金融行业网络安全

白皮书

（2020年）

组织编写：中国银行保险报
CHINA BANKING AND INSURANCE NEWS

智力支持：亚信网络安全产业技术研究院

版权声明

前 言

金融是国家重要的核心竞争力，是现代经济的核心。金融安全是国家安全的重要组成部分。国家高度重视金融安全。习近平总书记强调，要切实把维护金融安全作为治国理政的一件大事。近年来，随着新技术在金融行业的广泛、快速应用，金融业数字化转型不断加快，但新技术引发的风险问题也日趋凸显。金融行业网络安全面临的各项威胁和挑战持续升级。

为进一步推动金融行业网络安全体系建设，大力提升金融行业网络安全水平，由中国银行保险报联合亚信网络安全产业技术研究院共同发起，于 2020 年 4 月开展了金融行业网络安全专项调研活动。调研秉承全面、公平、客观的原则，采用广泛覆盖与深度走访相结合、线上与线下相结合的方式，在问卷编制、报告撰写过程中引入了咨询公司分析师与行业专家的指导。本次调研重点面向银行、保险、证券领域金融机构，覆盖国有商业银行、股份制银行、城市商业银行、农村商业银行等细分领域，同期组织线下访谈，与十余位金融机构网络安全负责人、业内专家进行了深度交流。

结合调研数据，本白皮书总结了金融行业网络安全整体态势，从网络攻击、“互联网+”金融快速发展以及数据安全监管和隐私保护难度等方面阐述了金融行业网络安全面临的风险与挑战，重点关注金融行业网络安全关键技术与创新领域的探索与突破，分析了金融行业网络安全发展趋势，为进一步提升金融行业网络安全建设和维护水平提供参考和帮助。由于时间较紧，本白皮书所呈现的分析与内容难免有不足之处，欢迎提出宝贵意见和建议。

目　录

综　述

在网络安全和信息化领域，要树立新的发展观，尤其要处理好安全和发展的关系。2014 年 2 月，习总书记在中央网络安全与信息化领导小组第一次会议上指出，网络安全和信息化是一体之两翼、驱动之双轮。2016 年在网信工作座谈会上，他再次强调指出：网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。

金融行业在国民经济发展中占据着重要地位，影响着国家产业经济发展的稳定性，作为国家发展的重点基础保障服务之一。当前新一轮科技革命和产业变革深入发展，数字化浪潮蓬勃兴起，数据作为国家基础性战略资源和关键生产要素的地位日益凸显，金融行业作为数据密集型和科技驱动型行业，在信息化建设已经走在各个行业前列。

2018 年 4 月 27 日，第十三届亚欧财长会议重点讨论了全球及亚欧宏观经济形势、税收与经济数字化、金融网络安全等议题，并发表了公报。会议认为，全球金融系统需要重点关注网络安全风险。金融部门的数字化和创新为全社会带来效率和便利，金融服务对于国际国内金融体系都至关重要。各方表示将共同努力打击金融犯罪以阻止非法收益，并不断提升金融行业和机构应对网络安全风险的韧性。

从国际范围来看，新型冠状病毒肺炎迫使许多金融机构加快了数字

化的步伐。由于办公室关闭，工作方式从线下转移至线上，许多机构被迫接受数字化转型。随着数字化和远程办公的加速发展，使得员工、客户、服务商和合作伙伴之间的界限越来越模糊，许多传统的网络边界和范围也变得模糊起来。用户、负载、数据、网络和设备无处不在，“零信任”网络安全架构的出现得到了越来越多金融机构首席信息安全官的认可。

与此同时，越来越多的国际金融机构使用新兴技术来创新和开发新的产品、服务和数字渠道，以保持机构的持续竞争力。首先，金融机构在产品和服务创新方面大量与金融科技公司展开竞争和合作，这些创新往往需要足够的速度和灵活性才能成功。其次，机构会寻求更新、更简单的方式与客户开展业务，但新渠道可能会伴随其自身的网络安全脆弱性。这些创新技术的应用和新渠道都可能带来新的网络安全威胁，这些转变给首席信息安全官和网络安全团队带来了成倍的问题，传统的网络安全控制措施已经不能满足需求，需要创新的网络安全技术才能提供足够的安全防护级别，否则安全将成为业务开展的绊脚石。

从国内金融行业网络安全总体态势来看，在行业监管要求日益严格细化的大背景下，金融行业已经普遍形成了较为完善的网络安全组织与制度管理体系，但是由于网络安全风险意识不足和宣贯不到位，部分安全管理要求流于形式；由于大型金融机构和中小型金融机构的信息化水平差距较大，网络安全防护技术体系的建设情况也呈现出明显的参差不齐，大型金融机构普遍构建了纵深的安全防御体系，中小金融机构则缺乏顶层的体系化设计，以单点被动防御为主，整体安全防护能力较差；

在网络安全投入上，国内金融行业网络安全投入比例只占营收的 0.1%，与国外同行 0.4%的平均水平有较大差距。

调研结果显示，在金融行业网络安全关键技术应用上，端点安全以防病毒和准入为主要防护手段，基本已全面部署，但 EDR 等主动威胁检测能力尚不具备；云安全和云平台基本采取同步规划建设的方式，防护现状较好，但也有部分中小金融机构存在云平台裸奔的情况；数据安全防护技术应用以数据脱敏、数据加密等成熟技术的场景化应用为主，尚未形成体系化的数据安全防护能力；态势感知和安全中台的建设已经成为行业热点，且人行推进的金融业态势感知与信息共享平台大大加速了这一进程，但由于多品牌安全产品联动实现有一定困难，因此部分机构建设效果未达到预期；在身份安全管理建设方面，中小金融机构和大型金融机构有明显差距，还有较大的提升空间；另外威胁情报的应用也备受关注，其应用场景呈现多样化特征。

随着国内外网络安全复杂、严峻形势的演变，我国金融行业网络安全形势日趋严峻，面临诸多新的风险和挑战。首先，金融科技创新大量采用新技术实现业务创新的同时，也给网络安全带来了更多隐性风险，提出了更高要求；其次，随着事件型漏洞和高危零日漏洞威胁的持续走高，网络攻击的种类、规模和方式也不断增加，隐蔽性更强的 APT 攻击成为常态；其三，金融数据涉及大量个人信息和资金等内容，数字化转型不断提升数据价值，金融业务的复杂性使得数据安全保护体系的建设难度不断加大；最后，金融行业的业务创新不断加速，各金融机构与第三方机构的连接越来越多，同时中小金融机构大量的依靠科技外包来获

得快速发展，风险的传导范围和信息科技外包风险不断加大，需要重点关注。

从国内金融行业网络安全发展趋势来看，受信息泄露事件和《数据安全法》、《个人信息保护法》等法规颁布的双重影响，数据安全和个人隐私保护将成为未来建设的重点；与此同时，金融行业对于网络安全服务需求持续增加，网络安全运营化和零信任架构也受到了普遍的关注，投入会持续上升；金融行业信息技术应用创新正在加速推动，为网络安全的基础性问题解决提供了新的契机；同时随着 5G 在金融领域的商业化应用，将产生新的基于场景应用的网络威胁，带来新的安全挑战，为金融网络安全带来新的研究课题。

针对金融行业面临的新的风险和挑战，结合目前存在的问题，我们需要进行充分的客观分析，积极抓重点、补短板、强弱项，加强金融业网络安全和信息化统筹指导，筑牢金融网络安全屏障。结合本次的调研分析结果，建议金融机构从以下几个方面着手，快速提升网络安全综合防护能力。一是以人为本，采取多种方式加强网络安全意识培训和宣贯，提升全员网络安全风险防范意识；二是以合规能力建设为基础，全面贯彻落实“三化六防”防护体系新思想；三是创新思路，统筹推进网络安全顶层规划工作；四是加强个人金融信息保护，逐步建设全要素的数据安全治理体系；五是加强人、工具协同，首先通过 XDR 解决方案的快速落地形成完整的威胁检测防御能力，其次建设安全中台，实现从被动响应到主动运营的转变，形成体系化的安全运营能力；六是注重网络安全人才培养，同时加强与专业机构的合作，持续提升网络安全人员的专业技能。

一、金融行业网络安全总体态势

（一）行业监管要求日益严格细化

2017 年 6 月 1 日，《网络安全法》开始施行。2017 年 7 月，国家互联网信息办公室公布《关键信息基础设施安全保护条例（征求意见稿）》，详细阐明了关键信息基础设施的范围、运营者应履行的职责以及对产品和服务的要求；并明确指出：通信、能源、交通、金融等行业主管部门和关键信息基础设施运营单位需要按照国家有关要求，建立健全网络安全责任制，积极采取有效措施，从制度机制、标准规范、教育培训、手段建设、技术创新等方面提升安全保护能力。

2019 年 12 月，网络安全等级保护 2.0 系列标准开始正式实施，扩大了保护对象的范围，丰富了保护方法，增加了技术标准，提高了测评合格分数，进一步细化和提升了合规要求。2020 年 11 月 11 日，中国人民银行发布《金融行业网络安全等级保护实施指引》系列标准，以及《金融行业网络安全等级保护测评指南》。该标准依据国家网络安全等级保护 2.0 相关要求，为金融行业的网络安全建设提供方法论、具体的建设措施及技术指导，完善金融行业网络安全等级保护体系。

在网络安全具体细分领域，2020 年中国人民银行也密集出台了多项金融行业网络安全相关标准，用于指导和促进行业整体网络安全防护能力的持续提升。

在数据安全保护领域，2020 年 2 月 13 日，《个人金融信息保护技

术规范》（JR/T0171-2020）正式发布并实施，该文件在个人金融信息范围、收集使用行为、安全技术标准、机构安全岗位设置等方面做出了细致的规定，对金融机构针对金融信息建立不同信息保护层级方面提出了更高的要求。2020 年 9 月 23 日，《金融数据安全 数据安全分级指南》（JR/T 0197—2020）正式发布，该标准给出了金融数据安全分级的目标、原则和范围，明确了数据安全定级的要素、规则和定级过程，并给出了金融业机构典型数据定级规则供实践参考，有助于金融业机构明确金融数据保护对象，合理分配数据保护资源和成本，是金融机构建立完善的金融数据生命周期安全框架的基础，能够进一步促进金融数据在机构间、行业间的安全流动，有利于金融数据价值的充分释放和深度利用。

在新技术应用风险控制领域，2020 年 2 月 5 日，中国人民银行编制并正式发布《金融分布式账本技术安全规范》，该规范有助于金融机构按照合适的安全要求进行系统部署和维护，避免出现安全短板，为分布式账本技术大规模应用提供业务保障能力和信息安全风险约束能力，对产业应用形成良性的促进作用。2020 年 7 月 10 日，中国人民银行正式发布《区块链技术金融应用评估规则》（JR/T 0193-2020）金融行业标准，该标准从基本要求、性能、安全性等方面为区块链技术金融应用提供客观、公正、可实施的评估规则，适用于金融机构开展区块链技术金融应用的产品设计、软件开发、系统评估。上述两个规范和标准的落地为区块链技术在金融行业的大力应用提供了安全合规框架。

时间	标准号	标准名称
2020 年 9 月 23 日	JR/T 0197—2020	《金融数据安全 数据安全分级指南》
2020 年 7 月 10 日	JR/T 0193-2020	《区块链技术金融应用 评估规则》
2020 年 7 月 10 日	JR/T 0191—2020	《证券期货业软件测试指南 软件安全测试》
2020 年 7 月 10 日	JR/T 0192—2020	《证券期货业移动互联网应用程序安全规范》
2020 年 2 月 5 日	JR/T 0068—2020	《网上银行系统信息安全通用规范》
2020 年 2 月 13 日	JR/T 0185—2020	《商业银行应用程序接口安全管理规范》
2020 年 2 月 5 日	JR/T 0184—2020	《金融分布式账本技术安全规范》
2020 年 2 月 13 日	JR/T 0171—2020	《个人金融信息保护技术规范》

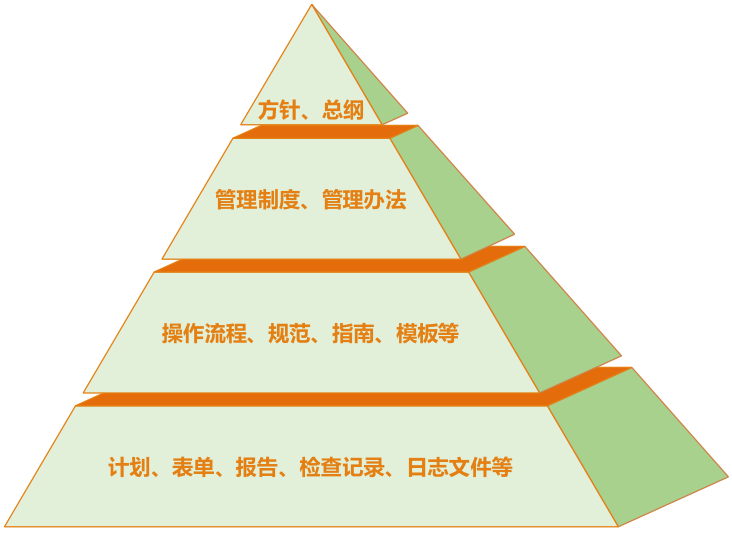
在行业监管落地方面，2019 年下半年，为落实习近平总书记“全天候全方位感知网络安全态势”的重要指示精神，提高行业网络安全态势感知和信息共享技术支撑能力，中国人民银行开始建设金融业态势感知与信息共享平台项目，目前已基本实现金融机构的全量接入，未来将实现对金融行业所有机构网络安全信息的总览监测、对网络安全态势数据的综合分析，建立上下统一调度的指挥平台，帮助成员单位快速共享情报，形成行业内安全资产的风险管控。接下来，这一平台将会成为监管机构制定监管要求以及对金融机构网络安全工作进行监管的重要抓手，为监管要求落地提供重要技术支撑。

