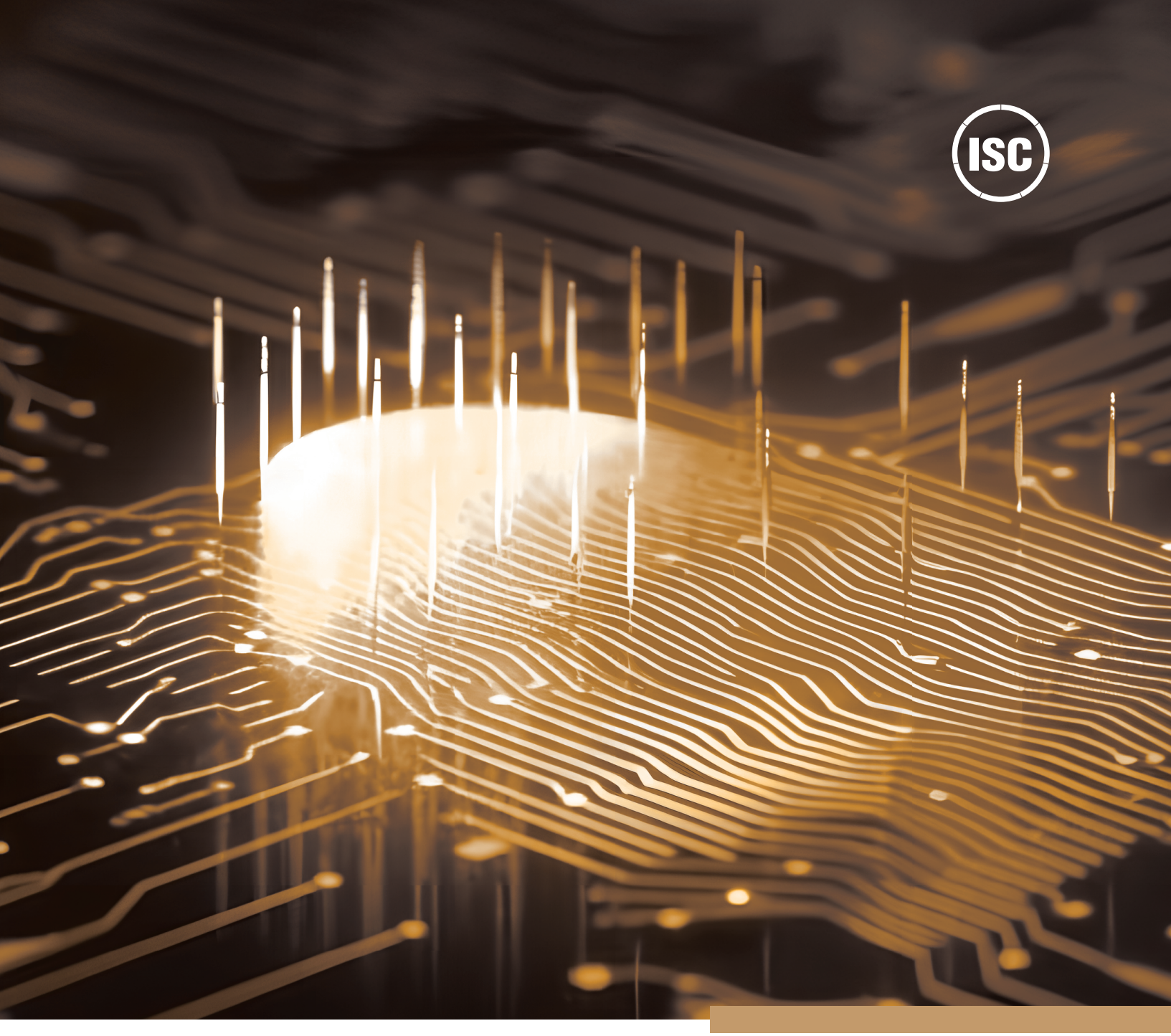


ISC 2024

数据安全技术创新发展报告

关于ISC

ISC成立于2013年，是国内唯一专注为数字安全行业赋能的平台。打造集会展服务、咨询服务、媒体服务、生态创投、安全课、红客社区、生态联盟、产业导入"八维一体"的生态模式，全面赋能国家、政府、行业、企业、个人。过去10年，ISC秉承创新引领、智慧洞察、专业高效的宗旨，创办了亚太地区乃至当今世界规格高、辐射广、影响力深远的全球性安全峰会——互联网安全大会，树立了中国网络安全产业名片。

版权声明

专 | 家 | 寄 | 语

就我自身的观点而言，我认为本报告最具价值的内容是第三章--数据安全技术创新热点及趋势。在此部分内容中，报告列举了最受产业界关注的主流数据安全技术，并各自对多种细分场景的驱动力，需求点，甚至是实现障碍都做出了"言之有物，且行之有效"的实践洞察，同时还给出了相应的解决方案。推荐业内同行，以及广大关注数据安全的人士阅读。

———— 数世咨询创始人 李少鹏

随着数字经济的快速发展，数据成为重要的生产要素，数据安全面临较为严峻的态势，数据安全市场迎来较大机遇。未来，在数字化浪潮的推动下，数据安全市场将与组织的业务场景紧密结合，构建以数据流转为视角的数据全生命周期防护体系。我国数据安全防护与治理产品正在加速与新兴技术融合，不断向新兴领域拓展渗透，越来越注重平台化、运营化的体系建设，逐步形成从事后向事中、事前转变的完整的数据安全防护思路。ISC本次报告中对数据安全态势管理、数据风险评估、数据安全治理等数据安全技术创新热点的介绍反映了这一趋势。此外，报告中丰富的案例相信会对关注数据安全前沿实践的从业者有所裨益。

———— 赛迪顾问总裁助理、软件与信息服务业研究中心总经理 高丹

数据作为新质生产要素，是驱动新质生产力的主要原材料。数据安全成为关乎国家安全与社会经济发展的重大问题。随着网络空间安全、人工智能和大模型技术的快速发展，自身技术突破及新质生产力用户新需求双轮驱动数据安全不断创新发展。该报告从数据安全合规内生需求出发，回顾了我国数据安全行业发展现状，梳理了数据安全态势管理等六个技术创新热点，提出与大语言模型（LLM）结合是数据安全技术创新趋势。选取了六个数据安全技术实践案例进行总结分析，包括案例背景、关键挑战、解决方案、创新与优势、应用效果、经验总结等内容。该报告内容详实、数据来源可靠，对我国数据安全行业相关人员具有较高的参考价值。

———— 北京科技大学计算机与通信工程学院 教授 博导

中国计算机学会高级会员、中国计算机学会计算机安全专委会执行委员 陈红松

国家数据局的成立以及《“数据要素X”三年行动计划（2024-2026）》的发布，意味着构建以数据为关键要素的数字经济，是推动高质量发展的必然要求。在这一过程中，数据安全技术的创新与应用是保证数据要素价值发挥的必备条件。

要实现要素价值发挥，一是要进行数据资产测绘、合规治理等活动确保数据可用性；二是需要确保数据访问、数据计算的安全确保机密性；三是需要数据存储的安全性，避免数据泄露、损坏。

本报告，从未来数据安全技术趋势出发，围绕数据安全使用为核心，分析技术趋势，对于未来数据安全技术的发展，具有一定的参考价值。

———— 华为中国区产业发展专家 刘鑫

由于数据安全应用场景的复杂性对数据安全行业从业人员的综合能力提出了很高的要求，而且需要一定的行业经验，数据安全行业对高水平的数据安全人才的需求非常迫切。我们应该充分发挥科技创新的举国体制优势，由政府相关部门出面组织，数据安全行业企业打破壁垒，贡献积累的历史数据，借助现有的人工智能技术，结合数据安全行业企业多年积累的数据和经验，有望训练出一个有问必答的数据安全行业的专家型机器人，从而降低数据安全企业的人才培养费用。

———— 北京亿赛通科技发展有限公司研究院院长 梁金千

前　言

中美对抗、俄乌冲突、以哈战争…，今天，大国竞争和地缘冲突愈演愈烈导致逆全球化格局的逐渐形成，此前好不容易建立的网络空间国际合作治理已经遭到严重破坏，这给了网络犯罪前所未有的发展空间。有关机构预计2023年网络犯罪将给全世界造成8万亿美元的损失，这相当于全球网络安全收入的40倍。我之砒霜，汝之蜜糖。巨大的经济利益激发了黑客无比的创新热情，在层出不穷的安全事件中，我们可以看到大语言模型、AI深度伪造、CaaS平台等前沿技术的身影，平台化服务已经使得网络犯罪不再有技术门槛，向分工化、分散化、规模化的方向狂奔。既有精准狙击，也有无差别扫射，政府和企业的数字化转型和生存真正成为了一个塔防游戏，安全底座不牢，开局就是终局。

至暗时刻也许就要到来，而被寄予守护世界厚望的网络安全行业则处于发展的寒冬。2023年国内26家上市网络安全企业有3/4处于亏损状态，前3季度的融资率同比下降超过50%，“供给质量不高，需求释放不够，产融合作不深，人才队伍不足”四大痛点未见好转，就像痛风，在大环境的寒气下，让整个行业更加疼痛了。何时能够在合规产品的同质化红海里停止厮杀？何时能够共同直面和解决强大对手不断制造的新问题？只有创新才能对抗创新！这是ISC平台上下求索和苦苦等待的。勿以善小而不为，行业在创新上迈出的每一小步都是ISC平台不会错过的。我们会通过技术创新系列报告的形式，告诉同行们，这个方向有人还在攀登。本期《2024数据安全技术创新发展报告》主要介绍了数据安全政策、行业、技术的最新发展，基于目前的浅见，我们认为政策法规监管要求和外部威胁引发的内生需求是推动数据安全行业和技术创新发展的核心力量。数据安全行业政策红利明显，但市场表现低于预期，内耗严重，创新不足是主要原因。数据安全行业未来的增长将更多的依赖创新，通过解决更多场景的问题对用户的需求进行开发和释放。数据安全风险识别、推动数据要素安全共享以及平台化集成各种成熟单点技术是目前数据安全技术创新的主风向。此外，随着人工智能大模型的横空出世，大模型在数据安全领域的应用正变得越来越普遍，与大语言模型（LLM）的结合是未来数据安全技术创新的必然趋势。最后，本报告中详细收录了6个数据安全创新技术的最佳实践，相信这些实践经验会对行业同类项目的实施有所裨益。

梅花香自苦寒来，没有“知其不可而为之”的精神，今天的世界谁还会坚守网络安全？而今天世界的“为之”是为了交给明天一个更好的世界。

ISC平台与你同行

2023.12

主要结论

随着我国新质生产力的高速发展，数据要素正在成为核心生产要素，数据安全倍受关注，行业进入快速发展期，国家合规监管要求和外部威胁引发的组织内生需求是推动数据安全行业和技术创新发展的核心力量。一方面数据安全被纳入总体国家安全观，进行顶层设计和合规监管，这是由国际竞争安全形势和国家发展战略所决定的；另一方面，国内外数字安全环境日趋恶劣，针对高价值数据的勒索攻击日渐猖獗，不断威胁各领域的机构运营，数据安全成为运营安全的内生需求。

数据安全行业政策红利明显，但市场表现低于预期，场景挖掘不够充分，人才和创新不足是主要原因。数字经济的运行中，数据安全工作需要围绕核心业务数据的流动来开展，要根据具体的业务场景和数据安全生命周期各环节的要求，配置相应的安全策略及安全工具，设计最佳数据安全解决方案。由于各行业的业务场景复杂而且繁多，现阶段紧密贴合业务的数据安全需求没有得到充分挖掘和释放，具体表现为数据安全产品场景少、同质化严重、成熟度不高、单点产品盛行等。除产品以外，数据安全的人才和服务亦存在巨大的缺口，阻碍了行业的高速发展。

数据安全行业未来的增长将更多的依赖创新，通过解决更多业务场景的问题对用户的需求进行开发和释放。数据安全与业务场景紧密结合，就必须以数据流转为视角构建数据全生命周期的防护体系，因为只有实现高效安全的数据流转才能创造数字经济价值。勒索攻击是当前及未来数据安全最大的威胁，而对勒索攻击亡羊补牢不如防患未然。因此事前的数据安全风险识别、风险评估、态势感知、安全服务边缘、安全治理类产品会很有市场，这些产品是数据安全防护体系逐步从事后向事中、事前转变的重要支撑。另一方面，打通数据壁垒，推动数据要素能够高效安全的共享、流通、使用是另一个重要需求。因此，隐私计算、同态加密、数据合成等技术将会有更多的应用场景和空间。最后，系统化、平台化集成各种成熟单点技术、管理流程，减少内部复杂性，提高运营效率的数据安全管控平台类产品将会逐步取代现有的分散的单点产品，成为政企用户数据安全管理的重要基础设施。以上场景构成了当前数据安全技术创新的主风向。

此外，随着人工智能大模型的横空出世，大模型在数据安全领域的应用正变得越来越普遍，在威胁检测和响应、安全运营自动化、欺诈检测、数据泄露和隐私保护、智能合约和区块链安全、安全智能体（AI Agent）等场景的应用纷纷涌现，赋能提升数据安全态势感知、风险研判等能力水平。尤其是安全智能体，承接了安全大模型"知"的能力，和各类安全工具"行"的能力，能够对安全任务进行记忆、分析、规划和行动，同时能够运用自然语言与安全运营人员进行交流、协同。可以肯定，安全智能体将在安全运营自动化和安全人员互动培训等场景发挥核心作用，大幅提升运营效率和降低培训、沟通成本，为高效完成海量安全运营工作，有效弥补安全运营人力不足带来希望。因此，与大语言模型（LLM）的结合将是未来数据安全技术创新的必然趋势，并有望给行业带来真正的变革。

目 录 CONTENTS

一、数据安全发展的驱动力量

1.1 我国已逐步完成数据安全顶层设计，基本建成政策法规监管体系 02

1.2 数字化生存环境威胁之下，数据安全成为机构运营安全的内生需求 08

二、数据安全行业发展现状

2.1 政策红利明显，为数据安全产业发展制定出明确的量化指标 12

2.2 市场表现低于预期，内耗严重，创新不足，数据安全需求没有得到释放 12

2.3 围绕数据安全的人才和服务存在巨大需求 13

三、数据安全技术创新热点和未来趋势

3.1 数据安全态势管理（DSPM） 15

3.2 数据风险评估（DRA） 17

3.3 数据安全治理(DSG) 18

3.4 安全服务边缘(SSE) 19

3.5 同态加密(HE) 20

3.6 数据合成 22

3.7 与大语言模型（LLM）结合是未来趋势 23

四、数据安全技术的最佳实践

4.1 360数字安全：XX头部国有股份制银行数据安全平台建设项目 26

4.2 炼石：基于免改造数据安全技术的工业领域数据安全保护方案 34

4.3 美创科技：某“双一流”高校的数据安全治理实践之路 43

4.4 东方通网信：电信行业数智一体化数据安全管控产品解决方案 48

4.5 数安行：证券信息系统数据安全计算与安全计量项目 53

4.6 一知安全：XX头部汽车制造商终端全场景数据安全防护系统建设项目 57

01

数据安全发展的驱动力量

1 | 数据安全发展的驱动力量

2022年我国数字经济规模达50.2万亿元，占国内生产总值比重提升至41.5%位居全球第二，彰显我国高度重视数字经济发展，持续促进数字技术和实体经济深度融合，协同推进数字产业化和产业数字化，加快建设网络强国、数字中国，已取得的突出成就。

根据IDC最新发布的GlobalDataSphere2023报告显示，我国数据量规模将从2022年的23.88ZB增长至2027年的76.6ZB，年均增长速度CAGR达到26.3%，为全球第一，政府、媒体、专业服务、零售、医疗、金融为主要数据产生的领域。在《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》等政策的持续推动下，“数据要素”概念逐渐成形，强调对数据信息的价值开发、产业赋能和流通利用。数据作为新质生产要素，是驱动新质生产力的主要原材料，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各环节，深刻改变着生产方式、生活方式和社会治理方式。

伴随着国计民生的运行逐步转移到由数据驱动的基础设施和各类应用上，数据安全必然成为事关国家安全与经济社会发展的重大问题。当前数据安全形势十分严峻，维护数据安全的责任重大。一方面数据安全被纳入总体国家安全观，进行顶层设计和合规监管，这是由国际安全竞争形势和国家发展战略所决定的；另一方面，国内外针对高价值数据的勒索攻击日渐猖獗，不断威胁各领域的机构运营，数据安全亦成为各领域机构运营安全的内生需求。这两方面因素是驱动数据安全行业和技术创新发展的核心力量。

1.1 我国已逐步完成数据安全顶层设计，基本建成政策法规监管体系

1.1.1 数据安全政策法规密集出台

2015年7月1日起施行的《国家安全法》规定：“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”。

2017年6月1日起施行的《网络安全法》规定：“国家鼓励开发网络数据安全保护和利用技术”，“任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动”。

2020年3月30日印发的《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》指出：“制定数据隐私保护制度和安全审查制度。推动完善适用于大数据环境下的数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护。”

2021年9月1日起施行的《数据安全法》规定：“维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。”该法的起草过程中，明确提出了“没有数据安全就没有国家安全”，这在历史上是首次。《数据安全法》还以法律的形式规定：“中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。”目前，国家数据安全工作协调机制已经到位，国家数据安全顶层设计基本完成。

2021年11月1日起施行的《个人信息保护法》明确提出“国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。”凸显个人信息保护不仅针对个人权益而且事关国家安全。

2022年12月2日印发的《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》（数据二十条）指出：“完善治理体系，保障安全发展。统筹发展和安全，贯彻总体国家安全观，强化数据安全保障体系建设，把安全贯穿数据供给、流通、使用全过程，划定监管底线和红线。加强数据分类分级管理，把该管的管住、该放的放开，积极有效防范和化解各种数据风险，形成政府监管与市场自律、法治与行业自治协同、国内与国际统筹的数据要素治理结构。”

2023年1月3日印发的《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》提出**到2025年，数据安全产业基础能力和综合实力明显增强，产业规模超过1500亿元，年复合增长率超过30%。**到2035年，数据安全产业进入繁荣成熟期。

2023年2月，中共中央、国务院印发《数字中国建设整体布局规划》提出“要强化数字中国关键能力。筑牢可信可控的数字安全屏障。切实维护网络安全，完善网络安全法律法规和政策体系。增强数据安全保障能力，建立数据分类分级保护基础制度，健全网络数据监测预警和应急处置工作体系。”

2023年3月，《党和国家机构改革方案》指出，组建国家数据局，负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，推进数字中国、数字经济、数字社会规划和建设等，为数据安全治理提供强力支撑。

2023年4月《商用密码管理条例》在1999年发布的24年后重新修订发布，旨在规范商用密码应用和管理，鼓励和促进商用密码产业发展，保障网络与信息安全，推动商用密码技术的研发和应用，促进数据安全产业的发展。

2023年12月国家数据局发布《"数据要素×"三年行动计划（2024—2026年）（征求意见稿）》推动数据要素在智能制造、智慧农业、商贸流通等十二个事关国计民生的领域的重点行动。

伴随着一系列围绕数据安全的顶层政策法规的密集出台，以及主管单位组织架构的完善，细分领域和地方性的实施细则、标准和创新试点纷纷涌现。据不完全统计，仅2023年上半年就有91项网络与数据安全相关文件发布，包括13项国家政策法规、10项重点行业政策、21项地方政策规章、31项国家技术标准、16项重点领域报告。

1.1.2 数据安全治理制度的顶层设计基本确立

目前，通过法律法规和政策文件，我国确立了以下主要的数据安全制度：

一是数据交易管理制度。用以规范数据交易行为，培育数据交易市场。从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核资料、交易记录。下一步将出台专门管理办法，对数据交易机构的设立条件、运行规则、监管要求等予以明确。

二是数据分类分级制度。按照《数据安全法》规定，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家已明确数据分为三级：一般数据、重要数据、核心数据，后两者直接关系国家安全。各地区和各部门可根据实际情况，明确本地区、本部门的数据分类分级方法，对重要数据和核心数据进行重点保护。

三是数据安全审查制度。对影响或者可能影响国家安全的数据处理活动进行国家安全审查。为了落实这一制度，国家网信办等十三个部委联合公布了修订后的《网络安全审查办法》，于2022年2月15日起施行。该办法将网络平台运营者开展数据处理活动纳入审查范围，防范核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险。审查制度还明确要求对国内企业赴国外上市活动进行审查，以防范上市企业存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险。

四是数据出境安全管理制度。鉴于数据安全的重要性，主权国家应当对数据出境实施安全管理。为此，我国对两类数据建立了出境安全评估制度，一类是重要数据，另一类是批量个人信息以及关键信息基础设施运营者掌握的个人信息。2022年9月1日起，《数据出境安全评估办法》正式实施。对个人信息出境，我国探索设立了认证途径和标准合同途径。当今世界，所有跨境贸易的实质都是数据跨境流动，故该议题已成为国

