2024年中国金融行业网络安全研究报告

2024年5月

数说安全 CYBERSECURITY REVIEWS

中国信息安全 China Information Security

目录

版权声明

免责声明

前言

网络安全一直是国家安全的核心组成部分，特别是在金融行业，金融机构拥有大量的敏感数据，包括个人信息、交易记录、财务报告等，这些数据的安全直接关系到消费者的利益和金融市场的稳定，因此金融行业在网络安全建设领域一直较为领先。然而，随着金融行业数字化改革的深化，网络安全挑战不断增加，新技术的应用、数据流转加速、金融交易/服务的拓展、信息系统迭代频率提升、第三方合作的深入、业务全球化的扩张、以及合规政策趋紧等因素，都对金融行业的网络安全提出了更高的要求。

在这样的背景下，“数说安全”与《中国信息安全》杂志一起编写了这份《2024 年中国金融行业网络安全研究报告》，通过对金融机构访谈、安全厂商调研、监管处罚内容解读和 CSRadar 商业分析平台[1]数据分析，希望了解中国金融行业面临的安全挑战、监管部门的要求与期望、网络安全市场发展情况、网络安全建设现状、安全厂商产品、服务和解决方案能力，并洞察金融行业网络安全发展趋势，帮助金融机构提高网络安全威胁的防范能力，促进安全厂商提升产品、服务和解决方案能力。

[1] CSRadar 商业分析平台是针对中国网络安全市场的数据可视化分析平台。平台数据源于市场公开招投标的信息，通过深度数据处理，形成质量可靠、分类清晰的中国网络安全市场公开招投标信息数据库。通过对这些数据的深度透视，CSRadar 商业分析平台为行业提供全新的视角，以洞察中国网络安全市场的现状和发展趋势。

一、概述

（一）主要发现

需求侧视角：

金融行业的整体网络安全支出在 2023 年出现下降，高预算低执行是主要原因。

金融行业的安全体系建设对实战应对能力的要求不断增强，但合规性依然是其核心驱动力。

安全体系建设的阶段发生转变，建设重心由采购和建设，向安全运营转移，更关注安全能力的深度应用和内部整合。

以国有商业银行、股份制银行和个别头部保险公司为代表的头部金融机构，安全合规建设相对完善，目前安全建设的重点根据自身情况各有侧重，其中数据安全和安全运营是关注最多的两个领域。

小规模的各类金融机构，合规仍是主要建设驱动力，常态化的实网攻防演习和攻防演练也促进了他们对场景化安全能力的需求，如外部攻击面管理、零信任访问接入等。

从安全体系建设的方式来看，大规模金融机构的投入大、能力强，更倾向于自研或联合开发。小规模金融机构的安全投入有限、能力较弱，会更灵活地通过购买产品及服务的方式补足安全能力短板。

漏洞管理、数据的安全使用、社工攻击、软件供应链攻击、业务逻辑安全风险是金融机构面临的五大主要安全难题。

数据安全管理平台是当下建设的重点，目的是实现对数据泄漏的发现、防护、溯源和定责。

头部金融机构对 AI 赋能安全的关注度较高，告警的分析收敛是目前最大的需求场景。

量子安全技术在密码领域正进行课题探索和小规模试点，区块链技术的应用逐渐增多。

主要金融机构目前的信创完成度在 30%～50%之间，大部分金融机构计划在 2027 年完成信息化系统的信创改造工作。

监管侧视角：

监管机构的网络安全处罚力度不断加大，银行仍是监管机构最关注的领域，90%的罚单处罚对象是银行。

监管机构对个人信息保护的要求不断增强，相关罚单数量占网络安全罚单总数的 70%。此外，最近三年农村金融机构收到的罚单数量明显增多。

金融行业网络安全政策法规的更新和完善速度加快，政策制定者持续关注技术进步的最新动态，

以确保网络安全监督管理能够跟上技术发展的步伐。

引入“行动计划/提升计划”型网络安全政策，通过对未来几年的规划指导和激励措施，引导并激发金融机构更主动地进行网络安全建设。

供给侧视角：

参与金融行业的网络安全厂商约 260 家。虽然综合型厂商是主要的参与者，但在细分领域能提供扎实的技术、产品和服务的中小型厂商同样具备较强的竞争优势。

安全厂商逐渐通过将“服务”和“产品”打包销售的方式交付客户，以具体应用场景为切入点，帮助客户解决安全问题。

市场视角：

2023 年金融行业网络安全甲方支出 91.9 亿元，约占总体网络安全甲方支出市场的 9%，同比下滑 12%，增速五年来首度转负。

随着金融行业数字化转型的深入，开放、敏捷、智能成为各大金融机构的建设目标，因此 API 安全、数据安全、攻击面管理、开发安全等领域的采购项目增速提高。

2023 年，金融行业网络安全采购项目预算价格中位数和中标价格中位数的偏差额达到 16%，约 12 万元，为近四年的最大差额。

（二）建议

网络安全公司负责人：

金融行业因独特的业务特性和严格的监管要求，形成具有明显行业特征的网络安全需求。然而，这些特殊需求往往未能得到完全满足，通常需要在标准产品的基础上进行额外定制，增加了金融机构的安全建设难度。安全厂商需重视“研发流程左移”，在深刻理解金融行业需求的基础上，将这些需求切实转化为有效的产品和解决方案，提升对金融行业的安全交付能力和效率，增强自身的市场竞争力，减少“闭门造车”式的安全研发。

金融行业部署的终端安全防护产品种类多，经常因为设备性能占用过高、不同品牌产品之间冲突引发问题，且难以定责，安全厂商应尽量整合终端安全能力，将终端设备上安全产品的数量减少到 2-3 种，并开发整体的终端安全解决方案，降低对设备性能的消耗，避免产品间的冲突。

金融行业网络安全建设早、脚步快，传统的基于合规性的大规模静态被动防御体系建设已经达到顶峰。未来，金融行业将加强动态的主动防御体系建设，并维持较高的投入水平。同时，这些动态防护措施将越来越多地采用服务化模式进行交付，因此，安全厂商应重视新型订阅制和服务化交付产品

或解决方案的模式。

金融行业对网络安全的高标准和对安全产品性能的严要求，使得该行业客户对产品的选择具有独到的见解和深刻的洞察，并愿意为好用的产品买单。目前，市面上很多安全产品（如数据安全、终端安全、供应链安全、零信任等）距离金融客户的要求仍有一定差距，安全厂商应保持开放的态度，学习全球范围内的优秀安全产品及技术，优化安全产品防护能力，提升企业在金融行业的竞争力。

金融机构网络安全负责人：

在过去的网络安全大规模建设阶段，通常会忽视对安全产品内在能力的有效使用。当下，应当深化对现有安全产品的使用，同时，与安全厂商共同开发并实现现有安全产品的定制化功能，以此来提升安全防护效果，实现资源的最优配置，并在一定程度上实现降本增效的目标。

在数据安全领域，大规模金融机构需采取更具前瞻性、系统性和全面性的策略来统筹规划其安全措施。规模较小的金融机构，重点应放在尽快明确数据安全责任人，建立可行的数据安全制度流程，加强数据安全防护措施，并确保这些措施的全面覆盖和有效执行。

在进行网络安全产品或服务采购时，应增加对技术因素的考量权重，避免过多地被短期直接成本影响采购结果。“低价者得”的采购策略虽然在减少初期投入方面有表面优势，但可能会牺牲安全产品和服务的质量，并最终导致整体安全成本的显著增加。

二、金融行业科技发展趋势与安全挑战

（一）数字化改革深化，新技术的应用带来新威胁

随着大数据、云计算、人工智能、区块链等前沿技术的飞速发展，金融科技领域经历了巨大的革新，为传统金融服务赋予了创新动力，极大提升了服务的效率，同时显著降低了成本。根据这些技术的应用程度和融合深度，金融科技的进化历程大致可以分为四个阶段：金融科技 1.0——金融信息化、金融科技 2.0——互联网金融、金融科技 3.0——金融与科技深度融合以及金融科技 4.0——金融数字化。

金融科技 1.0 时代：金融行业开始采用信息技术手段来实现业务流程的电子化、自动化和无纸化操作，有效提高了工作效率并削减成本。例如，POS 和 ATM 设备的普及极大地缩减了银行的日常开支。这一阶段，尽管金融科技在一定程度上优化了工作流程，但其对于既有金融模式的影响还相对有限。

金融科技 2.0 时代：即互联网金融阶段时，银行业受到移动互联网的巨大冲击和影响，金融机构开始创建线上平台，实现财产、交易、支付、资金等各环节的无缝连接。网络技术的渗透促进了一场

针对传统金融渠道的重大改造，促使了像 P2P 借贷、在线众筹、网络基金销售等全新财务模式的出现。

金融科技发展至 3.0 阶段：意味着金融服务与科技实现了深入的结合。在该阶段，传统金融搭配新科技（如大数据、云计算、区块链、人工智能等），重构了信息采集方式、风险定价模式、投资决策流程和信用中介的角色，带来效率的进一步提高，并催生了新型金融行为，包括大数据信用评分、智能投资咨询等。同时，相关政策也为金融科技的进步提供了有力的支持。

金融科技 4.0 时代：数字金融时代的来临被我们目睹。这一时期，金融服务模式呈现场景化和标准化的特征，并加速数字化转型过程。这其中包括基于场景的客户获取、标准化的风险控制和数字化的业务运作等方面。同时，开始形成一个能自我迭代、优化和学习的综合性生态系统，以及开放、灵活且可持续的金融科技生态系统。

在科技与金融深度整合的过程中，数字化彻底转变了金融业务的运作逻辑，网络安全风险成为了跟业务风险同等重要的议题。尽管技术创新极大地丰富了金融服务的便捷性和多样性，但也带来了新的安全挑战。因此，在推进技术创新的同时，我们需要保持警惕，构建动态且全面的网络安全防御系统，确保业务的安全可靠，避免因安全防护不足而酿成严重后果。

（二）数据流转加速，数据安全问题迫在眉睫

随着金融数字化转型不断深入，数据的开放性和流转性明显增强，大幅地提高了资源配置效率和金融产品风险定价的有效性，精准地捕捉了个人和企业潜在需求，拓宽了金融行业服务边界，因此，数字化成为推动金融行业转型升级的新引擎。

数据的快速流动和开放虽然带来了便利，但同时也加剧了数据安全问题的复杂性和严峻性。例如，非结构化数据分类分级的覆盖度和准确度还较低，导致这部分数据很难执行细粒度的保护标准；数据泄露防护 DLP 产品的工作方式依赖数据形态，其防护效果与业务效率之间的矛盾一直存在，泄露防护的技术和策略仍需不断提升；数据在多方共享时，无法有效保证及约束第三方的使用范围、用途及保护职责等。

数据泄露、滥用、窃取、篡改等安全事件的发生频率和严重程度不断提升，而金融数据通常包含大量的敏感信息，如个人和企业的身份信息、财务信息等，一旦泄露，可能会造成严重的经济损失，甚至影响金融市场的稳定。

金融数据保护的重要性不言而喻，但安全事件却频频发生。2023 年上半年，厦门银行因违反个人金融信息保护规定等 23 项违法行为，被中国人民银行福州中心支行处以警告，并没收违法所得 767.17 元并处罚款 764.6 万元；同年 2 月，厦门市公安局网安支队成功打掉一个集黑客攻击、数据清洗、买卖信息、提供资金、数据使用等为一体的全链条网络犯罪团伙，破获某公司被侵犯公民个人

信息案。这些事件不仅表现出我国执法部门在打击网络犯罪方面的决心和能力，也再次提醒我们网络安全形势的严峻性和加强金融数据保护的紧迫性。

金融数字化时代下，数据安全的紧迫性愈发显著，单点防护能力的提升已无法有效解决数据安全问题，需要金融机构以前瞻性的视角，不断完善更新数据安全体系的设计，提高员工数据安全意识，加强各种安全技术协同能力，并关注如区块链、人工智能等新技术的应用，才能更好地实现数据安全防护，发挥数据的价值，推动金融行业的持续发展。

（三）业务互联性加深，供应链安全风险不断扩大

随着金融行业数字化转型的不断推进，业务互联性逐渐加深，金融机构不得不依赖日益复杂的软件供应链来支持其核心业务。这一发展趋势在为金融领域带来巨大的便利性和效率提升的同时，也伴随着软件供应链安全风险的不断扩大，成为了业界的焦点和挑战。

从攻击角度来看，软件供应链安全的技术风险主要来自两个方面：第三方软件安全缺陷和开源软件漏洞。首先，第三方软件安全缺陷指的是在金融机构应用第三方开发和维护的软件中可能存在的漏洞、后门和恶意代码等，这些缺陷可能由于开发团队的疏忽而未被及时修复，或由于某种意图有意为之，从而成为潜在的安全威胁。其次，开源软件漏洞是指金融机构在其软件供应链中使用的开源组件中可能存在的漏洞，这些漏洞可能会被黑客利用，对金融机构的业务造成严重影响。这些组件包括基础设施、代码库、依存关系、构建工具、数据、模型等，每一个环节都可能成为潜在的攻击目标。随着软件供应链的组件数量和复杂性不断增加，金融机构需要面对更多的安全挑战。这种复杂性增加了金融机构在软件供应链安全建设中的难度，需要更多的资源和技术来保障安全性。

此外，软件供应链安全还涉及到供应商断供、数据泄漏以及法律合规等层面的挑战。供应商断供可能会导致金融机构在关键时刻失去软件支持，对业务持续性造成严重影响。数据泄漏可能会泄露源代码及客户敏感信息，损害金融机构的声誉。而法律合规方面的挑战涉及到金融机构在引用开源软件、专利和知识产权时需要遵守的法律要求，违反这些规定可能导致法律诉讼和罚款。

为了应对这些复杂的挑战，金融机构需要采取综合性的措施，包括：安全左移、多样化供应链、安全审查、漏洞管理、知识产权保护、合规管理和开源软件管理等。其中，安全左移是一种重要的策略，它要求在软件开发的早期阶段就考虑安全性，以减少后期修复的成本。多样化供应链是指金融机构应该多渠道采购软件组件，降低对单一供应商的依赖，从而减少断供风险。安全审查和漏洞管理是保障软件供应链安全的关键步骤，通过定期审查和修复漏洞来提高系统的稳定性和安全性。知识产权保护和合规管理则是确保金融机构在软件开发和使用过程中遵守法规和合规要求的重要措施。开源软件管理是帮助金融机构持续监控和更新其使用的开源组件，以及时修复可能存在的漏洞。

综上所述，金融机构在数字化转型的道路上必须认真对待软件供应链安全，采取一系列综合性措

施，以确保业务的连续性、数据的安全性和知识产权的保护。只有这样，才能在竞争激烈的金融市场中保持竞争力，并为客户提供安全可靠的金融服务。

（四）系统规模扩大，迭代频率提升，开发安全的重要性愈发凸显

随着金融科技的飞速发展，金融行业的系统规模不断扩大，迭代频率也在持续提升。这一变化背后，是金融业务需求的不断增长和对服务质量的更高要求。但与此同时，开发安全的问题也日益凸显，成为了行业发展的一大挑战。

从系统规模的角度看，随着金融业务的多元化和复杂化，金融系统的架构也在不断演变。从单体应用到分布式，再到云原生，每一次技术革新都带来了系统规模的急剧扩张。这意味着，系统的复杂性和潜在的安全风险也在成倍增加。在这样的背景下，传统的安全防护手段已经难以应对，金融行业亟需一种更加高效、灵活的安全策略。而随着系统迭代频率提升以及监管机构政策规划及意见的推出，敏捷开发体系以其快速响应、持续交付的特点，正在逐步受到金融行业的青睐。但与此同时，敏捷开发也带来了安全上的新挑战。在传统的开发模式下，安全测试往往是开发周期的最后一个环节，而在敏捷开发中，安全测试需要被前置，与开发、测试等环节并行进行。这就要求金融行业必须建立一种全新的安全开发流程，将安全真正融入到开发的每一个环节中。

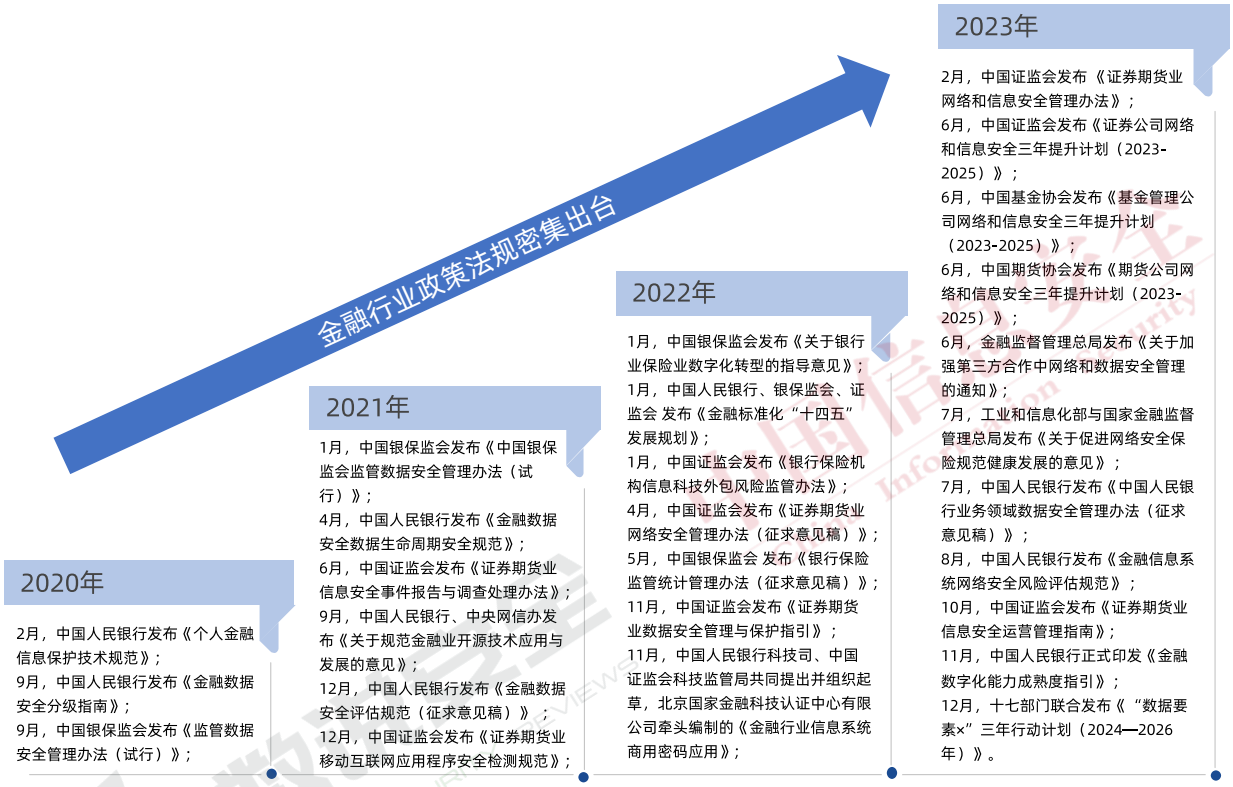
DevSecOps 正是应对这一挑战的有效手段，它强调在开发、测试、部署、运维的整个生命周期中，都要持续地进行安全检测与防护。通过自动化工具和流程，DevSecOps 可以在不降低开发效率的前提下，显著提高系统的安全性。

尽管已经取得了显著进展，但金融行业在开发安全领域仍遭遇多重挑战。首要挑战便是人才短缺。DevSecOps 要求人才具备开发、安全和运维的综合能力，然而，目前市场上这种复合型人才相当稀缺。其次，技术更新换代的速度令人目不暇接。金融科技日新月异，新的安全漏洞和攻击手段不断浮现，金融行业必须保持敏锐的洞察力，紧跟安全技术前沿，及时更新自身的安全防御策略。最后，合规性也是金融行业必须面对的重要问题。作为一个受到严格监管的行业，金融行业在确保符合法规要求的同时，还需保持开发的高效性和安全性，这无疑是一个复杂而艰巨的任务。面对这些挑战，金融行业需要采取更加积极有效的措施，以维护其业务的稳健运行。

综上所述，为了应对这些挑战，金融行业需要积极采纳 DevSecOps 等先进的安全开发理念和方法，培养更多的复合型人才，持续跟踪最新的安全技术，并在满足监管要求的前提下，不断提高开发的安全性和效率。只有这样方能在激烈的市场竞争中立于不败之地，为广大用户提供更加安全、便捷、高效的金融服务。

（五）法律法规不断完善，合规挑战逐渐增加

金融行业因其处理巨额资金流转和敏感个人信息，历来是网络安全法规的重点关注领域。随着中国网络安全法规体系的日益成熟，监管机构在“十四五”期间密集出台了一系列行业法规，为金融机构的网络安全合规提供了更明确的法律依据。这些密集发布的政策不仅明确了金融机构在网络安全方面的责任和标准，也显著加剧了合规挑战。



资料来源：数说安全根据公开资料整理

图 1：2020—2023 年金融行业网络安全政策法规

首先，合规成本显著增加，金融机构需要投入更多资源来满足新法规的要求，涵盖技术更新、系统改进和员工培训等多个方面，将导致合规成本大幅上升。其次，监管政策对金融机构的技术安全要求也在提高，强调金融数据和个人信息隐私的保护，要求金融机构采取更严格的数据加密和访问控制措施。此外，监管机构还要求金融机构加强抵御网络攻击的能力，包括强化内部风险控制体系和定期开展网络安全演练。同时，金融机构还需根据政策规定，建立完整的网络安全事件报告和应急响应机制。最大的挑战在于，金融机构需要在确保网络安全的同时，兼顾业务发展。这种日益严峻的合规环境不仅考验金融机构的合规能力，还迫使它们在网络安全保护与业务发展之间寻求创新和协调。

（六）日益复杂的访问，要求更严格的身份和访问管理措施

随着金融服务向便捷化和多元化的快速发展，访问的主体、场景和行为的都发生了明显的变化。具体来说，访问主体不再局限于内部员工和开发运维团队，而是扩展到了第三方合作伙伴、应用程序以及各种机器设备；访问场景由最初的开发运维和数据访问，延伸至远程办公、三方接入、多云接入和物联网等。这些变化导致访问行为本身也变得更加多样化和复杂化。

传统身份和访问管理系统已不能满足当下的安全需求。由于角色和权限更新较快导致权限管理难以及时更新，访问控制策略比较简单且覆盖度不够全面，不同产品之间不兼容导致访问控制措施难以有效协同等问题日益凸显。越权及违规访问的防护难度增加，信息泄露和网络安全事件频发，这就要求金融机构建立更严格的身份识别和访问控制体系。

零信任的理念虽然为身份和访问管理提供了指导和借鉴，但在实际应用时仍面临着诸多挑战。首先，应用层的技术改造存在较高难度，特别是对于遗留系统的升级和替换；其次，随着安全策略的持续更新，需要对现有的工作流程和业务系统进行相应的适配和调整，以确保与零信任模型的一致性；同时，推动这一变革还需要跨部门之间的紧密协作和协调，这在实际操作中可能涉及到协调不同团队和管理层的利益，也是一个不小的挑战。目前，金融机构主要将零信任架构用于解决访问接入问题，距离通过零信任架构进行更加全面和深入安全保护还有一定距离。

建立更加严格的身份和访问管理体系，不仅需要相关技术领域安全厂商加强研发投入，也需要金融机构做出更积极的回应和引导，并增强对该领域的安全关注，通过风险评估、管理制度、员工培训、应急策略等多维度的不断提升，来构建完善的身份和访问管理体系，防范访问行为带来的安全隐患，确保金融系统的安全稳定运行。

（七）金融科技广泛应用，复杂性增强对业务安全提出更高的要求

金融科技正在以其强大的应用范围和复杂的系统架构改变着传统金融行业的运作方式。然而，随着金融科技的广泛应用和复杂性的不断增强，业务安全问题也日益凸显，特别是在反欺诈、反洗钱以及防钓鱼等方面，对金融机构和整个行业提出了更高的要求。

首先，金融科技的广泛应用使得金融业务的边界得到了极大的拓展。无论是线上支付、网络借贷、智能投顾还是区块链技术，金融科技都使得金融业务能够触及更广泛的群体和地域。然而，这种广泛的覆盖也带来了更高的安全风险。由于金融科技涉及大量的个人信息、交易数据以及资金流动，任何安全漏洞或不当操作都可能导致重大的损失。因此，金融机构需要加强对金融科技的监管和风险控制，完善反欺诈和反洗钱机制，确保业务的安全稳定运行。

其次，金融科技的复杂性增强了对业务安全的要求。随着金融科技的不断发展，其系统架构和功

能模块越来越复杂，涉及的技术和算法也越来越多样化。这种复杂性不仅增加了系统的脆弱性，也提高了安全风险的隐蔽性和难以预测性。因此，金融机构需要投入更多的资源和精力来加强系统的安全防护，包括加强网络安全、数据安全、业务反欺诈和业务连续性管理等方面的工作。

此外，金融科技的发展也带来了新的安全挑战。例如，随着大数据和人工智能技术的广泛应用，金融机构需要面对更为复杂和隐蔽的网络攻击和数据泄露风险。这些新的安全挑战要求金融机构不仅要加强自身的技术防范能力，还需要与各方合作，共同构建安全可靠的金融科技生态环境。

为了应对这些挑战，金融机构需要从多个方面入手加强业务安全。一方面，加强技术研发和人才培养，提升金融科技的安全防护能力。另一方面，建立健全的风险管理制度和应急预案，确保在发生安全事件时能够迅速响应和处理。同时，加强与合作伙伴的沟通协作，共同应对新技术带来的安全风险。此外，加强用户教育和安全意识提升，让用户能够更好地保护自己的信息和资金安全。

（八）业务全球化带来的风险全球化

随着全球化的深入，中国金融机构积极扩展海外业务，主要聚焦于东南亚、北美和拉美等地区。这一战略虽然带来了巨大的经济机遇，但同时也暴露于多样化的网络安全风险之中，特别是跨境网络攻击，在全球化经营中成为不可忽视的挑战。

金融机构全球化意味着其业务和系统跨国运作，将面临 DDoS 攻击、APT 攻击、恶意软件和勒索软件等安全威胁。这些网络攻击不仅威胁系统稳定与业务连续性，还可能导致直接的财务损失。例如，2023 年 11 月，中国工商银行的全资子公司工银金融服务有限责任公司（ICBCFS）在美遭受勒索软件攻击，导致部分系统中断，严重影响了其业务运营。

除网络攻击外，合规风险亦是开拓海外市场时的重要挑战。在海外市场，金融机构必须遵守当地的网络安全法律和监管规定，否则可能面临罚款和业务暂停等后果。其中，北美地区的严格数据保护法规要求金融机构确保跨境数据传输和处理的合规性，并建立信息共享和数据泄露应对机制；拉美地区法律的多样性和监管环境的不确定性要求金融机构密切关注隐私法律的变化，并制定灵活的合规策略；东南亚地区对跨境数据流动的管理日益加强，金融机构需遵守区域和国家层面的数据保护规定。

简言之，全球化经营为中国金融机构带来了新的机遇，也提出了网络安全风险管理的新要求，需要综合应对策略和严格的执行力来保障其全球业务的安全与发展。

三、金融行业网络安全监管处罚分析

（一）网络安全罚单数量及趋势分析

在中国金融行业监管体系中，中国金融监督管理局（以下简称“金融监管局”）、中国人民银行（以下简称“央行”）和中国证券监督管理委员会（以下简称“证监会”）发挥着核心的监管作用。其中，金融监管局主要负责银行、保险、信托等证券业之外的金融业监督管理；央行主要负责银行业的监督管理工作。在这一领域，央行与金融监管局有着密切的合作关系；证监会主要负责中国证券市场的监管工作，包括股票、债券、基金等证券产品的发行、交易和监管，以及证券投资机构的监管。

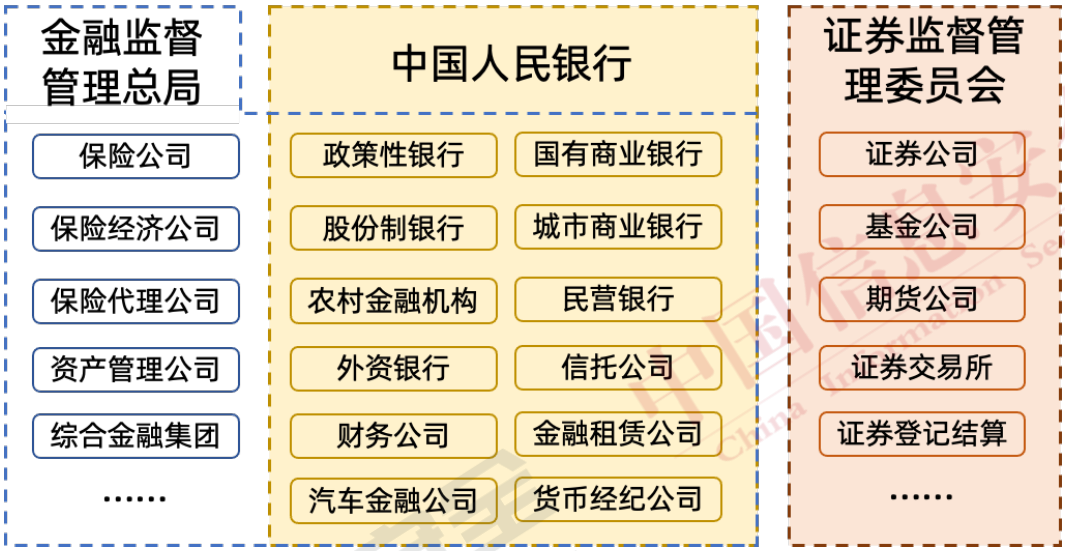
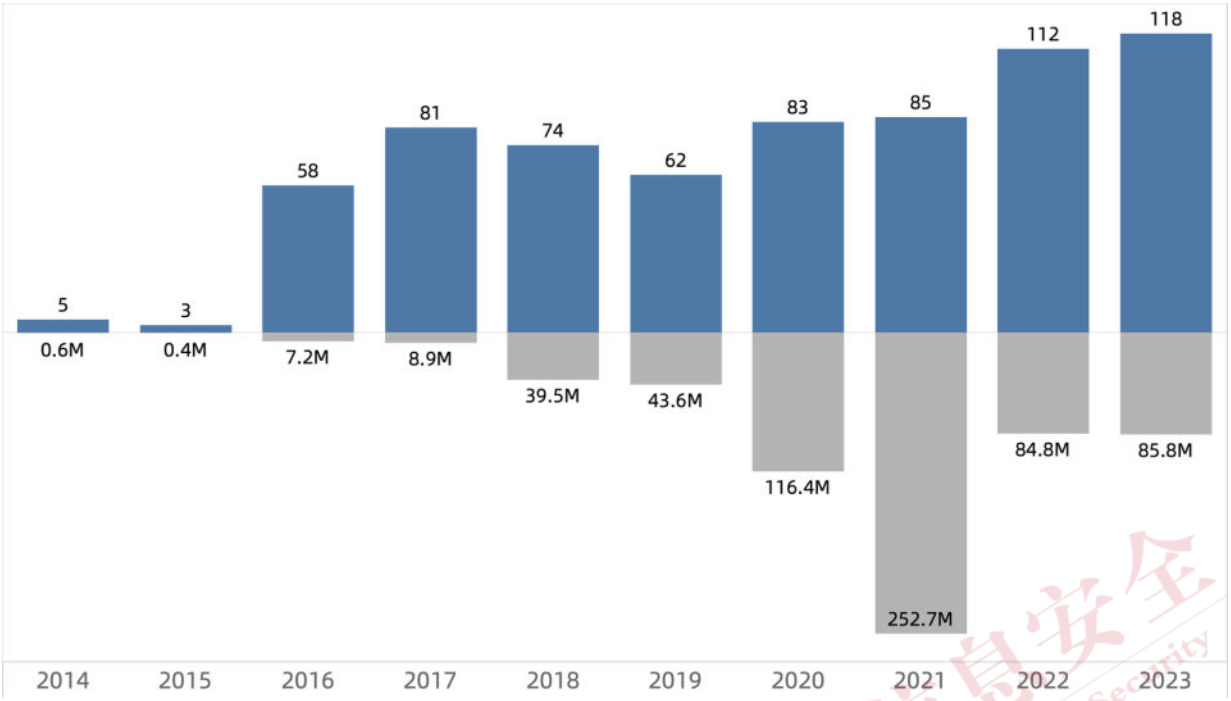


图 2：中国金融行业的三大监管机构及监管范围

三大监管机构中的科技监管司或科技司主要负责网络安全监督管理，同时肩负着制定信息科技发展规划、开展监管科技研究、拟定信息科技风险管理制度、促进金融科技发展与应用等职责，旨在确保金融行业的科技安全和合规性，并推动其数字化转型和创新发展。

2014 年到 2023 年十年间，三家主要的监管机构开出与网络安全强相关的罚单共约 680 张，处罚金额约 6.4 亿元。随着监管部门对网络安全的重视程度不断提升，罚单数量也呈上升趋势，罚款总金额的水平也在抬升。

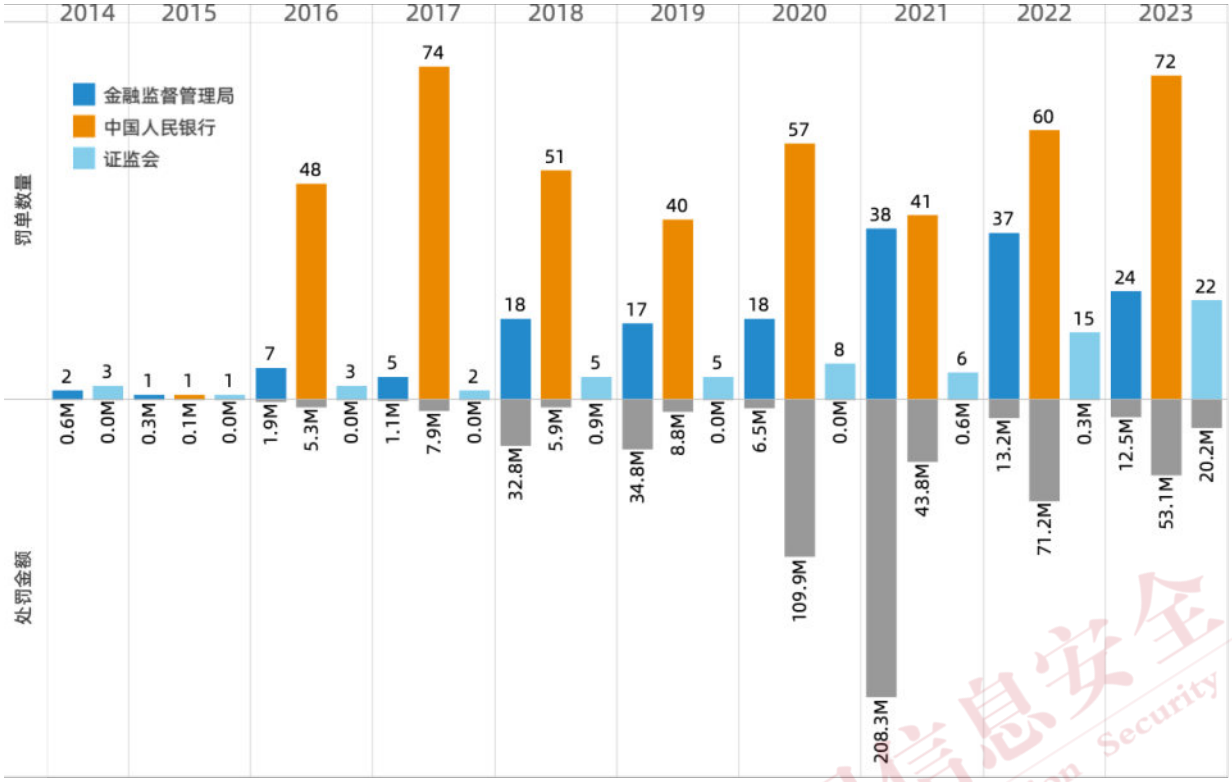


数据来源：数说安全根据公开资料整理

图 3：2014—2023 年三大监管机构开出的网络安全罚单数量及处罚金额

（二）网络安全罚单签发机构分析

央行作为三大监管机构之一，是罚单的主要签发部门，其开出的罚单数量占到了总罚单数的65.3%，同时，金融监管局和证监会开出的罚单占比分别为 24.6%和 10.1%。近几年，金融监管局的监管力度在不断加强，证监会的罚单数量也明显增加。