（二）组织与制度体系进一步完善

随着近几年行业监管机构对网络安全管理体系要求的不断深入和细化，各金融机构高度重视网络安全组织与制度体系建设工作。

70%的受访机构表示，已在机构内成立专门的网络安全管理部门；其他 30%的金融机构，虽然尚未成立独立部门，但已经将网络安全管理作为部门职能，开展了相关的工作。在已成立的独立机构中，多数由信息科技分管领导牵头负责，少数由合规/风险分管领导或其他领导牵头，网络安全在金融行业已成为信息技术体系的重要职能组成。

此外，安全管理制度体系是网络安全体系建设得以发挥实效的重要基础。调研显示，金融行业网络安全管理制度体系建设情况良好，通过建立各项管理规范和技术标准，规范基础设施建设、系统和网络平台建设、应用系统开发、运行管理等重要环节，形成了由信息安全方针、信息安全制度、信息安全流程等构成的全面的、系统的制度体系。但是由于网络安全风险意识不足和宣贯不到位，部分安全管理要求流于形式。



网络安全管理制度体系

（三）技术体系建设水平参差不齐

2019 年 4 月，中国银行保险监督管理委员会启动网络安全专项治

理工作，组织全国 3000 余家银行保险机构开展网络安全风险自查，对部分机构现场检查、现场督查，组织 3 家银行参加网络安全演练，并在此基础上开展 2019 年度信息科技监管评级，客观评价银行保险机构的网络安全管理水平。

其中，2019 年度信息科技监管评级方面，银行机构平均得分最高的是股份制银行，其次是大型银行；外资法人银行、民营银行平均分最低，仅相当于大型银行的 2/3。225 家主要保险机构方面，平均得分与银行机构差距不大，但分差较大，最低分仅相当于最高分的 50%，两级分化明显。不同类型机构中，保险集团公司平均分最高，其次是人身保险公司，再保险公司平均分最低。

本次的调研结果充分反映了金融机构网络安全技术体系建设水平参差不齐的现状。大型金融机构普遍构建了纵深的网络安全防御体系，同时配置了超过 50 人的网络安全团队，安全防护水平较高；而中小金融机构受限于整体投入及专业人员不足等问题，网络安全防御技术体系缺乏顶层的体系化设计，以单点被动防御为主，整体防护能力相对较差。

（四）网络安全投入比例总体偏低

随着国家和金融行业网络安全监管力度的加强，金融机构对网络安全建设愈发重视，投入也逐年递增，但从当前网络安全工作推进的实际情况来看，面临最突出的问题仍旧是人员缺失和资金不足问题。

结合 2019 年上市金融机构年报数据和本次调研数据，主要金融机构 IT 总投入占营收的比例约 3%，其中网络安全投入占 IT 总投入的比

例平均约 4%。综合来看，主要金融机构网络安全投入仅占金融机构总营收的 0.1%左右，这一比例距离 0.4%的国际水平有很大差距，网络安全投入总体处于较低水平。

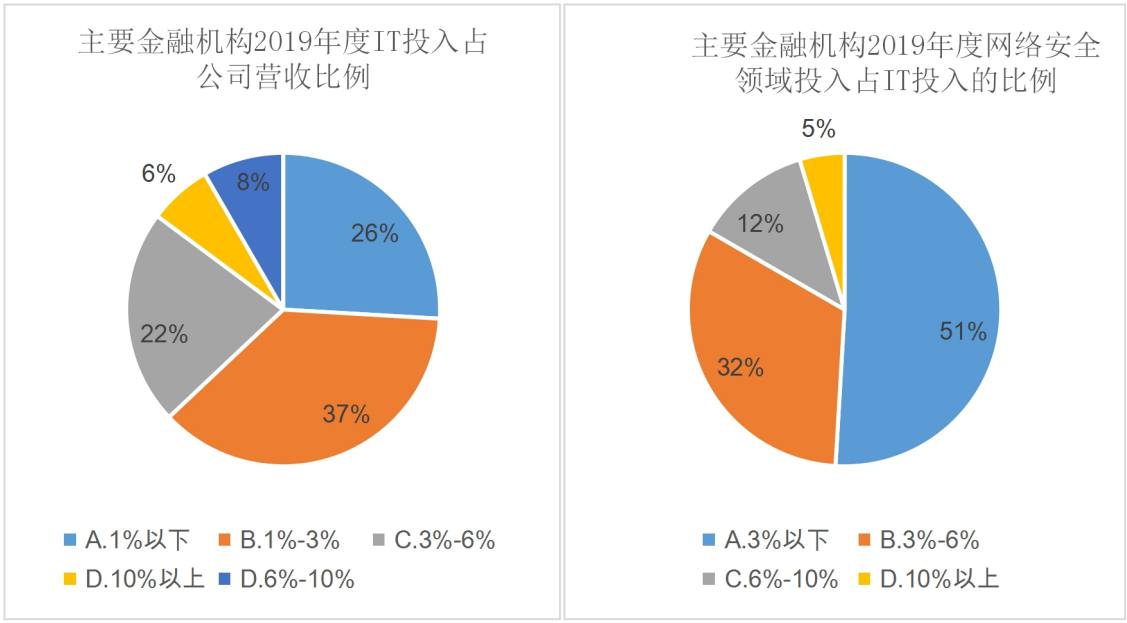


图 1：主要金融机构 2019 年度 IT 与网络安全领域投入占比

二、金融行业网络安全关键技术应用现状

网络安全技术实践为网络安全体系落地提供有效技术支撑，和安全管理体系相辅相成，缺一不可。网络安全技术实践种类繁多，本次调研主要涉及数据安全、云安全、端点安全、态势感知、身份安全和威胁情报等关键技术领域。

（一）端点仍以防病毒和准入为主要防护

端点安全的核心目标是防止网络受到本地或远程安全威胁。端点的范围很广，包括服务端和客户端的服务器、台式机、笔记本电脑、平板

电脑和智能手机等，其安全漏洞将给网络安全造成风险隐患和实际损害。防火墙、VPN、恶意软件防范和端点准入管控等是常规的端点安全技术手段。端点安全是网络安全体系建设中涉及范围最广，推广难度最大的部分，是安全团队最头痛的问题。

在终端安全管理方面，超过 90%的金融机构部署了防病毒软件和终端网络准入进行基本的终端安全防护，统一的补丁管理、外设管理和应用管理相对稍差，但也超过了 50%。

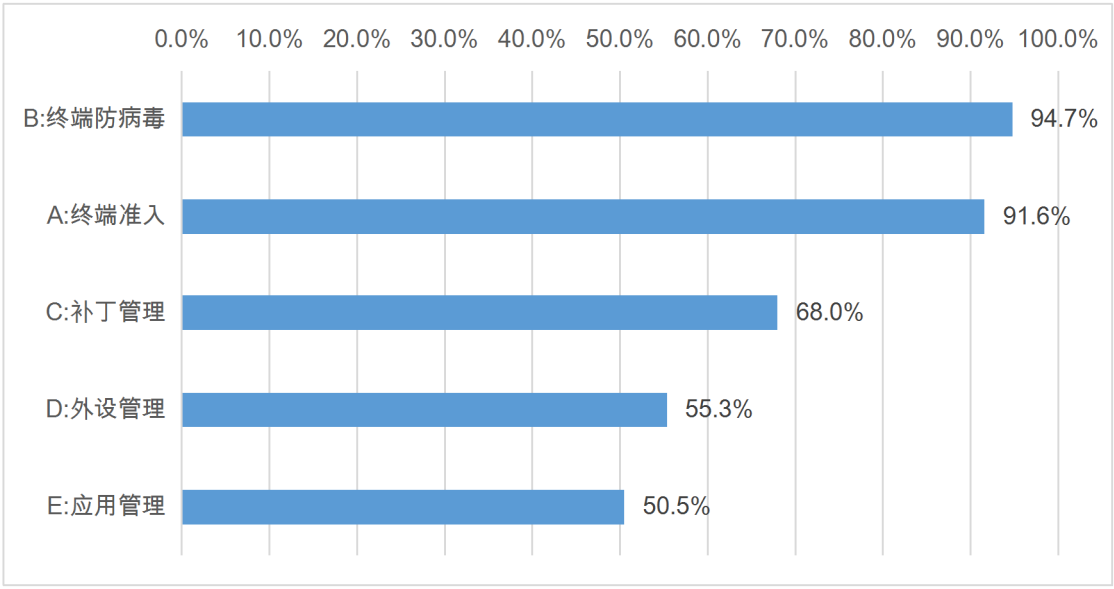


图 2：主要金融机构终端安全领域控制实施情况

在服务器主机安全管理方面，超过 70%的用户制定了主机安全基线并定期检查，同时定期验证并更新安全补丁；在主机恶意代码软件防护方面，Windows 平台服务器主机覆盖情况良好，但非 Windows 平台部署情况较差，只有不足 15%。

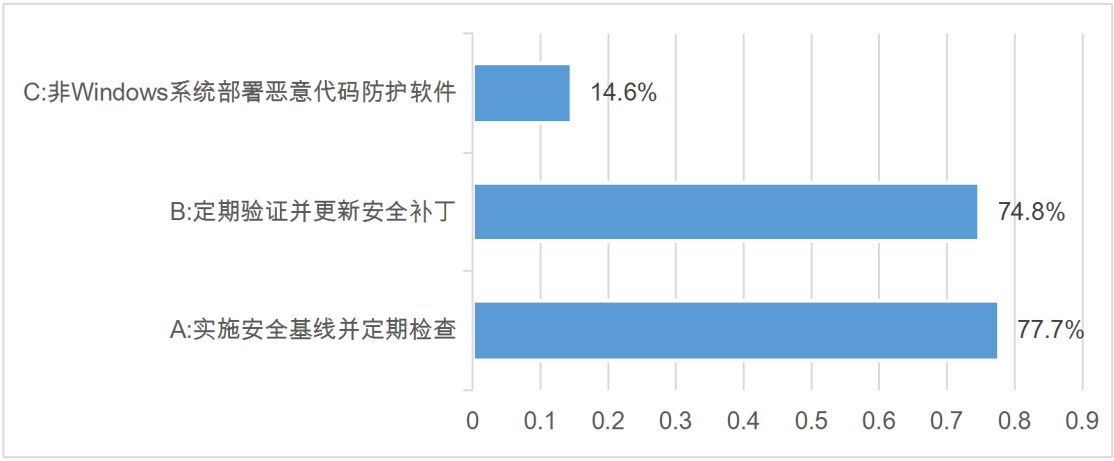


图 3：主要金融机构主机安全控制实施情况

（二）云安全和云平台基本同步规划建设

越来越多的金融机构采用云服务（私有云、混合云）模式部署自己的业务系统，云安全成为保证业务安全的核心诉求之一。云安全是一个统一的层次化安全防护体系，涉及基础设施、数据、应用等多个层面的安全能力构建和联动。

无论是公有云还是私有云服务形式，超过 85%的金融机构都部署了云安全管理系统，对云的安全防护进行统一的管理，以避免新技术应用隐藏的安全风险，但也有 13%的用户在私有云上尚未部署云安全管理系统，面临较高风险。

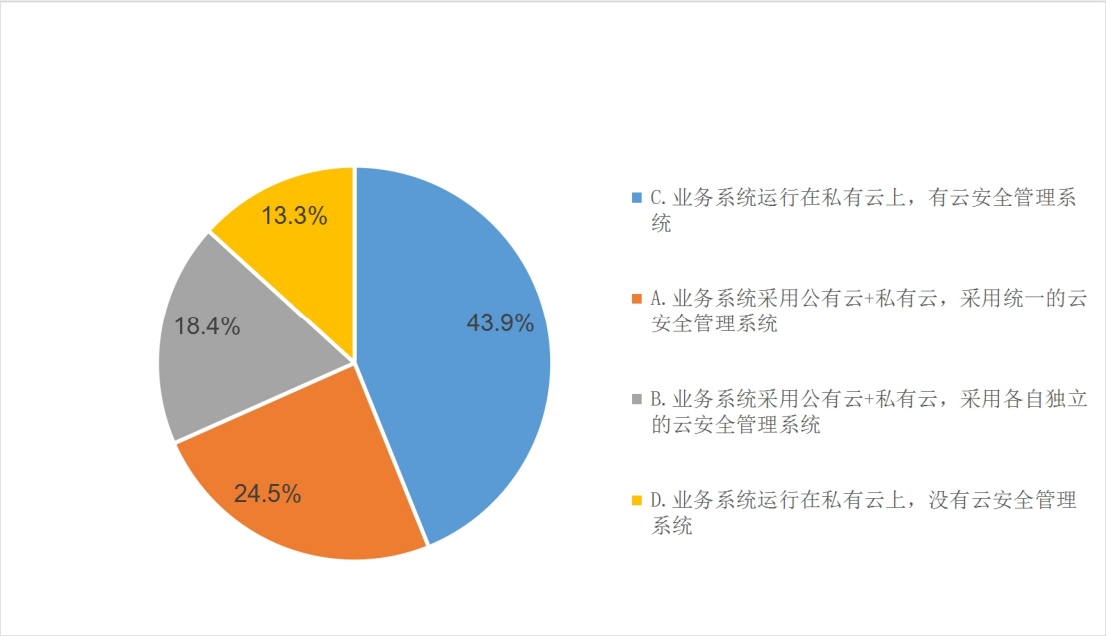


图 4：主要金融机构在云部署和云安全管理方面的情况

（三）数据安全以成熟技术点状应用为主

数据安全的核心目标是保证数据的机密性、完整性和可用性。数据安全也是金融行业的重要安全需求，受到高度关注，但目前主要的数据安全防护技术手段还是传统的针对数据本身的保护，在数据共享安全防护方面，仍然处于探索阶段。

在数据安全领域，针对重要数据的数据备份、数据加密、数据脱敏以及数据库操作审计应用比例已经超过 70%，得到了较广泛的应用；数据防泄密技术的应用情况稍差，但也达到了 50%的覆盖度，同时敏感数据发现、数据交换平台和数据水印技术应用情况只有 30%左右；多方计算平台作为数据共享场景下的新兴技术，应用比例很低，目前只在部分头部金融机构进行试点和应用推广。