际贸易规则重构的焦点，各国高度关注却远未达成共识，今后的国际博弈将更加激烈。

五是出口管制制度。国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。这一规定具有重大意义，是我国《出口管制法》在数据领域的落实。

六是对等反制制度。我国法律规定，任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。目前美西方国家以数据安全为由，全方位对我国围追堵截，遏制我国高新技术发展，故这一制度有着重要的现实意义。

七是跨境数据司法调取审批制度。美国《澄清境外合法使用数据法案》规定，在美国政府执法、司法机构提出要求时，任何美国企业在他国收集存储的数据都要交给美国政府。这种"长臂管辖"是对他国司法主权的严重侵犯。为维护我国国家安全利益，《数据安全法》规定，非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

1.1.3 数据安全落地实施的国家标准体系不断完善

数据安全国家标准是开展数据安全监管，规范行业数据安全要求，指导网络运营者提升数据安全能力的重要抓手，对促进数据应用规范化、提升数据活动安全性有着重要意义。目前，全国信息安全标准化技术委员会（SAC/TC260，简称"信安标委"）已开展9项数据安全标准研制项目，其中，已发布标准4项，在研标准5项。

数据安全系列国家标准

全国信息安全标准化技术委员会（SAC/TG260.简称"信安标委"）

分类分级保护
《网络数据分类分级要求》
《重要数据识别指南》
《重要数据处理安全要求》

安全要求类标准
·GB/T 35274《大数据服务安全能力要求》修订中
·GB/T 37932-2019《数据交易服务安全要求》
·GB/T 39477-2020《政务信息共享 数据安全技术要求》

全流程数据安全治理

实施指南类标准
CBVT 27973-2019《大数据安全管理指南》
GBT 39725-2020《健康医疗数据安全指南》
《电信领域大数据安全防护实现指南》

个人信息保护
GB/T 35273-2020《个人信息安全规范》
GB/T 41391-2022《移动互联网应用程序(APP)收集个人信息基本要求》

安全要求类标准
GBVT 37988-2019《数据安全能力成熟度模型》
GBV/T 41479-2022《网络数据处理安全要求》

分类分级保护是数据安全治理工作的第一步，《网络数据分类分级要求》在2022年9月14日公开征求意见，数据分类分级工作首先要参考这个国标，在识别和保护重要数据方面，也要参考《重要数据识别指南》和《重要数据处理要求》。

涉及使用和处理大量个人信息的企业或组织要参考GB/T35273-2020《个人信息安全规范》和GB/T41391-2020《移动互联网应用程序（APP）收集个人信息基本要求》。

数据安全系列国家标准分为三个类别：安全要求类标准、实施指南类标准和检测评估类标准，企业或组织参考标准的重点和阶段不同。

安全要求类标准：GB/T35274《大数据服务安全能力要求》修订中，GB/T37932-2019《数据交易服务安全要求》，GB/T39477-2020《政务信息共享数据安全技术要求》；

实施指南类标准：GB/T27973-2019《大数据安全管理指南》，GB/T39725-2020《健康医疗数据安全指南》，《电信领域大数据安全防护实现指南》。

检测评估类标准：GB/T37988-2019《数据安全能力成熟度模型》，GB/T41479-2022《网络数据处理安全要求》。

数据安全治理是以"让数据使用自由而安全"为愿景，旨在安全有序推动数据流动，平衡数据发展与数据安全，其方法论的核心内容包括：

·满足数据安全保护（Protection）、合规性（Compliance）、敏感数据管理（Sensitive management）三个需求目标;

·以数据为中心的分类分级安全治理内容包括：分类分级（Classifying）、角色授权（Privilege）、风险评估（Assessment）、场景化安全（Scene）；

·数据安全治理的建设步骤包括：组织构建、资产梳理、策略制定、过程控制、行为稽核和持续改善;

·核心安全框架为数据安全人员组织（Person）、数据安全使用的策略和流程（Policy&Process）、数据安全技术支撑（Technology）三大部分。

随着国家标准体系的逐步完善，组织在全流程的数据安全治理过程中，要更多地参照国标要求，应对数据安全挑战，形成一套包括组织、制度、技术和运营四个方面，贯穿整个组织架构的数据安全规划和平台建设。

1.1.4 数据安全监管体系构建完成

在最高层级方面，中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实

施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

在监管层级方面，明确各行业监管部门均负有数据安全管理职责，确定各部门、各地区分工负责的管理模式。具体为国家网信部门负责统筹网络数据安全监管，公安机关、国家安全机关在职责范围内承担数据安全监管职责，工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

在监管实施方面，明确各行业监管要求和监管内容，包括：

1.数据分级分类要求：要求通过数据的分类分级，明确不同数据的管理权限，对于不同类型和等级的数据，企业在数据处理、数据出境时将遵循不同的程序要求，履行相应的批准程序。

2.建立重要数据的保护制度：形成国家级的重要数据目录以及各地区、各部门将确定本地区、本部门以及相关行业、领域的重要数据具体目录，围绕目录建立重要数据保护制度。

3.要求明确开展数据处理活动的安全保护义务，落实等级保护管理工作：

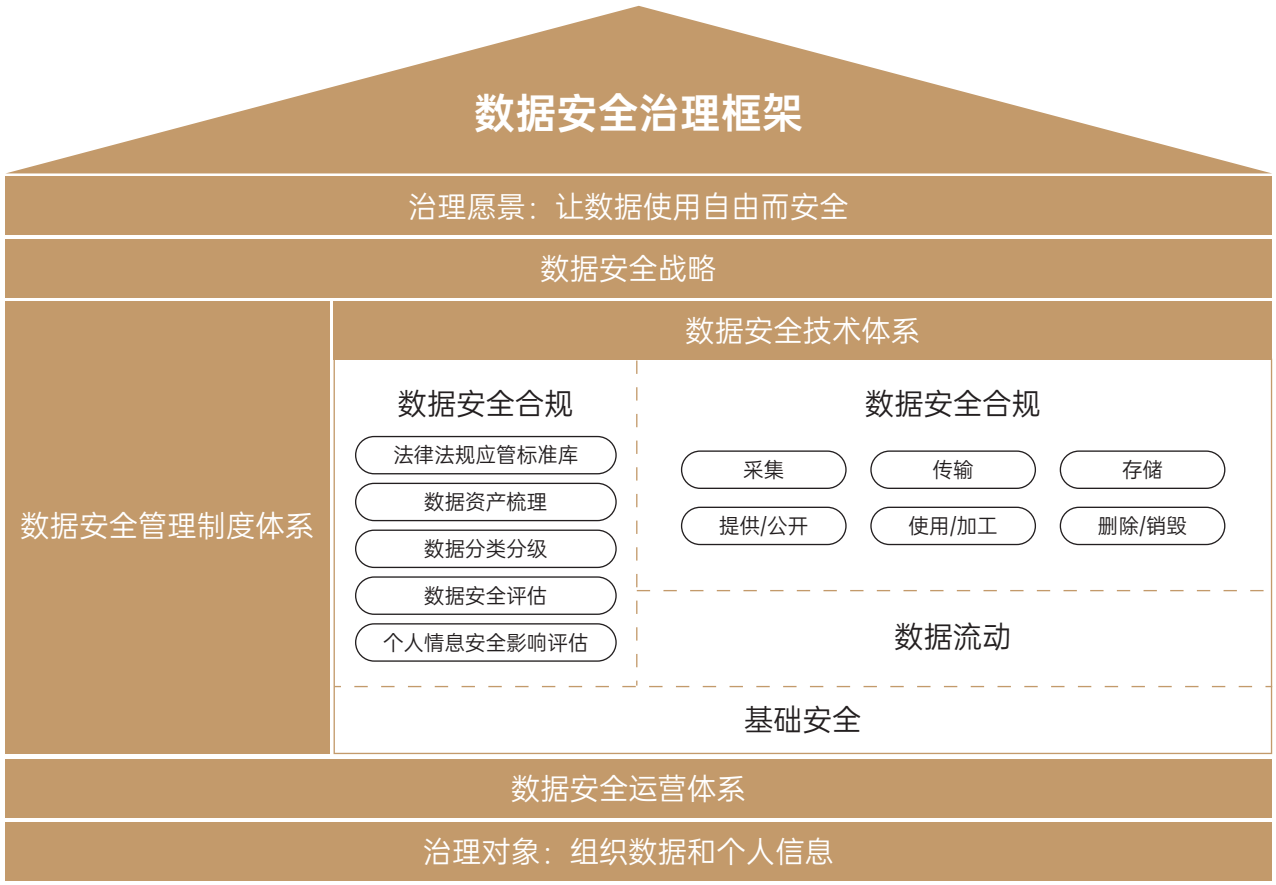
- 数据资产、数据流转和数据风险梳理；
- 建立健全全流程数据安全管理制度；
- 组织开展数据安全教育培训；
- 采取相应的技术措施和其他必要措施，保障数据安全；
- 利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行数据安全保护义务；

进行数据安全风险评估及应对，及时应对处理安全事件；

采取合法、正当方式收集数据，并在法律、行政法规规定的目的和范围内收集、使用数据，不得超过必要限度等。

4.明确向境外提供数据的监管适用情形，禁止未经批准向境外提供境内个人信息和重要数据信息：数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，对于国家网信部门规定的需要申报的数据出境安全评估情形应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

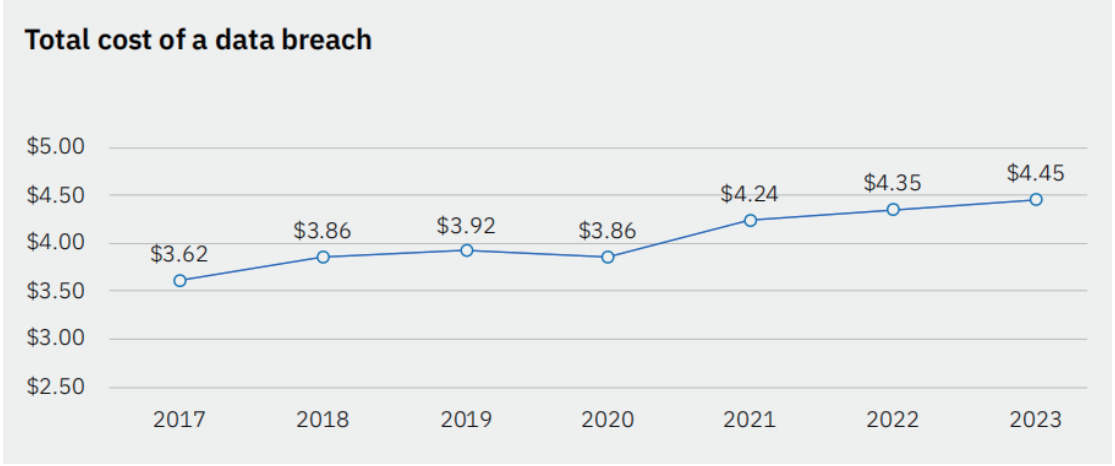
5.要求数据中介服务机构的数据交易行为需持牌经营，合规经营：将数据中介服务商纳入规范范畴，明确中介机构应要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

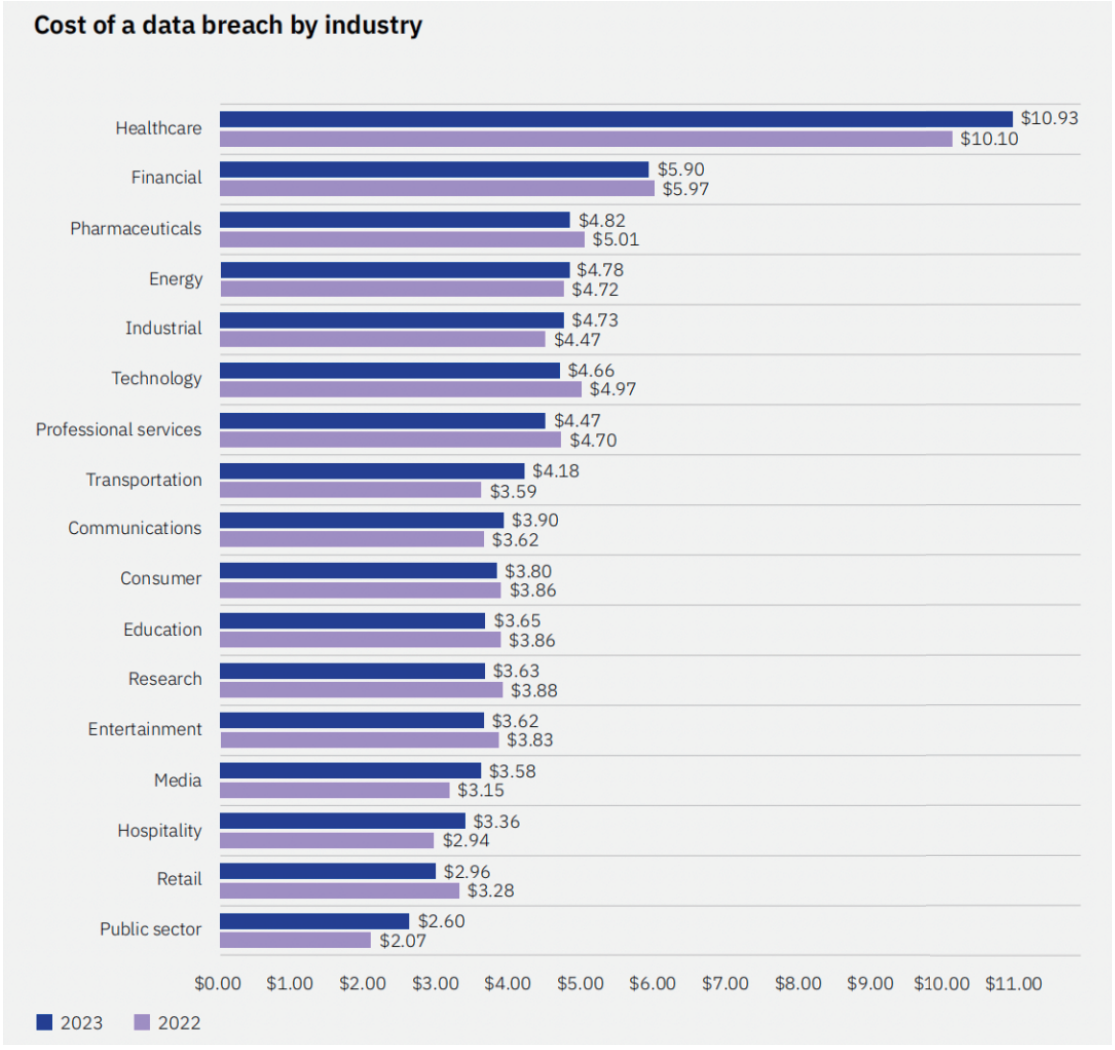


1.2 数字化生存环境威胁之下，数据安全成为机构运营安全的内生需求

2023年全球数字化生存环境面临更为严峻的威胁形势，据相关研究机构统计2023年全球由于网络安全造成的经济损失预计将超过8万亿美元，并将在今后的几年内保持两位数的高速增长。

针对数据的勒索软件仍然是2023年的头号网络安全威胁。勒索软件是最危险的黑客攻击类型之一，因为它实施起来相对容易且成本低廉。在平均每10秒发生一次的勒索软件攻击之下，全球71%的组织都遭受过不同程度的伤害，将近一半的网络攻击都针对小型企业。60%遭受勒索软件攻击的企业会支付赎金以取回数据，许多人支付不止一次。据IBM发布的《2023年数据泄露成本报告》，数据泄露的平均成本在2023年达到历史新高，为445万美元，比2022年的435万美元增加了2.3%，从长期来看，平均成本比2020年报告中的386万美元增加了15.3%。其中，医疗保健行业是数据泄露的重灾区，连续3年位居榜首，平均成本为1093万美元，相比2020年成本上升了53.3%。值得关注的是，所有的数据泄露事件中，80%是有组织犯罪。


Total cost of a data breach
$5.00
$4.50
$4.00
$3.50
$3.00
$2.50
$3.62
$3.86
$3.92
$3.86
$4.24
$4.35
$4.45
2017
2018
2019
2020
2021
2022
2023


Cost of a data breach by industry
Healthcare $10.93 $10.10
Financial $5.90 $5.97
Pharmaceuticals $4.82 $5.01
Energy $4.78 $4.72
Industrial $4.73 $4.47
Technology $4.66 $4.97
Professional services $4.47 $4.70
Transportation $4.18 $3.59
Communications $3.90 $3.62
Consumer $3.80 $3.86
Education $3.65 $3.86
Research $3.63 $3.88
Entertainment $3.62 $3.83
Media $3.58 $3.15
Hospitality $3.36 $2.94
Retail $2.96 $3.28
Public sector $2.60 $2.07
$0.00 $1.00 $2.00 $3.00 $4.00 $5.00 $6.00 $7.00 $8.00 $9.00 $10.00 $11.00
2023
2022

据2023年度IBM发布的《IBMX-Force威胁情报指数报告》，在X-Force2022年所监测到的所有网络攻击中，亚洲遭受的攻击占了近三分之一，超过其他任何地区，其中，在亚洲地区所观察到的所有攻击案例中，制造业占了近一半。另据全球领先的网络安全解决方案提供商CheckPoint软件技术有限公司发布的2023年第一季度全球网络攻击形势报告的数据，亚太地区每个机构平均每周受到1835次攻击，仅次于非洲地区的1983次，同比增幅最大、攀升16%。在实施勒索计划时，网络犯罪分子往往会瞄准最脆弱的行业、企业和地区，并施加巨大的心理压力，迫使受害者支付赎金。鉴于对停工时间的容忍度极低，制造业已连续两年成为遭受勒索攻击最多的行业，作为制造业大国的我国，正在面临严峻威胁。根据国家信息安全漏洞库（CNNVD）收录情况，2023年上半年新增漏洞12361个，高危和超危漏洞占比超过50%，漏洞危害程度趋向高危化，极易被病毒、木马、黑客利用，导致系统安全风险加大。据相关平台统计，2023年上半年我国遭受恶意软件攻击总次数接近150亿次，受攻击的重点目标行业包括医疗、科研教育、政府、金融和制造业等，受攻击的重点区域有广东省、浙江省、上海市、江苏省、山东省和北京市等。2023年上半年累计发现涉及我国的重要数据泄露事件超过100起，政府和教育行业是数据泄露的重灾区，两个行业数据泄露占比超过60%。2023年上半年，有超过30家国内企业被国际勒索组织公开泄露数据，主要包括账号凭证、API接口权限、网络访问权限、个人敏感信息、企业隐私数据等。

在越来越恶劣的数字化生存环境下，数据安全是当今组织的首要考虑因素。虽然数据可以是组织最大的资产之一（帮助做出更好的决策、实施战略计划以及建立更牢固的客户和合作伙伴关系），但如果不采取措施保护数据，它也可能成为组织最大的负债之一。例如，威胁到数十亿客户机密信息的数据泄露事件不仅会给组织带来经济损失，还将降低品牌价值并侵蚀客户信任。随着黑客变得越来越老练，组织采用更先进的技术和方法来保护数据安全的需求变得越来越主动和迫切。数据安全毫无疑问的成为了保障组织运营安全最重要的内生需求。

02

数据安全行业发展现状

2 | 数据安全行业发展现状

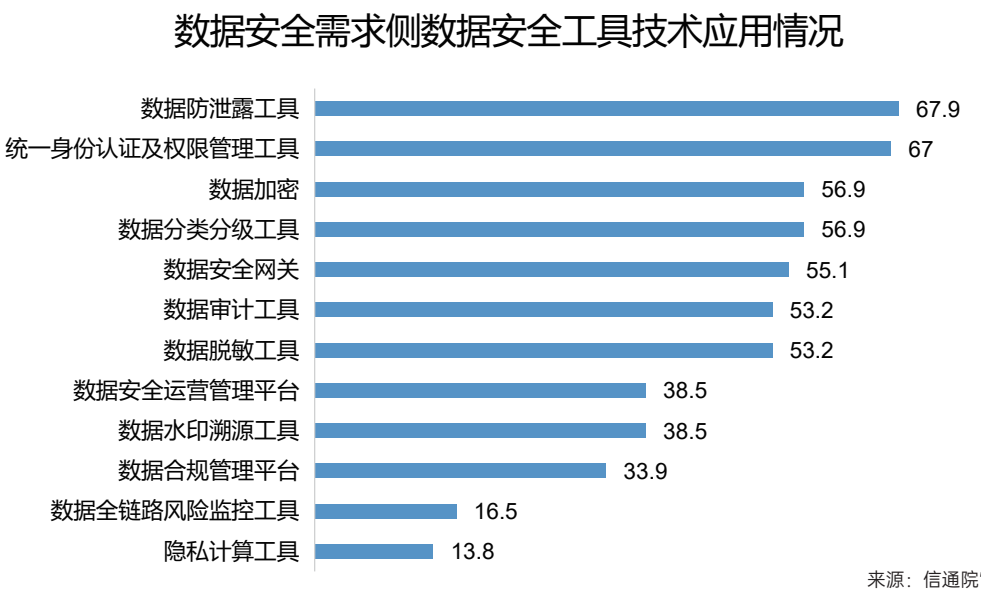
2.1 政策红利明显，为数据安全产业发展制定出明确的量化指标

2023年1月13日，工信部等十六部门发布《关于促进数据安全产业发展的指导意见》。《意见》指出我国数据安全产业要加强核心技术攻关，构建数据安全产品体系，布局新兴领域融合创新；推进规划咨询与建设运维服务，积极发展检测、评估、认证服务；推进标准体系建设与技术产品应用，并且最终构建繁荣产业生态。《意见》明确提出到2025年，我国数据安全产业基础能力和综合实力显著增强，数据安全产业规模超过1500亿元，年复合增长率超过30%；建成5个省部级及以上数据安全重点实验室，攻关一批数据安全重点技术和产品;打造8个以上重点行业领域典型应用示范场景，推广一批优秀解决方案和试点示范案例;建成3-5个国家数据安全产业园、10个创新应用先进示范区，培育若干具有国际竞争力的龙头骨干企业、单项冠军企业和专精特新"小巨人"企业等具体量化指标。

