2023年中国安全技术成熟度曲线

Published 25 October 2023 - ID G00804444 - 11 min read

By Analyst(s): Feng Gao, Anson Chen, Mia Yu, Angela Zhao

Initiatives: Digital Technology Leadership for CIOs in China

有限的预算、严格的监管要求和日益扩大的数字风险敞口，对中国企业机构的安全投资构成了挑战。首席信息官（CIO）以及安全和风险管理（SRM）领导者应参考这篇技术成熟度曲线，在艰难环境中优化安全投资。

分析

企业需要了解什么

2023年，在中国运营的企业机构面临诸多挑战：经济增长低于预期，限制了预算额度；日益严格的监管要求和日益增加的数字风险，意味着需要追加安全投资。企业机构必须平衡各项挑战，确保安全投资的优先级。

多种趋势推动着中国安全技术的发展，包括威胁暴露面管理、网络安全平台整合、零信任技术采用和身份优先安全（请参阅Top Cybersecurity Trends in China for 2024 and Beyond）。

由于使用非本地供应商的安全工具会面临较多的合规问题，本地安全供应商在中国安全市场占据了主导地位。

CIO和SRM领导者应参考这篇技术成熟度曲线，了解中国本土创新特点，优化中国安全投资。

技术成熟度曲线

这篇技术成熟度曲线介绍了中国安全领域的创新，包括今年新增的四项创新：

- 数据安全治理
- 暴露面管理
- 中国的隐私保护
- 安全服务边缘

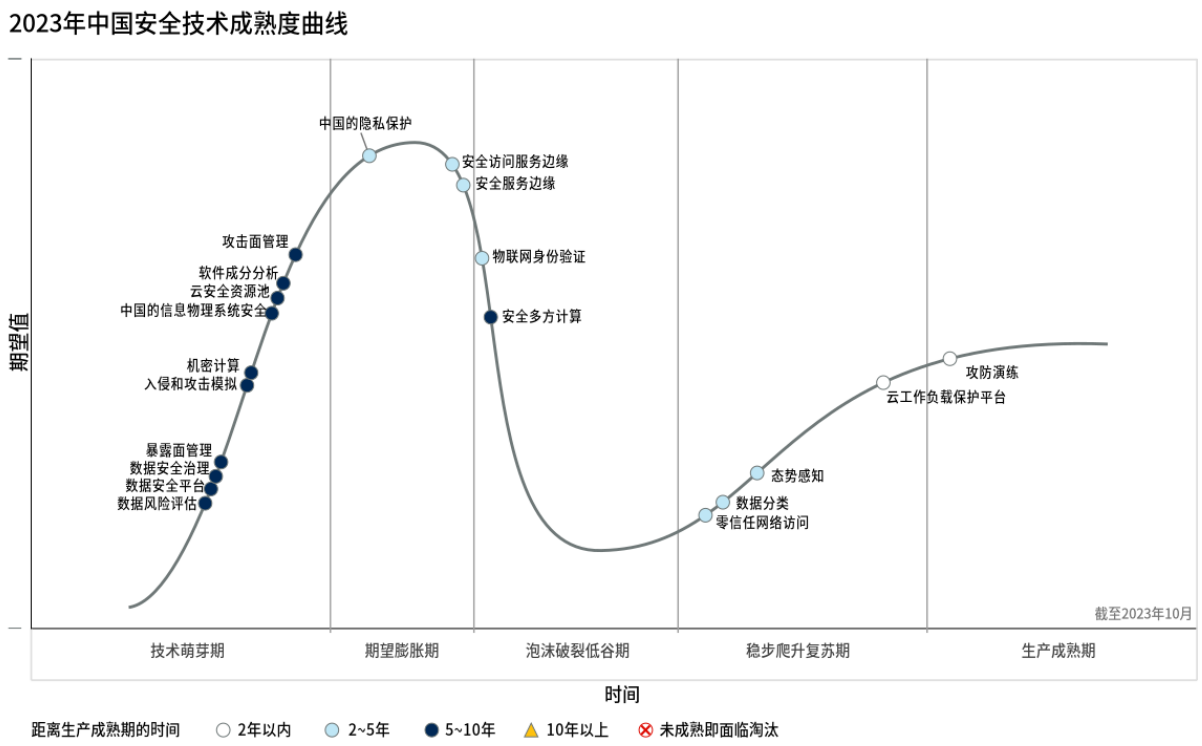
与去年相同的是，多数创新处于技术萌芽期。该阶段新入选的是数据安全治理和暴露面管理。数据安全是企业机构在中国运营的首要安全任务，数据安全平台和数据风险评估处于新兴阶段。随着数字资产数量的不断增加，暴露面管理对于企业机构提高可见性和确保降风险措施的优先级越发重要。

安全和隐私法规是中国的另一个热门话题。《中华人民共和国个人信息保护法》的出台，提高了个人信息保护意识，使隐私保护达到期望膨胀期的顶峰。机密计算在萌芽期逐渐爬升，而安全多方计算仍处于泡沫破裂低谷期，这两项技术均可在数据处理过程中施加保护。中国的国家层面攻防演练推动了攻防演练的发展，使其进入生产成熟期。

与全球市场一样，中国的网络安全平台整合也以多种方式展开，整合的推动力是国内客户预算紧张的现状。数据安全平台在逐步聚合不同的数据保护需求；云安全资源池是为云保护建立的综合平台；安全服务边缘（SSE）和安全访问服务边缘（SASE）整合了多种边缘访问能力，但由于客户兴趣低于预期，其位置已从膨胀期顶端下滑。

随着越来越多的中国客户制定零信任战略，零信任网络访问（ZTNA）的采用率得到提升，已进入稳步爬升复苏期。物联网（IoT）身份认证已从期望膨胀期快速进入泡沫破裂低谷期，预计二至五年即可达到生产成熟期。

图1：2023年中国安全技术成熟度曲线



优先级矩阵

优先级矩阵展示了安全技术和服务在中国的优势，以及实现主流采用的预计时间。表格所列为SRM领导者询问频率高并且对中国企业机构十分有益的技术，涵盖多个安全主题，包括应用安全、云安全、数据安全、网络风险、身份和访问管理，以及安全运营。

攻防演练是本文中唯一处于生产成熟期的技术，其进展得益于国家层面的攻防演练。由于云部署率的提高，云工作负载保护平台将在两年内走向成熟。

尽管客户对数据安全的兴趣度最高，但在相关技术中，只有供应商产品数量和用户采用率都很高的数据分类技术发展到距离生产成熟期二至五年的水平，而文中其他数据安全技术还需要五至十年才能进入生产成熟期，原因在于技术不成熟（安全多方计算、机密计算、数据安全平台），以及用户的数据安全治理和数据风险评估执行滞后。

越来越多的中国客户意识到软件成分分析、暴露面管理以及入侵和攻击模拟的重要性，使这些技术的位置继续爬升。

供需双方对降低复杂性、提高效率的共同需求，造就了网络安全平台的整合趋势。各项技术进一步融合，数据安全平台、SSE、SASE和云安全资源池等平台的采用率持续提高，使客户的安全态势得以改善。

Table 1: 2023年中国安全技术优先级矩阵

影响力	*距离主流采用的时间*			
↓	*2年以内* ↓	*2~5年* ↓	*5~10年* ↓	*10年以上* ↓
颠覆		安全服务边缘 安全访问服务边缘	安全多方计算 数据安全治理 数据风险评估 暴露面管理 软件成分分析	
较高	攻防演练	中国的隐私保护 数据分类 物联网身份验证	中国的信息物理系统安全 入侵和攻击模拟 数据安全平台	
中等	云工作负载保护平台	态势感知 零信任网络访问	云安全资源池 攻击面管理 机密计算	
较低				

来源：Gartner（2023年10月）

被移除的技术

中国的自带身份技术发展成熟，市场渗透率非常高，已从本技术成熟度曲线中移除。社交登录和注册已成为一项成熟的主流技术，提供由中国社交数字消费平台（如微信和支付宝）管理的数字身份。

萌芽期技术

数据安全平台

分析师: Anson Chen

影响力评级: 较高

市场渗透率: 目标受众覆盖率为1%~5%

成熟度: 发展阶段

定义:

数据安全平台（DSP）从数据发现和数据分类着手，整合了针对不同类型、存储孤岛和生态系统数据的保护要求。此类平台通常使用基于策略的授权控制（例如数据库应用编程接口[API]、动态数据脱敏、格式保留加密[FPE]或令牌化）数据保护措施，部分平台还会进行数据活动监控或数据风险评估。

为何重要

传统上，数据安全是通过不同产品实现的，各产品之间缺乏协调，运营效率低下，无法支持数据风险评估、数据和创新商业化，以及涉及数据的协作。数据安全平台可将以往分散的数据安全控制和功能连接到一起，集中部署本地和云数据存储的数据安全策略。

业务影响

数据安全平台能显著提高数据及其多种使用场景的可见性和可控性，例如与数据处理和交换行为相关的数据使用，而不仅仅局限于实现隐私相关的合规目标。因此，企业机构能够切实保护自身数据。可见性和可控性的增强，使个人、企业和政府之间的数据流动变得更安全，推动了 中国数据基础制度（“数据二十条”）的实施。

