而通过机器学习和人工智能的方法可以大幅度降低缩小检测时间和节约检测成本，因此建立和使用自动化虚假信息检测能力势在必行。

虚假信息基础概念

虚假网络信息是指带有主观意愿而生成的虚假信息内容或来源无法核实的信息内容，旨在使阅读者做出错误决策。由于制造和传播虚假信息的动机和内容具有一定相关性，我们以制造和传播虚假网络威胁信息的动机分析作为研究对象。

虚假网络信息产生的原因包括：

· 误导：通过虚假信息内容或者提供有偏见的信息内容，引诱阅读者做出错误判断。最常见的误导性虚假的形式有：仿冒钓鱼网站；仿冒社交媒体账号；散布虚假威胁资源（IP、Domain等）使得合法访问被阻断等。证券行业则重点体现在业务数据层面，以虚假财务信息、虚假交易信息为甚。

· 娱乐：以娱乐为目的而生成的信息，例如：愚人节（4月1日）发布的某些信息，但有些读者会误信此类信息。

· 其他：虚假信息可能还来自于未经验证而不负责任的传播、忽略信息本身而植入特定内容吸引阅读者等。

虚假网络信息自动化分析基础

虚假信息的分析方法带有一定的普适性，即研究虚假信息的自动化技术，可以应用于其子集-虚假网络威胁信息。

通常，分析虚假信息，可以从虚假信息的某些特征开始，包括：

· 基于特定主题的检测方法
· 基于读者评论的检测方法
· 基于传播路径的检测方法
· 基于特征选择的检测方法
· 基于新闻验证的检测方法
· 基于社交环境的检测方法
· 基于群体情报的检测方法

本文并未列举全部的检测方法，但依然可以看的出自动化分析方法的理论基础是基于检测算法。然而，需要注意的是信息的某些特征、读者的反应行为并不能用于验证信息的真实性，甚至是有偏见的读者所做出的反应行为可能会造成对信息真实性判断的误导。此外，一些技术流派的恶意信息制造者和传播者还可能利用机器人进行导向，使虚假信息看起来更真实，尤其是chatgpt的应用，使得虚假网络信息的制造者更加容易利用自然语言生成技术进行虚假网络信息的编造。

因此，在实际工作中需要采用多模态模型对虚假网络信息家族进行检测，以提高检出率和检测正确率。

虚假网络信息方法简介

新媒体使得单纯基于文本进行虚假信息检测不再可行，图像、视频更加频繁的出现在新媒体中，以下是在虚假网络信息检测组合中经常使用到的算法：

· 机器学习：朴素贝叶斯和支持向量机（SVM）作为分类算法的代表，常被用来和自然语言处理（NLP）一起处理虚假信息的检测。朴素贝叶斯在文本分类工作上的贡献和SVM的二分类能力，使得组合应用SVM 和朴素贝叶斯进行虚假信息的检测可以获得良好的效果。

· 深度学习：深度学习与机器学习有着千丝万缕的关联，在机器学习的基础上引入了层的概念对数据进行解释，作为深度学习家族的成员：循环神经网络（RNN）模型和长短期记忆（LSTM）同样在虚假信息的识别领域有着不俗的表现。

· BERT：全称为Bidirectional Encoder Representation from Transformers（双向编码器表示），基于预训练、支持多种语言，BERT最重要的一个特点是上下文语境（Context）理解，这个特点使得BERT更适合用于检测信息的真假。

· MFCN：模型使用CNN从样本的表面和边界提取篡改特征，从而可以识别图像中的拼接和局部去除问题。需要注意的是该框架中存在平滑操作，导致其常常会忽略细小目标。

接下来，本文通过群体情报的检测方法一窥算法与检测方法之间的关系。群体情报检测涉及社交环境、群体知识、群体行为等概念，他们对推断信息可信度有着不同贡献。社交环境是指信息来源用户和传播者之间的社会关系和互动等信息；群体知识是指用户参与信息的评级、评论；群体行为是指群体的互动模式等来自一组用户的总体行为。Twitter即支持基于汇总的用户意见进行推测和证明对虚假信息进行“自我检测”。为了便于理解，本文简化了该模型。

该模型假设当用户被认为是可信时，该用户发表的信息

被归类为可信信息，对该信息的回复、认可将被认为是可信的。该模型分为两个步骤，第一步：检测用户可信度，第二步,信息的可信度评价。

前面提到，一些带有特定目的的用户，希望这些虚假信息会被相信是真实的，从而进行关注或重复发布，或者未经身份验证的虚假用户为了实现个人利益而传播错误信息。

为了生成用户的可信度数据，需要对用户所发布的信息分析。当真正的用户（非机器人用户）在共享信息时，不能将用户的所有信息都视为虚假信息。因此，为了验证用户，系统将基于模糊决策分析获取并分析用户对可信信息的反应，从而计算出用户的信任度。

假设用户u发布了n条信息，si是第i条信息的可信度，f(x)代表用户信任函数，采用每条信息的信任度来计算用户信用度。此处信任函数 f(x)可通过模糊语言决策分析进行计算，即通过使用基于字典的方法分析正面和负面词的存在来计算每条信息的si：

$$f(x)=\sum_{i=0}^{i=n}(x:(s_i)\rightarrow[0,1])$$

为了计算si，信息中出现的单词和表情符号将被分类和计算， TP 代表正向项的数量，TN代表负向项的数量，T代表总项数。定义PR=TP/T；NR=TN/T。

正向项的总数 TP由Pw 和 Pe相加而得，其中 Pw 和 Pe 是正向词的数量和正向表情符号的数量。 每个单词的得分为1，表情符号的得分是单词的β倍。(β可通过距离向量进行优化寻找最优解)

$$TP=Pw+Pe$$

负向项的总数 TN由Nw 和 Ne相加而得，其中 Nw 和 Ne是负向词的数量和负向表情符号的数量。每个单词的得分为1，表情符号的得分是单词的β倍。

$$TN=Nw+Ne$$

最后，通过将 PR和 Nr相加来计算后分数：

$$si=PR+NR$$

第二步，通过定义模糊隶属度函数f(z)用于进一步分析，模糊隶属度函数定义如下：

$$f(z)=\begin{cases}\text{非常高},\ 0.99<z\le 1\\ \text{高},\ 0.90<z\le 0.99\\ \text{比较高},\ 0.66<z\le 0.90\\ \text{不确定},\ 0.33\le z\le 0.66\\ \text{比较低},\ 0.10<z<0.33\\ \text{低},\ 0.01<z\le 0.10\\ \text{非常低},\ 0\le z\le 0.01\end{cases}$$

经计算的信息可信度最终使用自然语言进行表示。如果用户的信息得分大部分为非常低 ，则该用户的信任度边界值被定义为非常低。非常低和低的用户信任度将被认为会更多地传播虚假或错误信息；非常高和高的用户信任度则表明该用户对信息真伪识别的可靠性；中等信任度（比较高、不确定、比较低）的用户对信息真伪识别将处于两难境地，即既不倾向于接受也不表示反对信息。

针对该模型的测试，可以利用新闻论坛进行，在目标论坛中进行用户可信度判定，随后对其发布的信息进行评估。即分析创建信息的用户的信任度，如果该用户具有良好的信任度，则利用回复信息和回复信息的用户的信任度来推断该信息的可信度。如果大多数具有高信誉度的用户对信息做出积极反应，则该信息被视为可靠信息。 如果具有良好信任度的用户对该信息持否定态度，则判定该信息不可靠。

通过对BloombergGPT所发表的论文进行研究，不难发现在证券行业对网络信息的检测与通用自然语言的不同，因此需要针对行业信息进行训练数据集的优化，这些优化所采用的数据集包括可以获得的金融领域相关网页、金融相关机构的出版物、可公开获取的公司财报等。

总结

虚假网络信息对经济、政治等有着重大影响，而证券行业的虚假网络信息可能导致金融风暴，因此研究虚假网络威胁信息检测方法的重要性也凸显出来，尤其是在这个全球“抗疫”的时期。虚假网络信息的检测方法和技术是一种多模态人工智能的技术组合运用，本文仅对其中的利用群体情报进行识别的技术进行了介绍。需要注意的是，选择训练数据集对虚假网络信息检测的准确性也有很大影响，需要我们重点关注。

互联网时代检测虚假网络信息虽然很棘手，但事实证明通过大量的知识积累，我们仍然可以在检测虚假信息的工作上取得良好效果。

参考资料

1.“COVID-19: Cyber Threat Analysis”，United Nations Office on Drugs & Crime，2020；

2.Munirathinam Nirmala1, Madda Rajasekhara Babu, “Fuzzy-based fake information detection algorithm to define the user trust on the content of social networks”, IET Netw., 2019；

3.Collins Ayuya, “Introduction to Automated Fake News Detection”, www.section.io, 2020；

4.《证券期货业网络和信息安全管理办法》，中国证券监督管理委员会，2023

5.《最高检、证监会联合发布证券违法犯罪典型案例》，中华人民共和国最高人民检察院，2020

6.BloombergGPT: A Large Language Model for Finance, arXiv:2303.17564 [cs.LG], 2023

7.Towards an AI-Based Counter-Disinformation Framework，THERANDBLOG，2021

以业务为中心的应用层零信任技术创新研究

文丨何艺

北京持安科技有限公司

摘　要： 基于业务的应用层零信任技术，通过基于业务身份的可信验证机制可以确保所传输的数据是可信的，并且能够自动拦截和过滤风险，包括未知风险防护，对于金融行业日益复杂的业务场景来说非常重要，它不仅解决了远程办公下钓鱼渗透的安全问题，还能够应对内网攻击，内部人员舞弊以及日益复杂的0day攻击和数据安全问题，本文将针对应用层零信任的技术原理和应用角度和对证券行业的价值进行深度探讨，通过新一代技术构建主动防御能力。

关键字： 应用层零信任、可信验证、最小权限、动态检测、数据安全

引言

研究背景和意义

随着数字时代的到来，越来越多的证券公司依托互联网和移动设备为客户提供证券交易和投资服务，包括配套的后端各类业务系统，通过数字化转型赋能证券业务。然而，随着业务的开放和敏感性，访问人员的复杂性，其对应的网络安全风险也随之增加，证券公司遭遇黑客攻击或数据泄露事件的情况也愈加频繁。同时，随着移动办公、云计算和物联网技术的快速发展，信息系统架构变得更加复杂，安全管理难度也大大增加。

在该背景之下，零信任作为新一代的网络安全体系，已经被海内外广泛接受和使用，但在金融行业中，对零信任的探索和使用更多还是在网络层面的接入和边界控制上，多用于远程办公场景的使用。但网络层的能力是不足以防护业务的风险，因此站在业务角度，通过应用层零信任技术创新来解决金融行业风险，使得安全可以更好地服务业务，保障业务。

研究方法和框架

本文采用实证研究与案例研究相结合的方法，探讨以业务为中心的应用层零信任技术在证券行业中的应用，并提出了相关的推行策略和最佳实践，包括对零信任技术进行了深入的研究，分析并比较了不同的零信任技术框架和实现方案，以及应用场景和优缺点。接着，结合证券行业的特点和安全挑战，提出了以业务为中心的应用层零信任技术架构设计，并详细介绍了该架构的各个模块和流程，从推行策略和实践角度进行了探讨，最后总结了应用层零信任技术在证券行业中的应用和优势，并提出了未来研究和探索的方向。希望本文的研究成果可以为证券行业企业和从业者提供实用的指导和参考，促进证券行业网络安全水平的进一步提升。

应用层零信任技术概述

什么是零信任技术

零信任技术（Zero Trust）是一种基于最小信任原则和动态身份验证的网络安全框架，旨在加强企业的安全边界、确保网络通信的合法性和安全性、提高用户体验和可控性。传统的网络安全模式基于信任边界来限制对网络资源的访问，但这种模式已经无法适应现代物联网时代快速变化的威胁环境和复杂的业务场景。而零信任技术则采用了一种以身份为中心、基于内外攻击者的实时身份验证和授权机制，来确保任何设备和用户都需要经过认证和授权才能访问系统资源或进行操作。

零信任技术的核心思想是“不信任任何东西”（Trust No One），它通过隔离和分割关键应用、数据和流量，使得网络上的每个请求都必须经过严格的身份验证、访问控制、监管和审计。这样可以有效地减少攻击面、提高防御强度，从而提升企业的网络安全水平。