2.2 市场表现低于预期，内耗严重，创新不足，数据安全需求没有得到释放

在政策红利的推动下2023年数据安全产业的市场表现却明显低于预期。据赛迪研究院发布的《中国数据安全防护与治理市场研究报告　　(2023)》，2023年数据安全防控与治理市场规模达到146.4亿元，增速为23.8%左右，明显低于30%+的预期。其原因一方面是受到全球经济增速放缓的影响，另一方面是行业内耗严重，创新不足的表现，数据安全的真正需求并没有被挖掘和释放出来。ISC分析认为行业未来的发展要靠针对高需求用户的细分需求场景提供差异化的创新产品来实现突破。

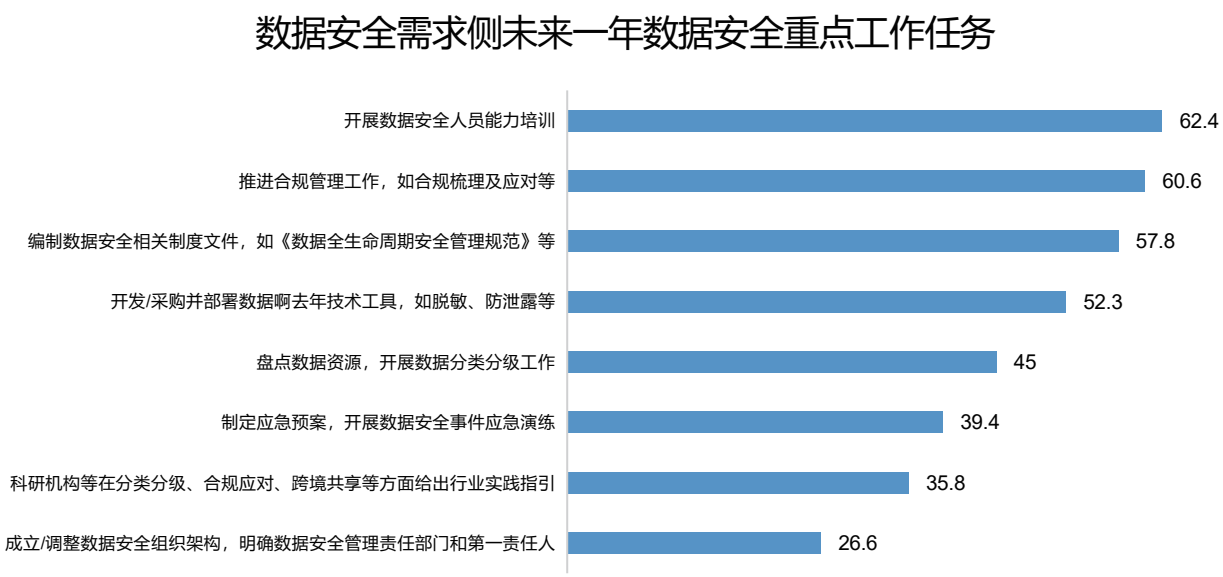
一个现实是我国数字化转型虽然已经取得瞩目成就，但是多数转型企业仍处于"上云用数赋智"三阶段的前两个阶段，对数据要素价值的认知和运用都处于较低水平。由于对数据的价值缺少切实体会，保护数据安全的意识主要来自于政策要求和媒体宣传，从而导致数据安全工作往往会流于表面和形式，表现为合规导向、零散不系统。这种现状也助长了数据安全产品同质化严重、单点产品盛行，对整个行业的发展产生不利影响。从**信通院数据安全推进计划**的一项调研可以看到，企业购买最多的是"数据防泄漏工具"、"统一身份认证及权限管理工具"、"数据加密"、"数据分类分级工具"等单点合规产品，就是这一现状的体现。从另一方面看，正是由于对企业的需求开发远远不足，数据安全企业通过创新实现快速的市场增长将存在巨大机会。



来源：信通院"数据安全推进计划"

2.3 围绕数据安全的人才和服务存在巨大需求

企业对数据安全的另一个巨大需求是对人才和服务的需求。由于数据安全是一个体系化的工程，需要专业人才、产品技术和制度流程全面配合运转才能达到目标效果。而其中起主导作用的必然是专业人才，而由于数据安全本身的复杂性对人才的综合能力提出了很高的要求，目前数据安全人才非常稀缺。因此，对数据安全人才的培训服务以及数据安全咨询、评估、托管等各类服务将会迎来可以预见的高速增长。这一点在信通院的数据安全推进计划调研数据中也有所体现。



来源：信通院"数据安全推进计划"

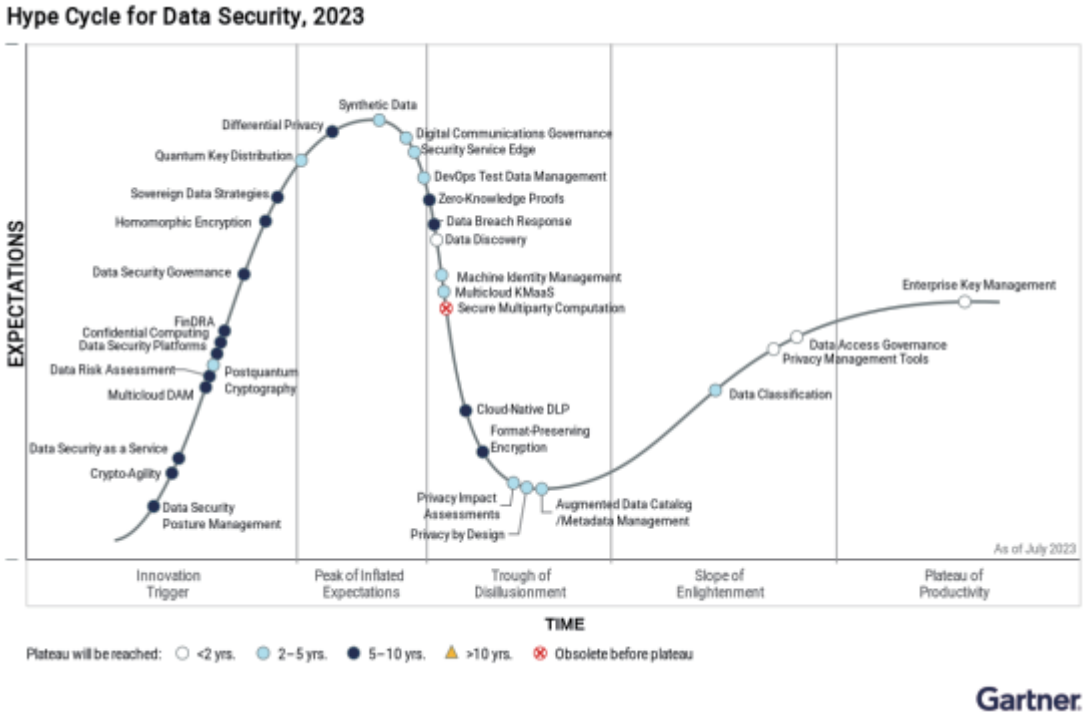
03

数据安全技术创新热点和未来趋势

3 | 数据安全技术创新热点

数据安全行业的发展趋势表明未来的增长将更多的基于对用户需求的开发和释放。众所周知，目前以及未来勒索攻击都将是数据安全最大的威胁，而对勒索攻击亡羊补牢远不如防患未然，最好的防御就是事前防御。因此事前的数据安全风险识别、风险评估、态势感知、安全服务边缘、安全治理类产品会很有市场。另一方面，打通数据壁垒，推动数据要素能够安全的共享、流通、使用是另一个重要需求。因此，隐私计算、同态加密、数据合成等技术将会有更多的应用场景和空间。最后，系统化、平台化集成各种成熟单点技术、管理流程，减少内部复杂性，提高效率的数据安全平台类产品将会逐步取代现有的分散的单点产品。

根据2023年Gartner2023年数据安全技术成熟度曲线，以上技术方向均被评为变革性或高价值的创新技术方向，是目前数据安全创新的主风向。



3.1 数据安全态势管理（DSPM）

3.1.1 定义：

数据安全态势管理(DSPM)通过对本地和云上数据资产进行全面测绘、分级分类、风险评估和漏洞修复为组织构建数据风险评估(DRA)和数据安全治理(DSG)策略实施评估的基础平台。数据安全态势管理（DSPM）

的两大特色一是发现组织本地和云上以前未知的数据，二是通过可视化技术展现数据分布和流转，帮助运营人员直观了解数据安全态势和面临风险。

3.1.2 需求痛点和解决方案：

随着数据在云中激增和流转，导致大量中间数据的位置和内容未知、未被发现或未被识别，安全风险成倍增加。因此分析这些"影子"数据的敏感性、来龙去脉、基础设施配置和访问权限成为必要。

DSPM通过创建和分析数据图和数据流来识别数据位置和用户对数据的访问，跟踪发现这些"影子"数据，并将这些"影子"数据及时纳入整体数据安全治理策略中，这使得组织能够减轻来自"影子"数据的安全风险。

DSPM的创新点主要体现在其对数据安全管理领域的全新方法和技术的应用，能够跨云服务平台和地理边界对数据进行深入的发现、分类及风险识别。这些创新点具体包括：

自动化的数据发现与分类技术：DSPM使用先进的算法自动识别和分类存储在各种环境中的数据，包括未结构化数据，大大减少了手动操作的需要。

深度的数据流分析和可视化：通过对数据流进行深入的分析和可视化，DSPM帮助企业理解数据的流动路径，识别潜在的安全风险点。

综合的风险评估框架：结合数据分类和数据流分析的结果，DSPM提供一个综合的风险评估框架，使得企业能够基于数据的实际使用情况来评估风险。

智能化的安全策略推荐与执行：基于对数据和风险的分析，DSPM能够推荐合适的安全策略，并协助企业执行这些策略，以保护敏感数据免受威胁。

跨平台的数据安全管理能力：DSPM支持跨多个云服务和本地环境的数据安全管理，为企业提供了一个统一的数据安全解决方案，简化了跨平台数据安全管理的复杂性。

通过这些创新点，DSPM在数据安全保护方面获得以下优势：

提升数据的可见性和透明度：通过自动化的数据发现和分类，企业能够获得对其数据资产的全面了解，包括数据的存储位置、类型以及相关的风险。

加强数据保护：DSPM提供的风险评估工具和安全策略帮助企业有效防范数据泄露和滥用。

支持跨平台数据安全管理：无论数据存储在哪个平台或地理位置，DSPM都能提供统一的数据安全管理，从而减少管理复杂性和成本。

促进合规性：通过自动化的监控和报告功能，DSPM帮助企业轻松应对数据保护法规的要求，减少合规风险。

强化安全态势：通过提供数据流的实时视图和安全警报，DSPM使企业能够快速响应潜在的安全威胁，增强整体安全态势。

DSPM通过其创新的技术手段和方法为数据安全和隐私保护提供了一个全面、高效和可靠的解决方案。企业通过实施DSPM，不仅能够加强对敏感和关键数据的保护，还能提高合规性，优化数据管理流程，最终建立一个更加安全和可信的数据环境。

3.1.3 技术发展的驱动因素和阻碍因素：

驱动一：不可忽视的未知风险切实存在。由于数据在本地和多云之间使用和流动，产生大量未被发现或无法识别的影子数据，这些影子数据会因其地理位置或配置错误或不适当的用户访问权限而产生风险。

驱动二：组织需要建立数据资产和数据流转的动态、全局视角。为了实现多源数据分析安全，组织需要掌握跨数据格式、跨终端的全局数据状态和流转过程。

驱动三：组织需要更高效、有效的实现全局数据安全风险评估和数据安全治理。通过建立数据资产和数据流转的动态、全局视角，组织有能力识别数据安全漏洞和不当暴露，结合其他技术事前阻断恶意攻击和风险操作，保护数据免遭泄露。

阻碍：DSPM产品与其他厂商的数据安全产品集成或协同时会遇到兼容问题。对现有数据安全产品的替换会增加成本。

3.1.4 客户建议

首先应从组织的整体DSG策略出发，选择功能对组织DSG策略支持力度最大的DSPM产品。其次要比较DSPM产品查找影子数据的能力以及创建全局、动态数据图谱的能力。最后，要考虑和其他安全产品集成的兼容性。

3.2 数据风险评估（DRA）

3.2.1 定义：

数据风险评估(DRA)是对组织内数据安全现状的全面认识，通过审查组织数据安全治理策略的实施情况，识别因不当访问、数据驻留、合规性、敏感信息泄露等造成的数据安全风险。

3.2.2 需求痛点和解决方案：

组织一直在收集、存储和使用越来越多的数据，这些数据不仅在本地存储和流通，而且扩展到许多云位

置。在当前数据的爆炸式增长和流转的情况下，组织很难保持对所有数据存储和流转的可见性，从而导致对拥有哪些数据及其存储位置、流转路径缺乏全面了解。这种可见性的缺乏给组织带来了巨大的风险，导致组织无法充分保护敏感信息、保证数据使用合规和避免数据泄露。因此，组织必须优先考虑数据资产的风险管理工作，以确保数据的可见性并保护其免受潜在威胁。

数据风险评估可识别潜在的数据敏感性、完整性和可用性风险并确定其优先级。通过将评估作为数据风险管理流程的一部分，组织可以更好地了解其面临的风险、实施适当的安全控制并遵守数据保护法规。数据风险评估对于任何数据安全策略都是至关重要的，并且应该定期执行以确保持续的风险管理。

数据风险评估可以：

• 降低具有财务影响的业务风险。基于组织的风险偏好对不同数据风险的优先级进行排序。

• 根据预算和对业务的影响，按照风险优先级排序，明确每种风险要降低到什么程度。优先级通常侧重于对业务的经济影响，以便决定安全预算应该有多大。

3.2.3 技术发展的驱动因素和阻碍因素

驱动一：数据风险评估是组织成功实施数据安全治理(DSG)基础。组织的数据安全治理要基于数据风险评估制定数据安全策略并监测实施结果。

驱动二：企业对紧密结合业务活动和需求的数据风险评估需求强烈，因为可以通过风险评估降低数据业务决策风险，并动态跟踪决策后的风险变化，最终使得整个决策流程风险可控，为业务运行安全提供保障。

驱动三：可视化的数据测绘技术的发展如数据安全态势管理(DSPM)等，为数据存储和流动提供了直观的分析结果，有力的提升了数据风险评估的全面性和准确性。

障碍：从组织管理层面数据风险评估需要调用组织所有的数据资源，包括数据集、数据流、用户账户等，如果得不到高层支持，将无法实施。从技术层面，目前组织部署的单点数据安全产品在互通和集成方面困难重重，无法整合形成整体视角。

3.2.4 客户建议

首先建议部署数据安全态势管理(DSPM)平台，使用统一的标准和工具对数据进行分级分类，为每个项目创建数据地图和风险分析，并制定数据安全策略。其次，要深入理解业务流程，分析每个业务项目如何处理数据、成果和风险，以业务的语言建立和传达数据风险，以便业务人员可以迅速理解和判断风险水平。

3.3 数据安全治理(DSG)

3.3.1 定义：

数据安全治理(DSG)是基于数据安全风险评估结果建立适合组织的数据安全策略，所建立的策略应能在保障安全的前提下最大化的支持业务运行，平衡好业务在发展与安全两方面的需求。

3.3.2 需求痛点和解决方案：

随着数据在本地和多云架构中激增，组织的数据安全问题变得复杂，过度的安全策略会阻碍数据业务的发展，而弱安全策略则会带来安全、隐私和其他合规性问题。因此，数据安全治理(DSG)的目标是通过可应用于整个IT架构的数据安全策略，在业务优先级和风险控制之间寻找和建立最优平衡。

数据安全治理(DSG)提供了一种平衡的方法来定义数据的访问和使用方式，以支持业务绩效目标和客户体验，同时实施适当的数据安全和隐私控制以降低风险。DSG要求首席信息安全官(CISO)、首席数据和分析官(CDAO)以及业务领导者通过专门的组织例如数据安全指导委员会(DSSC)进行协作。这将有助于打破沟通障碍并有助于取得业务成果。

3.3.3 技术发展的驱动因素和阻碍因素

驱动：以数据要素作为业务驱动的组织，时刻会产生新的数据流转和使用，必须使用DSG作为一个连续流程来管理、评估业务风险并确定业务风险的优先级，并创建可以减轻这些风险的有针对性的数据安全策略。例如在跨数据集场景、跨访问身份场景和跨多个安全产品场景，都需要站在全局视角组合实施一致的数据访问权限进行安全控制。

障碍：目前，大多数组织对数据的使用和管理分散，对数据安全产品、身份认证管理产品和数据分析产品的管理分散，同时数据安全产品、身份认证管理产品和数据分析产品之间也存在互不相通的问题，导致无法站在全局的角度部署统一的数据安全策略

3.3.4 客户建议

DSG属于顶层设计，应在组织架构、技术产品两方面做出能够统管全局业务数据的设计，站在组织全局的角度根据业务风险评估结果创建和管理一致的数据安全策略。具体来讲就是在组织架构层面要确保CDAO和CISO之间的合作与协作，以减少评估数据管理和安全性时的冗余和浪费。在技术产品层面确保在数据安全、IAM和应用程序管理产品中应用统一的数据安全策略来管理对每个数据集的交互访问。

3.4 安全服务边缘(SSE)

3.4.1 定义：

安全服务边缘(SSE)定位于保护对Web、云服务和内部应用程序的访问安全，功能包括自适应访问控制、数据安全、安全事件可见性和处置、高级威胁防御以及基于网络和API的集成访问控制。SSE主要作为基于云的服务提供，也支持本地部署。

3.4.2 需求痛点和解决方案

随着数字化转型的深入，组织内远程办公、混合工作模式，以及云服务等的广泛采用正在成为常态。SSE的目标是在访问网络、云服务和私有应用程序时实施安全策略，确保组织在业务上云以及多云组合的复杂网络架构下远程工作的安全性。SSE产品融合安全Web网关[SWG]、云访问安全代理[CASB]和零信任网络访问[ZTNA]）等网络安全功能，以降低复杂性并改善用户体验。

3.4.3 技术发展的驱动因素和阻碍因素

驱动：组织需要保护分布式、分散式且需要安全远程访问的用户、应用程序和企业数据。业务上云已经是多数组织的数字化现状，因此SSE主要基于业务上云的特点为组织提供可灵活设置的安全策略，包括针对SaaS类应用的数据防泄漏（DLP）、针对所有数据访问渠道的敏感数据检查和恶意软件检查等。此外，SSE允许组织精准监测每个用户的数据访问流量以及实施基于身份和上下文的态势感知。最后SSE包含的丰富功能，可以替代原有的多个单点产品，降低运营复杂性，提升效率。

障碍：首先，SSE产品融合安全Web网关[SWG]、云访问安全代理[CASB]和零信任网络访问[ZTNA]）等网络安全功能，但在各方面技术能力都突出的安全厂商比较少，导致集成后的产品某方面的功能可能存在短板。其次，由于以云为中心，SSE通常在满足内部防火墙等本地控制支持的所有需求。最后，一些供应商不太关注SaaS安全性和集成。然而，企业越来越需要这种可见性和保护。

3.4.4 客户建议

以ZTNA为SSE最重要的核心功能，再根据SSE融合的其他功能的实测表现逐步取代SWG、CASB和VPN等单点产品。

3.5 同态加密(HE)