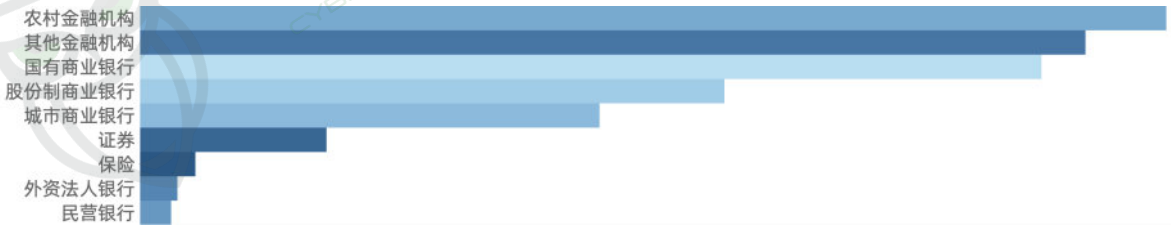


数据来源：数说安全根据公开资料整理

图 4：2014—2023 年三大监管机构开出的网络安全罚单数量及处罚金额情况

（三）被处罚金融机构类型分析

银行是监管机构最关注的领域，90%的罚单处罚对象是银行，其中国有商业银行和股份制银行一直是监管机构的重点关注对象，每个单位平均领到的罚单数量居于较高水平。



数据来源：数说安全根据公开资料整理

图 5：2014—2023 年金融机构收到的网络安全罚单数量分布

近几年，农村金融机构和证券的被关注度明显提升，收到的罚单数量明显增多。

三级行业标签 (组)	2019				2020				2021				2022				2023			
	金融监督管理局	中国人民银行	证监会	合计	金融监督管理局	中国人民银行	证监会	合计	金融监督管理局	中国人民银行	证监会	合计	金融监督管理局	中国人民银行	证监会	合计	金融监督管理局	中国人民银行	证监会	合计
国有商业银行	3	8		11	2	10		12	19	4		23	15	11		26	8	6		14
股份制商业银行	2	11		13	3	15		18	4	3		7	2	7		9	1	19		20
城市商业银行	2	4		6	4	17		21	7	1		8	2	6	1	9	7	3		10
农村金融机构	5	9		14	3	9		12		21		21	1	23		24	2	37		39
民营银行									1			1		3		3	1			1
外资法人银行										2		2					2			2
保险公司	1			1									8			8				
证券			2	2			3	3			2	2			6	6			7	7
其他金融机构	4	8	3	15	6	6	5	17	7	10	4	21	9	10	8	27	3	7	15	25
总和	17	40	5	62	18	57	8	83	38	41	6	85	37	60	15	112	24	72	22	118

数据来源：数说安全根据公开资料整理

图 6：2019—2023 年金融机构网络安全罚单明细

（四）监管机构重点关注领域分析

三家主要的监管机构对安全类型关注各有侧重，央行更关注个人信息保护，证监会更关注网络安全，金融监管局的关注方向则较为全面。

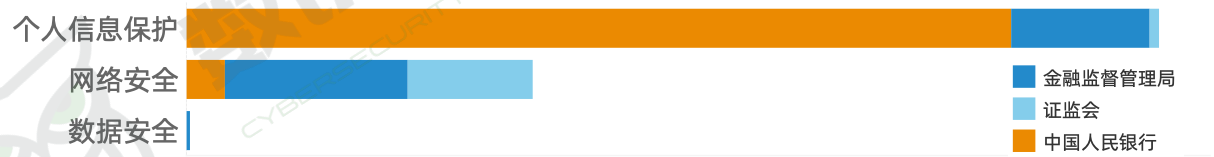
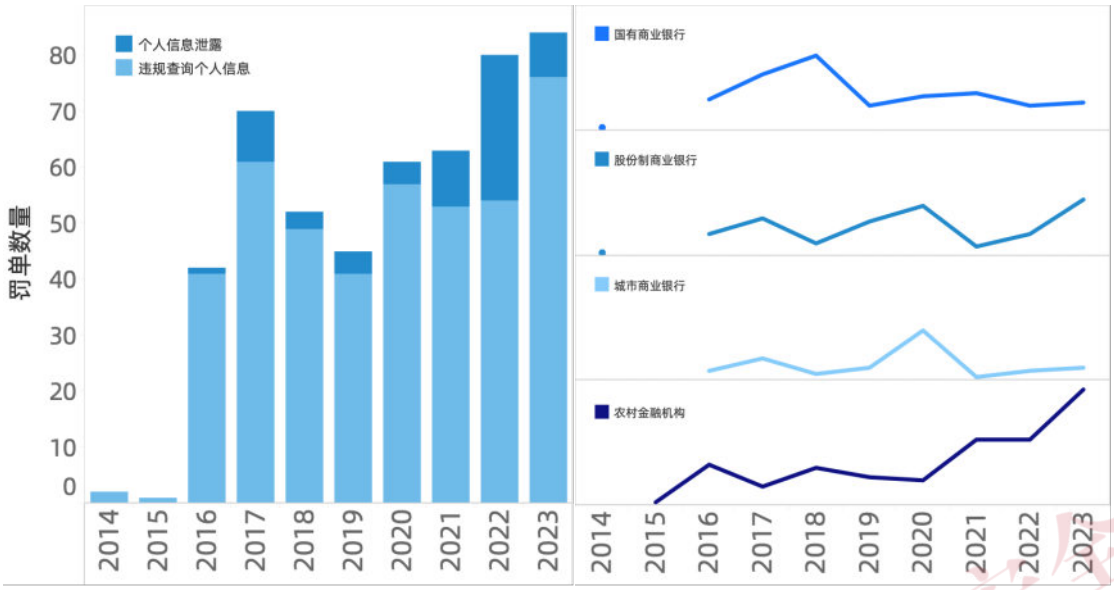


图 7：2014—2023 年三大监管机构的网络安全罚类型分布

个人信息保护一直是监管的重点关注领域，罚单数量占整体的 70%，主要可以分为违规查询个人信息和个人信息泄露两大类；其中未经授权或违规查询个人信息的处罚占比较高，近三年农村金融机构的该类罚单数量增加明显，说明金融机构在客户的个人信息保护方面仍需加强管理，同时监管单位也更加关注小型金融机构的个人信息保护工作。

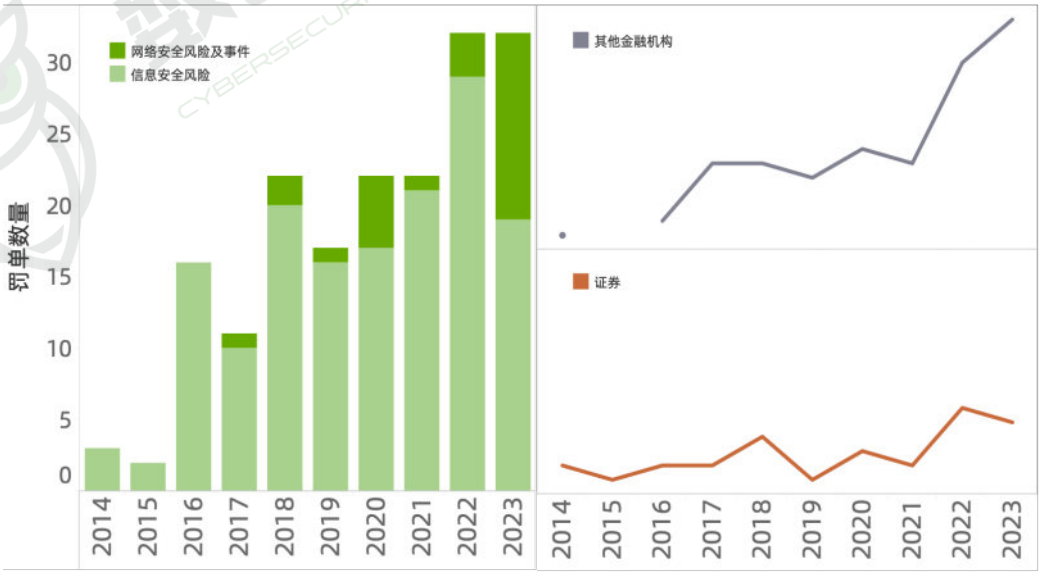


数据来源：数说安全根据公开资料整理

图 8：2014—2023 年个人信息保护类罚单数量及主要受罚机构收到的罚单数量

网络安全类处罚主要分为网络安全风险和信息安全管控风险两类，其中信息安全管控风险罚单占比较高，处罚原因 TOP3 是违反信息安全管理规定、信息科技风险管理不足、信息系统事故导致运营中断或灾备系统不满足要求，而网络安全风险则主要包括安全事件、漏洞、入侵、勒索等。

监管机构在网络安全领域的执法力度也在不断升级，证券机构和其他金融机构的罚单数量增加明显，反映出监管机构在内部控制和风险管理方面的要求愈发严格，忍耐度逐渐降低，希望通过更严格的处罚措施加强推动整个金融行业的风险管理和安全保障能力强化。



数据来源：数说安全根据公开资料整理

图 9：2014—2023 年网络安全类罚单数量及主要受罚机构收到的罚单数量

明确的数据安全类罚单首次出现在 2023 年，由国家金融监督管理总局上海监管局签发，因华美银行（中国）生产数据安全管控不足，责令整改，并处罚款 60 万元。

行政处罚决定书文号	沪金罚决字〔2023〕29号
被处罚当事人	华美银行（中国）有限公司
主要违法违规事实	1.生产环境安全管控不足 2.生产数据安全管控不足
行政处罚依据	《中华人民共和国银行业监督管理法》第四十六条
行政处罚决定	责令整改，并处罚款60万元
作出处罚决定的机关名称	国家金融监督管理总局上海监管局
作出处罚决定的日期	2023年11月2日

数据来源：国家金融监督管理局网站

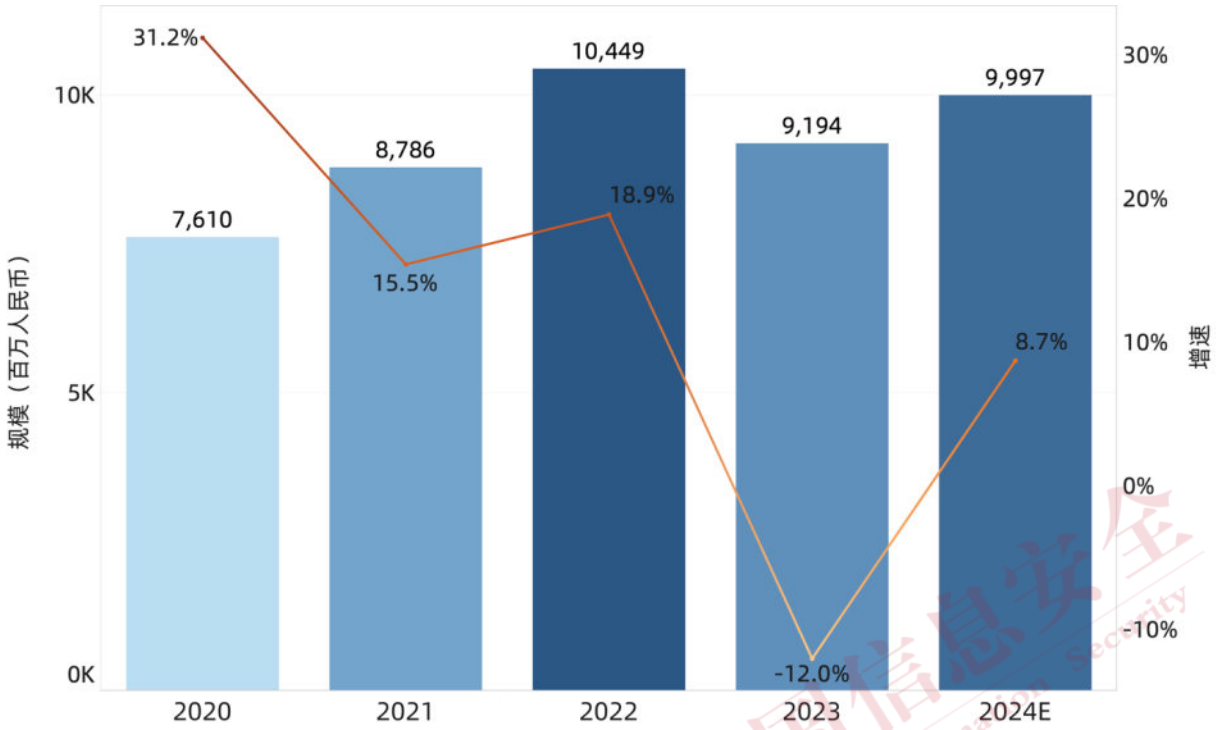
图 10：沪金罚决字〔2023〕29 号罚单主要内容

在过去十年间，随着网络安全、数据安全及个人信息保护变得日益重要，监管机构对这些领域的监管关注度和执法力度也持续提升。不同监管机构在各自的领域内有着特定的关注重点，但共同的目标是推动金融业的健全发展并维护消费者利益。展望未来，随着技术的不断演进和市场环境的变迁，监管机构将持续优化和更新监管策略，确保金融行业在安全、稳健的环境中前进。

四、金融行业网络安全市场分析

（一）金融行业网络安全市场规模及增速

2023 年中国金融行业网络安全甲方支出市场规模约为 91.94 亿元人民币，同比下降 12%，为近五年首次出现负增长。同时，通过对 2024 年第一季度市场情况的分析和研究，预计 2024 年中国金融行业网络安全市场的甲方支出规模约 99.97 亿元，较 2023 年增长约 8.7%。

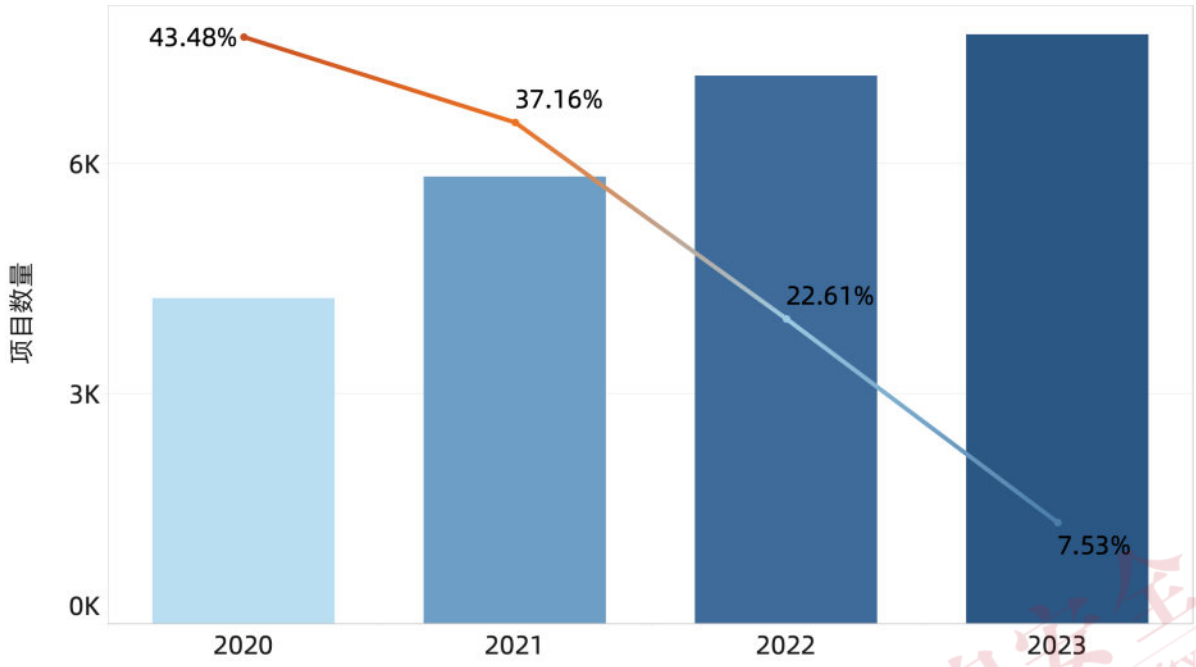


数据来源：数说安全 CSRadar 商业分析平台

图 11：2020—2024 年中国金融行业网络安全甲方支出市场规模

（二）金融行业网络安全市场项目情况分析

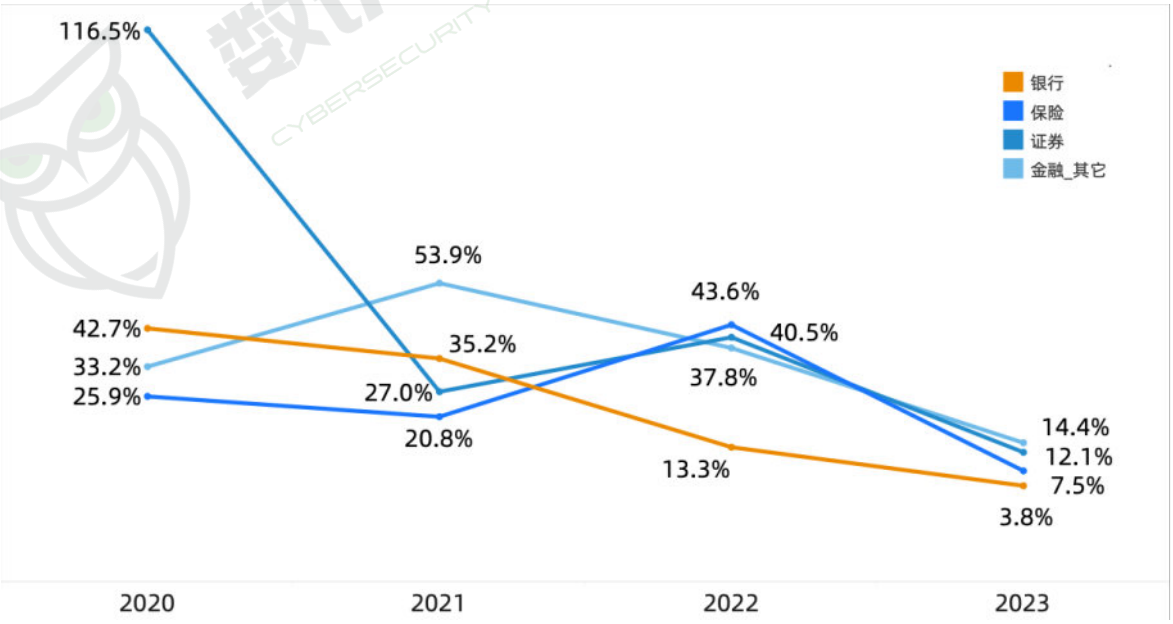
近四年，金融行业的网络安全需求持续增长，采购项目数量仍处于上升趋势中。但随着金融行业市场的日益成熟和网络安全建设的逐步完善，金融机构在当前经济承压的环境下，对网络安全的投入变得更加审慎，因此增速逐年下降。其中，2023 年第一季度的项目数量增速为负，是最近四年的首次季度性负增长，2023 年项目数量在第四季度的带动下实现了整体增长。



数据来源：数说安全 CSRadar 商业分析平台

图 12：2020-2023 年中国金融行业网络安全项目数量及变化趋势

银行作为金融行业核心组成部分，网络安全项目采购数量约占整体的 60%，对行业趋势有重要影响。受宏观环境影响，银行的网络安全项目采购增速率先下降，2023 年仅增长 3.8%。保险和证券行业则在延迟项目补建以及安全规范逐渐完善的推动下，2022 年出现增速回升，但随后也降至四年最低。根据 2024 年一季度的最新数据显示，银行和金融其他领域网络安全采购增速回升，而保险和证券的采购增速仍没有明显起色。

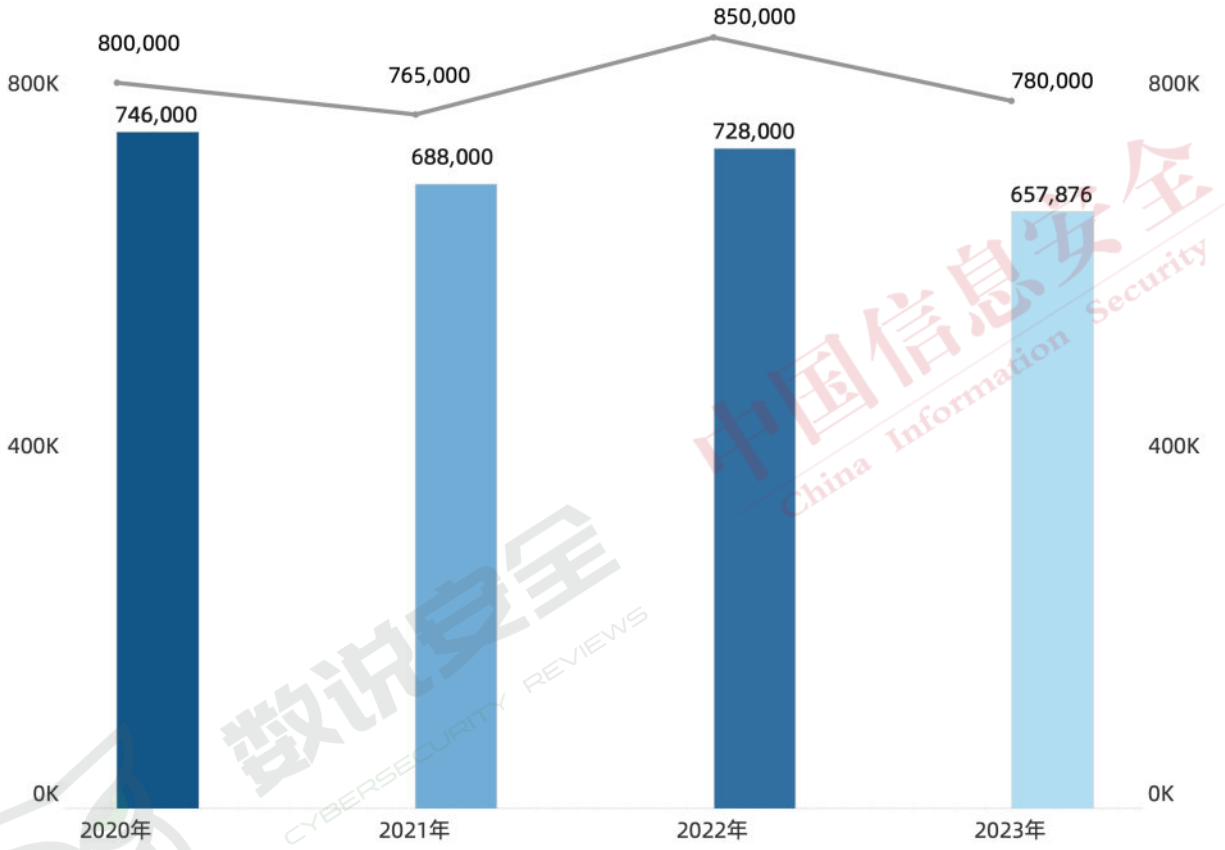


数据来源：数说安全 CSRadar 商业分析平台

图 13：2020—2023 年中国金融行业网络安全项目增速行业分布

（三）金融行业网络安全项目预算实现率分析

金融行业的网络安全项目预算实现率不断降低。2023 年预算金额中位数的实现率仅为 84.4%，与中标金额的中位数偏差额达到约 12 万元。这表明金融行业网络安全市场的竞争日益激烈，低价中标现象越来越普遍。厂商为了在竞争中生存和发展，不得不采取更为激进的定价策略，可能会导致市场价格体系的扭曲和行业利润的压缩。长期而言，这种竞争态势可能会对行业的创新能力和服务质量产生负面影响。

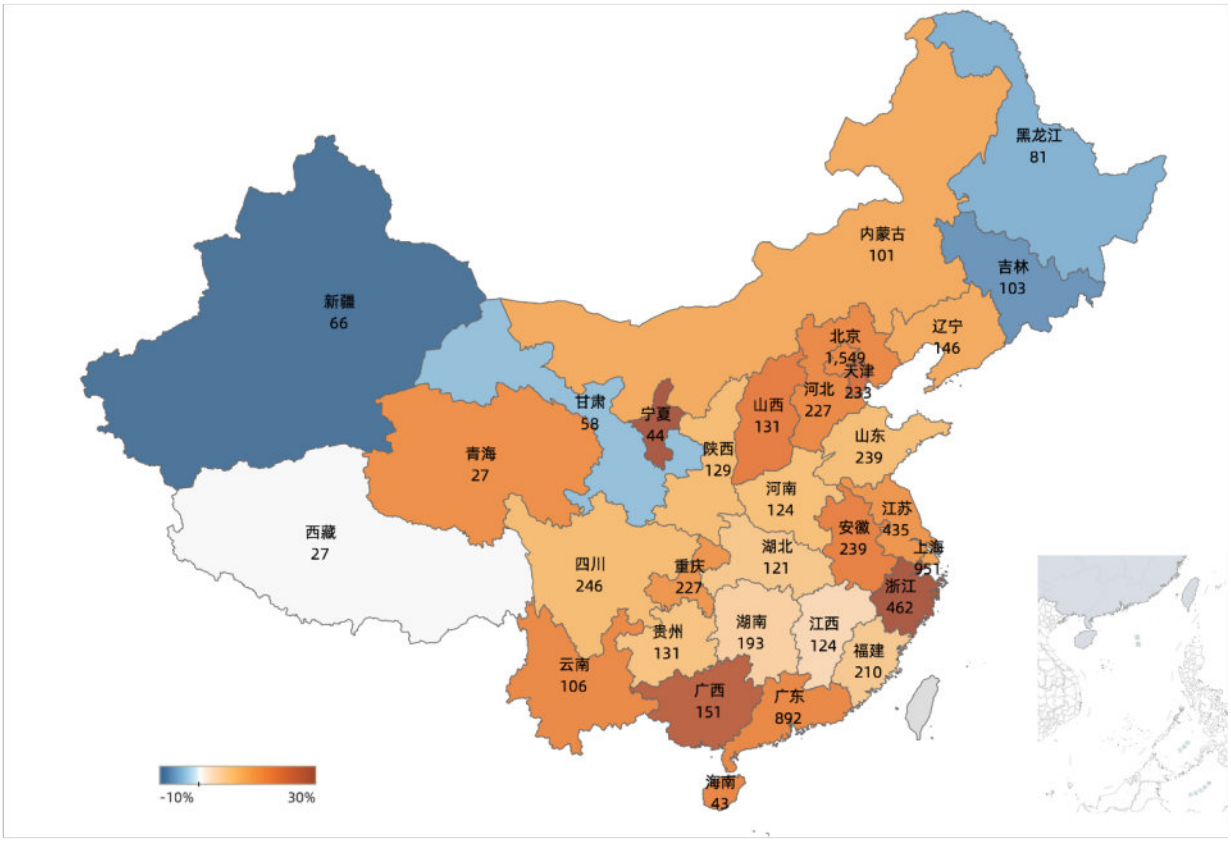


数据来源：数说安全 CSRadar 商业分析平台

图 14：2020-2023 年中国金融行业网络安全项目预算实现率

（四）金融行业网络安全项目地域分布

2023 年金融行业项目分布 TOP3 的区域是北京、上海和广东，三地合计项目数量占整体比重超过 40%，这与该地区的大型金融机构数量多、金融交易活跃度较高有关。同时，经济发展水平对金融行业网络安全项目量有直接影响，经济增长通常伴随着金融活动的增加，用以保护交易安全和客户数据的网络安全需求也随之提升，因此在这些地区金融机构投资网络安全项目的比例更高。



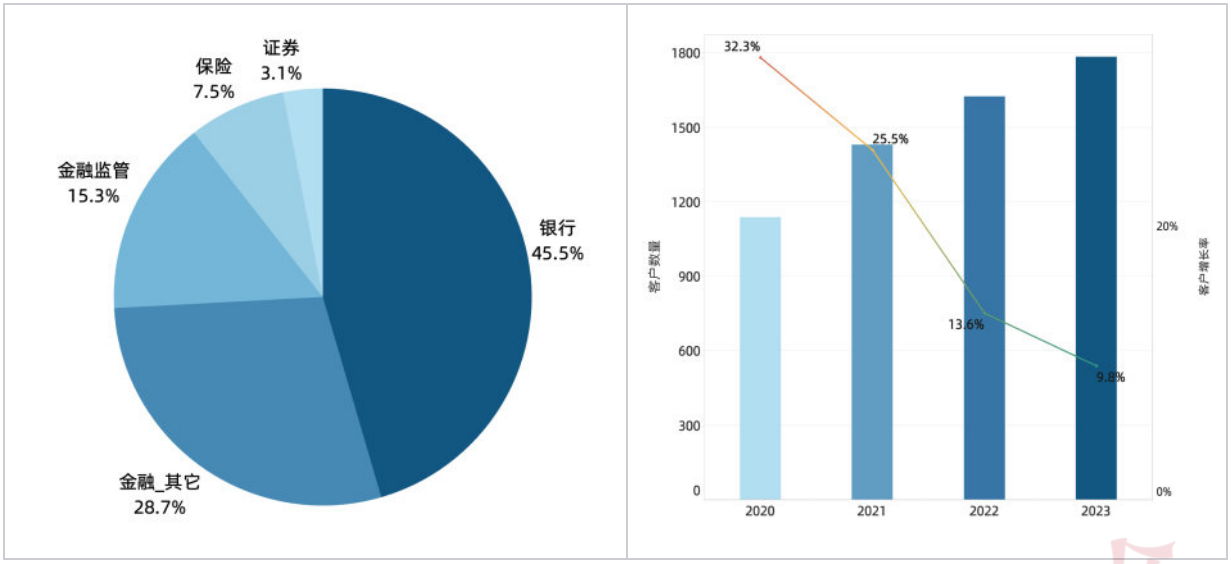
数据来源：数说安全 CSRadar 商业分析平台

图 15：2023 年中国金融行业网络安全项目量地图

（五）金融行业网络安全市场客户分析

CSRadar 商业分析平台当前监测到金融行业具有网络安全采购行为的客户数量超过 3500 家。金融行业参与网络安全公开采购的客户数量在 2020 年至 2023 年期间呈现逐年增长的态势，说明市场的透明度和活跃度在持续上升。但增速逐年放缓，由前三年 23%的平均增速降为 9.7%。其中，银行和证券客户数量的增长率相对较低。

头部金融机构网络安全采购已经形成体系化，成熟的安全品类通过集中采购或框架采购的方式周期性进行，整体项目数量大幅减少。同时，越来越多的中小规模的金融机构（如城商行、农商行）在加强网络安全建设，补齐网络安全基础建设短板，该部分用户基数庞大，带动整体项目量持续增长。



数据来源：数说安全 CSRadar 商业分析平台

图 16：2023 年中国金融行业网络安全客户分布及采购项目趋势

（六）金融行业网络安全典型产品热度指数[2]

通过分析 2023 年金融行业公开招投标数据中的产品类型和采购趋势，我们发现，尽管传统合规类产品在金融行业的采购中仍然占据着较大的比重，但随着金融机构的合规建设进入常态化，且完善度不断提高，这类产品的增长趋势逐渐放缓（如图 17 中红框所示）。

同时，在新兴的网络安全领域，如 API 安全、攻击面管理和开发安全等方面，尽管目前的热度指数相对较低，但其增长速度却异常迅猛。说明金融行业在数字化转型过程中，对于新兴技术的安全需求日益增长。随着金融科技的快速发展，金融机构越来越依赖于开放的 API 接口、云计算服务和敏捷的开发环境，这无疑增加了新的安全风险点。因此，对于 API 安全、攻击面管理和开发安全等新兴领域的关注和投资，成为了金融机构保障业务连续性和数据安全的关键。

此外，国家和行业层面的政策也在推动这一趋势的发展。例如，监管部门对于金融科技的安全性提出了更高的要求，强调了金融机构在采用新技术时必须确保风险可控。这促使金融机构在采购决策中更加重视这些新兴的安全产品，以满足监管要求并保护客户数据安全。随着金融行业对新兴技术安全的重视程度不断提升，预计这一趋势在未来几年将继续保持增长势头。

[2] 热度指数说明：热度指数是 CSRadar 平台针对网络安全领域市场洞察力的集中体现，它能够捕捉到行业内部的细微变化，不仅反映了当前的市场态势，也预示着未来技术发展和行业创新的潜力点。

数据来源：数说安全 CSRadar 商业分析平台

图 17：2023 年中国金融行业网络安全典型产品热度指数

五、金融行业网络安全建设情况

（一）银行业网络安全市场分析

政策解读

2017 年 6 月，《网络安全法》在正式施行后，对金融行业的数据管理和国际合作产生深远影响。该法律的实施不仅强化了信息安全的高标准管理需求，还重塑了网络空间的规则，有力地保护了客户的信息安全。与此同时，它也给银行业带来了前所未有的技术和管理挑战。面对这些挑战，银行业积极应对，认真落实细化《网络安全法》的各项要求，精心制定了一系列适应行业特性的安全政策法规和管理措施，在政策监管层面确保了金融信息的安全性和完整性，为银行业的健康发展提供了坚实的保障。这些网络安全政策法规的主要目的是加强银行业的信息安全管理，保障客户信息的安全，维护金融市场的稳定运行。表 1 展示了《网络安全法》施行以来，银行业制定的网络安全政策、法规和规范。

表 1:《网络安全法》施行以来银行业制定的网络安全政策、法规和规范

发布时间	政策法规	政策解读
2018 年 5 月	《关于进一步加强征信信息安全管理的通知》	该通知由中国人民银行等权威机构发布，要求银行业增强征信信息安全管理意识，完善业务操作流程和内控制度，提高技防能力，并建立应急处置和考核评级机制。这对银行业而言，意味着提升了征信信息安全管理水平，规范了业务操作，加强了技术防御，从而增强了客户信任和市场竞争力，为行业的稳健发展提供了有力保障。
2018 年 5 月	《银行业金融机构数据治理指引》	该指引由中国银监会颁布，其主要内容旨在引导银行业金融机构加强数据治理工作，提升数据质量，确保数据的有效性和安全性。该指引详细阐述了数据治理应遵循的原则、组织架构以及实施要求，为银行业金融机构提供了明确的数据治理指导。其发布有助于推动银行业金融机构完善数据治理体系，优化数据管理流程，提高风险防控能力，进而提升经营效率和市场竞争力。
2020 年 2 月	《网上银行系统信息安全通用规范》	该规范由中国人民银行发布，主要规定了网上银行的系统安全技术要求、安全管理要求、业务运营安全要求，为网上银行系统建设、运营及测评提供了重要依据。这一规范对银行业产生了深远影响，不仅提高了网上银行的安全性，降低了风险，还为银行业的数字化转型提供了有力支持，增强了客户对网上银行服务的信任，促进了银行业务的创新和发展。
2020 年 2 月	《个人金融信息保护技术规范》	该规范由中国人民银行发布，规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求。同时，该规范还从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。其发布有助于银行业加强个人金融信息安全管理，保障个人金融信息主体合法权益，指导各相关机构规范处理个人金融信息，最大程度保障个人金融信息主体合法权益，维护金融市场稳定。
2020 年 9 月	《监管数据安全管理办法（试行）》	该管理办法由中国银保监会发布，主要规范了银保监会监管数据的采集、存储、处理、使用等活动，强调数据的安全性和保密性，要求建立协同管理体系并明确各部门职责。对银行业而言，该管理办法提升了数据安全意识，规范了数据管理，促进了行业内的协同合作，推动数字化转型，并增强了客户信任，从而提升了银行业的整体竞争力和市场声誉。
2020 年 9 月	《金融数据安全数据安全分级指南》	该指南由中国人民银行发布，根据金融业机构数据安全性遭受破坏后的影响对象和所造成的影响程度，将数据安全级别由高到低划分为五级，并明确了各级别的具体要求和管理措施。对银行业而言，这一指南的发布有助于规范金融数据的安全管理，提高银行的数据安全意识和风险防范能力，促进银行业数字化转型的稳健发展，保障金融市场的稳定和客户的合法权益。