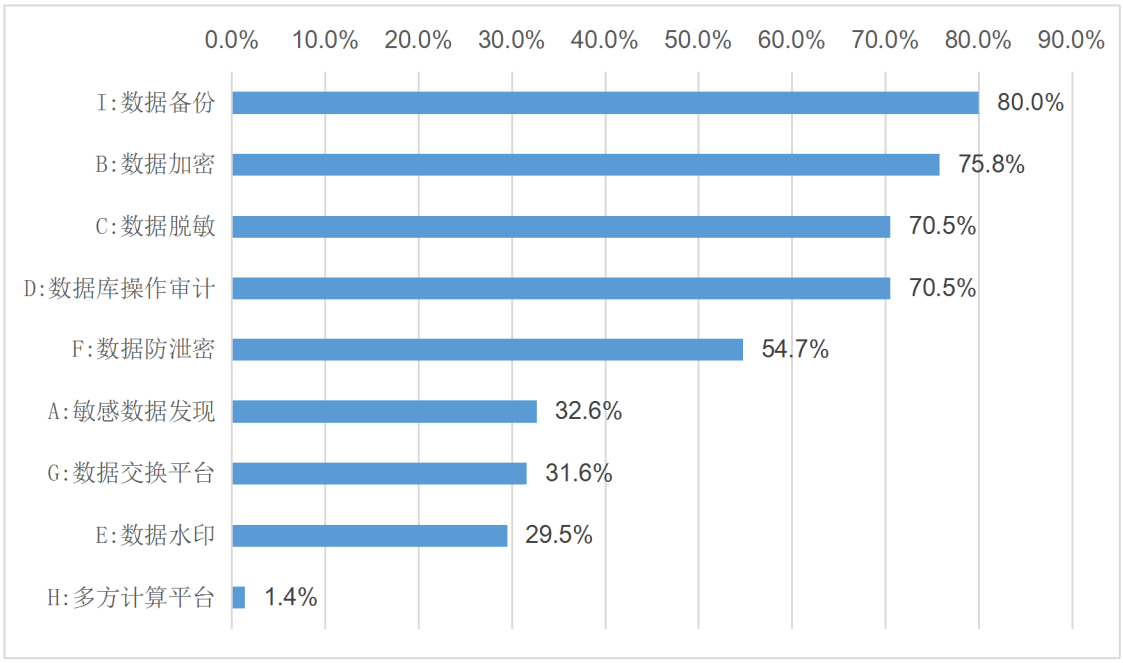


图 5：主要金融机构数据安全领域控制实施情况

（四）态势感知是目前网络安全建设热点

智能安全以自适应安全为发展方向。自适应安全架构（Adaptive Security Architecture）是 Gartner 提出的下一代安全体系框架，从预测、防御、检测、响应四个维度，强调安全防护是一个持续处理的、循环的过程，细粒度、多角度、持续化地对安全威胁进行实时动态分析，自动适应不断变化的网络和威胁环境，并不断优化自身的安全防御机制。态势感知和安全中台是智能安全的两大支柱。

态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终使能决策与行动，保证安全能力的落地。

态势感知平台作为近几年金融行业网络安全建设的热点，目前已经完成建设的超过 20%，其中有接近 6%的建成客户表示整体效果未达预期，究其原因基本都是因为机构内使用的安全产品品牌众多，同时产品的技术实现能力参差不齐，只能有限度的联动或根本无法联动。另有近 30%的用户正在建设过程中预计到 2020 年底，超过 50%的金融机构将完成基本态势感知平台的建设，在未来 3 年内，还将有 40%左右的金融机构计划完成自身态势感知平台建设。同时，2019 年下半年，中国人民银行开始建设行业级的金融业态势感知与信息共享平台，将大大加速中小金融机构态势感知平台建设进程。因此，未来 3 年，金融机构态势感知平台建设将进入高峰期。

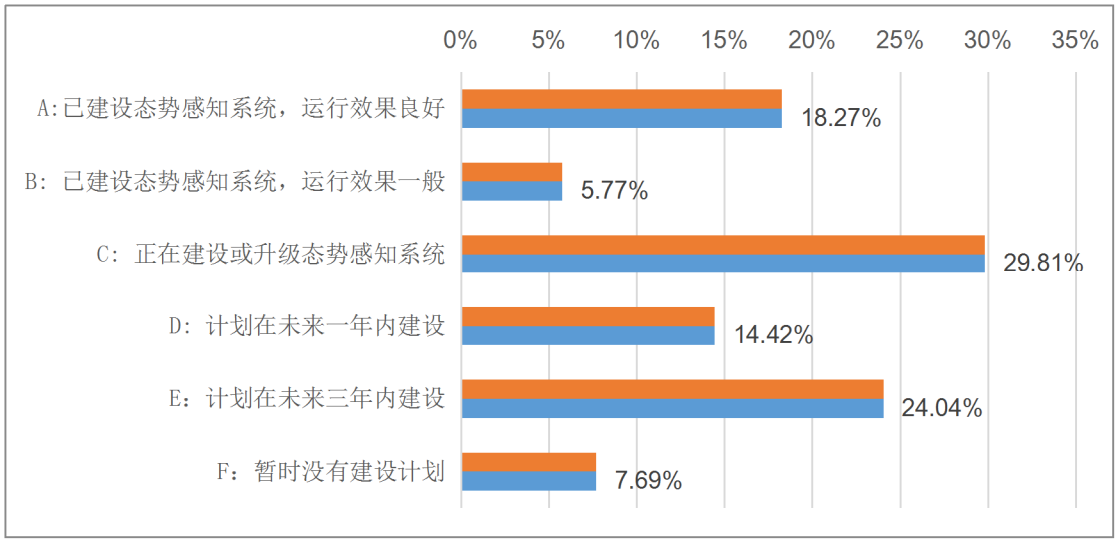


图 6：主要金融机构网络安全态势感知系统建设情况

安全中台结合安全编排自动化与响应（SOAR：Security Orchestration, Automation and Response）和软件定义安全（SDSec：Software Defined Security）等新的安全架构和技术理念，以“弹性、

自适应”为中心，以精密产品联动、自愈分析、自我学习输出为工作主线，以威胁情报、指挥平台和安全服务为辅助支持，以安全战略、安全流程闭环为目的，从技术、流程、服务等多个维度实现持续安全合规、能力对接和状态评估，提高安全运营效率，提升实际安全防御能力。

网络安全需要全息化、服务化和实效化，“安全中台”服务架构的提出成为网络安全建设的一个新趋势。安全中台的核心目标是提升安全效能、数据化运营服务、更好地保障客户业务持续、规模化地创新发展，是安全服务于业务理念的核心体现。从调研数据来看，10%的头部金融机构已经完成或部分完成了安全中台的建设，近一年内有超过 15%的金融机构计划建设安全中台，近三年内计划建设安全中台的金融机构比例超过了 45%，安全中台的建设将进入第一个高潮。

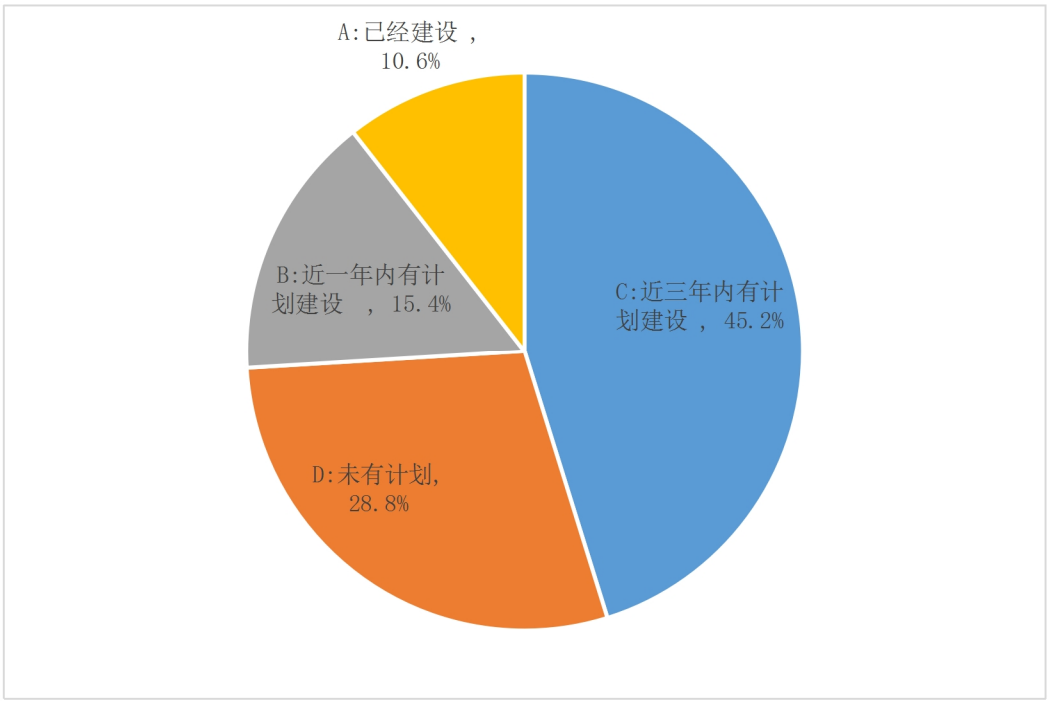


图 7：主要金融机构安全中台规划和建设情况

（五）身份安全管理建设有较大提升空间

身份安全围绕接入网络的各种对象（例如网络设备、应用、服务等）的标识、凭据和属性等因素建立身份管理，基于各种对象的唯一身份，对其进行授权管理，通过认证和鉴权对各种对象进行身份鉴别和访问控制，并收集各种对象的接入日志和操作日志等信息，进行行为分析和审计。身份安全引入零信任的理念，相关的技术和解决方案也正在逐渐成熟。

身份管理是用户管理的基础，直接影响信息系统的整体运维和管理效率。从调研情况来看，接近 30%的大中型金融机构实现了网络安全设备、主机系统、内部应用的统一身份管理；9%的头部金融机构同时还实现了合作伙伴及客户的统一身份管理。剩余 70%中小金融机构在统一身份管理方面情况不一，还存在较大改进空间。

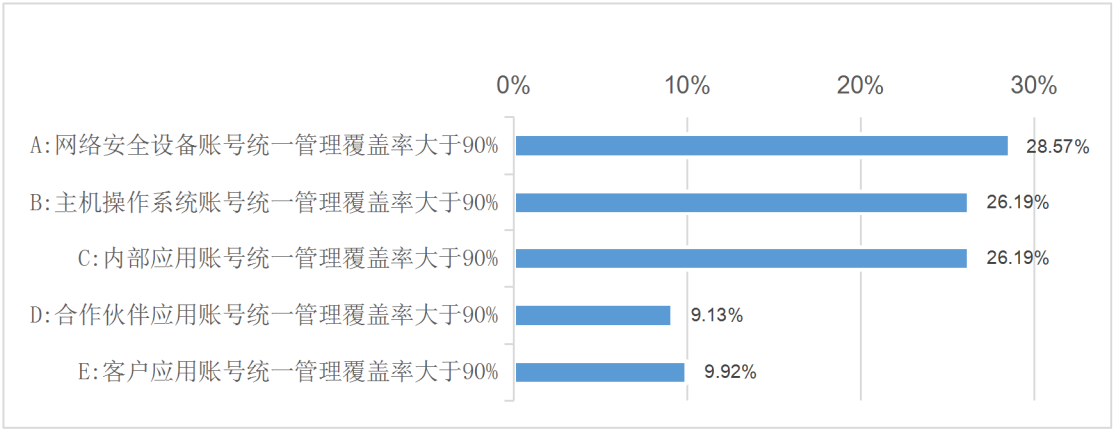


图 8：主要金融机构统一身份管理领域控制情况

（六）威胁情报受关注和应用场景多样化

近年来，国内威胁情报领域的投资和热度持续增加，对行业化威胁情报、政府主导威胁情报和商业化威胁情报的关注度不断提升，威胁情报的价值已得到普遍认可和接受。据统计，2019 年国内威胁情报市场为 15 亿元人民币，保守估计五年后，威胁情报平台市场规模将到达 65.1 亿元人民币，赋能市场规模 360 亿元人民币。

以亚信安全、360 企业安全、微步在线等为代表的威胁情报厂商进一步赋能安全应用产品，深化以威胁情报驱动的安全场景，提供多种用途的威胁情报，例如，供安全产品检测和报警排序使用的战术情报（Tactical TI，一般为已知攻击的 IoC 指标），供安全运营人员做事件分析、安全狩猎使用的作战情报（Operational TI，一般为安全事件的上下文信息），供安全管理者确定安全建设投入方向使用的战略情报（Strategic TI，一般为攻击团伙全景分析报告）等等。同时，威胁情报领域也开展了一些深层次的应用场景尝试：

1.威胁情报深入安全运维

过去威胁情报多以 IOC 形式的机读情报交付于企业客户，并不关心企业是否有能力消费这些情报，面对大量的 IOC 告警以及缺乏足够的上下文进行关联分析，运营人员无法用合理的方式区分出需要分析、处理的事件。针对此类的问题，提出了一类创新型产品 XDR（扩展检测和响应），通过从多个安全产品自动收集和关联数据，改进威胁检测和事件

响应的能力。在这个体系下，威胁情报能够在终端侧、网络侧和运营侧发挥更大的协同分析、精密联动效应。

2.威胁知识图谱逐步应用

追踪溯源是威胁情报的核心工作之一。威胁情报的分析越来越强调对威胁事件的深度挖掘能力，利用大数据、机器学习等技术在海量历史积淀的基础数据里，进行关联分析。解决关联分析、数据挖掘难点的最好方式，是提供基于可视化的自动关联分析能力，这是情报领域的一个重要创新领域。威胁知识图谱是知识图谱在网络安全领域的实际应用，包括基于本体论构建的安全知识本体架构，以及通过威胁建模等方式对多源异构的网络安全领域信息进行加工、处理、整合，转化成为的结构化的智慧安全领域知识库。