应用层零信任技术的特点与优势

零信任技术是一种基于“不信任”原则的安全模式，它不仅仅是一种技术，更是一种思想方式。零信任模式下，所有请求都需要通过身份验证和授权才能获得访问权限，即使是内

部用户也不例外。这种技术的特点包括多层次的身份验证、动态的访问控制和细粒度的权限管理。这些特点使得零信任技术具有高度的安全性和可扩展性，能够有效地保护企业的敏感数据和应用程序不受攻击。

而应用层零信任区别于传统网络层零信任方案，其差异在于它能够有效地减少企业面临的业务和应用安全风险和威胁，应用层零信任的技术使得它能够基于业务身份，对每一次资源访问过程中，使用默认阻断的方式，只有通过可信验证确认的访问者身份，才会被转发到业务系统上。因为是基于应用层代理技术，因此可以在访问、认证和授权的层面上实现对所有用户的访问行为深度监控和精准控制，例如针对API级别的控制或是敏感数据维度的控制，从而降低了内部和外部攻击风险，此外，还能够提高企业的可见性和透明度，使得安全团队能够更好地监控和管理企业的安全事件，并且可以防范未知威胁。

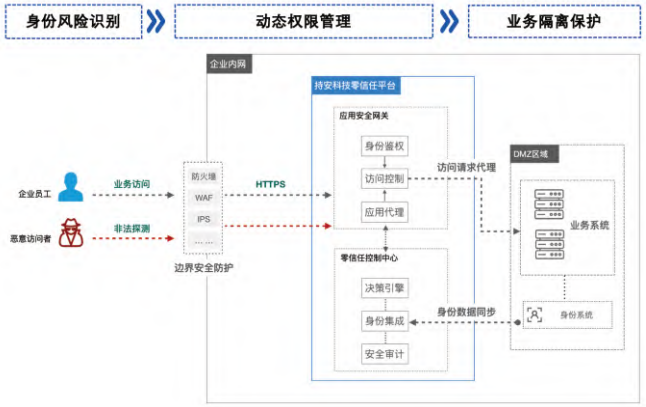


图1 应用层零信任访问模型

1）人员发起访问请求后，到达应用网关后，网关默认将进行请求拦截交由控制中心处理；

2）控制中心判断该请求是否为可信人员访问，如果请求无身份状态则交由身份认证组件或是第三方IAM进行验证；

3）身份验证通过后，通过业务身份由决策引擎继续进行决策判断，验证是否满足其他信任条件；

4）如决策引擎判断都通过后，通知网关进行转发处理，否则直接阻断请求；

5）业务系统返回数据通过网关进行转发，同时进行其他安全策略处理；

6）下次请求发起时，持续上述过程，进行持续验证。

如上图例所示，正常员工访问不受影响，而恶意访问者的所有请求均被自动隔离，能达到业务侧的请求数据均是合法身份数据，即便是后端业务存在高风险漏洞依然无法被攻击。

应用层零信任和SDP技术的差异对比

传统的基于SDP的零信任方案，更多是站在网络层来实现零信任访问和控制能力，其核心能力在于基于终端的身份认证，通过SPA（单包认证）进行敲门，当终端身份认证通过，以建立网络加密隧道的方式构建传输通道，进行后续的授权访问，如下图所示。

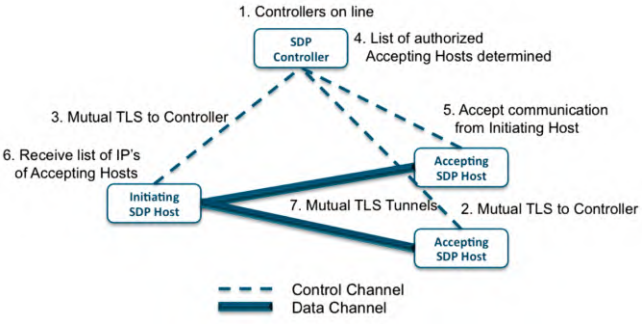


图2 SDP技术架构

在该模型下，由于所有的请求以及控制是基于网络层隧道构建，因此难以针对应用内部的风险进行控制，以及无法感知业务真实身份，无法基于业务的身份来进行控制，因此一旦隧道建立，拥有权限的设备即可发起访问，一旦该设备被控制攻击者就可以以此为跳板对后端业务系统进行攻击，因此SDP只能基于终端安全状态来进行控制隔离，但无法基于业务风险来进行防护。

此外在具体的访问模式、部署场景、管控力度以及审计维度和数据DLP维度上，应用层零信任网关和SDP网关上均存在极大差异，本质上是两套完全不同的技术路线，如下图例所示。后文中也将针对具体技术进行深度分析。

图3 应用层零信任和SDP差异性

在具体的优势上，应用层零信任具备以下特点：

1. 真正的最小化信任原则

应用层零信任模式下，所有请求都被视为不受信任的，并受到动态、分层和基于最小权限的访问控制和验证机制的限制，从而可以大大降低安全风险。

2. 动态身份验证：

应用层零信任技术可以识别业务身份，基于真正业务身份，对请求进行实时身份验证和认证与授权，并根据请求实时验证以及动态授权控制，只有经过认证的对象才能访问相关资源。

3. 细粒度授权：

应用层零信任技术可以对用户和应用程序资源进行细粒度的角色和权限控制，可以深入到业务接口和数据维度的控制，确保访问授权的精细化和可控性。

4. 基于策略的访问：

应用层零信任技术可以根据请求来源身份以及目标资源，通过人员身份、应用和数据的属性和状态，制定相应的策略和规则，灵活控制访问范围和流向。

5. 增强用户体验：

应用层零信任技术可以结合企业IAM的多因素身份验证、单点登录、自适应访问和云化部署等技术手段，可以提供更加安全、高效和便捷的用户体验。

6. 可扩展性与兼容性：

应用层零信任技术可以与多种安全技术和系统集成，同时支持混合云和多云环境，具有良好的可扩展性和兼容性，实现真正的安全一体化。

7. 全网部署落地能力：

应用层零信任可以基于业务所在位置进行部署，而不仅仅是远程办公访问，可以实现全网的零信任落地。

在安全的发展路径上，从网络层到应用层、最终到数据防护是一条必经之路，使用应用层零信任技术可以实现网络层SDP所不具备的诸多优势，具备深度的安全可见性以及防护能力，势必成为企业网络安全的重要趋势和发展方向。

证券行业业务应用现状和风险

证券行业的业务特点

相对于其他金融行业，证券行业的核心业务特点在于证券交易，在行业特点上，有以下几点是明显有别于其他金融行业：

1. 高频交易

高频交易在近年来得到越来越广泛的应用。高频交易通常指通过算法和自动化系统进行快速、大规模、高效的交易操作，利用微小的价格差异赚取利润。高频交易对系统性能和可用性要求较高。

2. 大数据分析领域

证券行业需要对大量的市场数据、资讯新闻以及公司财务报表等信息进行分析，以便做出正确的投资决策。因此，证券行业需要具备大数据分析和数据挖掘等技术的能力，因此会构建极强的中台和后端支撑系统，而在数据上同时也掌握大量敏感数据。

3. 多元化市场交易

证券行业不仅要面对股票市场，还涉及基金、债券、期货等多种证券品种以及不同市场的交易，如美国证券交易所、香港证券交易所等。因此，证券行业需要具备多样化、跨市场的应用能力，所以也会存在跨境数据交互访问的需求。

相对于上述的业务特点，在安全上证券行业也有自身的安全特点：

(1) 严格的安全监管

证券行业的交易规模庞大，涉及巨额资金，因此要求有严格的安全监管，包括交易数据的保密性、交易过程的完整性以及防止欺诈等，包括今年来针对证券行业的APT攻击也呈多发趋势，因此证券行业的安全防护会承担较大压力。

(2) 高度的可靠性和灵活性

证券行业需要具备高可靠性和灵活性，以保证在市场变化较快、风险较高的情况下，系统能够快速响应并做出适当的调整和决策，同时在后端比如投资部门等业务发展中，也需要具备较高的便利和灵活性可以随时访问后端支撑系统来开展业务。

综上所述，证券行业的业务特点包括高频交易、大数据分析、多品种多市场，以及拥有严格的安全监管以及高度的可靠性和灵活性。

证券行业的安全挑战

经过长年的安全投入和建设，证券行业普遍已有较多的安全产品，但在真实的对抗过程中，包括IT基础环境发生变化的过程中，依然存在大量传统安全产品和方案难以解决的问题，如下：

1. 边界隔离失效

黑客和网络攻击者可能会利用社交工程和钓鱼攻击来获得证券企业网络访问权限，或是利用近源攻击等方式，来获得敏感信息和访问权限，从而进行恶意操作。

2. 特征对抗失效

传统基于特征检测的安全设备，只能对已知风险进行发现，但对于未知的0day、新型攻击手法、混淆后的后门、未被使用过的后门IP、域名难以检测和发现。

3. 溯源响应过慢

安全事件是无法被彻底避免的，一旦发生后能否及时溯源响应则非常关键，但传统的分析能力上对攻击来源地分析都是基于某IP，但IP上承载的设备、人员、是否获取了敏感数据，这些则难以有效分析和形成完整的事件链，导致事件发生后的溯源分析往往要持续很久，错过最佳响应时间，甚至出现反复对抗拉扯过程，甚至遭受加密、删除数据等恶意报复情况。

4. 应急处置不足

一旦发现了安全事件，首要做的是消除影响，包括对系统漏洞进行修复，但真实的对抗场景中，往往补丁修复需要等应用系统的厂家提供，修复周期从数天到数月都有可能，这时业务往往不能下线，但系统又存在风险，导致安全不能够及时处置风险。

上述问题尽管证券企业在网络安全方面已经采取了许多措施，但基于传统边界隔离思想和纵深防护体系建设的安全

能力，依然对上述问题难以有效解决，而这也恰恰是如beyondcorp这类先行者通过构建零信任能力，尤其是应用层零信任能力的建设来进行解决。

以业务为中心的应用层零信任技术架构设计

设计原则

以业务为中心的应用层零信任技术架构设计原则包括采用应用层的零信任技术、将业务身份作为基础、基于上下文进行访问控制、采用统一身份和访问管理系统、多层次的安全检测，以及实时监控和响应。这些原则可以确保受保护的资源只能被经过授权的用户或设备访问，以及在访问过程中提高安全可见性，从而提高了企业的业务安全防护能力以及数据安全性，如图例所示。

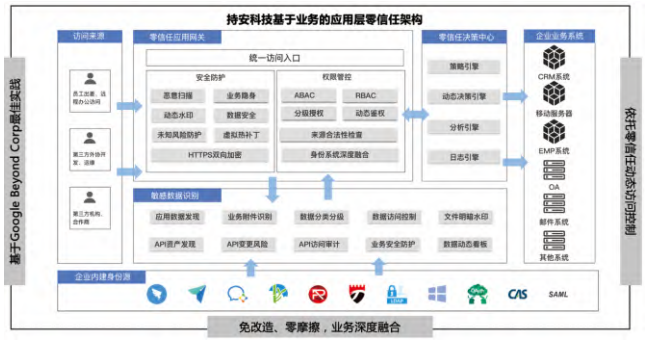


图4 应用层零信任架构

在该架构模型中，只有通过应用层零信任代理能力，以业务的身份为基础，基于上下文请求来构建访问控制能力，同时结合多层次的检测和实时响应能力来及时发现和处置危险，如下：

1. 应用层零信任

采用应用层的零信任代理技术，而非网络层或设备层的防御。通过对每个用户或设备的身份、请求的数据、业务的状态、环境等多维度认证和授权，实现对应用程序的精细化访问控制。

2. 业务身份为中心

将业务身份作为中心，而非网络地址或设备作为中心，以确保只有经过授权的业务身份才能够访问受保护的资源。这种方法类似于Google BeyondCorp，强调在业务系统的访问身份而非终端登录者的身份。

3. 敏感数据识别和控制

基于业务的数据进行主动敏感数据识别以及控制能力，实现数据安全的前置化也同时作为零信任决策条件参与到访问控制和决策过程中。

4. 基于上下文进行访问控制

考虑到用户或设备的身份、设备状况、网络环境等因素都可能影响到资源访问的安全性，因此需要根据不同的上下文因素进行访问控制，同时应用层拥有极高的可见性，因此可以构建完善的上下文信息。