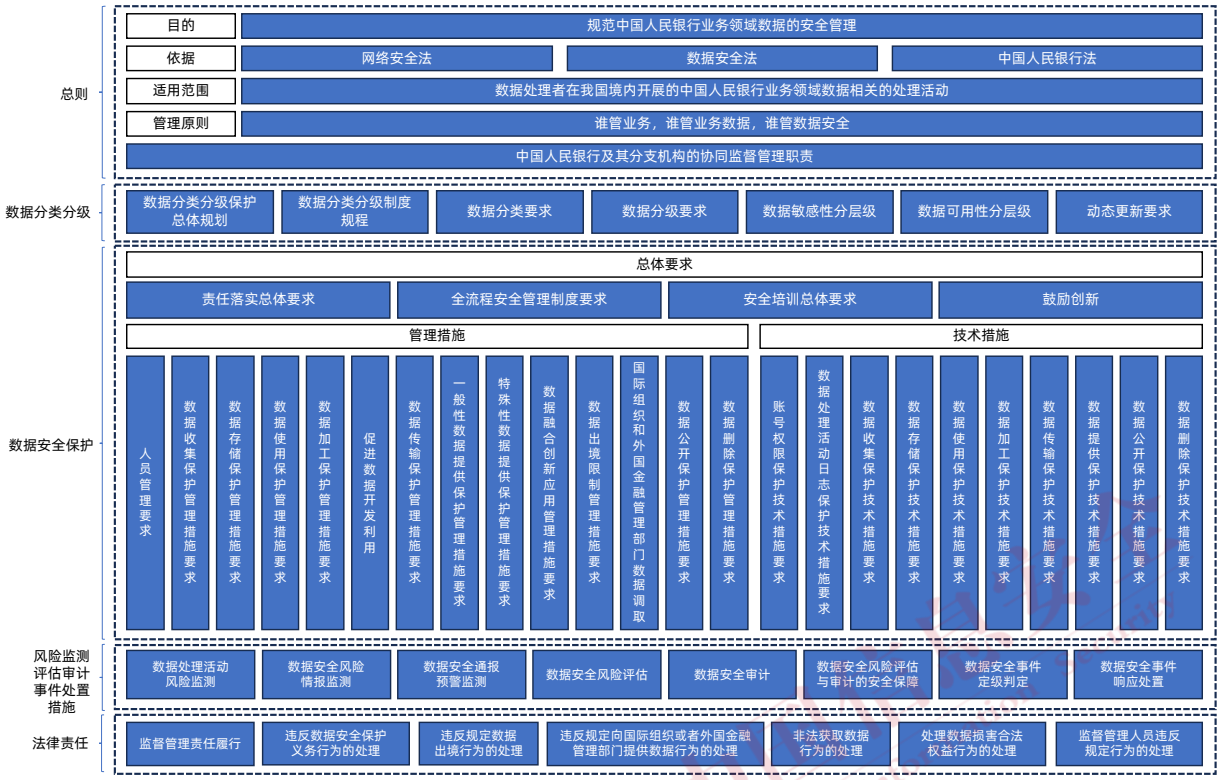
2021 年 1 月	《征信业务管理办法（征求意见稿）》	该管理办法由中国人民银行发布，突出了信息安全的重要性，并规范了信息采集的过程，保护了被征信人的信息权属，明确了征信授权。同时，管理办法还规范了个人征信全流程，为未来常态化监管创造了条件，对征信企业使用征信数据获利方面进行了规范，对信息使用者作出了规范化要求。
2022 年 1 月	《关于银行业保险业数字化转型的指导意见》	该指导意见由中国银保监会发布，明确了银行业保险业数字化转型的目标和原则，提出了数字化转型的重点任务，强调了合规与风险管理的重要性。其发布对于推动银行业和保险业的数字化转型具有重要意义，将有助于提升银行业保险业服务效率和质量、创新业务模式、加强风险防控以及推动国际合作与交流。
2022 年 12 月	《银行保险监管统计管理办法》	该管理办法由中国银保监会发布，统一了银行业保险业监管统计制度，为解决当前监管统计工作实际问题提供了制度支撑。其发布进一步夯实了统计工作基础，对银行业保险业监管统计工作具有指导性作用。
2023 年 6 月	《关于加强第三方合作中网络和数据安全管理的通知》	该通知由金融监督管理总局发布，指出金融机构在第三方合作中的网络和数据安全风险问题，强调银行保险机构在数字生态场景合作中缺乏统筹管理、数据安全风险识别不清等问题，要求银行保险机构自查风险、加强科技风险统筹管理，并关注非驻场外包风险。同时，通知还要求银行保险机构强化网络和数据安全保护义务，采取针对性安全保护措施，并建立健全应急处置机制。这一通知旨在提高银行业对第三方合作中网络和数据安全管理的重视，加强风险防控，确保金融业务的稳健运行。
2023 年 7 月	《中国人民银行业务领域数据安全管理办法（征求意见稿）》	该管理办法由中国人民银行发布，旨在加强银行业务领域的数据安全管理。它对数据分类分级、数据安全保护总体要求、数据处理活动全流程安全合规底线、风险监测、评估审计、事件处置等环节提出了明确要求，并强调了中国人民银行及其分支机构对数据处理者数据安全保护义务的执法检查权。其发布将将有助于提高银行业数据安全水平，保障银行业务安全和客户数据安全。

2023 年 8 月	《金融信息系统网络安全风险评估规范》	该规范由中国人民银行发布，其主要内容涵盖了金融信息系统网络安全风险评估的原则、流程、方法和要求。它强调了风险评估的全面性、及时性和准确性，要求银行业在评估过程中充分考虑业务需求和系统特点，确保评估结果的科学性和有效性。同时，该规范还提出了一套风险评估指标体系和计算公式，以帮助银行业准确评估自身的网络安全风险等级，为风险防范和应对提供有力支持。通过遵循规范进行网络安全风险评估，银行业将能够更好地识别和管理潜在的安全风险，提升系统的安全性和稳定性。同时，该规范有助于防范金融风险。通过规范定义的风险评估流程和方法，银行业将能够及时发现和应对潜在的安全威胁，降低金融风险的发生概率。此外，该规范的实施还有助于促进银行业的发展。通过提高网络安全水平和防范金融风险，银行业将能够增强自身的竞争力和创新能力，为客户提供更优质、更安全的金融服务，推动整个行业的健康发展。
2023 年 12 月	《“数据要素×”三年行动计划（2024—2026 年）》	该计划由国家数据局会同中央网信办、工信部、中国人民银行、金融监管总局等十七部门联合印发，旨在充分发挥数据要素的乘数效应，赋能经济社会发展。其主要内容包括明确工作目标、强调基本原则、选取重点行业和领域推动数据要素价值释放，并明确了加强组织领导、开展试点工作、推动以赛促用等实施措施。同时，该行动计划提出了一系列网络安全激励政策，包括资金支持网络安全技术研发、奖励符合安全标准的企业、促进网络安全与包括银行在内的业务深度融合，以及强化网络安全监管等，由此全面提升网络安全防护能力，确保数据要素的安全应用。对于银行业而言，该计划的实施意味着数据将成为银行业创新发展的重要驱动力，有助于提升银行业务的智能化水平，优化服务流程，提高风险防控能力，推动银行业向数字化、智能化方向转型升级，进而促进整个金融行业的健康发展。
2023 年 12 月	《银行保险机构操作风险管理办法》	该管理办法由国家金融监督管理总局发布。其目的是为了提高银行保险机构操作风险的管理水平，确保金融系统的稳定运行。该办法强调了审慎性、全面性、匹配性、有效性等原则，明确了董事会、监事会和高级管理层的责任，规定了风险管理的基本要求，细化了管理流程和管理工具，并完善了监督管理职责。在网络安全和数据安全方面，该办法要求银行保险机构制定网络安全管理制度，采取必要措施以防范网络安全风险和威胁，同时制定数据安全管理制度，对数据进行分类分级管理，保护数据免遭非法篡改、破坏、泄露等风险。这些规定对银行业网络安全和数据安全的建议影响显著，推动了银行保险机构加强内部控制、提高对网络安全事件的应对能力，以及加强对数据的保护，从而提升了整个银行业的网络安全和数据安全水平。

2024 年 3 月	《银行保险机构数据安全管理办法（征求意见稿）》	该办法由国家金融监督管理总局发布，旨在规范银行保险机构的数据处理活动，确保数据安全，并促进数据的合理开发利用。其主要内容包括要求银行保险机构建立数据安全责任制、制定数据分类分级保护制度、强化数据安全管理、健全数据安全技术保护体系等。这一法规的出台对银行业具有深远的影响，有助于提升金融服务数字化、智能化水平，保护个人和组织的合法权益，同时也为银行保险机构在数据管理方面提供了明确的指导和规范。
2024 年 5 月	《关于银行业保险业做好金融“五篇大文章”的指导意见》	该指导意见由国家金融监督管理总局发布，旨在深入贯彻落实中央金融工作会议的决策部署，围绕发展新质生产力，提高金融服务实体经济的质量和水平。它明确了银行业保险业在科技金融、绿色金融、普惠金融、养老金融、数字金融等方面的发展目标和基本原则，要求银行保险机构优化金融产品和服务，加强内部管理机制建设，坚守风险底线，并强化监管引领。它还强调了数字化转型的重要性，要求建立数字化监管架构流程，提升监管数字化智能化水平，同时在风险防控方面提出了严格要求，以确保金融活动的安全性和合规性。

资料来源：数说安全根据公开资料整理

自 2023 年以来，金融监督管理总局和中国人民银行相继发布了一系列关于网络安全和数据安全的新政策，其中包括《关于加强第三方合作中网络和数据安全管理的通知》《中国人民银行业务领域数据安全管理办法（征求意见稿）》（如图 18 所示）《金融信息系统网络安全风险评估规范》《银行保险机构操作风险管理办法》《银行保险机构数据安全管理办法（征求意见稿）》和《关于银行业保险业做好金融“五篇大文章”的指导意见》等。它们不仅涵盖了网络安全和数据安全的基础要求，还新增了对第三方合作、外包服务商管理以及跨境数据传输等方面的具体规定。通过这些新政策的实施，监管部门展现了对网络安全和数据安全问题的全面关注和深入思考，同时也为银行保险机构提供了更明确的指导和要求，以更好地执行网络安全和数据安全保护工作。



资料来源：数说安全根据公开资料整理

图 18:《中国人民银行业务领域数据安全管理办法（征求意见稿）》框架内容

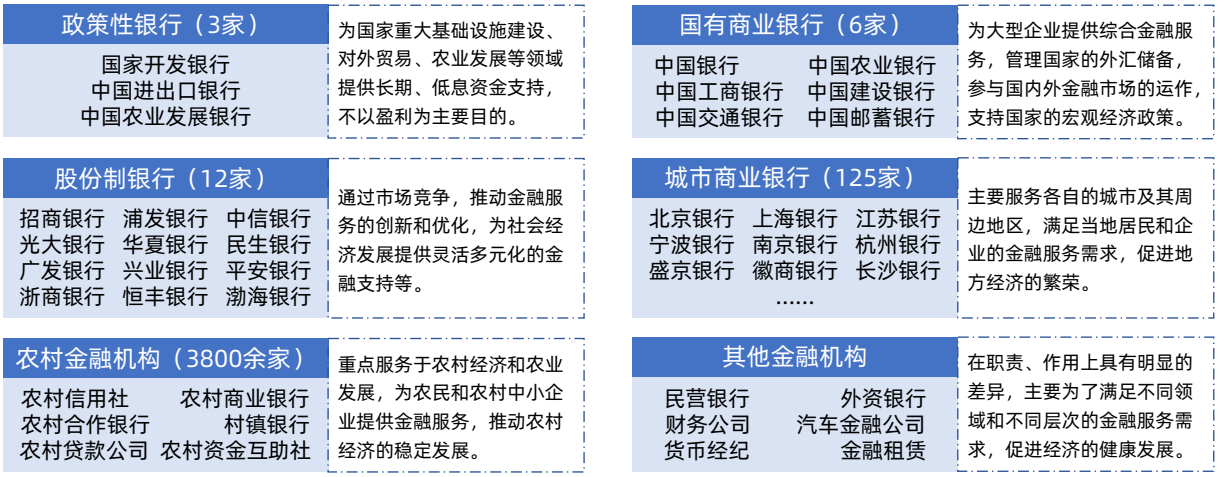
随着技术的不断进步和网络安全形势的日新月异，相关政策和法规还在不断更新和完善中，以适应新的挑战和需求。这种持续更新和完善的过程，进一步强化了我国银行业对网络安全的重视，提升了行业的整体安全水平，为银行业的健康发展提供了坚实的制度保障。

银行网络安全建设现状及关注点

作为金融行业的重要参与者，银行是资金流转的重要枢纽，几乎所有的金融交易都离不开银行系统的参与，银行系统的安全性直接关系到整个金融系统的稳定性和人民的财产安全。

我国银行业金融机构主要分为政策性银行、国有商业银行、股份制银行、城市商业银行、农村金融机构和其他类金融机构。金融监督管理总局最新发布的数据显示，截止 2023 年末，我国共有银行业金融机构 4490 家，其中传统意义上的银行（国有商业银行、政策性银行、股份制银行、城市商业银行、农村商业银行、村镇银行、农村信用社）共 4002 家。

各类金融机构在组成和职责上有所不同，形成了互补的金融服务体系，共同促进社会资金的高效流动和社会经济的发展。本章节主要针对国有商业银行、股份制银行、城市商业银行和农村金融机构展开分析。



资料来源：数说安全根据公开资料整理

图 19：银行业机构分类情况及主要功能

◆ 安全建设驱动力：

银行业网络安全建设的驱动力主要源自三个方面：

- 合规性要求的持续更新与完善。法律法规的不断更新和完善，促使金融机构不断强化安全建设,以满足最新的法律法规要求；
- 实网攻防演习深入进行。通过模拟真实网络攻击，帮助银行提升真实环境下的安全体系防御能力重视度，加强对安全威胁的持续检测、快速响应和有效处置能力；
- 数字化转型中新技术的广泛应用。为了有效支持业务增长，银行需要提供更便捷、个性化的金融产品和服务，构建全面而灵活的获客渠道，并深化数据驱动的决策机制，以增强风险管理和运营效率。这就需要银行采用新技术，提升自身的敏捷性、开放性、智能化水平和生态系统的完整性。这些新技术的应用为金融服务带来便利和高效的同时，也带来了新的安全挑战。因此，银行业在不断推进网络安全建设，以应对这些挑战。

整体上，银行业安全建设的核心目标是保障金融服务的稳定性与安全性，防止安全事故的发生。

◆ 安全预算及采购情况：

我国银行的数量众多，且在规模上呈现出显著的“头部集中，尾部分散”现象，少数大型银行拥有着庞大的资产规模和市场份额，而数量众多的农村金融机构则构成了市场的长尾部分，这种规模的巨大差异导致了银行业在资源和技术投入方面的不均衡分布。

国有商业银行的网络安全支出约在 1.5 亿元-3 亿元之间，占整体 IT 支出 7%-10%。

股份制银行因业务体量和 IT 基础水平不同，网络安全支出存在较大差异，技术发展相对靠前的招商银行、中信银行、平安银行每年网络安全支出约在 1 亿元-2 亿元之间，股份制银行的网络安全

支出占整体 IT 支出比例在 5%-10%之间。

城商行的安全投入相较大型银行来说有限，每年网络安全支出在 1 千万-5 千万之间，网络安全支出占整体 IT 支出比例大概 3%-6%。

农村金融机构又分为很多类型，不同类型的机构也存在很大差距。农信社的信息系统和安全建设通常由省级农信社统一管理，网络安全支出在百万到千万不等，约占 IT 支出的 3%-5%。农村商行银行和村镇银行的数量庞大，安全建设情况的差距也更加明显，头部银行的网络安全投入在千万级别，尾部银行则可能不足百万。

通过调研我们发现 2023 年银行业的网络安全预算呈现高预算低执行的情况，整体建设投入明显下降，这与银行业的整体经营情况直接相关。具体表现为传统网络安全产品的采购价格降低、采购更新周期拉长，非急需补足的安全能力建设延后等，但在数据安全、安全运营、开发和供应链安全等领域，安全投入依然保持在较高水平。

◆ 安全技术团队：

银行业的安全团队在规模上有明显差距，同时，外包安全人员通常占总安全人数的 30-50%。

国有商业银行的安全团队规模相对较大，人数通常在 100 人到 400 人之间。股份制银行的安全团队规模稍小，通常在 100 至 200 人之间。城市商业银行的安全团队人员数量则依据其规模而异，从十几人到近百人不等。农村金融机构的安全人员配置更加有限，大型农商行和农信社能达到 40、50 人，小型村镇银行则仅配备一名安全专员，或者由开发或运维人员兼任安全职责。

◆ 安全建设现状：

按照不同的网络安全建设情况，银行大体可以分为三个梯队：

- 这一梯队的银行主要包括国有商业银行、股份制银行和个别互联网属性较强的民营银行，他们占有主要的市场份额，拥有充足的安全资源和投入。在网络安全领域，已经具备非常成熟的基础安全防护能力；在纵深防御体系的构建方面，已经进入深化阶段，根据挑战的变化和技术的发展，不断加强数据安全、开发安全、供应链安全等领域的安全能力。主动防御体系的建设是第一梯队银行当前的关注重点，他们通常会自研或联合开发安全平台，目标是深化对安全工具和平台的深度运用与内部整合，构建自主化、场景化和体系化的可持续运营安全体系，提升主动检测、快速响应与及时恢复的能力。
- 第二梯队主要包括城商行、少数大规模的省级农信社和农商行，这些银行的安全资源和投入相对有限，但已有较完善的基础安全能力。目前，他们正在积极推进纵深防御体系的建设，优先补足重点领域的安全能力短板。这些银行已有基础的主动防御体系，现阶段的关注重点是推进各领域的平台化和联动化建设，完善安全运营体系，实现对安全资

源的更高效管理，同时加强内外部的攻击面管理能力，减少潜在的安全风险。

- 第三梯队包括小规模的农信社和农商行，他们在安全领域的投入较少、专家人才短缺、安全力量薄弱，具备满足合规要求的基础安全防护能力，但安全体系建设往往处于初级阶段，因此，未来的安全建设重点在于尽快加强安全防护措施，并搭建安全管理体系。这一梯队的银行虽然资源和投入较少，但面临的安全风险和外部威胁却与大中型银行类似，所以他们也很重视安全事故的防范，为加强实战攻防应对能力，通常会根据自身需求，采取更加灵活的策略来弥补安全运营能力的不足。

尽管银行在安全建设方面可以大致划分为三个梯队，但深入到各个具体的安全领域进行考察，我们会发现不同梯队银行在不同领域的安全建设方面也有明显差异：

a) 基础的终端及网络安全

银行业的终端及网络的防护能力建设比较完善，通常都采购了网络终端准入 NAC、数据泄露防护 DLP、防病毒、移动终端加固、防火墙 FW、Web 应用防火墙和网络检测与响应 NDR 产品。

第一梯队机构拥有更为复杂的 IT 架构，面对的威胁风险也更加多样，因此对终端设备的统筹管理、检测与响应能力提出了更高的要求，通常还会部署终端响应与检测 EDR、网络流量分析 NTA、终端安全防护平台 EPP 以及移动终端管理平台。

b) 云安全

由于严格的安全和监管要求，银行业对云架构的使用较为保守，私有云是主要建设方向，仅有少量新闻、资讯类应用系统会放在公有云上。

在云技术使用方面，虚拟化仍是主要技术手段。头部银行的容器数量近年来虽然增长迅速，但现有的 IT 运维、业务流程与容器的快速迭代和自动化部署未能完全匹配，容器的使用并不理想，Serverless 和 ServiceMesh 的应用情况也比较基础。

对云技术的保守应用的确规避很多安全问题，但也减缓了云安全/云原生安全在金融行业的技术进步，多数银行只部署了主机入侵检测系统 HIDS，云工作负载保护平 CWPP 和容器安全的使用渗透率和覆盖度还有较大提升空间。

c) 身份与访问管理

银行普遍建立了基础的身份与访问管理系统，主要包括身份认证与访问管理 IAM、运维审计堡垒机、MFA 多因素认证，但这套系统已不能满足对日益复杂的访问行进行控制和管理。

零信任安全架构作为一种新兴的安全理念，正在逐步被银行机构采纳并实施，但仍面临技术成熟度不足、系统应用改造困难、业务流程协调复杂等诸多问题，距离在银行机构中全面铺开仍有一定距

离。目前，中小规模的银行机构主要以 VPN 替代为切入，解决访问接入问题，应用在远程办公和三方接入场景上。

头部银行在加快扩展零信任的应用场景及试点业务系统，同时加强终端安全评估与防护能力、安全分析能力的联动，并探索更细粒度的访问控制策略，逐步搭建自己的零信任架构。通过调研，我们了解到某互联网属性较强的民营银行基本全面实现了应用级别的访问控制，并实现了基于任务的访问控制 TBAC 这样更细粒度的访问控制策略。

d) 开发安全

随着安全左移理念在银行业的广泛采纳，银行在开发安全领域也不断增加投入。处于第一梯队银行的开发需求较高，普遍已经建立了 DevSecOps 体系，整合了敏捷和持续集成/部署工具 CI/CD、安全组件库 SDK、应用程序安全测试 AST、软件成分分析 SCA 等技术产品，并定制化或自研了开发安全平台，同时，也在引入运行时应用保护 RASP 保护应用程序运行时安全。

对第二梯队的银行而言，虽然也使用了 SDK、AST 等开发安全工具，但开发安全体系仍较为基础，当前的主要挑战在于完善开发和安全协作的流程制度、降低 AST 类工具的检测耗时和误报率，从而提升整体开发安全水平。

北京银行2023年年报

优化软件开发风险管理流程，把控开发安全工作管控。加强开发过程质量管理，严格执行数据脱敏、严防敏感信息泄露，确保安全管理到位。

图 20：上市银行 2023 年年报中关于开发安全的建设情况

e) 供应链安全

银行业务的复杂性和对多样化供应链的依赖，加之供应链透明度的不足和日益严格的监管要求，使得供应链安全管理成为银行当前面临的一项复杂且充满挑战的任务。为了应对这一挑战，银行通常会采用软件成分分析 SCA 工具，然而，应用程序的复杂性和供应链中第三方组件的层层嵌套使得 SCA 工具的检测效果并不理想。此外，由于软件物料清单 SBOM 缺乏统一标准，以及通常不够详尽，也增加了银行的供应链风险管理难度。

为了提高供应链安全管理的效果，一些头部银行正在自研或联合安全厂商建设供应链管理平台，并将经验沉淀到平台中，以提高供应链安全管理效率。

通过调研，我们了解到某互联网属性较强的民营银行在供应链安全管理方面取得了显著成效，能够对所有上线前的代码和组件进行彻底的扫描评估，确保没有漏洞和后门的存在，并在应用上线后，严格限制可运行的程序、函数、插件类型等，从而实现了更加全面的安全防护。

江阴银行2023年年报

- 提高供应链安全风险防范意识。建立供应链风险监控机制，明确供应链风险管理监控指标，持续监控供应链服务商的财务、内控及安全管理情况加强供应链网络安全监测。
- 加强代码审计与安全检查，同时要求供应商提供清单，要求其列明使用的所有代码组件，以识别与开源组件漏洞相关的潜在风险，并考虑在实施代码前，增 加额外的自动化或手工检查，并利用第三方工具或软件及相关产品源代码进行安全分析。
- 构建完整的供应链风险管理流程。为了防控供应链中每个阶段面临的不同安全风险，本行计划对供应链安全进行体系化管理，从而更好的对供应链进行风险治理。

图 21：上市银行 2023 年年报中关于供应链安全的建设情况

f) 数据安全

数据安全是近年来银行业的重点投入领域之一，由于合规要求，大部分银行的基础数据安全建设都比较完善，如数据库安全（数据库审计、数据库防火墙、数据库加密）、数据防泄漏 DLP、静态数据脱敏以及数据水印等，动态脱敏产品目前率先在头部银行逐渐推进应用。

在组织架构方面，一、二梯队银行基本都完成了数据管理部的设立，负责组织数据安全管理工作规划和实施，完成了责任和职责的界定，目前正在加紧完善本行的数据安全管理办法、制度和流程制定。没有成立数据管理部的银行，也都明确了数据安全负责人，及相关的职责和责任。

数据分类分级是数据安全防护的基础，大部分银行已经通过自动化程序，基本完成了对结构化数据的分类分级和打标工作。但非结构化数据的分类分级仍面临较大挑战，第一梯队银行正在努力提高分类分级的覆盖程度和准确度，并通过人工+机器学习的方式提效率，该环节的难点在于非结构化数据特征的提取和识别的准确度不高，因此打标数据的准确率也参差不齐，这是未来需要不断提升的方向。

相较于数据安全，数据安全治理强调建立一套完善的管理体系，包括组织架构、管理制度、流程规范等。第一梯队的银行已经建立了数据安全治理的基础框架，并在持续优化流程建设。相比之下，第二、三梯队银行的关注重点仍在构建足够的数据安全防护能力上。

银行的数据安全平台建设进程也在不断加快，一方面由于该类产品的成熟度不断提升，数据安全整体管控能力不断增强；另一方面，银行也亟需实现对数据泄漏的发现、防护、溯源和定责。第一梯队的银行更倾向于通过自主研发或与安全厂商合作的方式，定制化开发平台，第二梯队的银行业主要是直接采购安全平台，来不断加强数据生命周期管控能力。

隐私计算一直是银行业的重点关注领域，虽然其理论方法尚不成熟，但部分头部银行已经针对联邦学习、同态加密、多方安全计算等技术涉及了研究课题，并尝试通过三方合作的方式进一步探索。

中国工商银行2023年年报

- 完善数据安全管理体系。①健全数据安全管理制度，2023年修订了《数据安全管理办法》等制度。②优化数据安全技术管理框架，强化数据安全技防体系，完善数据安全技术平台，沉淀标准化的数据安全技术能力。③持续推进数据安全分类分级贯标能力建设，开展数据安全风险评估和应急演练，加强培训和宣传。
- 探索隐私计算在跨机构场景的应用，联合金融同业实现基于该技术的银行间资金流水核验。

中国农业银行2023年年报

- 2023年修订《数据安全管理办法》，继续提升重点领域数据安全管控水平。
- 升级终端数据防泄露系统，开展对公客户敏感数据集中整治活动，持续提升终端客户数据保护水平。
- 强化数据出行安全管控，进一步规范数据委托处理、共同处理、对外提供等场景的管控机制和流程。
- 规范数据出境管理，完成数据出境业务场景梳理，稳步推进数据出境监管报告和评估申报工作。
- 根据数据隐私泄露事件的不同类别场景，本行制定了有针对性的处置措施。
- 隐私和网络数据安全员工培训，2023 年共千余次数据安全宣教活动，覆盖所有员工，触及 177 万人次。

中国银行2023年年报

- 落实数据安全责任，推动数据全生命周期安全防护，在金融行业内首批通过了数据安全管理认证，保障客户信息安全。
- 其加快推进隐私计算、物联网、区块链、人工智能等新技术平台的建设，覆盖超1800个业务场景。

中国建设银行2023年年报

- 制定《数据安全管理办法》，配套制定了《数据分类分级保护实施细则》《数据安全事件应急预案》专项制度。
- 优化生产数据敏感信息检查功能，实现生产数据取数后的自动化脱敏，增强数据保护能力。
- 推广数据共享安全计算平台的功能完善和使用，加快数据访问控制技术框架在数据查询、数据批量使用、数据接口调用等数据使用场景的应用 。

中国交通银行2023年年报

- 形成以数据安全办法为基本遵循，覆盖分类分级、权益影响性评估、出行出境、应急管理等领域的数据安全制度体系，推进数据生命周期重点环节的安全管控精细化、流程化。

中国邮储银行2023年年报

- 强化数据安全管理，推进数据全周期分类分级。
- 推进数据资产管理平台建设，当前，平台已建设数据资产管理、数据资产治理、数据安全管理、数据需求与服务管理、数据资产运营、数据资产及产品服务等相关功能。

招商银行2023年年报

- 针对零售客户，进一步完善覆盖个人信息处理全生命周期的安全保护体系，以及个人信息保护监督检查、个人信息投诉通道等处理机制。
- 针对公司客户，严格管控客户联系方式、账户余额、账户交易、客户营销轨迹等敏感信息，按需分级分类授权使用。

兴业银行2023年年报

- 持续推动网络安全、数据安全顶层设计，成立数据安全工作领导小组，着力做好攻防演练、安全检测、数据分类分级等工作。
- 制定《兴业银行个人信息保护管理办法》《兴业数据安全管理办法》等相关管理制度

中信银行2023年年报

- 在内部研发安全制度规范中明确信息系统在需求、设计、开发、测试、发布等阶段的数据安全保护措施，确保数据安全保护贯穿于信息系统开发全过程。
- 进一步完善内部数据安全管理制度；制定和推行数据分类分级保护策略，针对客户信息与数据划分安全级别，明确差异化管控措施；通过数据加密与脱敏、用户权限管控、安全审计等措施强化客户信息与数据全生命周期安全防护能力。

民生银行2023年年报

- 针对物联网、数字人、大模型、区块链、隐私计算五项关键技术开展新技术应用的探索与孵化，积极参与金融监管创新试点项目。

光大银行2023年年报

- 数据安全管理方面，坚持推动数据安全与业务场景相结合的管理机制，完成300 余项重点业务场景的数据安全影响评估。

图 22：上市银行 2023 年年报中关于数据安全的建设情况

g) 安全运营：

随着实战攻防演练的不断深入，金融机构的安全运营目标已从被动防御转变为主动防御、协同联动和全局集中管理，相应的安全运营重心也逐步从关注合规和基础建设，转变为更加重视威胁预警、响应、协同联动分析以及快速恢复，例如大部分的银行在 2023 年都重点加强了灾备体系的建设和切换演练全流程管理。

银行是金融系统的核心机构，因此连续的监控和快速响应是至关重要的，大部分银行都实现了7*24 的安全运营。

一、二梯队的银行通常会购买或与安全厂商共同开发安全编排自动化与响应 SOAR、威胁情报 TI、

态势感知 SOC 平台，强化自身安全运营的能力。同时，他们也积极关注 AI 安全运营技术的进展，希望通过 AI 的赋能提升安全运营效率。

相比之下，第三梯队的银行由于资源和能力有限，没有建立起安全运营体系，因此会采购渗透测试、入侵与攻击模拟 BAS、外部攻击面管理 EASM、威胁情报 TI 及重保驻场服务等服务来增强自己的安全防护能力。

攻击面管理近几年的热度较高，但这是一项长期的工作，银行也持续在资产发现与管理、漏洞发现与管理和威胁情报领域投入资源。第一梯队的银行由于其系统庞大且结构复杂，通常会自主研发平台，实现对资产及漏洞的统一发现管理，同时还会自主或联合建设运营众测平台，允许外部的安全研究人员、白帽子黑客和普通用户参与到银行系统的安全测试中，帮助发现和修复潜在的安全漏洞。在威胁情报方面，这些银行通常还会采购多家安全厂商的威胁情报作为补充，并自主开展暗网情报监测。

小规模的银行通常以采购产品或服务的方式加强自身的攻击面管理，并且不断提升对外部攻击面管理 EASM 的关注度，主要为了在实战攻防中减少外部暴露面，从而有效降低被外部攻击的风险。

中国工商银行2023年年报

- 持续健全网络安全统筹管理机制，丰富威胁情报库，提高漏洞威胁感知能力，强化互联网攻击源处置。
- 加强网络安全团队及攻防能力建设，积极推动安全攻防靶场优化升级。
- 积极开展全集团网络安全专项排查加固，完善勒索病毒攻击等网络安全预案。
- 全面升级灾备保障体系，提升重要业务系统同城高可用和异地灾备接管实战能力，推进异地自主可控灾备云平台建设。

中国农业银行2023年年报

- 强化境外机构和子公司网络安全管理，提升全集团网络安全防护能力，加强漏洞治理。
- 推进云安全防护体系建设，云容器安全工具覆盖率 100%。
- 全面建成面向业务连续性的容灾体系，推动容灾能力向更多系统模块和分行特色场景延伸，进一步加强系统应急保障能力。

中国银行2023年年报

- 建立覆盖集团的网络安全运营中心，推动集团网络安全运营中心(SOC) 有效运转，依托全领域、纵深化的网络安全防御体系，实现对系统、网络、终端、数据等各类保护对象的全面防护，具备快速有效应对大规模网络攻击的能力。

中国邮储银行2023年年报

- 自动化运维平台、安全态势感知系统等已推广至分行应用，新一代动环监控系统建成使用，不断提升运维水平。
- 加强系统灾备管理，提升灾备系统建设质量。制定灾备恢复能力等级评估模型，加大真实场景切换演练，通过一体化运维管理平台实现多系统一键式组合切换，不断完善信息系统灾备建设和切换演练全流程管理。

民生银行2023年年报

- 推行集团一体化安全运营，加强权限管理、应用安全服务及反电诈防控体系建设，守护安全运行底线。

平安银行2023年年报

- 构筑新形势下网络安全纵深防御体系，加强数据安全管控，安全风险感知和处置时效提升至分钟级。

北京银行2023年年报

- 完善信息系统安全漏洞管理，全力提升信息科技风险防范水平。持续推进服务器安全加固，优化验证安全防护措施。

青岛银行2023年年报

- 全面夯实信息科技风险管理体系，持续完善业务连续性管理体系建设和常态化风险监控预警机制。
- 建立内网入侵监测平台，建立全流程的闭环网络安全风险管理体系，动态更新安全设备防护策略，全面开展关键系统及设备切换演练。

宁波银行2023年年报

- 深化信息科技风险管控。开展信息科技全面自查和风险评估，有效识别薄弱环节，并落实整改;优化信息科技关键风险指标，强化信息科技风险监测。
- 梳理重要业务关联信息系统外部供应商连续性计划， 持续开展业务连续性演练，完善应急恢复流程与策略。

图 23：上市银行 2023 年年报中关于安全运营的建设情况

h) 密码应用：

银行的国密和商密改造工作已经取得了一定的进展，大部分银行的主要业务系统，尤其是与客户直接交互的如网上银行和支付系统的改造已经完成，农村金融机构也在进行改造，但具体情况可能因地区和机构而异。

头部银行也在探索新的密码技术，并尝试新技术与密码的结合应用，例如区块链技术在银行业的应用逐渐增多，特别是在跨境支付、智能合约、身份验证等领域，区块链的分布式账本和加密技术为金融交易提供了更高的透明度和安全性；同时，个别银行也在开展量子安全技术的专项课题和试点，以提升金融服务的安全性、效率和创新能力。

中国工商银行2023年年报

积极探索金融行业量子计算应用，在外拓业务终端试点量子密钥分发和加密功能，提升金融数据传输安全。

图 24：上市银行 2023 年年报中关于密码应用的建设情况

i) 信息技术应用创新：

在国家政策的积极引导和有力支持下，我国银行业在信创建设方面已经取得了一定的成绩。得益于日益坚实的数字化基础，目前银行在基础硬件和基础软件方面的信创完成度相对较高，近两年应用软件的信创采购比例也在明显提升，银行的信创替代正在不断深入。

同时，监管机构对于不同的银行也都提出了相应的信创建设要求，总体上要求国央企在 2027 年达到 100%的信创率，因此，政策性银行、国有商业银行和股份制银行的信创建设程度较为领先，新采购设备的信创率基本达到 100%，整体基础设施和信息系统的信创率约在 50%左右。城市商业银行的整体信创率在 30%左右，新采购的设备同样需要满足一定的信创比例。

信创产业的发展不仅依赖于国家政策的扶持，还需要技术供应商的持续创新和努力。目前，信创产品在技术、性能上和安全性仍然有很大进步空间。以国产数据库为例，一款成熟的数据库产品通常需要十多年的研发投入，但为了快速满足信创需求，很多数据库产品在底层技术上仍然会在底层封装开源数据库代码，其核心技术、知识产权、开源规则等并未实现自主可控，客户在使用这类数据库产品时将面临一系列风险，包括开源协议的合规性问题、安全漏洞的及时修复、知识产权的保护、代码的安全性以及开源项目的持续性等，也会导致数据安全的威胁。内核是否完全自研、具备完整的知识产权、能够支撑大型生产系统稳定运行等，是衡量国产数据库是否真正实现安全可控的重要指标，也是国产数据库厂商需要不断进步、提升的方向。

安全负责人的思考与洞见

- 0day 漏洞，软件供应链攻击，社工攻击，业务逻辑层面的风险滥用，数据的使用流转安全这五类威胁，仍然是我们需要去持续应对的网络安全问题。
- 银行业在新技术的接受和应用上处于领先地位，然而，业内对待新技术的态度，不应该是“为了用新而用新”，在引入新技术前，应首先评估自身是否真正需要这些技术，并确保在架构、技术、安全等方面做好充分准备，以支撑新技术的应用。
- 安全人员应该将安全数据和业务更紧密的结合起来，帮助业务部门提高攻击防御和反欺诈的能力，通过这种方式，业务人员能够更直观地认识到安全的关键作用，从而促进安全的持续发展。
- 银行业的网络安全成熟度相对较高，过去大家过于关注建设，忽视了对安全产品功能充分使用。随着当下建设节奏的放缓，反而为行业提供了一个很好的机会，让大家可以沉下心，深入挖掘并释放已有安全产品的功能和潜力，更好的发挥安全的价值。有时候，放缓步伐也是一种加速前进的方式。
- 国产安全产品仍有很大的改进空间，甲方用户更了解自身的实际安全需求，因此乙方不应闭门造车，而应深入一线，了解用户的具体需求，使产品功能更贴合用户的实际需要。