3.5.1 定义：

同态加密(HE)是使用算法来对数据进行加密以支持隐私计算的方法。部分HE(PHE)仅支持简单数学运算，例如减法和加法，但对性能影响很小。全同态加密（FHE）支持任意数学运算从而对算力要求较高。

3.5.2 需求痛点和解决方案：

为解决数据要素可用不可见的安全需求，同态加密(HE)通过数据加密实现隐私计算，在数据库级别取得了突破性的效果。最大的优势就是数据在加密的状态下可共享、可使用，保证数据的使用效果却不会泄露敏感信息。企业可以放心的将数据发送给其他人进行处理并返回准确的结果，而不必担心数据会丢失、泄露或被盗。恶意行为者截获的任何数据都会被加密且无法读取，即使是下一代量子计算机也是如此。主要应用场景包括：

- 加密搜索
- 数据分析
- 多方计算
- 机器学习(ML)模型训练
- 安全、长期的记录存储，无需担心未经授权的解密

3.5.3 技术发展的驱动因素和阻碍因素

同态加密技术（HE）的发展受到多种因素的驱动，主要包括：

1、全球数据驻留限制的加强：随着全球范围内对数据驻留限制的加强，组织面临着必须保护正在使用中的数据的需求，而不仅仅是在数据传输或处于静态状态时的保护。这种需求促进了对同态加密等先进技术的探索和应用，以确保数据在处理过程中的安全。

2、隐私和数据保护立法的成熟：全球日益成熟的隐私和数据保护立法要求组织更精确地关注敏感数据的处理和保护。同态加密技术允许在不暴露原始数据的情况下对数据进行加工和分析，满足了法律对敏感数据保护的高标准。

3、数据池、共享和跨实体分析的需求增长：随着数据池、共享和跨实体分析用例的增多，对前瞻性和可持续技术的需求也在上升。同态加密技术在这方面提供了一种解决方案，使得在保持数据机密性的同时，可以进行有效的数据分析。

4、行业应用扩展：除了金融行业的跨实体欺诈分析等主要用例外，其他行业，如医疗保健，也开始受益于同态加密。在医疗保健行业中，对不同实体间的敏感数据进行分析时，数据通常需要在使用时得到保护，同态加密在这方面提供了解决方案。

5、安全多方计算（sMPC）的结合：结合安全多方计算解决信任与合作问题，将有助于数据的内部和外部保护。同态加密技术与安全多方计算相结合，可以在保护数据隐私的同时实现数据的协作分析。

6、应对量子计算的威胁：正如NIST和加拿大数字基础设施弹性论坛所强调的，即将到来的量子计算可能会威胁到几乎所有数据的机密性。现有的传统加密技术可能无法抵御量子计算的攻击。在这种情况下，及时采用同态加密将可持续地保护数据，即使面对量子计算的挑战。

同态加密技术的发展受到数据保护需求增加、立法要求提高、行业应用拓展、多方计算结合及量子计算挑战等多方面因素的推动。这些因素共同促进了同态加密技术的研究、开发和应用。

障碍：同态加密技术（HE）的发展面临着多个阻碍因素，包括技术复杂性、市场接受度和应用局限性。首先，将HE应用于日常用例会增加操作的复杂性，可能导致操作速度下降，同时需要高度专业化的技术人员来实施和管理，这对于许多组织来说是一个重大挑战。此外，市场对同态加密技术的不熟悉也是一个重要障碍，这阻碍了其快速采用和普及。尽管部分形式的同态加密（如部分同态加密PHE）理论上可以实现图灵完备，能够执行任意指令集，但目前缺乏供应商提供强大的实现方案，这限制了其在更广泛场景中的应用。最后，某些场景可能永远不适合使用HE，尤其是那些除了数据分析和处理之外还需要考虑组件安全的场景，如生产数据库和专有算法的保护。这些限制因素共同构成了同态加密技术发展和广泛应用的障碍。

3.5.4 客户建议

首先，要贴近业务需求，找到高价值的适用场景，开展实验试点。其次，HE不能取代原有的其他数据安全策略，但可在重要场景同时部署，进一步增强安全性。

3.6 数据合成

3.6.1定义：

数据合成是根据真实数据的特征人造数据，合成数据在各种研发场景中替代真实数据使用，包括数据匿名化、人工智能和机器学习开发、数据共享和数据货币化。

3.6.2 需求痛点和解决方案

当今人工智能开发的一个主要问题是训练数据的获取问题，真实数据获取困难并且成本高昂。针对这一痛点，合成数据被作为可选择的解决方案提出。此外，数据合成还可用于补足缺失数据，让分析数据更加完整。最后，数据合成不涉及个人身份信息，能够有效保护隐私。随着人工智能领域的高速发展，预计对合成数据的采用率将大幅增加，对于机器学习模型训练，合成数据有可能通过更低的成本，更高的效率实现更好、更安全的效果。

3.6.3 技术发展的驱动因素和阻碍因素

驱动：

- 在医疗保健和金融领域，由于合成数据能有效解决隐私保护问题，成为热点需求。
- 合成数据应用已经在汽车、计算机视觉、数据货币化、外部分析支持、平台评估和测试数据开发等场

场景广泛应用，让用户看到实效。

• 人工智能模拟技术和基础模型的进步让合成数据的效果越来越好，推动数据合成市场的发展。

障碍：

数据合成技术的发展受到多重阻碍，包括生成数据可能存在的偏差问题、无法捕捉自然异常、开发过程的复杂性以及无法为现实世界数据提供新信息。此外，数据合成的质量直接受限于使用的模型，并且该领域目前缺乏标准化方法。合成数据的完整性和真实性往往具有主观性，加上用户对于何时及如何使用该技术的困惑和缺乏必要技能，这进一步加剧了这一挑战。安全性问题也不容忽视，合成数据可能意外泄露敏感信息，尤其是在机器学习模型能够通过主动学习进行逆向工程的情况下。如果边缘情况不被包含在种子数据集中，合成数据可能无法有效处理这些情况。最后，用户对合成数据的质疑，如将其视为"劣质"或"虚假"，也阻碍了该技术的接受和应用。这些因素共同构成了数据合成技术面临的主要挑战和限制。

3.6.4 客户建议

首先，确定组织中阻碍人工智能项目的数据缺失、不完整或获取成本昂贵的区域，在医疗保健或金融等受监管行业，注意合规要求。其次，当需要个人数据但要求数据隐私时，使用原始数据的合成变体或部分数据的合成替换。第三，通过培训计划对内部利益相关者进行有关合成数据的好处和局限性的教育，并制定防护措施，以减轻用户怀疑和数据验证不足等挑战。最后，评估和总结合成数据项目的业务价值、成功和失败案例。

3.7 与大语言模型（LLM）结合是未来趋势

2022年，ChatGPT的发布引领了大模型应用突破；2023年，"百模大战"开启了AIGC元年。作为大模型落地场景之一，安全行业垂直大模型发展迅速，基于各类安全场景的大模型应用进入加速探索和落地期，安全行业即将迎来智能主义时代。

人工智能大模型（如GPT-3、BERT、360安全大模型等）在数据安全领域的应用正变得越来越普遍，这主要得益于它们在理解、生成和处理自然语言方面的高级能力。这些模型的应用趋势主要集中在以下几个方面：

1、威胁检测和响应：AI大模型可以通过分析网络流量、日志文件和其他监控数据来识别潜在的安全威胁和异常行为。这些模型通过学习正常的网络行为模式，可以高效地识别出与众不同的行为，从而实现早期威胁检测。此外，AI还可以协助自动化响应措施，例如隔离受影响的系统，减少人工干预的需要。比如360安

大模型基于自身的优势安全大数据能力在防勒索软件和捕获APT方面取得了不错的实战效果，正在得到越来越多的市场认可。

2、欺诈检测：在金融服务行业中，AI大模型被广泛用于识别和防范各种类型的欺诈行为，如信用卡欺诈、保险欺诈等。通过分析交易模式、用户行为和其他相关数据，能够快速有效的预测和识别欺诈行为，保护消费者和企业不受损失。

3、安全运营自动化：AI大模型可以自动化许多安全运营中的任务，例如事件响应、威胁狩猎和安全策略的更新。这不仅提高了安全团队的效率，还使他们能够专注于更复杂和战略性的任务，使得安全人才稀缺的问题有望得到缓解。

4、数据分级分类和安全使用：基于大模型自然语言处理能力的优势，可以更好的理解和分级分类大量的结构化和非结构化数据，对数据进行特征提取，识别敏感数据，监控其在网络上的流动，实时智能化监测和阻断数据的泄露和滥用，识别潜在安全漏洞，从而更好地保证企业安全合规的数据使用。

5、智能合约和区块链安全：随着区块链技术的发展，AI大模型在智能合约审计和区块链网络监控中的应用也在增加。它们可以帮助识别智能合约中的漏洞和潜在安全风险，保护交易和资产的安全。

6、安全智能体（AI Agent）：基于优秀的自然语言处理能力，基于安全大模型的安全智能体具有媲美人类的交互能力，可以与安全运营人员用自然语言交流，协同工作，具备记忆、分析、规划和行动能力，能够在自动化安全运营和安全人员互动培训等场景发挥核心作用。

随着技术的不断进步，人工智能大模型在数据安全领域的应用将持续扩展和深化，为防御复杂的网络威胁提供更强大、更智能的解决方案。然而，这也带来了新的挑战，如保护AI模型不被恶意利用，AI模型本身存在的数据泄露风险，以及处理由AI决策带来的道德和法律问题等。因此，继续研究和发展这些技术的同时，对相关的伦理和监管问题进行深入讨论也十分重要。但可以肯定的是，与大语言模型（LLM）的结合是数据安全技术创新的必然趋势。

04

数据安全技术的最佳实践

360数字安全：XX头部国有股份制银行数据安全平台建设项目

案例提供方： 360数字安全 数字安全的领导者

案例背景：

随着国家监管力度不断增强，法律法规顶层设计已经完成，行业要求不断落地，安全建设要求越来越高，安全不合规将会给企业带来巨额罚单、影响企业社会声誉等风险。与此同时，数字化面临的外部威胁不断升级，对手变了、目标变了、手法变了、危害变了，最终让风险研判过程更加错综复杂，安全运营中单纯依靠规则进行网络威胁研判将不再能满足分析的精度要求。

对于银行行业客户来讲，有效、高效的安全运营对于保护金融数据、满足法律法规合规要求、促进网络金融发展、防止勒索攻击、金融欺诈等威胁以及支撑新型业务技术的引入等方面至关重要，一方面能够提高客户信任度，另一方面可以确保业务的可持续发展，防止损失。

某银行客户作为头部国有股份制银行，在合规要求和安全运营的双重背景下，启动建设一套数据安全一体化平台以更好地支撑客户安全业务。一体化背后的本质特征是将多种安全能力进行联动、联通与协同，是对数据安全多元化需求的行之有效的解决手段。平台一体化把多种安全能力联动，多方安全协同，将平台化和智能化作为两翼，增强数据要素全生命周期的生态融合。

关键挑战：

1、内部威胁：

- 员工可能会滥用他们对敏感数据的访问权限，例如未经授权地查看客户信息。
- 或者将数据用于未经授权的目的，例如个人谋利或者窃取客户资料。

2、外部威胁：

- 黑客可能会试图通过网络攻击或社会工程手段来获取公司数据。
- 公司网站或数据库可能受到恶意软件或网络钓鱼攻击。

3、合规性要求：

- 公司可能需要满足特定的法规和标准，如 GDPR、HIPAA 等，来保护客户数据。
- 违反这些法规可能导致巨额罚款和声誉损失。

4、API安全风险：

API的数量急剧增长，与之相关的安全风险也在同步增长，尤其是数据安全风险。企业使用API来连接服务、传输数据，许多重大数据泄漏问题，其幕后原因都在于API 遭到破坏、泄露或攻击。API一旦被攻陷，会让敏感的医疗、金融和个人数据公之于众，被不法分子利用。近年来，国内外大规模数据泄露事件频出，企业级API安全面临巨大的挑战。

解决方案：

为满足上述需求并应对当前的关键挑战，交付团队在深入调研业务实际运行场景后有针对性的设计构建出一套一体化数据安全平台。此平台由几大主要部分构成：

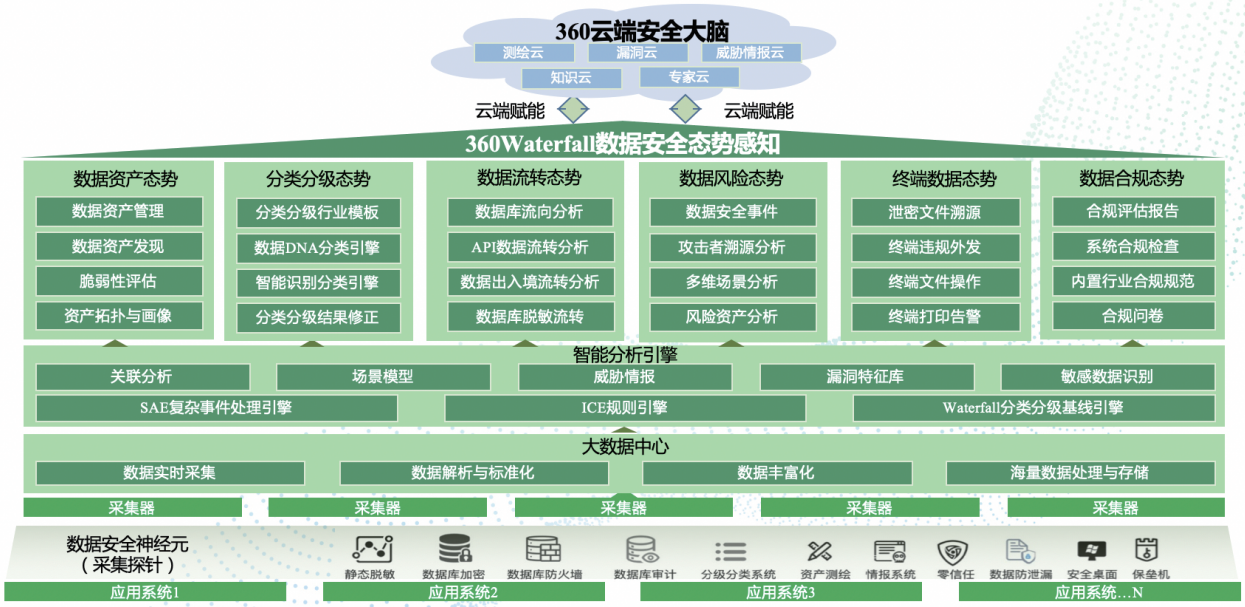
数据安全态势感知平台

360Waterfall数据安全管理平台是基于云计算、大数据、人工智能等新一代信息技术，整合了360云端安全服务能力，具备数据安全分析与态势全可视等的数据安全体系管控类产品，产品集成了全流量数据资产聚合存储、海量数据安全信息处理和查询、资产全量识别盘点、客户行为深度分析、大数据实时智能响应等能力，重点解决客户以下数据安全风险问题，包括：

- 数据资产盘点不清
- 无法呈现客户数据资产态势
- 无法全局掌握数据资产的使用情况和流转情况
- 无法掌握客户数据安全合规态势
- 数据安全运营管理方面缺少安全专家服务
- 无法打通数据孤岛
- 避免数据孤岛
- 避免单点安全风险
- 数据与告警去重编排等

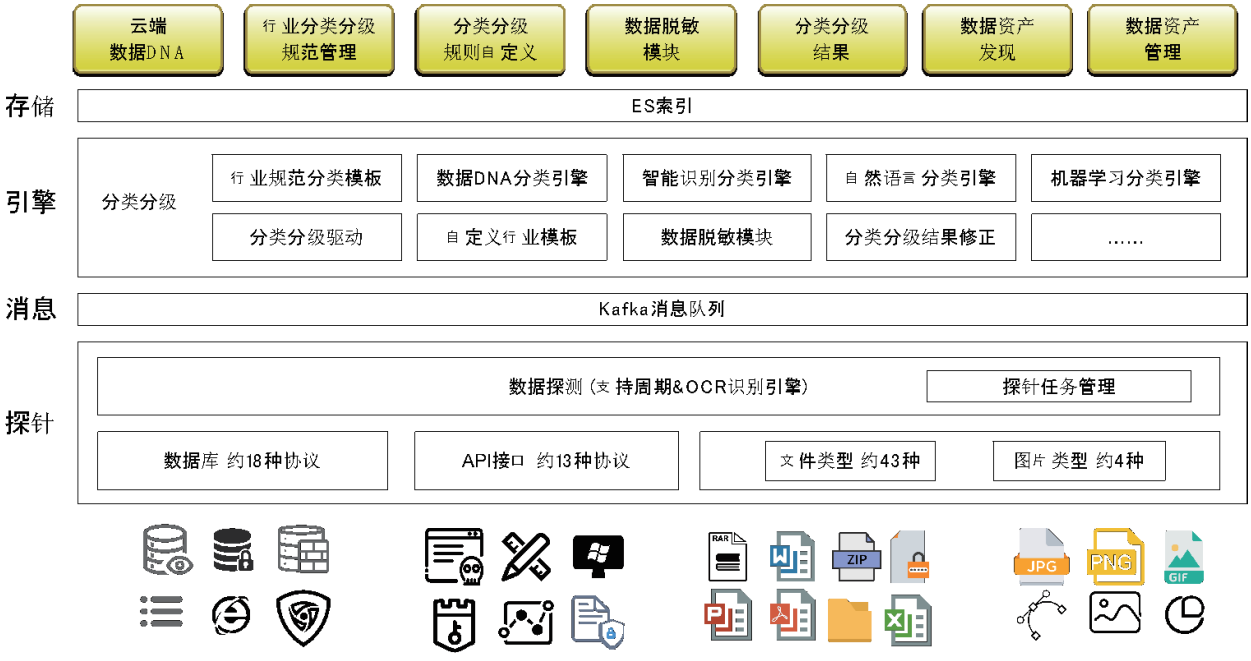
帮助客户实现全面掌握全局数据资产态势、数据资产漏洞和风险态势、数据资产的使用情况和流转情况、数据安全合规态势，全面提供安全风险管控能力、提升多源异构数据统一分析能力及全面提升数据分析研判能力，充分盘活客户数据安全防护场景。

360Waterfall数据安全管理平台接受云端赋能、连接安全设备、汇聚安全数据、积累安全知识，帮助客户实现数据资产态势、数据流转态势、数据使用态势、数据风险态势、数据合规态势等功能，全面提升客户的全景安全知识融合，全栈核心技术融合、全视安全大数据融合，全方位提升安全体系能力。



分类分级态势:

数据安全分类分级首先会引入企业所在行业标准分类分级规范，根据规范中的分类分级要求对数据库资产、API接口资产、文件存储服务器三大类内容进行敏感扫描并做分类分级工作。在数据扫描的过程中，通过关键字、正则表达式、自然语言识别、机器学习等匹配技术，结合上下文信息对结构化数据进行识别;针对数据库分类分级支持分类分级历史快照比对。



通过与内置的行业分类分级规则进行匹配，从而针对数据按行业进行定级。数据安全专家、企业安全部门与业务部门相互配合，根据分类分级流程，对最终结果进行确认与修正，针对确认的结果还可以生成数据DNA信息库以供下次分类分级直接引用分类分级结果。

• 支持数据库 18 种：MongoDB、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase、Redis、ElasticSearch、DB2、Clickhouse、Hive、GreenPlum、MariaDB、Informix、Oracle、SQL-Server、Opengauss、Kafka 等进行分类分级；

• 支持API接口，主要针对HTTP协议调用接口进行分类分级；

• 包括常见文件28种：txt, html , doc, docx, docm, dotx, dotm, xls, xlsx, xlsm, xlt, xltx, xltm, ppt, pptx, ppsx, ppam, potm, ppsm, pptm, pdf, csv, wps, wpt, et, ett, dps, dpt；

• 支持源文件类型7种：java, cpp, c, sh, sql, xml, py；

• 支持压缩文件6种：7z, zip, tar, gz, bz2, xz；

• 支持图片类型4种：jpg, png, bmp, tif；

• 支持音视频文件3种：Mp3, flac, wma等进行分类分级。

数据流转态势：

针对数据库流转、API流转、文件流转过程进行动态测绘，展示敏感数据的流向和终端用户的访问情况，包括：

• 在数据库间的流转　• 在部门间的流转　• 在区域间的流转　• 数据的跨境流转

数据库流转主要针对企业访问数据的应用、客户端进行检测，特别是针对发现新用户访问、用户访问过程中自动进行分类分级检测、访问历史与内容审计等。

API数据流转主要针对企业数据流量监测，包括：

• 对外开放数据接口调用　• 系统间接口调用关系发现　• 调用内容抽样分类分级检测

针对API流转过程中新API资产、服务、接口发现、数据出入境进行动态监测；　展示敏感数据的流向、首次访问时间、最近访问时间、新发现资产数、新发现服务数、客户端数、未确权数、访问次数、请求与应答流量大小、访问关系黑白名单，最24小时访问量分布情况等等。