推动因素

- 进行数据安全治理，是遵守中国 《数据安全法》的重要前提。企业机构需要集成的数据安全平台，以支持数据安全治理的实施，全面了解数据的驻留、流通和使用情况。同时，也要能够更轻松地为所有不同的产品实施一致的安全政策，简化数据风险和合规评估流程。
- 旨在加强数据安全和隐私的各项企业议程，在DevSecOps方法上（例如测试数据管理）的竞争日趋激烈。除此之外，开放数据的规定和由人工智能和机器学习支持的先进分析也是竞争激烈的领域。

- 企业机构数据日益分散在不同服务与信任边界中，甚至经常脱离传统的本地数据中心。数据很可能在各类基于基础设施、平台或软件即服务（SaaS）的私有云、混合云和公有云服务中进行处理和存储。这一现状要求企业机构大幅提升数据安全管理的效率。

- DSP支持对数据产品应用一致的数据安全策略和控制，而“数据产品”是成熟客户最关心的问题。这带来了一种范式转变，其目标是使各种内外部消费者更容易共享和使用数据，提高“安全数据”（带有适当保护的数据）的利用率。

阻碍因素

- 中国大多数终端用户的数据安全平台采用刚刚起步。企业机构只有在发现传统控制措施无法满足需求或同步效果不佳时，才会意识到数据安全平台的意义。然而，以集成平台替代单一功能产品需要强有力的业务论证、持续多年的过渡计划，以及大量精力和成本的投入。

- 大部分数据安全平台可以很好地与同一供应商的安全产品配套使用。如果买方现有的产品组合中大部分是来自不同供应商的多种产品，分散的技术可能很难集成。

- 数据安全平台更偏好结构化数据。许多企业希望对结构化数据和非结构化数据提供同等的保护，然而即便是领先供应商，在支持数据发现、非结构化数据分类和文件级加密方面的进展也十分缓慢。

使用建议

- 为数据安全平台投资进行优先级排序时，应评估各平台对数据安全新项目的支持力度，例如技术实施可否支持数据安全治理、数据网格架构转型和基于云的数据湖转型。

- 优先选择应用范围广的平台，其各项控制之间应有良好的集成性，能够将数据管理、安全策略和后置绑定访问控件集于一体。数据安全平台使用当下流行的后置绑定访问控制，这项加密转换技术可将明文转换为加密或不易识别的格式，例如令牌化和FPE、动态数据脱敏（DDM）以及专有连接器和代理。

- 鉴于数据安全平台的发展尚未成熟，预计很长时间内此类产品的覆盖面无法统一，数据安全问题也无法全部解决。

- 选择能与其他供应商的异构产品高度集成的数据安全平台，例如提供基于互操作性标准的API的产品，以弥补平台覆盖面的不足。

厂商示例

昂楷科技、安恒信息、安华金和、观安信息、山石网科、IBM、绿盟科技、天空卫士、天融信、明朝万达

Gartner相关推荐阅读

2023 Strategic Roadmap for Data Security Platform Adoption

Innovation Insight: Data Security Posture Management

Market Guide for Data Masking

Market Guide for Data Loss Prevention

Use Enterprise Key Management to Provide Stronger Data Security and Privacy

数据风险评估

分析师: Anson Chen

影响力评级: 颠覆

市场渗透率: 目标受众覆盖率为5%~20%

成熟度: 发展阶段

定义:

数据风险评估（DRA）流程用于检查数据安全与隐私控制是否得到有效部署，以及能否满足企业机构在各项安全产品和应用中的风险偏好。这些控制措施旨在降低业务风险，例如违规、侵犯隐私和数据泄露。

为何重要

随着中国数字业务计划的不断扩展，数据安全治理（DSG）方面的监管规定也在不断加强。因此，在对降低业务风险的方式进行评估时，数据风险评估（DRA）成为必不可少的一部分。数据安全、隐私和身份认证管理产品采用的控制措施各不相同，因此会出现不同的DSG政策，而DRA流程会分析多种政策之间的差别和不一致性。要成功实施DSG并确保其符合法律法规和行业规定，DRA流程是基础。

业务影响

DRA为安全和风险管理（SRM）领导者提供了洞察，有助于其根据企业机构的风险偏好确定各类数据风险的优先级。DRA流程可对已实施的数据安全政策进行偏离识别，以及评估财务方面的业务影响，从而为领导者设计风险处置策略提供更多信息。开展DRA流程有助于企业机构满足中国有关数据处理方面的合规要求，以及其他行业规定（金融、电信和汽车等）。

推动因素

- 中国的国家数据经济计划和监管要求，促使公共和私营企业机构在衡量DRA的影响时考虑国家安全和公共利益（如医疗、交通和公共事业），特别是在企业机构的业务活动涉及重要数据、大量个人信息和数据跨境传输的情况下。
- 在业务领导者的支持下，DRA可以解决直接带来业务风险的数据风险，同时识别和评估业务用户的数据访问需求，从而提升业务成果。
- 财务数据风险评估（FinDRA）流程使业务部门能够就数据安全预算做出明智的决策，通过评估风险对业务的财务影响，并根据预算限制确定最佳风险缓解水平及其对业务成果的影响。
- 为降低业务相关数据风险而做出的每个决定，都需要通过DRA明确所有风险的发展路径，同时实施可以识别结构化和非结构化数据，并利用安全、隐私和业务元数据的数据分类流程。
- 使用数据安全态势管理（DSPM）产品创建数据映射并进行DRA分析，可根据某个范围内的数据，评估每个用户或机器帐户所获得的权限。
- 创建数据风险登记表，必须要执行DRA流程，实施以数据为中心的安全架构（DCSA）方法。登记表旨在评估数据安全控制措施之间的差别和不一致性所导致的业务风险。

阻碍因素

- 不同机构和监管部门的合规要求不尽相同，因此DRA流程的风险因子也多种多样，包括全域数据安全风险、数据出境传输风险、隐私风险和技术漏洞。这些风险因素使DRA的实施变得复杂，也增加了人工执行DRA流程的难度。
- 完成DRA流程需要不同领域专家的专业知识，以及对已部署的安全控制进行有效性评估，而这些通常很难获取。
- 数据处理活动随着业务流程的变化而发展。基于固定周期的DRA流程难以迅速、动态地识别时时变化的数据安全风险。
- DRA流程的成功，有赖于业务领导者对数据安全控制需求提供的支持。然而，多数中国企业机构难以调动业务部门充分参与的积极性，也无法通过DSG成功吸引利益相关者。

使用建议

- 采用流程自动化来简化DRA决策判定，同时生成报告模板以满足各种DRA合规要求。
- 通过数据安全平台（DSP）或数据安全态势管理（DSPM）启用DRA流程，使其作为日常数据安全运营的一部分。
- 通过数据安全指导委员会（DSSC），与支持DRA的所有利益相关者合作，将委员会成员在业务成果、业务项目对数据集处理的要求以及业务事件影响等方面的直接了解和洞察应用到实践当中。
- 识别尚未缓解的数据风险——例如数据驻留控制不足、数据活动监控不一致，评估其可能带来的业务风险，并对风险缓解措施进行优先级排序。
- 通过数据安全治理（DSG）框架，向集团企业风险管理（ERM）和DSSC传达DRA的结果，以获得业务端对人员配备和预算变更的支持。

Gartner相关推荐阅读

安全和风险管理领导者指南：中国的数据安全

为中国数据出境安全评估做准备

Innovation Insight: Data Security Posture Management

A Data Risk Assessment Is the Foundation of Data Security Governance

Use the Data Security Governance Framework to Balance Business Needs and Risks

数据安全治理

分析师: Anson Chen

影响力评级: 颠覆

市场渗透率: 目标受众覆盖率为1%~5%

成熟度: 发展阶段

定义:

数据安全治理（DSG）可对由数据安全、隐私与合规问题引起的业务风险进行评估和优先级排序。由于数据需要跨生态系统处理或与合作伙伴共享，数据安全性、数据驻留和隐私方面会产生一些风险，而数据安全治理有助于企业机构建立数据安全策略，以支持业务成果，平衡业务需求与相关风险。

为何重要

本地和多云架构中数据量的激增，导致了一系列安全、隐私与合规方面的业务风险，而数据安全治理能够对这些风险进行评估、排序和缓解。数据安全治理通过适用于整个IT架构的安全策略来实现业务重点和风险控制之间的平衡，让企业专有的数据集可以基于排序后的业务风险在企业机构内外部处理和共享。

业务影响

数据安全治理实现了一种可以平衡数据访问控制和使用的方式，该方式在支持业务绩效目标和客户体验的同时，也进行适当的数据安全保护和隐私控制，降低风险。数据安全治理要求安全、数据和分析（D&A）、合规和业务领导者通过数据安全指导委员会（DSSC）进行协作。这有助于打破沟通障碍，实现业务成果，满足当地法规要求。