- 目前，终端设备上的安全产品数量过多，既对设备性能有较大消耗，还会导致不同产品之间的冲突，而冲突引发的问题又难定责，给员工的工作带来了诸多不便。因此，希望未来有一到两款产品，能够全面覆盖终端安全的解决能力。
- 金融行业的监管要求非常严格，一旦出现问题就会面临处罚，金融机构在采购安全产品时，经常要面对“买了不一定能解决问题，不买不一定就会出问题”的挑战，因此，金融行业需要大量的定制化产品和解决方案。希望安全供应商能针对金融行业的特点，提供具有定制化和开放性的功能和策略，并将这些需求标准化，以降低交付成本，并提高安全效果。
- 随着金融行业的数字化转型加速，暴露面扩大，攻防对抗性增强，提升安全重要性并加强风险管控的优先级变得尤为关键，这是确保数字化转型平稳进行的基础。同时，随着数字化转型的深入，金融行业在安全管理和业务效率之间的矛盾也将日益凸显，因此，金融安全领域也需要实现自身的数字化和自动化，以适应不断变化的安全挑战。

（二）保险业网络安全市场分析

政策解读

保险业的网络安全政策、法规和规范是保障行业稳健运营和客户信息安全不可或缺的基石。它们围绕保险数据的全生命周期，包括采集、存储、处理、传输和使用等环节，设定了明确的管理要求和标准。为确保业务的合规性和客户信息的安全性，保险业必须恪守国家法规，如《网络安全法》和《个人信息保护法》。这些法律为行业提供了数据保护、隐私维护和网络安全事故应对的核心指导。此外，行业内也细化落实了一批相关政策、法规和规范，为保险业提供了网络安全组织架构、人员培训、安全审计和风险评估等具体的实践指导，以确保行业在应对网络安全挑战时能够迅速、有效地采取行动。表 2 展示了《网络安全法》施行以来，保险业制定的网络安全政策、法规和规划。

表 2:《网络安全法》施行以来保险业制定的网络安全政策、法规和规划

发布时间	政策法规	政策解读
2020 年 9 月	《中国银保监会监管数据安全管理办法(试行)》	该管理办法由中国银保监会发布，针对保险业网络安全保障提出了明确要求。它强调保险机构需建立健全监管数据安全治理架构，加强数据安全风险防控，确保监管数据的完整性、可用性和保密性。对于保险业而言，这一管理办法的出台意味着监管对数据安全的重视程度再度提升，要求保险行业在保障数据安全方面采取更为严格的措施。这不仅有助于提升保险业整体的数据安全水平，防范潜在的网络风险，还能促进保险机构在数字化转型中更加注重数据安全和隐私保护，进而推动保险业的稳健发展。

2020 年 12 月	《互联网保险业务监管办法》	该办法由中国银保监会发布。它明确了互联网保险业务的定义和范围，提出了对互联网保险业务的市场准入、经营行为、监督管理等方面的具体要求。其中提到保险机构应加强网络安全保障，确保互联网保险业务的数据安全、系统安全和信息安全。这一规定对保险业的意义在于通过强化网络安全管理，提升了互联网保险业务的风险防范能力，保护了消费者信息安全，维护了市场稳定。同时，这也推动了保险业在数字化转型中更加注重网络安全建设，促进了行业的健康发展。总体而言，网络安全要求的加强为保险业在互联网时代的安全运营提供了有力保障，提升了行业的整体竞争力和服务质量。
2021 年 12 月	《保险科技“十四五”发展规划》	该规划由中国保险行业协会发布。这是我国保险行业首次以行业共识的方式发布保险科技领域中长期专项规划。规划内容分为四个部分，包括发展形势、指导思想、基本原则、发展目标、重点任务和保障措施等，旨在推动保险行业数字化转型和高质量发展。其中强调了保险行业在数字化转型中网络安全的重要性，并提出了加强网络安全保障、完善网络安全治理体系、提升网络安全防护能力等措施。相关内容明确了网络安全是保险业科技发展的重要基石，是保障客户信息安全、防范网络风险、促进业务创新的关键所在。通过加强网络安全建设，保险业能够提升风险防范能力，确保业务的稳定运行，同时也有助于推动保险行业的数字化转型和高质量发展。因此，保险业应深入贯彻落实规划中关于网络安全的要求，不断提升网络安全保障水平，为保险业的稳健发展提供有力支撑。
2022 年 1 月	《关于银行业保险业数字化转型的指导意见》	该指导意见由中国银保监会发布，针对银行业和保险业网络安全提出了明确的要求和指导。该意见强调，在数字化转型过程中，保险业应高度重视网络安全，加强网络安全风险管理和防范，确保业务系统的稳定运行和客户信息的安全。为此，意见提出了完善网络安全治理架构、加强网络安全技术研发和应用、提升网络安全防护能力等一系列措施。对于保险业而言，该意见的发布具有深远的影响和意义。首先，它明确了网络安全在保险业数字化转型中的重要地位，提升了行业对网络安全问题的关注度。其次，通过加强网络安全风险管理和防范，该意见有助于提升保险业的整体风险防控能力，保障业务的稳健运营。最后，该意见还鼓励保险业加强网络安全技术研发和应用，推动行业在数字化转型中实现技术创新和突破。总体来说，该意见为保险业在数字化转型中保障网络安全提供了有力的指导和支持，有助于推动行业的健康、稳定发展。

2022 年 12 月	《银行保险监管统计管理办法》	该管理办法由中国银保监会发布，强调了保险机构在网络安全方面应承担的责任，包括确保监管统计数据的真实性、准确性和完整性，加强数据安全保护，防止数据泄露和滥用。同时，该办法还明确了监管机构在网络安全方面的监督职责和权力。对于保险业而言，其发布和实施具有重要意义。首先，它提升了保险业对网络安全的重视程度，促使保险机构加强网络安全建设和管理，提升风险防范能力；其次，该办法有助于规范保险业的监管统计行为，提高监管数据的质量和可靠性，为监管部门提供更为准确、全面的信息支持。通过加强网络安全和监管统计管理，该办法有助于推动保险业的数字化转型和高质量发展，提升行业的整体竞争力和服务水平。
2023 年 7 月	《关于促进网络安全保险规范健康发展的意见》	该意见由工信部和国家金融监督管理总局联合发布，旨在促进网络安全保险规范健康发展。该意见针对完善政策标准、创新产品服务、强化技术支持、促进需求释放、培育产业生态等五方面提出了 10 条意见，以加强网络安全保险的发展。其中包括提升行业认知、完善行业规范、丰富网络安全保险产品、创新保险服务模式、提升风险量化评估能力、加强全生命周期风险监测、推进网络安全保险落地应用、促进企业网络安全能力提升、培育网络安全保险优质企业以及加强网络安全保险推广等。
2023 年 12 月	《关于组织开展网络安全保险服务试点工作的通知》	该通知由工信部正式发布，旨在引领和推动网络安全保险服务走向规范化发展，并通过试点工作，积极探索网络安全保险服务的新模式和新路径。通知中不仅强调了网络安全保险服务的重要性和未来的发展方向，还为保险业注入了新的活力和发展机遇。通过试点工作的实施，保险业将更深入地理解网络安全风险，进而提升其风险评估和管理能力。此外，试点工作的实践也将为保险业积累宝贵的经验，为未来网络安全保险服务提供更为成熟和完善的产品和服务。总体而言，该通知的发布将助推保险业在网络安全领域的创新与发展，从而增强行业的整体竞争力，并提升服务水平和质量。
2024 年 1 月	《科技保险业务统计制度》	该制度由国家金融监督管理总局办公厅发布，旨在贯彻落实国家的创新驱动发展战略，支持科技自立自强，通过保险力量促进创新型国家的建设以及重大科技创新的进展。其主要内容包括对科技保险业务的统计要求，明确了统计内容、填报机构、统计报表勾稽关系等，特别指出了科技活动风险保险业务和科技活动主体保险业务的分类与定义，如网络安全保险、人才创业保险等。该制度要求保险公司强化科技保险业务数据治理，优化信息系统建设，建立健全对科技保险产品、科技活动主体的识别及管理机制，从而提升保险业在网络安全和数据安全方面的管理和服务能力，确保数据的真实性、准确性和完整性，促进保险业的高质量发展。

资料来源：数说安全根据公开资料整理

2023 年，工信部与国家金融监督管理总局在保险行业细分领域联合发布了具有里程碑意义的政策文件《关于促进网络安全保险规范健康发展的意见》（如图 25 所示）。这一文件的出台，标志着我国网络安全保险行业正式迈入规范化、健康化的发展轨道。通过实施相关措施，将有力推动网络安全保险行业的有序发展，提升行业企业应对网络安全风险的能力，为中小企业数字化转型提供坚实保障，并构建起完善的网络安全社会化服务体系。这不仅有助于提升我国制造业和网络安全领域的整体实力，更将为建设制造强国和网络强国注入强大动力。

资料来源：数说安全根据公开资料整理

图 25：《关于促进网络安全保险规范健康发展的意见》框架内容

以上所提及的政策、法规和规划共同构筑了我国保险业网络安全的坚实基石。它们不仅凸显了技术安全措施的关键性，还加强了对个人信息保护的法律约束。鉴于技术的飞速发展和网络安全挑战的日益严峻，保险业必须与时俱进，持续更新和完善这些政策、法规和规范。特别是在云计算、大数据和人工智能等前沿技术的运用中，以及网络安全保险服务的探索过程中，保险业更应确保技术的安全性和合规性，从而为客户提供更加稳健可靠的服务，为市场注入更多信心与活力。

保险网络安全建设现状及关注点

截止到 2023 年 6 月，我国不同类型的保险机构有 240 家，具体情况如下图所示。

资料来源：数说安全根据公开资料整理

图 26：保险业机构分类情况及主要功能

保险行业的市场集中度较高，大型保险集团（控股）公司通常拥有包括寿险、财险在内的多个子公司。头部保险机构占据了市场上的较大份额，根据 2023 年原保费收入的统计数据，中国人保、中国人寿、平安保险和中国太平洋保险的保费收入占据了我国总体原保险收入的将近 50%。

保险机构的组织架构通常包括集团总部、子公司、区域办事处、营销服务部等多层次机构，形成了一个层级分明的管理架构。在网络安全方面，这种多层次的结构也同样适用。以中国人寿为例，该公司已经建立了一个多层次的网络安全组织架构，有效地保障了人寿集团的网络安全建设。

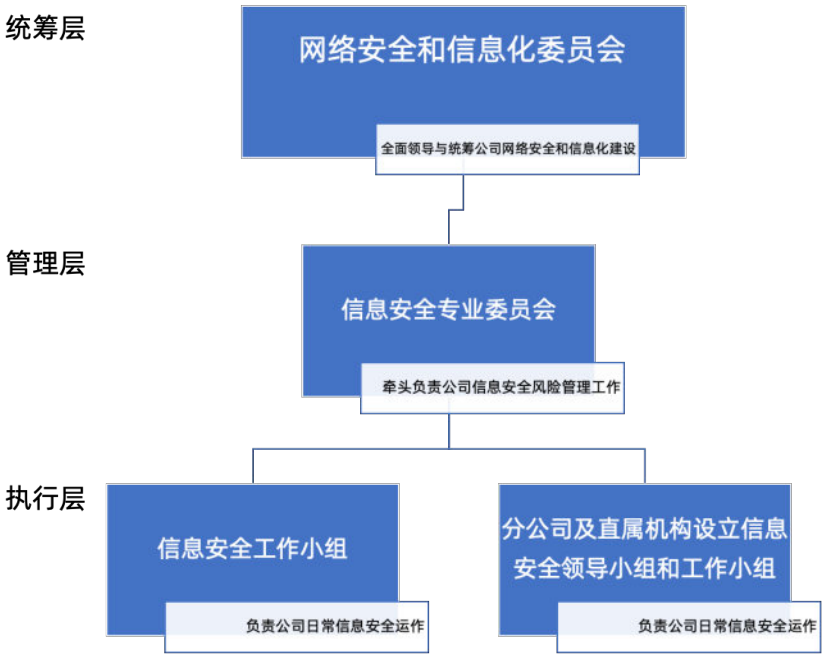


图 27：中国人寿保险股份有限公司网络安全组织架构图

◆ 安全建设现状：

由于市场的高度集中，因此头部险企是保险行业网络安全建设的重要参与者。通过分析这些头部险企近年的网络安全采购情况，我们发现它们的安全体系已经较为完善，鉴于保险行业涉及大量个人隐私信息，业务操作中对客户信息的真实性、数据分析的可靠性以及与第三方共享协作的保密性有着较高的要求。因此，这些公司的网络安全建设重点集中在身份与访问管理，个人信息和数据的安全保护、隐私计算以及安全运营等方面。

a) 基础终端及网络安全

近年来，随着等级保护合规、实网攻防演习以及数字化转型的推进，大中型保险公司已经逐步构建起基本的网络安全防护体系。他们通常已经采购了网络终端准入 NAC、数据泄露防护 DLP、防病毒、防火墙 FW、Web 应用防火墙 WAF 和网络检测与响应 NDR 产品。特别是在疫情期间，远程工作成为保险行业的主流趋势，同时随着保险公司的数字化转型，定价核保、营销分销、理赔处理等在内的环节越来越多地采用线上方式，线上业务比例逐年提高，客户也愈发依赖移动应用进行保险的相关操作，因此自 2020 年起，大中型保险公司开始加强移动应用的安全防护。

观察发现，领先的保险公司已经开始部署终端检测与响应 EDR 系统以及网络流量分析 NTA 等设备。

b) 云安全

国内的大型保险企业普遍采用云化分布式的 IT 架构，构建了以私有云为主、公有云为辅的混合

云平台。在云技术应用方面，近两年头部保险企业的上云速度显著加快。比如，中国人民保险集团已经完成了核心应用的全面改造并成功上云；太平洋保险则建立了基于全栈信创技术的保险云原生平台。截至 2023 年，中国太平洋保险已经完成了四朵云的建设，涵盖了从验证、开发测试到生产灾备云的各个阶段，并实现了超过 50 个应用的云上运行。中国人寿已经实现了重点产品的云原生化。

从安全角度来看，云安全的建设略显滞后于上云的速度。目前，虽然多数保险企业已经部署了云主机防护系统，但在容器安全方面的使用率和覆盖范围仍然有限。2023 年头部保险企业明显加大了对云安全的投入。例如，人保科技启动了云安全管理平台建设项目，旨在建立面向云环境的安全管理体系和安全运营规范。

c) 身份与访问管理

保险机构机已经建立了基础的身份与访问管理系统，大部分险企已经购买了堡垒机、特权账号管理、多因素认证、统一身份管理平台 IAM 等系统。在 2022 年，作为信创试点，大部分险企开始采购国产化终端和堡垒机，进一步加强身份与访问管理。目前，部分险企已经开始探索零信任技术，并部署了零信任系统，以满足公司员工安全远程工作和移动办公的需求。

d) 开发安全

随着保险业数字化转型的加速，构建敏态的业务逐渐成为保险机构建设的共识。大型头部险企普遍已经建立了 DevSecOps 体系，该体系整合了敏捷开发和持续集成/部署工具 CI/CD、应用程序安全测试 AST，并且定制化或自主研发了开发安全管理平台。

对于中小型险企来说，它们尚未建立起完整的开发安全体系，而是主要通过购买代码审计相关服务以及基础工具如 AST 来保护代码安全。

e) 数据安全

近两年，数据安全的防护和个人信息保护体系的建立成为了保险行业的重点关注领域。过去几年，头部险企在数据领域的投入持续增加，它们通过自主研发或巨额投资，引入了一系列大数据技术产品和服务。同时，通过合资或外部采购的方式，建设了适用于保险行业的大数据应用平台。在业务需求和合规要求的推动下，这些企业普遍已经建立了基础的数据安全防护体系。自 2021 年起，头部险企开始通过自建或定制开发的方式建设数据安全管理平台，实现对数据全生命周期的管理。

隐私计算也是保险业重点探索的领域，尽管对隐私计算新技术的应用和研究有待提升，但是部分头部险企已经建设了隐私计算平台，以实现内部数据能力整合，更安全引入外部数据能力，充分发挥数据智能在保险业务中的应用价值。

中国太平洋保险2023年年报

- 成立网络安全和信息化领导小组，统筹推进数据安全管理工作落地。制定更新《数据安全管理暂行办法》《应用系统信息安全管理办法》等制度。
- 建立数据指标监控体系，规划实施“DiTP 数智安全运营项目”，加强网络安全、数据安全、智能运营等重点环节的管理。
- 面向专业人员组织应用防范社工攻击、开发安全持证、信息安全专业技能等培训，围绕数据安全制定应急预案并定期开展演练。

中国人民保险2023年年报

- 加强数字化顶层设计，成立集团数字化发展委员会，统筹领导集团数字化建设和发展工作，并优化集团信息化建设委员会数据治理委员会职能，统筹推进集团信息化建设和数据治理工作。
- 优化数据中心异地双活数据备份布局架构，北方信息中心投产运营，保持信息系统安全稳定运行，加快建立健全自主可控安全高效的金融基础设施体系，加快推进隐私计算、物联网、区块链、人工智能等新技术平台的建设，覆盖超1800个业务场景，网络安全防护和管理水平逐步提升。

图 28：上市保险公司 2023 年年报中关于数据安全的建设情况

保险行业在个人信息保护方面起步较晚，整体体系建设相对薄弱。但在近两年的严格监管推动下，个人信息保护逐渐成为行业的重点关注领域之一。作为个人信息密集型行业，保险业在个人信息的收集、储存和使用方面体量大、范围广、敏感度高，涉及复杂的业务流程。随着保险科技的发展和业务范围的扩大，个人信息的开发运用变得更加多元化，保护工作面临更多挑战和风险。特别是对于机构复杂的大型保险机构，如何平衡各部门间的个人信息保护工作，同时实现业务的可持续发展，成为一大难题。

f) 安全运营

为了应对监管机构日益常态化的实战化演练，保险机构普遍加大对产品或服务的采购力度，以提升攻击面管理能力。大型保险企业持续在资产发现、漏洞管理和威胁情报方面加大资源投入。领先的险企已经建立了漏洞管理平台，并自营或与其他机构合作构建众测平台。在威胁情报领域，多数保险机构倾向于采购多家安全公司的情报服务，以提高对潜在威胁的识别和响应能力。

头部保险机构通常以总部安全运营团队为中心，当地分支机构力量为支撑，构建总分一体化运营体系。目前，部分头部保险机构已实现 7*24 小时的安全运营，并采购了态势感知 SOC 平台、威胁情报 TI 等工具来强化安全运营能力。

然而，绝大部分保险机构仍主要通过采购安全服务，如重保、渗透测试、攻防演练等服务来提升运营能力。

我们还观察到近期部分头部保险机构开始与外部厂商合作建设安全运营平台，以推动集团网络安全运营工作向专业化方向发展。

中国人寿2023年年报

- 完善信息系统全生命周期安全管理要求。通过开展上线前后的安全测试和质量检查，不断提升信息系统的安全性；
- 通过制定信息系统应急预案并定期演练，不断提高网络攻击或安全事件的应急处置能力；综合运用云计算、大数据等新兴技术，建设安全态势感知平台，并依托企业总控中心，建立全网联防、联动、自动化的联控机制，实现各类安全风险的集中分析和联动处置。
- 通过意识培训、宣传教育、模拟钓鱼等形式，持续强化人员信息安全意识，营造“人人讲安全”的企业文化。

图 29：上市保险公司 2023 年年报中关于安全运营的建设情况

（三）证券业网络安全市场分析

政策解读

自《网络安全法》颁布实施以来，我国证券业积极响应国家号召，深入贯彻落实网络安全政策和法律法规，以加强证券市场的信息安全为核心目标，全力保护投资者的合法权益，坚决维护市场秩序。在这一背景下，证券业内制定并实施了一系列细化的网络安全政策和规范，涵盖了网络基础设施建设、信息安全保障、数据保护、应急响应等各个方面。这些政策和规范不仅强调了技术防范和风险管理的重要性，还明确了责任主体和监管要求，确保了证券市场在网络环境下的安全稳定运行。表 3 展示了自《网络安全法》施行以来，我国证券业制定的网络安全政策、法规和规范。

表 3：自《网络安全法》施行以来，我国证券业制定的网络安全政策、法规和规划

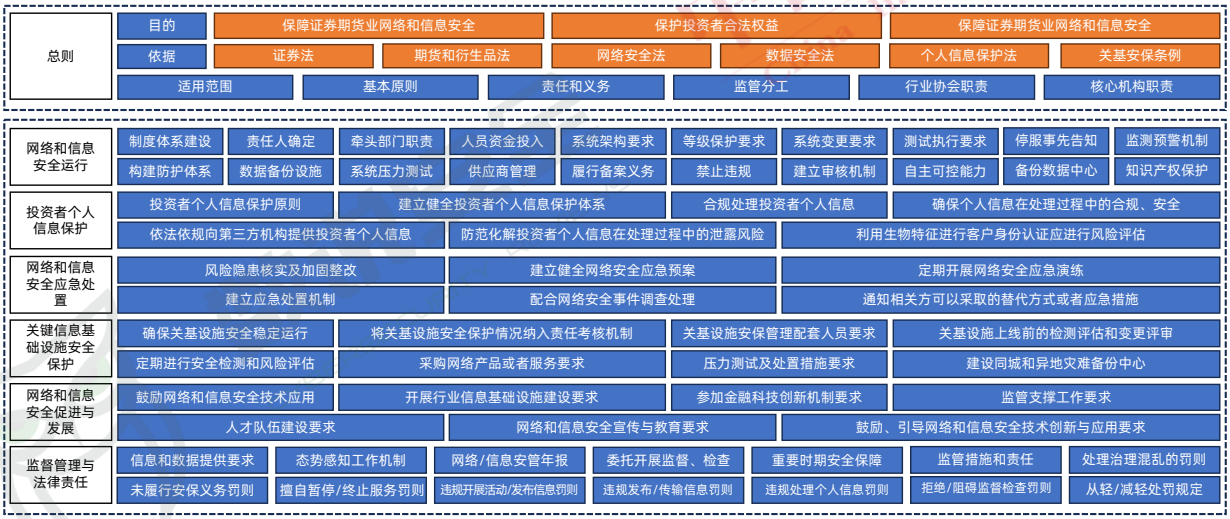
发布时间	政策法规	政策解读
2018 年 12 月	《证券基金经营机构信息技术管理办法》	该办法由中国证监会发布，系统全面地规范了证券基金经营机构在信息技术管理方面的行为，着重强调了信息系统安全、合规运行的重要性，并致力于保护投资者的合法权益。这一法规的出台，不仅显著提升了证券业的信息技术应用水平，更强化了信息安全防线，为证券市场的稳健、有序发展提供了有力保障。
2021 年 6 月	《证券期货业信息安全事件报告与调查处理办法》	该办法由中国证监会发布，旨在规范证券期货业信息安全事件的报告、调查与处理流程。办法强调事件报告的时效性和准确性，并明确了各级机构在信息安全事件中的职责与协作机制。它对证券业的意义在于提升了行业信息安全保障能力，减少了信息安全风险，同时维护了市场秩序和投资者利益。

2021 年 12 月	《证券期货业移动互联网应用程序安全检测规范》	该规范由中国证监会发布，详细规定了证券期货业移动应用的安全检测标准和流程。它通过强化移动应用的安全性，规范提升了证券业的信息安全水平，有效防范了网络攻击和数据泄露风险，保护了投资者的合法权益，并促进了证券市场的健康稳定发展。
2022 年 4 月	《证券期货业网络安全管理办法(征求意见稿)》	该办法由中国证监会发布，旨在全面强化证券期货业的网络安全管理与数据安全保障。该办法详细规定了网络安全监督管理体系、网络安全运行规范以及数据安全统筹管理等方面的要求，为行业提供了明确的操作指引。该文件的发布不仅提升了证券期货业对网络安全重要性的认识，更通过规范化管理有效减少了潜在风险，保护了投资者的合法权益，为行业的稳定、健康发展奠定了坚实基础。
2023 年 2 月	《证券期货业网络和信息安全管理办法》	该管理办法由中国证监会制定发布。它以安全保障为基本原则，对网络和信息安全管理提出了规范要求。这一办法的出台，标志着我国证券期货业在网络安全和信息安全领域的管理正式迈入更加规范化、系统化的新时代。它广泛涵盖了从关键信息基础设施运营者到核心机构、经营机构，再到信息技术系统服务机构等各类主体，为整个行业提供了清晰、明确的网络安全和信息安全指导与要求。该办法以安全保障为核心原则，对网络和信息安全管理制定了严格规范。这不仅将极大提升证券业机构在网络安全监测预警、应急处置以及风险管控等方面的能力，还将有效防范和化解行业面临的网络和信息安全风险，从而确保市场的稳定与高效运行。
2023 年 6 月	《证券公司网络和信息安全三年提升计划（2023-2025）》	该计划由中国证券业协会制定并正式发布，旨在通过加强网络安全和信息安全建设，提升证券公司在这两方面的能力。该计划明确了未来三年内证券公司需要达到的网络和信息安全目标，包括完善技术防范措施、加强数据安全保护、提升应急处置能力等。同时，它还提出了一些具体的网络安全激励政策，包括设立专项资金支持网络安全技术研发和应用，对达到网络安全标准要求的证券公司给予奖励，鼓励行业间网络安全经验共享和合作，并强化网络安全监管和评估，以全面提升证券业网络安全防护水平。这一计划的实施将对证券业产生深远影响，不仅有助于保障市场的平稳运行和客户信息的安全，还将推动证券公司不断创新和完善网络和信息安全管理体系，提升行业的整体竞争力和服务水平。

2023 年 6 月	《期货公司网络和信息安全三年提升计划（2023-2025）》	该计划由中国期货业协会制定并正式发布，致力于提升期货公司的网络安全工作能力和水平。它通过强化信息技术治理、系统运行维护以及自主研发能力等多方面措施，有效防范化解系统性风险。同时，它还提出了一系列网络安全激励政策，包括设立专项资金支持网络安全技术研发与投入，鼓励提升信息技术治理能力，加强系统运行维护管理，提高网络安全保障水平，并对培育自主研发能力给予政策倾斜，以全面强化期货公司的网络安全防护体系。这一计划的实施意味着期货公司在网络和信息安全方面将获得更为坚实的保障，有助于推动期货市场的健康稳定发展，提升行业整体竞争力，为行业的持续创新和高质量发展奠定坚实基础。

资料来源：数说安全根据公开资料整理

其中，2023 年 2 月颁布的《证券期货业网络和信息安全管理办法》（如图 30 所示），相较于证券业过往政策，展现出更为全面、细致且具有前瞻性的特点。该办法不仅广泛涉及基础设施安全、数据安全、应用安全等关键领域，还针对云计算、大数据、人工智能等新技术、新业务模式提出了具体的管理要求。此外，该办法还强调了网络安全与信息安全之间的协同管理，促进了技术防范与管理措施的融合。这一办法的出台，不仅显著提高了行业对网络安全和信息安全的重视程度，强化了风险防控能力，确保了业务的连续性和客户资料的安全，同时也推动了证券业在技术创新和业务转型方面迈出坚实的步伐。



资料来源：数说安全根据公开资料整理

图 30：《证券期货业网络和信息安全管理办法》框架内容

在这些网络安全政策和法律法规的精心指导和规范引领下，我国证券业的网络安全建设取得了令人瞩目的成绩。市场的信息安全得到了坚实保障，投资者的利益得到了周全保护。展望未来，证券业将继续深化网络安全管理，不断创新和完善相关政策和规范，为构建更加安全、高效、透明的证券市

场提供坚实的支撑和保障。

证券网络安全建设现状及关注点

根据中国证券业协会信息，截止到 2023 年 6 月 30 日，我国证券公司数量为 141 家，141 家证券公司 2023 年上半年度实现营业收入 2,245.07 亿元。

◆ 安全预算及采购情况：

目前，网络安全投入约占 IT 投入的 3%-5%，头部券商机构安全人员 10 人左右。证券机构一般由集团总公司统一进行采购，分支机构负责轻量级的 IT 运维，没有单独采购权。国内头部证券公司的网络安全建设已逐渐从前期的安全基础设施建设阶段过渡到安全运营阶段，越来越重视安全实战效果。

◆ 安全建设现状：

a) 基础安全领域

近年来随着法律法规的逐步完善，在合规性的驱动下国内大部分证券公司已经建立了基础网络安全防护体系。在基础网络安全领域方面，大型证券公司普遍采购了边界安全产品、病毒防护、网络流量分析等安全产品。终端安全方面，由于证券行业的特性，移动端的主要场景是证券 APP 访问，因此大部分证券公司在移动终端安全防护投入较小，主要侧重于对物理 PC 和笔记本电脑等设备的防护管理和病毒防护。

b) 密码和信创

密码方面，大部分券商从 2022 年开始进行国密改造，主要在数据传输环节采购了密码机等产品以满足合规的需求。但以当下的技术下交易系统难以应用密码产品，主要是由于加密过程会增加交易时间，影响交易速度。

信创方面，金融类信息和数据涉及国家和居民安全，在政策的推动下，证券行业正在加速推进信创全栈式升级改造，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。多数证券机构从 2021 年开始推进信创，网络安全领域已经进行了 30%至 40%的信创产品的替换，而对于新采购的设备，信创比例已经几乎达到了 100%。并预计在 2027 年之前实现所有相关产品的完全替代。

c) 云安全

整体来看，目前证券上云进度是缓慢的，相应的对云安全的投入也相对较小。当下部分证券公司在云方面开始了初步探索和应用，虚拟化仍是主要技术手段；证券机构会普遍采用把重要系统放在私有云，公有云的使用相对较少，通常会将新闻、资讯类应用放在公有云上，云安全的建设也主要依赖公有云厂商提供的安全产品。据调研，部分证券公司在部分系统上开始使用容器的部署方式，并采购

了容器安全产品。

d) 数据安全

证券行业的数据特点是规模庞大、价值高，应用场景复杂。因此，保护客户个人信息、交易数据、市场行情和资讯等数据对于确保交易系统的稳定运行至关重要。鉴于外部攻击形势严峻，内部数据风险加大，如数据在网络环境暴露面大、数据外发渠道多样化、员工接触数据机会多等内外部多重因素影响，证券机构面临的数据安全风险持续加大。

大部分证券公司已经采购了数据库审计、动静态脱敏、数据防泄漏等数据产品进行数据防护。通过调研得知，大多数机构对隐私计算技术依然处于关注状态，尚未应用到机构的数据安全防护体系中。整体来看，数据安全的体系建设还处于初级阶段，大部分证券机构的技术手段未能全面覆盖数据全生命周期。

大部分机构已经意识到数据治理工作是建立数据安全体系的基础，部分证券机构已经开始展开数据治理工作。然而，由于涉及繁多的数据资产梳理、多部门间协作复杂等原因，数据分类分级工作面临标准制定周期长、落地难度大、分级后难以应用等挑战。

如今，头部券商正在积极关注数据安全平台，期望通过建立数据安全平台来构建覆盖数据全生命周期的安全保障。通过调研得知，多家证券机构也表示在当前及未来三到五年内，公司的主要任务之一将是数据治理及数据安全体系的搭建，以应对日益严峻的数据安全挑战。

银河证券2023年年报

- 探索隐私计算在跨机构场景的应用，联合金融同业实现基于该技术的银行间资金流水核验。

图 31：上市证券公司 2023 年年报中关于数据安全的建设情况

e) 开发安全

在开发安全方面，近两年在数字化转型的大背景下，头部券商加大投行、财富管理、资管、自营等业务及运营、风控、财务、法律合规等中后台的数字化建设，开发需求逐步提高。但是大部分券商的开发流程和安全流程尚未完全结合起来，没有建立起开发安全的体系。目前大部分券商机构的开发安全工作主要集中在软件开发阶段，通过部署敏捷和持续集成工具 CI/CD 平台，结合安全测试工具帮助公司在软件开发阶段识别潜在的安全漏洞。另外，通过调研我们发现，还有多数机构在积极关注软件成分分析 SCA 工具，预计未来一两年内会使用软件成分分析 SCA 工具，以解决应用程序安全测试 AST 类工具误报率较高的问题。

f) 身份安全与访问控制

在身份安全方面，大多数机构采用了堡垒机、身份和访问管理 IAM、特权访问管理 PAM 等安全

产品来管理员工账号,并设立了访问控制规则。整体而言,领先的券商已经实现了对访问控制的细化,达到了应用级别的管理。

尽管零信任概念近年来备受瞩目,且其架构已经从理论走向实际应用,但券商在采用零信任相关产品时仍面临诸多挑战。零信任的改造需要与现有的网络基础设施、基础服务平台、各类资产和应用进行整合,这要求多个部门的协同合作。目前,大多数券商尚未开始零信任改造的工作。不过,一些头部券商已经开始采取行动,以替代传统 VPN 为切入点,推进零信任架构的改造工作。

g) 安全运营

目前大部分证券机构尚未实现 7*24 小时的安全运营支持,普遍是在工作日实现 5*8 的安全运营支持,而在非工作日或工作时间外,通过短信和启维的通知告警系统进行远程处理。另外通过调研,发现多数证券机构通过购买态势感知 SOC 平台、安全信息与事件管理 SEIM 等工具作为安全运营的核心工具,有能力的券商机构会与安全厂商合作自建安全编排自动化与响应 SOAR 平台等工具。此外,大部分证券机构在积极关注 AI 大模型及其相关产品的应用,未来可能用于提高安全运营的自动化和效率。

攻击面管理方面多数证券公司较重视提升外部威胁发现以及漏洞扫描的能力。部分证券机构通过资产管理系统,进行数字资产的数据采集和管理,并与内部系统进行对接。同时,这些券商通过安全运营平台结合外部情报和扫描工具来发现安全漏洞。也有头部的券商通过自建内生情报平台和外购商业情报结合的方法提升威胁检测能力。

目前,大部分券商对内部威胁管理重视度仍然不足,主要通过堡垒机和日志管理来防护内部威胁。目前有能力的券商在内、外网都部署了蜜罐,但是考虑到监管,部分券商外网蜜罐并不打开。

银河证券2023年年报

- 建立健全网络和数据安全管理体系,持续完善投资者个人信息保护机制,落实网络安全责任制,充分利用各类技术手段,加强网络和数据安全技术保障体系建设;
- 在网络边界部署防火墙、应用防火墙、流量安全检测系统等网络安全设备,部署防病毒和数据防泄露系统,防范恶意网络攻击与数据泄露风险;

华泰证券2023年年报

- 加强信息安全及客户隐私保护制度体系搭建,通过加强隐私保护、保障交易安全等举措,推进信息安全及隐私保护工作进程。

华泰证券2023年年报

- 公司持续加强信息系统安全建设,制定了完善的信息安全事件应急预案,定期对应急主预案、子预案开展评估。

中金公司2023年年报

- 建立信息安全管理机制，制定和实施信息安全计划，监控信息安全威胁；
- 建立数据治理组织架构，确保数据统一管理、持续可控和安全存储；
- 通过建立有效的问题管理流程，追踪、响应、分析和处置信息系统问题及信息技术突发事件；

图 32：上市证券公司 2023 年年报中关于安全运营的建设情况

安全负责人的思考与洞见

- 面对当前日益复杂的网络威胁环境，尤其是在勒索软件攻击和客户数据泄露事件频发的背景下，证券公司已经将安全能力的提升重心转移到更加贴近真实攻击场景的实战化建设上。为此，证券公司已经建立了定期参与网络安全演练的机制，通过模拟真实攻击，检验并不断提升自身的安全防护、监测和响应能力。券商应该积极参加实网攻防演习行动，提高实战能力。
- 数据安全应以数据治理为前提，进行数据分类分级。数据安全不是一蹴而就的，是未来3-5 年的建设重点。目前数据安全领域也存在较大的挑战，市场上的数据安全的理论和技术还停留在十几年前，建议数据安全厂商进行技术重构和价值链重构。
- 安全平台在企业的安全能力的建设中起到非常重要的作用。通过整合各种安全工具，实现自动化和安全运营的效率，减轻人力负担，尤其是对安全人员较少的金融机构，应该充分利用平台赋能，提高公司的安全水平。
- 国内的安全产品在安全防护效果上与国外的安全产品相比仍存在一定的差距。特别是在应对新型威胁方面,部分安全产品的表现欠佳，不能满足实际需求,存在较大的改进空间。因此，安全厂商应该更加贴近客户的实际需求来设计产品,提高其防护能力。尤其是在终端安全产品，大多数产品存在被绕过的风险，导致其防护能力不足。
- 提高内部管理的重要性，关注两项重点举措：一是做三年规划，用规划来统一思想；二是将技术选型和测试过程结构化，提升科学性和先进性。安全建设应该结合外部威胁以及内生业务需求，制定安全规划，通过规划引领可以确保安全建设的目标明确，避免盲目跟风。
- 由于部分证券公司网络安全已经过了大规模建设期，一些硬件的投入可能会降低，但是安全服务的预算依然维持在较高的水平。部分证券公司由于 IT 投入的下滑，安全预算可能会降低，但不需要过于担忧，随着中国在全球产业链地位的提升，安全重视程度会逐渐得到提升。