数据流转态势：

随着网络安全法、数据安全法、个人信息保护法等法律法规的出台，各级单位必然会越来越重视数据安全的合规建设。出于对自身数据保护的需求，企业必须要开展的数据安全活动是定期开展数据安全评估。

通过合规态势和合规管理功能, 将数据安全合规的管理工作标准化、流程化、规范化,以法律法规和行业监管部门的考核要求为基础, 结合企业自身的业务场景, 定制化输出安全评估模板, 以半自动化的方式开展数据安全风险评估工作, 形成电子化的风险评估报告, 帮助企业从宏观角度发现数据安全薄弱环节, 提出整改建议, 从而有的放矢地进行数据安全能力建设; 支持法规有:

- 等保一二三四级: 144条
- 数据安全法: 74条
- 个人信息保护法: 176条
- 网络安全保护法: 44条
- 电信互联网数据安全: 72条等相关法规

通过合规问卷功能, 可以根据问卷模板在企业内部创建调研问卷, 针对企业内部工作任务、节点、内容进行自检反馈提供便捷调研管理工具。

数据风险态势:

全面收集和审计各类数据安全设备采集的安全日志, 通过智能分析引擎的关联分析和场景建模, 识别其中潜在的安全风险并及时告警。包括:

- 数据安全事件
- 弱口令
- 攻击热力图
- 合并告警
- 邮件威胁
- 攻击者分析
- 账号爆破
- IP威胁情报
- 风险资产分析等

企业管理员可以通过及时的风险处置, 遏制数据泄漏事件的发生, 防范于未然。

支持本地文件、目录、Syslog、SNMP-TRAP、Netflow、数据库、Kafka、HDFS、ElasticSearch、SFTP、WMI、SNMP协议格式;

支持search、where、eval、bucket、stats、sort、join、fields、head、top、format、append等搜索命令进行各种统计操作;

支持数值计算, 包括: 平均值、计数、去重计数、最大值、最小值、差值、求和等统计聚合函数;

支持1000个以上函数调用, 包括对字符串、数字、时间等类型的参数进行常见函数调用;

支持对满足检索条件的所有合并告警进行实时统计, 包括不限于, 合并告警级别、数据、趋势、受害主机top、 攻击源top、攻击类型top等, 并可下载符合条件的告警;

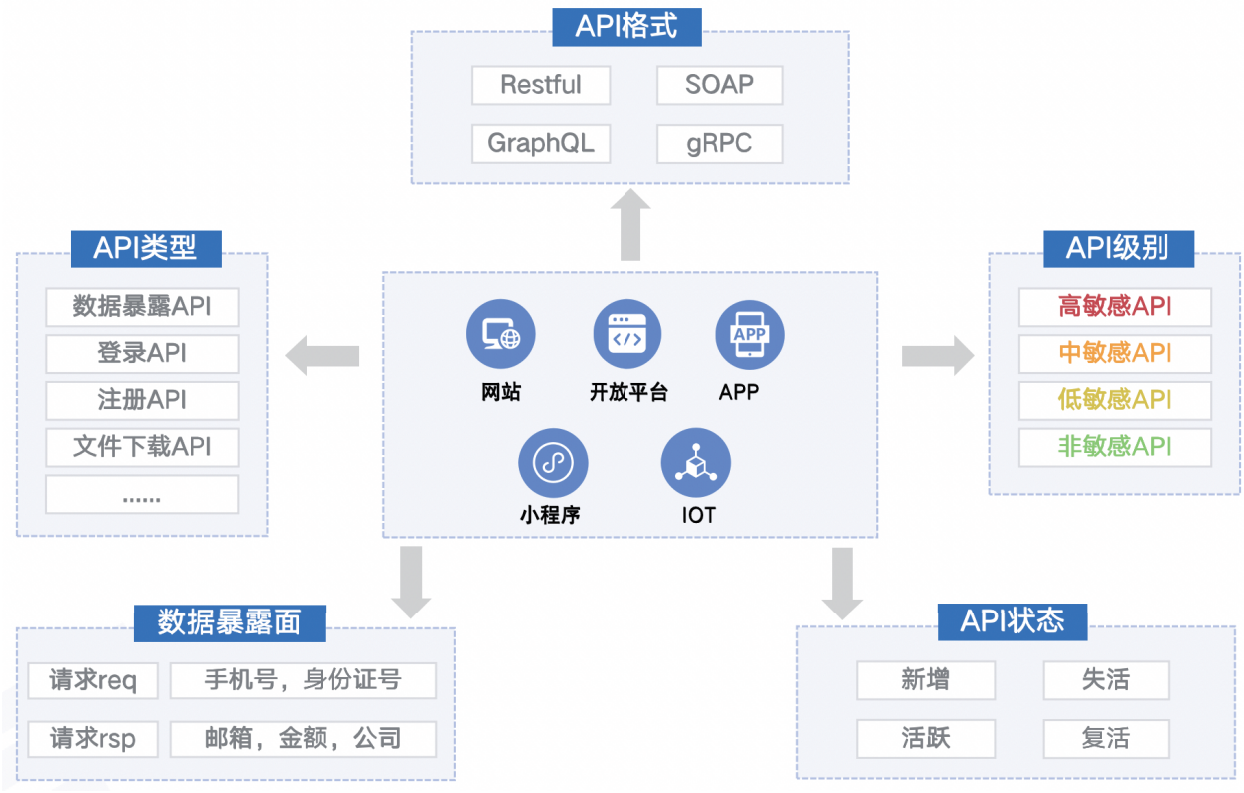
支持安全事件, 并对安全事件的分析、处置状况进行管理。对每个安全事件进行跟踪分析, 查看原始日志、相关资产的画像、攻击链路的分析, 根据研判结果进行及时处置, 填报处置措施和结果。

API风险监测系统:

API风险监测系统采用自动化API识别技术，结构化还原网络流量中的API的请求和响应，提取参数配置，识别API的技术设计格式，包括RESTful、SOAP、gRPC、GraphQL。

通过持续的监测和分析API交互，识别API请求和返回内容中包含的敏感数据，并及时更新敏感数据暴露的细节，以便更好地了解API的功能、使用情况、数据暴露面情况和潜在的安全风险。

结合API携带的数据和作用独创API分类分级算法，对API进行分类定级，从功能层面，类型包括登录API、注册API、短信验证码发送API、导出API、文件上传API、文件下载API等，从API数据暴露面层面，类型包括数据暴露API、数据采集API等，其它层面，包括服务调用API、人机访问API等。级别包括高敏感、中敏感、低敏感、非敏感。



通过持续发现能力能够自动监测和跟踪API的变化，API状态包括新增API、活跃API、失活API和复活API。及时了解和管理API的变化，进行相应的验证和评估。确保API清单与实际情况保持同步，并能够在开发/测试阶段到生产环境的全过程中保持API清单的最新和准确。

UEBA用户实体分析系统：

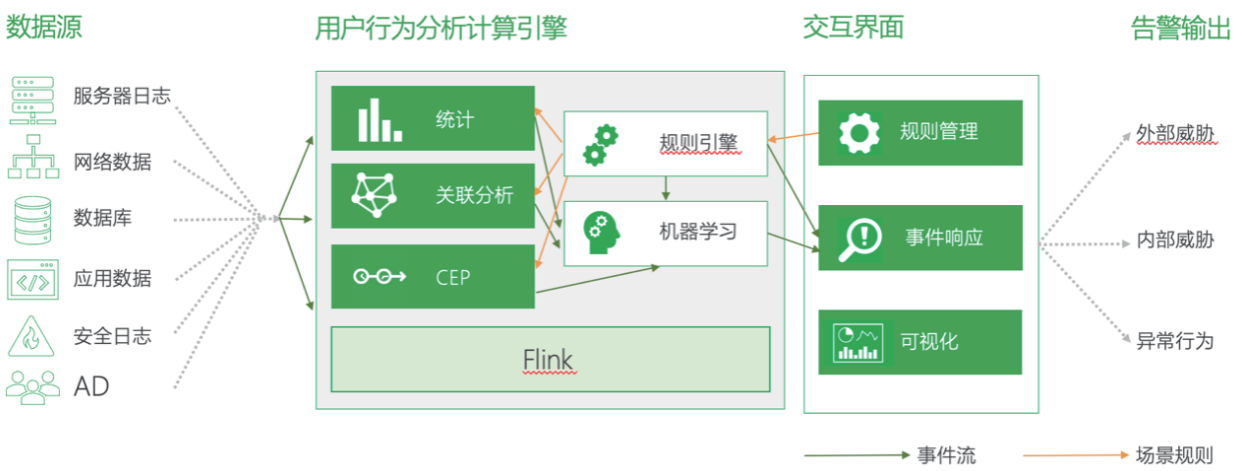
UEBA设计的核心是“用户”（User）和“实体”（Entity），UEBA的项目首先明确的就是分析的对象或主体，以及分析对象或主体在网络中的唯一标识。

UEBA围绕用户唯一标识展开数据的收集和处理，通过建立安全数据中心，实现对围绕用户唯一标识的各类网络行为数据、终端数据、网络流量、应用系统数据、基线、社交数据、访问行为数据等的集中化采集和标准化工作。并利用大数据分布式架构实现对全量原始数据的集中存储，实现数据的采集存储查询并为UEBA分析提供数据依据，同时满足网络安全法等相关法律法规中对全量日志集中存放六个月的要求。

通过安全数据中心将各类安全数据集中处理后，将标准化的字段输入给用户异常分析中心，异常分析中心利用规则引擎、算法引擎、基线引擎按照不同应用场景对海量数据进行分析，输出以用户为维度的正常或异常的网络行为，形成综合用户威胁雷达图和场景分析结果。

同时利用平台自身的威胁事件溯源、安全事件可视化等能力实现对异常事件的调查、管理、溯源、监控、分析等目的。

最终利用可视化手段实现对全量安全事件的管理、分析、监控、预测。构建用户异常行为分析平台。并对分析结果进行整体展示，发生安全事件后，能通过业务流程、邮件短信的方式进行通报、确认。



创新性与优势：

1、数据流转，敏感访问。考虑到现有API的数量急剧增长，与之相关的安全风险也在同步增长，尤其是数据安全风险。在API安全、数据库安全问题日益突出的当下，针对API数据流转、数据库数据流转以及针对它们进行分类分级后的敏感信息访问与使用进行确权与监控，针对非确权访问进行安全处置。

2、基线拟合。通过提取行为数据中的特征字段（时间、频次、登录结果等），进行用户行为基线的拟合，通过对比个人基线和部门基线，检测判定用户行为是否异常。

3、API高级风险检测。伴随着Owasp API security Top10的发布，企业面对的更多是API业务逻辑攻击

手法，防不胜防的组合攻击链。API监测产品通过分析API接口的输入输出、数据流动路径和业务逻辑的规则和约束，识别出可能导致业务逻辑漏洞的输入和操作，评估API系统中的业务逻辑风险，发现并识别潜在的攻击威胁和安全漏洞，发现不符合预期逻辑、可能导致数据篡改、越权访问或非法操作的情况。而传统的API安全控制方法主要关注基本的认证、授权和传输层加密，而忽略了业务逻辑上的风险。

4、分类分级。支持三大类分类分级：18种数据库分类分级、API接口分类分级、40多种文件分类分级。通过关键字、正则表达式、自然语言识别、机器学习等匹配技术，结合上下文信息对结构化数据进行识别，并支持数据安全专家、安全部门与业务部门，根据分类分级流程，对最终结果进行确认与修正。

应用效果：

1、API数据流转可以帮助客户实现不同系统之间的数据集成和共享，使得数据能够在不同平台和应用程序之间自由流动，提高数据的可访问性和可用性。通过API数据流转，客户可以实现自动化业务流程，减少手动数据输入和处理，提高工作效率和生产力。例如，不同系统之间的数据同步和交互可以通过API实现自动化，避免了手动操作的繁琐和错误。

2、UEBA用户实体分析系统，帮助客户在内部威胁上以更快的速度分析做出决策，在复杂的情况和大量的日志下能够更迅速地抓出内鬼，找到外部攻击者。

API风险监测系统能够为客户提供API资产发现、API接口分类分级、API弱点评估、风险监测、威胁拦截、异常行为审计、集中管理等API安全闭环能力，提高企业对API风险管控机制的建设与运营实践。

经验总结：

通过此案例，总结获得了以下几方面经验：

1、数据安全一体化设计及落地过程中，花大力气去充分理解该客户的真实安全运营体系，积累了丰富落地经验，为后续在其他金融行业客户推广、落地更多的数据安全项目树立了标杆。

2、当前数据安全一体化设计通过在此项目的实践应用中，平台功能在复杂性、准确性、全面性等方面的应对能力获得了补足和完善，并且经过本项目案例的检验，当前的数据安全一体化能力能够达到实战攻防应用的标准，后续有信心作为最佳实践进行广泛推广。

客户环境是不断变化的，对于数据安全来讲，底层探针更新、自身体系完善都会造成数据安全安全运营体系的不断迭代变化，而一体化中探针检测作为数据安全运过程中的关键环节，也需要保证自身具备灵活的迭代能力和可扩展性。本项目中落地的探针检测能力充分重视后手，并将扩展和迭代计划与客户未来安全运营流程体系规划对齐，确保能够持续有效支撑客户未来的安全运营领域的技术升级和模块扩展。

炼石：基于免改造数据安全技术的工业领域数据安全保护方案

案例提供方： 炼石 CipherGateway

案例背景：

工业系国家经济命脉，数字化发展强劲。数字时代下，加快数字化、网络化、智能化技术在各领域的应用，推动工业发展质量变革、效率变革、动力变革，为我国制造业重构竞争优势提供了难得机遇。《"十四五"信息化和工业化深度融合发展规划》提出"到2025年，信息化与工业化在更广范围、更深程度、更高水平上实现融合发展，新一代信息技术向制造业各领域加速渗透，范围显著扩展、程度持续深化、质量大幅提升，制造业数字化转型步伐明显加快，全国两化融合发展指数达到105"的目标。《"十四五"智能制造发展规划》提出，2035年规模以上制造业企业全面普及数字化网络化，重点行业骨干企业基本实现智能化。

保障制造业高质量发展，数据安全是关键。随着数字化的持续推进，网络与外部的界限逐渐模糊，传统的数据安全保障手段变得失效，制造业企业正在面临更多的攻击和风险，尤其商业秘密和技术专利等与企业生死存亡密切相关的重要数据保护，正变得日益迫切。数据是制造企业的重要战略资源，防范数据安全风险、构建数据安全保护体系、完善数据安全治理机制对提振制造企业数字化转型信心至关重要。2024年2月26日，工信部印发《工业领域数据安全能力提升实施方案（2024—2026年）》，围绕工业企业数据保护、数据安全监管、数据安全产业支撑三类能力展开部署，并提出"到2026年底，工业领域数据安全保障体系基本建立"。

创新免改造数据安全技术，以新质生产力为高质量发展注入强大动力。新质生产力作为同"新兴产业"、"未来产业"关联紧密的代表生产力演化中的一种能级跃迁，技术含量高、发展前景广阔、富含创新驱动，是科技创新在物质生产中发挥主导作用的生产力。数据安全与新一代信息技术扭结缠绕的特点决定了其技术含量，无处不在的数据要素决定了数据安全发展前景广阔，"与人斗"的攻防对抗内在禀赋决定了数据安全富含创新驱动，因此数据安全有望成为新质生产力的典型领域，反过来数据安全也为新质生产力提供关键安全保障。数据安全本质在于攻防两端基于成本消耗的效率对抗，有效提高了防守效率的免改造数据安全技术，在经历技术创新、实战检验、产业推广等阶段后，有望成为数据安全领域新质生产力的关键驱动，实现数据安全产业高质量发展。

针对基于免改造数据安全技术的工业领域数据安全保护方案，制造业用户单位提出的"云上/当地数据库敏感数据加密及脱敏"技术需求，炼石面向含有个人隐私信息和重要商业数据的应用场景，对数据进行全面识别和

打标，对其中敏感数据进行加密或脱敏保护，有效避免敏感数据泄露或被不当利用的风险。通过此项目，制造业用户单位将进一步加强数据安全防护能力，实现一次建设、多重合规、有效防护，为未来产业研发生产数据安全保驾护航。

关键挑战：

1、制造业应用系统通过大规模开发改造方式补充和增强安全能力不可行；

2、企业积累数据量巨大，在应用密码技术进行安全防护的同时要保障效率问题；

3、众多应用系统所采用的数据库品牌不统一，增加了保护数据的难度；

4、制造业各应用系统供应商所采用的应用开发技术不统一，给数据安全防护增加了复杂度；

5、建设一个统一的管理平台能够管控企业内的所有需要数据安全保护的应用系统。

解决方案：

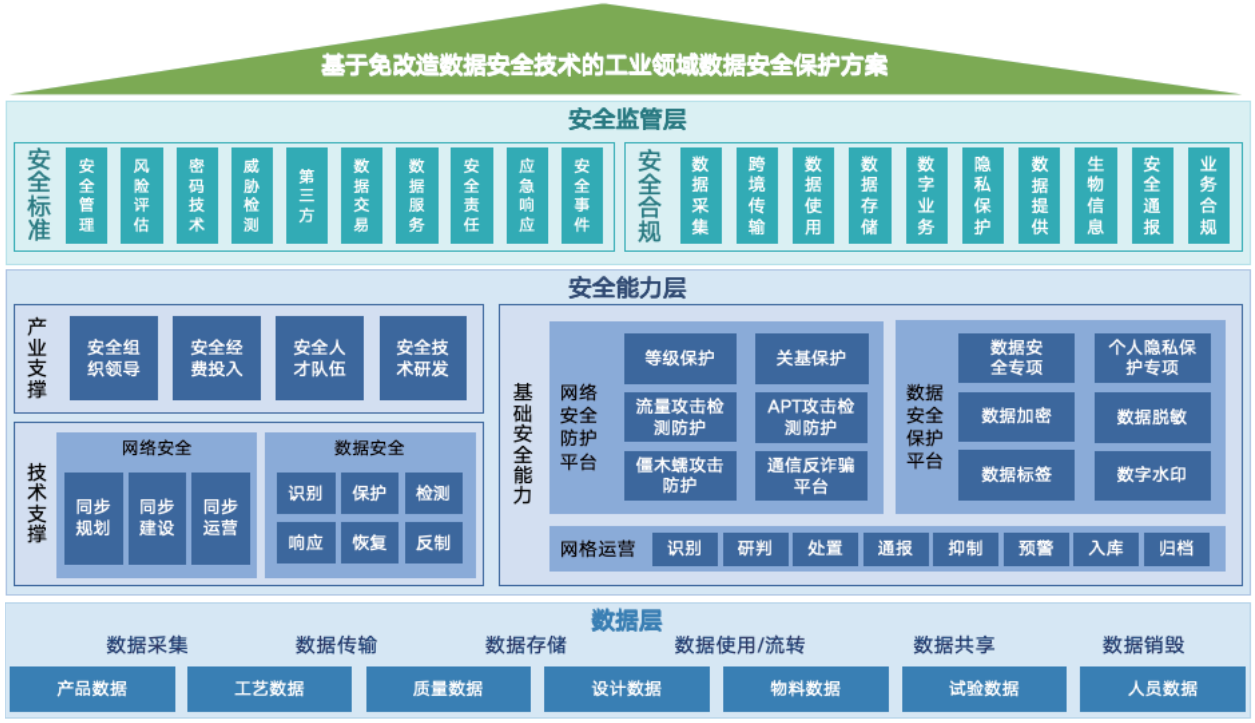


图 1 基于免改造数据安全技术的工业领域数据安全保护方案架构

基于免改造数据安全技术的工业领域数据安全保护方案，结合工业制造业的实际需求和现实生产环境的风险分析，开创性将CASB技术改进并实现应用免改造的细粒度数据防护。基于面向切面安全技术，将安全与业务在技术上解耦、但又在能力上融合交织 ，实现主体到应用内用户、客体到字段级的防护，“以加密和去标识化技术为核心，融合数据识别、防护、检测/响应、追溯等多种安全技术”，为工业用户单位提供数据使用流程中的安全保