推动因素

- 中国于2023年2月公布的数字发展规划，要求中国企业机构在受保护基线之上共享和交易有价值的数据资产，以创造商业数据价值（见 中共中央国务院印发《数字中国建设整体布局规划》）。数据安全治理有必要成为长期持续的流程，用于管理、评估和优先处理与数据使用相关的业务风险，创建可以减轻相关风险的重点数据安全策略。

- 数据安全控制的可持续实施需要安全、数据管理、法务、合规和业务职能部门多个领导者的协作。因此，需要应用一套治理原则、流程和做法来简化协作任务，同时建立明确的职责分工。

- 在数据集组合中实施一致的数据安全策略和控制（例如身份与访问管理[IAM]、访问控制、屏蔽、加密、审计等）颇具挑战性，需要考虑多种内外部要求（涉及隐私性、机密性、完整性、可用性、业务目的和生命周期风险等）。数据安全治理有助于创建数据安全策略，指导和协调实施流程，最大限度地减少数据安全控制中的落差和不一致。

- 市场上没有一种产品能充分降低业务和数据安全风险，因此需要集中创建和协调数据安全策略。

- 为降低数据驻留和数据主权风险，需要通过数据安全治理来进行充分的隐私影响评估（PIA）、数据风险评估（DRA）和数据出境安全评估。

阻碍因素

- 业务领导者在数据管理方面的职责比较分散。安全、数据和分析、合规领导者有各自的任务，但又都很关注数据安全治理的实施。除非各领导者就共同的数据安全治理运营模式达成一致，并且合作制定数据安全策略，否则无法平衡业务成果和减轻风险这两个需求。

- 数据安全、IAM和应用安全产品的部署，由不同的领导者进行采购和管理。每个产品都使用独立的安全控制，毕竟IAM产品并不控制数据访问。数据安全产品通常对非结构化或结构化数据进行操作，并且将控制措施应用于特定平台，因此很难针对异构安全产品部署一致的数据安全策略。

- 在中国实施的数据安全治理，侧重于满足当地监管要求，而不是缓解业务风险和实现业务成果。

使用建议

- 考虑通过数据安全指导委员会与首席信息官（CIO）或风险官沟通，以互联治理的方式来扩展数据安全治理运营模式。这有助于实现最复杂的跨企业、跨地区风险治理计划。
- 确保首席数据和分析官（CDAO）、首席信息安全官（CISO）和数据保护官（DPO）之间的协作，以减少数据管理和安全评估中的重复任务和资源浪费。
- 根据业务风险等级的定义，利用数据安全治理创建和管理跨数据集的统一数据安全策略。
- 考虑利用数据安全平台（DSP）或数据安全态势管理（DSPM）平台自动识别数据安全风险并部署数据安全策略。
- 通过数据安全治理分析特定安全技术变现方式引发的业务风险及其影响，从信息经济学视角评估其对业务成果的财务影响。

Gartner相关推荐阅读

安全和风险管理领导者指南：中国的数据安全

Use the Data Security Governance Framework to Balance Business Needs and Risks

4 Critical Steps to Accelerate the Adoption of Data Security Governance

Use a Data Security Steering Committee to Realize Data Security Governance Objectives

Security Leader's Guide to Data Security

暴露面管理

分析师: Angela Zhao

影响力评级: 颠覆

市场渗透率: 目标受众覆盖率为1%~5%

成熟度: 发展阶段

定义:

暴露面管理涵盖一组流程和技术，使企业能够持续一致地对可见性进行评估，并对企业数字资产的可访问性和漏洞进行验证。有效的持续威胁暴露面管理（CTEM）计划可为暴露面管理提供治理。

为何重要

由于在经济和地缘政治方面具有重要影响，中国已成为网络攻击的主要目标。随着攻击面的迅速扩大，传统的漏洞管理已无法满足需求。有效的暴露面管理能够通过对威胁暴露面进行盘点、优先级排序和验证，来减少中国企业机构所面临的挑战。暴露面管理还可协助中国企业机构遵守敏感数据保护和关键基础设施方面的网络安全法规。

业务影响

现代企业需要对所有使用的系统、应用和订阅服务进行评估，而暴露面管理能够实现企业风险降低工作的治理和优先级排序。此外，暴露面管理还能够：

- 暴露出被利用的可能性（企业机构攻击面的可见性）。
- 盘点并确定优先级（漏洞、基于威胁情报的数字资产）。
- 验证任何攻击的潜在成功率，以及安全控制是否有助于检测或预防攻击。

推动因素

- 中国出台了严格的网络安全法律法规，如《网络安全法》和《信息安全技术关键信息基础设施安全保护要求》，促使企业更加关注风险管理和减少暴露（请参阅《信息安全技术关键信息基础设施安全保护要求》）。
- 在数字化转型过程中，中国企业机构中的应用和云服务数量不断增加，这会导致攻击面不断扩大，环境日益复杂。
- 针对中国企业机构的网络攻击的频率和复杂性不断升级，凸显出管理暴露面以降低风险的紧迫性。
- 通常来说，企业机构的渗透测试、威胁情报管理和漏洞扫描等暴露面管理活动会各自独立执行，这些做法很难或根本无法展示企业机构所面临风险的完整情况。
- 人工智能（AI）、机器学习和自动化等创新技术正在被整合到暴露面管理解决方案中，以提高其有效性并提升中国企业机构对其的兴趣。
- 基于大量的安全验证结果，对暴露面的范围和优先级缺乏限制和判断，使企业机构在暴露面领域有很多需要处理解决的问题，但却缺乏相关指导。
- 企业机构需要一种程式化、可重复的方法来回答“暴露程度如何？”这个问题，从而根据快速变化的IT环境来重新确定任务优先级。

阻碍因素

- 中国企业机构不断变化的IT环境可能会使识别和管理所有潜在风险的复杂性升高，导致暴露面管理范围扩大，产生新的复杂情况和额外的预算。
- 中国的许多企业机构都难以区分基于风险的漏洞管理和暴露面管理，因此仍然以修补漏洞为目标。
- 大多数企业机构几乎都缺乏管理端到端暴露面感知的流程（从潜在攻击向量的可见性到入侵响应），这些企业机构通常只是出于合规性原因对其网络进行扫描和测试。
- 缺乏有效的平台来整合各类工具（如攻击面管理、漏洞评估[VA]以及入侵和攻击模拟[BAS]）中的分散数据，并生成暴露面的整体视图。

使用建议

- 设定切合实际的目标并采用分阶段的方法，重点关注关键业务资产和已知的高风险领域，例如外部攻击面和中国的主要威胁向量。
- 采用覆盖面更广的CTEM计划，以覆盖不可修补的攻击面，而不是简单地利用VA工具处理漏洞。在修复操作中，通过配置管理和软件升级来为修补提供补充。
- 关注可见性。终端用户必须要了解风险所在，并为应对威胁做出计划——即使企业机构无法减少风险暴露。
- 务必在暴露面管理计划中涵盖企业机构间接拥有的资产，例如社交媒体帐户、软件即服务（SaaS）应用和供应链合作伙伴持有的数据。
- 持续整合相关安全工具和/或数据，以简化日常运营流程。

Gartner相关推荐阅读

Implement a Continuous Threat Exposure Management (CTEM) Program

Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

Top Trends in Cybersecurity 2023

入侵和攻击模拟

分析师: Angela Zhao

影响力评级: 较高

市场渗透率: 目标受众覆盖率为1%~5%

成熟度: 发展阶段

定义:

入侵和攻击模拟（BAS）技术可以持续、自动地测试横向移动和数据渗漏等威胁向量，帮助企业机构更好地了解其安全态势的薄弱环节。BAS无法完全取代攻防演练或渗透测试，而是对其进行补充。BAS可以测试企业机构检测各类模拟攻击的能力，从而验证其安全态势。此类模拟攻击可在软件即服务（SaaS）平台、软件代理和虚拟机上实施。

为何重要

BAS技术的主要优势是对企业威胁向量提供持续的自动化评估，使企业机构能够检测出由于配置错误而导致的安全态势问题，或对即将进行的安全投资重新评估排序。BAS还有助于中国的企业机构为构建实战能力明确工作重点，并为强制性安全验证（例如，国家级攻防演练）做准备。

业务影响

BAS允许企业机构对攻击面分析和安全态势管理工具所指示的潜在特定威胁进行影响评估。企业机构可以持续执行这些评估，以更快的频率了解更多资产的情况，比如评估安全控制的有效性、发现对最关键资产的攻击路径，从而确定修复措施的优先级。

推动因素

- 已具备网络安全验证计划的企业机构主要使用BAS技术来确保跨时间和地点的安全态势的一致性，并持续改进。
- BAS工具可以通过API或读取警报日志与预防性安全控制技术集成，赋能安全配置管理并提高防御问题的可见性。
- BAS提供“更安全”的验证，可以在生产环境中运行，但不会影响数据或导致中断。
- BAS可以自动执行企业机构重视的评估举措，以为强制性网络安全验证（例如合规渗透测试、国家级攻防演练等）做好准备，或使红队重新聚焦于更复杂的场景。
- IT和业务利益相关者经常支持BAS技术的部署，因为他们认为这是评估企业机构当前的安全控制能力、配置和事件响应流程的更安全方法。通过对“验证”步骤实现更深层次自动化，BAS还可以为持续威胁暴露面管理（CTEM）提供支持。
- BAS提供可量化和可视化的安全情况概述，说明每项安全控制对安全态势的作用，有助于指导和优化安全投资。