3.特定领域情报共享

虽然当前国内威胁情报的发展一帆风顺，但在威胁信息的共享和协作层面，仍然存在较为明显的短板，起步较为缓慢。其中重要原因是厂商之间“竞争大于合作，封闭分散大于开放联动”。国内有数十家威胁情报厂商，不可避免地出现重复造轮子的情况，而高质量的情报不能靠单打独斗，需要生态合作，强强联合，实现团队协同作战。因此，开放的心态和协同的行动至关重要。

4.利用威胁情报增强 APT 防御

APT 攻击一般来自特定攻击团伙的攻击，由于金融行业的数据与信息具有高价值特点，也是 APT 攻击的常见目标。利用威胁情报系统，研究黑客团伙的攻击手段、规律以达到针对性防守的目的，平衡攻防的不对等，实现威胁情报的痛苦金字塔的最顶端 TTP（Tactic，Technique，Procedure）问题。这也为金融行业对抗 APT 攻击提供了一种有效的手段。国内部分领先的金融企业已经开始通过建设威胁情报系统来收集网络犯罪分子的 TTP 信息，从而更深入了解威胁行为者的意图，时刻准备、应对和缓解当前和未来的威胁。通过威胁情报平台的赋能，增加全网威胁可见性，结合动态沙箱技术、机器学习技术等提升检测能力，对威胁攻击过程进行分析狩猎，提升对业务网络中威胁与全攻击过程的可见性。

三、金融行业网络安全风险和挑战

近年来，随着大数据、人工智能、区块链等技术的发展，金融业与科技加速融合，新业务、新技术的大量涌现，金融风险、信息技术风险敞口加大。同时，随着金融对外开放力度不断加大，金融信息基础设施直面国内外不同形式的网络风险。金融业一旦发生安全风险，不仅会威胁到用户的利益，也会给金融企业本身带来巨大的损失，破坏整个行业的发展，甚至带来系统性金融风险。金融业网络安全面临的风险和挑战持续升级。

（一）金融科技创新对网络安全提出高要求

近年来，金融科技呈现蓬勃发展的态势，中国金融业的数字化发展

尤其迅猛。与此同时，在新一轮科技革命和产业变革的大背景下，金融数字化转型对网络安全提出更高要求。

1.敏捷开发快速迭代对运维安全带来持续挑战

在持续提升网上银行、手机银行、直销银行、网上消费/信贷等线上业务能力的同时，机构的业务系统发生了诸多变化。例如，系统开发普遍采用敏捷开发方式，力求产品的快速上线与版本功能的灵活更迭，整体架构逐渐向“胖前置、瘦核心”转变，并更多地采用开放式架构，这些变化导致金融机构在互联网环境下面临更多威胁。金融机构需要关注业务系统在市场快速响应与安全建设保障之间的冲突性，尽量减少因新业务或新功能可能带来的业务安全风险和用户个人隐私泄露。

因此，需严格遵从《中华人民共和国网络安全法》三同步建设的要求，在业务系统的规划设计、系统开发、评估上线及使用运维等所有环节对网络安全展开整体设计、建设与维护。

2.IPv6 推广与 5G 商用等新技术的快速应用带来隐性安全风险

2019 年，5G 商用牌照正式发放、IPv6 网络流量快速增长助力金融发展等，这些新技术带来了新活力，新业务蓬勃发展。5G 技术与 IPv6 的特点决定两者必将产生深度融合，引发智慧金融、远程协作、个人 AI 辅助等新技术、新应用、新业态不断涌现，然而对于给金融行业带来怎样的新威胁和风险，产生怎样的新攻击类型，采用怎样的防御应对手段等亟待研究。

在 5G 网络加快覆盖的大背景下，金融行业关键信息基础设施暴露在互联网上的情况持续增多。由于承载服务、信息的高价值性，预计在

未来三年，针对金融等关键信息基础设施的网络窃密、远程破坏攻击、勒索攻击会持续增加。

3.区块链等新技术的快速应用带来隐性安全风险

区块链、移动互联、云计算和大数据技术的广泛应用已对金融机构的网络安全保障提出了更高的现实要求。金融机构在利用高新技术面向市场提供快速金融产品的同时必须面对技术高速发展带来的网络安全的不定性。

在区块链技术方面，近年来区块链相关系统安全问题频繁暴露，“技术+金融”等新型攻击手段涌现，引起的安全事故损失高达上百亿美元，又由于区块链技术的匿名性和节点全球分布的特征，使用区块链数字资产做资金转移隐蔽性高，难以追溯和识别身份，为犯罪分子利用勒索病毒收取勒索资金等犯罪行为提供了便利。亟需深入研究区块链的安全风险，健全区块链系统级安全防护技术和安全评估手段，建立适应区块链分布式技术机制的安全保障体系。

以云计算为例，大中型金融机构已开始建立私有云，需考虑私有云自身虚拟系统平台的安全性以及在云计算环境中东西向和南北向的安全隔离防护控制建设，并定期开展安全评估与测评；小型机构则大量使用行业云，需考虑云服务商的服务能力和安全防护能力，确保租户安全。

此外，大数据应用在带来可观业务价值的同时，也为不法行为带去了更多便利，集中的数据平台使得攻击者目标更为明确，而数据挖掘分析结果则大大提升了获取信息情报的价值。因此，在大数据应用分析过程中更需重视对数据中心及数据的保护，避免信息丢失、泄露与滥用。

（二）事件型漏洞和零日漏洞威胁持续走高

漏洞包括操作系统、数据库等基础平台的漏洞，网络传输协议和加密技术方面的漏洞，攻击者利用金融机构网络安全建设不完善的弊端，对金融机构业务系统进行的破坏性攻击，通常会导致重要数据丢失、泄露、内部投毒、敲诈勒索等严重后果。

国家信息安全漏洞共享平台 CNNVD 在 2019 新收录通用软硬件漏洞数量同比增长 14.0%，创下历史新高。这些漏洞影响范围从传统互联网到移动互联网，从操作系统、办公自动化系统（OA）等软件到 VPN 设备等网络硬件设备，以及芯片、SIM 卡等底层硬件，广泛影响我国金融行业基础软硬件安全及其上的应用安全。

蠕虫病毒和木马，由于传播速度快、感染性强等特征成为最受金融行业攻击者青睐的攻击手段，通常会产生大范围感染，造成金融行业系统不可用、数据损坏或丢失等现象。

近 5 年来，零日漏洞（从漏洞公布于世后，厂商还没有及时提供修复补丁或更新程序，在这段时间里统称为零日漏洞）收录数量持续走高，年均增长率达 47.5%。2019 年收录的零日漏洞数量继续增长，占总收录漏洞数量的 35.2%，同比增长 6.0%。这些漏洞在披露时尚未发布补丁或相应的应急措施，严重威胁我国金融行业网络空间安全。

（三）网络攻击种类、规模与方式不断增加

近年来，针对金融行业的网络攻击行为大幅增长，给各类企业、用

户以及金融行业造成的损失每年达百亿元之巨，并有继续快速升级的趋势。相关监测报告显示，针对金融机构的网络攻击类型较多且方式灵活多变，以盗取资金、盗取敏感信息为目的，以 SWIFT 攻击、ATM 攻击、信息泄露、恶意软件、网络诈骗、系统故障、勒索软件和 DNS 攻击等为主要攻击手段，金融机构经营发展和商业声誉受到严重影响，承受巨大损失。

1．暴力攻击（强力破解密码，DDoS 攻击）

长久以来，远程入侵计算机系统的工具和技术并没有发生翻天覆地的变化。在大多数情况下，暴力攻击是通过利用密码管理缺陷来入侵系统的最简单实用的方法，因此黑客热衷于对系统管理员密码、资金账户密码等各类密码进行强力破解。DDoS（分布式拒绝服务）对金融行业的威胁由来已久，已成为网络攻击者们勒索金融企业的常用手段。 DDoS 攻击是目前最大的网络安全威胁之一，主要是通过将巨大流量引向目标来达到压垮和瘫痪网站的目的。

2．网络攻击组织化与全球化愈发严重

当前，金融机构已成为国内外敌对势力、黑客组织、不法分子实施网络攻击、电信诈骗和渗透窃密的重点目标。针对银行业金融机构的 APT（高级持续性威胁）攻击、精准式网络攻击日益猖獗。随着移动互联技术的普及应用，网络安全边界日益模糊。开放的网络环境必然带来更高的网络安全风险，金融行业信息系统的复杂程度和技术跨度决定了网络安全保障面临的难度。与此同时，数据大集中和全球一体化系统运行模式对业务连续性提出了更高要求，局部的网络系统故障可能波及全

行网络与关联系统，给网络系统安全运行带来了更大压力。

一些专业化的黑客组织出于非法牟取经济利益的目的，通过实施攻击渗透并植入勒索软件等方式，将单位内网中的重要网络资产和数据进行加密，使其日常业务无法开展，从而勒索大量赎金。从攻击手法来看，勒索软件逐渐呈现出专业性高、针对性强的特点，有向“泛 APT 攻击”发展的趋势。

金融行业主要面临一些成熟的网络犯罪团伙的攻击威胁，如 MageCart、 Cobalt Group 等等，其组织化的成员结构和成熟的攻击工具实现对目标行业的规模化攻击，这与过去的普通黑客攻击是完全不同的。

2020 年 3 月，英国金融科技公司 Finastra 被勒索软件攻击，导致关闭服务器。其网站的声明称，这家金融科技巨头表示已感染了勒索软件。Finastra 表示，在员工检测到他们所谓的“潜在异常活动”后，才发现入侵了其系统。

3. 利用“后门”程序

金融机构大量使用了第三方公司的 IT 设备和软件，这些厂商可能在产品中预留一些具有系统最高控制权限的“后门”程序，从而被攻击者发现和利用。

2019 年 4 月 18 日，网络安全专家发现了俄罗斯网络犯罪集团的活动。据研究人员称，攻击者利用远程访问特洛伊木马攻击美国和世界各地的金融机构。这些黑客倾向于使用像 tRat 和 ServHelper 这样的后门程序。

4．社会工程学手段（诈骗电话、带木马程序的电子邮件、钓鱼网站、勒索软件）

从网络空间安全的角度来看，所谓“社会工程学”主要指的是一类特殊的黑客攻击手段。它的攻击目标是人，是要充分利用人性的弱点、本能反应、好奇心、信任、贪婪等心理特质，对受害者进行诈骗、恐吓等，给客户端安装恶意软件，盗取银行卡、网银密码和支付验证码。

2020 年 3 月 Cofense 钓鱼防御中心（PDC）发现了旨在针对非洲金融服务集团 ABSA 的网络钓鱼活动。网络钓鱼邮件内容为通知用户来自另一家需要授权的银行的待转账信息。用户必须下载并打开 htm 附件才能连接到在线银行门户。打开 htm 文件后，用户将被定向到假冒的 ABSA 在线银行门户网站，该网站与合法的 ABSA 门户网站几乎相同。然后提示用户输入访问帐户号码、密码和用户号码，这些凭据将被发送到攻击者所劫持的域。

（四）数据安全和隐私保护需求与难度加大

金融行业自身业务价值高，涉及资金、个人信息、征信信息等重要数据，金融行业的数据正在成为不法分子紧盯的重点对象。另外，金融行业自身业务对信息化依赖程度的加深，业务的多样化、服务的开放化等使得应用越来越复杂，这也将导致出现技术脆弱性或者业务安全隐患的几率增大，防御阵地过大。金融行业中个人金融信息由于其数据价值高，信息非法交易问题尤其严峻，近些年金融用户隐私泄露事件及侵犯公民个人信息违法犯罪频频发生，暴露出第三方内控不严、信息系统出

现安全漏洞，信息泄漏传输链条长，难追溯等问题。

根据中国互联网协会发布的《网民权益保护调查报告》，78.2%的网民的个人身份信息、63.4%的网民的网络金融交易记录曾被泄露过。近年来，每年发生的金融隐私泄露事件大约以35%的速度在增长，有公开报道或记录2016年1093起，2017年1511起，2018年1967起，2019年2300余起。报告认为，与欧美国家相比，我国隐私保护体系建设起步相对较晚，加之近年来各类新技术在金融行业迅速广泛应用，金融隐私保护问题日益凸显。银行数据、保险数据和其他平台金融数据泄露频发，网贷业务及大数据风控乱象屡禁不止，金融用户隐私保护形势严峻，难度较大。

一是法律法规层面，缺乏完整的体系。相比国际，我国数据安全及隐私保护相关的立法起步较晚，今年《中华人民共和国数据安全法(草案)》和《中华人民共和国个人信息保护法（草案）》刚刚开始公开征求意见，行业监管机构也陆续发布了个人金融信息相关的安全标准，但总体来看，我国尚未形成严谨的金融隐私保护法律体系，针对各机构和平台主要以行政处罚为主。

二是技术层面，5G+ABCDE等新技术的快速应用给金融隐私保护带来了更多的风险挑战。截至2019年12月，针对App违法违规收集使用个人信息行为的举报渠道——微信公众号"App个人信息举报"共收到网民举报信息12125条，涉及2300余款App；其中移动金融App是违规收集使用个人信息的重灾区；云计算和大数据为大数据分析提供便利的同时，也汇集了大量高价值数据，成为黑客攻击的重点目标。

三是业务场景复杂导致的数据保护难题。由于业务的不断快速发展，金融机构的业务系统多达几百上千个，应用场景繁多，其中承载着大量的客户基础信息、业务交易数据、业务产品数据、企业经营数据、机构数据、认证信息、生物特征信息、企业员工信息等大量业务和系统数据。这些数据由于业务需要在各个系统间不停的流转，其面临的风险也随之变化。数据安全管理需要根据业务需要实现动态的体系化的安全防护能力，才能保证机构数据安全管理策略的良好落地。