护，构建高性能、安全、易用、场景覆盖完整的卓越密码能力，满足合规和实战防护两大需求，有效保护工业数据安全。

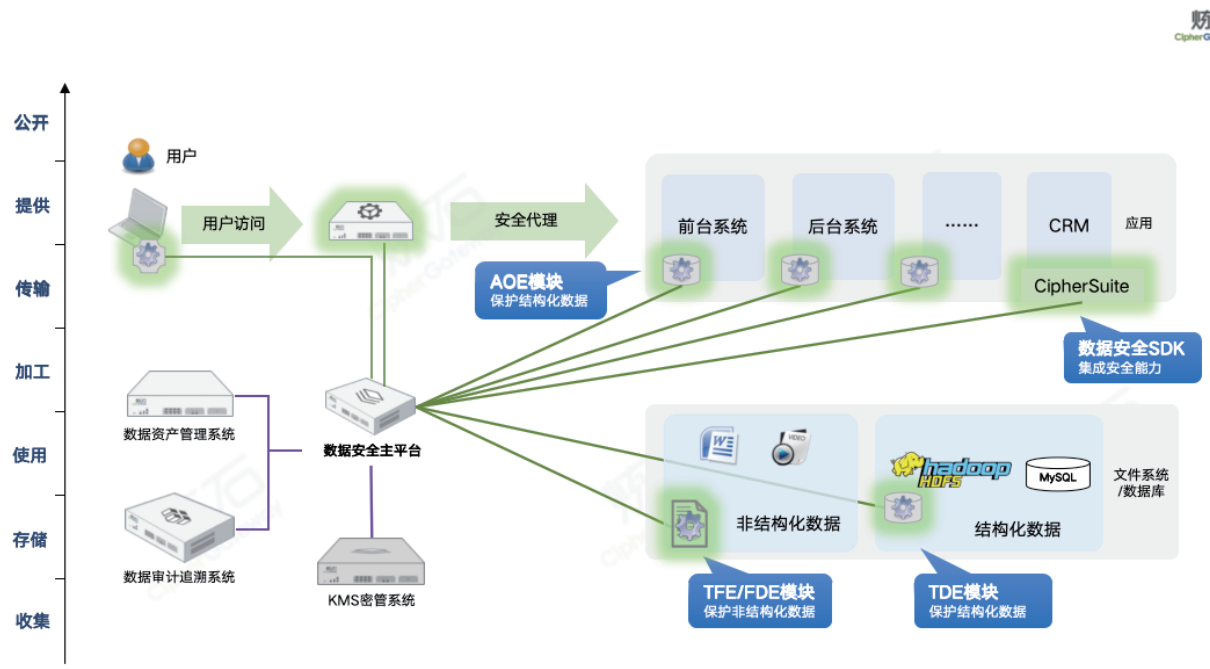


图 2 基于免改造数据安全技术的工业领域数据安全保护方案产品组成

方案主要包含**数据安全主平台、密钥管理平台以及数据安全模块**三部分，通过数据资产管理系统对数据进行发现、分类分级等，再结合部署在应用系统主路的加密模块形成高覆盖的数据控制点，并在这些控制点上对流转数据实现加密、访问控制、风险监测、审计追溯等保护能力，构建适用于工业领域的防绕过保护机制。

数据安全主平台：

数据安全主平台可统一数据资产管理、集中安全策略管控。数据安全主平台针对工业业务应用提供多种安全能力供给，通过多安全模块组件下发、策略管理、功能监测，全面覆盖应用系统、数据库、文件系统、磁盘、终端等数据流转多层级，以及数据全生命周期各环节，并支持在高覆盖率的免改造控制点灵活施加数据识别、防护、检测、响应、恢复、反制等保护能力，实现横向覆盖广泛应用、纵向叠加多阶安全能力，保障工业数据全生命周期安全。此外，主平台可有效保障结构化和非结构化数据安全，面向SQL语句的结构化数据识别和保护，支持按列保护、按规则匹配的行保护等字段级安全；面向OS文件驱动层的非结构化数据识别和保护，支持文档级防护。

数据安全旁路部署数据资产管理系统、数据审计追溯系统。其中，数据访问审计系统主要是针对主体访问数据的操作进行安全审计，由数据安全插件进行反馈数据库操作数据，通过接收数据库操作数据实现对数据库操作的安全审计。此系统在部署时可选，可以由管理平台将审计数据直接传递给第三方的审计平台。

密钥管理平台:

密钥管理平台统一进行加解密所使用的密钥的管理工作。密钥管理实现标准的密钥多级派生机制, 在数据安全管理平台中根据加密策略具体生成工作密钥, 最终下发给数据安全插件以执行加解密。

数据安全模块:

数据安全模块部署在应用服务端, 只需进行简单配置, 应用无需再进行任何额外修改, 即可向数据库存储密文。数据库加密模块包含高性能国密软件（国密SDK）, 在对数据进行加解密时, 插件调用国密SDK在本地执行加解密工作, 适用于业务高速运转, 数据大量交互的场景。模块与数据安全主平台进行交互, 获取安全策略以及密钥。

创新性与优势:

技术创新方面:

1、面向切面的安全技术

方案实现面向切面的数据安全技术, 将工业应用服务中的数据库访问层进行包装, 使得经过此"切面"的所有数据库操作命令都可以被进行过滤和加工, 实现入库的数据的加密, 读取库中的数据进行解密, 与后端的数据库品牌或版本无关, 可以完全解耦数据库。同时对于经过此切面的数据, 可以进行"加工", 实现动态脱敏的效果。

2、高性能加密技术

方案支持工业数据高性能加密技术, 基于中国、美国、日本的三国PCT专利, 利用Intel芯片上的AES-NI实现SM4的性能优化, 单颗Intel/i9/18核CPU上SM4加解密速度突破140Gbps, SM2签名达到90000次/秒, 验签15000次/秒, 实现对国外算法的等效替换; 在安全性上获得显著提升, 可抵御TLS协议中算法套件攻击, 有效抵抗各类侧信道攻击; 同时全面覆盖工业多种应用场景, 可满足工业现场设备、工业控制系统、网络基础设施、工业应用程序等多种应用场景需求。

3、主体到应用内用户, 客体到字段级"的细粒度防护

方案能够提供"主体到应用内用户, 客体到字段级"的细粒度身份访问控制, 可通过数据安全管理平台对工业企业员工进行权限管理。其中, 访问主体的用户信息可以与企业的统一用户身份管理进行集成, 也可以与应用的用户管理进行同步。在密文数据被访问时, 则根据用户身份, 向授权的用户展示明文数据或部分遮掩数据, 而向未授权用户展示密文或脱敏数据。工业系统安全管理员可通过设置加解密和脱敏策略, 对不同的数据库字段采用不同加密算法和密钥, 实现敏感数据访问授权最小化。

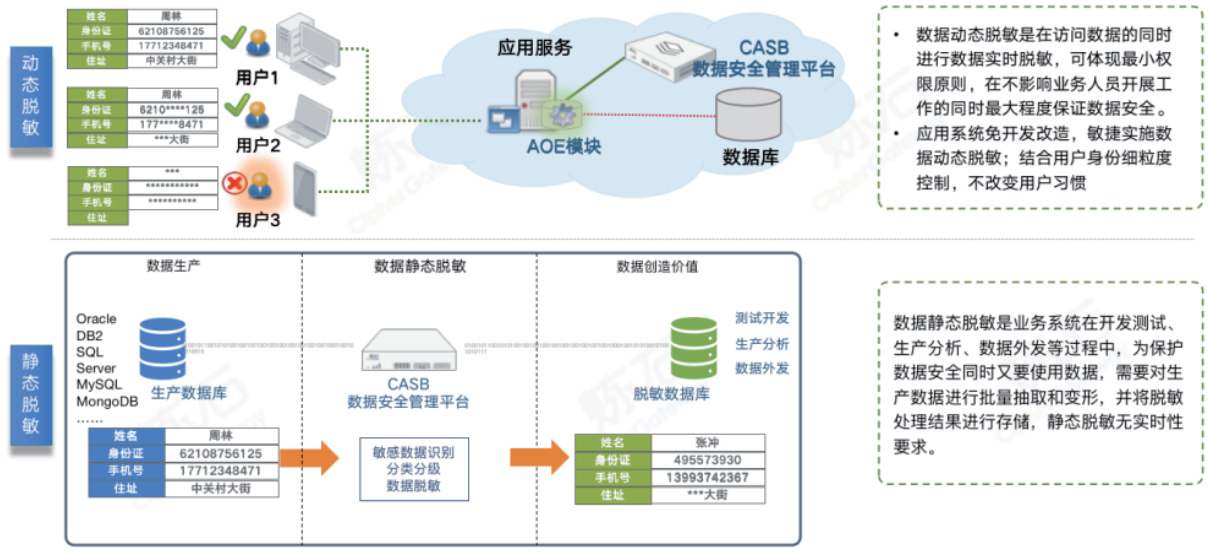


图 3 细粒度访问控制示意图

4、密码安全一体化

方案采用的数据安全主平台在数据解密的锚点，结合身份访问控制、审计等技术，构建"防绕过"的工业数据安全防护体系。当数据被访问需解密时，在解密的锚点上施加访问控制策略，只向有访问权限的用户展示明文数据，而向非授权用户展示脱敏数据，实现结合用户身份的动态脱敏，保证对于敏感数据的严格管控，并支持可追溯、防篡改的第三方数据操作审计，每条日志支持主体追溯到人，保证可事后追责。

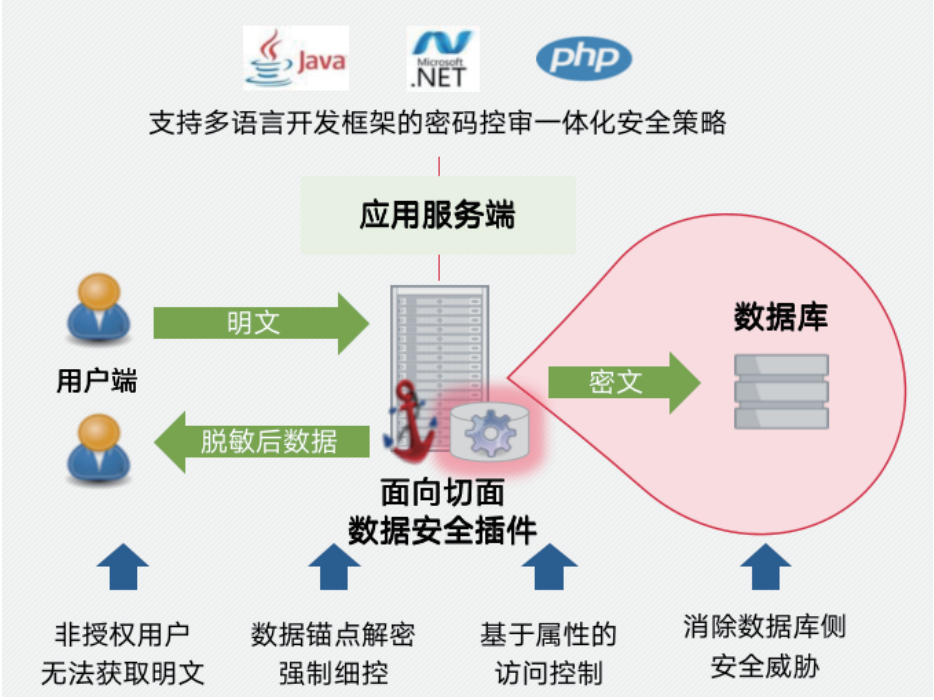


图 4 支持多语言开发框架的密码安全一体化安全策略

5、支持多种数据库类型

方案的数据安全主平台采用在应用侧加密的方式，能完全解耦数据库品牌及版本，支持包括但不限于Oracle、MySQL、DB2、SQL Server、PostgreSQL、MongoDB、MariaDB、Vertica、teradata及国产达梦、南大通用、人大金仓等数据库，工业用户只需在应用中进行插件配置，重启服务即可完成安装。

6、安全与合规性增强

方案采用的高性能国密SDK在保证了国密算法性能满足应用的同时，也实现了自主可控。遵循《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》的规定，方案中采用的密码模块（包括硬件与软件），均具备国家密码管理局颁发的商用密码产品型号证书，需要采用国密算法保护重要数据的机密性、完整性等。该标准中对于重要信息系统的密码应用做了明确规定，包括但不限于应用和数据安全以及密钥管理等方面。

方案基于数据安全主平台将敏感数据在应用服务内加密，除实现将数据加密后存入数据库，还能实现数据从应用服务到数据库之间以密文形式传输，因此，安全性更高，合规性更好。同时，在数据库的控制范畴内，不论是存储磁盘还是数据库范围内的内存、缓存，关键敏感信息是密文状态，可解除DBA风险。

应用创新方面：

1、免改造应用增强安全能力

通过应用开发改造的方式来实现工业数据安全防护，需要投入大量的工作，而且已经上线运行的系统经过安全底层的改造，势必带来较大的风险，会影响到正常业务的开展。因此，需要一种应用系统免改造的方案，较短周期、较低风险的实现数据安全防护效果。

方案采用数据安全主平台可在应用层以不改造应用的方式，对数据进行字段级加解密和遮掩，为原有应用系统增强数据安全能力。敏捷实施数据加密，能在较短时间以低风险实现数据安全防护效果。核心加解密能力以插件的形态部署到原有的应用系统中，其他的子系统、模块则以旁路模式进行工作，不会影响到原有系统的运行。数据安全主平台对于原有系统是透明的，不需要原有系统进行任何架构上的、程序上的调整，不需要原有系统进行改造和重新开发。

2、支持"分布式部署、集中式管控"应用部署模式

方案支持"分布式部署、统一集中管理"的模式，即支持目标应用的分布式或微服务部署模式，可以在工业多个应用节点或服务实例上安装插件，实现敏感数据的分布式加解密和脱敏，同时可以通过数据安全管理平台统一进行策略配置。这样加解密以及访问控制等的执行在部署的插件中进行，避免了所有的执行在单个点执行所引

起的性能和稳定性的问题; 而统一的数据安全管理平台可以管控所有部署的加密插件, 工业管理员可在此平台上进行安全策略的设置, 包括加解密策略、数据脱敏的规则、访问控制规则等, 无需在各个加密套件上分别进行维护管理, 使本产品的运行维护便捷易用。

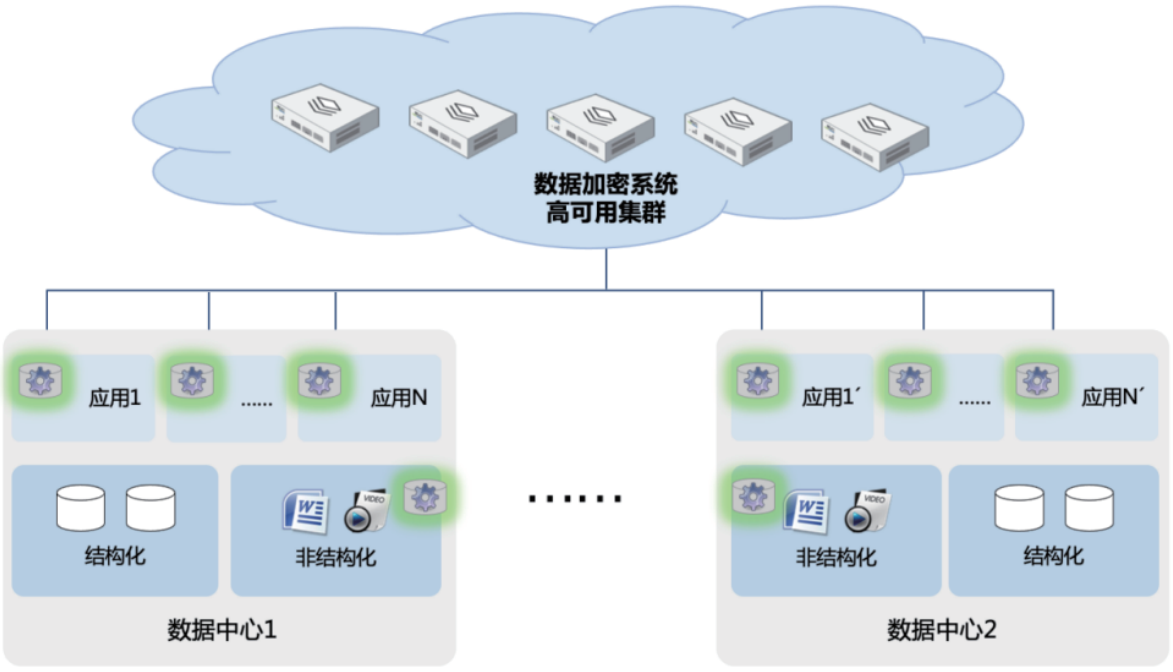


图 5 分布式加密部署图

对于建设方案中应用系统众多的情况, 数据安全主平台支持"分布式部署、集中式管控"的部署方式便于集中数据安全管控等, 即: 部署一套统一的密码管理平台, 负责整体的策略管理和密钥管理, 在应用系统中部署插件的方式, 实现每个应用系统独立执行加解密, 避免了集中在单点资源池集中执行加解密的"高可用和性能"的风险, 同时, 可实现"A处加密、B处解密"的模式, 降低维护和管理成本, 确保数据能安全流动的目标。

3、满足总部及分支机构系统不断增加的扩容需求

考虑到随着业务的发展, 工业企业的应用系统和数据库实例都在不断的增加, 数据安全主平台具备较好的系统承载能力和良好的可扩展性, 能够应对不断增长业务量的挑战。

本方案提供的产品在架构设计上具备良好的可扩展性, 支持以横向扩展的方式实现对工业业务发展的支撑, 可以根据运行压力情况扩展系统能力。

易于升级: 数据安全主平台由各组成模块组成, 每个模块都配有灵活的配置文件, 易于助力工业企业开展升级工作, 能够方便地进行功能性和兼容性版本升级, 能够满足密码应用业务需求变更和操作系统、数据库等基础环境补丁升级的需求。

易扩展性: 当工业企业需要为新增的应用系统和数据库实例提供数据加解密服务时, 只需通过数据安全主平台配置, 即可完成添加数据源和应用系统的操作, 将从平台下载的加密插件部署在应用系统服务端, 这样仅对系统做少量简单的配置操作后就完成了数据加解密服务的扩展。

可弹性扩容: 数据安全主平台是以旁路的方式部署, 具有良好的可扩展性, 支持弹性扩容, 支持单机、双机主从、多机集群式的多种部署方式。根据工业用户单位实际业务需要, 支持从单机部署模式弹性扩容双机主从式部署, 也支持从双机主从式部署弹性扩容至多机集群式部署。

应用效果:

1、系统部署简单，实施周期短，建设成本低。基于免改造数据安全技术的工业领域数据安全保护方案，采用的免开发改造应用的加密技术，系统部署简单快捷，实施周期短，建设成本低。同时对实施技术人员的要求，也不需要像开发人员那样的高级编程技术，降低了人工成本。系统易扩容，可只在制造业用户单位部署一套管理端集群即可，各分支机构仅部署加密插件即可。在多个目标应用的节点上分别部署加密插件，通过一套数据加密系统集群，对多个应用节点上的多个加密插件进行统一管理，从而实现分布式部署，集中管控。后期新增系统需要进行加密防护时，可利用前期工程及同期建设相关工程的软硬件设备，以提高资源的利用率，降低建设成本，充分保护原有的投资。

2、大大降低了因数据安全风险造成经济赔偿的风险。数据作为新型生产要素，是实现业务价值的主要载体，数据安全威胁伴随业务生产无处不在。因此，凡是有数据流转的业务场景，都会有数据安全的需求产生。本方案中的工业领域数据安全主平台，对应用系统中个人敏感信息、企业商业秘密等进行了加密保护，即使"被拖库"泄露，也是密文数据，没有任何价值，大大降低了因数据泄露给企业带来的舆论危机、品牌影响、法律惩罚、个人索赔等经济损失的风险。

经验总结:

通过此案例，总结获得了以下几方面经验:

1、在基于免改造数据安全技术的工业领域数据安全保护方案的实际部署过程中，我司深入了解了制造业用户单位业务流程，全面掌握其业务状况和系统关联，积累了宝贵的行业性安全建设实践经验，将为我司未来在工业其他用户项目推广和实施部署奠定坚实的基础。同时，经过本项目案例的检验，免改造数据安全技术的安全防护能力在工业领域得以验证和完善，实现安全与业务在技术上解耦、但又在能力上融合交织，能够达到实战攻防部署应用的标准，我司有充分的信心将此作为最佳实践，全面推广至政务、金融、运营商、

教育、医疗、文旅、能源等更多行业场景，为行业整体的安全防护水平提升作出贡献。

2、本项目方案属于业务系统中数据安全的支撑，服务于工业各业务线和相关数据服务团队。该方案可以灵活部署集群规模，从用户投资成本角度考虑，该方案在技术上能保障本期需求以及未来五到十年的发展需要，充分发挥了安全系统的计算能力，保证合理投资效益的最大化。此外，该方案的应用集群可以灵活扩展部署，保障业务增长不受影响。