阻碍因素

- BAS的配置、持续维护以及为集成企业机构内部安全堆栈而进行的定制化，都需要投入大量时间。目前，中国只有成熟度较高的企业机构才拥有专门的能力和资源。
- BAS技术还处于成熟初期，相关工具还不为中国企业机构所熟知。因此，要让企业机构优先考虑BAS并阐明在现有的网络安全验证（如渗透测试）之外使用BAS的必要性，将具有挑战性。
- BAS工具需要广泛的内部支持，不仅来自安全团队，还来自其他IT团队，如网络和应用团队。修复BAS工具发现的问题会是一个复杂的过程。
- 随着越来越多的同类工具都增加了攻击模拟功能（例如漏洞管理、攻击面管理和自动渗透测试），BAS技术面临的竞争日益激烈，因此需要扩展和覆盖更多的环境，例如云基础架构和SaaS。

使用建议

- 确定企业机构用例的优先级，专注于简单但常见的使用场景。优先考虑易于部署和维护的BAS解决方案，或可以提供专家服务以支持BAS实施项目的供应商。
- 在做出购买决定之前，了解BAS技术的使用场景、优势和挑战。将BAS集成到网络安全验证路线图中，成为CTEM计划的一部分。
- 确保BAS产品提供的结果是可行的。动员其他IT团队就修复行动计划达成共识。
- 评估BAS供应商持续交付价值的能力，比如定期添加新的功能（如外部攻击面管理[EASM]）、突出显示安全态势的变化，以及以最大程度地减少诊断疲劳的形式提供报告。

厂商示例

360数字安全、矢安科技、北京知其安科技、长亭科技、墨云科技、绿盟科技、华云安

Gartner相关推荐阅读

Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?

Implement a Continuous Threat Exposure Management (CTEM) Program

Top Trends in Cybersecurity 2023

Using Security Testing to Grow and Evolve Your Security Operations

机密计算

分析师: Anson Chen, Feng Gao

影响力评级: 中等

市场渗透率: 目标受众覆盖率为1%~5%

成熟度: 发展阶段

定义:

机密计算是一种在基于硬件的可信执行环境（TEE，也称为enclave）中执行代码的安全机制。该环境将代码和数据与主机系统以及主机系统所有者隔离，并为这些代码和数据提供保护，同时还可提供代码的完整性检查和认证。

为何重要

- 中国的监管要求正在推动企业寻求数据保护。2023年发布的《数字中国建设整体布局规划》鼓励企业机构在保护数据安全的基础上，创造数据的商业价值。
- 机密计算将芯片级TEE与传统密钥管理和加密协议相结合，基础设施提供商无须访问计算设施，即可在不共享数据或知识产权的情况下，为基于合作的项目提供支持。

业务影响

对于受到高度监管的企业和担心第三方在未经授权的情况下访问公有云中的数据的企业机构来说，机密计算可以缓解其对数据安全的担忧。在竞争对手、数据处理者和数据分析师之间数据保密性和隐私控制的基础上，这一技术推进了高级数据分析、商业智能和人工智能（AI）模型训练，而传统加密方法很难做到这一点。

推动因素

- 中国的《数据安全法》和《个人信息保护法》于2021年生效，对数据安全和个人信息保护作出了严格规定，推动了企业机构采用机密计算来保护使用中的数据，尤其是国内外公有云上的数据。
- 全国信息安全标准化技术委员会（TC260）和 中国信息通信研究院（CAITC）已发布了TEE安全规范和技术测试方法。越来越多的商业TEE平台——在2021年之前已有超过15个平台——通过了CAICT评估。
- 中国的企业越来越多地寻求与第三方交换和处理用于分析、商业智能和AI模型训练的数据，以实现数据价值的最大化。这推动了机密计算的采用，以便为数据交换和处理提供安全的计算环境，例如洁净室（clean room）。
- 软硬件解决方案的组合，如隐私增强计算集成平台，正日益受到中国用户的青睐。从隐私增强计算供应商的角度来看，这种组合被认为是既能克服性能问题，又能通过采用机密计算来确保承诺的安全水平的完美解决方案。
- 对竞争的担忧——不仅是个人数据方面，还有知识产权方面——推动了机密计算的增长。对于第三方访问机密性与保护的需求也是推动因素之一。
- 在中国的“十四五”规划中，芯片、生物技术和AI等前沿技术的创新项目数量都出现增长，促使更多本土芯片制造商推出可支持基于x86或TrustZone平台TEE的中央处理器（CPU）和图形处理器（GPU）芯片。这样，受严格监管的企业机构除了可以选择国际厂商（如英特尔、Arm和AMD）的产品之外，也有了本土的TEE硬件选择（如海光、鲲鹏、飞腾和兆芯）。

阻碍因素

- 机密计算会产生潜在的性能影响和额外成本。例如，为了确保现有的软件栈可以在机密计算环境中运行，必须使用专门的开发工具、库或应用编程接口（API）。无论是采用基于英特尔的Software Guard Extensions（Intel SGX）或Trusted Domain Extensions（Intel TDX），还是Arm的TrustZone、机密计算架构（CCA）等方法，基于基础设施即服务（IaaS）的机密计算实例运行成本都更高。
- 不同技术框架的差异性，以及缺乏训练有素的工作人员和对最佳实施方法的理解，都可能会阻碍采用或削弱部署。
- 机密计算不是一种即插即用的部署，应留给高风险用例使用。根据厂商的不同，可能需要进行大量的部署工作。然而，与传输层安全（TLS）、多因素身份认证（MFA）和客户控制的密钥管理服务等更普通的控制措施相比，该技术对安全的边际改进正在减少。

使用建议

- 利用现有的抽象机制来设计或复制样本应用，并通过enclave将其部署到实例中。对体现了实际生产工作负载中预期的敏感信息类型和数量的数据集，需要进行处理。这样做有助于确定机密计算是否影响应用性能，并可寻找出将负面结果降至最低的方法。
- 利用产品已获得可信第三方（如CAICT）认证的机密计算供应商。
- 根据用例和所需的稳健性，审查可对所用敏感数据提供相似保护的替代方案，例如多方或同态加密。
- 分析机密计算对于多方参与数据共享项目的适用性。这里的各方可能无须对彼此信任，却需要处理（但不访问）敏感数据，以最终使各方都能从所输出的共同成果中获益。在这一场景下，任何一方都不应对TEE进行控制。

厂商示例

阿里巴巴集团、蚂蚁集团、百度、华为、冲量在线、英特尔、腾讯

Gartner相关推荐阅读

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

2022 Strategic Roadmap for Compute Infrastructure

中国的信息物理系统安全

分析师: Angela Zhao

影响力评级: 较高

市场渗透率: 目标受众覆盖率为5%~20%

成熟度: 发展阶段

定义:

信息物理系统（CPS）是一种工程系统，可通过协调传感、计算、控制、联网和分析，与物理环境（包括人）进行互动。在有保障的情况下，CPS可实现安全、实时、可靠的运作，具有韧性，而且适应性强。

为何重要

在“数字经济”和“新基建”项目的推动下，信息物理系统已经成为交通运输、能源、医疗保健和政府事务等部门的关键基础设施和支柱。然而，目前组织环境中既有多年前部署的、缺乏内在安全性的遗留基础设施，也有同样充满漏洞的新设施。当务之急是建立一个系统的安全保护体系，提高信息物理系统的安全性，减少安全风险。

业务影响

运营技术和物联网等信息物理系统，是中国数字经济和“十四五”规划的重要组成部分。信息物理系统安全事件可能会影响公民、组织以及政府的财务、权威、生存和声誉。其涉及范围很广，包括个人隐私和安全受到侵犯，以及关键功能中断或故障，例如交通瘫痪、停电和医疗系统故障。

推动因素

- 近年来，中国相继出台了多项信息物理系统安全相关国家标准，例如《等级保护制度》（等保2.0）、《智慧城市安全体系框架》（GB/T 37971-2019）以及《工业控制系统信息安全防护能力成熟度模型》（GB/T 41400-2022）。这些标准从政府角度强调了信息物理系统安全对于支持关键任务领域的重要性。
- 信息物理系统安全事件的后果，不仅包括以网络安全为中心的数据丢失，还包括运营关闭、环境影响、财产和设备损坏和破坏，甚至包括个人和公共安全风险。
- 中国是发展智慧城市的领先国家之一。大量的智能终端和传感器接入智慧城市综合网络，因此信息物理系统无处不在，成为了恶意攻击的理想对象。
- 人工智能（AI）和物联网（IoT）传感器的部署，涉及大量个人和业务数据，是一个未知的风险领域。因此，希望数据受到妥善保护的公民与合作伙伴会对隐私问题产生担忧，而企业机构需要采用信息物理系统安全解决方案来保护数据，或确保数据处理的安全性。
- 各类信息物理系统和协议的存在，导致访问方式复杂多样。为应对信息泄露、数据窃听、非法劫持和篡改的风险，需要对终端和数据传输接口进行统一、有效的安全管理。