2019 年 6 月，房地产和产权保险巨头 First American 在其网站上暴露了 8.85 亿份敏感客户财务记录，包括社会安全号码、驾照、银行账号和对账单、抵押贷款和税务文件，以及电汇收据，这些记录可以追溯到 2003 年，而且任何人都可以进行访问。随后，First American 关闭了数据所在的网站。根据公司声明，此次事件可能是一个应用程序存在的设计缺陷，导致了他人能未经授权就访问客户数据。这次泄露主要涉及密码和用户名的组合，First American 泄露的数据将给潜在的受害者带来灾难性的长期影响。

（五）金融行业风险冲击的传导性愈演愈烈

随着金融科技的高速发展，网络安全事件的“蝴蝶效应”也屡见不鲜。一是金融业务的高度关联性使银行、证券、保险、第三方支付等金融服务机构网络互联互通。在带来便捷、高效的同时，也为跨系统、跨机构、跨区域的网络攻击和风险传染，以及利用薄弱点为“跳板”进行风险渗透提供了路径。此类风险发生后，可能产生诸多连锁反应而对金

融业形成冲击。分行业的微观管理无法解决跨机构、跨系统的风险传染，存在“盲区”。

二是不同类型金融机构的网络安全发展水平不均衡，分业监管的力度也参差不齐，在数据安全等监管方面可能存在“洼地”。存在混业经营的金融机构仅从成本利润考虑，从而在行业、区域间等选择性开展业务，以规避监管。这种行为极大地增加了金融业整体数据安全风险，有损金融消费者权益，分业的微观监管难于覆盖，存在“漏洞”。

（六）金融行业信息科技外包风险形势严峻

金融机构业务的迅速发展和市场竞争的日益激烈，大大提高了对科技支持能力的要求。金融机构特别是中小型机构普遍存在信息科技人力资源匮乏、技术能力欠缺等问题，人员数量和质量均不能满足业务发展对科技的要求。因此，大部分金融机构大量采用信息科技外包的方式，作为自身科技力量的补充。银行业金融机构得益于信息科技外包服务，科技水平显著提高，凭借着外包供应商优质的软硬件环境最大化了金融机构的竞争优势，在得到极大优势的同时必然要面临相应的风险。近年来，金融行业陆续出现的外包风险事件给金融机构和监管机构敲响了警钟。主要包括以下几类风险：

1.跨境外包风险。金融机构过多的依赖某一国家服务供应商的信息产品、系统等相关外包服务，在合同期间该国家的经济、政治、社会事件产生了国家级别的风险，从而导致该合作供应商不能正常经营，致使对金融机构经营造成重大影响。

2.高集中度风险。金融机构当前在基础设施、核心系统、数据中心外包等领域，非驻场外包呈现集中化的趋势，外包服务商集中托管多家银行业金融机构，一旦发生风险，影响面大、传导速度快，容易演化发展为系统性、全局性风险。

3.信息窃取风险。信息科技外包服务供应商信息安全总体管理水平参差不齐，其内部控制有出现漏洞或管理风险的可能，致使金融机构遭受黑客攻击、银行客户信息和资产被窃取等事件的发生，导致包含客户信息在内的金融机构非公开数据被服务商、黑客等非法获得。

4.业务中断及服务水平下降风险。金融机构由于更换服务供应商、供应商更新或停止某项服务等原因造成无法持续享有外包服务，导致金融机构某项业务中断或服务水平下降风险。

针对日益严峻的信息科技外包风险形势和层出不穷的外包风险事件，监管机构高度重视，监管要求逐步加强。早期，银监会印发《银行业金融机构外包风险管理指引》，全面规范银行业金融机构外包行为。结合外包最新发展态势和信息科技外包风险特点，又印发了《银行业金融机构信息科技外包风险监管指引》，从加强机构对外包风险控制角度，明确了金融机构建立信息科技外包战略和风险管理体系的要求，指导银行业金融机构加强外包风险评估、供应商尽职调查、合同和外包过程监控，并着重强调对重要外包服务的管理。针对非驻场集中式外包存在的突出风险和监管空白问题，银监会不断强化监督要求，建立起有针对性的风险管控机制，对强化非驻场集中式外包风险管理、防范集中度风险发挥了积极作用。[1]

[1] 金融科技时代的信息科技外包风险管理 李燕 - 金融科技 时代 - 2019-08-02

四、金融行业网络安全发展趋势

（一）数据安全将是未来建设与投入重点

国家高度重视数据安全保护。2020 年 4 月，中共中央、国务院近日发布《关于构建更加完善的要素市场化配置体制机制的意见》，首次明确将数据作为生产要素，并要求加快培育数据要素市场，加强数据资源整合和安全保护。2020 年 7 月，《中华人民共和国数据安全法(草案)》公布，提出“确立数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；坚持安全与发展并重，规定支持促进数据安全与发展的措施；建立保障政务数据安全和推动政务数据开放的制度措施”，将成为数据要素国家战略重要的法制基础。10 月，十三届全国人大常委会第二十二次会议审议了《中华人民共和国个人信息保护法（草案）》，个人信息保护即将有专门性统一立法，在个人信息保护方面形成更加完备的制度，提供更加有力的法制保障。

近年来，金融机构也不断提升对数据安全与隐私保护的重要性的认识水平。《金融数据安全 数据安全分级指南》、《个人金融信息保护技术规范》等标准规范密集出台，对数据安全和隐私保护赋予了更加明确的定义，对安全保护能力提出了更高要求。调研数据显示，14.49%的金融机构将“数据安全”作为未来三年重点投入的第一选择，“数据安全”已经成为未来建设投入首要重点。

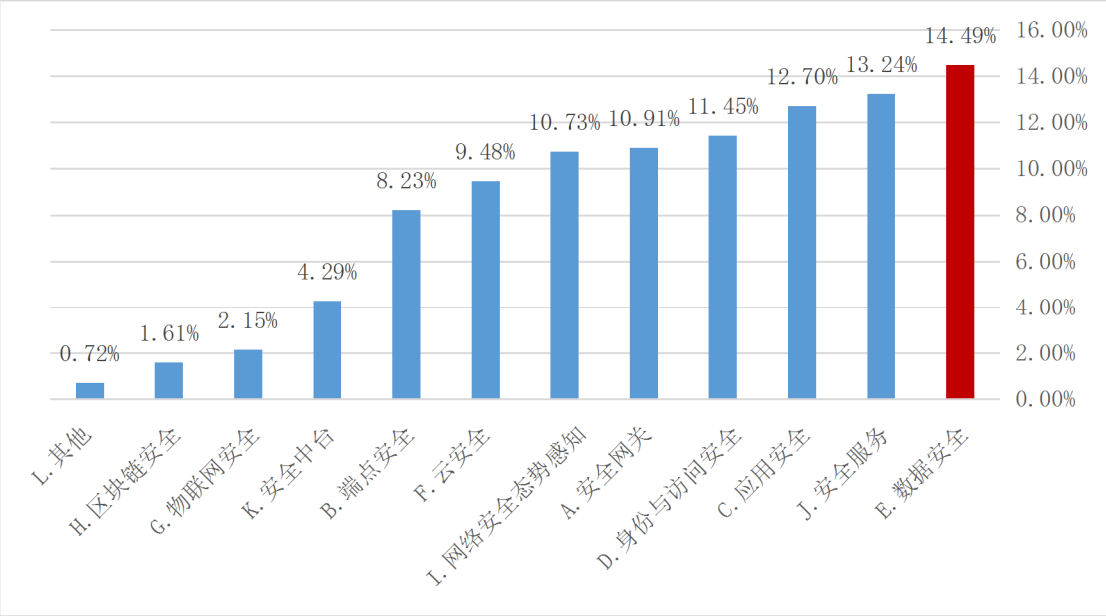


图 9：主要金融机构未来三年网络安全主要投入领域

（二）网络安全运营化和服务化需求日盛

相对于金融行业信息化建设投入，网络安全投入小、力度弱、且较为分散，这点在中小型金融机构表现的更为明显。伴随数字经济、金融科技的快速发展，“搭积木”式的产品堆砌已经无法满足动态、全面和长期的网络安全防御需求，专业的网络安全服务成为金融机构的必然选择。

一方面，安全服务可有效解决金融机构人手不足、专家不足等问题，提升安全建设的有效性；另一方面，安全服务结合平台与云化服务能力，正在进一步演化为安全运营的创新服务模式，将发挥长期、巨大价值。安全运营通过积累日常行业、业务相关威胁情报、安全事件等数据，并结合行业、机构数据赋能，逐步形成密切契合机构需求的“安全数据运营”能力，不断提升安全检测、防御和处置效率，令数据作为生

产要素的价值在网络安全领域得以充分展现。

调研数据显示，金融行业对于网络安全服务需求不断增加。2019年，安全服务已成为主要金融机构排名第二的投入重点；在未来相当长的时间内，金融机构在网络安全服务方向的投入将保持持续增加，成为仅次于数据安全的重点投入领域。

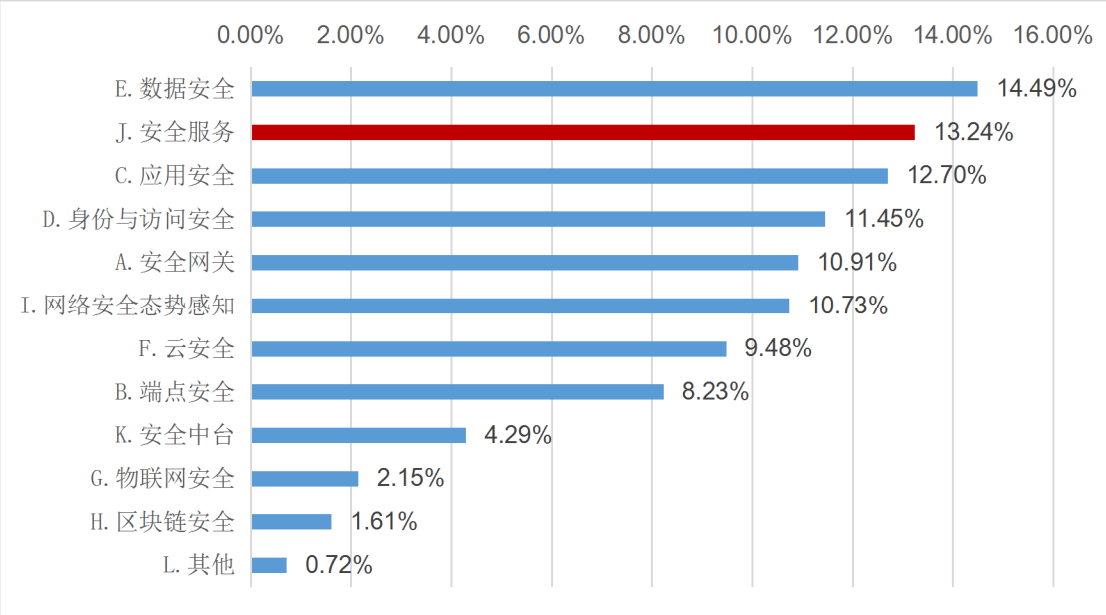


图 10：主要金融机构未来三年网络安全主要投入领域

（三）零信任网络安全架构应用备受关注

当前，金融科技、数字经济正在加速推动，无处不在的网络扩大了攻击者的攻击面。机构关键数字资产暴露于各种攻击火力之下，已成为用户在向数字化转型过程中的主要挑战之一。过去数年，被披露的数起重大数据泄露案件均是由“身份冒用”引发，因此，基于重要场景（例如：线上金融交易、机构间的数据交换等）进行二次认证等安全机制约束需求开始得到重视，这就是“零信任”的雏形。“零信任”（ZT，Zero

Trust）最早由市场研究机构 Forrester 在 2010 年提出，后经 Gartner 和 Forrester 对其概念、应用场景、迁移方式进行了完善和补充。

零信任的核心思想可以概括为：网络边界内外的任何访问主体（人/设备/应用），在未经过验证前都不予信任，需要基于持续的验证和授权建立动态访问信任，其本质是以身份为中心进行访问控制。零信任可以降低数据泄露、数据丢失事件的发生频率，拒绝未授权的访问，在数据安全方面价值巨大。因此，应建立以身份为基础，持续进行信任评估和动态访问控制，将各种安全产品、安全模块整合起来、紧密耦合的安全体系，进而构建安全的 ICT 基础设施，保障应用和数据的安全性。

目前金融机构已在多个业务场景进行了零信任架构改造的积极探索，尤其集中在传统安全方案普遍认为难以管控的场景：开发测试互联网出口的安全管控；内网跨区高危端口的访问控制；零信任安全远程办公等。

此外，新技术、新应用也在不断融入金融业务、管理与服务中，以人工智能、区块链等为代表的新金融技术，结合 5G 云网一体化的新型基础设施，将深度改变传统金融业务的产品结构和运营模式，重构金融行业在数字化产业的支撑作用。

（四）金融信息技术应用创新在加速推动

信息技术应用创新（以下简称“信创”）的发展是目前的一项国家战略，也是当今形势下国家经济发展的新动能。发展信创是为了解决本质安全的问题。信创发展已经成为经济数字化转型、提升产业链发展的

关键。

当前金融行业网络安全面临的一些突出问题，如核心设备和技术的发展水平相对落后、技术趋同性可能产生“同频共振”风险，高关联性的关键金融基础设施遭受网络攻击受损后可能影响金融体系正常运行等等，需要建立相应的指标体系进行风险监测、评估并加以处置、防范，以防止发生金融业网络安全系统性风险。

为应对这一挑战，我国正逐步建立自己的 IT 底层架构和标准，形成自有开放生态。当前，我国核心关键技术突飞猛进，从芯片到基础软件等都已具备一定的规模化推广能力。伴随着信创工作的开展，为金融行业从技术标准、系统架构等整体视角体系化的重新梳理和解决网络安全问题提供了契机。金融信息化系统采用分布式架构，同时更好的将可信计算、国密算法等自有技术融入新安全架构，从而从整体上制定更完备的安全解决方案。未来 5 年将是信创快速推进的重要阶段。