5. 统一身份和访问管理

采用统一身份和访问管理（IAM）系统，以确保对于每个用户或设备，以及业务身份的一致性，确保经过验证的合法者可以实现对所有受保护资源的访问控制和授权操作，而隔离未授权的非法人员访问。

6. 多层次的安全检测

在访问控制的基础上，需要对访问请求进行多层次的安全检测，以确保安全性。例如，通过对请求流量的分析、对数据泄露监控等技术。

7. 实时监控和响应

需要实时处理用户的访问行为，基于业务的真实身份进行风险和威胁发现，以及快速决策和响应，同时可以使用大数据分析和AI技术，增强识别异常活动并自动触发响应机制。

技术架构的主要组件

1. 认证和授权组件

用于对用户或设备进行身份认证和授权操作。该组件可以包括多种认证方式，如密码、双因素认证、生物识别等，并支持对身份和权限进行细分管理。

2. 访问控制组件

用于根据认证和授权信息，对访问请求进行控制和限制。该组件可以基于角色、策略等方式进行访问控制，同时支持多维度的上下文因素，如网络环境、设备状况等。

3. 统一身份和访问管理（IAM）组件

用于管理用户和设备身份，并对其进行统一的访问控制和权限管理。该组件可以提供用户/设备注册、身份验证、授权管理等功能。

4. 安全检测和攻击防御组件

用于对访问请求进行多层次的安全检测，并提供实时的攻击防御机制。该组件可以包括恶意软件检测、数据泄露监控、入侵检测等多种安全检测和防御技术。

5. 监控和响应组件

用于实时监控访问行为，并对发现的威胁进行快速响应。该组件可以采用大数据和AI技术，自动分析异常活动并触发相应的响应机制。

6. 安全日志和审计组件

用于记录所有的安全事件和操作行为，并提供审计和报告功能。该组件可以支持对访问控制过程进行审计，包括认证、授权、访问控制等方面的审计。

综上所述，以业务身份为中心的应用层零信任技术架构的主要组件包括认证和授权组件、访问控制组件、统一身份和访问管理（IAM）组件、安全检测和攻击防御组件、监控和响

应组件，以及安全日志和审计组件。这些组件共同构成了一个完整的零信任架构，并能够保证只有经过授权的业务身份才能够访问受保护资源，从而提高了企业数据的安全性。

实施落地

假设一家证券企业需要保护其业务应用程序和数据资源，以确保只有经过授权的业务身份才能访问，从而保护业务免招攻击以及对内部行为进行审计，同时保护其核心数据安全性。该企业可以采用以业务为中心的应用层零信任技术架构来加强其安全性。

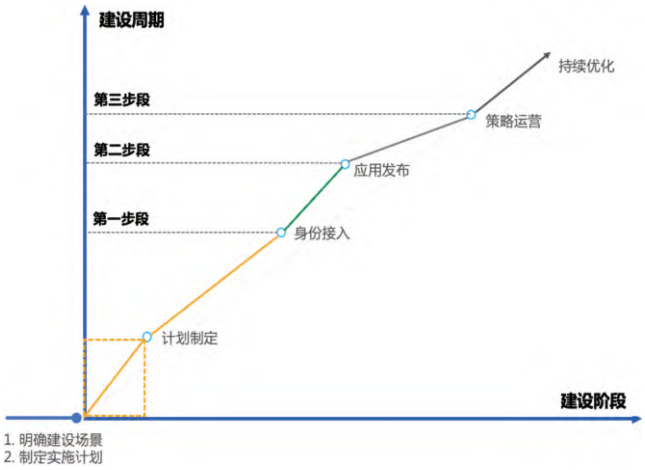


图5 实施计划

1）计划制定：在计划阶段明确确认需要保护的业务以及访问场景，例如员工对于移动办公应用访问、第三方合作伙伴通过互联网直接访问业务系统，内部员工访问的系统，或是安全和运维所使用的集权管理类系统。

2）身份接入：在该过程中通过接入认证和授权组件来验证用户或设备的身份，并根据其权限限制其访问资源，可以使用密码、双因素认证等认证方式，不同权限级别的用户将获得不同的访问权限，如果企业有自建IAM也可以进行集成整合，实现用户无感零摩擦上线。

3）应用发布：将目标业务系统发布到管理控制中心上，以限制对特定资源的访问和保护，并进行灰度验证。

4）策略运用：结合业务特点可以使用角色、策略等方式进行控制，并支持多维度的上下文因素，如网络环境、设备状况、数据使用等策略。

5）持续优化：通过安全日志和数据审计组件记录和分析所有的安全事件和操作行为，检测并防止不同类型的安全威胁，并逐渐收紧访问权限，限制特定的数据获取场景，完善安全预警策略和决策条件。

上述实施方案可以灵活地根据业务阶段，分批或是一次性全量上线，在确保可用性、用户体验的同时，逐步实现全网的应用层零信任落地，最终实现为企业提供全方位的安全保护，不论来自外部访问还是内部访问，均可保障其核心业务应用程序和数据资源的安全性。

应用层零信任技术在证券行业实践中的价值

应用层零信任技术在证券行业中的应用，可以为企业提供强大的安全性、保护数据、降低成本和优化用户体验的优势，如下：

（1）打破传统边界隔离风险

基于应用层的零信任使得即便边界被突破后，例如钓鱼等方式进入企业内网后，依然无法突破应用层零信任的防护，解决了边界隔离带来的内网隐性信任风险。

（2）特征对抗转移到可信对抗

在用户访问业务系统的过程中，应用层零信任不再基于终端身份和攻击特征，而是基于可信验证，只有通过可信验证的请求才会被转发到后端业务系统上，使得攻击者攻击成本和难度大幅增加。

（3）基于身份的溯源分析

应用层零信任可以实现对每一次请求的身份跟踪，精准的知道什么人在访问什么系统做了什么操作和获取了什么数据，一旦出现安全事件后可以快速构建安全上下文，精准分析到人员行为；

（4）实时应急处置能力

当应用系统出现漏洞，或是发现恶意人员的违规行为，可以通过应用层零信任网关实现实时动态处置，不需要第三方系统介入和改变业务系统，实现实时应急处置能力。

（5）老旧系统安全合规能力

应用层零信任技术可以在不用业务系统改造的情况下，实现多类安全合规能力，从而解决老旧系统改造成本与迁移风险等难题。

通过应用零信任技术，安全可以助力业务发展，让证券行业公司可以更加自信地采取新技术、创新产品和服务，并满足合规、适应即时市场变化等挑战。

结论

本研究旨在探讨应用层零信任技术在证券行业网络安全中的应用及实践。通过对该行业存在的安全挑战和威胁进行分析，本文提出了应用层零信任技术在身份认证与授权、风险评估与访问控制、数据保护与加密、恶意活动检测与响应等方面的应用实践，并深入探讨了这些技术的优势和应用效果。

通过研究实践和落地，应用层的零信任能力可以为证券行业企业提供基于零信任模型的安全架构，来帮助其更好地应对传统安全难以解决的隔离风险、未知攻击风险、数据安全风险、合规管控等威胁和风险。

在未来的研究方向和展望上，应用层零信任技术还可以在下述但不限于以下几点上有更多突破，包括面临的复杂业务场景挑战、如何进一步提高其安全性和可靠性、结合人工智能和机器学习能力，以提高安全防御和响应效率，以及不同证券企业之间的安全共享和协同能力。

最后，随着安全对抗的深入，国家对于安全的重视程度，将迫使安全行业深入到业务侧提供更加贴合业务的安全能力，并构建起真正的主动防御和常态化的能力，相信在这个过程中，应用层零信任能力一定能发挥重要的作用和价值，最终提高整个行业的安全水位。

证券期货行业扩展检测与响应（XDR）实践沉淀

文｜吴昌坤、杨闯、朱路光

深信服科技股份有限公司

摘　要： 通过长期调研整理出证券期货行业用户在进行安全体系建设中用户普遍的痛点：资产梳理及脆弱性修复工作开展难、高级威胁检测看不清防不住、安全能力碎片化、高阶人才稀缺，运营难有效持续。本文针对上述问题，通过XDR技术全面梳理组织资产，区别于传统安全运营中心技术引入传统特征检测+启发式检测+IOA攻击信标提高针对高级威胁检测能力，同时基于XDR可拓展特性实现跨网络、端点以及云基础架构打通用户端安全孤岛，提高整体安全能力，从而实现网络安全从被动向主动、从静态到动态、从单点到整体、从粗放到精准防御的转变，全方位全天候的保障网络信息系统安全可靠，全面监测和阻断已知网络攻击和未知入侵渗透风险，防范来自外部和内部多类型攻击，以安全保发展，以发展促安全，推动证券基金行业的网络安全发展迈向新的高度。

关键字： XDR、高级威胁检测、IOA、IOC、自动化处置、SOAR

业界痛点及需求

业界痛点

通过大量行业调研，证券/基金企业在数字化转型中的网络安全建设普遍会面临着以下痛点：

1. 资产管理、脆弱性修复等工作难开展

影子资产难发现，资产定位不清晰，资产管理混乱，缺乏完善的资产全生命周期管理流程；

海量漏洞无法区分优先级，难以识别真正需要处理/容易被黑客利用的漏洞；

突发的热点威胁缺乏快速全面排查影响面的手段。

2. 威胁看不清、防不住、难溯源

检测到入侵行为但生成了弱告警，淹没在海量告警/日志当中；

过往检测平台存在大量误报，业务误判、扫描器与定向攻击难区分；

以白利用、加密流量通信、自定义特征为主的流量层对抗技术让传统检测技术难以识别。

3. 安全能力碎片化，难以在统一策略下完成协同响应

传统的设备联动效果不佳，联动杀毒软件做查杀难以有效遏制；

事件遏制仅是响应工作的其中一环，大多数用户并没有完成加固工作，导致重复失陷；

多源安全设备处置割裂，溯源工作极其复杂，难以协同响应。

4. 高阶人才稀缺，运营难有效持续

传统的统一安全分析平台大量依赖于人，对人员能力与精力要求很高；

人工服务不持续，大量攻击在午夜发生；

高阶安全人员缺口巨大且人才培养成本高昂，多数用户难以培养规模化安全运营团队。

共性需求

随着信息安全形势的发展，国家相关监管部门对信息安全提出了明确的政策要求。这些要求进一步明确了信息安全主体责任，按照“分级管理、逐级负责”和“谁主管谁负责、谁使用谁负责”的原则，完善网络安全监管制度，并建立合规以及监管机制，这也使得监管力度不断增强。

单位网络安全工作存在较大的短板，从应用系统、网络边界防护、内部全流量监测、安全效果运营机制等多方面都存在较多的安全风险。

针对218号令第五十八条监管机构网络和信息安全态势感知工作机制要求，与行业技术支撑单位合作，加强机构的安全通报与预警能力建设。落实监管部门关于网络和信息安全态势感知工作要求，开展机构网络安全风险信息的收集、汇总、分析，与行业网络和信息安全态势感知平台进行系统对接，报送网络安全监测预警信息，及时接收、处置来自国家、行业的网络安全预警通报信息。加强安全通报与预警能力建设，进一步优化安全事件、漏洞信息、威胁情报等内外部安全信息的通报和预警工作机制，制定监测、预警、通报和处置全流程的管理制度，开展技术平台的建设，提升公司内部监测预警、溯源分析的能力，实现上下联动、联防联控、群防

群治的效果。

解决思路及方案

建设思路

扩展检测与响应XDR体系建设建议以证券基金行业的网络、重要服务器、核心业务系统等IT资产为保护对象，依据网络安全法、网络安全等级保护要求和相关标准规范，围绕实战化的威胁对抗能力，以效果为核心、以闭环为目的，聚焦检测能力提升，实现精准高效的效果。建立与网络信息化与组织架构相配套的扩展检测与响应中心，实现网络安全从被动向主动、从静态到动态、从单点到整体、从粗放到精准防御的转变，全方位全天候的保障网络信息系统安全可靠，全面监测和阻断已知网络攻击和未知入侵渗透风险，防范来自外部和内部多类型攻击，以安全保发展，以发展促安全，推动证券基金行业的网络安全发展迈向新的高度。