阻碍因素

- 信息物理系统一般由业务部门部署，不会征求安全团队的意见。信息物理系统安全管理资源不足，缺乏整体规划、跨部门协作以及清晰的角色和职责。
- 信息物理系统通常由多层硬件、软件和网络以及不同的协议组成，这使其安全风险的识别和管理比较复杂。
- 中国的许多信息物理系统都是在安全因素成为优先考虑之前设计和部署的，容易受到攻击。升级或替换遗留系统可能既困难又昂贵。许多设备的存储和计算能力不足以支持安全机制。
- 对信息物理系统安全管理的整体认知是网络优先于物理，物理安全有时并没有得到充分重视。
- 虽然政府标准已经到位，但企业机构做安全解决方案评估和比较时，仍缺乏广为接受的标准。

使用建议

- 向业务高管宣贯信息物理系统安全对于数字化业务的重要意义。
- 建立信息物理系统安全治理模式，包括组建由全体利益相关者参与的指导委员会、设置合理的组织架构，以及正式划分角色和职责。
- 通过培养、招聘或采购，补足信息物理系统安全管理专门能力。
- 将安全纳入从开发到部署和持续维护的整个生命周期。对于无法在短期内修复的遗留漏洞，实施访问控制、入侵检测和预防、加密和网络隔离等补偿性控制。
- 评估物理访问漏洞、资产损失和无线网络干扰等物理安全风险，并且部署相应的控制和监控系统。
- 盘点现有的信息物理系统安全解决方案，评估不断增加的解决方案，确定通用场景和行业特定用例。

厂商示例

360数字安全集团、安恒信息、新华三、华为、绿盟科技、奇安信、天防安全、天融信、启明星辰

Gartner相关推荐阅读

CPS Security Governance — Best Practices From the Front Lines

Predicts 2023: Cyber-Physical Systems Security — Beyond Asset Discovery

Tool: Cyber-Physical Systems Protection Platform Rating and Selection

云安全资源池

分析师: Feng Gao

影响力评级: 中等

市场渗透率: 目标受众覆盖率为5%~20%

成熟度: 成型阶段

定义:

云安全资源池是一个基于软件的安全工具资源集合，整合了统一管理和监控、安全编排与自动化，以及合规管理能力，可与供应商生态系统中的各类安全工具相集成，也可纳入第三方安全工具，还能够实现安全资源的按需及灵活使用。

为何重要

在孤岛中工作的传统安全工具交付速度较慢，缺乏可扩展性，并且监控和管理效率低下。随着中国云部署的增加，企业机构需要采用新的方式来交付安全能力。此外，采购不同供应商的安全工具来构建安全能力会增加复杂性和成本。云安全资源池为中国企业机构解决此类挑战提供了简单的综合解决方案。

业务影响

云安全资源池作为一项安全平台解决方案，可帮助企业机构：

- 综合设计企业安全解决方案。
- 降低集成复杂性和风险，因为大多数安全工具都是由同一供应商或企业机构自身的生态系统提供。
- 通过统一的管理和监控以及安全编排和自动化服务，提高效率并减轻安全人员的负担。
- 通过扫描检测出不合规的配置，并且提供中国法规所要求的安全功能，从而降低合规风险。

推动因素

- 在中国，随着云服务（特别是私有云）采用的不断增加，企业机构需要一个简单的平台安全产品来满足其安全需求并保护其云资产安全。
- 云安全资源池顺应了安全厂商整合的趋势，提供了单一厂商安全集成解决方案，可与其他厂商工具开放集成。
- 中国的企业机构缺乏熟练的安全专业人员，因此更加需要简化的安全工具来提供统一的管理和监控以及安全编排和自动化服务，降低集成工作量。
- 在网络安全方面，中国出台了严格的规定，因此安全产品需要帮助客户满足合规要求。云安全资源池可提供满足网络安全等级保护制度（等保）等监管要求的安全能力。
- 本土供应商正在将碎片化的安全产品整合到各类平台中，以实现更高效且有效的增长。

阻碍因素

- 缺乏标准，而且大多数功能来自供应商生态系统。这些因素可能会制约第三方安全工具支持。客户可能会对供应商锁定问题顾虑重重。
- 内外部的部署模式均面临挑战。外部部署可能会面临延迟、吞吐量瓶颈和单点故障等问题，而内部部署需要与云技术密切整合，可能会导致进一步的集成问题。
- 云安全资源池与多种技术的整合较为复杂，因此客户部署和运营的难度很大。
- 集成解决方案涉及捆绑定价，这会导致退订部分服务非常困难。供应商会声称原始价格包含捆绑服务，因此客户可能无法实现资源节约。
- 主要由政府和电信私有云采用，缺乏其他行业或公有云的用例。

使用建议

- 将云安全资源池（单一平台）与集成平台（如安全访问服务边缘[SASE]、云原生应用保护平台[CNAPP]，以及扩展检测和响应[XDR]）进行比较和评估，根据评估结果整合安全功能。
- 在供应商甄选阶段，应首先询问供应商是否支持企业所使用的云技术，以及其产品能否与现有安全工具集成，并且应向所有入围供应商发出征求建议书。
- 对入围产品进行概念验证，确认该产品能否与企业现有的云技术和安全工具相集成。除了评估所需的安全能力之外，还应仔细验证产品的统一监控和管理、可扩展性、自动化和编排能力。
- 评估应用编程接口（API）功能，审查相关标准，并且与特定合作伙伴一道，针对供应商不具备的安全能力开展测试，以避免供应商锁定。
- 针对包括未来撤销某一特定组件或采购更多组件等在内的情况，进行折扣谈判。应留意一眼看上去非常诱人的捆绑折扣，因为此类折扣可能会使企业长期受制于不灵活的消费模式。

厂商示例

安博通、亚信安全、安恒信息、新华三、山石网科、绿盟科技、奇安信、瑞数信息、深信服科技、天融信

Gartner相关推荐阅读

Innovation Insight for Cloud Security Resource Pools in China

软件成分分析

分析师: Angela Zhao

影响力评级: 颠覆

市场渗透率: 目标受众覆盖率为5%~20%

成熟度: 成型阶段

定义:

软件成分分析（SCA）产品是专门的应用安全工具，用于对已知存在安全漏洞的开源软件和第三方组件进行检测，并识别潜在的有害许可授权和供应链风险。作为企业机构安全策略的一项必备要素，SCA的作用是确保软件供应链组件的安全可信，并且有助于安全应用的开发和组装。

为何重要

在数字化时代的中国，开源组件在软件开发中的使用十分普遍。SCA通过识别已知漏洞、确保组件获得所需许可证以及提高对软件供应链的信任等方式，推动开源软件在应用开发中的使用。考虑到开源软件在各类应用中的大量使用以及潜在的重大风险，SCA必不可少。

业务影响

SCA在应用安全方面发挥至关重要的作用，可识别开源软件包和其他工件中的已知漏洞和供应链风险。在开源软件和第三方组件的早期应用阶段解决集成问题，可减少重复评估的需要，从而加快开发进程。许可证评估曾是SCA的主要用例之一；对于法务和采购团队来说，现在这仍是SCA的重要功能。

推动因素

- 随着网络攻击频率和严重程度的增加，中国企业机构对第三方软件组件可能产生漏洞的认知日益加深。企业机构也愈发重视与开源和第三方代码相关的风险，因为此类事件一旦发生，将引发巨大关注。
- 中国的合规要求，例如《信息安全技术 软件供应链安全要求》，规定企业机构需要对软件组件进行全面评估和管理。
- 由于底层组件在企业机构中的广泛使用，高影响漏洞在开源软件中反复出现已变得普遍。为应对这一问题以及一直存在的供应链攻击，需要更好地了解开源软件和商用软件包所带来的风险。
- DevOps实践在中国的采用正在增加，但快速的应用开发可能会导致对安全问题的忽视。安全团队希望使用可以集成到DevOps管道中的SCA工具，通过在开发早期阶段审核代码来帮助平衡敏捷性和安全性。
- 在修复问题时，针对既要应对供应链风险，又要提高开发人员工作效率的新能力要求，企业机构不得不重新考虑其现有SCA工具的适用性。现在，更有效的SCA工具可为首选软件更新提供指导，平衡稳定性、缺陷修复和对现有代码功能的潜在不利影响。为软件物料清单（SBOM）分析和生成提供不同程度的支持，则是另一个快速出现的需求。
- 满足合规性要求以及道德和法律标准是企业机构日益关注的问题，而SCA技术可以帮助确保开发人员满足这些要求。SCA技术有助于减少可能给企业机构带来知识产权风险的不需要或未经批准的代码的可能性。