（五）5G+金融为网络安全带来全新挑战

5G 作为新一代通信技术，将实现物与物、人与物、人与人的全面高速连接，并将通过与人工智能、大数据、云计算等技术叠加，释放出具有乘数效应的技术支撑潜力，为金融行业带来新的服务手段、交互方式，催生金融服务新业态，助推对客服务、运营模式、金融生态发生巨大变革。金融机构陆续推出 5G 与应用场景结合的创新试点，2019 年 5 月，中国银行宣布在北京推出首家 5G 网点；6 月，工商银行公告在苏州试验该行首家新型智慧网点；建行首批 3 家 5G 科技无人银行也于 7

月中旬在北京正式营业。试点项目探索以 5G 技术增进人机交互，结合人工智能、生物识别等先进技术，提高网点工作效率和客户体验。同时，金融机构也在尝试规划围绕精准营销、业务创新、风险控制等各方面，结合 5G 网络和技术特点进行创新突破。

5G 技术赋能金融行业的同时，也带来了隐性的网络安全风险，按照网络安全建设“三同步”原则，5G 安全应在金融领域 5G 创新应用中进行同步规划、同步实施。5G 网络是基于虚拟化、云化的网络架构，针对引入的边缘计算、网络切片等新技术，传统防护手段难以满足需求；5G 时代在物联网等领域终端种类和数量增加，易被攻击利用，对网络运行安全造成威胁；5G 新应用场景从移动互联网拓展至物联网，会产生新的基于场景应用的网络威胁。因此，需要面向新时代，持续开展 5G 环境下的安全特性预研，包括 MEC 安全、切片安全等，为 5G 时代开放银行、智慧资管等场景下的安全风险控制提供安全技术支撑，制定新的 5G 安全解决方案，保障 5G 在金融机构的场景化落地和推广。

五、金融行业网络安全能力提升策略与建议

（一）加强网络安全宣贯提升风险防范意识

金融行业一旦遭到网络攻击，会给国家、企业、民众造成重大的经济损失。近几年，中央网信办、公安部等监管部门日益提高执法监管力度，加大对违规采集和使用个人信息、泄露或售卖用户数据、侵害用户隐私权益的企业查处力度。但重要数据和个人信息泄露或滥用问题仍较

为严重，存在个人信息滥用及不合理披露的情况，对公民个人生活造成影响。金融机构应全面加强内部人员的网络安全意识教育和培训，以避免由于人员安全意识不足导致的安全事件发生。

一要细化管理措施，进一步落实网络安全责任。金融机构要全面落实金融行业等级保护 2.0 等监管机构相关管理要求，健全组织机制，明确相关部门责任，建立明晰的员工操作规范和流程，使安全管理工作落到实处。

二要提高风险意识，加强条线协作。金融网络安全形势日趋严峻，金融机构应严格落实客户信息保护和网络安全风险排查等相关工作要求，对信息科技风险进行全面梳理与排查，通过排查自检在进一步消弭风险隐患的同时提升员工信息安全意识与合规意识。

三要强化全员宣教，共筑网络安全防线。金融机构要广泛开展线上线下网络安全宣传教育活动，向机构全员普及《网络安全法》及相关知识，通过负面案例、网络安全知识手册、知识竞赛等多种形式不断增强全员网络安全意识，共筑网络安全防线。

（二）贯彻落实网络安全三化六防体系建设

受国际环境和金融科技快速发展的影响，金融行业网络安全防护呈现诸多新特点。随着网络攻击日益高级化、复杂化和持续化，金融机构原来主要基于边界防御、漏洞检测、规则匹配等静态安全防护手段的传统安全防御体系，在面对当前日益复杂的网络安全威胁时已经显得“力不从心”。在金融数字化转型的大背景下，大数据、云计算、人工智能、

区块链、物联网等新兴技术已经开始快速应用，在提升用户体验、创造价值的同时，给网络安全带来了新的挑战。

网络安全等级保护制度 2.0 标准和规范提出了我国关键信息基础设施安全保障的原则、方法与手段，是我国未来十年关键信息基础设施安全保障最基础、最核心、最重要的权威标准规范。从总体来看，等保 2.0 是一部完整的以主动防御为目标、以技术保障为基础、管理运营为核心、以监测预警为支撑的网络安全防御体系框架性指导标准与规划建设指南，从理念上更加注重全方位主动防御、动态防御、整体防控和精准防护。

金融行业网络安全防御体系建设在设计顶层框架时，需要转变思路，以“实战化、体系化、常态化”为新理念，以“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”为新举措，在全面落实等保 2.0 的基础上，对关键信息基础设施进行重点防护。

在体系化中，要做到威胁情报、侦查打击、落实等保，通过全局整体设计，建立保护生态、建立完善信息预警通报机制及应急机制和队伍建设等立体化全方面建设；在实战化和常态化中，建立全天候的态势感知与安全运行，金融机构应依据等级保护标准开展安全建设并进行等级测评，发现问题和风险隐患及时整改。

同时，金融机构要以风险管理为指导，针对攻击方法、攻击途径的变化，实现网络安全状态持续监测、及时反馈、动态调整防御策略、技术和手段，由传统的静态防御向动态防御转型；要基于可信计算技术构建可信安全管理中心支持下的安全防护框架，结合威胁情报、态势感知，

及时发现和处置未知威胁，落实主动防护措施，由“被动监控”向“主动防御”转型；要实行分区域管理，区域间进行安全隔离和认证，事前监测、事中遏制及阻断、事后跟踪及恢复，实现攻击的层层阻击，全流程纵深防御；要基于资产的自动化管理，协同威胁情报，监测未知威胁、异常行为等，实现对核心资产的精准防护，提高内生安全、主动免疫能力，做到精准防护；要以保护关键业务链为目标，进行整体安全设计，建立协同联动、高效统一的安全防护体系，实现整体防控；要建立与国家监管部门、保护工作部门、其他利益相关方的协调配合、联动共防机制，建设“打防管控”一体化网络安全综合防控体系，提升国家整体应对网络威胁攻击能力，实行联防联控。

（三）创新思路统筹推进网络安全顶层规划

随着网络互联程度的不断提高，安全木桶效应越发明显。从总体调研数据可以看出，受限于整体网络安全投入不足，大部分金融机构网络安全体系建设基本围绕合规要求开展，缺乏整体的规划和设计。这一点在中小金融机构中表现得更为突出。

2019 年 8 月，中国人民银行发布的《金融科技（FinTech）发展规划（2019—2021 年）》中明确指出，要加强金融网络安全风险管控，完善网络安全技术体系建设，健全金融网络安全应急管理体系，加强网络安全顶层设计、协作创新能力，以及威胁情报、态势感知、监测预警、应急响应、攻防对抗、追踪溯源和联合处置能力等。为避免木桶的短板效应，形成可持续提升的网络安全防护能力，加强网络安全防护体系顶

层设计已经成为金融机构下一阶段的首要任务。

网络安全和信息化是一体之两翼、驱动之双轮。金融行业作为关键信息基础设施，是网络安全重点保护领域，要以身份安全为基础，以云网安全和端点安全为重心，以安全中台为枢纽，以威胁情报为支撑，构建‘立体、联动、可视’的安全机制和‘实战化、智能化、云化’的技术战略，赋能 5G 时代的数字化安全运营能力，助力金融机构数字化转型和拓展业务发展边界。金融机构可以新的合规能力建设框架为基础，结合自身安全战略对机构的网络安全体系进行统筹优化和设计，分步骤建设，从而形成网络安全防护体系的“四梁八柱”，不断持续优化网络安全防护体系整体能力。

同时为应对大规模的网络攻击，应面向行业建立网络安全漏洞、网络病毒、网络攻击活动等威胁情报共享与威胁治理技术平台和工作机制，形成国家、省（市、区）、行业有机联合的纵深防御体系，以提供有价值的威胁情报和畅通的治理通道。通过行业态势感知和安全运营中心的建设，实现金融行业各单位和各数据中心监控预警信息的互联互通，加强信息共享能力、优化协同监控流程、完善协同运营机制，全面提升安全运营和响应处置能力。

（四）逐步建设全要素的数据安全治理体系

新冠疫情的爆发促使工作方式从线下转到线上，与此同时，随着 5G 应用的逐步深入和 AI 技术的广泛使用，新基建的投资建设步伐加大，金融行业数字化转型不断提速。在此过程中，在不同渠道和界面对

客户或合作商户开放或共享部分业务数据不可避免，如交易的密码、认证的身份信息等，甚至认证所需要的证书、生物特征信息等。在灵活进行业务管理的同时，需要根据业务进行细分，根据敏感程度、业务类别，采取针对性的安全管理策略，收敛安全威胁的敞口。从金融行业目前的数据安全防护实践情况来看，数据脱敏、加密、审计、防泄漏等防护技术已经得到了一定程度的应用，但整体效果尚未完全达到预期。

数据最大的特性是流动，并且在不断的流动中创造新的价值，这也是数字经济得以大力发展的基础。数据安全防护应从单一的场景防护转变为体系化建设的思路来开展，逐步完成从顶层规划到管理和技术体系的细化落地，才能达成数据安全保护的终极目标。因此以管理体系和组织建设为先导，构建数据安全治理的管理体系；以数据安全风险管控为出发点，设计数据安全治理技术体系，逐步健全数据安全技术防护手段，构建场景化的安全能力联动模式，实现“数据资产可视、数据使用可控、数据操作可审、数据泄漏可溯、数据开放可信”，最终形成可持续提升的数据安全治理体系能力已经成为业内建设的必然选择。

（五）建立可感知可视可管的安全运营能力

近年来，金融安全威胁与风险持续升级。首先，攻击者对金融科技系统的渗透从网络服务、金融业务逐步深入到核心业务与数据、用户财产和隐私。网络安全威胁、数据安全威胁、业务安全威胁与日俱增，金融网络安全形势日趋严峻。其次是政策法规推动下的合规要求的增强，基于安全运营的安全管理中心是等保 2.0“一个中心，三重防御”的新

增核心要求。第三是常态化对抗下的安全能力不足的现实问题。各金融机构虽购置了大量的安全设备，但专业人员不足、专业技能不足导致防护效果未达预期。近几年的红蓝对抗和实战化演练，充分暴露出各金融机构核心安全能力不足，人员、设备、流程、机制无法有机结合等问题。因此，简单的安全工具堆砌不会形成真正的安全防护能力，要从根本上解决问题，就需要以业务活动场景为基础，构建动态的、可持续发展的“可感知”、“可视”、“可管”的一体化智慧安全运营生态体系，智慧协同内外部各方资源，共同抵御内外部威胁。

为适应新的变化和发展，金融行业需要完成从被动响应到主动运营的转变。全面加强金融行业网络安全核心技术攻关，建立健全本行业网络空间安全一体化防护能力。强化威胁预测，开展网络安全未知威胁检测技术研究，利用机器学习、人工智能等新技术，提升海量流量中高级威胁线索发现水平，实现网络攻击事件的快速发现与场景还原。强化威胁感知，增强态势感知预测技术，基于大数据分析与宏观微观态势研判，实现对重大网络攻击事件的提前预警，及时做好防范与有效应对。强化威胁防御，构建网络攻击实时防御技术，实现监测体系与处置体系的实时联动，确保受到网络攻击时能第一时间高效处置。

结合基础平台和多元化的安全分析能力建设，对于发现的安全事件，以流程化、结构化的安全运营体系，驱动安全事件处置落实，形成“常态化”的安全运营闭环，提升整体的安全运营能力。

首先，建议中小金融机构以 XDR 为基础快速构建覆盖全网的威胁检测与响应能力，XDR 解决方案包括了 EDR（终端检测及响应）、NDR（网

络检测及响应）以及 MDR（智能管理平台的检测及响应）。每个维度的检测响应都不是单独存在的，而是紧密相连的。囊括了多种技术、产品及服务，如 APT 检测，沙箱技术，安全网关，终端产品，安管平台，多回路威胁情报，态势感知，立体建模，渗透服务，应急服务等等。XDR 一方面通过快速集成多种安全产品可以提高安全运营的效率和价值，增强检测的准确度，缩短响应时间；另一方面可以大大降低安全运营的复杂度。统一的 XDR 解决方案，不需要对每个产品进行单独的对接调整，可以在一个产品界面进行安全事件的展示、响应和处置，将大大降低安全运营的对接成本和使用成本；

其次，对于大型金融机构来说，应大力推进安全中台建设。以安全中台为枢纽，以威胁情报为支撑，实时采集分析全网安全态势数据，同时联动行业云端威胁情报库，分析潜在的安全风险及未来发展趋势，形成网络安全攻防指挥中心，实现对内外部威胁进行高效的检测、分析、响应和处置；

最后，组建配套的安全运营和应急响应团队，根据需要配置一二三线的安全分析及处置人员，对安全人员和场景进行编排，制定自动化剧本，形成常态化安全运营任务及流程，主动有序展开各项安全活动；同时协同外部专业的安全服务资源，以保证安全运营体系的健康良好运行。

（六）注重网络安全人才培养和社会化协作

网络安全竞争实际上是高层次人才的竞争，但目前我国网络安全高层次人才十分稀缺。据 IDC 预测， 2023 年我国网络安全人才缺口将会

超过 200 万。新时期金融行业要进一步提高认识，认真贯彻落实网络强国战略思想，培养更多优秀网络安全人才，有效保障金融安全。

首先，根据网络安全工作需要，金融机构应从岗位人员配备和人才培养等方面加强网络安全队伍建设，建立网络安全队伍建设长效机制，完善薪酬体系等激励措施，多渠道引进人才、留住人才；

其次，以针对性提高金融行业网络安全防御能力和水平为导向，制定金融机构与安全企业的网络安全人才培养计划，开展社会化协作，积极鼓励安全管理人员参加网络安全职业培训、认证和实战演练等活动，不断提升从业人员职业素养和能力；