XDR的认知是有共同点的。2021年8月，曾经Gartner的研究VP，当前Google Cloud安全战略负责人Anton Chuvakin 发起了一个调研，最终总结了几点业界对XDR的共识。综合这些信息，可以认为XDR具备以下两个基本特征：

1. XDR的最佳效果是基于云原生的

XDR的检测能力需要较全面地覆盖已知黑客攻击技战术，同时需要针对新出现的攻击技战术快速开发对应的检测模型&算法，以及相关的调查、响应、狩猎功能。因此当前较完善的XDR产品均是基于云原生SaaS化提供的，可以基于集中的专家、算力和遥测数据和情报资源，更快、更好地快速迭代产品，可以认为云原生是XDR 快速发展的必要条件。即使一个本地化部署的XDR平台，也需要基于云端的持续运营来提供快速的更新。通过云原生提升安全对抗效率，一个典型的案例就是在2021年Log4j2 漏洞爆发时，CrowdStrike基于其云原生架构，在漏洞披露24小时内就提供了检测、处置和修复的完整能力，并且在数天内提供了专项的漏洞数据统计监控，这种速度对于单纯依赖本地化平台的产品是难以想象的。

2. XDR覆盖检测和响应

XDR顾名思义包括检测和响应能力，需要集成全面、完善的检测技术在行业内没有争议，但在响应技术上还有不同的认识。全面、完善的检测技术，即需要包括：

· 传统的特征检测（恶意代码特征、漏洞特征、IOC失陷指标）；

· 启发式检测（对抗混淆、加壳恶意代码的一种检测方式，关注代码运行过程中的恶意行为检测）；

· 基于行为的检测（IOA攻击信标）；

· 各种威胁狩猎能力，包括被动、主动和自动化不同的方式。

扩展检测与响应的建设要以让威胁对抗更高效、运营工作更省心为方向，通过数据融合编织、情景检测、威胁定性、故事线还原、资产定位到人、SOAR、工单流程等各项手段，强化检测与调查能力、达成资产可视可控、加强高效处置并推进安全运营的持续有效落地。

图1 安全效果运营

扩展检测与响应架构模型

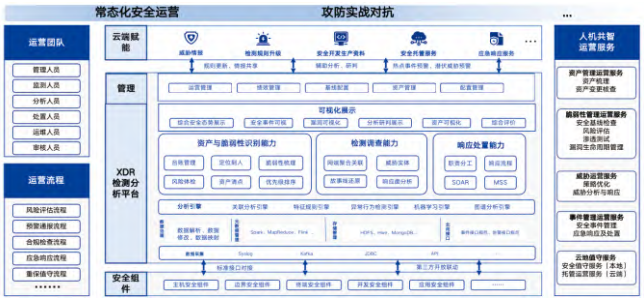


图2 扩展检测与响应中心框架

面向未来的安全运营，立足“人员、流程、工具、服务”，构建”3+1+N“体系，基于3项核心能力、1类配套服务打造基于XDR方案，可有效涵盖N类场景，充分整合 XDR、自动化工单剧本、云端专家情报等元素，让实战对抗更高效，让运营工作更省心。

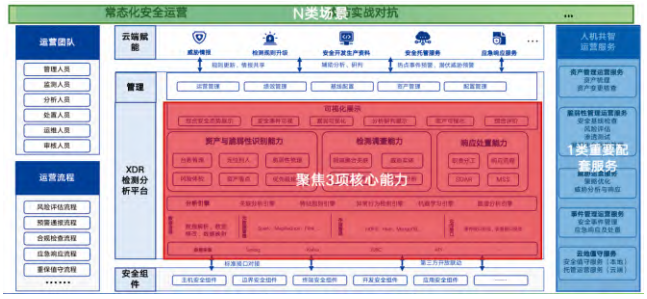


图3 扩展检测与响应中心框架

项目背景

图4 扩展检测与响应核心能力说明

1. 资产管理与攻击面管理

资产管理

基于XDR的资产管理可以解决资产分散、不集中等一系列管理问题。具有识别IT资产、梳理访问关系和建立责任人员组织架构的功能，实现资产的统一管理。其中，可识别的资产类型，包含服务器、终端、网络设备、物联网设备、移动设备和网络安全产品等。

通过主动扫描识别、被动流量识别和用户手动三种方式导入资产列表，结合用户页面操作资产信息，对资产进行关联、合并、去重和除错等处理，补充更新资产数据信息。

图5 资产管理模型

攻击面管理

从攻击者视角看来，能够被攻击者利用以发起攻击，进而对业务造成安全风险的所有攻击点，都是攻击面管理的内容。

传统自下而上的设计受限于采集能力，只能根据采集到的内容被动分析和响应；采用自上而下的设计思路，深度洞察攻击面，并根据洞察结果主动提升检测和分析能力，使攻击面管理更主动、更全面、更准确。以攻击视角进行深度资产威胁建模，通过动态运营，收缩暴露面威胁建模，找出攻击关键路径，组件延伸出可能的攻击和利用点，对应出解决方法，进行精准有效加固。

结合漏洞全生命周期机制，对漏洞全生命周期进行管理，包括：漏洞发现、漏洞验证、漏洞处置、漏洞复测，实现漏洞全生命周期状态闭环跟踪，确保重要的漏洞及时处置。具体过程定义如下：

漏洞发现：能够主动地对系统、应用层、中间件、数据库等漏洞检测。

漏洞验证：能够对紧急漏洞进行排查，主动检测、网络安全设备、主机网络安全管理软件、网络安全漏洞发现算;法等来源的漏洞信息进行自动化的或手工的验证，确定漏洞的有效性。

漏洞处置：对发现的漏洞提供处置建议，提供可落地的漏洞修复方案，包括：漏洞修复步骤、补丁下载链接等，漏洞处置方案支持自定义。

漏洞复测：当漏洞修复后，对漏洞进行复测，确定漏洞是否已被成功修复。

2. 检测调查能力

XDR平台具备聚合分析流量和端点一手数据的能力，同时可通过微剧本半自动化响应事件，实现少量精准的检测效果、自动高效的处置效果，也是构建实战化威胁检测相应体系的核心。通过网侧流量+端侧行为数据以及第三方日志汇聚分析，平台提供的攻击链溯源图能准确还原攻击故事线，对恶意入侵、异常外联、侦查、横向移动、数据外泄等每个阶段发起的所有安全事件和造成的影响进行全面的剖析，形成具有承上启下的安全事件关联集，并围绕被攻击者的攻击链视角进行呈现和告警。

关联分析能力

将终端侧和网络侧收集的数据，与云端威胁情报、资产、时间等因子做复杂关联，最终生成平台侧的关联事件。

对与组件强加强的告警信息，平台提供可视化和高可见性，结合精准详尽的处置响应建议，帮助安全运营人员提高效率，显著降低了MTTD（Mean Time To Detect，平均检测时间）/MTTR（Mean Time To Response，平均响应时间）。

对于组件弱加强的告警信息，平台通过多因子关联提升检测精度，有效降低告警误报量，针对原本单一网络侧或终端侧无法精准检测的攻击，如Webshell上传成功、RDP爆破成功等，基于E+N关联分析实现网络和终端数据相互印证，互为补充，大幅提升了检测精度。

对于组件弱加弱的告警信息，平台对于二者进行整合，提升了威胁检测的覆盖广度，无论是低危的自动化脚本攻击，还是高危的高级持续威胁，在XDR平台下都将无处遁形。

威胁定性

通过上下文、资产和脆弱性数据、威胁情报等数据进行大数据关联分析，对安全设备上报的海量告警数据进行威胁定性，确定威胁等级（区分事件和威胁）和主机失陷等级。并能够挖掘出攻击成功事件，包括暴力破解成功识别、Web攻击成功识别、漏洞攻击成功识别等。以上安全事件，和威胁检测算法的C&C（DGA、隐蔽隧道通信），以及木马后门、勒索、挖矿、webshell等构建全面的安全事件/攻击成功识别。

3. 相应处置能力

设备联动能力

通过XDR构建分层响应体系，可协同联动相关组件，具备自动化响应与处置能力，提升威胁应对的效率。通过XDR提供的事件响应处置能力，制定全面的事件响应（IR）计划，帮助安全团队对网络安全事件做出完整，快速和有效的响应，通过准备、检测、抑制、根除、恢复、跟踪等多个阶段的响应处置工作，降低因安全事件带来的损失。

工单流程化

通过工单的功能，实现所有事件的处置能全流程追溯进度，实现过程与结果的可视化。在证券/基金企业内部不同部门可实现不同角色间的协同和流程化运维。依靠安全运维主管进行任务发起及归档，推动具体责任部门或下属单位的运维人员完成相关事件处置工作。对安全问题进行流程化实现，可便于风险处置的协作和管理，避免无责任人管理导致的风险淹没。

SOAR剧本

依托XDR平台内置的SOAR模块，可进行图形化的安全编排，根据不同的安全事件可自行灵活地编排不同的处置流程，将安全运营相关的技术、流程和人员等各种能力整合在一起工作。可通过剧本的方式编排响应处置流程，可通过SOAR统一构建自动化分析、响应、处置剧本，一旦发现安全问题就立即启动预定义的剧本，快速将安全事件进行闭环，实现了根据不同类型的风险自动化执行不同的处置流程。

4. 多样化对接能力

多源数据对接

XDR平台需要实现统一管理与统一调度能力，需要实现与第三方日志、第三方应用的对接，需要收集网络流量数据、主机终端数据、安全设备告警数据、情报数据等。

云平台对接

需要通过标准API接口方式，或者SIEM日志同步的方式，实现VMware云平台、阿里云平台、腾讯云平台等平台的对接，保障多云内不同的日志能统一汇聚、统一分析。

5. 安全效果运营配套服务

威胁管理

依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单。

事件管理

根据当前网络安全现状和证券基金的业务情况，结合外部安全专家的输入，建立常见高发性安全事件类型的应急响应处置预案，提升单位网络安全事件的响应处置效率，有效的指导网络安全事件的应急响应处置，有效止损。

落地难点及对策

落地难点

1. 难点1-网络层安全风险

1)网络分级分域缺失，需要对互联网提供服务的业务系统服务器直接从内网经过网闸方通提供互联网接入，一旦有一台服务器失陷就导致内部全网被攻陷；

2)边界应用层监测及防护机制缺失，网络边界现有的传统防火墙无法记录服务器的访问行为和应用层攻击行为，导致攻击行为无法快速发现，攻击成功后难以发现，响应溯源无迹可查；

3)内部网络全流量监测分析手段缺失，现有安全设备无法记录全流量的主机行为，仅记录明确的攻击行为，对高级威胁攻击的识别和行为记录留存不起作用；

2. 难点2-终端主机层安全风险

1)主机上现有部署的杀毒软件仅能实现基于文件特征的检测，无法做到主机文件异常和行为异常的识别，对webshell、命令执行、挖矿、勒索等病毒行为无法做到有效的检测和防御；

2)主机未及时更新系统补丁，如勒索病毒传播利用的漏洞相关的MS17-010等安全补丁有大量的主机都未修复；

3)主机存在大量的安全漏洞未修复补丁，对主机漏洞存在的安全隐患缺乏有效的管理手段做到处置闭环；

4)内部主机存在大量的僵尸网络、勒索、挖矿等失陷事件，缺乏主动发现和处置手段，导致网络内部潜在威胁不断增多。

3. 难点3-安全效果运营保障机制缺失

1）缺乏信息化资产管理机制，对IT资产没有清晰的梳理和持续的变更管理跟踪，导致资产信息脱节严重，安全工作保护的目标都不清楚，僵尸资产、暴露面较多；

2）信息化资产脆弱性缺乏有效管理，无法做到业务系统脆弱性问题的闭环管理；不管是技术保障还是管理机制都难以匹配脆弱性闭环管理的要求；

3）安全威胁管理基础几乎为零，威胁监测、分析研判、响应处置等方面技术手段和管理机制保障都很缺乏，仅有基础的网络层访问控制措施；

4）缺乏高阶安全人才，基本的安全事件应急预案和事件快速响应能力不足，在安全事件发生时无法做到主动发现和快速止损。

建设对策

1. 对策1-人员能力补齐

人是安全运营工作的主体与关键。证券基金行业在实际网络安全运维工作中，普遍存在着专业网络安全运维人员数量不足、权责划分不具体不清晰、安全运营技能和经验缺乏、

安全应急响应周期长效率低等问题，因而对于安全运营团队能实现梯队分工、提能增效，普遍具体有以下需求：

· 按单位现有人力情况，结合实际运维工作需要，参照相关政策要求，优化安全运营团队组织架构设计，引进外部专业的安全服务，基于“平台+组件+服务”的思路来达到运营人员分工明确、权责对应、层次搭配合理、团队运营能力逐步提升的目标；