阻碍因素

- 目前，中国的许多企业机构都是将SCA工具作为软件开发过程之外的一个单独步骤来使用。但是，该环节会造成软件交付速度放缓，因此可能导致SCA检测环节被跳过，从而使潜在安全风险进入到生产环境中。
- 中国企业机构在开发需要快速交付的数字项目的过程中，不同的项目和产品团队可能会使用不同的源代码库。当新的漏洞出现时，很难使用SCA工具快速追溯到各个代码库，导致事件应急响应失败。
- 使用SCA来持续监控应用开发后新发现的开源漏洞，这一做法在中国企业机构中并不常见。
- SCA的使用涉及多个部门，每个部门都有不同的优先事项。这些部门包括安全部门、开发部门、业务部门、法务部门和采购部门。有时，不同部门之间缺乏整体规划和协作。

使用建议

- 将SCA技术作为每个软件安全计划的关键组成部分。选择与开发环境和持续集成/持续交付（CI/CD）管道高度兼容的工具。
- 优先采用具备强大供应链风险管理支持、能够使用和生成SBOM的SCA工具。
- 定期使用SCA工具审核开源软件和第三方组件存储库。每当开源软件和第三方组件的漏洞信息得到披露，就立即检查现有存储库，确定企业机构所使用的软件是否受到影响。
- 在评估解决方案时，与所有利益相关者沟通，并评估工具支持多个用例的能力。为SCA工具开发不同的界面，供不同用户使用。

厂商示例

安天、思客云、安恒信息、鸿渐科技、默安科技、墨云科技、奇安信、腾讯、启明星辰、悬镜安全

Gartner相关推荐阅读

Critical Capabilities for Application Security Testing

Magic Quadrant for Application Security Testing

Tool: Vendor Identification for Application Security Testing Tools in China

攻击面管理

分析师: Angela Zhao

影响力评级: 中等

市场渗透率: 目标受众覆盖率为1%~5%

成熟度: 发展阶段

定义:

通过合理配置人员、流程、技术和服务，攻击面管理（ASM）可持续发现、存储和管理企业内外部可能会带来数字风险的资产。ASM技术能够帮助企业机构克服资产可见性和漏洞管理等长期存在的困难。提高攻击面的可见性，有助于减少可能被恶意威胁者利用的资产暴露。

为何重要

对于多数企业机构来说，中国的数字经济使其数字资产的数量和复杂性陡增。ASM可集中实现其他产品或服务资产信息的可视化，包括数字资产、面向互联网的系统及其相关风险，以所有何潜在的数字风险。同时，ASM技术还可帮助安全分析人员不断识别已知和未知的资产，评估并减少暴露，及时提供威胁预警。

业务影响

ASM使安全团队能够通解数字资产和漏洞、发现攻击者最有可能利用的安全问题以及资源修复优先级，从而改善基本的安全卫生。同时，ASM还有助于安全团队识别攻击路径、实现安全工具覆盖范围的可视化、调整和改进安全控制、增强安全态势以及降低可能影响业务运营或声誉的风险。

推动因素

- 随着网络安全验证（例如国家级攻防演练）需求的不断增加，中国企业机构希望从攻击者的角度了解自身面临的威胁。全面了解企业机构潜在的攻击面和现有的安全漏洞是基础。
- 中国企业机构的资产数据通常较为分散，资产类型也多种多样。简化跨部门的资产管理成为安全团队的首要任务，因此推动了持续、自动化的资产发现流程。
- 云采用、敏捷应用程序开发、混合工作模式以及物联网（IoT）和运营技术（OT）等信息物理系统（CPS）的融合等数字化项目带来了新的风险。
- 不断发展的商业环境和面向公众的数字资产的扩张，将使用场景延伸到企业机构之外，包括数字足迹、品牌保护、帐户接管、数据泄露检测和高价值目标（例如VIP/高管）监控。这些需求加速了ASM产品在中国市场的增长。
- ASM具备全面的可见性，为企业机构制定资产信息使用战略提供了可能性，也为许多网络安全项目奠定了坚实的基础。
- 中国的外部攻击面管理（EASM）和数字风险防护服务（DRPS）市场正在整合，使用户能够在一个解决方案中获得整套集成的功能。这满足了用户构建暴露面管理项目的愿望。

阻碍因素

- 用户对于不断有“一个又一个”工具感到痛苦，网络资产攻击面管理 （CAASM）供应商提供的产品与企业机构现有的资产清单和漏洞管理工具存在重叠功能。
- 中国的ASM解决方案在资产可见性和动态管理能力方面仍处于早期阶段。大多数ASM产品与第三方数据源的集成都有局限性，需要大量的人力来验证不同数据。
- ASM解决方案中的优先级设置规则相对简单，或者不支持定制化设置。同时，风险等级主要由漏洞级别和资产关键性决定，缺乏上下文相关性。
- 许多ASM解决方案专注于企业机构内部的IT环境，但缺乏对云和CPS的可见性。
- 攻击面管理的最终目标是减少暴露。仅依靠ASM产品很难实现，还需要安全专业人员的参与。

使用建议

- 根据网络安全验证结果（例如国家攻防演习），检查现有安全解决方案在攻击面可见性方面的差距。如果需要购买其他新工具，请利用概念验证的机会“先试后买”。
- 检查ASM与企业机构现有工具集成并自动执行交叉验证和重复数据删除的能力。
- 评估解决方案成熟度，对定制化风险模型进行定义，或将ASM输出与其他安全洞察相结合，从而改进风险评估和决策。
- 优先选择了解中国云服务、IoT、OT和IT系统能力的供应商，在云和CPS环境中拥有资产的企业机构尤应如此。
- 评估和构建安全团队的能力，以确保有适当的资源可用于处理已识别的攻击面。与安全工具集成，在有可能被修复的情况下执行响应措施。

厂商示例

360数字安全、华顺信安、长亭科技、默安科技、绿盟科技、奇安信、腾讯、微步在线、斗象科技、华云安

Gartner相关推荐阅读

Innovation Insight for Attack Surface Management

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

Implement a Continuous Threat Exposure Management (CTEM) Program

膨胀期技术

中国的隐私保护

分析师: Bernard Woo, Anson Chen

影响力评级: 较高

市场渗透率: 目标受众覆盖率为5%~20%

成熟度: 成型阶段

定义:

中国的隐私保护主要受《中华人民共和国个人信息保护法》（以下简称个人信息保护法）监管，同时也需要遵守特定行业、跨行业和跨境数据传输的相关法规。虽然个人信息保护法与欧盟《通用数据保护条例》（GDPR）等隐私保护法律存在相似之处，但具体要求有所不同，并且由多个监管机构指导执行。

为何重要

个人信息保护法极大地改变了中国的法律和监管格局。此前，相关领域的主要执法依据是网络安全法和个人信息安全标准的相关规定，而个人信息保护法则针对中国公民的个人数据保护，提供了一个范围更广的框架，还规定了严厉的处罚措施：五千万元以下或者上一年度营业额百分之五以下罚款（以较高者为准）。

业务影响

合规风险以及违法违规的潜在处罚是切实存在的。业务领导者必须在制定市场增长战略时考虑隐私问题，尤其是监管比较严格的、与国家安全相关的行业，例如金融服务机构和在中国拓展市场的跨国企业。

虽然中国的监管框架与其他地区的法律相似，但中国企业在制定隐私战略时仍须谨慎分析和处理复杂的数据本地化、数据授权和跨境传输需求。

推动因素

当前的监管框架正在持续完善，以平衡个人数据处理领域中的创新和社会福祉。2017年以来实施的一系列法律可供参考：

- 2017年——全国人民代表大会通过了《中华人民共和国网络安全法》（斯坦福大学 DigiChina官网提供英文译本），对个人数据处理提出要求。

- 2018年——国家标准化管理委员会发布的《个人信息安全规范》（又称"隐私标准"）和《互联网个人信息安全保护指南》，作为网络安全法的补充。
- 2019年—— 网络安全等级保护制度（等保）2.0生效，对IT系统（包括处理个人数据的IT系统）的安全实践做出了规定。
- 2020年——中华人民共和国国务院颁布了 民法典，明确了自然人的隐私权。
- 2021年—— 《中华人民共和国个人信息保护法》生效（斯坦福大学 DigiChina官网提供英文译本）。
- 2022年——跨境数据传输的相关规定出台（请参阅《数据出境安全评估办法》和 中共中央网络安全和信息化委员会办公室[斯坦福大学DigiChina官网提供英文译本]）。
- 2023年——中国希望组建新的监管机构并在各地设立其分支机构，共同执行中国数据管理的法律法规（请参阅 海南省大数据局公告）。

监管机构已经表现出对违规行为实施处罚的意愿，滴滴全球股份有限公司被处以12亿美元的罚款就证明了这一点。

阻碍因素

- 个人信息保护法规定，企业机构在数据处理流程中需要取得个人授权，同时需要承担举证责任。
- 跨境数据传输相关规定对跨境数据传输进行严格控制，对数据跨境战略管理带来了巨大负担。此外，这些法规适用于消费者和员工的个人数据。
- 将IT安全框架（如等保2.0）纳入监管范围，意味着本地授权机构的评估和认证成为必需。因此，企业机构需要与当地机构开展合作，了解所有适用的法规要求（如跨境数据传输相关法规）并实施合理措施，对快速变化的环境做出应对。
- 可能需要进行大量的额外投资。企业机构需要投资使用一系列新技术，包括IT基础设施、应用架构，以及数据管理解决方案。此外，企业机构也需要设立新的角色和制定新的数据控制措施与政策。