美创科技：某"双一流"高校的数据安全治理实践之路

案例提供方： 美创 MEICHUANG

案例背景：

某高校是全国重点大学，国家部委和市人民政府共建的"双一流"、"211工程"高校，中国著名的高等学府。

近年来，方兴未艾的数字化浪潮为高校注入新内核，校园管理工作逐步从线下模式转变为线上服务模式，通过服务大厅，为学生、教职工提供一站式服务。为进一步消除"数据孤岛"，该高校网络信息中心（下称"信息中心"）探索建立数据平台，形成学校各部门之间的数据共享，包括人事处、教务处、财务处等业务部门，实现学生选课、资产报修、学校公章、在读证明、就业手续办理等业务对接。

然而各类型应用系统不断增多，系统间业务协同交互场景逐渐增加，业务数据不断汇聚整合，也带来新挑战，数据安全问题也随之而来，在合规监管要求不断提升的背景下，如何进一步加强数据安全和师生个人信息保护提上了日程。

为响应国家号召，全力保障"智慧校园"发展，同时也为有效摸清目前高校在管理、技术层面可能存在风险隐患，规划下一阶段数据安全建设目标，该高校携手美创开启本次数据安全治理工作。

关键挑战：

1、安全理念不匹配：高校内部部门二十多个，且系统多样，有统推部门系统（如教师职称、学生入学、学籍管理等），也有学校自建系统（如招生就业、门户网站、校园一卡通等），这些业务系统负责的部门由于缺乏专业的网络和数据管理人员，对这些系统业务数据的使用和管理上缺乏了解和控制。

2、职责划分不清晰：数据安全治理工作是一项从上至下、持续性、长期的系统工程，从现有的组织架构上看，目前数据安全管理组织架构比较完整，但职责划分上仍需进一步明确，尤其是数据共享使用场景下，暂未形成规范化的流程，一旦发生数据安全事件，将无从定责追责。

3、数据标准不统一：虽然该校信息中心建立了数据平台，实现了多部门之间数据共享，并按照教育部《教育系统核心数据和重要数据识别认定工作指南（试行）》文件要求，制定了数据分级分类策略，但由于业务系统庞杂，并且业务优先的原则，导致各部门使用数据标准不统一，阻碍了数据分类分级的落地。

4、数据安全难保障：在目前的安全建设体系中，数据安全存在一定的风险隐患。例如数据库运维管理松散，

学校合作第三方开发人员和运维人员私存数据库账号密码，存在数据泄露风险，并且数据资源的使用没有约定范围和有效期，导致数据使用失控。

解决方案：

针对该高校上述存在的各方面问题，美创结合高校当前实际情况，认为可从以下几个方面进行入手：

1、对现有的应用系统数据库进行全面摸底，做到“底数清、情况明”，熟悉各部门业务系统、数据敏感程度、数据使用多方面情况，尤其需要关注个人信息数据存储、使用情况；

2、数据所属业务的职能部门是数据的主管单位，应当向各业务部门明确数据使用处理规则和防护要求，尤其是业务部门在数据共享交换的场景下，应当对申请的数据资源范围、期限进行明确；

3、参考DSMM模型内容，开展数据安全风险评估，了解目前的数据安全工作程度，也可完善高校的数据安全检查内容，作为定期开展安全检查的依据；

4、根据风险等级，结合现有的安全技术手段，以及部门间业务运行、数据流转过程，规划下一阶段的改进和建设任务目标，并针对具体场景的风险程度进行优先级设定。

具体内容包括：

1、数据资产梳理。以系统级、表级的颗粒度，对针对评估范围内的数据开展梳理工作，共计梳理3万张表、50万个数据字段，数据类型覆盖业务数据、个人信息等，如流程表单、户口所在地等。大部分数据为“个人身份信息类”、“个人财产信息类”等敏感个人信息，如户口地址、一卡通卡号、余额等。

2、基础环境风险评估。对系统和数据库服务器进行安全扫描、安全配置核查和分析，以及对数据权限分配情况的探查，发现配置的不合规项。例如高权限的废弃账户，美创结合实际需求提出了整改修复建议。

3、数据安全能力评估。结合高校现状以及对数据安全管理的目标诉求，从组织建设、制度流程、技术工具和人员能力等方面，分别对标数据安全能力成熟度模型（DSMM）二级和三级能力要求，从差距分析的结果来看，组织与三级能力仍存在较大差距，故后期若开展能力规划，可先设定到二级，再逐步进行推进。

4、数据安全合规评估。根据所在教育（高校）行业和地区的法律法规、政策规范等，进行筛选、识别、关联分析，对相关条款逐一进行阐述，根据现状进行对标分析。通过合规评估工作，除了发现潜在的合规风险，也帮助高校对数据安全相关政策要求有了更进一步理解。

5、数据安全风险评估。数据安全风险评估是以围绕数据全生命周期的数据处理活动，采用了定性和定量相结合的风险分析方法，对数据资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能

性的评估。通过风险分析，发现数据在全生命周期的处理活动中，均存在不同程度的风险。

6、数据安全建设规划。在管理层面，根据行业、地区、上级要求以及高校现行制度，结合实际场景，制定了《个人信息保护管理办法》、《数据全生命周期安全管理制度》、《数据分类分级规范》、《数据安全事件应急预案》、《数据安全监督检查管理办法》等制度文件，明确了数据在多个阶段的安全管理要求。同时对多个现行的制度内容进行了审查，提出了优化建议以及持续关注点，如网络安全事件应急预案、数据共享交换规范等。在技术层面，结合具体的数据使用场景，根据风险情况提出下一步的整改建议，包括技术手段、依托产品工具的建设方式、建设周期、建设优先级等。

数据生命周期风险分析

创新性与优势：

1、分钟级输出双一流高校完整的数据全生命周期风险评估报告。针对组织数据生命周期各阶段活动，可依据前置数据采集和分析结果，自动完成生命周期各阶段的风险分析，生成数据资产的全面风险清单，为风险治理提供依据，也为从数据全生命周期体系化考虑数据安全建设奠定基础。

2、提供专业工具"数据安全综合评估系统"，依托该工具，人员投入量有效降低90%以上，交付时间缩短84%以上。该工具内置极为丰富的知识库，全面覆盖法律法规、标准规范、各类分析模型及规则等，数据安全合规库（覆盖300+文件）、数据安全风险库（覆盖17大类、83子类）、安全处置策略库（覆盖5000+条策略），实现评估检查更精准、更全面。

3、通过“数据安全风险评估系统”，极大降低对人员的能力要求。简化咨询分析流程，大幅缩减评估分析过程周期，实现快速、敏捷的项目交付，将传统安全治理方式化繁为简，化重为轻。

应用效果：

通过本次数据安全治理，该高校明晰了当下数据资产的重要性以及潜在的安全风险，确定了下一步的工作任务和重心，主要产生的成果价值如下：

1、厘清了数据资产敏感程度：通过资产梳理明晰了目前数据的规模、敏感程度，以及存在的废弃数据。结合风险评估结果识别出存在中、高风险级别的数据资产，同时以同行业最佳实践做法为参考，讨论现有的分类分级策略的合理性，提出了数据分类分级的改进方向。

2、落实了数据安全主体责任：依据教育部发文以及现行的数据管理相关制度，在现有的部门职责定义的基础上进行了修订和更新，按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，与信息中心讨论并重新定义了“数据主管部门”、“数据运营部门”、“数据使用部门”三大数据职能机构的责任和义务。

3、健全了数据安全管理体系：参考ISO四层体系要求和DSMM模型，规划数据在各个阶段、场景的安全管理规范和流程，通过逐步建立具体的安全操作规范和流程，制定更具体的约束性措施，全面满足管理需求。在本项目过程中落实的部分制度内容，也在一定程度上完善了高校的数据安全管理体系。

4、提升了数据安全防护理念：目前数据安全整体缺乏体系化建设，没有从数据全生命周期来考虑数据安全建设，仅基于合规要求部署网络安全设备或单点防御、检测设备，造成风险隐患。通过从数据处理风险较高的场景入手，结合现有的安全技术手段，以及部门间业务运行、数据流转过程，规划建立围绕数据资产的安全保障体系。

经验总结：

1、分类分级是建设基础。高校应结合法律法规、部门规章、行业标准（如：《教育部等七部门关于加强教育系统数据安全的通知》、《教育系统核心数据和重要数据识别认定工作指南（试行）的通知》等），制定数据分类分级标准，梳理出高校信息系统重要的数据目录，明确个人隐私和敏感数据保护范围，达到分类分级保护的效果。其中达到秘密级的数据应当遵循《保守国家秘密法》的规定。

2、借助专业工具、流式作业，助力控制成本、快速交付，实现数据安全治理敏捷咨询。基于数据安全综合评估系统、暗数据发现与分类分级等自动化工具的数据资产梳理、数据权限梳理、安全现状分析、数据合规基线分析、安全能力差距分析、数据安全风险分析、数据分类分级等多重能力，可有效降低人员投入量，并大幅缩

短交付时间。

3、数据安全管理制度、操作流程等是建设的依据与落地的关键。高校可从决策层、管理层、执行层、配合层、监督层5个层面进行组织建设，明确数据安全责任人；在制定数据安全管理与隐私保护相关办法中，明确数据收集、存储、处理、共享等关键环节的操作规范、管理部门职责分工、应急管理与安全检查机制，从而充分发挥各部门和各类人员在数据安全保障工作中的作用，共同遵守和执行安全规章制度，保障数据安全策略的贯彻落实。

体系化规划、体系化建设、体系化运营。高校需从制度、技术和运营着手，以数据分类分级为起点，以管理制度为依据，在具体建设过程和环节中，充分利用和发挥好各种关键技术的作用，分段实施，体系规划，逐步构建覆盖数据全流程、全链路的数据安全防护技术体系，最后构建数据安全运营体系，实现数据安全的持续优化和提升。

东方通网信：电信行业数智一体化数据安全管控产品解决方案

案例提供方： 东方通 TongTech

案例背景：

随着数字经济发展企业数字化转型的加快，电信行业内部的应用系统越来越多，存储的数据也越加庞大，数据的交互流通越来越复杂，企业数据安全面临着数据存储风险、数据流动共享风险、行业数据监管要求等多方面的压力与挑战。企业数字经济发展所带来的数据安全风险，主要包含：首先目前越来越多企业都已将部分核心业务上云管理，随之而来的是企业IT环境更加复杂，云化环境与传统IT环境混合传统的设备边界变得不那么清晰、设备资源不断的进行动态调整设备信息变得更加难以掌握；其次随着企业数据化转型的加快，将会引入越来越多的业务系统进行细分化管理，数据电子化管理需求愈加旺盛，存储的数据重要程度也越来越高，一旦发生数据泄露事件必定会给企业带来严重的影响和损失。再次，随着国家数字赋能、“互联网+政务服务”等服务的开展数据共享与开放的场景越来越多，数据的交互流通虽然能更好地实现数字价值，但是伴随的数据安全挑战也越加多样。最后随着我国大数据、云计算等新兴技术的发展，企业存储的数据类型与数据量级越来越大。与此同时，藏身暗处的“灰黑产”对经济利益的极度渴求令大数据环境变得更为波云诡谲，而面对内部人员、合作伙伴及外部黑客的数据安全风险与威胁，如何满足企业自身数据安全管理需求、国家及行业监管成为电信行业数据安全保障的核心问题。

关键挑战：

1、电信行业如何开展数据安全治理工作

国内外对于数据安全治理的理论依据及顶层设计众多，包括：国际Gartner数据治理框架DSG、国内DSMM数据安全能力成熟度模型等，如何将数据安全治理的理论依据及顶层设计的指导思想，结合国内电信行业现状，推导出符合当前电信行业现状的特点的数据安全治理解决方案，寻求企业最佳数据安全治理建设路径，是本次申报方案拟解决的首要关键挑战。

2、电信行业数据安全保障体系应如何构建

数据安全保障目标是保护数据权属性、保密性、完整性、可用性、可追溯性，实现数据“可管、可控、可信”。保障企业数据资产及用户隐私,应遵循国家层面对数据安全保障的重要指导精神为工作指引，全面规划落实各项数

据安全保障手段，如何构建完善的数据安全保障体系，保障管理制度、安全生态、创新安全服务的有效落地，支撑业务健康发展及建设，将成为业链各环节主体的首要目标，是本次申报方案拟解决的第二个关键挑战。

3、如何构建自动化数据安全技术支撑手段

在国家对技术创新支持力度不断提升的大背景下，产业链各环节主体将数据脱敏、数据加密、数字水印算等数据安全关键技术的能力提升和创新发展提供有力支撑，联邦学习、多方安全计算等处于萌芽期的新兴技术，为解决数据利用，与数据保护之间的矛盾提供了新的解决方案，随着应用领域的不断扩展和需求的不断释放以及理论研究的不断深入，实现核心技术的持续演进，随着新老技术不断交替，企业如何构建符合自身要求的数据安全技术支撑手段，是本次申报方案拟解决的第三个关键挑战。

4、电信行业数据安全运营应如何推进

数据安全能力建设与数据安全运营应是相辅相成，只有能力没有运营，能力则成为了"空架子"，无法体现最终价值与成效，包括数据分析、风险管理、应急处置、策略优化、关键环节的风险隐患识别、防控、应急等方面的意识、明确关键岗位职责、加强日常培训等要求，都需要配套常态化运营保障机制，在有能力基础的前提下，只有真正将数据安全运营做的好，数据安全能力建设才会发挥最大的效能，故电信行业数据安全运营应如何推进，是企业面临的最后一个关键挑战。

解决方案：

东方通以国家法律法规、行业标准规范、顶层设计理论为指引，结合电信行业数据安全现状，采用"管理管控双管齐下"的方式，围绕电信行业数据全生命周期特点，分阶段构建由内到外的数据安全纵深防御体系，从威胁防御、风险管控、数据追踪溯源、数据共享与交换、数据防篡改等多个层面，打造数智一体化数据安全能力，提供符合电信行业特色的数据安全一站式全景化产品解决方案，全面落实电信企业数据分类分级、数据对外接口管理、数据安全风险监测、数据泄露分析溯源等多方面数据安全管理能力要求，具有"能力自动化、分析智能化、交互便捷化、效果可视化"等显著特点，从而辅助电信企业科学规划安全体系、全面提升企业自身数据安全防御及风险感知能力，赋能政企市场高质量发展，满足注智赋能需要，具体包括：

聚焦"两条主线"，通过"四个标准化动作"，对"五个重点方向"持续深化，支撑电信行业数据安全工作管理要求，实现关基、网络云、5G专网的数据安全集中运营，着力构建世界一流高质量网络和安全保障体系。

"两条主线"：紧跟国家十四五战略规划、行业监管要求， 聚焦"能力建设"、"能力运营"两条业务主线，发挥技术、数据要素价值，构建易用、好用、管用的数据安全能力，切实做好数据安全运营管理工作。

"四个标准化动作": 推出符合电信行业现状的保障体系,明确职责、管理、技术要求, 形成考核机制, 推进"以评促改、以评促建", 强化省内协同, 实现统一指挥、联动治理、能力协同的整体目标。

"五个重点方向": 结合DSG、DSMM理论基础, 借鉴行业领先技术及最佳实践经验, 在五个重点方向, 包括: 数据分类分级、数据权限管理、数据共享与交换、数据风险追踪溯源、数据安全问题处置等方向, 实现"数据清、权限清、接口清、问题清、处置清", 严格落实数据全生命周期管理工作, 强化了数据安全全生命周期管理能力。

整体架构设计思路是根据收集、传输、存储、使用、提供、销毁等数据安全治理建设路径, 以问题为导向, 以流程为驱动, 以任务为抓手, 责任到人、问题闭环, 加快应用创新智能技术手段, 实现向任务化、流程化、自动化、智能化转变, 构建一体化的数据安全运营、数据安全技术、数据安全管理的保障体系。

数据安全运营保障体系, 提供专业的数据安全运营服务能力, 实现包括数据分析、风险管理、应急处置、策略优化等运营服务, 全方位保障企业数据安全运营环境。

数据安全管理保障体系, 是指一系列的法律法规、规章制度和组织管理措施, 确保数据安全管理有法必依、有法必行、有规可循, 旨在保护数据的完整性、可靠性、保密性和可用性。

数据安全技术保障体系, 基于现有数据安全能力, 构建上层数据安全态势感知及下层数据安全管控, 搭建整体数据安全保障框架, 从而实现企业数据安全管理的可知、可察、可控和可管。

创新性与优势:

1、结合顶层设计理论, 形成电信行业数据安全治理最佳实践

结合Gartner数据安全治理理念及DSMM数据安全能力成熟度模型, 将理论与实际相结合, 推导出符合电信

行业能够快速落地的最佳实践方法，创新性的通过"五个步骤"，包括：

- 网络数据资源清单式管理
- 数据使用情况梳理
- 安全策略制定与下发
- 网络数据资源威胁及风险分析
- 数据安全问题处置与跟踪

最后通过以人员为基础、以任务为驱动、以能力为抓手，构建数据安全运营体系，将管理工作与工具化的数据安全能力深度拉通，并加强与现网其他平台的协同与联动，深化现网安全系统协同成效，解决单一系统仅能聚焦在特定领域等问题。

2、首创基于"去混淆"技术及复核规则识别电信行业敏感数据

基于"去混淆"技术，结合NLP、相似度、AI等多种复核规则的方式识别敏感数据，可对经过特殊处理的敏感数据，如数据杂质化、加密、模糊化的原始内容进行数据标识及验证，并且首次提出通过"错峰+断点+抽样+异步流式处理+脱敏+指令通道"等保障手段，能够在保证安全性的同时最大限度降低分类分级对业务侧的性能损耗。

3、依托AI能力，实现数据共享接口的高效、智能化管理

结合AI算法，自动化识别API、FTP/SFTP、交换机旁路镜像等方式进行数据共享的对外接口，并创新性的以"工具化、脚本化"的形式，对外提供数据共享接口核查服务，仅需在设备上执行检测指令，即可了解该设备存在的数据共享接口，落地快速简单，可有效保证电信行业用户对于数据共享接口管理的全面性及准确性。

4、结合"数据血缘"及互联网"画像"技术实现泄露过程中数据"变换"等数据安全风险问题。

依托"数据血缘"技术，对泄漏主体内容进行血缘分析，有效识别泄露数据"变换"类问题（如：原始文件做过分割、影像、杂质话等特殊处理），并根据"UEBA"理论为基础，通过对自然人的行为规律进行AI建模及正态分布算法等，得出自然人行为基线轨迹，从而分析基线偏离的异常行为，自动化的找出数据安全问题和风险等，过程中无需任何策略配置，即可实现数据安全问题动态分析，有效支撑应对未知数据安全风险。

5、基于商用密码技术构建"可信数据安全网盘"。

基于多种数据安全管控能力，包括：数据识别、金库、脱敏、水印，结合商密算法，建立可信数据传输通道，彻底解决"敏感数据不落地"的问题，对非法数据外发进行威慑，有效降低数据泄露风险及隐患。

6、实现SaaS化的数据安全服务模式，对内满足按需交付的新型服务模式，对外满足通信企业能力变现需要。

精选关键数据安全能力，适配云化防护特性及国产化需求，创新性的构建一套"数据安全能力货架"，打造基于租户的产品化、自助式、按需交付的IT云资源及安全支撑服务模式，形成集中管理、按需服务的安全

场景化应用，赋能政企业务高质量发展，满足"注智赋能"需要。

应用效果:

应用于移动公司内部, 切实保护重要和和核心数据以及个人用户信息, 夯实由内到外的事前防御、事中管控、事后审计的主动安全纵深防护体系, 全面落实了《国家安全法》 、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规要求, 现已推广至中国移动数个省份, 实现电信行业数据安全治理过程中的数据清、权限清、接口清、问题清、处置清等"五清"成效, 强化了数据安全全生命周期管理能力, 实现电信行业数据安全基础管控及防护能力, 收敛数据安全风险暴漏面。

经验总结:

该产品解决方案已为电信行业企业探索出一条落实数据安全管理要求的最佳实践方法, 可全面落实了《国家安全法》 、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规要求, 在支撑企业监管需要的同时, 聚焦企业"能力建设、能力运营"两条主线, 强化企业纵深数据安全防护成效, 具有落地时间短、落地方式简单、落地效果明显等特点, 十分的"务实、接地气", 目前该方案已经成功在电信、能源、教育等多个行业的头部企业用户进行落地, 可复制推广性极强, 未来可面向更多行业推广使用。

数安行：证券信息系统数据安全计算与安全计量项目

案例提供方： 数安行 DataSecOps

案例背景：

随着2021年数安法、个保法相继公布实施，金融行业相关监管部门在数据安全方面的监管日趋加强。证券行业作为金融业的重要领域之一，同样处于金融业的强监管之下。除了国家法律法规的监管要求，证券行业自身也有一系列监管要求，比如2018年中国证券监督管理委员会发布《证券期货业数据分类分级指引》；2020年中国证券业协会发布《证券公司信息技术治理工作指引》；2021年中国证监会科技监管局发布《证券期货业"十四五"数据治理规划（征求意见稿）》），指导金融机构建立企业内部数据安全体系，规范管控和技术标准，明确数据全生命周期安全要求，以解决数据安全治理、管理、技术、基础支撑各层次的历史难题。在国家、行业一系列的监管要求下，保障数据安全也是证券行业的从业根本。如果确保在数据的使用过程中合规可控成为热点问题。隐私计算等大量技术的兴起也是在寻找合规共享数据是的问题，但目前仍缺乏有效的应用，如何在现有机制下，控制数据的使用范围，安全分享和使用数据一直是一个难点问题。