· 提升安全运营工作效率、增强安全事件应对能力、缩短安全事件响应时间，一方面将大量重复性的人力工作固化成工具能力自助化输出（如：日报、周报以及病毒、攻击等各类统计报告；工具自动化实现安全日志关联分析与攻击链溯源等），另一方面，通过外部专业人员的帮扶，逐渐增强安全运营团队整体的技能水平，及时高效响应安全事件，避免被主管单位通报处罚；

· 通过外部运营团队的能力与经验的补充，促进单位的整体安全运营工作逐步规范化、全面化、专业化，如让过去注重事后扑火式的安全运营工作，转向关注事前评估预防、事中持续监测、事后加固优化的全局安全运营。

2. 对策2-技术与工具高度整合

技术工具是安全运营工作的主要载体和基础。现有各类安全设备和组件各自为战、日志分散、能力不集中，且对内网横向流量与虚拟化平台内部东西向流量缺乏有效检测，无法全面看清全网流量风险。

· 实现全网安全流量与日志的统一汇聚、检测与分析，提供集中安全告警，收敛安全运维入口，提高安全分析与运维效率；

· 增强对安全日志的关联分析能力和深度挖掘能力，通过AI、UEBA等新技术的运用，发现新型威胁、潜伏威胁与未知威胁；

· 实现安全风险实时可感知，风险多维度可视化监控，可以定期查看整体网络安全态势报告、资产与脆弱性风险报告、运维报告等；

形成自动化联动处置能力，针对高危事件与已失陷主机，能提前预设剧本，联动防火墙、EDR等安全系统自动化执行策略，缩短MTTR时间。

传统开发过程中关注需求开发，缺少安全设计及开发安全经验沉淀

过去在开发设计中，往往缺少安全视角的考虑，更缺少设计、开发过程的安全考量、最佳实践、安全经验沉淀；如何提升证券、期货行业的开发水平、实现软件上线即安全，并将相关经验在行业内进行发声，成为亟需解决的问题。

传统外挂式的应用安全防护产品难以准确定位应用安全隐患

过去应用安全主要依赖应用开发完后，进行验收式风险评估和外挂式加固，主要通过部署WAF等安全设备进行安全防护。这种外挂式的方式无法识别应用内的详细属性信息，主要通过产品通用的安全检测规则进行检测和防护，存在缺少针对性、效率低下的问题。尤其是在应用数据安全建设方面，大量外挂式应用安全防护产品，依托传统网络安全的技术，通过流量和终端采集的方式对数据安全风险进行检测和分析，存在数据资产识别不准确、数据管控精细度不足等各类问题，很难真正保护好应用的数据安全。

传统应用开发安全工具严重依赖人工，实际效果难以发挥

在开发过程中的应用安全建设主要通过产品研发过程中增加安全开发工具和流程对研发过程进行安全管控。但在实际过程中，研发人员依赖众多割裂的应用风险扫描工具，例如SAST源代码安全分析、SCA软件成分分析、DAST动态应用测试，由于这些工具技术实现原理先天决定了无法完整、准确分析出应用全部的安全风险，导致使用这些工具的研发团队问题发现不全面、发现无效问题多、使用不方便拖慢研发创新进展等问题，使得开发安全工作在企业中无法有效落地。同时，在解决应用自身安全问题的过程中，主要依赖研发人员在安全方面的能力积累，普遍存在无法保障问题解决效果、重复造轮子反复解决同类安全问题等现象。大量金融客户高水平安全研发人才稀缺、成本较高，导致无法有效落地在开发阶段的安全控制。

开发与运行环节缺乏有效协同和联动，对已发现的安全问题补救低效，整体应用安全防护效果不佳

开发阶段相比应用运行阶段，先天可以获得大量的应用内生资产和属性信息（如应用中间件架构、API调用流、开源组件构成等），这些应用内生属性信息对于应用安全防护来说可以起到提供重要的“先验知识”输入，帮助运行时的安全防护更精准更高效。而传统开发安全和运行时安全之间缺乏有效的协同和联动，导致开发安全缺乏高效的技术闭环，而运行时安全缺少对应用内部属性信息的感知，进而造成整体各个环节安全建设的效率和效果不佳。

技术前沿

11 云原生

从构建到运行：云原生应用全生命周期防护

文丨张政

北京小佑科技有限公司

摘　要： 在当前趋势中，证券行业的应用系统从最初的虚拟化、私有化、公有化等模式发展到多云、混合云、边缘计算、云原生等多种模式，这些新模式的发展带给证券行业发展便利的同时也带来了新的难题。Gartner在2017年和2019年两次将容器安全列入十大安全项目，安全风险主要几个方面：容器管道和容器应用的保护、容器部署环境与基础设施的保护、企业安全工具的整合与现存安全策略的解决或加强。

关键字： 信息安全、容器安全、云原生安全、全生命周期

概述

近年来云原生模式逐渐被业界认可和接受，在国内包括政府、证券、金融、运营商、能源等众多行业，均将其业务进行不同程度的云原生化。随着云原生的广泛应用，带来了IT架构和软件发布流程的重大变化，同时其安全问题也不容小视，进入云原生阶段后，云原生的技术特性使安全防护模式发生了转变，发展为以应用的生命周期作为安全防护视角，从基于边界的防护模式转变为更接近基于资源属性和元数据的动态工作负载的防护模式，从而有效识别并保护工作负载，以满足云原生技术架构的独特属性和应用程序的安全需求。

云原生演进面临的安全风险

云原生的理念经过不断丰富、落地、实践，云原生已经渡过了概念普及阶段，进入了快速发展期。云原生技术以其高效稳定、快速响应的特点驱动引领企业的业务发展，成为企业数字业务应用创新的原动力。过去几年中，以容器、微服务、DevOps、Serverless为代表的云原生技术正在被广泛采纳，2020年43.9%的国内用户已在生产环境中采纳容器技术，超过七成的国内用户已经或计划使用微服务架构进行业务开发部署等，这使得用户对云原生技术的认知和使用进入新的阶段，技术生态也在快速的更迭。

而容器技术之于云计算的发展，已经成为目前主流的虚拟化技术，成为敏捷开发人员的首选，以Docker、containerd技术为代表的容器技术，重点解决了容器技术使用和维护上的复杂度问题，通过对容器管理引擎以及容器镜像的标准化，降低了容器技术使用的复杂度，同时围绕容器技术构建应用生态圈，丰富容器技术在行业内的应用和推广，以容器、Kubernetes和微服务应用模式作为数智化转型的驱动力。

云原生技术架构充分利用了云计算弹性、敏捷、资源池和服务化特性，在改变应用的设计、开发、部署和运行模式的同时，也带来了新的安全要求和挑战。以容器为载体的云原生应用实例极大地缩短了应用生命周期；微服务化拆分带来应用间交互式端口的指数级增长；多服务实例共享操作系统带来了单个漏洞的集群化扩散；研发运营流程增加了软件全生命周期各个环节的潜在风险。云原生的特有属性带来了架构防护、访问控制、研发运营等领域带来了以下的安全隐患：

制品的安全威胁：Docker Hub镜像仓库作为全球开源的镜像制品平台，任何人都可以注册账号进行镜像的上传，据统计Docker Hub开源仓库中，超过半数镜像存在中高危未修复的软件漏洞，并且包含类似带门罗币挖矿病毒的镜像、包含Graboid镜像，门罗币挖矿镜像被下载超过500万次，其中Graboid挖矿病毒，至少感染了超过2000台以上的节点，并且存在镜像的“冒名顶替”的现象，例如公共Docker Hub中发现的“TesnorFlow”镜像，明显要用拼写错误的手法冒名顶替“TensorFlow”。而容器是基于容器镜像文件启动，镜像的安全将影响到整个容器的安全，容器镜像安全隐患主要有：镜像软件可能存在漏洞、镜像文件完整性被破坏、镜像文件遭受恶意配置或者更改（比如上传或者下载过程被修改，植入后门）导致容器被利用；镜像仓库不安全，无论是官方的Docker仓库还是私有的仓库，如果仓库被攻陷，则仓库上镜像可能被篡改。

容器自身的安全威胁：容器是硬件资源共享，同时需要提供资源隔离，保证容器计算、存储、网络资源在不同租户之间的隔离，保证不同容器的之间资源独立，不相互影响，保证不

同用户的容器运行在同一主机上，攻击者不可利用容器攻击主机或者主机上的其他容器。同时，除了下层的镜像不可变基础设施层，在业务真实的运行过程中，最上层的容器可写层，可能面临基于镜像含有的漏洞、内核漏洞、业务代码漏洞等被利用后，导致容器逃逸，造成破坏面的扩大，以及上传后门，基于业务深入研究后，导致的数据泄露、财产被盗。容器删除后，剩余信息安全，计算及网络资源释放安全等风险，而且由于容器的特性、业务深入渗透测试的多部门协调等问题，导致容器自身的风险无法很好的在静态时体现。

集群网络安全威胁：集群网络主要是提供对容器的监控、容器的操作、容器对外的接口等网络平面，如果这些网络平面受到攻击，容器正常运行状态将不能保证，甚至承载容器业务数据会被泄露，并且云原生环境的网络形式多数为虚拟网络，当前的硬件网络安全设备是基于IP作为防护对象，无法保障云原生环境下的东西向和南北向的网络访问流量。

编排组件安全威胁：编排组件是调度和管理pod的编排工具，管理整个pod的生命周期，主要有如下威胁：权限滥用-编排程序未使用权限最小的访问模型，可导致用户对其工作角色所需之外的特定主机、容器和图像执行操作，滥用访问权限。未经授权的访问-如果编排程序在公用网络中开放了API和端口，攻击者可以未经授权接入，通过盗用或滥用管理权限，使用编排程序访问和修改环境中的所有资源。编排节点受损-受损节点如不能够被隔离并从集群中移除，将会干扰或降低整个编排集群操作。容器编排策略错误-编排策略没有被正确设定，如未正确分割应用的网络流量，将导致攻击可以通过对公网开放的应用蔓延到内部应用，无法被有效限制。

业务自身安全风险：即使采取了相关预防措施，如果由于运行的应用存在缺陷，容器仍可能受到入侵。这不是容器本身的问题，而只是容器环境中典型软件缺陷的表现。例如，容器化的 Web 应用可能容易受到跨站脚本漏洞的攻击，数据库前端容器可能会受到 SQL 注入的影响。当容器遭到入侵时，容器可能会通过多种方式被滥用，例如允许非授权访问敏感信息，或实现对其它容器或主机操作系统的攻击。

云原生应用全生命周期防护要点

随着云原生安全近年来的不断发展，云原生安全需要关注容器的整个生命周期，针对生命周期中的各个阶段所存在的安全风险形成对应的应对手段，并且在安全运营、运营流程中形成最佳实践，形成完善的可控可靠的云原生安全防护运营体系。

图1 安全防护思路

云原生应用全生命周期的安全能力建设如图2所示，主要包括五个部分：分别为构建阶段的镜像安全能力，运行时阶段容器安全防护能力，对外暴漏访问后的应用安全能力，集群东西向网络隔离能力，以及针对基础平台安全防护的集群安全能力。

图2 云原生全生命周期安全防护

供应链安全部分，除了制品安全本身，在制品供应链中镜像仓库安全风险主要涉及仓库账号及其权限的安全管理、镜像存储备份、传输加密、仓库访问记录与审计等，这些方面如果存在加固或配置策略不足的问题，都可能导致镜像仓库面临镜像泄露、篡改、破坏等风险。容器镜像从镜像仓库到用户端的完整性是镜像仓库面临的一个重要安全问题。如果用户以明文形式拉取镜像，在与镜像仓库交互的过程中极易遭遇中间人攻击，导致拉取的镜像在传输过程中被篡改或被冒名发布恶意镜像，从而造成镜像仓库和用户双方的安全风险