使用建议

- 在企业现有的隐私实践基础上进行扩展，以遵循中国的相关法规要求，在必要的情况下制定新流程。
- 发现、标示和归类处理中的个人数据，为管控数据处理过程和满足本地化要求打好基础。

- 专注于打造隐私用户体验（UX），增强个人信息处理行为透明度，收集和管理用户许可与偏好，满足用户的主体权利要求。
- 梳理和记录个人信息的处理目的，将其融入隐私影响评估（PIA）流程，实现数据处理量的最小化。
- 根据个人信息的敏感程度采取保护控制措施，例如加密、数据脱敏/匿名化，以及访问控制（包含日志记录或监控）。
- 确保整体业务战略符合数据本地化和出境传输要求。

Gartner相关推荐阅读

Still a Moving Target — What to Do With the Chinese Data Security Law

State of Privacy — China

Executive Leaders: Top 10 Questions About Digital Business in China, 2022

安全和风险管理领导者指南：中国的数据安全

安全访问服务边缘

分析师: Evan Zeng, Feng Gao

影响力评级: 颠覆

市场渗透率: 目标受众覆盖率为5%~20%

成熟度: 成型阶段

定义:

安全访问服务边缘（SASE）提供了融合网络和安全即服务能力，例如软件定义广域网（SD-WAN）、安全Web网关（SWG）、云访问安全代理（CASB）、下一代防火墙（NGFW）和零信任网络访问（ZTNA）。除了其海外的使用场景，SASE在中国也可以支持行业云和客户本地访问安全的使用场景。由于中国企业对云平台即服务（PaaS）和软件即服务（SaaS）的采用率低于全球同行，CASB的采用应为建议性的，而非核心能力。

为何重要

SASE是数字业务转型的关键推动因素，采用平台而非单个产品的方式提供网络和安全服务，从而提高可见性、连接性和安全性。在中国，SASE平台通常会绑定一些常用功能，例如对云（公有云和行业云）的低延迟访问和即付即用定价模式，这提升了SASE的重要性。

业务影响

SASE可以：

- 提供统一管理广域网（WAN）和安全的平台，从而大幅简化运营流程、增强网络安全能力。
- 提供涉足中国本地的安全和网络平台，既满足合规要求，又可降低WAN基础设施和安全服务的成本。
- 增强位于数据中心、云和边缘的企业数字资产安全性和治理。

推动因素

- 企业数字业务转型要求在不增加复杂性和重复购买的前提下，安全地连接到分布式托管和基于云的工作负载。
- 中国企业将零信任网络和SD-WAN视为重要能力，两者都是SASE解决方案的核心能力。
- SASE提供即服务型基础设施，缩短客户采购和部署时间。同时，还可以增强安全保护，缩短修复时间，从而为基于云和边缘的资源提供更好的可观测性。
- 数字化劳动力的分散和现代企业常见的动态访问需求在中国普遍存在。SASE为网络安全带来了更完整、更具变革性的方法，比传统解决方案更适合这些场景。

阻碍因素

- 部门孤岛、现有投资、文化变革、安全管理成熟度和技能差距是中国SASE采用的主要障碍。
- 由于公有云在组织和监管方面存在风险，中国企业更青睐本地环境，因此SASE的云交付架构在中国不太适用。
- 在中国，本土的SASE产品通常尚不成熟，因为大多数解决方案仍缺乏完全融合的能力，例如统一管理平台和策略控制。
- 在中国，考虑到安全问题和云安全服务法规，国外的SASE提供商需要花费大量时间探索国内的监管和商业环境，以决定其业务战略以及如何在中国部署SASE解决方案。
- 托管SASE产品是另一种SASE采用方案，在中国仍处于早期阶段，因为对大多数技术提供商而言，这些产品的优先级较低。

使用建议

- 采用SASE产品，整合安全和网络供应商的双重业务效益。
- 与首席信息安全官（CISO）以及安全和网络领导者一起，对现有和新兴供应商的SASE产品和路线图做出评估，以确保采用集成平台方法。
- 避免选用两个以上供应商参与的SASE解决方案，尽可能优先选择单一厂商。对于涉及三家以上供应商的SASE产品，只在产品以托管服务形式提供时予以考虑。
- 更多地考虑可以跨SASE平台服务提供统一管理和运营方法的供应商产品。
- 候选SASE供应商应同时适用于全球和中国的特殊使用场景，例如跨境网络全球SaaS的加速部署。
- 在单一部署中结合机构网点访问和远程访问的需求，确保策略的一致性，并尽可能地减少所需供应商的数量。部署ZTNA来增强或取代传统虚拟专用网络（VPN）。

厂商示例

阿里云、华为、绿盟科技、奇安信、深信服科技、天融信、网宿科技

Gartner相关推荐阅读

Accelerate SASE Adoption by Leveraging the Security Vendor Consolidation Wave

Emerging Tech: Leverage Cloud Connect Infrastructure to Improve Connectivity Experience of Cloud Workloads for SASE Solutions

Market Guide for Single-Vendor SASE

2022 Strategic Roadmap for SASE Convergence

安全服务边缘

分析师: Feng Gao, John Watts

影响力评级: 颠覆

市场渗透率: 目标受众覆盖率为1%~5%

成熟度: 成型阶段

定义:

安全服务边缘（SSE）可对Web、云服务和私有应用访问进行保护，主要功能包括自适应访问控制，以及数据安全性、可见性和可控性；其他功能包括高级威胁防御，以及可接受的使用控制（基于网络和应用编程接口[API]集成而实施）。SSE的主要交付形式为云服务，可能包含本地组件或基于代理的组件。

为何重要

SSE可提高企业机构灵活性，为Web、云服务和远程工作模式的使用提供保护。中国的SSE产品融合了不同安全功能（至少融合了安全Web网关[SWG]和零信任网络访问[ZTNA]），通过额外的软件即服务（SaaS）安全功能来降低复杂性、改善用户体验。此类产品可在本地或云中交付。如果SSE与软件定义广域网（SD-WAN）搭配使用，可形成安全访问服务边缘（SASE）架构。

业务影响

混合办公持续推动着SaaS应用等公有云服务的采用。混合办公模式和公有云服务的采用，仍是大多数Gartner客户的业务推动因素。SSE允许企业机构使用以云为中心的方法在Web、云服务和私有应用访问中实施安全策略，随时随地为员工提供支持。同时，SSE可降低多产品运行管理的复杂性。

推动因素

- 云和混合云在中国日益普及，因此企业机构分布式数字资产的远程访问安全需要得到保障。
- 对于管理员来说，SSE有助于增强用户流量可见性，并且提供了用于流量配置和监控的单一位置。
- SSE允许企业机构在边缘基于身份和上下文进行态势分析。
- SSE可提高数据访问和传输的可见性和可控性，能降低与中国安全法规（如数据出境法规）相关的合规风险。
- 通过供应商整合，企业机构可以降低实施安全策略的难度和成本。
- SSE允许敏感数据检查和恶意软件检查并行，这比单独执行各项检查性能更优越、配置更统一。
- 自适应访问可纳入更多输入信号，并且执行过程更具一致性，不受应用位置或类型的影响。
- 建立SASE架构时，企业机构需要更深层的安全功能，而一些供应商只是将最少的安全功能集成到SD-WAN产品中。

阻碍因素

- 市场随着各项能力的融合而变化，供应商可能在某些能力上很强，而在其他方面很弱，例如可见性和数据安全性。在中国，大多数供应商的SSE功能之间或与SD-WAN供应商之间仍然缺乏整体的紧密集成。
- 中国多数供应商并未提供足够敏感的数据识别和保护来管理业务风险。
- 由于中国SaaS供应商的API有限，SaaS的安全性和集成性不够完善，但可见性和安全性对企业而言是必需的。
- 中国客户倾向于本地部署，因此本地网络基础设施和网络连接能力的影响仍然重要。
- 管理或实施不善的本地设备（SSE网关）会导致攻击面的扩大。
- 多数本地供应商完全专注于中国市场，对全球推广的支持有限。
- 现有供应商的变更成本或合同到期时间，阻碍了企业机构在短期内做出合并产品的决策。

使用建议

- 采用SSE并填补其功能空白，以取代SWG和虚拟专用网络（VPN）等独立安全产品，降低复杂性。
- 除非不符合监管要求，否则应倾向于SSE云交付，因为这种方式的控制功能和用户体验更好。
- 选择具有中国因特网接入点（POP）并在本地处理数据的供应商，避免产生出境数据传输问题。
- 积极参与分支机构转型、SD-WAN和多协议标签交换（MPLS）卸载计划，将基于云的SSE纳入项目规划。