最后，积极发挥“产学研用”多元化合作，形成政府机构、学校、金融机构等多方紧密协作和共同参与的人才培养机制。优化人才培养模式和教学方法，创新和完善师资队伍建设机制，制定政策鼓励专项实践活动，举办各类创新模式的网络安全竞赛等，满足金融机构不同层次的网络安全人才需求。

附录：金融行业网络安全典型案例

（一）某银行全感知动态响应安全防控体系建设实践

1、项目概述

某银行全感知动态响应安全防控体系建设项目，从网络出口、内网安全、主动预防、动态响应四个方面，构建了总分联动的全感知动态响应安全防护体系。实现了从重点防护到全面防护、从边界防御到内网防

御、从被动整改到主动预防、从静态应急预案到动态响应的转变。提升了全行整体安全防护能力，为银行业务的快速发展提供了安全保障。

2、背景和意义

从网络安全的整体形势来看，商业银行面临的威胁日益严峻。从国际形势来看，由于利益冲突或政治目的，网络暗战无时不刻正在发生，商业银行面临来自个人，组织，甚至国家层面的网络攻击。另外，网络黑产早已形成完整的产业链，可以说外在威胁层出不穷。从国内的行业动态来看，监管要求愈发严格，包括《网络安全法》的颁布，等级保护2.0的实施，也包括金融行业内部日益严格的安全检查和审计。此外，类似公安部重大安全专项实战演习这样大规模、全行业的攻防演练也给商业银行带来了前所未有的考验。

国有商业银行，多数已建立纵深防御体系，但在实战考验下，仍暴露出一些弱点。一方面，传统防护体系重视互联网出口防御，但是对第三方外联出口和邮件出口的防御比较弱，容易被作为突破口。另一方面，传统纵深防御采用多层边界防护，重点防御纵向攻击，但是往往对突破边界之后的横向移动攻击难以觉察。另外，往往还存在发现攻击告警之后应急响应相对滞后的问题。

针对这些问题，某银行开展了总分行全感知动态响应安全防控体系项目建设，主要目标是建立总分行全感知动态响应安全防护体系，包括建立各网络出口的全面防御体系、内网安全和主机防御体系、安全漏洞的运营管理体系以及动态的安全事件应急响应体系。主要意义包括：

(一)全感知动态响应安全防控体系提高了银行信息安全技术和管理水平，有效保证银行业务安全稳定运行，防范金融风险，加快银行信息化建设和数字化转型的步伐。本项目的研究和建设成果对整个银行业的网络安全防护都具有良好的普适性，为银行同业的安全防护体系建设提供了参考和借鉴。

(二)应用前景方面，商业银行不断产生新的业务形态，同时也面对着不断深化的外在安全威胁，需要更灵活自主的防护体系和更扎实的技术积累。信息安全漏洞运营体系和安全策略动态响应体系确保了银行应对信息安全漏洞威胁的主动性和灵活性，加上深度包检测、大数据日志处理等技术能力积累，使得银行可备战未来更严峻的安全态势。

（三）未来，银行还将进一步推进安全防护体系的迭代完善，使其具备更强力且更高效的安全防护能力。以业务安全为核心，最终实现网络安全风险可监测、可测量、可控制，为全行的业务运行提供有力的保障和支撑。

3、项目主要建设内容

全感知动态响应安全防控体系分为网络出口、内网安全、主动预防、动态响应四个方面，建立了全方位、全周期的安全防护。在网络出口方面，着重加强了对第三方外联出口的安全防护，和对进出双向的邮件安全建设。在内网安全方面，增强了对内网流量的监控，并建立了广泛的服务器安全防线。在主动预防方面，基于自研漏洞运营管理系统，持续开展漏洞扫描、渗透测试等工作，主动发现并修复漏洞。在动态响应方

面，基于双核评价体系建立起高效的自动处置机制。

(一)网络出口方面，建立外联出口和邮件出口的全面防御：构建了覆盖总行及36家分行的外联出口安全监测体系，增强入侵防护能力及高级持续性威胁对抗能力；基于邮件防泄露、邮件反垃圾系统建立了的进、出双向邮件防护体系，降低信息泄露风险，抵御恶意软件和钓鱼攻击。

(二)内网安全方面，建立了主机防御和横向流量监控体系：对重要服务器部署安全代理，并对系统日志和安全代理日志集中监控，建立全行服务器安全防线；建立了对总分行间以及总行重要网络区域间横向流量的监控，提升对内网横向移动攻击的防御能力。

（三）主动预防方面，以自研系统为基础构建了信息安全漏洞运营体系，贯穿漏洞扫描，渗透测试、安全众测、威胁情报工作，全面提升主动预防能力。

（四）动态响应方面，建立安全威胁自动阻断和安全事件人工研判的双路处置流程，并集中管理全行的安全监控、处置策略，可根据外部安全态势快速调整监控和处置策略。

通过项目的建设，某银行提升了全行外联区安全防护能力，提升了对恶意邮件防护和敏感信息保护能力,提升了全行服务器安全防护能力,提升了安全漏洞的主动发现能力和处置效率，提升了策略零活调整和事件快速处置的能力，以及提升了自动化响应处置水平。安全防护能力的提升，相应地减少了银行因信息泄露带来的经济损失，减小了因漏洞攻击造成的资金和声誉损失，保障了银行业务安全稳定运行，保护了银行

和客户的经济利益。

4、项目效果

项目成果在某银行总、分行范围全面推广，包括网络出口、内网安全、主动预防、动态响应四个大的方面。

在网络出口方面，着重加强了对第三方外联出口的安全防护。自项目建设约一年时间内，纳管了 36 分行的上百台第三方外联区防火墙，IPS 设备上线千余条安全防护策略，两地数据中心外联区的防 APT 及流量回溯系统检测到攻击告警十余万次，IPS 设备共阻断数十万次攻击事件。

在网络出口方面，也着重加强了进出双向的邮件安全防护建设。外网邮件防护中，反垃圾邮件网关月均拦截邮件数十万封，约占邮件总量的 15%左右，高级邮件检测工具月均识别高阶威胁邮件千余封。内网邮件防泄露系统通过拦截、审批、审计等技术手段防护敏感信息泄露行为，已拦截和审计邮件上百万封，极大地降低了因通过邮件泄露行内信息造成的经济损失和社会影响。

在内网安全方面，增强了对内网流量的监控，并建立了广泛的服务器安全防线。在“网安 2019”行动过程中,发现和阻断多次服务器非法外联、危险命令执行、账户密码的异常建立和修改，对账户异常的行为管控及时有效,对于来自外部穿透外围防护的非法访问、SQL 注入、Struts 2、IP 仿冒等多种手段的攻击也进行了高效的防护。

在主动预防方面，基于自研漏洞运营管理系统，持续开展漏洞扫描、

渗透测试等工作，主动发现并修复漏洞。项目建设至今，共计发布漏洞排查处置任务单上千个，覆盖行内众多应用系统和信息系统资产，基础软硬件漏洞数量明显下降，所建立的我行信息系统漏洞库收录上百个漏洞，切实提高了我行应对漏洞威胁的能力与风险管理水平。

在动态响应方面，基于双核评价体系建立起高效的自动处置机制。项目建设至今，除 WAF、IPS 自动拦截之外，自动封禁危险 IP 数量二十余万个，日常运维自动处置率接近 100%，有效提高了对恶意攻击的拦截能力。

综上，本项目将纵深防御扩展到全方位、全周期防御，全面增强了应用系统的安全防护能力；部署了同业领先的服务器安全防线，大幅提高了内网防护能力；自研的双核安全评价系统，实现了安全事件快速自动化编排及处置，且安全策略可针对外部安全态势做到灵活调整，快速切换，有效提升了告警的准确性、处置的高效性、策略的灵活性。项目成果提升了银行整体安全防护能力，有效保障银行业务的稳定运行。

（二）某保险集团业务安全平台建设实践

1、项目概述

随着金融行业整体的互联网化、移动化、数字化和智能化的演进，推动了银行保险业创新业务、尤其是线上金融业务的迅猛发展。特别是经过这次疫情的洗礼，整个保险行业更加的拥抱互联网，线上业务的趋势和规模得到持续扩大。保险集团顺应保险行业的发展趋势，推动“三

个在线”，即客户在线、销售在线、管理在线的创新发展，通过规划和建设线上多渠道，为客户和员工提供灵活的、垂直的业务入口。

业务安全平台建设项目，依托集团“三个在线”的创新发展方向，旨在通过建设一整套业务安全平台，以健全保险集团的整体安全防护架构，构建从设备识别、人机识别到业务反欺诈的综合防护能力，有效防止机器攻击及业务欺诈的侵害，为集团和子公司的各大业务板块提供业务安全解决方案。

业务安全风险存在于线上业务的全流程多环节中，唯有全生命周期做好安全防护才能取得良好的效果。本项目优先接入注册登录、营销场景，通过规则与模型设计，形成适合现状的各类业务安全的解决方案。最终目标是提高集团和子公司的业务安全技术和服务能力，降低欺诈损失，提升客户体验，促进业务更好更快的发展。

2、项目背景及意义

近年来，随着信息安全环境的演变，信息安全本身逐渐由“以系统为核心的安全”转为“以业务为核心的安全”，利用业务规则漏洞或者防范死角来进行欺诈的行为获利不断增加，且成为主要的获利方式。攻击破解工具不断提升，黑产形成产业链，面对此现状，业务安全防控的策略也应该是多维度，组合拳。避免因防控能力限制新业务大规模展开。

2.1 服务于集团业务发展战略

保险集团依托保险、资管、医养三大业务板块，打造长寿、健康、富足三个闭环，构建大健康产业生态体系，其总体业务开展、业务运营

和客户服务都会通过“线上+线下”联动的方式展开。特别是在当前的后疫情时代，保险集团大力发展“三个在线”创新业务，坚持为客户提供更好的线上服务和体验，极大地扩展了保险发展空间的边界和功能。但这也是使得安全问题大量暴露出来，线上线下安全风险交织被放大，在推动创新业务发展的同时，需要未雨绸缪、提早防控，针对集团业务安全进行研究、防控和预警。

2.2 沉淀集团业务安全场景

业务安全是为业务服务的，业务目标的实现才是根本。在对当前线上主要服务渠道和门户进行需求调研和风险梳理后，对主要业务安全场景进行归类，沉淀了账号安全、营销活动、交易、支付等业务场景的解决方案。系统还支持与模型、数据的对接，通过离线分析实现策略的自我演进，更好的适应业务安全的变化速度，持续更新迭代反欺诈的防控手段。

2.3 业务安全防控的示范实践

通过集团业务安全平台建设项目的实施，探索并实践出一整套适配保险行业多业态环境下的业务安全防控方法，包括：实时决策引擎/设备指纹/智能无感验证，面向实时反欺诈核心场景，提供全流程多环节、全链路按需组合的快速风控决策构建以及智能辅助的自主演进，最大程度的保护了业务安全，同时也为保险行业的业务安全防控提供建设思路和实践经验。

3、项目主要建设内容

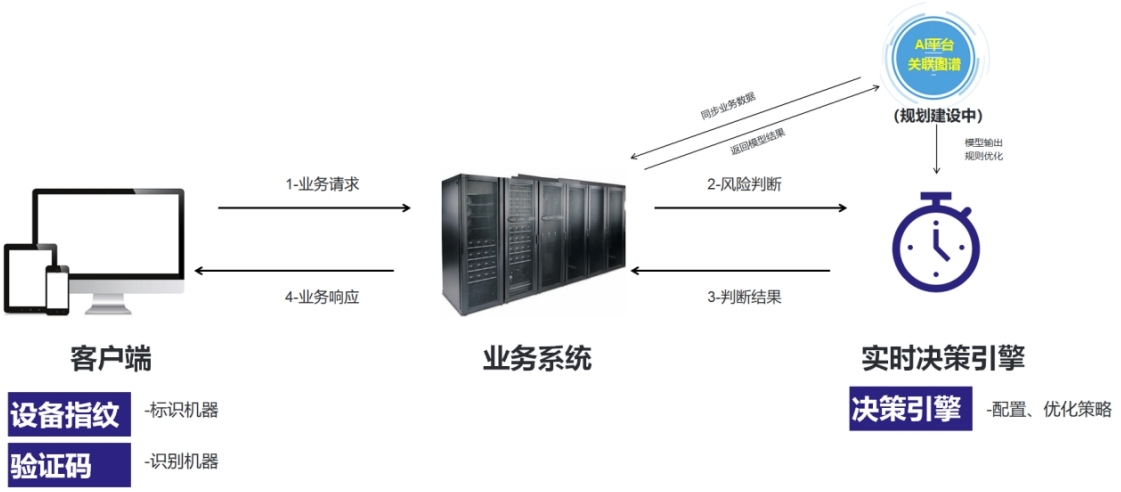
业务安全平台，基于前沿的业务风控、实时反欺诈、终端安全和大数据智能技术，实时感知、发现、分析保险线上业务中出现的安全威胁与业务风险，秒级决策拦截威胁与风险，打造基于实践需求的安全大脑及全场景、智能化、可信赖的业务安全体系，降低资产损失，提升业务效率。

3.1 平台建设思路

随着公司业务增大和变化，灰黑产的攻击模式也在变化。同时，在遭受防御和抵抗后，灰黑产的攻击方法和模式也是不断变化的。因此，在被保护的业务系统现有架构和应用不变的前提下，业务安全系统需要具备灵活应对风险变化的能力，通过简单的配置调整或新增策略，便能有效阻挡变化的风险和威胁。

基于业务数据的重要性、业务负载的递增性、业务风险的变化性以及风控方案的落地性考虑，平台总体建设思路如图 1 所示：

在客户端（Web、Android、iOS、H5、小程序）集成设备指纹和验证码，在客户业务端集成数据转发及风控结果处置 SDK，决策引擎、建模平台独立部署，风控评估过程中涉及到的指标、规则、策略、模型均在平台进行配置和计算，实时返回风控判断结果。