（四）基金业网络安全市场分析

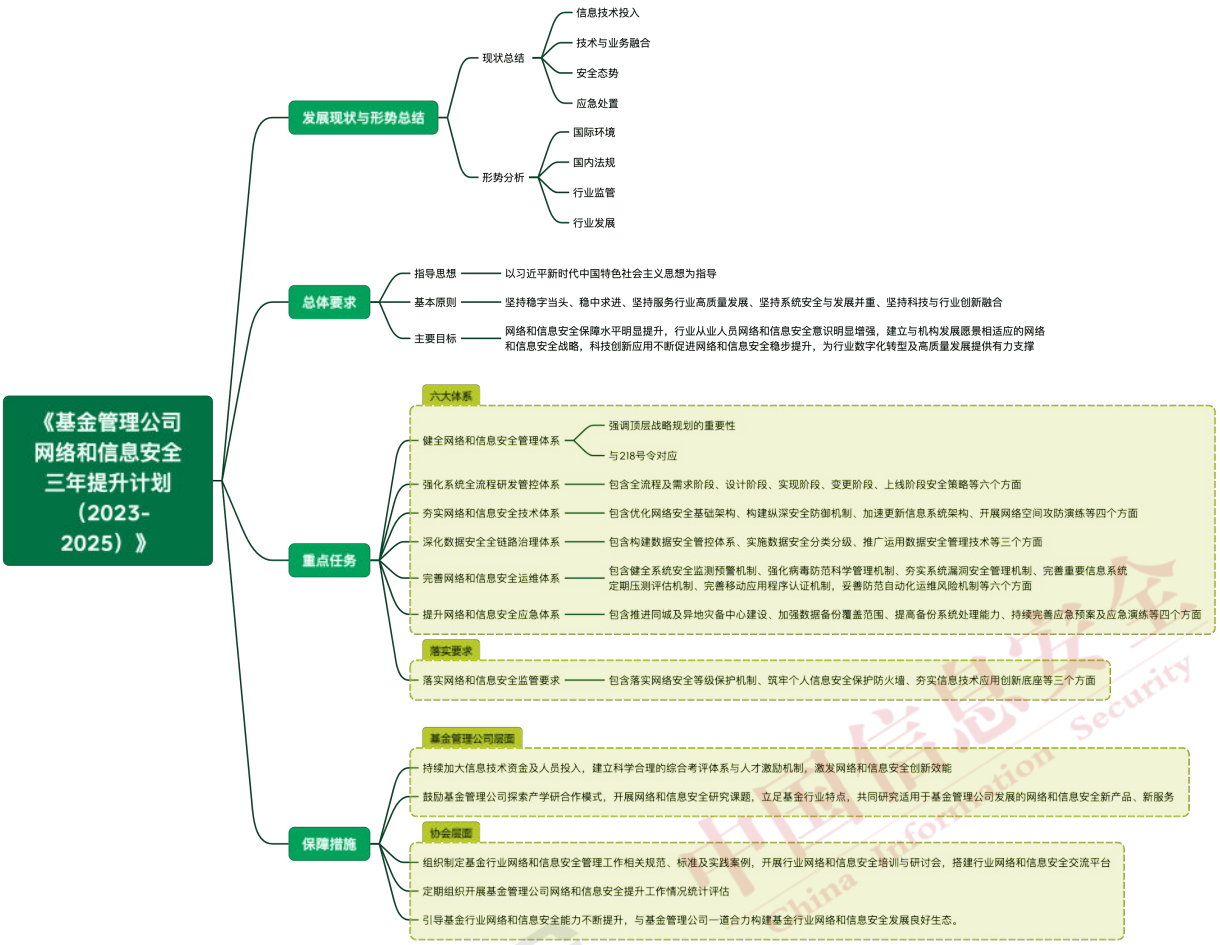
政策解读

网络安全政策对基金业的健康发展起到了至关重要的保障作用。它们不仅为基金业提供了法律法规的框架，确保业务运营符合规范并保障数据安全，还通过强化系统防护措施、完善风险管理机制，为基金业打造了一个更加稳固和安全的网络环境。自《网络安全法》实施以来，我国针对基金业颁布了一系列网络安全政策和法律法规，这些政策和法规主要聚焦于加强基金管理公司及相关服务机构的网络安全管理。它们不仅要求这些机构建立健全网络安全防护体系，提升技术防范能力，还强调了对投资者信息和资产安全的严密保护。通过这些网络安全政策和法律法规的颁布与实施，我国基金业在网络安全领域的管理水平得到了显著提升，为行业的长远发展奠定了坚实的基础。表 4 展示了自《网络安全法》施行以来，我国基金业制定的部分重要的网络安全政策、法规和规划。

表 4：自《网络安全法》施行以来，我国基金业制定的网络安全政策、法规和规划

发布时间	政策法规	政策解读
2018 年 3 月	《关于推动资本市场服务网络强国建设的指导意见》	该指导意见由中央网信办和证监会联合发布，旨在通过发挥资本市场在资源配置中的重要作用，支持和促进网信企业创新发展，以推进网络强国和数字中国建设。对于基金业来说，这一指导意见的发布意味着资本市场对于网络信息技术产业的支持力度加大，为基金业提供了更多的投资机会和市场空间。同时，指导意见还强调了保障国家网络安全和金融安全的重要性，这也有助于提升基金业的风险管理能力和市场竞争力，促进行业的稳健发展。
2023 年 2 月	《证券期货业网络和信息安全管理办法》	该管理办法由中国证监会制定发布，全面规范了证券期货业网络和信息安全的治理架构、基本制度、保障措施和监督责任。针对基金业而言，这一管理办法的出台进一步强化了基金业务的信息安全保护，有效防范了网络攻击和数据泄露，确保了基金运作的稳定性和投资者资金的安全，促进了基金行业的持续健康发展。
2023 年 6 月	《基金管理公司网络和信息安全三年提升计划（2023-2025）》	该计划由中基协制定并发布，重点聚焦基金管理公司在网络和信息安全领域的核心挑战和发展需求。主要内容涵盖强化技术防护、完善信息安全管理体系、提升应急处置和风险管理能力等方面，旨在确保基金管理公司能够有效应对网络安全威胁，保护投资者利益和市场稳定。该计划的实施不仅将提升基金管理公司的信息安全水平，还将促进证券市场的健康发展，增强投资者信心，为行业的长期稳健发展奠定了坚实基础。

资料来源：数说安全根据公开资料整理



资料来源：数说安全根据公开资料整理

图 33:《基金管理公司网络和信息安全三年提升计划（2023-2025）》框架内容

其中，中基协于 2023 年 6 月新颁布的《基金管理公司网络和信息安全三年提升计划（2023-2025）》（如图 33 所示）以其前瞻性的行动计划和创新性，凸显了其在网络安全领域的独特地位。相较于过去基金业所发布的网络安全政策，该计划展现出了更为全面的视角、更为系统的规划，以及对未来安全趋势的敏锐洞察。它不仅涵盖了传统的网络安全议题，更将信息安全、数据安全等多元化安全领域融入其中，构筑了一个全方位、多层次的安全防护框架。此外，该计划为基金管理公司提供了未来三年的明确发展蓝图，确保了基金业在网络安全领域的有序和持续进步。同时，它还倡导技术创新和业务升级，激励基金公司运用前沿技术和创新模式，不断提升其网络安全防护能力，以灵活应对日益复杂的网络安全挑战，确保行业的稳健发展。

这些政策、法规与规划相互交织，共同铸就了中国基金业网络安全的稳固基石，它们涵盖了信息系统安全管理的各个层面，从数据保护到风险控制，无所不包。随着网络技术的日新月异和网络安全环境的动态演变，基金业的网络安全政策和法规也在与时俱进，不断进行优化和更新。这一系列的努力确保了基金业在面对网络安全挑战时能够保持高度的警觉和应对能力，为行业的稳健发展提供了坚实的保障。

基金网络安全建设现状及关注点

根据中国证券基金业协会信息，截止到 2024 年 2 月底，我国境内基金管理公司 146 家，其中外商投资基金管理公司 49 家（包括中外合资和外商独资），内资基金管理公司 97 家；取得公募基金管理资格的证券公司或证券公司资产管理子公司 12 家、保险资产管理公司 1 家。存续私募基金管理人 21,151 家。

相较于银行、证券和保险等其他金融机构，基金行业在安全防护水平上显得略为薄弱。这种差异主要由以下因素造成：一方面，银行、证券、保险等金融机构受到了更为详尽和严格的网络安全监管标准的约束；另一方面，由于基金行业的数字化进程相对较慢，且其交易频率和资金流动性相较于银行和证券较低，因此其安全防护驱动力相对较弱。并且，国内不同基金公司的之间能力差异较大，还有很多公司处于亏损阶段或面临生存挑战，对安全的投入资金非常有限。

头部基金公司普遍已经建立了基础的网络安全体系，以满足等保合规和数字化转型的要求。当下中大型基金企业重点关注数据安全和个人信息保护的合规性方面。有能力的基金公司已经开始推进数据安全建设，制定数据安全管理制度，并梳理业务系统中的数据，推进数据治理工作。

鉴于网络安全防护的资金和人力资源通常有限，大多数基金公司自有安全能力不足，中型基金公司安全人员可能仅有 1-2 人，因此更倾向于依靠外部供应商来满足基本的网络安全合规需求。特别是许多中小型基金公司，由于它们可能仍处于亏损阶段或面临生存挑战，导致它们在安全方面的投入通常较为有限，所采取的网络安全措施也相对基础，这往往使得它们难以有效应对复杂的安全威胁和挑战。

随着投资者对专业资产管理的需求不断增长，基金行业内的竞争也日趋激烈。在这种竞争加剧的背景下，数字化能力的提升逐渐成为基金企业获取竞争优势的关键。为了在投研、风控、交易、运营、营销等多个业务场景中保持领先，基金公司正投入大量的人力物力资源，全面推动金融科技手段的应用。随着数字化转型的深入，信息安全的重要性也日益凸显，预计未来基金行业将加大对信息安全的投入和重视程度。

安全负责人的思考与洞见

- 目前网络安全建设存在诸多挑战，例如数据安全的责任归属不够明确，导致内部部门职责划分不清晰；安全人员数量有限，公司不得不过度依赖外部服务提供商的技术支持，从而影响了自身安全能力的提升；员工的安全意识有待进一步加强，信息泄露事件偶有发生；网络安全建设的步伐未能与业务发展保持同步，难以充分满足业务扩张带来的安全需求。
- 数据安全建设需要先做基础工作，不能直接购买工具就实施。基金公司当下比较关注数据安全和个人信息保护方面的合规要求，这是强监管的部分，也是当前工作的重点。基

金公司目前正在按照监管要求，进行数据分类分级和脱敏等工作。

- 公司在购买安全产品时，要充分考虑产品的适用性和效果。例如，某企业在 2019 年购买的网络 DLP 产品，虽然产品本身没有问题，但由于当时数据治理工作没做好，使用效果并不理想。现在，该企业会先做好前期准备工作，再考虑购买数据安全相关的工具。
- 希望监管部门推动行业内的交流合作，共同制定数据安全标准，并提供行业最佳实践指导，以助力企业网络安全建设的持续进步和发展。

六、金融行业网络安全发展趋势展望

（一）安全技术发展趋势

Gen AI 引领网络安全与数据安全新范式

Gen AI（生成式人工智能）与传统的网络安全窄域人工智能技术（基于机器学习和深度学习的小模型技术）相比，具有更强的知识学习和逻辑推理能力，可跨领域处理多种复杂任务，并通过强大的自然语言交互能力可以实现更广泛的场景应用。Gen AI 对整体网络安全产业的影响无疑是巨大的，未来或将在产品结构、技术创新、商业模式等多个方面重塑产业格局。从目前实际情况来看，Gen AI 在网络安全领域已经完成了多种应用场景的技术落地，并显示了初步成效。在辅助网络安全防护方面，利用 Gen AI 技术可以提高威胁检测的准确率，更为全面的实现对恶意软件、攻击流量、钓鱼邮件等网络威胁的判定；在辅助网络安全运营方面，通过 Gen AI 实现智能运营助手、威胁分析、攻击溯源、自动化处置等能力，降低网络安全事件检测与响应的时间，提升安全运营效率；在辅助数据安全方面，可以利用 Gen AI 强大的内容理解能力，达成更为自动化、高效的敏感数据识别和数据分类分级效果。

金融作为数据密集型行业，是网络攻击的主要目标，其具有高度的网络安全需求，通过 Gen AI 技术的加持，金融行业可以不断提升自身实战化对抗的能力，有力应对未来更加严峻的网络安全威胁，并在数据安全治理和个人隐私保护方面实现进一步的突破。当然，随着 Gen AI 在网络安全与数据安全领域的应用逐渐广泛，我们也必须正视其可能带来的新挑战和新风险。例如，Gen AI 技术的安全性和稳定性问题、数据隐私保护难题以及技术滥用风险等，都需要加以审慎对待。因此，金融机构在应用 Gen AI 技术时，必须充分评估这些风险，并制定相应的安全策略和措施，确保金融行业的网络安全与数据安全得到坚实的保障。

网络安全度量和安全有效性验证成为业界瞩目的新焦点

网络安全度量是用于评估和量化网络安全性能的一种工具，核心是安全有效性验证。可以提供有关网络安全性能、安全措施有效性、风险防御能力和安全投资回报率等方面的定量信息，例如漏洞数

量和严重性、事件平均检测和响应时间、合规性满足程度、用户异常行为、安全防护措施有效性等，这些定量信息与传统网络安全指标不同，它可以推动企业网络安全的决策。网络安全度量包括安全成熟度评估、实战化、自动化的网络安全防护能力验证、红队/蓝队评估、用户行为分析、安全培训和意识测评等多种方法，利用自动化攻击手段，结合丰富的漏洞库、规则库、情报库等知识库，量化评估边界防护、主机防护、邮件防护等各类防护设备策略设置、规则配置和防护能力，定位防御失效问题、发现网络和系统存在的重大风险、输出针对性防护指导意见，帮助用户单位掌握防御能力现状。企业可以根据自身实际情况和需求选择单独或组合使用这些度量方法。随着金融业务数字化程度不断深入，金融机构面临的网络安全威胁也日趋复杂多样。如何精准评估网络安全状况，及时发现并应对潜在风险，已成为金融行业亟待解决的难题。网络安全度量凭借科学的方法和手段，通过有效性、实时性、可用性等全面监测检查组织单位内安全防护措施状况，为金融机构提供了全面、客观、量化的安全评估。它不仅能清晰展现全局安全视图，为金融机构提供风险预警，更有助于其制定精准有效的安全策略，从而提升安全防护的整体水位。

未来，网络安全度量的发展将更加聚焦于数据驱动、标准化和跨平台协同。随着大数据、人工智能等技术的突飞猛进，网络安全度量将越来越依赖于对海量安全数据的深度挖掘与分析，以实现对安全风险的精准感知和预测。同时，随着网络安全法规的不断完善和行业标准的日益统一，网络安全度量将更加注重标准化和规范化，确保安全评估的准确性和公正性。此外，随着云计算、物联网等技术的广泛应用，网络安全度量将更加注重跨平台、跨领域的协同与整合。通过构建更加全面、高效的安全防护体系，网络安全度量将为金融机构提供更加全面、精准的安全保障，确保其在数字化转型的过程中保持安全和稳定。

身份管理与访问控制平台化筑牢金融安全新屏障

云计算、物联网、移动 APP 的广泛应用导致现代企业网络边界模糊泛化，依赖于固定边界的传统防御模式已经变得不够安全和可靠，因此，构建新的、以业务为中心、以身份为边界的企业安全架构变得越来越重要，这有助于企业实施更精细化的访问控制策略，减少潜在攻击面和内部威胁，实现更为灵活、自适应的网络安全防御体系，驱动身份优先机制演变并在企业数字化转型过程中提供安全支撑。

零信任、ZTNA、SASE 等技术的应用，便是将身份作为访问控制和安全决策的基础，并强调通过有效的身份管理和监控来增强安全性，但在实际落地和改造的过程中通常面临不同业务系统间存在数据孤岛现象，导致身份信息整合不完整、访问控制粒度不细致等问题，极大程度上限制了新技术的应用和发展，因此，将多个身份管理与访问控制的功能集成到一个统一的平台上，便于集中管理和自动化处理与身份相关的任务，将成为企业安全体系升级过程中的重要工作。

身份管理与访问控制平台化可以为企业最终向身份优先机制转变提供必要的技术和工具支撑，包括在一个中心化系统中管理企业所有用户的身份和权限、实现基于角色的访问控制 RBAC 或基于属性

的访问控制 ABAC、简化身份相关的流程并降低运维成本等。在数字化转型大背景下，相信身份管理与访问控制平台化将在金融行业呈现更明显的发展趋势，并在网络安全、数据安全、业务安全等多方面发挥更加关键的作用。

攻击面管理成为提升主动防御能力的新方向

攻击面管理技术受到广泛关注并非偶然，这是网络安全攻防对抗技术升级过程中的必然趋势。随着金融行业数字化和云化进程持续加速，金融机构暴露的网络攻击面正不断扩大，传统基于静态、被动的安全防护手段已经难以应对日益复杂多变的网络安全威胁。攻击面管理作为一种主动性防御技术，以其独特的视角和管理策略，将成为护航金融行业网络安全的重要手段。与传统风险评估技术相比，攻击面管理的主要特点是立足于攻击者视角，以黑客思维来发现、分析和评估企业内外部资产，以发现真实存在、可被利用的暴露面、攻击向量和风险。攻击面管理的目的是帮助防御者发现自己的盲区，并合理排定防御工作的优先级，以此来推动企业防御体系的不断优化。在攻击面管理技术应用中，目前主要分为面向企业内部资产的网络资产攻击面管理 CAASM 产品和面向企业互联网/外部资产的外部攻击面管理 EASM 产品。

2022 年末发布的关键信息基础设施安全保护要求中，提出了主动防御和收敛暴露面的明确要求，金融行业作为重要的关基单位也势必会加强相关方面的投入，目前在一些头部金融机构已经开始采购攻击面管理相关产品和服务（以外部攻击面管理产品 EASM 居多），相信未来随着政策影响不断深入，攻击面管理技术在金融行业的应用将进一步扩大。

入侵与攻击模拟 BAS 技术标定金融网络安全新高度

BAS 是指通过自动化主动验证的方式，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安全防御体系有效性的一种技术，包括验证各安全设备是否正常工作、设备上安全策略与配置是否生效、检测/防护手段是否按预期运行等。BAS 为金融机构提供了一种实战化的安全验证方式，能够精准识别安全防御体系的缺陷，进而实现防御策略的优化和增强。相较于传统的经验型防御手段，BAS 验证的方式更有针对性和实战性，可以有效应帮助金融机构应对复杂多变的网络攻击。同时，区别于传统防御视角，BAS 要求对攻击原理，攻击手段，攻击方式，攻击工具，以及各类漏洞利用都有深入的研究和积累。不仅需要有较强的攻击技术能力和攻防实战积累，更关键的是要求具备丰富的安全运营经验和实践的赋能。BAS 技术以其前瞻性的以攻促防理念，正逐步获得金融机构的广泛认可，同时从网络安全成熟度和安全投入来看，金融行业非常适合 BAS 类技术的应用，未来也将成为从 BAS 技术中获益的高价值客户群体。

从发展趋势来看，BAS 正在向着更简化的产品部署、更高的定制和集成能力，以及更精细的验证报告等方向不断演进。随着云计算、大数据等技术的进步，BAS 将能够更精准地模拟和预测网络威胁，为金融机构提供更为高效、精准的安全验证服务。同时，BAS 也将进一步简化产品部署流程，使得金

融机构能够更加便捷地集成和使用该技术。此外，BAS 技术还将不断提升其定制和集成能力，以满足金融机构多样化的安全需求。通过提供灵活的定制选项，BAS 可以根据不同金融机构的业务特点和安全需求，进行个性化的安全验证配置。同时，BAS 也将与其他安全技术进行深度融合，实现更为立体化的安全防护。可以预见，BAS 技术将成为金融行业网络安全验证的主流选择。随着金融行业对网络安全要求的日益严格，BAS 将在提升金融行业整体安全防护水平方面发挥更加重要的作用。

（二）安全建设展望

建设重点从安全产品堆砌向安全运营过渡

随着网络安全法和等级保护制度的日益深化，金融机构的基础安全防线已日趋坚实。然而，网络安全威胁的演变与复杂化，使传统静态、被动式的防御策略显得力不从心。以往那种以产品堆砌、“护城河式”模式的安全架构，虽然看似层层设防，但在现代网络攻击面前，其效果已经越来越有限。

当前，金融机构正面临安全理念转型的时期，其安全建设的重点除了持续优化安全防御体系，还应重视安全运营能力的提升。这一转型不仅是技术进步的体现，更是应对复杂网络环境、提升自身实际防护能力的关键。安全运营的本质是在于构建一个动态的防御体系，通过持续监控、深入分析、快速响应和不断优化，形成一个闭环的安全管理循环。要实现这一目标，金融机构必须转变静态防御思维，积极拥抱动态、主动的安全运营理念，不仅要建立起完善的安全监测与预警系统，实时掌握关键信息，更要能够灵活应对各种安全挑战，制定出符合自身业务需求和风险预期的安全运营策略。

攻防不对等性导致企业难以实现 100%绝对的安全，因此，企业在构建安全防线时，盲目的建设防线并不是最优的选择，更好的办法是在安全运营过程中时刻感知威胁与风险，采用更具针对性、动态的安全策略，并不断加强防御系统的韧性，保证即便发生攻击或系统被攻破，也能够及时发现、阻断攻击并快速恢复业务。另一方面，对于一些企业来说，很难衡量网络安全投资的回报率（ROI），这导致它们在网络安全方面只拥有有限的预算和资源，安全运营可以帮助他们将安全技术、安全人员与安全管理制度进行高效聚合，实现更为主动、快速、贯穿全局的防御能力，帮助企业最大程度提高系统的安全性，同时实现在有限资源下进行有效管理。金融机构安全运营体系的建设是一个长期而复杂的过程，需要持续投入和不懈努力。通过构建先进的安全运营体系，金融机构可以不断提升自身安全防御体系的水平，以更好地应对网络安全挑战。

数据安全将成为金融行业中长期建设任务

数据安全是维护金融行业客户信任和机构声誉的基石，它不仅关乎金融机构的长远发展，更直接关联到客户的隐私权益和资金安全。随着金融业务数字化转型的加速，数据量的激增和数据类型的多样化为数据安全带来了前所未有的挑战。同时，网络攻击手段的不断翻新和攻击者策略的日益狡猾，要求我们必须持续提升数据安全防护的能力和水平。因此，数据安全建设已成为金融行业一项长期且

至关重要的任务。

在推进数据安全建设的过程中，我们应坚持预防为主、综合治理的方针。首要任务是建立和完善数据安全管理制度，对数据的收集、存储、使用、共享和销毁等各个环节制定严格的安全规范，确保每一步操作都有法可依、有章可循。此外，技术防护是构建数据安全防线的关键，应积极采用先进的数据加密技术、访问控制机制和审计手段，打造坚不可摧的技术屏障，防止数据泄露和篡改。同时，提升从业人员的数据安全意识同样不容忽视。通过定期培训和宣传教育，增强每位员工对数据安全重要性的认识，营造一个全员参与、共同维护数据安全的良好环境。这不仅能够提高员工的安全防范技能，还能促进安全文化的内化与实践。

数据安全领域将迎来更多挑战与机遇并存的局面。大数据、云计算、人工智能等前沿技术的应用，将为我们提供更加智能化和高效的数据安全防护手段。随着法律法规的持续完善，数据安全监管也将变得更加严格和规范，为金融机构的数据安全提供更加明确的指导和法律保障。因此，金融机构需要不断创新和完善自身的数据安全体系，积极探索和应用新的防护技术和方法。同时，应加强与同业机构、安全技术厂商以及监管部门的合作与交流，共同推动金融行业数据安全建设向更高水平发展，为金融行业的稳健运行和长远发展提供坚实的安全保障。

智能化安全运营平台将成为解锁安全运营发展问题的钥匙

安全运营初期的发展阶段，确实取得了令人瞩目的进展，充分展现了其潜力和价值。然而，在这样的背景下，我们需要意识到，仍有一些关键问题还没有被解决。首先，人才短缺已经成为制约安全运营发展的关键因素。尽管先进的技术和产品可以提升安全防护能力，但真正决定安全运营最终效果的关键仍在于人，然而一些企业中高级安全人才不足，这将直接影响安全运营的效果。同时，不同经验背景的安全人员对同一安全事件的判断可能存在显著差异，这也无疑增加了安全运营的复杂性和不确定性。因此，如何培养更多的中高级安全人才、实现人机协同、确保安全运营效果成为安全运营可持续发展的核心所在；其次，在安全运营过程中面临告警疲劳、误报、漏报等严峻挑战，这些问题不仅大大降低了安全运营的工作效率，更可能导致关键安全事件的遗漏，对企业造成巨大风险；此外，我国网安行业长期存在的异构安全生态和低开放性也是企业安全运营过程中面临比较大的挑战。由于市场上安全产品种类繁多、接口兼容性差，导致安全运营类产品与其他安全产品的联动响应变得异常困难，这不仅增加了安全运营的复杂性和成本，也会限制安全运营的发展，已经成为当前安全运营领域亟待解决的关键问题之一。

为了有效应对这些挑战，智能化将成为网络安全运营发展的一个主要方向，并在很大程度上真正帮助安全行业实现降本增效。例如，针对告警噪声等问题，智能化的安全运营平台通过 AI 技术的加持，以更科学的研判方法对海量告警事件进行关联分析与合并，在降低告警的数量的同时提升告警的质量，使得运营人员能够更容易地发现真正有价值、需要关注的安全事件；针对中高级安全人才缺乏的问题，智能化网络安全运营平台可以结合 AI 技术，将安全运营领域的高级知识和经验固化形成知

识库。这样一来，安全人员可以更加便捷地获取和应用这些知识，从而提升自己的专业能力。同时，知识库的建立也使得整体安全经验知识达到了一致的新高度，降低对中高级专家的依赖性，进一步提升安全运营的效率和可靠性。未来通过 AI 技术持续赋能，我们期待智能化的安全运营能够凭借强大的数据分析能力，不仅可以发现正在发生的威胁，更能对攻击者的潜在行动进行预测，帮助企业实现更为积极主动的防御策略，全面提升企业对抗威胁和风险的能力。

（三）重点关注领域

零信任架构可信身份与访问管理体系

随着金融业务的不断创新和拓展，金融机构面临着来自外部黑客攻击、内部人员滥用权限、数据泄露等多种安全威胁。传统的基于边界的网络安全防护模式已无法有效应对这些威胁，亟待引入更为先进的安全架构和管理体系。因此，构建零信任架构的可信身份与访问管理体系成为金融行业网络安全发展的必然趋势。零信任架构是一种全新的网络安全防护理念，其核心思想是在访问任何资源之前，必须对请求访问的主体进行严格的身份验证和授权。这种架构强调不信任任何用户、设备或系统，而是通过持续的身份验证和授权来确保只有经过验证和授权的主体才能访问特定的资源。零信任架构的价值在于能够有效降低内部和外部威胁的风险，提高网络安全的整体防护能力。

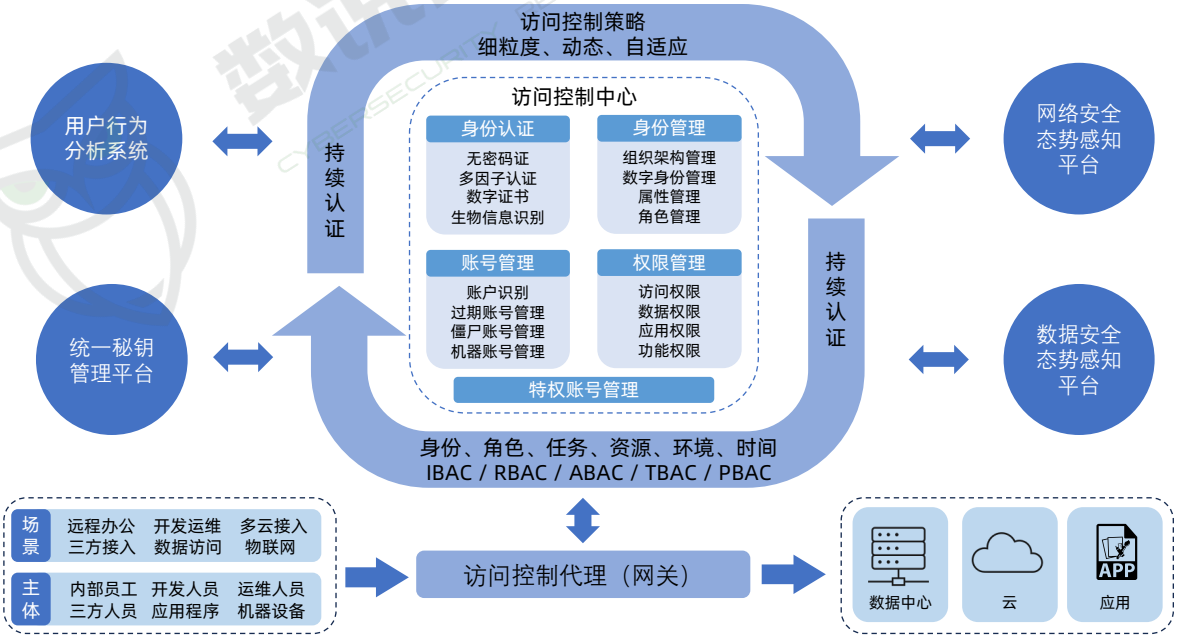


图 34：零信任架构可信身份与访问管理体系

构建零信任架构的可信身份与访问管理体系需重点关注以下几个方面：

1．制定全面的战略规划

金融机构应明确零信任架构建设的目标和愿景，制定详细的战略规划。规划应包括短期、中期和长期的建设目标，以及相应的实施计划和时间表，确保零信任架构建设的科学性、合理性和可行性，为后续建设零信任架构的可信身份与访问管理体系时提供有力的指导和支撑。

2．完善身份认证与授权机制

身份管理是零信任的核心能力。金融机构应建立完善的身份认证与授权机制，识别所有的访问者，包括人、设备、应用等，并对系统中的多个身份管理系统进行联邦管理，通过无密码认证、生物信息识别，多因子认证等手段进行持续验证，确保用户身份的真实性和可信度。同时，根据业务需求和安全策略，制定合理的访问授权策略。通过动态授权、最小权限原则等手段，确保用户只能访问其被授权访问的资源，降低安全风险。

3．建立持续信任评估与动态访问控制能力

在访问过程中，需要持续地对访问主体进行信任评估。这包括对访问主体的行为、位置、设备状态等进行实时监控和分析，以及对其历史访问记录进行审计。通过这些信息，可以实时地评估访问主体的信任度，从而动态地调整其访问权限。同时，基于信任评估的结果，实现对访问主体的动态访问控制。这包括根据访问主体的信任度动态地调整其访问权限，以及在其信任度降低时及时采取相应的安全措施，如限制访问、强制下线等。

4．协同数据安全、网络安全与终端安全能力

在构建零信任架构时，应确保所有敏感数据都经过加密处理，并在传输和存储过程中得到充分保护。在网络控制技术中，利用软件定义边界（SDP）技术隐藏内部网络结构和服务，仅允许经过验证和授权的访问；或采用微隔离技术（MSG）隔离不同系统和服务之间的通信，减少潜在的横向移动攻击面。此外，终端作为资源访问的重要主体，其安全管理与防护是零信任安全能力的关注重点，包括终端安全管理（终端准入、补丁分发与漏洞修复）、终端防病毒、终端检测与响应（EDR）、主机安全与系统加固、终端数据防泄露等。

5．构建全面安全分析与持续监测能力

在零信任架构中，全面的安全分析能力与技术是策略引擎的核心组成部分，包括网络监控、终端监控、威胁情报、用户行为分析、关联性分析引擎等，根据对多维度的信息的关联分析，以支持给零信任策略引擎做出判断并下发合适的策略，从而实现对网络、终端、用户等全方位的安全监控和威胁识别。此外，零信任架构的建设是一个持续的过程。金融机构应建立完善的监测与评估机制，定期对网络安全状况进行监测和评估。通过收集和分析安全日志、漏洞扫描报告等信息，及时发现和应对安

全威胁，确保网络安全的持续稳定。

6．加强安全培训与意识提升

构建零信任架构不仅是一个技术问题，也是一个文化问题。因此，金融机构需要加强对员工的网络安全培训，提高他们的安全意识。这包括教育员工如何识别网络钓鱼攻击、保护个人登录凭据等。只有员工具备足够的安全意识，零信任架构才能真正发挥其作用。

综上所述，构建零信任架构的可信身份与访问管理体系是一个综合性的工程，涉及战略规划与顶层设计、身份与权限管理、信任评估与访问控制、网络数据与终端安全、安全威胁分析与监测以及人员培训等多个方面。通过这些措施的实施，金融机构将能够有效应对日益复杂的网络威胁，提升网络安全防护能力，为金融业务的稳健发展提供有力支撑。

安全与业务开发运营融合 BizDevSecOps

随着金融行业数字化转型的加速推进，网络安全问题日益凸显，传统的网络安全防护模式已难以满足业务快速迭代和持续创新的需求。在这样的背景下，安全与业务开发运营融合的 BizDevSecOps（业务开发安全运营一体化）模式应运而生。BizDevSecOps 强调在业务开发运营的全流程中融入安全思维，确保在业务规划、设计、开发、测试、部署和运营的全流程中始终遵循安全原则，将传统的“事后补救”转变为“事前预防、事中监控、事后快速响应”的安全防护模式。该模式以业务为中心，通过跨部门协作，打破安全与业务之间的壁垒，实现安全团队与开发运营团队的深度融合。这种融合不仅提高了安全团队对业务的理解和参与程度，还有助于提升开发团队的安全意识和技能，从而构建更加安全、高效、灵活的业务系统。

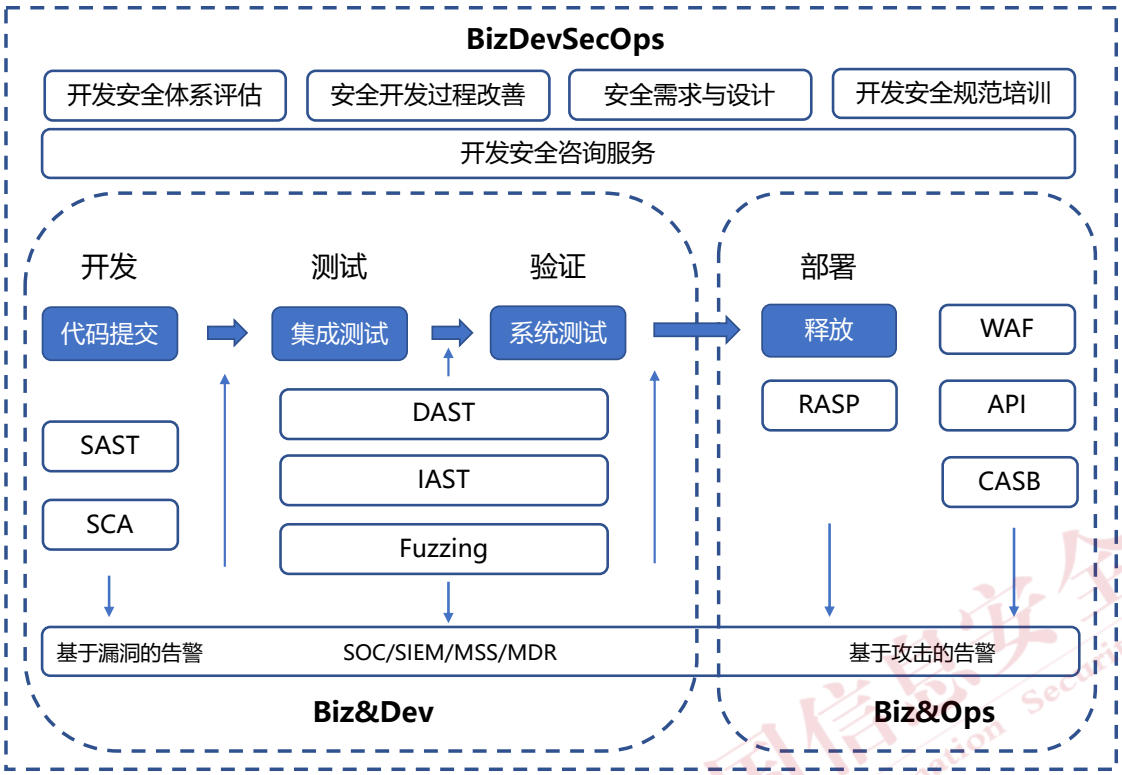


图 35：安全与业务开发运营融合 BizDevSecOps

实现安全与业务开发运营融合的 BizDevSecOps，可重点关注以下几个方面：

1．构建跨部门协作机制

建立跨部门协作机制，将安全团队、业务团队、开发团队和运维团队紧密结合起来，共同参与业务规划、设计、开发、测试、部署和运维等全流程。通过定期召开跨部门会议、共享安全信息和资源、共同制定安全标准和规范等方式，推动安全与业务开发运营的深度融合。