某地方证券公司拥有员工3000人，各分公司驻扎在全国各地，并在不同的业务方向上各有发展。该公司在业务方面有多年的发展和积累，形成大量的客户资源。以前对客户关系的管理和服务、产品的构建、形势预测分析等，主要依赖人工分析决策方式。在客户量小、客户服务诉求简单的情况下，这种方式在服务效果、业务拓展方面能够取得一定的成就，但随着公司的发展和客户量的持续增长，出现如下主要问题：

1、针对性不强，无法更好地理解现有客户需求并提供更个性化的服务，影响客户满意度和粘性；

2、产品创新力、竞争力有待提升，产品层面的优势难以发挥；

3、信息服务能力需要数据处理和分析能力的支撑，信息服务亟需更加精准、高效和个性化。

在上述背景下，公司从2020年开始尝试数字化转型，期望是通过大数据计算，一方面获得即有客户的满意度，提升持续服务的能力；另一方面公司也期望通过大数据分析提高信息服务的质量和效率，构建创新性的产品，并指导公司层面制定战略计划。因此，公司建立了数据研究室，数据研究室成员主要来源于总部，还有一部分属于一个擅长数据分析的子公司。公司期望通过数字化转型，对数据充分利用的基础上，促进商业模式的转变。

关键挑战:

大数据计算意味着给这些数据可能带来新的问题:

1、计算分析的过程扩大了数据暴漏面, 可能造成更严重的数据泄露;

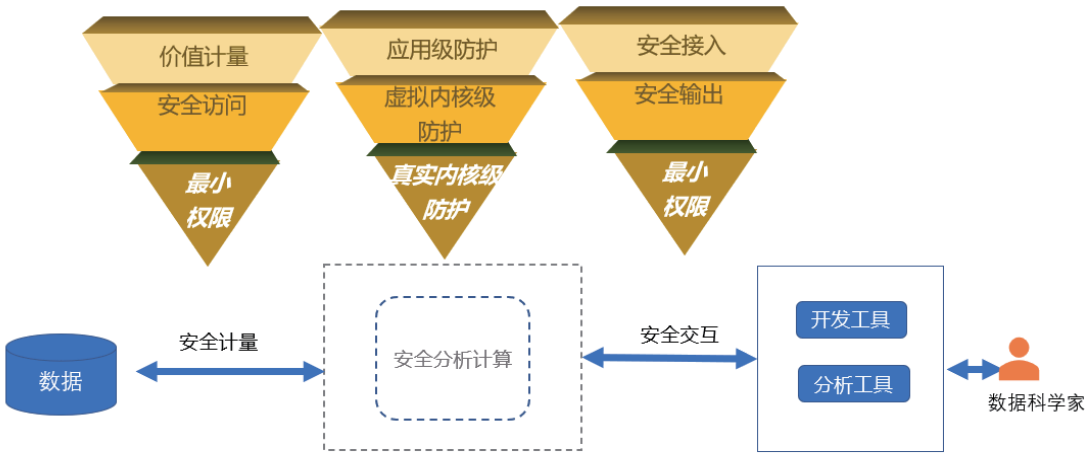
2、计算分析过程中, 如果能够保护数据安全, 那采取的安全方案或者是安全措施是否会给计算效率带来明显的降低, 甚至影响分析结果;

3、数据本身的价值难以预估;

4、大数据分析的投入与产出难以衡量。

解决方案:

在《证券信息系统数据安全计算与安全计量项目》中, 主要采取以下安全技术应对数字化转型的风险:



无感数据安全沙箱

1、数据安全沙盒保护大数据计算节点安全

数据安全沙盒为计算节点构建了一个虚拟化的计算环境。计算环境与外界隔离, 所有参与计算、分析的原始数据对数据分析人员是不可见的, 经过计算后计算结果不包含原始数据, 计算结果对数据分析人员来讲是公开的。

将数据从数据源获取到数据安全沙盒计算节点时, 获取过程受到身份鉴权及数据访问权限的控制。

数据安全沙盒对计算过程无影响, 这得益于数据安全沙盒技术的基因, 一方面通过逻辑隔离建立计算节点的外围屏障, 另一方面从应用层、虚拟层、内核层分层采取安全防护措施, 防止数据在计算过程中被泄露。参与计算的数据在数据安全沙盒中可用不可见。

2、数据资产图谱构建数据价值计量

数据资产图谱是对大数据计算全过程中，参与计算的数据的多维映射，包括了数据资产的分类、数据资产的敏感度、数据资产的初始价值、参与计算的频率以及计算结果应用以后所能产生的价值。以计量模型为依据，形成数据资产图谱，对公司所掌握的总的资产值、通过数据创造的价值形成价值计量。同时，结合计算结果输出以后，实际给公司带来的效益，做中长期的数据价值的预测。

创新性与优势：

1、新型安全模式：数据安全计算不断探索新的计算模式，数据安全沙箱技术能够在不暴露原始数据的情况下进行数据的共享和计算，为数据的隐私保护提供了创新的解决方案；

2、量化数据价值：通过数据资产图谱安全计量，对数据的价值进行精准量化，帮助企业更好地了解数据的经济价值，为数据交易和流通提供可靠的定价依据。通过量化数据价值，促进数据的合理流动和有效利用，从而推动数字经济的发展。

3、优化资源配置：通过数据价值安全计量，企业更清晰地了解不同数据的价值差异和潜在价值，从而根据业务需求和市场变化，优化数据资源的配置和利用，有助于提升企业的决策效率和市场竞争力，实现数据资产的最大化利用。

4、高安全性：数据安全计算和安全计量采用了细粒度的身份鉴权与访问控制，结合安全沙箱的多层级保护，确保数据的机密性、完整性和可用性有效防止数据泄露、篡改和滥用，保障数据的安全。

5、高效率：通过优化安全算法，数据安全计算和安全计量能够在保证安全性的同时，实现较高的计算效率和数据处理速度，在实际应用中发挥更大的作用。

创新性与优势：

1、数据计算过程获得安全保障。数据安全计算通过采用一系列安全措施，确保数据在处理过程中的安全性，有效地防止了数据泄露、篡改和滥用。为企业提供了强大的数据安全保障，能够促进数据的开发利用。

2、计算效率高，无影响。2、在不增加时间损耗的前提下，数据处理得到正常的计算结果，使得数据安全计算和安全计量能够更好地满足实际应用的需求，为各行业的数字化转型和升级提供了参考。

3、资产价值获得衡量。通过项目的实施，对公司的资产价值有了比较全面的掌握，当前的计量模型和实际公司数据资产的价值符合度比较高。

4、合规遵从性：4、通过数据安全计算与安全计量，企业能够更好地了解和掌握数据的安全状况和价值，从而更有效地制定和执行数据安全政策和措施，增强了合规性。

经验总结：

通过此案例，总结获得了以下几方面经验：

1、深入理解用户数据处理的场景，精确技术选型：选择适合特定场景和需求的数据安全计算和安全计量技术，确保所选技术既满足安全要求，又符合性能标准，不影响用户的处理过程。

2、依据现有安全能力和用户数据处理过程，制定全面安全策略，确保数据在整个业务流程中都得到妥善保护。优化数据处理流程，降低数据泄露和滥用的风险。

3、平衡数据的利用和安全，在设计和实施数据安全计算和安全计量方案时，权衡安全性和可用性，确保方案既安全又易于使用。

4、保障数据处理过程中良好的安全效果，需要综合考虑技术、管理等多个方面的因素。企业应根据自身的实际情况和需求，制定合适的实施方案和策略，确保项目的顺利推进和取得实效。

5、技术的整合与协同：企业已部署多种类型的安全能力，需要考虑不同技术之间的兼容性和互操作性，将数据安全计算与安全计量技术与现有系统进行整合，确保技术之间的协同工作，提升整体的效果。

一知安全：XX头部汽车制造商终端全场景数据安全防护系统建设项目

案例提供方： 一知安全

案例背景：

伴随数字化转型，随着信息化到数字经济的演进，数据要素应用场景越来越广泛，现代的企业经营活动已经离不开数据要素的运营，它直接参与生产与服务过程，大幅提高供需对接水平，优化生产流程，促进产业链协同，增强企业竞争力。但是随之而来的安全问题也日益凸显，对于企业网络与数据的入侵事件高频发生，。国家虽然出台了以《数据安全法》为核心的一系列法律法规，指导企事业单位进行数据安全建设。但是传统数据安全解决方案在面对企业数字化建设过程中出现的新办公模式、多终端接入、内外部人员接入等多场景的数据建设比较无能为力，企事业单位对于如何落地数据安全建设，如何做到全场景适配依然比较茫然。

对于企事业单位而言，传统的企业安全边界已经被打破，出现了更多的远程办公、离线办公场景，这些终端成为了企业数据安全的突破点。同时不仅是企业统一发放的终端需要进行管控，员工个人的终端，外部的一些终端都有需求需要接入公司网络，企业核心数据都有可能落地到这些终端上被攻击和产生泄露。在整个数字经济的推动下，企业数据安全建设已经不可能将数据锁在公司内部使用，单纯的进行内部人员数据安全管控了。企业业务系统有大量的供应商、合作伙伴、外包人员等角色需要访问，企业的数据需要在这些角色中进行流转才能发挥最大价值，如何对于多种多样的角色使用数据进行管控，也是企事业单位认为传统数据安全方案无法解决的难题。

某汽车行业客户作为汽车头部制造商，为了满足企业数据安全在技术层面的保障和制度层面的规范，建立完善的数据权限管理制度，对敏感数据在传输和存储过程中进行保护，确保数据的保密性、完整性、可用性和可审计性；建立安全审计与管控机制，对数据访问和使用进行实时管控，对异常操作进行及时告警和处置，确保汽车数据的安全和合规使用，促进汽车行业的健康发展。在合规要求和安全运营的双重背景下，通过使用山河安全工作空间平台，利用核半虚拟化和零信任理念，保障数据在非可信环境中的安全使用。实现收敛数据暴露面、认证的安全和灵活加强、落地到终端的数据可控。

关键挑战：

1、公司内部很多研发设计人员，对于终端性能要求非常高，不能因为数据安全的建设降低生产效率，员工使

用体验需要放在第一位。

2、公司员工出差频繁，并且需要到很多极端环境中进行电池性能的测试，这些环境中是没有网络的，如何在安全的前提下保障正常出差人员的远程办公，以及进行极端环境下离线终端的管控是在进行数据安全建设方案的选择时需要考虑的核心问题。

3、公司内部也划分了不同子公司，文件之间流转交互情况非常多，子公司内同部门之间、子公司内不同部门之间、不同子公司、甚至是内部与外部的数据流转都需要进行严格的管控和审计。

4、接入公司业务系统、存放公司数据的终端非常多，，IT运维人员压力非常大，数据安全系统的日常运维需要非常简单，尽量减小日常管理运维工作量。

解决方案：

为满足上述需求并应对当前的关键挑战，一知团队在深入调研业务实际运行场景后有针对性地为客户提供了一套山河安全工作空间解决方案。

山河安全工作空间是一款以原生安全、极致体验、轻量敏捷为特点的工作平台，是以自研的内核级半虚拟化技术为核心，隔离互联网区域和涉密业务区域，采用零信任接入手段，打造安全的接入与访问，实现终端数据安全的数字化工作空间。由端侧数字化安全工作空间、端侧安全检测与分析、零信任安全网关、策略控制中心和后端应用模块（包括云文档备份、应用集市等）构成。内核级半虚拟化技术构建的数字化工作空间实现对网络、文件、进程、用户、会话、外设等完全隔离，搭配基于零信任架构的安全网关、控制中心、后端丰富应用模块，在复杂的终端环境中构建统一、安全可控的工作空间。同时做到收敛业务在网络上暴露面以及数据在终端暴露面，保障企业核心数据从产生到使用、流转以及销毁的全生命周期安全，提升员工效率，减轻运维压力。

山河数字化工作空间客户端负责在不可信终端上构建可信使用环境，对数据进行保护，同时与安全网关进行通信，建立加密通信隧道，保障访问可信。相较基于sandboxie的用户态沙箱类产品，山河数字化安全工作空间使用完全自研的内核级半虚拟化技术，复用宿主操作系统的内核能力，性能与物理主机相同，无虚拟网卡（增加嗅探面）添加，构建出可信环境，与个人空间完全逻辑隔离，具体体现在网络、文件、进程、模块、用户、会话、外设等层面进行完全隔离，配置有诸如剪切板控制、屏幕水印、截屏录屏控制、外设控制等相关数据保护功能，阻止一切数据主动或被动的泄密方式。

山河策略控制器是参考零信任架构实现的整体调度与管理中心。该组件负责认证、授权、策略管理与下发。负责控制建立连接和切断终端到业务中心的通信连接。它负责生成客户端用于访问应用的身份验证凭证。策略

控制器支持自适应身份认证、动态权限控制，对接入的身份、终端、环境、行为进行信任评估，基于策略引擎配置的策略结果，决定最终允许或拒绝会话。策略控制器使用SPA单包授权技术，只对已授权的山河环境可以接入进行认证，不可信环境无法访问。

山河安全网关是参考零信任架构实现连接与访问安全的网关设备。此组件负责建立、监视及切断终端到业务中心之间的连接，构建安全、可信访问通道。安全网关负责对山河客户端环境访问网络的流量加密，同时安全网关受 SPA 单包授权技术对设备本身的服务进行隐身保护——隐藏对外服务端口，只有已授权的山河客户端环境才能通过安全网关访问业务。安全网关还会记录所有的访问请求，包括源IP、目标 IP 以及访问的 URL 的路径，进行日志审计，方便溯源追责。

创新性与优势：

1、安全、体验与兼容性：基于内核层做内核半虚拟化，将文件、网络、外设、服务、RPC调动、命名对象、缓存、IO、协议栈等，都对其进行了模拟，和本机操作系统的相应部分完全隔离，并基于此构建出了独立隔离的数据环境，在隔离环境中完成数据全生命周期的管控。相比于传统的应用态沙箱重定向路线的打补丁的方式，在安全性、终端性能损耗、兼容性方面进行了极大的优化。

2、低成本一机两用：客户内部网络分为内部办公网与外部互联网，两套网络彼此互相隔离。而对于部分员工，既有内网办公的需要，同时也有在互联网查阅素材和下载资料的诉求。之前对于此部分员工，往往采用2台电脑的方案，一方面成本非常高，所以只有个别员工可以使用。另一方面，内网与外网数据交互非常麻烦，需要建设数据中转平台，也是一笔巨大的投入。通过山河安全工作空间，在终端上隔离出来一个或多个使用环境，不同环境之间完全隔离，可以完成在一套硬件上，在不同的环境中使用内网与外网，并且内网数据无法泄密，外网环境中了病毒之后对于内网环境完全没有影响。同时数据流转可以通过山河进行审批与审计，不需要额外建设中转平台，减少投入，减轻运维压力。

3、重构终端环境：对于传统安全边界外接入的终端，客户一直担心此部分终端本地病毒会通过接入内网产生蔓延和扩散，对内网安全造成影响。同时接入内网后下载的数据也会直接落地到这些终端上，有数据泄露的风险。山河安全工作空间通过在不可信终端上构建隔离的可信环境，使用可信环境接入公司业务系统，屏蔽本地病毒攻击威胁对于企业数据或业务系统造成影响，同时业务系统上下载的数据直接落地到可新环境进行保护。

4、统一办公入口：客户内部办公场景复杂，包含内网安全办公、供应链数据交互、外部终端接入内网、离线终端使用、远程访问、分支机构接入等多个有数据保护需求的场景，通过借助山河安全工作空间既具备网络管

控能力，同时能够在终端进行隔离环境、数据保护的能力，将山河安全工作空间打造成统一办公入口，对不同人员、不同终端、所有业务、全部工作数据都可以进行管控，满足客户各种使用场景。

5、低成本完成数据安全改造：通过轻量级的交付，低成本的完成客户数据安全改造，不需要购买大量服务器甚至复用原有计算资源即可实现终端数据安全保护，达到降本增效，提升安全防护级别的效果。

应用效果：

1、通过山河安全工作空间客户端，重构终端环境，在终端上构建一个可信的工作环境，对企业核心数据进行保护，防止一切主动或被动形式的数据泄密事件发生。同时不会降低终端性能，并且对于本地员工个人数据几乎没有侵犯，对于员工操作习惯没有任何改变，员工学习成本低，接受程度高。

2、通过零信任架构的山河后端，打造无边界的安全办公区域，满足员工或外部人员远程接入公司网络进行办公需求，同时可进行内外网的严格划分，对于公司网络分区分域提供帮助，增强公司网络管理能力。

3、通过操作简约化、日常可视化的界面，为客户IT人员减轻运维压力，丰富的日志报表可以为客户提供终端数据安全风险评估依据，轻量级客户端的低事故率让客户避免了之前焦头烂额解决终端问题的麻烦。

经验总结：

通过此案例可以获得以下几方面经验：

1、客户数据保护场景往往是复杂多样的，不能祈求以改变用户办公习惯的方式来进行安全建设，而面对庞大的用户群体、巨大的终端数量、多种的使用方式，传统的数据安全解决方案是无法全覆盖的，本案例中产品尽可能地满足了用户业务全场景的使用方式，解决了各场景下数据安全使用的难题，对于数字化转型浪潮下的企事业单位该如何进行数据安全建设具有重大参考意义及推广价值，有着极强的可复制性。

2、客户在保障安全的前提下，对于投入的预期一定是越少越好，本案例几乎没有硬件成本，并且在多个场景中降低原本的终端预算，低成本地完成了数据安全改造。对于各企事业单位的数据安全改造有着标杆性影响。

3、数据安全的改造不应该以牺牲生产效率的代价完成，客户的重心工作是生产，安全是为了保障更好的生产，产品一定要与业务结合，协助业务更好的发展。本项目中，在保障终端办公效率的同时，通过附带的文件流转、文件备份、应用安全管理平台等功能，对于员工的生产办公产生了积极的促进作用，增强了员工的办公体验，提升了员工的工作效率。给之前犹豫着在效率与安全之间进行取舍的用户极大信心，没有损失的进行数据安全建设。

4、企事业单位IT运维人员在面对终端管理时，人手都是不足的，压力非常大。数据保护不应该过多增加运

维人员工作量。本项目中通过可视化主页、人性化简易操作、强大的日志报表系统、轻量级客户端使用极大的丰富了运维人员管理工具的同时，相比传统数据安全解决方案减轻了运维人员的管理工作量。是企事业单位对于数据安全运维管理的典范。

总　结

政策法规监管要求和外部威胁引发的内生需求是推动数据安全行业和技术创新发展的核心力量。一方面数据安全被纳入总体国家安全观，进行顶层设计和合规监管，这是由国际竞争安全形势和国家发展战略所决定的；另一方面，国内外针对高价值数据的勒索攻击日渐猖獗，不断威胁各领域的机构运营，数据安全亦成为各领域机构运营安全的内生需求。

数据安全行业政策红利明显，但市场表现低于预期，内耗严重，创新不足是主要原因。数据安全的潜在需求没有得到充分释放，具体表现为数据安全产品场景少、同质化严重、成熟度不高、单点产品盛行。除产品以外，数据安全的人才和服务亦存在巨大的缺口，对整个行业的发展不利。

数据安全行业未来的增长将更多的依赖创新，通过解决更多场景的问题对用户的需求进行开发和释放。目前以及未来勒索攻击都将是数据安全最大的威胁，而对勒索攻击亡羊补牢不如防患未然。因此事前的数据安全风险识别、风险评估、态势感知、安全服务边缘、安全治理类产品会很有市场。另一方面，打通数据壁垒，推动数据要素能够安全的共享、流通、使用是另一个重要需求。因此，隐私计算、同态加密、数据合成等技术将会有更多的应用场景和空间。最后，系统化、平台化集成各种成熟单点技术、管理流程，减少内部复杂性，提高效率的数据安全平台类产品将会逐步取代现有的分散的单点产品。以上场景是当前数据安全技术创新的主风向。

此外，随着人工智能大模型的横空出世，大模型在数据安全领域的应用正变得越来越普遍，在威胁检测和响应、欺诈检测、安全运营自动化、数据泄露和隐私保护、智能合约和区块链安全、安全智能体（AI Agent）等场景的应用纷纷涌现，与大语言模型（LLM）的结合将是未来数据安全技术创新的必然趋势。

ISC
2024
数据安全技术创新发展报告