图（一） 业务安全平台总体建设思路视图

3.2 系统总体架构

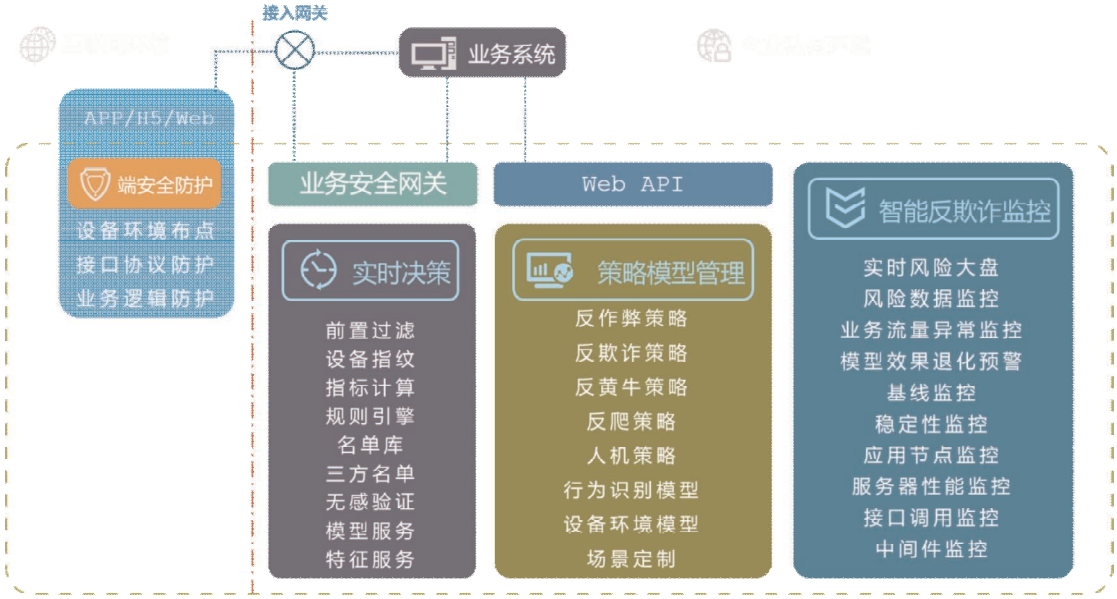
业务安全平台可以有效阻挡线上化中的设备反欺诈、账号反欺诈、数据反欺诈、交易反欺诈、信贷反欺诈、营销反欺诈等业务安全问题。本项目建设实施实时决策引擎、设备指纹、智能无感验证三个模块，计划在后续项目中展开智能模型平台、知识图谱的建设。该平台的系统架构图如图 2：

图（二） 业务安全平台系统架构图

3.3 系统核心功能

1）实时决策引擎

实时决策引擎是构建业务安全体系的核心，快速建设大数据智能风控体系，实现线上服务的业务反欺诈的实时风控管理。实时决策引擎的功能模块图 3 所示：



图（三）实时决策引擎功能模块

2）设备指纹

黑灰产拥有专业的设备牧场，通过使用模拟器、刷机改机等手段，批量、反复地利用终端设备作案。对互联网场景下的金融、电商等行业，进行恶意爬取、虚假注册、账号盗用、薅羊毛、推广作弊等其他恶意行为。设备指纹技术，为每一台设备生成一个全球唯一的设备指纹 ID，不可被篡改，保持追踪设备，设备指纹 ID 不会随模拟器、虚拟机、刷机改机而改变。同时设备环境风险检测可辅助识别终端设备作弊行为，为集团的业务安全提供实时风险决策提供设备信息。

3）智能无感验证

智能无感验证，是基于用户行为特征与设备指纹信息，进行智能人机识别的行为验证方式。根据用户的风险程度，采取不同难度的验证方式，安全用户无感知通过，避免恶意攻击带来的业务损失，留存真实用户。系统从技术上实现全平台兼容，支持多平台接入，包括Web、Android、IOS、小程序等。系统毫秒级响应，极速采集丰富基础数据，匹配多维度风险特征。通过多重验证，集成专家策略与人机模型，核心模块交互验证，对环境信息和用户行为特征进行综合判断。业务安全管理人员通过可视后台，丰富的可视化图表，防御拦截数据尽收眼底，实时查看当日验证详情与近期验证趋势。通过智能场景模式可智能识别并应用于任何需要验证的应用场景，实现全场景覆盖。

后续计划建设的智能模型分析平台利用建模方式实现基于数据分析的风控模型训练与部署，能够将训练成熟的模型与实时决策平台无缝对接，实现闭环应用。知识图谱可实现基础数据的标准化、统一化，提高信息遍历速度的同时能够自动挖掘、更新知识信息，其可在对接大数据平台基础上实现知识图谱网络的搭建，并在后续增量数据补进的同时实现图谱自动扩展，同时可与实时决策引擎、智能模型分析平台实现技术对接，实现图谱知识的高效挖掘与利用。

4、项目效果

业务安全平台有效降低了成本，提高了效率，原本需要大量人工审核工作进行客户风险识别，现在利用实时决策引擎可以实现秒级响应，

业务人员审核效率大大提高，在降低人工成本的同时，显著缩减了业务环节内的时间成本，提高了集团的市场竞争力。同时，沉淀下四个成果：

4.1 构建通用业务安全技术能力

本项目构建保险集团通用的业务安全技术能力，包括精准的设备指纹技术、人机识别技术、毫秒级实时计算能力的智能决策引擎，对保险客户获客、交易、设备、人员等数据进行清洗和分析，深度挖掘数据之间的关联关系，为防范保险业务线上化欺诈场景的扩展打下基础。

4.2 业务安全服务能力

紧密贴合业务场景，做好业务风险控制，有效降低虚假注册、营销欺诈、薅羊毛、推广作弊、盗用冒用等业务安全风险，提高风控效率和水平。方案部署后，风险欺诈的定位与决策效率得到有效的提升。

4.3 降本增效

传统的客户风险识别需要大量人工面审，难以满足客户高效率、便捷性的需求，通过接入业务安全基础平台，在降低人工成本的同时，也缩减业务环节内的时间成本。

4.4 提升客户体验

通过业务安全防控体系的建设，建立各业务场景的服务能力，在面对黑产团伙的恶意行为的同时，兼顾业务适应性、客户集成灵活性、实时大并发流量支撑、用户体验，达到利益制衡。系统快速响应客户需求，减少客户等待时间，优化客户体验。方案部署后，正常用户访问占比得到了提高，用户体验满意度大幅度上升。

4.5 为保险行业在业务安全平台建设进行了有益探索

该项目运用科技赋能实现保险金融数字化服务化落地及共享，不仅在业务安全树立了标杆。更帮助业务部门挖掘用户准确信息，完善用户画像以收集统一化标准的用户数据，突破渠道壁垒，实现资源与服务共享，产生更高的商业价值。

（三）某银行网络安全态势平台建设实践

1、项目概述

某银行通过在终端构建一体化安全防护体系、管道安全的 APT 攻击防护、威胁内容阻拦及垃圾邮件拦截的一体化安全防护体系、数据安全脱敏和统一管控一体化安全防护体系，形成多层安全防护体系，建设成全网网络安全态势感知平台。XX 行安全防护体系和安全态势感知平台已于 2017 年 12 月全行上线，分别在生产网、办公网和互联网区域部署相应的安全产品和提供相应服务，进一步完善、增强行内整体信息安全防护和监控，实现威胁态势可视化，并提供全网威胁态势预警。

2、项目背景和意义

随着网络安全威胁和安全风险在不断增加，网络病毒、邮件病毒、Dos/DDos 攻击、APT 威胁等构成的威胁和损失越来越大，网络攻击行为向着分布化、规模化、复杂化等趋势发展，仅仅依靠防火墙、入侵检测、防病毒、访问控制等单一的网络安全防护技术，已不能满足网络安全的需求，迫切需要新的技术，及时发现网络中的异常事件，实时掌握网络安全状况，将之前很多时候亡羊补牢的事中、事后处理，转向事前自动

评估预测，降低网络安全风险，提高网络安全防护能力。

目前国家对网络信息安全越来越重视，《中华人民共和国网络安全法》已获人大常委会表决通过，已于 2017 年 6 月 1 日开始实行，及 2019 年 5 月 13 日网络安全等级保护制度 2.0 发布，国家网络安全法、等级保护制度的出台和实行将极大地推动和加强网络信息安全的建设和发展。

终端病毒威胁、管道安全的 APT 攻击、威胁内容传播及垃圾邮件困扰和数据防泄密等一直以来都是银行业所需面临的重要问题。仅仅依靠以往防火墙、入侵检测、防病毒、访问控制等单一的网络安全防护技术，已不能满足网络安全的需求。

在以往传统模式中，普遍以各个安全产品单一管控。无法对网络数据等信息进行自动分析处理与深度挖掘、网络的安全状态进行分析评价并感知网络中的异常事件与整体安全态势，缺乏从整体上动态反映网络安全状况和防御，并对网络安全的发展趋势进行预测和预警。

3、项目主要建设内容

本项目通过在终端构建一体化安全防护体系，包括恶意文件防护、勒索防护、web 信誉、机器学习及可疑文件提交等技术构建终端安全防护体系。管道安全防护体系，利用边界安全防护设备，实现对 APT 定向威胁防护、C&C 违规外联防护、零日攻击及漏洞防护、提供精细化内容安全策略，利用邮件安全网关防护设备，实现对病毒邮件、垃圾邮件、钓鱼邮件和高级威胁邮件防护，利用内网深度威胁发现设备，实现对内

网横向移动攻击、内网外联监控防护构建全方位态势感知平台。

系统框架策划上，吸收 PPDR5 安全模型 ，同时也借鉴 Gartner 自适应安全防御理念，在获取、理解、评估和预测的基础上，增加了行动环节，通过在网络、中间件、主机等设备上部署探针和日志收集程序，获取基础设施、安全设施、网络和应用系统等相关的日志信息、通过分析处理并展示整体态势和威胁态势。

态势感知平台融入了大数据技术、人工智能技术、 云安全技术、自动化防御技术、威胁情报等等。通过第三方接口输出给行业共享与系统对接，让整个态势感知平台服务于更多的行业和应用场景。适用性更为广泛，服务领域也逐渐增多，同时也促进了安全行业的发展和进步。

4、项目效果

安全防护体系及态势感知平台建设包括终端、管道、数据、资产等，安全防护体系及态势感知平台已于 2017 年 12 月全行上线，分别在生产网、办公网和互联网区域部署相应的安全产品和服务，进一步完善、增强行内整体信息安全防护和监控，实现威胁态势可视化，并提供全网威胁态势预警。态势感知平台融入了大数据技术、人工智能技术、 云安全技术、自动化防御技术、威胁情报等。使整个态势感知平台适用性更为广泛，服务领域也逐渐增多，同时也促进了安全行业的发展和进步。

编辑委员会

刘洞宾、胡婷、庞勇、廖双晓、吴强 、张东、牛玲芳、郭晗 、于忠臣、张勇 、李晓波、肖菲菲

致　谢

感谢参与金融行业网络安全调研活动的金融机构从业人员！

感谢对本白皮书提供建议的金融机构！主要参与的金融机构如下（排名不分先后）：

中国光大银行、中国农业银行、北京农商银行、广东省农村信用社联合社、中国人民财产保险股份有限公司、中国银行保险信息技术管理有限公司、泰康保险集团股份有限公司、阳光保险集团股份有限公司、中国人寿财产保险股份有限公司、大家保险集团有限责任公司、天安人寿保险股份有限公司、安信证券股份有限公司

关于中国银保传媒

中国银保传媒是我国第一家整体实行股份制的新闻传媒企业，注册资本 1 亿元，曾被评为中央出版转型示范单位、“第二批”数字出版转型示范单位。公司旗下的《中国银行保险报》是中国银保监会主管的唯一工作日报，连续两届被原国家新闻出版广电总局评为“中国百强报刊”，连续荣获“中国十大行业报”。

《中国银行保险报》作为中国银保监会主管的唯一工作日报，坚持“政治家办报”方针，坚持积极宣传国家经济金融大政方针，正确解读金融监管法律法规，紧密围绕服务实体经济、防控金融风险、深化金融改革三大任务，服务中国银保监会中心工作需要，不断丰富传播媒介，加快推进媒体深度融合，打造全媒体传播矩阵，现已初步形成一报(《中国保险报》)、一网(中国保险报网)、两微(官方微信公众号、官方微博)、两端(中国保险家客户端、手机报客户端)六维一体的传播格局，同时开通今日头条号、百家号、抖音等主流新媒体传播平台官方账号，传播渠道多维立体化，覆盖用户超百万。

关于亚信安全

亚信安全是既“懂网”又“懂云”的网络安全公司。承继亚信 20 余年精准敏锐的电信服务市场洞察和数字化服务经验，以及 10 余年云安全的核心技术积淀，亚信安全持续引航网络安全的发展和创新。

亚信安全以安全数字世界为愿景，以护航产业互联网为使命，在云安全、身份安全、终端安全、安全管理、数据安全、高级威胁治理和威胁情报等 7 大领域拥有核心技术。亚信安全是国家身份认证体系和身份安全的核心技术力量，守护亿级用户的每一次网络接入和认证。依托平台级网络安全解决方案与服务，亚信安全不断助推 5G 时代的网安技术创新。亚信安全从“实战”出发，以身份为基础、以攻防为视角、以联动为策略、以运维为关键，加强全方位防御能力，为金融行业建设符合等保要求的、自适应的安全体系。亚信安全在金融安全领域的技术实力十分突出，拥有庞大的用户基础，涵盖了国内主要银行、证券，及保险客户。其中，亚信安全长期服务于中国人民银行、中国工商银行、中国农业银行、中国建设银行、中国银行、交通银行、中信银行、招商银行、光大银行、民生银行、浦发银行、广发银行、兴业银行、华夏银行、中国人民保险、中国人寿、平安保险、太平洋保险、中信证券、海通证券等行业头部用户，并为其提供着智能化、联动化、一体化的解决方案与配套服务，深得用户信赖。

亚信安全 护航产业互联网

商务咨询热线 800-820-8876

技术售后热线 800-820-8839