2．强化安全意识与技能培训

加强对业务开发运营人员的安全意识与技能培训，提高他们的安全意识和技能水平。通过定期组织安全培训、分享安全最佳实践、开展安全知识竞赛等方式，提升业务开发运营人员的安全素养，使他们能够在业务开发运营过程中主动考虑安全因素。

3．引入先进的安全技术与工具

积极引入先进的安全技术与工具，建立安全开发全生命周期管控平台，通过集成 SAST、DAST、IAST、SCA、RASP 等安全工具，实现对代码、应用和过程的持续安全监控，及时发现和响应安全事件。同时，加强对供应链安全的管理，确保使用的组件和库的安全性。通过制定供应链安全策略，建立安全审查机制，降低供应链安全风险。

4．建立完善的安全监控与应急响应机制

根据自身业务特点和安全需求，建立完善的安全监控与应急响应机制，实时监测业务系统的安全状况，发现潜在的安全风险并及时进行处置。通过建立安全事件应急响应团队、制定应急响应预案、定期开展应急演练等方式，提高应对安全事件的能力和效率。

5．推动安全与业务开发运营标准的统一

应推动安全与业务开发运营标准的统一，制定统一的安全规范和技术标准，确保业务开发运营过程中的安全要求得到一致性和标准化的执行。通过制定并推广行业标准、参与国际安全合作等方式，推动金融行业网络安全水平的整体提升。

综上所述，安全与业务开发运营融合是金融行业网络安全发展的必然趋势和重要方向。通过将 DevSecOps 的核心思想融入到 BizDevOps 中，形成 BizDevSecOps 模式，将有效提升金融行业的网络安全防护能力和水平。未来，随着技术的不断进步和业务的不断创新，BizDevSecOps 模式将在金融行业网络安全领域发挥更加重要的作用。

以“AI+业务安全”打造智能反欺诈风控体系

随着数字化、智能化的浪潮席卷全球，金融行业迎来了前所未有的变革与机遇。与此同时，网络欺诈风险也呈现出日益复杂和隐蔽的特点，对金融业务的安全稳定构成了严重威胁。为了有效应对这一挑战，越来越多的金融机构开始探索将人工智能（AI）与业务安全相融合，提高金融机构的风险识别、预警和处置能力，优化业务流程，提升客户体验，逐步实现以“AI+业务安全”为核心，构建高效、智能的反欺诈风控体系。

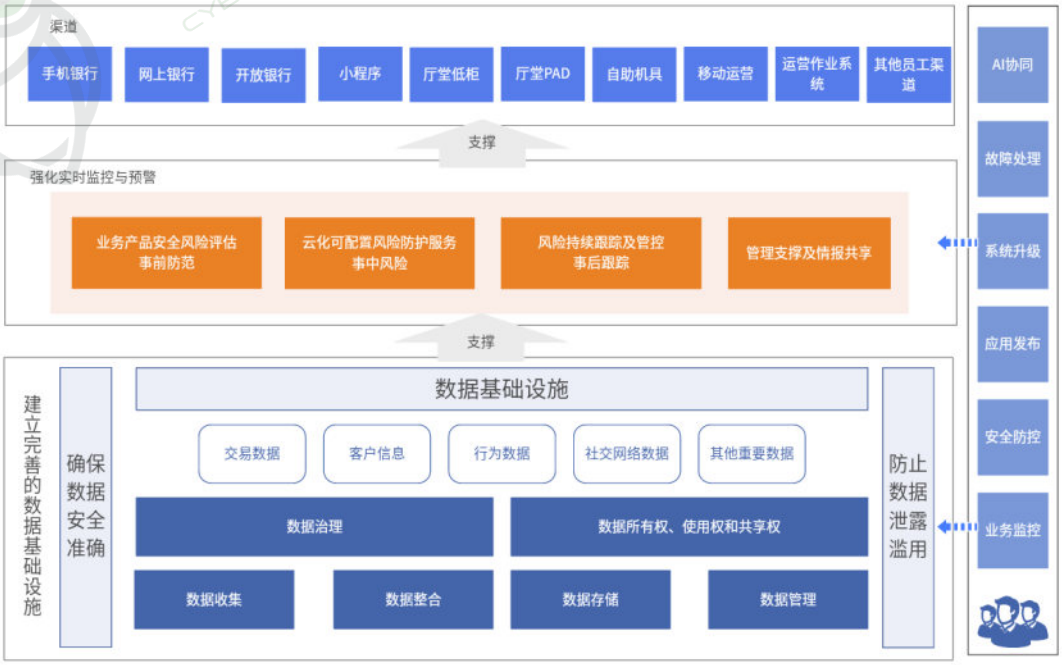


图 36：智能反欺诈风控体系

智能反欺诈风控体系的核心要素包括：数据驱动、模型算法、实时监控与预警和人机协同等，在建设过程中需重点关注以下内容：

1．建立完善的数据基础设施

构建智能反欺诈风控体系的首要任务是收集、整合和分析大量数据。这些数据不仅包括传统的交易数据、客户信息等，还包括行为数据、社交网络数据等，以全面捕捉欺诈风险的特征和趋势。为了确保数据的准确性、完整性和安全性，金融机构需要建立完善的数据基础设施。这包括建立统一的数据收集、整合、存储和管理机制，确保数据的质量和可靠性。同时，金融机构还需要制定严格的数据治理政策，明确数据的所有权、使用权和共享权，防止数据泄露和滥用。

2．优化欺诈风险识别模型

欺诈风险识别模型是智能反欺诈风控体系的核心组成部分。金融机构应根据欺诈风险的特点和业务需求，选择合适的机器学习或深度学习算法，对收集到的数据进行处理和分析。通过构建欺诈风险识别模型，金融机构可以自动学习和识别欺诈行为的模式，提高风险识别的准确性和时效性。为了不断提高模型的性能，金融机构还需要定期对模型进行评估和更新，以适应不断变化的欺诈手段和风险特征。这包括使用新的数据源、调整模型参数、引入新的算法等。

3．强化实时监控与预警能力

实时监控与预警是智能反欺诈风控体系的重要功能之一。通过实时监控交易行为、客户行为等关键指标，金融机构可以及时发现异常和可疑行为，并发出预警，进而快速响应、及时处置，降低欺诈风险造成的损失。为了强化实时监控与预警能力，金融机构需要建立高效的监控系统和预警机制，包括选择合适的监控工具、制定合理的监控规则、设置准确的预警阈值等。同时，金融机构还需要建立专门的团队，负责监控系统的日常维护和管理，确保系统的稳定性和可靠性。

4．建立人机协同的工作机制

虽然 AI 技术在欺诈风险识别方面具有很大的优势，但人的判断和经验仍然不可或缺。因此，金融机构在构建智能反欺诈风控体系时，需要建立人机协同的工作机制。这意味着 AI 技术与专业风控人员应该形成互补，共同应对欺诈风险。风控人员可以利用 AI 技术提供的风险识别和预警信息，结合自身的专业知识和经验，做出更加准确和及时的决策。同时，金融机构还需要加强对风控人员的培训和教育，提高他们的 AI 技术应用能力和风险管理水平。

5．加强与监管部门的沟通与合作

在构建智能反欺诈风控体系的过程中，金融机构还需要加强与监管部门的沟通与合作。这有助于确保体系的建设和运营符合相关法律法规和监管要求，同时也有助于金融机构及时了解和应对监管

政策的变化。通过与监管部门建立良好的沟通机制，可以获得更多的政策支持和资源支持，推动智能反欺诈风控体系的不断完善和发展。

6．培养专业人才队伍

智能反欺诈风控体系的构建和运营需要一批具备 AI 技术、风险管理和金融知识的专业人才。因此，金融机构应加强对员工的培训和教育，提高他们在 AI 技术、风险管理和金融领域的专业素养和技能水平。同时，还应积极引进具备相关专业背景和工作经验的人才，为智能反欺诈风控体系的建设和运营提供有力的人才保障。

综上所述，以“AI+业务安全”构建智能反欺诈风控体系是金融行业网络安全发展的重要趋势。通过建立完善的数据基础设施、优化欺诈风险识别模型、强化实时监控与预警能力、建立人机协同的工作机制、加强与监管部门的沟通与合作以及培养专业人才队伍等措施，金融机构可以有效提升业务安全水平，降低欺诈风险对业务运营的影响。同时，在这一过程中也面临着诸多挑战，如数据安全和隐私保护、模型泛化能力、技术更新迭代速度等。因此，金融机构在构建智能反欺诈风控体系时，需要充分考虑这些因素，采取有效的措施加以应对。

新一代高效主动安全运营体系建设

随着网络攻击变得更加复杂化、自动化和隐蔽化，传统的网络安全防御体系已难以有效应对持续性的安全威胁。尽管金融机构在过去已经部署了大量的安全设备，但这些设备往往来自不同的供应商，彼此之间缺乏协同作战的能力，导致检测与防护功能分散，且存在大量的误报信息。此外，这些设备难以将不同节点的安全数据自动关联起来，形成一个完整的安全事件视图。多年来，尽管金融机构采用了 SOC、SIEM 等技术方案，但由于这些方案存在产品碎片化、告警信息繁杂、事件响应流程混乱等问题，因此安全团队在应对安全事件时仍然面临诸多挑战。针对这一现状，金融机构迫切需要构建一个新一代的安全运营平台，该平台应能够实现云、管、边、端的高效协同和灵活调度，打破安全孤岛，构建一体化的主动防御体系，以应对日益严峻的网络安全威胁。

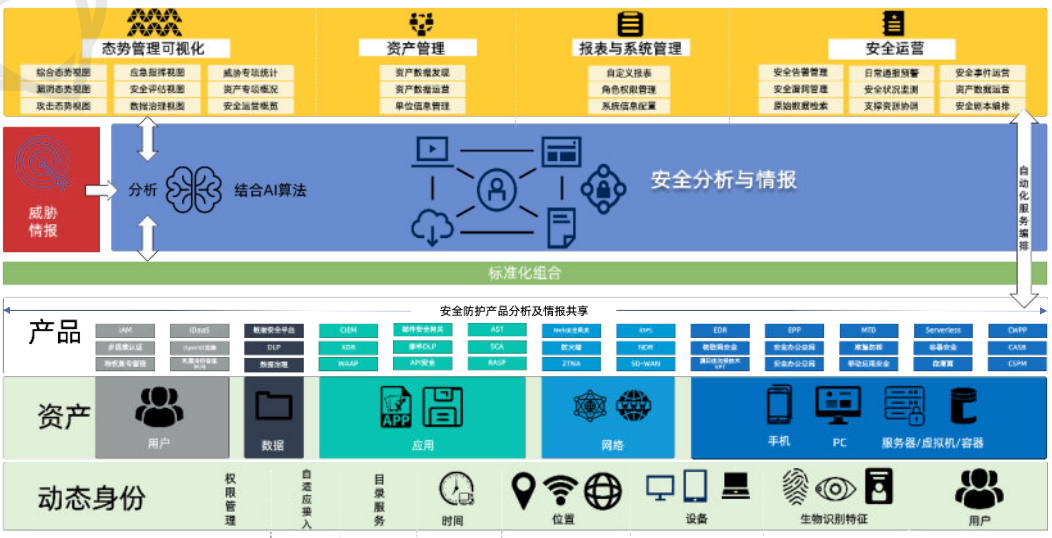


图 37：新一代高效主动安全运营体系

新一代安全运营平台需要实现技术突破，可以跨区域收集来自多种安全设施的检测数据，并对其进行统一的集成、关联和上下文等事件化分析，以全局视角进行威胁研判，从而获得更准确和全面的检测结果。同时，新一代安全运营平台旨在高效集成产品，打破信息孤岛，降低企业内的无效告警和安全运营成本，其核心能力包括以下几个方面：

1．资产识别与全面可视化

平台需要能够全面识别并可视化展现金融机构的所有资产，包括硬件、软件、数据库、云服务等，不仅限于传统的 IT 基础设施，还包括新兴的物联网设备、容器和微服务等。在识别资产的基础上，系统还需要分析这些资产的安全配置和漏洞情况。通过直观的仪表板和报告，展示资产分布、状态、风险等级等信息，帮助安全团队快速了解整体安全态势。

2．威胁情报与动态分析

平台需要从多种来源收集威胁情报，包括公开情报、私有情报、合作伙伴情报等，将收集到的情报进行整合和标准化，消除冗余和矛盾，提高情报质量。同时，能够对整合后的情报进行深入分析，提取有用的威胁信息和攻击模式，进而帮助安全团队了解最新的威胁动态，发现潜在的安全风险，并提前做出应对。

3．威胁检测与自动化响应

平台需要能够实时检测网络流量、用户行为、系统日志等，发现潜在的安全威胁。当检测到安全事件时，平台需要能够自动通知相关安全团队，并提供协作工具，帮助他们快速响应和处置。同时，平台需要提供自动化响应流程配置功能，允许安全团队定义针对不同威胁的响应措施，提高安全团队的工作效率，减少人为干预的延迟。

4．事件关联与深度分析

平台需要能够将来自不同安全设备和系统的日志、告警等信息进行跨源关联，找出它们之间的内在联系。通过上下文分析技术，能够分析事件之间的因果关系和攻击链，揭示攻击者的真实意图和手法。同时，利用数据挖掘技术，平台需要能够从海量安全数据中挖掘出潜在的安全威胁和攻击模式，并能够提供攻击模拟功能，允许安全团队模拟真实攻击场景，测试安全策略和响应流程的有效性。

5．协同作战与统一指挥

平台需要提供团队协作工具，帮助不同安全团队之间实现高效沟通和协作，能够实现安全信息的共享和交换，确保各个团队之间能够及时了解彼此的工作进展和安全事件情况。同时，平台提供统一视图功能，将各个安全团队、设备和系统的信息整合在一起，为安全团队提供一个全局视角。此外，平台提供决策支持功能，如威胁评估、风险分析等，帮助安全团队制定更加有效的应对策略和措施。

6．灵活性与可扩展性

随着技术的不断发展和安全威胁的不断变化，平台需要具备高度的灵活性和可扩展性，可提供灵活的配置管理功能，允许安全团队根据需要自定义平台的功能和界面。同时，平台需要具备良好的性能优化能力，能够处理不断增长的安全数据和流量。并能够支持横向扩展，允许通过增加节点或服务器来提高处理能力和性能。

7．AI 赋能安全运营

平台需要通过利用 AI 技术，构建一个更加智能、高效和自适应的安全防护体系，有效应对日益复杂和多样化的网络威胁。例如：利用机器学习算法，AI 可以对大量安全数据进行深度分析，以发现潜在威胁。AI 技术可以帮助安全运营平台将来自不同源的安全事件、日志和警报关联起来，形成一个完整的安全事件视图。AI 技术使安全运营平台能够自适应地调整安全策略和防护措施，以应对不断变化的威胁环境。AI 可以为安全团队提供智能决策支持，帮助他们在面临复杂的安全事件时做出快速而准确的决策。

综上所述，新一代安全运营平台通过整合多项核心能力和功能，可为金融机构提供了一个全面、高效、智能的安全运营体系。这个体系不仅能够帮助金融机构应对当前复杂多变的安全威胁挑战，还能够为其未来的业务发展提供有力的安全保障。

数据全生命周期安全治理体系构建

在企业数字化转型过程中，数据安全扮演了至关重要的角色，其建设的核心在于构建一套以数据为中心，覆盖数据全生命周期的安全治理体系。在数据风险防护与合规监管的推动下，结合具体的业务场景和生命周期的各个环节，金融机构需从数据的识别、梳理、防护、监测及响应等多个层面出发，不断建立和完善系统化、平台化的安全防护体系，进而实现在数据充分开发利用的同时，保障业务应用的持续安全发展。然而，随着网络攻击手段的隐蔽性越来越强，面对海量数据、流动数据、未知数据及未知风险的识别难度逐步提升。在以数据为中心建立安全体系的趋势下，则需要融合 AI 技术、API 安全、零信任数据安全、隐私计算、区块链、数据风险评估等新技术手段，持续构建一体化数据安全治理体系，打破传统的数据安全孤岛，让数据可以自由流转、共享和使用。

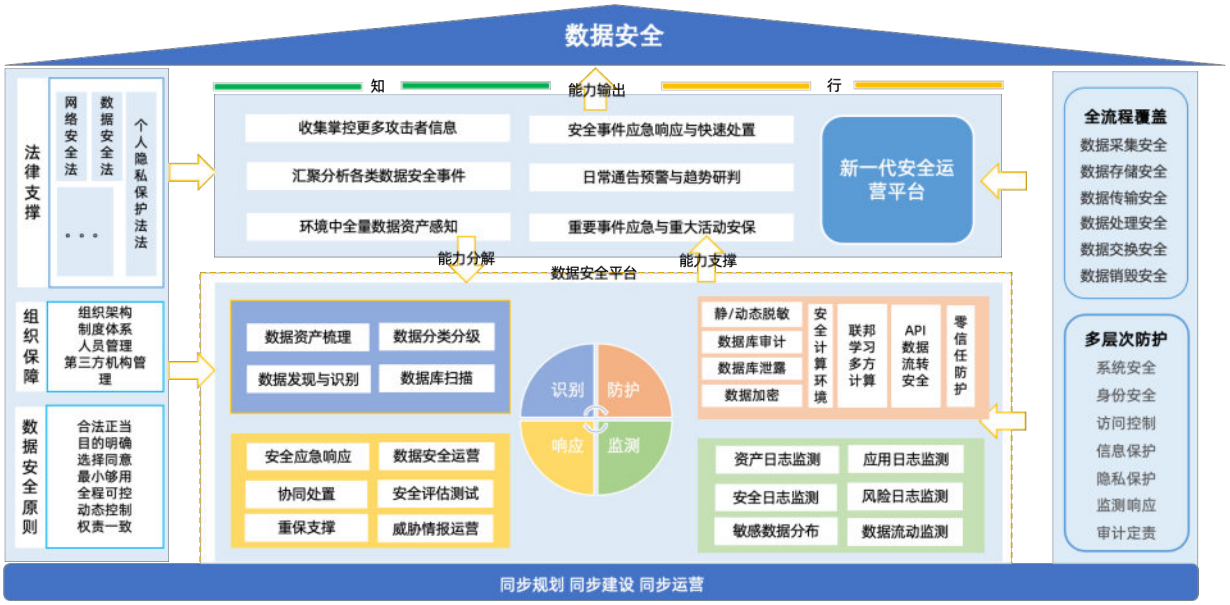


图 38：数据全生命周期安全治理体系

数据安全体系建设过程中需重点关注以下几个方面：

1．制定全面的数据安全政策和标准

金融机构应制定全面的数据安全政策和标准，明确数据安全的目标、原则和要求。同时，应建立数据安全组织架构，明确各级职责和工作流程，确保数据安全工作的有效实施。

2．强化数据分类分级和权责关系

根据数据的敏感性、重要性和用途等因素，金融机构应对数据进行分类分级，识别不同数据的敏感程度和价值，并据此对数据进行风险评估和制定相应的保护措施。同时，还应确定数据所有权、使用权、处理权和监督权等权责关系，确保各方职责清晰。

3．加强数据安全检测与防护能力

在数据存储、传输、处理和交换过程中，应实施精细化的权限管控策略，确保只有授权用户才能访问敏感数据，提升数据防泄露能力。采取数据脱敏、加密、签名等安全措施，确保数据的安全性、完整性和可靠性。同时，应定期对数据进行备份和恢复测试，确保数据在发生安全事件时能够迅速恢复。

4．建立一体化数据安全治理能力

依据数据安全管理目标，从数据安全管理体系、数据安全技术体系、数据安全运营体系三方面完善数据安全能力建设，从组织、制度、流程、平台、技术措施等，明确数据安全建设路线和管控措施。建立一体化数据安全平台，实时监控数据的识别、流转和使用情况，当发现异常行为时可联动防护手段及时处置。同时，应制定详细的应急响应计划，明确应急响应流程和责任人，确保在发生数据泄露

等安全事件时能够迅速、有效地进行处置。

5．推广先进技术应用和创新安全理念

金融机构应积极推广先进技术应用，如零信任、人工智能、区块链等，提升数据安全治理的效率和准确性。同时，应创新安全理念，结合隐私技术、API 安全等技术方案，探索数据共享和使用的新模式，实现数据的安全流通和价值最大化。

6．加强合作与信息共享

金融机构应加强与外部合作机构的合作与信息共享，共同应对网络安全威胁。同时，应积极参与行业组织和监管机构的交流与合作，共同推动金融行业网络安全水平的提升。

综上所述，构建数据全生命周期安全治理体系是金融行业网络安全发展的必然趋势，随着技术的不断进步和监管政策的不断完善，金融行业网络安全将迎来更加广阔的发展空间和更加严峻的挑战。因此，金融机构应持续关注网络安全发展趋势，不断创新和完善数据安全治理体系，确保金融业务稳健运营和客户信任度持续提升。

云原生安全能力提升

云原生技术以其轻量级、容器化、微服务化等特点，为金融行业提供了快速响应业务需求、提高系统弹性、降低运营成本等优势。然而，随着云原生技术在金融行业的广泛应用，其安全问题也日益凸显。容器逃逸、微服务间通信安全、无服务架构下的权限管理等新型安全威胁不断出现，给金融行业带来了前所未有的挑战。因此，构建云原生安全防护体系成为金融行业网络安全的重要任务。

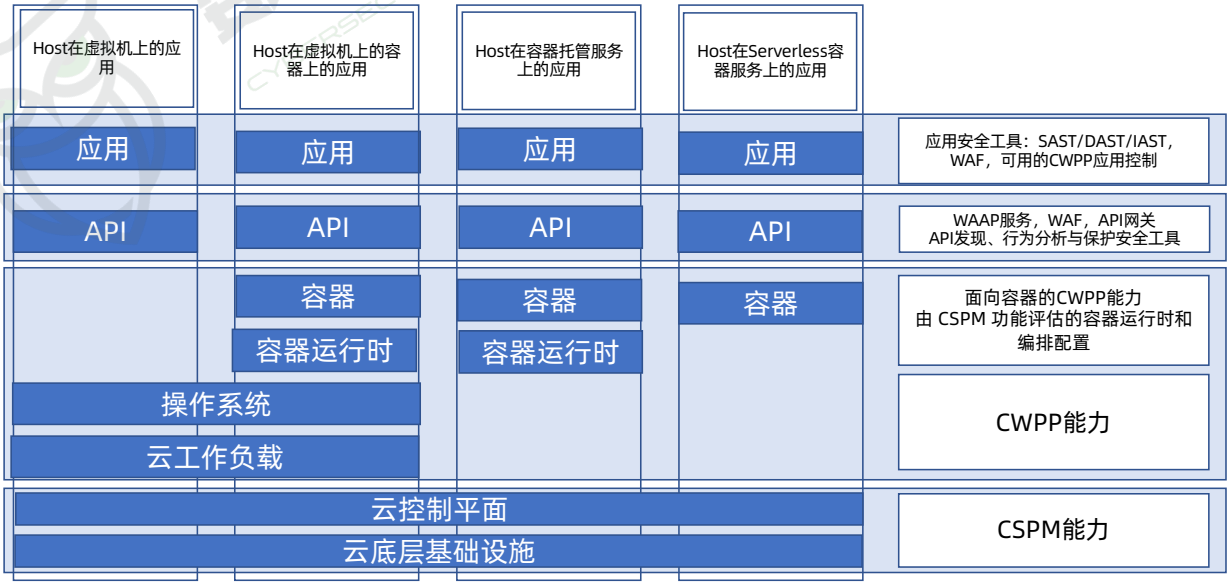


图 39：云原生安全体系

云原生安全体系建设过程中需重点关注以下几个方面：

1．建立云原生应用及工作负载运行时保护能力

云原生应用和工作负载的运行时保护是构建云原生安全防护体系的核心环节。这要求金融机构能够发现并管理在云部署和本地基础设施中运行的所有工作负载。为此，需要建立一个集中式的解决方案，以扩展对云资源的可见性，并实现对云工作负载的全面保护。具体包括：建立云工作负载保护平台，实时监控容器运行时的安全状态，检测并预防潜在的安全威胁；集成云原生应用运行时监控工具（RASP 等），对应用性能、资源和风险等关键指标进行实时分析，发现异常行为；通过网络流量监控和分析，确保数据传输的安全性，防止数据泄露。

2．建立云原生应用程序全生命周期开发运营安全能力

在云原生应用的全生命周期中，从开发、测试、交付到运营的每个阶段都应嵌入安全能力。这要求金融机构通过引入安全开发生命周期 SDLC 和 DevSecOps 实践，开发团队能够在编写代码时即考虑安全性，从而在早期阶段就识别和修复潜在的安全漏洞。在测试阶段，安全团队可以利用自动化工具和框架对应用进行全面的安全测试，确保其在发布前符合安全标准。交付和运营阶段则强调持续的监控和响应，实现对云原生应用的实时保护。

3．建立云资产全面风险可视、威胁响应及漏洞修复能力

为了有效管理云资产的安全风险，金融机构需要建立全面的风险可视化、威胁响应和漏洞修复能力。这包括全流程安全规则管理、变更管理和操作审计，以及云资源对外服务暴露面的安全管理；使用云原生安全保护平台，实现云资产的全面可视化和风险评估；建立威胁情报收集和分析机制，及时发现并响应安全威胁；制定并执行漏洞修复计划，确保所有已知漏洞得到及时修复；实施严格的变更管理和操作审计流程，防止未经授权的更改和操作等。

4．建立云安全基础防护能力

为了提升云原生应用的整体防护效能，金融行业需要建立强大的云安全基础防护能力，进而能够快速、弹性地针对云应用进行全面防护。这包括使用 Web 应用和 API 防护（WAAP）技术，保护 Web 应用免受各种网络攻击；建立安全能力快速响应机制，确保在发生安全事件时能够迅速提供所需的安全资源和服务；利用容器和微服务架构的弹性特点，实现安全能力的动态扩展和调整等。

5．建立云基础设施安全能力

云基础设施的安全是云原生应用安全的基础。金融行业需要确保系统和镜像的标准化（包括精简、加固、更新），以及运行环境的安全检查（包括主机安全和容器安全）。这包括：制定系统和镜像的标准化规范，确保所有云基础设施的部署和运行都符合安全标准；实施定期的安全加固和更新计划，确保基础设施的安全性和稳定性；使用主机安全和容器安全工具，对运行环境进行全面检查和监控，及

时发现并处理潜在的安全威胁等。

综上所述，随着技术的不断进步和应用场景的不断拓展，云原生安全防护体系将进一步完善和优化，为金融行业的数字化转型提供更加坚实的安全保障。同时，云原生安全防护体系的构建是一个长期而复杂的过程，需要金融行业各方共同努力和持续投入，保持高度的警惕和前瞻性思考，不断探索和创新安全防护手段和方法，确保金融行业的云原生安全体系稳定可控。

七、金融行业网络安全安全厂商分析

（一）金融行业网络安全品牌热度分析

通过对网络安全厂商在 2023 年金融行业项目热度指数表现进行分析，我们发现，头部安全厂商由于产品品类全，销售渠道覆盖广，因此在整个金融行业中占据主要优势。小型安全产商虽然市场份额较少，但在细分领域也展现出较强的竞争力。

数据来源：数说安全 CSRadar 商业分析平台

图 40：2023 年中国金融行业网络安全品牌热度格局

（二）金融行业细分网络安全领域品牌热度词云

通过数说安全 CSRadar 分析平台的数据，我们对不同网络安全厂商在金融行业各安全领域的项目参与度、中标频次等维度进行了分析，并形成了市场品牌热度的情况（如图 41-48 所示），其中，品牌的字体大小直接映射了其市场活跃度和渗透力——字体越大，代表该品牌在市场上的影响力和关注度越高，从而反映出更强的市场竞争力。(数据截止日期为 2024 年 4 月)

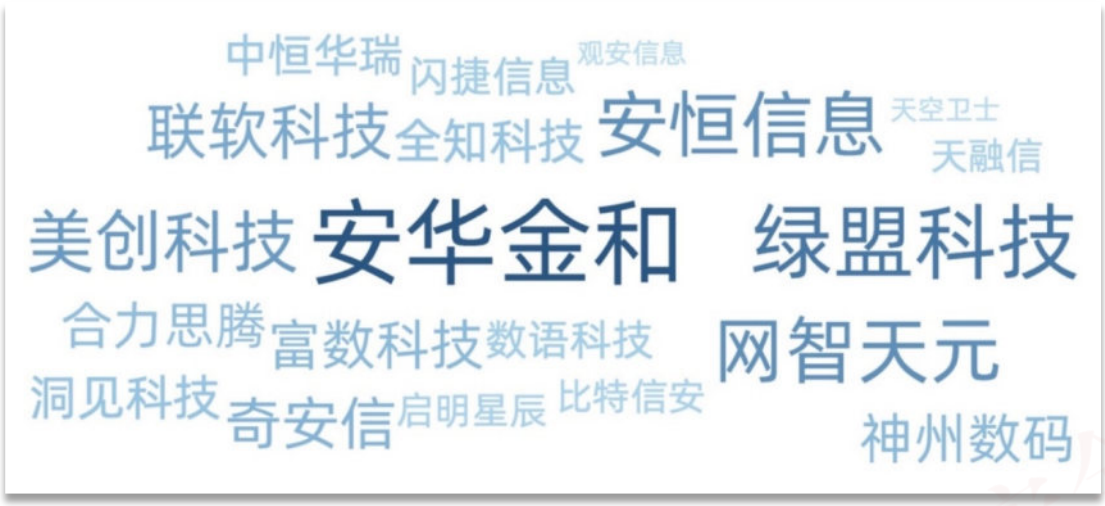
2024 年中国金融行业开发安全市场品牌热度词云

数据来源：数说安全 CSRadar 商业分析平台

图 41：2024 年中国金融行业开发安全市场品牌热度词云

（领域包含：DevSecOps/静态应用安全测试 SAST/动态应用安全测试 DAST/交互应用安全测试 IAST/软件成分分析 SCA/模糊测试 Fuzzing）

2024 年中国金融行业数据安全市场品牌热度词云



数据来源：数说安全 CSRadar 商业分析平台

图 42：2024 年中国金融行业数据安全市场品牌热度词云

（领域包含：数据库安全/数据脱敏/数据泄漏防护/数据安全管理平台/电子文档管理与加密/数据分类分级/数据安全治理/隐私计算/存储备份与恢复/API 安全）

2024 年中国金融行业零信任应用市场品牌热度词云

数据来源：数说安全 CSRadar 商业分析平台

图 43：2024 年中国金融行业零信任应用市场品牌热度词云

（领域包含：零信任/SDP）

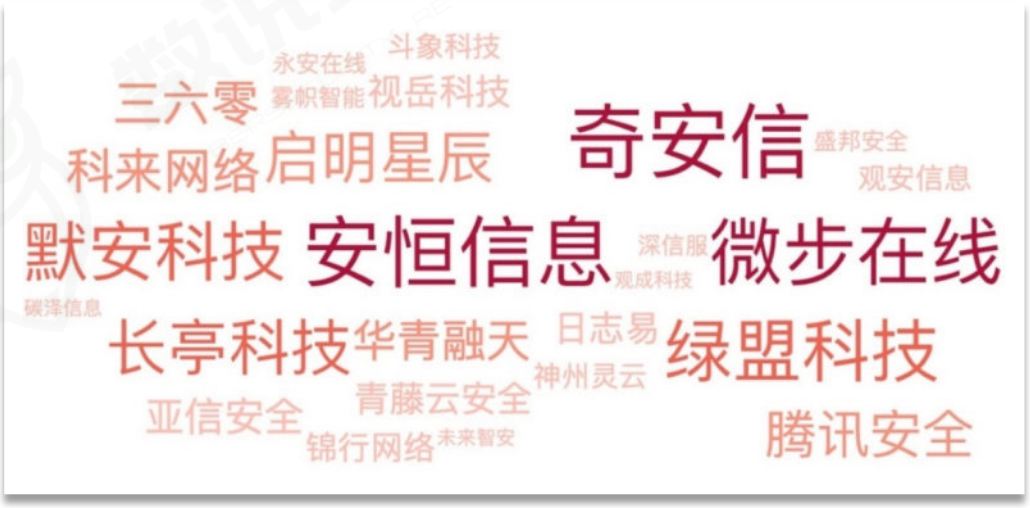
2024 年中国金融行业移动安全市场品牌热度词云

数据来源：数说安全 CSRadar 商业分析平台

图 44：2024 年中国金融行业移动安全市场品牌热度词云

（领域包含：移动终端防病毒/移动应用安全管理/移动终端安全管理/移动威胁防护）

2024 年中国金融行业威胁管理市场品牌热度词云



数据来源：数说安全 CSRadar 商业分析平台

图 45：2024 年中国金融行业威胁管理市场品牌热度词云

（领域包含：网络流量检测与响应/高级持续性威胁防护/终端检测与响应/安全管理平台/态势感知/欺骗防御/蜜罐/蜜网/安全编排与自动化响应/安全情报/扩展安全检测与响应）

2024 年中国金融行业网络与基础架构安全市场品牌热度词云

数据来源：数说安全 CSRadar 商业分析平台

图 46：2024 年中国金融行业网络与基础架构安全市场品牌热度词云

（领域包含：防火墙/UTM/第二代防火墙/网络入侵检测与防御/网络行为管理与审计/网络隔离与单向导入/防病毒网关/虚拟专用网 VPN/抗 DDos/网络准入与控制 NAC/软件定义广域网 SD-WAN/应用交付）

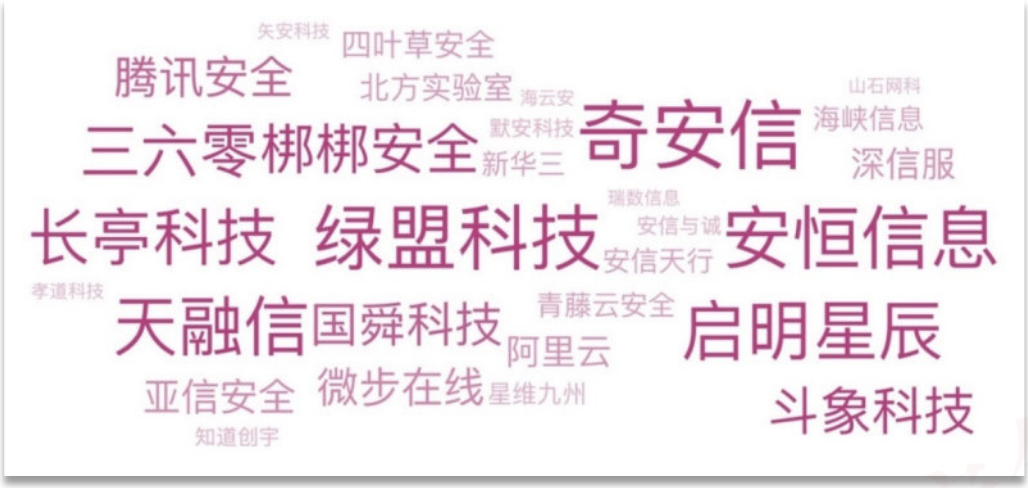
2024 年中国金融行业网络资产测绘与攻击面管理市场品牌热度词云

数据来源：数说安全 CSRadar 商业分析平台

图 47：2024 年中国金融行业网络资产测绘与攻击面管理市场品牌热度词云

（领域包含：网络资产攻击面管理/外部攻击面管理/网络资产测绘）

2024 年中国金融行业安全服务市场品牌热度词云



数据来源：数说安全 CSRadar 商业分析平台

图 48：2024 年中国金融行业安全服务市场品牌热度词云

（领域包含：安全运维/风险评估/渗透测试/红蓝对抗/应急响应/攻防实训/靶场/安全意识教育/安全众测）

（三）主要网络安全厂商经营概况

通过对近百家参与金融行业网络安全建设的厂商进行了调研，我们发现，数据安全、开发安全、身份认证与访问管理、综合安全、安全运营、云安全、终端安全的厂商数据量较多，占据整体调研厂商的 60%，这也从侧面说明金融行业的主要安全建设需求所在。