针对供应链所存在的安全风险，一是针对所涉及的镜像仓库提供对应的安全管控能力，对仓库本身的配置进行安全性检测，及时发现和避免由错误的配置造成的安全隐患，二是针对镜像流转中的完整性提供校验，通过对镜像的存储加密、签名等手段，确保镜像流转过程中的安全性，避免镜像在传输过程中被篡改。

镜像安全部分，镜像作为容器运行的基础，如果存在的安全隐患、风险问题直接影响到容器环境的安全性，常见安全风险之一就是用于创建容器的镜像存在安全漏洞，从而导致所部署的容器存在漏洞，同时镜像配置缺陷也会导致应用风险增加，例如镜像未使用特定用户账号进行配置导致运行时拥有的权限过高；镜像含 SSH 守护进程导致容器面临不必要

的网络风险等。

面对镜像中可能存在的安全问题，对镜像可能存在的软件漏洞、webshell、软件、病毒木马、密码/密钥敏感信息、不允许的软件许可等安全风险进行识别，同时建立镜像来源的可信检测能力，从基础镜像、镜像、仓库多个维度确保镜像供应链安全，针对风险的镜像形成阻断能力，禁止含有风险的镜像流入生产环境，造成安全威胁，解决当前国内外开源仓库内镜像，大多含有漏洞或恶意文件以及镜像构建过程中引入的安全问题。

容器安全部分，无论是 Docker、Containerd容器、还是Kata类安全容器，都暴露过各类逃逸漏洞，逃逸风险对于容器化的云原生场景是一个不可避免的风险面，特别是在多业务系统、多租户环境下，风险更高，直接危害了底层宿主机和整个云计算系统的安全。而容器逃逸则主要为：危险配置导致的容器逃逸、危险挂载导致的容器逃逸、相关程序漏洞导致的容器逃逸、内核漏洞导致的容器逃逸等

针对容器运行时存在的安全风险，以多种方式保证容器运行时的安全，第一是针对已知的威胁，根据恶意行为特征、流量，建立检测规则，对此运行容器进行实时的安全监测，第二是通过行为学习的方式，云原生技术下容器作为不可变基础设施，每个容器内的行为都是固定可预期的，天然具备行为学习的技术优势，自动建立业务行为模型，将行为模型关联至容器及镜像，当模型建立后，当容器行为偏离业务行为模型时，可进行预警。在发现风险后同步建设了威胁处置能力，对风险进行自动或手动的处置，包括暂停、重启、隔离或报名单等方式。

应用安全部分，随着云原生环境中微服务的增多，暴露的端口数量也急剧增加，进而扩大了攻击面，且微服务间的网络流量多为东西向流量，网络安全防护维度发生了改变，随着业务规模的增大，微服务API数量激增，恶意的API操作可能会引发数据泄漏、越权访问、中间人攻击、注入攻击、拒绝服务等风险

应建立对云原生环境中的微服务的自动发现以及类型识别能力，对现有资产进行发现识别，梳理服务并与容器对应关系；针对微服务所存在的安全漏洞进行检测和识别，解决OWASP等维度的安全风险，实现对微服务的访问流量进行审计，形成溯源和审计分析手段。针对异常的访问请求和异常流量提供流量阻断能力，能够应对1 day场景下的快速响应需求。

网络安全部分，云原生环境下，服务实现了细粒度拆分，业务依赖关系复杂。如果容器网络层不能依据业务关系实现细粒度的访问控制策略，就会带来网络权限放大的风险，例如：无需被外网访问的业务被默认设置了外网访问权限，容器网络可无限制访问宿主节点的下层网络等。攻击者将利用这些漏洞，获取权限外甚至核心系统的访问控制权限，最终实现越权甚至提权攻击。

默认情况下，Kubernetes允许所有资产之间进行开放式通信，这种“默认允许”的方式简化了开发，但增加了安全风险，内网流量无法得到有效管控，需要把传统防火墙的隔离规则转移到容器云环境中的Pod、工作负载、租户空间等层面应用，避免容器云环境的东西向流量失控，使容器云内的流量和访问能够得到有效管控，并且自动绘制链路跟踪图谱，有效的帮助安全人员/运维人员快速分析容器云集群内的网络情况。

集群安全能力部分，云原生编排系统中组件众多、各组件配置复杂，配置复杂度的提升增加了不安全配置的概率，而不安全配置引起的风险不容小觑，可能会导致编排工具中帐户管理薄弱，或部分帐户在编排工具中享有很高特权，入侵这些账户可能会导致整个系统遭到入侵。

基础运行环境的安全代表着其上运行业务的安全，当前基础运行环境的风险主要来源于两大类，一类为基础运行环境漏洞，一类为合规配置，都可能引发基础运行环境的崩溃，针对此情况，建设了基础运行环境组件漏洞、配置、事件相关风险检测能力。最终基于四大部分的能力研究及建设，形成覆盖容器全生命周期的安全能力，形成可检测、可处置、可溯源的安全闭环，并覆盖开发交付各个阶段。

云原生应用全生命周期防护应用措施

以云原生安全防护平台作为安全抓手，建立云原生应用全生命周期运营闭环体系，并且将云原生安全能力同步建设至DevOps流程，同步风险数据，整体架构实现了各个阶段的闭环管理，实现可检测、可处置、可溯源，基于建设的诸如镜像、容器、集群、应用等安全能力，覆盖到了容器从镜像构建之始，直至容器消逝后的数据保留全生命周期。

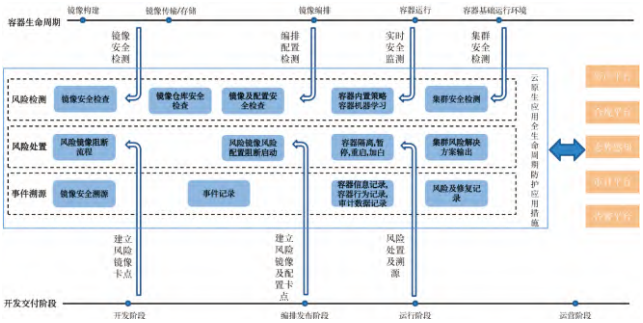


图3 云原生应用全生命周期防护应用措施

并且当云原生集群发生扩缩容的时候，平台通过自动调度的算法进行分析出新加入的节点，实现新节点的自动化部署，并且对新节点进行防护，从而实现安全平台和容器云平台的联动，进一步实现云原生安全的内生化建设。

以MITRE ATT&CK为指导：未知攻，焉知防。在入侵检测时，云原生安全防护平台以ATT&CK为指导框架，对入侵事件

进行所属分类，明确各类入侵事件以及攻击链上所处位置，并构建恶意行为的完整攻击链，使安全运维人员更方便地进行事件回溯和后续预防。

图4 MITRE ATT&CK Containers Matrix

自适应行为基线：基于“不可变基础设施”的理念，每个容器只运行特定软件，其行为模式是可以预期的，这为容器行为白名单模式提供了理论依据。通过对不同容器内行为进行学习，持续建立自适应安全基线模型。当监测到行为模型外的进程、文件访问、异常网络连接和系统调用时，会通过关联分析风险事件列表，进行告警处置。通过白名单模式，可以有效提升异常事件检出率，可以用于防御0day风险。

图5 自适应行为基线

镜像可持续性自动修复：基于安全左移的思想，在镜像检测和加固的阶段实现左移动作，进而实现DevSecOps的方案构建；镜像安全检测通过在持续构建流程中进行介入和卡点，实现多卡点检测控制，尽早将风险暴露出来，避免业务镜像“带病上阵”；安全卡点动作提供多种维度、多个阶段的支持，其中包括IAC检测、容器镜像文件检测、容器镜像自动同步等；当发现容器镜像存在安全风险，提供容器镜像检测报告，运营人员根据报告内容中的DockerFile修复建议可以实现一键式的镜像修复和加固。

图6 镜像扫描和修复

可信镜像源：针对容器镜像供应链存在的痛点，建立可信镜像源（黄金镜像），对基础镜像的来源进行管控，确保使用的基础镜像是安全可信；在镜像同步过程中通过容器镜像自动签名和加密的方式，解决镜像泄露或中间人攻击的安全风险；镜像存储是以明文的方式进行，一旦镜像发生泄露后将发生的数据泄露，针对镜像明文存储所带来的安全隐患，提供镜像存储的多种机密方式，并且完成国密算法的引入，解决镜像明文存储造成的安全隐患。

图7 可信镜像源

动态检测扩展：当威胁情报发现针对云原生集群爆发新一轮0 day或N day时，依赖常规检测引擎无法精准检测和识别，需要通过更新检测引擎规则库来实现覆盖，此时无法对集群进行快速审查和确认风险，为解决同类问题，云原生安全防护平台支持手动上传自定义检测PoC/脚本，以无害化方式进行快速检测和响应，对可能存在漏洞进行精准识别和预警。

结论

通过对云原生应用的整个生命周期进行梳理，发现各阶段存在的安全隐患，以安全左移的思路，将安全能力集成到业务的持续构建流程中，在流程中形成安全的质量门禁，降低后续安全运营成本，并且将云原生安全平台通过自动化的方式对接到部署流程中，实现业务扩缩时的自动覆盖，提升企业安全运营能力，进一步提升和释放云原生的生产力，完成云原生安全防护体系的建设和落地。

参考文献

1.CNCF：Cloud Native Security Whitepaper
2.CNIA：云原生架构安全白皮书
3.CAICT：《中国云原生用户调查报告 2020》
4.CAICT：《云原生架构安全白皮书》
5.CAICT：《云原生发展白皮书》
6.Gartner：Innovation Insight for Cloud-Native Application Protection Platforms

云原生场景下微服务跨域校验安全机制研究

文丨盛硕、车堃

证通股份有限公司

摘　要： 证券期货领域跨服务认证问题，一直是现代微服务体系结构应用中安全的研究热点。本文介绍了微服务对服务认证的主要运行机制，包括令牌和证书的使用，特别对于在面向服务体系结构领域工作并对安全问题比较重视的开发人员来说，提出了一个基于服务的认证体系结构实例，并提供了对机制的广泛概述身份验证以及微服务体系结构设计原则，同时在微服务部署中，将MutualTLS (mTLS) 协议作为保证服务间通信安全的最流行方式，在这种方法中，跨服务身份验证的责任在于部署在系统每个微服务附近的mTLS代理，mTLS代理充当微服务之间的中介，接受建立安全通信通道的请求。代理方法允许简化两个微服务之间的身份验证过程，这两个微服务可以在不同的平台上运行，使用不同的协议和数据格式。由于使用了mTLS代理，该解决方案很容易扩展，因为当系统中出现新的微服务时，只需要部署一个新的mTLS代理实例，代理也不依赖于它使用的语言或系统实现了与之相关的微服务，这使得解决方案在证券期货等金融领域是通用的。

关键字： 微服务架构、服务校验、可信网络

背景介绍

随着技术的飞速发展和处理数据量的增加，微服务体系结构越来越受到开发者的青睐。微服务的软件开发方法涉及将应用程序分解为许多小型服务，每个服务负责特定的功能。这使您可以加快开发速度，提高应用程序的可伸缩性和灵活性[1]。微服务交互是微服务架构的一个关键方面，它确保整个应用程序的运行。每个微服务都是一个执行特定功能并与其它服务通信以执行特定任务的小应用程序。在微服务架构中提供可靠和安全的交互以安全地使用它是极其重要的[2]。交互中最重要的步骤是建立连接，在此期间进行各方身份验证[3]。Service-to-service身份验证是应用程序微服务架构中两个服务之间的身份验证过程。该过程确保了服务之间数据的安全传输，并保护它们免受未经授权的访问。服务-服务身份验证机制的设计可能是一个非常耗时的过程，因为项目架构师需要考虑许多不同的因素[4][5][6]：

(1) 交互微服务可以是在不同的平台上实现，使用不同的编程语言；

(2) 身份验证机制必须是安全和抗攻击类型流量拦截、代币欺骗等；

(3) 可能需要配置复杂的基础设施，如密钥管理系统；

(4) 鉴于跨服务身份验证问题的重要性，开发人员必须仔细规划和组织微服务的交互，以确保应用程序的安全性；

(5) 微服务身份验证。

文章讨论了认证机制设计的各种途径，特别是给出了一个微服务应用程序架构的示例，这将有助于配置跨服务身份验证。

微服务架构基础

基于微服务的应用系统由多个组件 (微服务) 组成，这些组件通过同步远程过程调用或异步消息传递系统相互通信[7]。每个微服务通常实现一个 (很少是两个或更多) 单独的业务流程或特定的功能 (例如，存储客户数据、存储和显示产品目录、处理客户订单等) [8].一些服务可能提供 (REST) full API，其它微服务或客户端应用程序使用这些API，其它微服务可以实现Web 用户界面(UI)。

微服务可以以多种方式部署。它可以是应用程序服务器、虚拟机或容器中的进程。

微服务应用程序的开发基于以下原则[9]：

(1) 每个微服务都必须独立于其它微服务进行管理、复制、扩展、更新和部署；

(2) 每个微服务都必须执行相同的功能，并在有限的上下文中运行 (对其它服务的依赖)；

(3) 所有微服务都必须是容错的，必须能够快速恢复；

(4) 对于状态管理，建议使用现有的受信任服务 (例如，数据库、缓存和目录) 。

微服务体系结构中服务间交互类型

基于微服务的应用程序不受任何特定技术的限制，它们由通过轻量级机制相互通信的小型独立实体 (端点) 组成，具体实现逻辑基于业务API文档。端点API 有几种类型，例如SOAP（简单对象访问控制）或REST （ 超文本传输协议(HTTP) ）[10]。对服务的访问由不同的平台或客户类型提供，例如Web浏览器或移动设备，使用称为"客户机"的组件。服务定义使用接口描述语言(IDL) (例如Swagger/OpenAPI)，服务开发的第一步包括接口定义，在开始服务实现之前与客户开发人员一起考虑并达成一致，这样，API就充当了客户机和服务之间的契约，同时选择IPC机制 (服务间通信机制)决定了API的类型。

IPC 机构	API
异步的、基于消息的（例如 ，高级消息队列协议（AMQP ）或简单（或流）面向文本的消息（STOMP））	由通道组成消息和类型
同步请求/响应（例如，基于 HTTP REST 或 Thrift ）	由 URL、请求、响应格式组成

表1 IPC引擎与API之间的对应关系

如表1所示，IPC可以使用不同类型的消息格式：文本格式，如JavaScript Object Notation(JSON)或可扩展标记语言 (XML)，或二进制格式，如Apache Avro或Protocol缓冲区。

查询答复

可以定义两种不同的请求模式，其中包括无状态支持请求和对有状态支持业务功能的命令请求。在第一个模式中，微服务对信息发出特定请求，或采取任何行动并等待响应。在第二种模式中，一个微服务访问另一个微服务，以便它采取一些与业务功能相关的操作，以改变状态。在请求-响应类型中，涉及的两个微服务之间存在很强的运行时依赖关系，表现为以下两种方式：只有当另一个微服务可用时，一个微服务才能执行其功能；执行请求的微服务必须确保由于请求-响应协议中通信的性质，请求已成功传递到目标微服务采用HTTP等同步通信协议。如果微服务使用REST API 实现，则微服务之间的消息称为HTTP REST API。REST API通常使用标准RAML (RESTful API建模语言) 来定义，该语言旨在定义和声明微服务接口。HTTP是一种阻塞通信类型，它启动请求，并且只有在收到响应时才可以继续执行。

最简单的示例REST请求API

```
GET/api/users/1 HTTP/1.1
Host：example.com
Accept：application/json
```

实例1. REST请求API示例

此请求从托管在example域上的REST API中请求ID为1的用户数据。对此请求的响应可以表示为JSON对象。

```
{
"id":1,
"name": "huangli",
“email": "huangli@example.com"
}
```

实例2.以JSON对象的形式响应请求

请求-响应交互的另一个示例是SOAP请求。

```
<?xml version="1.0"encoding="UTF-8"?>
<soap：Envelope
xmlns：soap="http://www.w3.org/2003/05/soap-envelope"xmlns：ns="http://example.com/" >
<soap：Header/>
<soap：Body>
<ns：GetUserRequest>
<ns：UserId>1</ns：UserId>
</ns：GetUserRequest>
</soap：Body>
</soap：Envelope>
```

实例3.示例SOAP请求

这个SOAP请求查询用户数据标识符1，它使用命名空间用于定义查询元素的GetUserRequest和UserId，UserId元素包含值1。

对这一请求的答复可作为XML文档：

```
<?xml version="1.0"encoding="UTF-8"?>
<soap：Envelope
xmlns：soap="http://www.w3.org/2003/05/soap-envelope"xmlns：ns="http://example.com/" >
<soap：Header/>
<soap：Body>
<ns：GetUserResponse>
<ns：UserId>1</ns：UserId>
<ns：UserName>John
Doe</ns：UserName>
<ns：UserEmail>
john.doe@example.com</ns：UserEmail>
</ns：GetUserResponse>
</soap：Body>
</soap：Envelope>
```

实例4.作为XML文档的示例响应Python

SOAP响应包含请求的数据用户，包括ID、姓名和电子邮件地址。

签名相关

当微服务需要进行交互以实现复杂的业务流程或事务时，就会使用这种类型，"发布-订阅"为基于业务域事件的方法或基于域事件的订阅方法，在给定的模式中，微服务注册或订阅业务域事件 (例如，对特定信息感兴趣或能够处理特

定请求），这些事件通过事件总线接口发布到消息代理。这些微服务使用事件驱动API构建，使用异步消息传递协议，如消息队列遥测传输(MQTT)、高级消息队列协议(AMQP)和Kafka 消息，这些协议提供通知和订阅支持。在异步协议中，消息发送者通常不会等待响应，而只是将消息发送给消息代理[11](例如，RabbitMQ队列)。这种方法的一个用例是基于特定事件将数据更新传播到多个微服务。

使用RabbitMQ异步发送Python消息的示例如下所示。

```
import pika
#连接到RabbitMQ
connection=
皮卡.BlockingConnection(pika.Connection
Parameters(
'localhost'))
channel=connection.channel()
#创建消息队列
channel.queue_declare(queue='hello')
#在队列中发送消息
channel.basic_publish(exchange='',
routing_key='hello',body='hello,World !')
print("[x]Sent'Hello,World!'")
#关闭连接
connection.close()
```

实例5.使用RabbitMQ为异步Python消息发送。

此代码连接到本地主机上的RabbitMQ代理，创建名为"hello"的队列，并注册消息处理程序。当消息进入队列时，将调用处理程序并将消息内容输出到控制台。

使用ApacheKafka异步发送和接收语言消息的示例

```
from kafka import KafkaProducer,KafkaConsumer
#定义连接到Kafka的参数-
bootstrap_servers= ['localhost：9092']
#创建一个Kafka制作人并向主题发送消息
producer=KafkaProducer(bootstrap_servers=
bootstrap_servers) producer.send('test-topic',b'Hello,
World !')
#创建Kafka消费者并阅读主题消息
consumer=KafkaConsumer('test-topic',bootstrap_
servers=bootstrap_servers，auto_offset_reset='earlies
t',group_id=None)
for message in consumer：
print(message.value.decode())
```

实例6.使用Apache Kafka异步发送和接收Python消息的示例

此代码创建了一个Kafka制作人，该制作人发送消息"Hello，World！"测试主题。然后，它创建一个Kafka消费器，该消费器从该主题读取消息并将消息内容输出到控制台。

服务-服务机制

身份验证：无论选择哪种类型的服务间交互，都可以使用以下方法来确保此交互安全性：

(1) 可信网络
(2) mTLS
(3) JWT

可信网络

假设在服务间交互期间不以任何方式提供安全性。该模型依赖于网络层的系统安全性。信任网络方法的体系结构如图1所示。

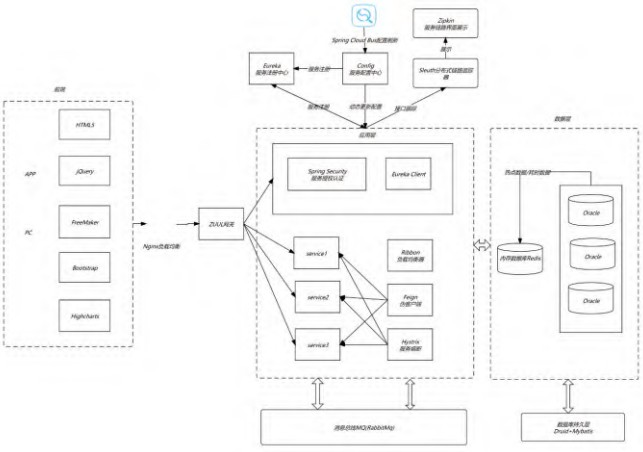


图1 信任网络体系结构

在这种情况下，网络层的安全性确保攻击者无法拦截微服务之间的通信量[12]。同时，每个微服务都是一个可靠的系统。这意味着微服务声称的关于本身和用户依赖项，其它微服务都信任并且不会以任何方式检查。这种方法并不流行，但仍然用于对每个应用程序组件的高度信任。零信任网络方法与给定的方法相反。它假设网络环境是不可靠的和敌对的。任何信息在被信任之前都会经过仔细检查。每个请求在被接受进行进一步处理之前，必须在每个节点上进行身份验证和授权[13]。

双向TLS（mTLS）

双向TLS是在部署微服务时确保服务间通信安全的另一种流行方法，连接安装示意图如图2、3所示。这种方法是当今使用的最常见的跨服务身份验证形式。

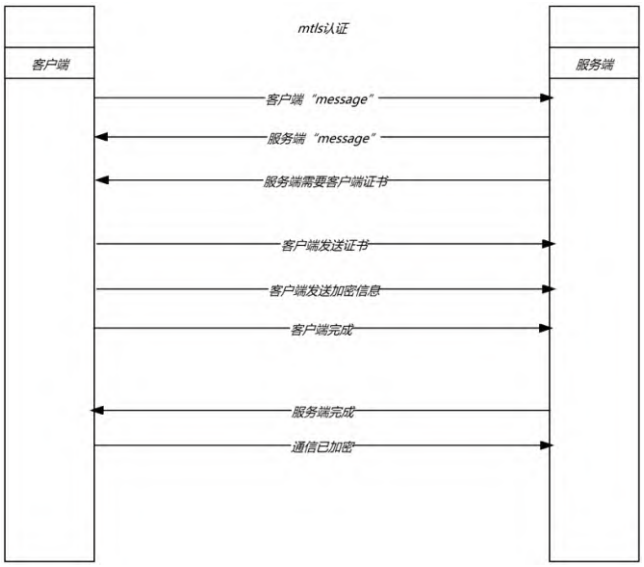


图2 mTLS连接图

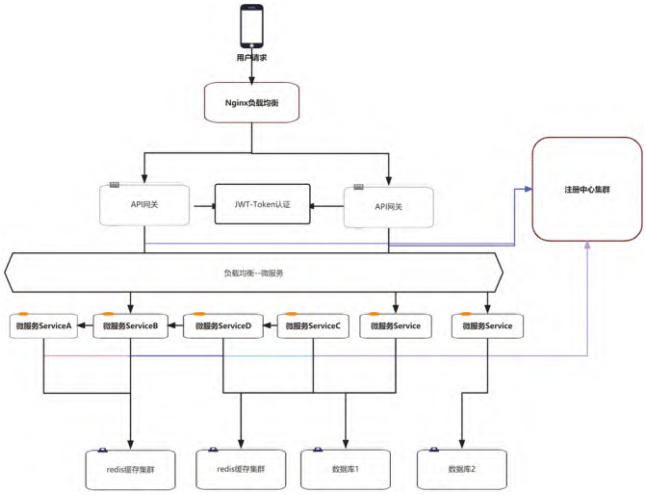


图3 基于mTLS方法体系结构

部署时的每个微服务都必须拥有公钥和私钥，这些公钥将用于通过mTLS与其它微服务交互时的身份验证。TLS确保传输数据的保密性和完整性，并识别服务。在mTLS中，每一方都有自己的证书，用于身份验证，微服务客户端发送其证书微服务服务器，并发送它的证微服务服务器到微服务客户端。每一方应检查另一方的证书，以确保其是届会的合法参与者。如果身份验证过程成功，则在微服务客户端和微服务服务器之间建立安全通信通道。如表2所示，表中显示了TLS和mTLS的差异。