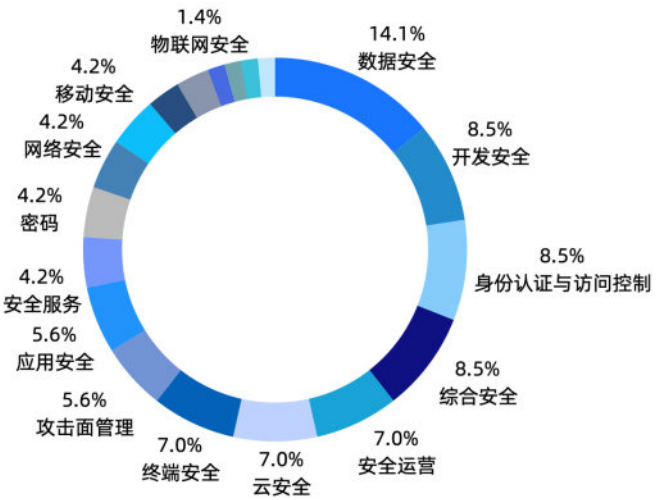


图 49：参与调研的安全厂商类型分布

金融行业的收入超过 1 亿元企业约占整体的 25%,其中主要是综合型安全厂商和终端安全厂商，也有个别应用安全、移动安全、数据安全和攻击面管理的厂商。约六成安全厂商的金融行业收入在 5000 万以下，这说明金融行业客户对安全建设有很深的理解，同时也有自己的方法和体系，并不一味地追求大包大揽式的整理解决方案。

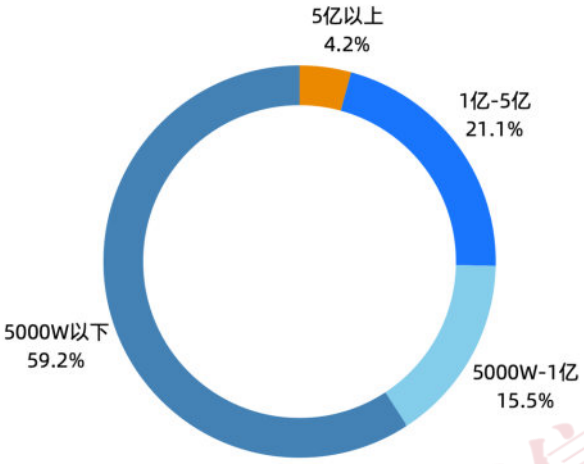


图 50：参与调研的安全厂商收入情况分布

参与金融行业的安全厂商在销售模式上并没有明显的偏向性，但收入在 1000W-5000W 元的厂商由于仍然需要更直接的接触客户，因此采用直销模式的数量较多。但若要实现收入的持续增长，渠道的作用不可或缺。

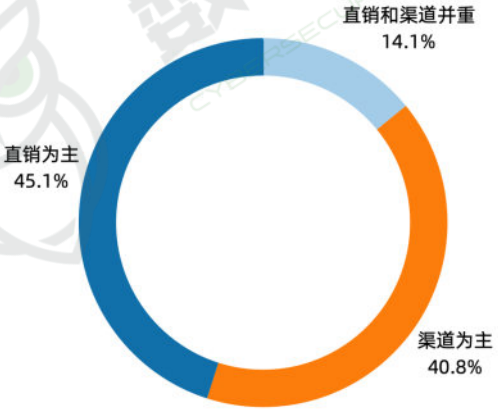


图 51：参与调研的安全厂商销售模式分布

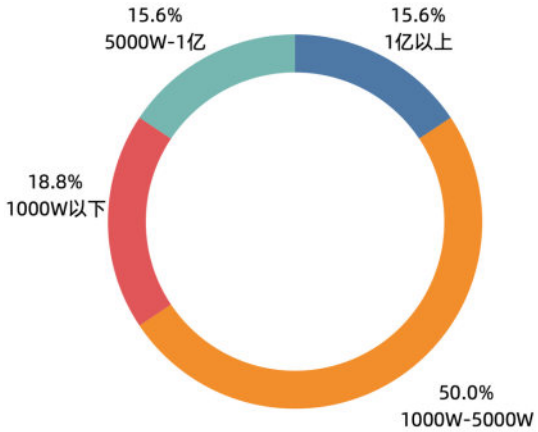


图 52：其中以直销为主的安全厂商收入分布情况

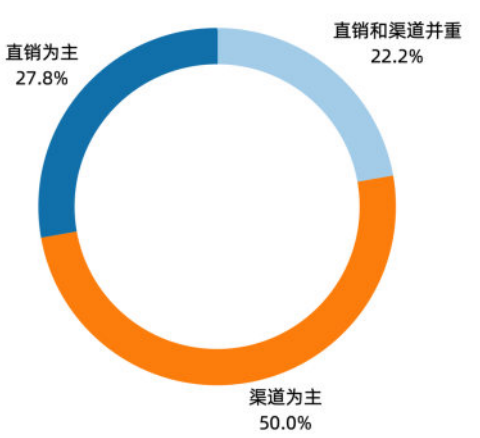


图 53：其中金融收入 1 亿元以上的厂商销售方式

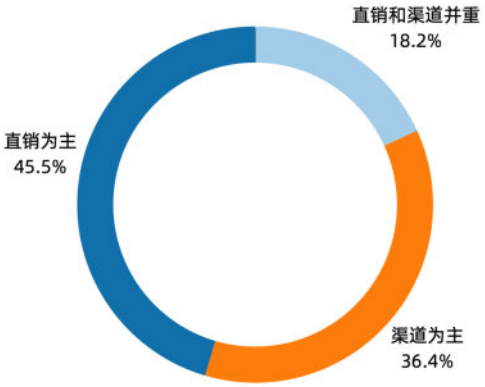


图 54：其中金融收入 5000W-1 亿元的厂商销售方式

八、金融行业项目案例展示

（一）安全服务品牌推荐及项目案例

优秀的渗透与漏洞挖掘能力

北方实验室拥有自主研发的自动化渗透平台，实现智能化、自动化地利用各种漏洞进行信息侦查和渗透测试，大幅提升渗透测试效率。团队拥有丰富的大赛经验，在多个高水平的国家级网络安全和工业信息安全竞赛中取得了优异成绩。

丰富的顶级资质

北方实验室拥有信息化工程建设全业务链的顶级第三方信息技术服务资质，同时是国家CNAS认可实验室，工信部认定的国家中小企业公共服务（信息技术）示范平台，在业内具有权威地位。

身份中立，博采众长

公司作为独立的第三方服务机构，整合众多网络安全厂家优秀的安全产品作为服务工具为用户带来优质的服务。没有产品色彩与包袱，可更好地追求安全本质，通过优质的服务而不是过度依赖产品，让用户享用更加高效、更具性价比的网络安全保障。

某农商行基于实战攻防的一体化网络安全运营服务案例

一、项目背景

某农商行为了提高信息系统安全以及信息系统密码应用安全，降低信息科技风险，确保系统稳定运行，满足《中华人民共和国网络安全法》《中华人民共和国密码法》等相关法律要求，邀请具有漏洞挖掘、渗透测试、密码评估能力的服务机构开展集渗透测试、漏洞挖掘、电子银行密码安全性评估等一系列一体化的网络安全服务。

◆ 客户痛点

- 客户网内系统繁多，脆弱性识别不到位，业务体系复杂，有限的时间精力让网络安全工作变得主次不清；
- 客户网内缺少精准防护手段和识别能力，针对高频攻击行为缺少深度防御能力；
- 缺乏响应机制及联防联控机制，网内安全事件响应不及时。

二、方案实施

对全网络几十个业务系统开展渗透测试，全方位识别安全脆弱性和风险；

对个人网上银行、企业网上银行等重要的信息系统开展电子银行渗透测试，强化供应链安全和源代码安全；

对重要的业务系统开展等保测评与商用密码安全性评估工作，针对密改难点问题进行专家研讨；

为了确保安全服务的高效进行，公司采用了悬赏竞赛的方式。在这种模式下，将发现的安全问题分为高危、中危和低危三个等级，并对应设置不同额度的奖励赏金。这一机制不仅激发了测试人员的积极性，还确保了问题被彻底排查。同时，执行严格的监控措施，确保渗透测试过程受控，最大限度地降低了潜在的风险；

通过既有安全产品加持，利用一系列工具，建立主动防御和联防联控机制，针对疑难问题进行专家研判。

三、项目亮点

◆ 自研技术加持，助力客户网络安全全方位提升

众所周知，金融机构安全防护手段相对齐备，渗透攻击难度较大。公司连续多年成为该银行安全众测单位，多年来已经累积发现数百个高等级安全威胁隐患。渗透团队利用公司自主研发的北实正剑·自动化渗透系统对目标网络和信息系统开展深度渗透测试和漏洞挖掘，发现高价值安全漏洞，持续推动客户安全开发、安全运维、安全应急响应能力提升。该系统核心技术已取得多项专利授权，搭载原创漏洞载荷，基于自研的自动化引擎，精准挖掘积累 27000+资产指纹、400+安全漏洞载荷和 34 万+动态映射库，自动化开展信息收集、漏洞发现等工作，为网络安全渗透测试人员提供全过程的自动化支撑，平台攻克了基于 PPW 三层架构的渗透框架引擎、基于工作流的并发测试、基于漏洞特征的自定义载荷加载、基于动态映射库的测试用例收敛等多项核心技术，实现了通过自动化渗透系统替代人工开展渗透测试，将单一系统的渗透测试时间从数天缩减到十几分钟，解决了人工测试效率低、准确率低的难题。

◆ 第三方视角，公正测评护航

公司在服务过程中，发挥作为第三方服务机构具有的天然生态聚集效应，身份中立，以裁判员、教练员的视角为信息化建设保驾护航。博采众长，整合众多网络安全厂家优秀地安全产品作为服务工具为用户带来优质的服务。没有产品色彩与包袱，可更好地追求安全本质，通过优质的服务而不是过度依赖产品，让用户享用更加高效、更具性价比的网络安全服务。

四、技术服务商简介

北方实验室（沈阳）股份有限公司是一家以网络安全服务和信息技术咨询服务为主营业务的信息技术服务提供商，是国家专精特新“小巨人”企业、国家中小企业公共服务示范平台、国家高新技术企业、瞪羚企业，依托自有智能渗透攻击、主机攻击监测预警等核心技术，聚焦电子政务、金融、能源、电信、交通、军工等信息化工程重点领域，致力于为客户提供覆盖信息化工程建设全生命周期的综合性、跨阶段、一体化的第三方网络安全服务与信息技术咨询服务。

（二）数据安全品牌推荐及项目案例

NSFOCUS

深厚的安全服务能力

深耕多年，从国家和金融监管要求出发，为客户提供可落地的规划及咨询服务。

丰富的金融行业经验

积累国有大行、股份制行、城商行、省农信等合规咨询和分级管控实践经验。

完善的数据安全体系建设能力

以数据流转及共享交换的安全为重点，构建基于分类分级的数据流转监测；以数据安全合规为基础，构建分类分级防护、“一监一查”体系，为数据交换、共享、流转提供安全基础设施。

天空卫士 SkyGuard

数据泄露防护DLP领导品牌

DLP产品不仅包括网络DLP和终端DLP，还涵盖了应用DLP和云DLP，具备复合型指纹技术、智能学习、图像识别等先进功能，能够多维度地发现和保护敏感数据，同时支持混合云部署，满足不同企业的需求。

扎实的底层技术助力数据安全解决方案

数据安全解决方案结合了大数据、人工智能、机器学习、行为分析等先进技术，构建了持续、动态、自适应的数据安全治理体系，对风险用户进行智能化的监督和控制，有效降低数据泄密风险，并提高效率。

行业覆盖度和市场认可度高

产品在各个行业如银行、证券、保险、航空、互联网、大型制造、能源和政府机构中得到成功部署，客户遍及全国，其产品和解决方案得到了客户的高度赞扬和市场的认可。

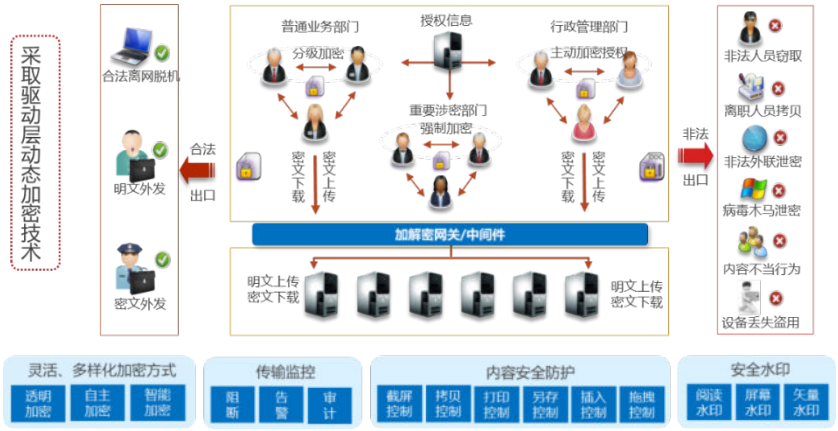
某国有大型商业银行终端数据泄漏防护案例

一、项目背景

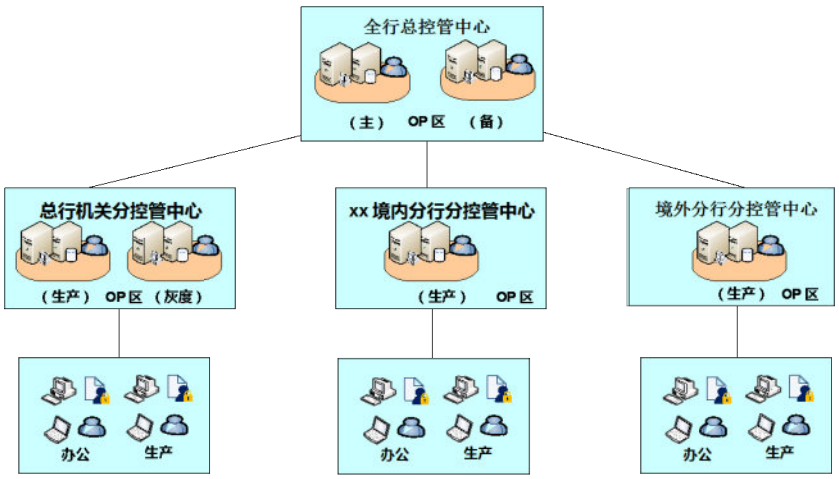
本次终端数据安全治理前，行方已部署终端管理、防病毒等安全软件，但终端数据安全泄漏防护效果甚微。传统终端 DLP 产品性能消耗大，经常导致电脑卡顿，影响工作开展，由于未筛选出匹配需求的终端 DLP 产品，行方数据中心只能依靠人力进行管理，针对几十万台终端电脑数据资产合规管理明显力不从心。在 2021 年银保监会的常规检查中，行方因数据管理粗放、制卡数据违规明文存储等问题，被处以罚款并责令限期整改。

二、方案实施

我司协助行方开展终端敏感数据安全整治，结合行方自身数据安全需要以及监管机构对行业数据安全监控要求，解决办公终端以及其它应用软件传送敏感数据可能产生的泄漏风险，建立健全数据安全相关管理制度，并建设推广终端数据防泄漏（DLP）系统，在全行范围内约 46 万台 Win 办公终端、5 万台信创终端、4 万台生产终端实现数据防泄漏的统筹建设和统一管理，依托终端 DLP 系统组织开展客户个人敏感数据集中整治，对办公终端文件开展“全方位、无死角”扫描，删除大量非必要文件，在全行打了一场风险“歼灭战”。



为支撑行方管理需求，本项目采用分布式、分级、高可用部署方案。



三、效果评估

经整治，个人客户信息泄漏风险得到全面压降。对确需留存的少量文件，实施“管理+技术”双管控，实行两级主管审批，涉敏文件整体压降率超 99%。

行方给予评价“贵司协助行方完成敏感数据‘扫描—通报—核实—清理’常态化闭环管理机制的推广，对终端 DLP 系统应用模式上进行了革新，改变了行方终端安全管理模式，能够支撑行方常态化检查工作开展，实现了终端数据安全风险的长效管控。”

目前产品应用效果如下：

- 解决了只能被动接受监管检查，不能主动自查自处理的问题。
- 支撑行方每月一次的常态化自查工作。
- 创新终端数据安全管理模式，实现了数据安全全员参与，明显缓解安全管理部门的管理难度和压力。
- 利用可视化技术进行呈现资产分布、敏感数据流转等情况，帮助行方全面掌握全网数据安全态势。

四、技术服务商简介

绿盟科技集团股份有限公司（以下简称绿盟科技）成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构。

绿盟科技在数据安全领域有着完备的产品和服务体系。在金融行业，绿盟科技在数据分类分级、数据安全风险评估、管理体系咨询以及分级管控措施落地方面积累了显著的差异化优势。

- 绿盟深耕金融行业多年，专业团队研究国家和金融监管要求，可为客户提供可落地的规划及咨询服务。
- 在数据分类分级方面，绿盟积累了国有大行、股份制行、省联社、城商行等落地实践经验，同时可实现自动化分级管控，协助客户做好技防管控。
- 以数据流转及共享交换的安全为重点，构建基于分类分级的数据流转监控和审计的数据安全保障体系；以数据安全合规为基础，为客户构建分类分级防护、“一监一查”技术体系，为数据交换、共享、流转提供安全基础设施。

在金融安全领域，绿盟科技专注金融行业的信息安全研究，持续跟踪信息安全发展趋势，不断地洞察和深入分析银行、证券、保险及互联网金融等行业客户在信息安全方面所面临的信息安全风险和信息安全需求。

同时，在电子银行整体安全防护、移动金融交易安全、网上证券防盗买盗卖、网上保险交易安全、金融企业安全运营中心建设、金融云安全防护、金融数据安全规划与建设、金融供应链安全、资产和漏洞管理、互联网应用风险监测、勒索病毒防护与防御有效性评估等具体业务场景不断推出适应安全需求的产品和服务，并在企业攻防演练、企业员工内部安全意识教育等运维和管理方面提供相关服务，以巨人背后的专家为使命为金融客户的发展提供坚实有力的信息安全保障。

某头部证券公司基于信创的数据安全建设案例

一、项目背景

随着信息化建设的发展，证券行业企业都已经建立了比较完备的信息化系统。但部分业务数据、办公资料、客户信息却可能分散在终端电脑、文件服务器等处，而丢失、不当使用或未经授权访问不仅给企业客户带来财产损失，也影响证券公司自身品牌声誉，甚至给整个金融行业的秩序带来不确定性和不稳定性，可谓“牵一发而动全身”。

新《证券期货业网络和信息安全管理办法》提出了“采取有效安全防护手段，防范数据损毁泄露风险”，以及“确保个人信息在收集、存储、使用、加工、传输、提供、公开、删除等处理过程中的合规、安全，防止个人信息的泄露、篡改、丢失”等.

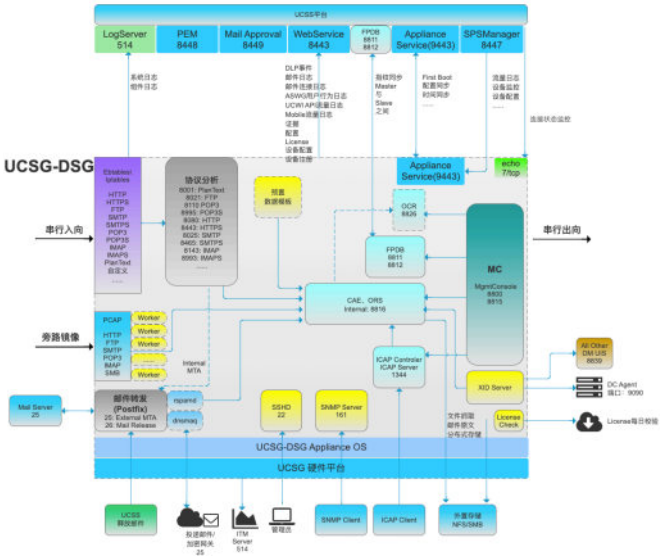
二、方案实施

网络 DLP 在该证券企业内部的部署为旁路（镜像）模式。网络镜像位于网络出口点，支持 650M 带宽。它会对网络数据包副本进行分析，检查数据是否违反策略。镜像模式支持的网络协议有：SMTP、HTTP、FTP 流量、IM 流量。对非标准和专有协议的自定义监控可通过通用 TCP 协议定义实现。

网络镜像可被动检查网络流量，并在敏感信息离开网络之前对其进行检测（覆盖所有网络协议和内容类型），使企业能提前预知数据泄漏风险。具体实现方式如下：

- 网络镜像可以检测到员工使用 IM 或公共 Web 邮件程序向竞争对手发送含有敏感信息的文档。网络镜像模式还可以监控文件加密的使用情况和类型，包括检测是否未经授权而使用加密以及验证是否遵循加密策略。
- 可以通过网络镜像扫描离开组织的所有数据以检查其中是否包含敏感信息，比如 web、论坛是否传输了敏感数据和不合规内容，实时发现敏感数据的传输并阻断，防止敏感数据通过互联网发送出去，同时将所有的违规操作记录为日志，为事后审计提供依据。

天空卫士国产化数据安全产品的可移植性、兼容性、功能性、性能效率都已经在实际项目中得到有效验证。



三、效果评估

天空卫士的网络 DLP 产品，采用旁路部署的方式，作用是对公司上网流量做监控审计，主要监控(HTTP, FTP, SMTP,自定义协议)公司全部出网流量。目前部署了一套统一内容安全管理平台(UCSS)和一套网络 DLP（DSG)。UCSS 负责策略、规则的统一定义和推送、数据泄漏事件的统一展示和证据存储；DSG 负责对流量的解析和内容识别，把结果反馈到 UCSS，方案部署可以达到如下效果：

- 大大地提高了公司 IT 部门对于数据泄密风险的评估和预防能力。
- 有效地帮助公司快速地定位到责任人，并且获得其违规的真实原因。
- 在使用了 DLP 系统一段时间后，公司的可疑违规事件得到有效的降低，敏感数据的泄密风险也得到了有效的控制。

天空卫士网络数据防泄漏方案既可以帮助用户对全集团网络外发的数据进行深度审计，防范集团内部与客户机密敏感数据泄漏，又能够全局记录跟踪数据外泄，提供证据留存与回溯能力，帮助用户满足国家法律法规与集团安全合规性要求。

四、技术服务商简介

北京天空卫士网络安全技术有限公司成立于 2015 年，是一家总部设立在北京经济技术开发区的数据安全技术企业。目前，天空卫士拥有七大品类，近二十种数据安全产品。核心的产品有数据防泄露（data loss prevention DLP)、云访问安全代理（cloud access security broker CASB)、内部威胁管理（insider threat management ITM)、移动接入网关（Mobile Access Gateway MAG)、统一内容安全管理平台(unified content secure server UCSS)、增强型 Web 安全网关(advanced secure web gateway ASWG)、增强型邮件安全网关（advanced secure email gateway ASEG)、数据安全扫描仪(data security scanner DSS)、应用数据安全审查平台(unified content webservice inspector UCWI)、云安全平台(gatorcloud)、数据安全治理自动化平台(data security automated governance DSAG)。

天空卫士在亚太地区独树一帜，同时入选 Gartner 的 ESG 邮件安全网关市场指南与 CASB 观察者名单，并且是亚太唯一一家在 2018-2023 年 5 次入选 Gartner E-DLP 全球企业级数据防泄露指南的中国企业（2019 年 Gartner 未发布此报告)。

（三）开发安全品牌推荐及项目案例

BlingSec 比瓴科技

国内优秀的开发安全技术应用创新厂商

国内率先推出“ASOC”和“ASPM”两项核心技术，并逐步将全线产品向信创标准靠拢。

构建高可运营的软件安全体系

比瓴可提供“知识库+工具+平台”的完整解决方案，弥补国内以安全检测工具为核心，但未形成平台化综合解决方案这一空白。

创新产品市场应用率快速上升

比瓴科技凭借六大营销和技术服务中心，已完成金融、运营商、电力、能源、工业制造等重点行业安全市场深度覆盖，实现客户业务与安全融合增长。

海云安 secidea

多核智乘AI大模型，攻克软件卡脖子难题

海云安基于核心技术突破的8年沉淀，持续攻克基础软件“卡脖子”问题，创造性应用多核智乘AI大模型，率先推出安全左移新产品，市场反应热烈。

核心团队成员技术实力雄厚

海云安核心团队主要来自清华、新加坡国立、中科院、北理工等世界一流高校院所，具有“清华+博士”的深厚技术底蕴。

服务头部客户，更懂行业需求

陆续获得了国家部委、各大金融机构及大型企业的使用，积累了丰富的案例，直击客户痛点及需求，形成市场行业进入壁垒。

某股份制银行开发安全技术支持平台案例

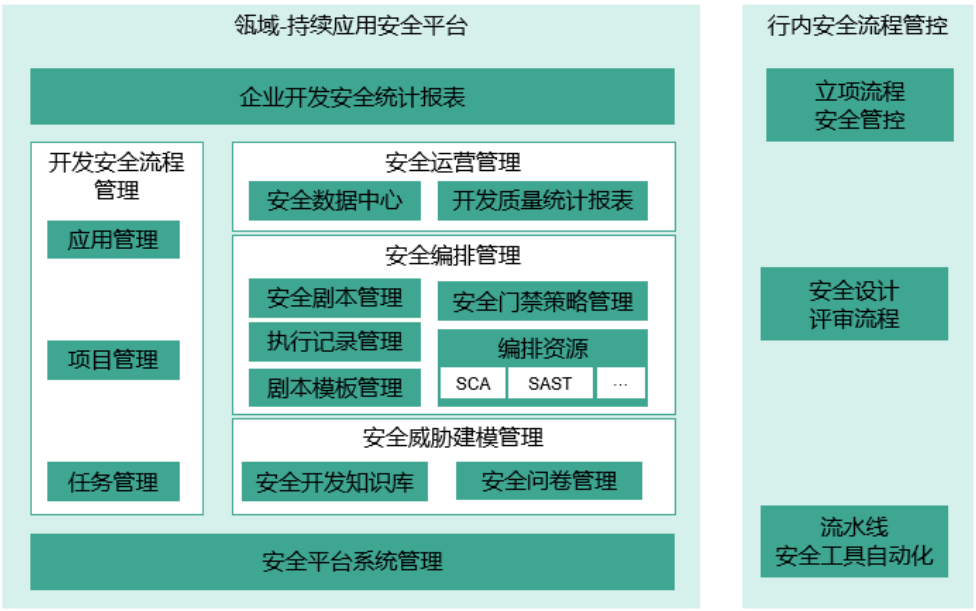
一、项目背景

某股份制银行有大量的应用程序，包括网站、移动应用、内部系统等。一方面，这些应用程序由不同的团队开发，使用不同的编程语言和技术栈，导致管理和维护安全性变得复杂；另一方面，在敏捷开发和研发运维一体化模式下，开发和部署的速度显著加快，但安全活动难以跟上节奏，给开发活动带来阻力，增加了银行面临的安全风险。

在这样的背景下，银行迫切需要一种综合的、高效的安全解决方案，以提升安全开发成熟度水平，加强安全活动效率，降低安全风险。

二、方案实施

比瓴科技与银行深入沟通，了解其安全需求、业务特点和现有安全情况，制定以安全平台为核心的项目目标。通过部署安全平台，结合必要的安全服务，在银行拥有庞大且复杂的应用生态系统的情况下，简化安全管理，帮助银行汇总安全能力、流程和数据，减少了信息孤岛和重复劳动，提高效率，整体建设方案如下图所示。



◆ 整合安全工具统一输出安全能力

第一阶段的主要工作是完成安全平台的安装、配置、集成、调试。安全平台集成银行内部多种安全测试工具，包括 SCA、SAST、DAST、容器安全扫描等。这些工具覆盖了应用开发生命周期的不同阶段，帮助银行全面地发现安全问题，并加速安全漏洞的修复过程。

◆ 汇聚工具漏洞形成数据中心

第二阶段的主要工作是通过安全平台的应用安全编排技术自动化执行安全活动。安全平台将不同安全测试工具的数据，发现的安全漏洞与具体的应用程序相关联，相关漏洞归类为同一个安全问题，

自动化生成测试报告和提供修复建议，提高了安全测试的效率和准确性，有助于银行更全面地理解安全威胁的全貌，并采取相应的措施进行修复和改进。

- 数据关联分析识别漏洞优先级

第三阶段的主要工作是通过安全平台的漏洞优先级技术识别出最紧急的安全问题，避免将所有漏洞一视同仁，导致资源分配不当的问题。漏洞优先级技术结合了漏洞的严重程度、影响范围和可能被利用的概率等因素，再结合外部威胁情报综合计算安全风险，为银行提供了一种有效的漏洞修复优先级排序方式。通过漏洞优先级技术，银行能够快速确定哪些漏洞最需要优先解决，从而有效地分配资源，降低安全风险。

三、效果评估

通过安全平台，银行有效提升了安全开发成熟度水平，提高了安全测试工具的使用效率，降低了安全风险，让安全与业务交付保持统一速度。

- 首先，银行提升了安全开发成熟度水平。银行的安全开发流程得到了优化和加强。这有助于加强开发团队的安全意识，提高开发流程的规范性和质量，从而提升了整体的安全开发成熟度水平。
- 其次，银行提高了安全测试工具的使用效率。安全平台的自动化漏洞扫描和关联分析功能极大地提高了安全测试工具的使用效率。自动化执行漏洞扫描、自动生成测试报告和提供修复建议等功能，减少了人工干预和手动操作的需求，加速了安全问题的发现和解决过程。
- 此外，银行降低了安全风险。银行能够更及时地发现和修复安全漏洞，优先处理最严重的安全问题，从而降低了面临的安全风险和潜在的损失。同时，安全平台的自动化漏洞扫描和关联分析功能有助于银行更全面地理解安全威胁的全貌，提前采取防范措施，减少安全事件的发生概率。

四、技术服务商简介

比瓴科技是行业优秀的软件安全解决方案供应商，面向企业客户提供覆盖软件生命周期的安全产品。在一个被软件定义的世界，比瓴致力于帮助客户快速交付安全、合规、可信赖的软件，让安全与业务保持同一速度。

比瓴科技当前三大应用安全产品线，分别是瓴域、瓴知、瓴镜。其中瓴域产品线为平台类产品，应用安全态势管理系统（ASPM）提供了以应用资产风险为视角的应用安全画像能力；安全开发管理系统（SDLM）则提供了安全开发全流程的管控功能，提高安全开发管理效率。瓴知产品线主要为应用安全威胁建模系统（TMA），以比瓴科技强大的安全专家团队提供的安全开发知识库为基础，帮助客户快速开展安全威胁建模工作。瓴镜产品线提供了对应用代码和程序的安全检测工具，包含软件成分分析系统（SCA）、交互式应用安全检测系统（IAST）、源代码安全审计系统（SAST）。

比瓴科技产品线提供了国内系统化、平台化的综合解决方案。基于系列产品向客户提供与软件开发过程生命周期相关的安全咨询及安全服务。

截止目前，比瓴科技为金融、互联网、运营商、工业制造、交通、零售及消费等行业的 100+客户、50000+软件系统提供安全技术支撑，帮助企业构建数字化业务安全基石。

某银行 AI 大模型赋能开发安全与效能提升案例

一、项目背景

该银行业务主要在线上开展，有大量的业务系统待开发维护，对迭代响应速度要求高。虽然该银行的研发体系都已经逐步采用 DevOps 模式，但随着新技术不断更新，及国家、行业监管要求的加强，对该银行开发安全能力及研发效能提出新的要求。该银行面临的主要痛点包括代码质量与安全合规压力大、老旧代码维护困难、内外网不通导致研发问题解决难、源代码安全检测工具协同效率低等问题。

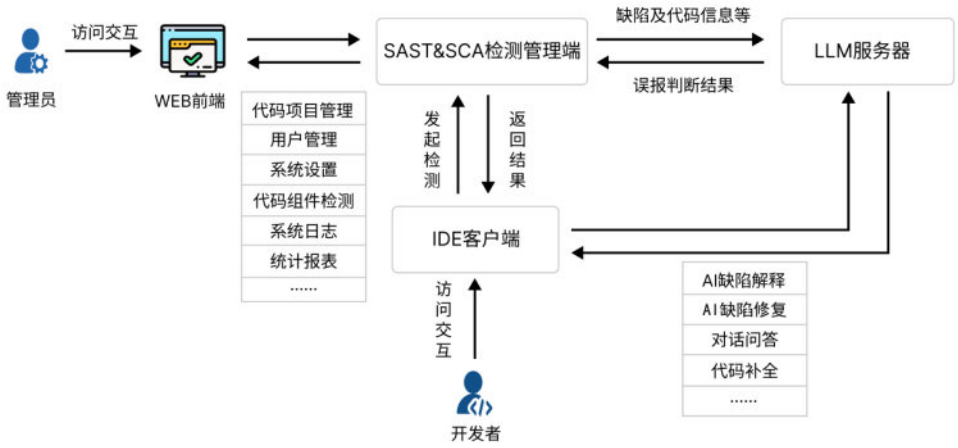
二、方案实施

海云安将过往多年在开发安全领域丰富的落地实践经验、SAST（静态应用程序安全测试）和 SCA（软件成分分析）技术与当前热门的人工智能大语言模型进行深度融合，对大模型进行微调、训练和优化，形成海云安智乘 AI 大模型。以智乘 AI 大模型作为基座进行支撑，形成一套在 IDE 中给开发人员使用的开发者安全智能助手，极大地降低了源代码检测结果的误报，通过实时生成缺陷成因解释，生成漏洞修复建议代码，加快漏洞修复闭环，根据上下文自动补全代码提升编码效率，通过智能交互式问答功能快速解答各类与研发、安全相关的问题。在开发编码阶段，开发者安全智能助手在安全、合规、质量、效能四个方面为该银行提供全方位赋能，极大地提升了研发安全能力与研发效能。

开发者安全智能助手功能架构图

开发者安全智能助手分为 IDE 客户端、SAST&SCA 检测管理端和 LLM 服务器三部分。IDE 客户端为开发者提供实时的安全检测和 AI 缺陷解释，SAST&SCA 端面向管理人员，LLM 服务器提供 AI 技术支持。

主要实现：左移代码安全检测——实时源代码和组件安全检测，发现安全漏洞。左移合规检测分析——内置安全合规检测，如隐私合规、加密算法、组件许可证合规。软件代码质量把关——提升代码可读性、可维护性、健壮性等。提升研发安全效能——AI 降低误报率，自动生成修复代码，智能交互式问答，提升研发效率。



开发者安全智能助手技术架构图

三、效果评估

◆ 从管理者角度看：

- 效能提升：快速扫描，精准发现安全漏洞，并提供切合实际的修复方案，加快安全风险发现和修复闭环，有效节约 10%的成本；
- 安全左移：在开发编码阶段全面深入地检测出代码安全、质量、合规等问题，有效提升软件安全与合规水平，安全每一行代码有抓手，提升开发者效能；
- 开发自治：将安全检测和修复赋能开发人员，而不是让安全团队充当看门人并审查每一行代码并签署所有内容。

◆ 从开发者角度看：

- 以开发者为本，在代码自动补齐，代码检测、组件检测和修复方面提供良好体验，特别是 AI 降低误报和精准缺陷代码定位及漏洞修复能力；
- 优先级排序，帮助开发者确定问题整改优先级，有效平衡安全和效率的要求；
- 为开发者赋能，提升开发者安全开发意识，将开发人员转变为安全专家。

◆ 实践效果：

- 在该银行应用的业务系统数达到 3000+，开发者用户数达到 7000+，日均交互次数 10 万+，通过融合 SAST、SCA 与 AI 大语言模型，漏洞检测准确率提升 90%，千行代码漏洞率下降 50%，开发者编码效率提升 35%，漏洞修复成本降低 40%，整体研发效能提升 10%。

四、技术服务商简介

深圳海云安网络安全技术有限公司成立于 2015 年，是一家专注于安全左移的国家专精特新“小巨人”企业。秉承“成就安全美好的数字化新世界”的愿景和“安全中国代码，保护数据价值”的使命，海云安提出了“左移开发安全，右拓安全运营”的思想，专注于提供安全左移系列工具、平台方案，将安全和数据合规从传统的右移模式转变为左移模式，在软件开发的早期阶段就引入安全和合规措施，提高安全保护能力，降低安全合规成本，降本增效。

（四）零信任品牌推荐及项目案例

以Google GeyondCorp项目为原型的应用层零信任技术创新企业

贴合业务通过应用层零信任能力构建零信任体系，实现了应用0day防护和数据管控能力，通过团队近10年的零信任实践落地积累，让零信任真正成为业务安全底座。

解决人在数据访问过程中的安全风险

创新性实现了Gartner提出的“基于人的身份对数据进行安全管控”，通过零信任实时动态决策，解决人对数据的访问安全闭环，可动态免改造无打扰实现数据管控、审计、脱敏、溯源等能力。

全网零信任落地能力

可实现内外网、全行业部署，实现了多家超大型企业在内外网全面零信任落地，在金融行业，成功签约证券、基金、城商行、保险客户等数十家金融客户，真正做到让安全无界，助力业务发展。