TLS	mTLS
安全传输层	双向安全传输层
仅服务器对自己进行身份验证	客户端和服务器端都有对自己进行身份验证

表2 TLS和mTLS差异

项目背景

JSON Web令牌是在部署微服务时确保服务间通信安全的第三种方法，组成如图4所示。

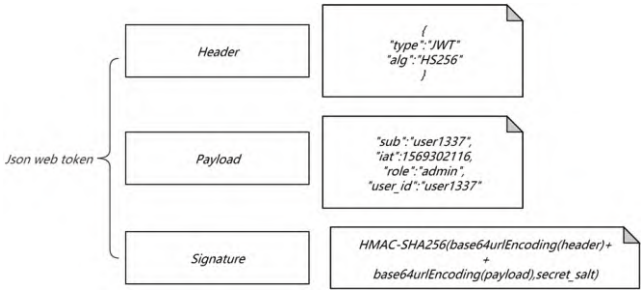


图4 JWT组成

与mTLS不同，JWT运行在应用层，而不是ISO/OSI参考模型的传输层。JWT是一个容器 ，可以将一组断言从一个地方传递到另一个地方。使用 JWT方法的架构的最简单示例如图所示。如图5所示。例如，最终用户属性 (电子邮件地址、电话号码)或最终用户权限可以作为断言。智威汤逊包括这些字段 ，并由智威汤逊的发行人签署。发布者可以是外部安全令牌服务 (STS)，也可以是微服务调用者本身。

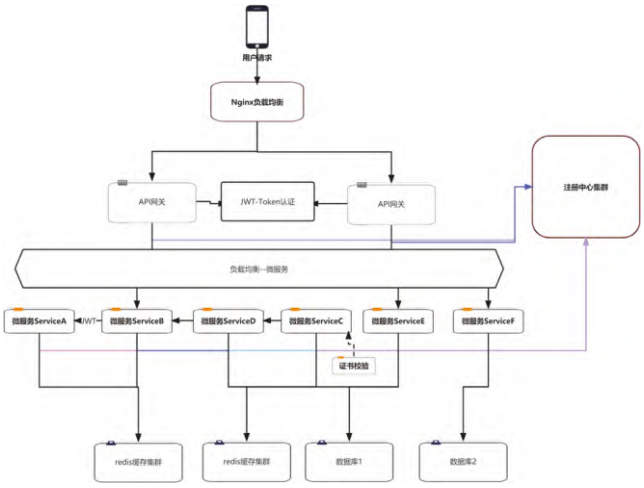


图5 使用JWT的方法体系结构

如图5所示，有自签名的JWT令牌与mTLS一样，如果使用基于JWT的自签名身份验证，则每个微服务都必须有对应的密钥对，相应的私钥用于JWT签名。在大多数情况下，基于JWT的身份验证通过TLS工作；同时，JWT提供身份验证，TLS提供传输数据的保密性和完整性。

微服务跨服务认证体系结构

对于可以访问受保护资源或被迫交换敏感信息的微服务，无论是用户的个人数据、商品信息、订单和付款信息，mTLS是最首选的服务验证方法。在安全性方面，与使用

JWT的方法不同，mTLS提供了双方的身份验证。然而，使用mTLS的方法要比JWT复杂得多，因为它需要更复杂的网络设备认证和配置基础设施。为了运行mTLS，需要在客户端和服务器端配置和安装证书，并配置网络硬件以支持TLS和mTLS协议。为了简化mTLS部署，建议使用代理mTLS，如图6所示：

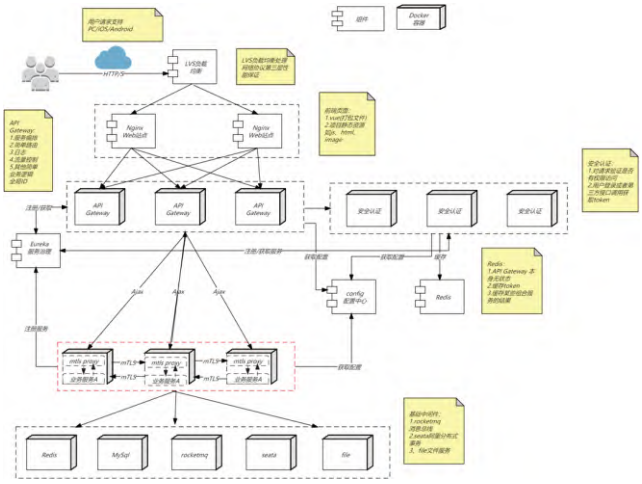


图6 基于mTLS代理服务间身份验证体系结构

在这种方法中，跨服务身份验证的责任在于部署在系统每个微服务附近的mTLS代理。mTLS代理充当微服务之间的中介，接受建立安全通信通道的请求。代理方法允许简化两个微服务之间的身份验证过程，这两个微服务可以在不同的平台上运行，使用不同的协议和数据格式。为了建立安全的通信通道，mTLS代理使用证书并验证各方的身份。每个微服务都必须有自己的证书来确认其真实性。如果证书没有通过验证，代理mTLS将不允许建立安全连接。在部署这种架构时，最重要的组成部分是公钥基础设施。

公钥基础设施

公共密钥基础设施 (Public Key Infrastructure，PKI) 建立在一组组件和过程之上，用于管理公钥和私钥对。

典型的PKI架构由以下组件组成：

证书-签名的数字文档：证书颁发机构用于确认PKI中公钥的所有者。证 书具有序列号、有效期、密码算法和加密参数等一 系列属性。证书还包含主体名称，这是标识所有者 的信息。例如，它可以是DNS名称或IP地址。

公钥/私钥对：私钥以及与之相关的公钥在数学上相互关联。公共密钥 作为公共证书自由分发钥匙。私钥确认了身份的所有权，必须由微服务或 其对应的代理保密。

证书颁发机构 (Certificate Authority，CA)：颁发对象证书，并在PKI中充当受信任的组件。证 书颁发机构颁发的任何证书都由拥有给定CA公钥的 所有对象信任。

吊销证书列表(Revocation List(CRL)是证书颁发机构(CA)撤销的 TLS证书列表。在收到证书撤销请求后，CA将唯一 的证书序列号输入CRL列表，CRL列表：

1.由证书颁发机构数字签名保护-除证书颁发机 构外，任何人不得更改；

2.每天至少更新一次-包含证书颁发机构吊销的 证书的最新列表。

下一段为上述跨服务身份验证架构提供了证书验证过程的抽象示例：

证书验证过程如图7所示。Certification Authority Server是公钥基础设施的一个组件，充当证书颁发机构。微服务A和B的私钥存储在各自的mTLS代理中。

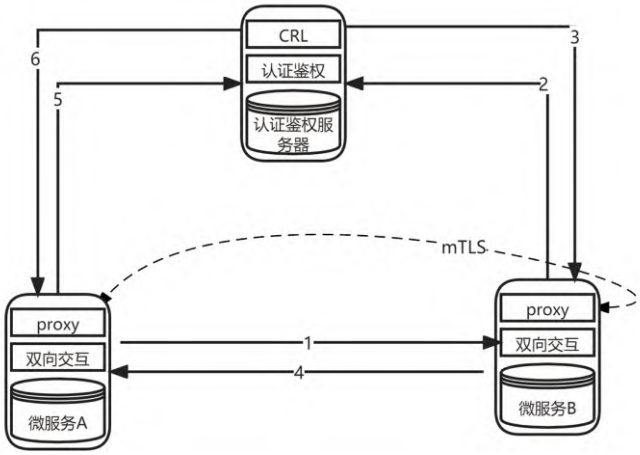


图7 基于mTLS代理验证服务间身份验证过程

连接建立阶段证书验证过程：

1.微服务代理A的mTLS向微服务代理B发送其mTLS证书。

2.微服务代理B访问具有微服务证书A的证书颁发机构服务器以验证其身份。证书颁发机构服务器 检查证书是否出现在证书吊销列表 (CRL) 中，还检查微服务A证书的真实性。

3.在进行必要的检查后，证书颁发机构服务器向微服务代理B发送有关检查成功/失败结果的信息。

4.如果成功，微服务代理B又将其证书发送给微服务代理A。

5.类似地，微服务代理A访问具有微服务证书B的证 书颁发机构服务器。

6.在进行必要的检查后，证书颁发机构服务器将有 关检查成功/失败结果的信息发送给微服务代理 A。

7.如果每个步骤都成功通过，则在微服务A和微服务B的mTLS代理之间建立安全连接，这意味着微 服务A和B之间建立了连接。

因此，我们得到了微服务中最简单的服务认证架构。由于使用了mTLS代理，该解决方案很容易扩展，因为当系统中出现新的微服务时，您只需要部署一个新的mTLS 代理实例。此外，代理不依赖于实现相关微服务的语言或系统，这使

解决方案具有通用性。同时，TLS用于微服务的交互，确保传输数据的保密性和完整性。所有这些都使这样的体系结构足够安全，可以在传输敏感数据或访问受保护资源时使用。

结论

微服务架构中的基于服务的身份验证机制在确保应用程序组件之间交互的可靠性方面发挥着关键作用。开发人员在设计服务之间的交互机制时，必须考虑安全需求。在这样做时，重要的是选择适当的技术和协议，并在不同级别对系统进行仔细测试。尽管在实现方面存在一些困难，但具有服务间交互机制的微服务体系结构是开发复杂服务的有效方法，易于扩展的应用程序并长期保持。文章中介绍的体系结构可以是不仅对微服务应用程序有用，而且对于任何其它应用，特别是那些需要高度的安全性同样适用。因此可以得出结论，文章中介绍的Service Service体系结构身份验证是一种有用的工具，用于微服务应用程序架构师，并可以应用到需要的各个领域安全高效的跨业务身份验证。

参考文献

1.张文芳、孙海锋、王宇、蔺伟、王小敏.基于自更新哈希链的安全高效车-地鉴权方案[J].西南交通大学学报，2020，55(6):11.DOI:10.3969/j.issn.0258-2724.20190205.

2.朱于军,林晓东,廖建新,等.UPT系统中的鉴权和密钥分发协议[J].电子学报，1999，27(007):51-54.DOI:10.3321/j.issn:0372-2112.1999.07.013.

3.辜希武,李瑞轩,卢正鼎.Web服务组合规范WS-CDL的类型化形式化模型[J].东南大学学报(英文版)，2008，24(3).DOI:10.3969/j.issn.1003-7985.2008.03.012.

4.何涛,缪淮扣,钱忠胜.基于π-演算的web服务流的分析与建模[J].东南大学学报(英文版)，2006，22(003):315-318.DOI:10.3969/j.issn.1003-7985.2006.03.006.

5.杜旭涛,邢春晓,周立柱.使用NWA对组合web服务进行可达性分析[J].东南大学学报(英文版)，2008，24(3):293-295.DOI:10.3969/j.issn.1003-7985.2008.03.010.

6.佚名.基于并发事务逻辑的Web服务编制验证 Support info[J].Chinese Journal of Electronics[2023-06-13].

7.吴恒,郝庭毅,宋云奎,等.面向微服务架构的容器级弹性资源供给方法[J].计算机研究与发展，2017，54(3):12.DOI:10.7544/issn1000-1239.2017.20151043.

8.叶盛,王菁,辛建峰,等.云边环境下微服务组合系统的动态演化方法[J].计算机应用，2023，43(6):1696-1704.DOI:10.11772/j.issn.1001-9081.2022060882.

9.杨舒,苏放.基于微服务的分布式数据安全整合应用系统[J].计算机工程与应用，2021，57(18):238-247.DOI:10.3778/j.issn.1002-8331.2005-0368.

10.尹磊,周风余,李铭,等.基于微服务的服务机器人云服务设计方法[J].山东大学学报 (工学版), 2019, 49(6).

11.王焕强,俞东进,金一科,等.基于微服务架构和支持业务过程可靠执行的数据通信方法[J].计算机集成制造系统, 2019, 25(4):8.DOI:CNKI:SUN:JSJJ.0.2019-04-017.

12.吕中梁,韦化,祝云,et al.EMS高级应用微服务Web架构[J].电力系统及其自动化学报, 2019.DOI:CNKI:SUN:DLZD.0.2019-05-007.

13.陈立哲,吴际,杨海燕,等.基于日志挖掘的微服务测试集缩减技术[J].软件学报, 2021, 032(009):2729-2743.