某证券机构应用层零信任安全接入案例

一、项目背景

某证券公司是一家综合类上市证券公司，是中国证券监督管理委员会核准的七家合规试点证券公司之一。公司现有客户超过 30 万户，托管的证券市值和保证金超过 280 亿元。目前在全国各地设置了多个分支机构、子公司、营业网点等，办公人员身份来源多样化，公司业务系统掌握着大量数据信息，公司对内部数据安全的保护工作尤为重视，需要加强企业内部的数据安全管控能力。并且近年来随着互联网的逐渐普及，证券公司的边界安全防护模型也逐渐失效，大量业务需要在互联网端开展，此时如存在对外暴露的系统，黑客可直接针对相关系统发起攻击。此外，公司还需要在保障办公系统安全性的同时，不给业务部门增加安全负担，保障业务可以时刻连续、高效地开展。

二、方案实施

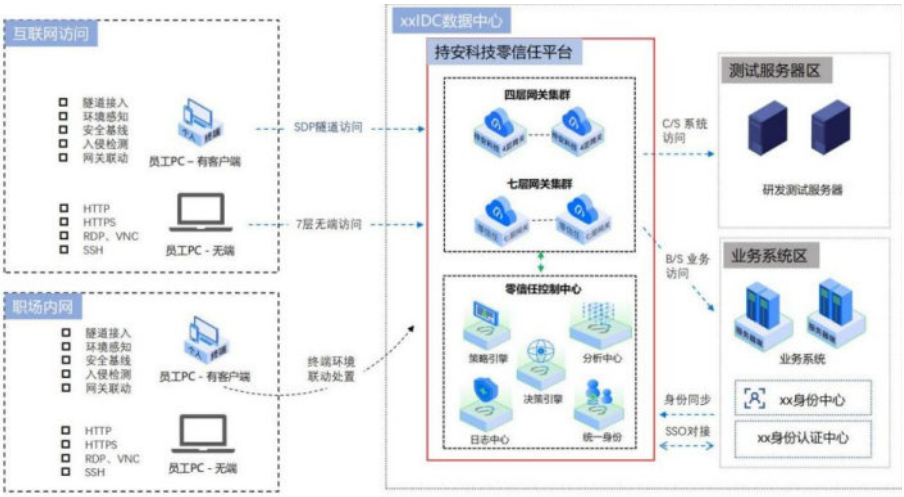
基于对证券行业的调研与深刻理解，持安科技联合该证券公司打造了基于 Google BeyondCorp 应用层零信任架构的零信任平台。

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。能够基于业务身份，在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。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，从而提高企业的业务安全防护能力以及数据安全性。

平台使用独立部署模式，支持本地化部署云端部署，或是与企业的 K8S、容器环境融合，实现全场景的部署和使用。持安自主研发高可用架构，可收敛所有访问入口，分布式就近访问，具备低延时、高传输性能。

- 数据平面：以网关的形式部署在机房，通过部署四层与七层网关，将集团设备进行统一管理，收敛业务暴露面，保障了接入设备的安全管控，对接入设备进行了有效的身份鉴别、安全基线等。保证了业务访问的安全，也提升了用户的使用体验。

- 控制平面：可视化的平台，可一键调配适合企业的安全策略，让安全可见、可感、可控。



三、效果评估

企业基础架构承载零信任改造后，全员无感知接入、业务访问不区分内外网，且兼顾了效率和安全，帮助用户实现应急响应速度提高 300%，攻击事件减少 99%等目标：

- 数据安全性提高：采用了应用层零信任技术，通过对用户身份认证、权限管理和数据加密等多种措施，保障了数据安全性，降低了风险。
- 互联网暴露面收敛：通过应用的统一发布、统一管理，使部分原本发布在公网访问的业务系统，统一收缩到了零信任 SDP 网关后，对外仅暴露了应用网关的端口，减少了暴露在互联网上的安全风险和暴露面，经验证，无法扫描识别。
- 用户体验提升：通过对接现有的统一身份认证，实现了一站式用户认证、应用访问、授权和审计等功能，使用户可以通过一个入口、一次认证实现所有应用的登录和访问；终端提供了强大的自运维能力，通过下发基线修复脚本，员工可在终端实现“一键修复”。
- 部署灵活简洁：支持本地、云和混合部署等多种部署方式，根据具体场景和需求进行选择。
- 扩展性、可靠性好：采用了云原生、微服务化的设计理念，产品可拆分为多个组件分别部署在不同的环境下，支持横向和纵向扩展，可以随着业务需求的增长而快速扩容和升级，所有的组件均支持高可用及负载均衡，提高了系统的可用性和稳定性。
- 终端安全防御能力强：终端提供的 EDR 能力，通过服务端配置的基线，支持对恶意攻击和漏洞利用等多种威胁进行告警、拦截，同时与网关联动，提高了终端接入的安全性。

四、技术服务商简介

持安科技拥有 9 年零信任落地经验，2015 年在国内开启甲方零信任实践并全面落地。致力于站在业务视角，通过一体化平台的方式，提供安全、高效、无感知的办公方式。2022-2023 年将金融业务作为主要业务增长方向，并成功签约证券、基金、城商行、保险等客户，解决企业远程/移动化/本地办公安全、攻击渗透、未知风险防护、数据安全和内控风险问题。

（五）网络资产测绘与攻击面管理品牌推荐及项目案例

丰富的网络攻防实践经验

在产品方面，云科安信强调用攻击者思维，以及风险优先级理念，思考审视目标系统，为客户量身打造最有效的安全赋能方案。

多维度的风险度量

在“强合规高要求”的金融行业，云科安信通过“资产测绘、漏洞验证、收敛暴露面”等方式，动态、持续、全局地对目标进行风险度量。

高效精准的风险收敛能力

帮助客户快速、精准地收敛安全风险，同时还可与云科防御类产品互为驱动，快速构建更优的实战安全防御解决方案。

西南地区某股份制城商银行攻击面管理服务项目

一、项目背景

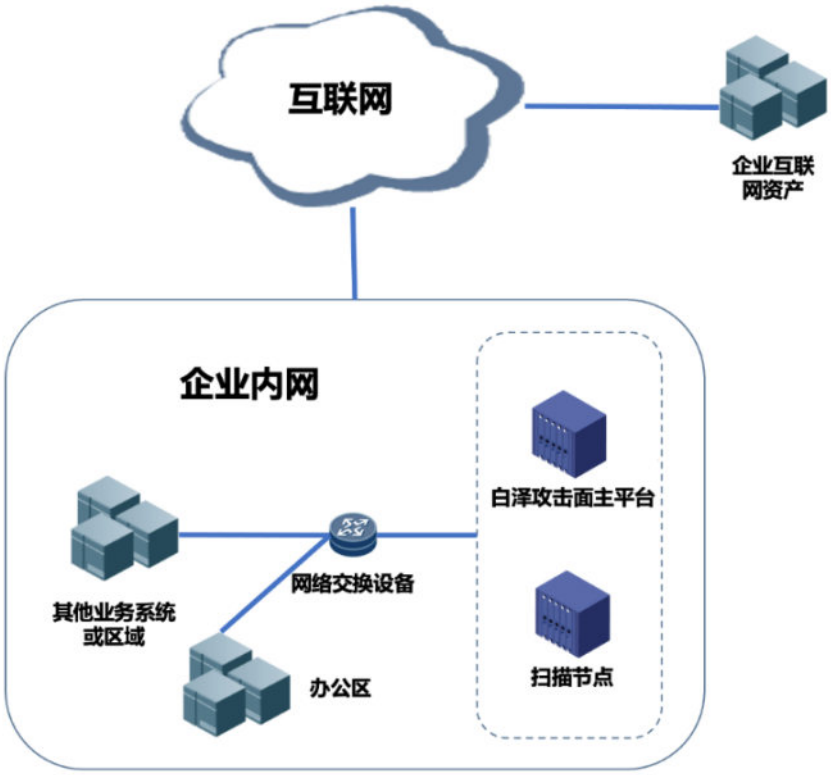
随着西南地区 X 股份银行（以下简称城商行）业务类型和范围的不断扩张，伴随而来的信息化建设和互联网应用业务系统在不断落地和深化，数字资产的管理成为信息工作的关键焦点。数字资产面临的潜在攻击隐患和业务安全漏洞对城商行的业务稳定运行和经营风险构成了挑战，如何去发现和管理成为目前城商行面临的最大的难题。

城商行作为所在地区金融行业的重点企业，关乎相关区域的经济、社会和政治稳定。一直都被作为信息安全管理和建设的标杆企业，每年的攻防演练和实网攻防演习行动都被作为重点关注单位。一方面单位的管理责任很重，另一方面安全管理的能力提升却仍然缺乏技术手段。因此，单位从高层到业务层都希望有更贴合信息安全实战管理的平台重构安全管理能力。

二、方案实施

为确保系统正常运行，降低业务风险，提供高效的服务支持业务发展，必须从该银行的数字资产攻击面方面审视已知资产、未知资产、数字品牌、泄露数据等一系列可存在被利用的风险资产，进行检测发现、分析研判、情报预警、响应处置和持续监控，从安全性方面检查其脆弱性和缺陷。部署攻击面管理系统成为目前较为急迫的事务。

通过部署攻击面管理平台，及时发现新增、变更、注销的互联网资产，确保安全团队全面掌握本企业网络资产暴露面，有效防范敏感信息泄露带来的商誉风险，防御对该城商行的信息系统安全入侵风险。



因为银行是对数据管理要求严格的企业用户，本项目采用在银行本地部署模式：将“主平台、扫描节点”部署到本地，扫描数据也存储在本地。

攻击面管理平台实现：

- 互联网资产暴露面管理：基于分布式监控源，对网上银行、银行关联业务机构、银行系统软件供应链等相关 IT 资产、域名、APP 应用、邮箱等互联网资产进行检测，形成多维度的互联网风险面的暴露报告，揭示城商行互联网暴露面的真实情况。
- 敏感信息暴露检测：监控多平台代码泄露和文档，包含 Git、云盘、社区等，检索与本城商行相关的信息暴露，并对数据进行类型和风险标记。
- 深度安全漏洞识别：银行新上线业务如果有安全漏洞被不法分子利用，易造成提权获取和散播敏感信息、主机被非法挖矿、主机沦为肉鸡被利用等恶劣后果，通过定期扫描和验证系统漏洞及时发现并对网站进行防御准备，防范于未然。
- 可视化分析：通过自定义的数据看板、可配置的安全报表以及多维度的态势大屏展示，全方位展示用户环境的态势情况。

三、效果评估

- 本项目实施后，解决了城商行信息安全监控资源大量投入的问题，信息安全管理部门按需调整自动化攻击面检测的时间周期、检测方式，实现 7x24 小时自动化检测，安全风险问题发现和解决的时效大幅提升。
- 城商行通过落地攻击面管理，通过攻击者视角进行检查，把所有暴露出来的风险可能性完整直观展现在信息安全管理者面前。实现日常安全运营管理、安全检查前的自我审查、攻防演练前的安全预演等场景可视、可控、可预防。
- 项目实施当年，城商行被选定参与当年的攻防演练活动，用户在演练开始之前通过以攻击队视角、先于攻击队掌握可能攻入的突破口及攻击路径，从而做出针对性的修复和加固准备。在整个攻防演练过程中做到了完全不失防、不丢分，获得当年的演练嘉奖。

四、技术服务商简介

北京云科安信科技有限公司创立于 2018 年，创立之初就建立以技术创新驱动风险管理理念，基于自身对互联网风险边界的认知和全新理解，提出了以风险为核心的全新安全边界框架，发布了“数字风险边界模型”，并基于“数字风险边界模型”及“一切风险管理的本质是度量被防御目标的变化”的认知，打造了信息图鉴系列产品矩阵。云科安信技术团队中超过 90%的成员具备多年信息安全从业背景，在证券、银行、保险等金融行业有相当数量的实施案例。

（六）移动安全品牌推荐及项目案例

优秀的移动安全技术服务提供商

梆梆安全的移动安全产品和服务品类的覆盖度全，适配性强，为客户提供移动应用开发、测试、发布和运营阶段的全面安全产品及解决方案，确保其移动应用在各个环节的安全可靠。

持续的技术创新能力

梆梆安全将移动安全领域的技术优势扩展至数据安全，助力客户在API安全防护和APP个人隐私保护等方面构建更加坚固的安全防线。

扎实的金融行业实践经验

金融行业客户涵盖金融监管及审查机构、政策性银行、国有银行、股份制银行、城商行、农商行及保险、证券等近千家金融机构，拥有非常丰富的金融业移动安全服务经验，以技术创新和专业服务为客户提供全方位安全解决方案。

某国有银行端到端全渠道安全监测案例

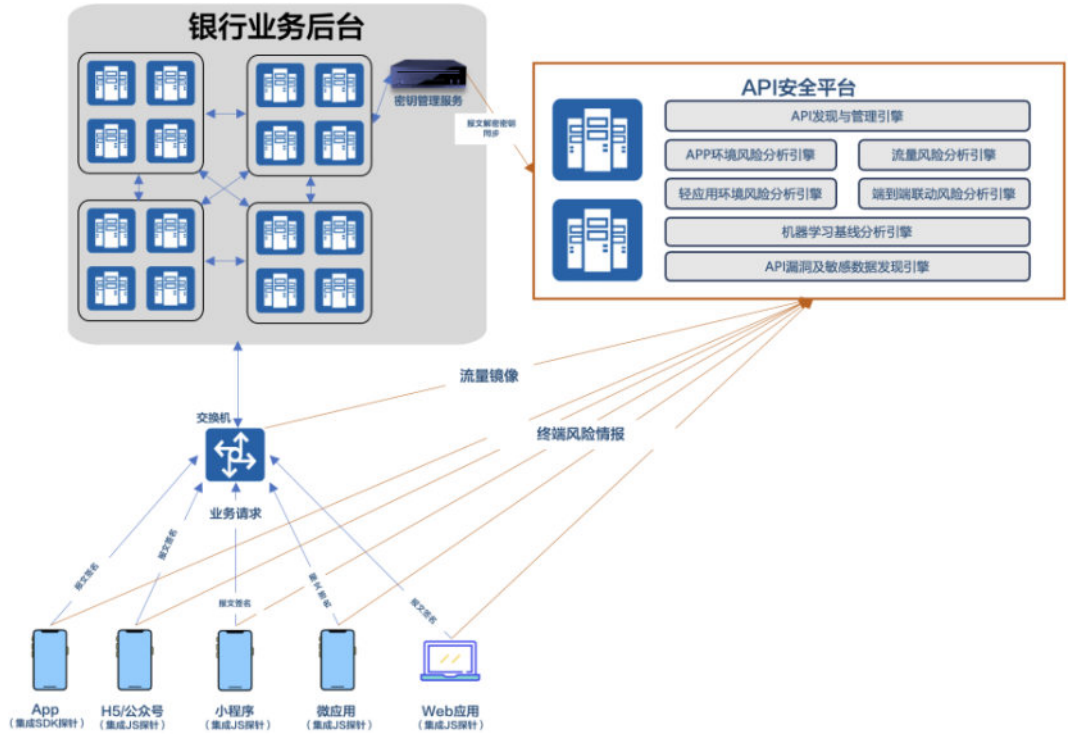
一、项目背景

某大型国有银行在内部的攻防演练中，发现其生产系统的某些互联网侧 API 接口存在越权漏洞，利用此类漏洞可以批量遍历和窃取行方系统中的重要生产数据，导致敏感金融信息泄露等严重问题的发生。在行业监管部门针对数据泄露风险严查高压的态势下，此银行只能暂时下线此类 API 业务，避免风险影响的扩散。

对于此银行来说，虽然已经构建了围绕 App 端的涵盖加固、检测、监测的完整防护体系，但是随着线下渠道线上化和线上渠道多样化的趋势，行方在互联网侧的 API 资产已经成为不可忽视的安全攻击面，并且 API 也正在被 H5、小程序、轻应用等多种新的业务应用形态暴露出来，单纯围绕 App 构建的防护体系已经无法对行方的 API 安全问题进行有效的攻击发现和攻击链溯源了。行方需要建设新的安全防护措施实现针对互联网侧 API 资产的自动化发现管理、攻击发现和攻击溯源评估。

二、方案实施

在本方案中，综合利用先进的后端流量分析技术与前端风险检测技术。在平台侧部署 API 安全平台，对接交换机进行 API 访问流量的镜像接入，实现对 API 访问流量的实时分析；同时，在终端侧的 App 和轻应用内集成 SDK 探针，对终端侧的风险进行深度检测。结合流量侧和终端侧的安全情报，进行综合分析判断，实现 API 资产发现和管理、API 攻击发现、API 漏洞及敏感数据发现等安全能力。



三、效果评估

在本案例中，主要帮助行方实现以下安全效果：

- 渗透嗅探攻击发现：通过集成在终端侧的 SDK 实现传输报文签名，在 API 安全平台监控报文中间人劫持篡改、重放、报文时间异常，同时关注访问设备环境风险情况，形成攻击链，对于黑客进行 API 漏洞的渗透嗅探行为实现了有效的发现。
- 批量刷接口监测：通过报文篡改监测，同时针对 IP、设备、用户等维度进行统计分析，发现某些访问源持续只访问个别接口，访问目标分布不合理，存在 API 接口被批量刷数据的问题。
- 越权漏洞发现：经过行方内部协调，获取了 API 访问报文内层对称加密的解密密钥，对于 API 访问报文传输 body 进行了解密，通过在 API 安全平台配置越权漏洞检测模型相关参数，发现未授权 API 接口访问及横向越权疑似漏洞 API 接口。

四、技术服务商简介

北京梆梆安全科技有限公司（以下简称：梆梆安全）成立于 2010 年，开创、繁荣了移动应用安全市场，建立了全面的移动应用安全防护生态体系，业务上形成以移动安全为主体，联动安全服务和物联网安全的“一体两翼”业务体系，通过专业的安全服务为政府、企业、开发者和消费者等客户打造安全、稳固、可信的网络空间生态环境；技术、产品、解决方案和咨询服务构成“四位一体”的产研体系，做到软件、硬件与控制的多管齐下，逐步实现由软及硬、由内而外的联防联控。目前，梆梆安全拥有 10 万家以上企业及开发者用户，安全技术覆盖的移动应用软件超过 100 万，这些应用已经累计安装在 10 亿个移动终端上，用户遍及金融、互联网、物联网、政府、运营商、企业、医疗、能源、教育等各大行业。

（七）威胁管理品牌推荐及项目案例

科来

深度研判与回溯取证体系，构建安全最后一道防线

率先推出国产化信创平台40GBPS高性能全流量采集与实时分析能力，一体存储全面全量的网络流量数据，深度研判告警事件，为网络攻击追溯、取证及责任判定提供重要依据，构筑网络安全最后一道防线，全力支撑金融机构信创建设，为“关基”安全保驾护航。

全流量分析，全面感知未知威胁

通过威胁检测规则、情报、网络行为模型实时感知网络威胁状态，及时预警可疑网络活动与“未知威胁”，提升金融机构网络恶意活动发现能力和“未知威胁”防御能力。

主动进行网络资产梳理与业务识别，全面掌握威胁动态

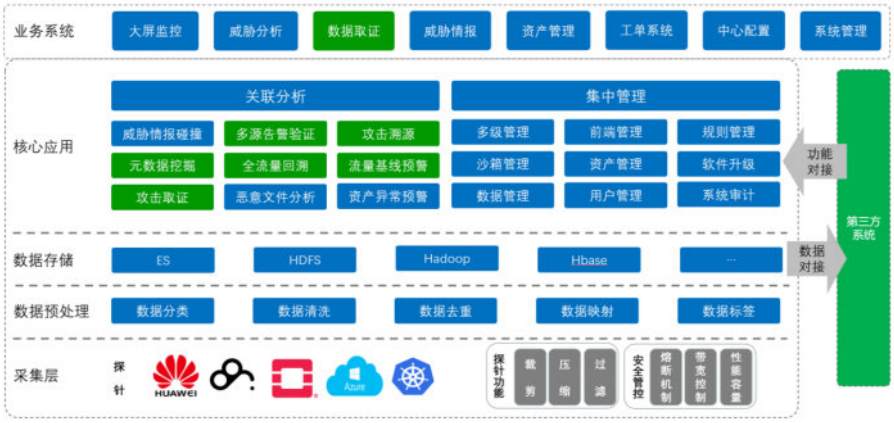
主动梳理网络资产、网络敏感数据，进行业务识别，构建实时更新的网络资产暴露面和敏感数据流转情况，全面掌握数据中心内部网络空间威胁动态，助力金融机构安全运营中心“数智化”转型。

某大型商业银行云上云下安全分析平台建设案例

一、项目背景

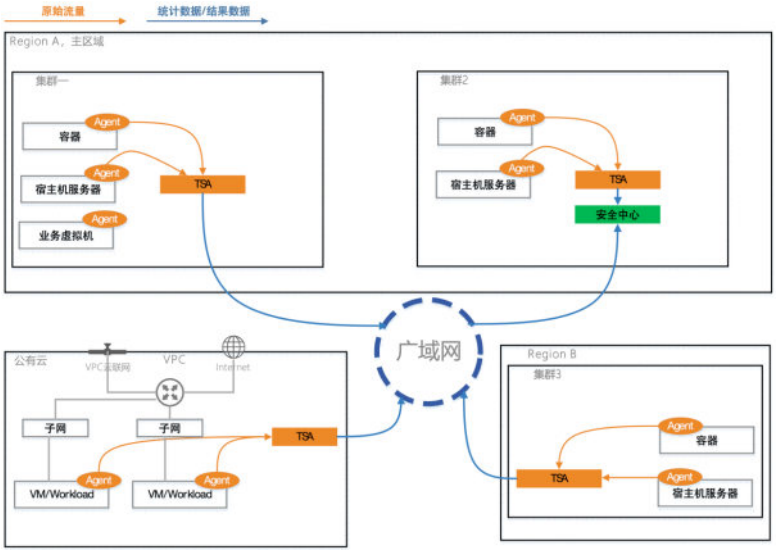
随着云计算技术的广泛应用，某大型商业银行大量业务系统逐渐迁移上云。在整个上云过程中，由于业务系统的特性、对网络带宽和质量的要求、数据的敏感性以及政策合规等多方面原因，该银行选择多个公有云或者混合云等模式部署不同业务系统。多云 IT 架构带来业务方便的同时，也凸显了新的安全问题。包括云上云下安全无溯源手段，安全防护无法保障 100%拦截，当出现安全失陷或 APT 攻击、零 Day 事件时，无有效手段进行溯源分析，安全应急响应及影响评估效率无法突破。

二、方案实施



（方案架构图）

- 核心应用&业务系统（BFC）
  - 面向用户的操作中心，也是唯一门户入口。
  - 接收分析层 TSA 组件上传的结果化数据进行展示。
  - 采集控制器：单区域时可与应用中心统一部署，多区域时在不同区域或不同集群中部署；主要对接云平台信息及管理、监控 Agent。
- 数据存储&数据处理
  - 存储原始数据包，并解析数据内容。
  - 多维度数据关联，如资产和流量关联。
- 流量处理层组件
  - 存储原始数据包，并解析基础统计字段。
- 流量采集层组件
  - 各类 Agent 家族，实现云平台宿主机、虚拟机、容器上流量引流，实现云上的流量采集能力。



支持公有云、私有云、容器云的混合云环境，Agent 可部署于业务虚拟机、宿主机服务器、容器节点上，对云上虚拟机、容器的流量进行全量采集，并对对象的流量进行流量标记，通过 GRE、VXLAN、TCP 等多种流量封装模式将流量送到网络全流量安全分析系统（TSA）。

三、效果评估

◆ 全天候全方位实时地识别网络流量数据

通过与威胁情报、行为模型匹配，发现未知威胁、木马通讯、隐蔽信道等异常行为。利用流量可视化能力，看见资产、看清安全洼地、看透安全隐患，为用户构建灵敏的网络威胁感知能力，展示全方位的网络安全态势。

◆ 云上云下安全的态势早发现、早研判、早预警、早处置

对云上云下网络原始通讯数据进行全流量完整保存，通过秒级提取海量历史流量数据，还原网络安全事件发生时的全部网络通讯内容，实现数据包级的数据取证和责任判断，并对攻击事件的影响和处置效果进行长期跟踪与评估。

◆ 海量数据的快速回溯分析

通过高效的数据检索，实现海量数据的快速回溯分析，可随时分类查看及调用任意时间段的数据，并从不同维度和时间区间，提供 L2-L7 层网络协议统计、会话日志、元数据日志，进行数据逐层挖掘和关联检索。通过深度网络会话关联分析、数据包解码分析、载荷内容还原分析、特征分析和日志分析，真实还原黑客入侵的全过程，从而对网络安全事件进行精准的定性分析。

四、技术服务商简介

科来成立于 2003 年，专注于网络流量分析技术二十余年，致力于让数字化互联智能系统更安全、更可靠、更高效，研发的产品广泛应用于网络安全分析、工控安全、业务性能管理、云网运维等重要领域。

目前，科来的技术已应用于全球 110 个国家和地区，服务于全球 10000+商业用户。在政府、金融、能源、运营商、交通、制造、教科文卫等行业的众多头部客户均采用科来的解决方案，进行数字化转型实践、关键基础设施安全防护与业务连续性保障。

（八）网络与基础架构安全品牌推荐与项目案例

金融行业广泛应用

华为USG系列防火墙在业界同等性能的防火墙中排名第一，在6大行、12家股份制银行、各地方性城商行以及农信等金融客户都有成熟应用。

高可靠和高安全性部署

软硬件多种方式增强网络韧性，提供电信级可靠性，保障金融业务“0”影响。

安全防护能力优秀

专用安全引擎，防御检测性能提升3倍，具备全球威胁样本采集分析能力，基于AI检测方式，威胁检测率达96%；采用动态图谱关联分析技术，威胁实时态势感知，网、安和终端EDR一体化联动，威胁秒级闭环，保护金融业务安全。

某国有商业银行防火墙案例

一、项目背景

某银行全球拥有 1.7 万+个网点以及网银、电话银行和自助银行，服务 1000 万多家公司和 7.2 亿个人客户，持续深化重点发展战略，积极发展金融科技，加快数字化转型，是金融行业的信息化标杆企业。为满足互联网金融和大数据信息化银行业务发展需求，网络稳定性和安全性是业务系统正常运行的重要保障，对其网络架构以及设备的性能有极高的要求。

二、方案实施

华为基于客户的业务应用及实际网络需求分析设计，**推出满足金融业务场景需求的华为防火墙安全防护方案。**该方案部署华为 USG12004 设备，在不同等级的网络区域边界部署防火墙设备，控制不同业务及区域之间的访问并提供安全防护。该方案特点如下：

- 高性能

华为防火墙采用自研多核处理器及分布式硬件平台，创新的混合硬件加速，内置网络加速引擎，实现混合流量模型下的大吞吐量和大象流超强转发能力，同时集成了超高带宽的接口和交换能力，拥有大吞吐量、高新建、高并发、低时延等优势性能，保障业务无忧运行。

- 高可靠

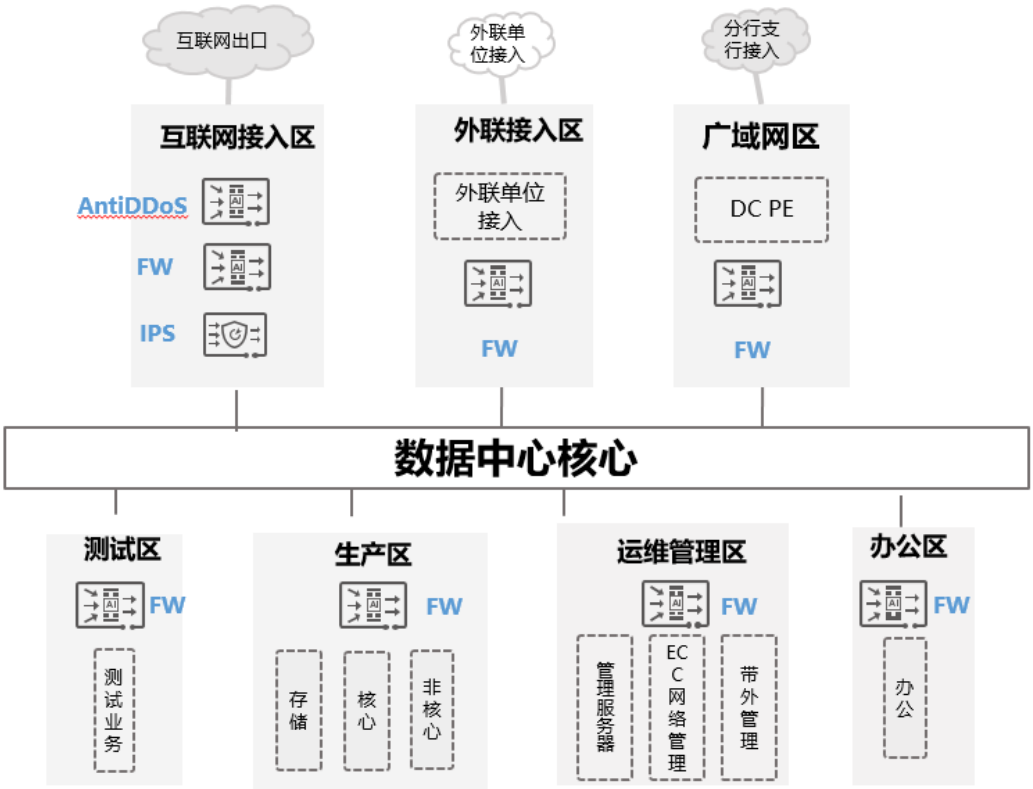
华为防火墙从硬件平台、板卡部件到链路组网、软件平台提供多重可靠性技术保证。管理、检测、数据三层面分离，主控板、接口板、业务板冗余配置，支持热插拔，局部故障不影响业务正常运行。双机热备支持主备、主主、镜像部署模式，创新性提供心跳线断开极限逃生机制，保证高可靠组网。NSR、GR 多种可靠性机制，满足业务对网络的可靠性要求。

- 威胁防护全面

华为防火墙内置模式匹配引擎、加解密引擎和 AI 引擎，提供应用识别、入侵防御（IPS）、反病毒和 URL 过滤等内容安全功能，支持亿级病毒及 URL 过滤，高效防御病毒、木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁，有效保证内网服务器和用户免受威胁的侵害。

- 精细化访问控制

华为防火墙支持五元组、域名、用户、时间段、标签、业务应用、内容安全等多维度的精细化安全策略控制，实现不同业务、不同区域间的隔离与访问控制，阻断非法访问，保障金融业务安全。



三、效果评估

华为防火墙在客户现网部署后，设备运行稳定，在全面保障内容安全业务场景下，防火墙提供业务处理性能 100+Gbps，最大可扩容 400+Gbps，满足未来 5 年的业务发展诉求。数据中心生产区域高可靠部署，双机秒级切换，提供电信级 5 个 9 可靠性。精细化的访问控制帮助用户实现了对各业务区的安全隔离和权限控制，保障内部网络安全。

四、技术服务商简介

华为在安全产品领域沉淀了 24 年的专业经验，始终致力于研发差异化的创新产品。不断将云计算、大数据、AI 等前沿技术与网络安全产品及解决方案的安全能力构建相结合，为客户提供更强大、更智能的安全防护。

华为安全在全球范围汇聚精英，拥有超过 2500 名研发人员与 20 余位科学家和领军人物，专注于安全技术的深度研发与创新。华为已斩获 3000 余项安全专利，在防火墙、DDoS 防御、入侵检测与防御、安全态势感知以及安全云服务等多个领域保持业界卓越地位。

此外，华为在全球 150 多个国家与数万家渠道和合作伙伴建立了紧密的合作关系，共同推动网络安全事业的发展。凭借卓越的产品和服务，华为在全球网络安全市场中占据了重要地位，市场份额位居前列。

（九）信息技术应用创新数据库品牌推荐及项目案例

代码及产权自主可控

SUNDB是拥有完整的自主知识产权和代码自研率高达98.3%的原生分布式数据库，是全球范围内极少数真正自主掌控关系型通用数据库根技术的源厂商，能够合法向全世界所有终端客户发放使用权许可证。SUNDB是真正的中国品牌数据库使用权授权方，实现了法律权限的高度自治，符合国家安全可靠标准。

具备客户实践经验

SUNDB专为数据安全而生，拥有7*24小时链接互联网实时交易的国家关基领域超大型生产系统多年稳定运行典型应用案例，产品规划清晰，战略布局专注服务银行、保险、证券、电信、交通、能源、军工、政府等国家关键信息基础设施的核心业务系统。

中国品牌智能数据库

科蓝SUNDB非开源中国品牌数据库能真正保证国家关键信息基础设施和高端行业的国家级数据安全。底层核心的计算引擎和存储引擎没有任何国外数据库开源代码，与国外甲骨文的MYSQL和伯克利大学的PG等开源数据库无关。科蓝软件已经与清华大学成立“先进智能数据库联合研究院”，致力于打造国际技术领先的AIDB。

江西某省级城市商业银行企业网银系统 SUNDB 应用实践

一、项目背景

江西某省级城市商业银行携手科蓝软件，对企业网银系统进行了技术架构升级和业务重构，采用全栈创新技术，以提升金融产品研发效率和客户业务处理能力。通过分布式微服务架构，系统并发能力和横向扩展能力得到增强，同时前端实现客户端无感更新，动态调整功能布局，提升金融客户体验。该银行基于 SUNDB 分布式数据库进行数据模型设计，充分发挥分布式数据库的计算、存储的优势，支撑用户高并发、高性能的需求，并真正实现了基础软硬件的自主可控。这一举措不仅强化了金融行业的系统性安全，也为该银行带来了更高效、更稳定的业务处理能力。

二、方案实施

该银行企业网银系统搭配科蓝“双鱼座”中台以及科蓝自主知识产权的 SUNDB 分布式数据库，支持分布式微服务，打造企业互联网统一平台。

- 基础软硬件全面创新：在服务器、操作系统、数据库、中间件等核心技术领域实现全面创新，确保产品和服务的完全自主可控，保障其可持续性发展，不受外部环境因素的制约。
- 构建开放敏捷的金融技术体系：为满足金融行业日益增长的业务需求，构建了一个开放且敏捷的全新技术体系框架，确保客户在数字化转型过程中享受到所需的弹性、敏捷性和协同共享能力。
- 利用 SUNDB 实现高效计算与扩展：通过采用 SUNDB 分布式数据库，实现分布式架构能力，满足弹性扩缩容需求，具备线性水平扩展能力，从而满足了业务发展的高扩展性需求。
- 发挥 SUNDB 最大优势：利用 SUNDB 分布式数据库来存储业务数据，并依据其分布式特性、利用内存引擎和磁盘引擎双引擎特性，最大化地发挥分布式数据库在性能、扩展性和可用性方面的优势。
- 分布式微服务架构实现高性能与稳定性：通过采用分布式微服务架构，实现计算能力的下移，并成功确保了系统的线性扩展能力、稳定性运行、性能提升和高可用性，为业务提供了强有力的技术支撑。

三、效果评估

该案例在进行数据模型设计的过程中，通过梳理银行业务数据特点及归纳，依据 SUNDB 分布式数据库的分区能力制定数据模型设计规范，同时进行实际测试验证，确保了分布式数据模型的设计合理、高效。

- 性能提升。主机下移改造的业务应用系统功能满足业务要求，整体系统可靠性达到 99.99% 以上，满足金融行业业务双活、性能提升、稳定运行的要求。
- 技术先进性。构建开放敏捷的全新技术体系框架，满足未来的 IT 发展和业务需求，满足数字化转型所需要的弹性、敏捷和协同共享等。 使用 SUNDB 分布式数据库进行业务数据的存储，并按照分布式数据库特点进行数据模型设计，确保发挥分布式数据库的最大优势。

◆ 创新基础软硬件。创新基础软硬件包括：服务器、操作系统、数据库、中间件等，全面符合创新要求，摆脱对国外厂商的依赖，产品服务的可持续性不受外部环境因素影响。

四、技术服务商简介

科蓝软件公司作为金融科技领域的佼佼者，致力于为金融领域客户提供前沿的数字银行解决方案和数据库技术。公司成功研发了高性能关系型数据库 SUNDB，为金融机构提供了稳定、安全的数据存储解决方案。

科蓝软件的数字银行解决方案同样具有显著优势。该方案结合了先进的云计算、大数据、人工智能等技术，为银行提供了全面的业务支撑和智能化管理。通过与 SUNDB 数据库的紧密结合，数字银行解决方案能够充分发挥数据价值，提升业务决策效率和风险控制能力。

在生产实践方面，科蓝软件拥有丰富的经验，提供一站式端到端的信创解决方案，并注重与客户的深度沟通，以满足客户的个性化需求。这些实践经验使得科蓝软件在金融网络安全领域发挥着重要作用，为金融行业的稳定发展提供了有力保障。

数说安全
CYBERSECURITY REVIEWS

中国信息安全
China Information Security