厂商示例

绿盟科技、Palo Alto Networks、奇安信、深信服、网宿科技

Gartner相关推荐阅读

2022 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Adopt Security Service Edge (SSE) to Replace Stand-Alone SWG, CASB and ZTNA Products

低谷期技术

物联网身份验证

分析师: Mia Yu

影响力评级: 较高

市场渗透率: 目标受众覆盖率为5%~20%

成熟度: 成型阶段

定义:

物联网（IoT）身份验证是指某个单一物品（通常是设备）在与设备、应用、云服务或在物联网环境中运作的网关等实体发生互动时，为该物品的身份建立信任的机制。物联网身份验证会考虑到物联网设备的潜在资源限制、所用网络的带宽限制，以及各种物联网实体之间的机制性交互。

为何重要

从汽车到智能家居和智慧楼宇、智能家电市场、工业物联网（IIoT）、运营技术（OT）等，物联网市场呈现出爆炸式增长。这些互联设备能够联通网络和物理世界，但也会引发全新的攻击威胁。完善的IoT安全需要具备强大IoT身份验证能力的IoT设备，从而缓解并最大限度地减少网络攻击及/或其他问题和漏洞。

业务影响

IoT身份验证能够缓解：

- 针对互联设备的攻击，此类攻击可能导致产品或服务中断。
- 针对工业设备的攻击，此类攻击可能会影响运营，并且可能导致安全要求很高的生产区域发生重大事故。

推动因素

- 中国信息通信研究院预测，中国的物联网连接数2025年将达到80亿（请参阅 物联网白皮书[2020年]）。物联网连接数的增加将推动人们对物联网身份验证方法的关注和资金投入，以解决安全问题。
- 对用于物联网身份验证的安全凭证存储和轮替方法，目前有迫切的需求。医疗等公共部门正在为此进行方法定义和设备识别（请参阅 食品药品监管总局发布的《医疗器械网络安全注册技术审查指导原则》）。

- 设备的识别和验证仍然主要是通过证书完成的。北京数字认证股份有限公司、亚洲诚信等中国的公钥基础设施（PKI）供应商，投资并专注于这一领域，利用其PKI能力支持物联网身份验证用例。
- 有助于提供统一方法的全球标准，包括RFC 8628、OAuth 2.0设备授权扩展，以及互联网工程任务组（IETF）下设的ACE工作组。ACE工作组明确了基于OAuth 2.0的身份验证和授权交换应如何针对受限设备进行优化，以便基于受限应用协议（CoAP）、消息队列遥测传输（MQTT）以及其他消息传输协议而使用。
- 中国本土法规和标准推动了企业机构对物联网身份和身份验证的投资，例如网络安全等级保护制度（等保2.0）对可信计算的基本要求，以及对物联网的其他要求。

阻碍因素

- 物联网安全环境比较复杂。由于市场过于分散，要确定合适的人员、流程和技术十分困难。同时，由于设备类型和操作环境的不一致，也很难将其产品化。
- 某些物联网设备受资源或功能的限制，计算能力低且安全存储容量有限，因此某些身份验证方法并非合适的选择。
- 对于通过物联网平台进行身份验证，目前的支持尚不成熟或不完整。IIoT等用例领域的协议彼此无法互操作，而且往往不能与TCP/IP等标准适配，对身份验证形成了持续挑战。此外，大多数IIoT系统都是独立的，自带专有的身份验证方式。

使用建议

- 发现IoT设备和网络并对其进行分类，辨别每种类别的功能和安全要求。利用基于设备和网络的场景信息来获取额外的保证。
- 评估并采用身份验证框架，以支持运行中IoT领域中不同设备类型的身份验证需求。
- 使用可信计算技术（如硬件信任根）来防止对设备和传感器的物理攻击，以及防止外部软件攻击对软件代码进行未经授权的读取、分析和操控。在此情况下，中国的关键信息基础设施运营者（CIIO）在选择可信计算技术和供应商时，应关注中国的密码法。
- 采用融合团队来管理IoT项目及实施中的不同技术和法规要求（请参阅Fusion Teams: A Proven Model for Digital Delivery）。

厂商示例

阿里云、数字认证、派拉软件、奇安信、天方证券、亚洲诚信

Gartner相关推荐阅读

Innovation Insight for Cyber-Physical Systems Protection Platforms

Managing Machine Identities, Secrets, Keys and Certificates

安全多方计算

分析师: Anson Chen

影响力评级: 颠覆

市场渗透率: 目标受众覆盖率为1%~5%

成熟度: 发展阶段

定义:

安全多方计算（SMPC）是一种分布式计算和密码学方法，支持多个实体（例如：应用、个人、企业机构或设备）进行数据运算，同时使各方的数据或加密密钥受到保护。具体来说，SMPC可使多个实体共享洞察，同时保证可识别数据或其他敏感数据对除己方外的其他实体不可见。

为何重要

中国出台的新法规（如《个人信息保护法》和《数据安全法》）和企业机构实现本地业务目标的需求，增加了在数据共享/数据交换与隐私保护之间取得平衡的挑战。长期以来，数据保护主要用于确保静态数据和传输中数据的安全。采用SMPC方法，可以保护使用中数据的安全，支持在不受信任的计算环境中，采用机密的方式处理分析和商业智能中使用的数据。

业务影响

SMPC支持数据的加密分析，使多个实体可以通过专门软件，共享包含了在使用中受保护的数据的洞察；还可实现对业务的安全赋能，使企业机构在披露和交换信息的同时，兼顾解决安全与隐私问题。该技术可用于多种数据分析和基于人工智能（AI）的使用场景，例如信用风险检测、联合营销和客户画像，以及联合医学研究等。

推动因素

- 中国的《个人信息保护法》和《数据安全法》于2021年生效，对数据安全和个人信息保护作出了严格规定，推动了企业机构采用SMPC来保护使用中的数据——尤其是在与不受信任的第三方交换敏感数据时。
- 针对使用中的数据和在数据共享场景中发生的数据盗窃和泄露，传统的静态数据加密无法提供强有力的保护。
- 新型用例，如大数据分析、人工智能或机器学习（ML）模型训练，引发了新的隐私和网络安全问题，由此产生了对使用中的数据进行保护的要求。
- 随着SMPC在金融、医疗卫生和公共部门的概念验证（POC）中获得越来越多成功案例，SMPC的实际应用部署也在不断增多。金融领域的概念验证包括联合风险控制和联合营销；在医疗领域则包括跨机构医学研究；公共部门的案例包括跨机构数据共享、开放政府数据和受监管的数据交易。
- 开源SMPC项目（如CrypTen、OpenCheetah、PySyft、Rosetta和SecretFlow）和可用的行业标准的增多，降低了新供应商的进入门槛，并为未来不同数据源的跨平台集成奠定了基础。

阻碍因素

- SMPC算法对延迟非常敏感。在有些情况下，其性能可能无法满足客户需求或预期。
- 多数SMPC的部署项目，从业务流程到数据和系统，都是为客户量身定制的。高度定制化增加了SMPC的部署工作量和成本，对其广泛采用造成阻碍。
- 与同态加密类似，SMPC也需要使用专门的重新编码工具来执行数据分析工作。缺乏对该技术特性的理解，也阻碍了终端用户对这项技术的使用。
- SMPC产品存在一定的局限性，某些数据类型（如浮点型数据）无法使用，在递归机器学习方面也可能产生一些问题。
- 与现有技术（即基于硬件生成和存储密钥的加密技术）相比，认证机构对SMPC不够熟悉，导致终端客户可能面临潜在的审计问题。

使用建议

- 考虑采用集成了硬件（可信执行环境TEE）和SMPC软件的解决方案，在确保达到承诺的安全性和易用性水平的同时，缓解纯软件SMPC技术的性能问题。
- 与开发人员、架构师和数据分析师合作，建立有关SMPC适用性的宏观立场和未来采用愿景（包括POC）。
- 对用例进行评估，重点关注云环境中的数据保密性和隐私增强（个人）数据分析。
- 研究用于数据和分析用例的安全、专用数据挖掘，包括数据湖安全和区块链安全——例如，钱包保护和基于法定人数的多重签名操作。
- 与SMPC产品在安全性、性能、功能和可用性方面已获得可信第三方认证的厂商接洽。可信第三方包括 中国信息通信研究院（CAICT）、 银行卡检测中心（BCTC）和 中国金融认证中心（CFCA）。

厂商示例

阿里云、蚂蚁集团、亚信科技、百度、翼方健数、华控清交、洞见科技、锘崴科技、腾讯云、微众银行

Gartner相关推荐阅读

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

复苏期技术

零信任网络访问

分析师: Feng Gao, Thomas Lintemuth

影响力评级: 中等

市场渗透率: 目标受众覆盖率为20%~50%

成熟度: 主流采用起步阶段

定义:

Gartner将零信任网络访问（ZTNA）定义为：围绕企业用户以及内部托管应用或应用集，创建基于身份和情境的逻辑访问边界的一类产品和服务。应用处于隐藏状态，并且通过信任代理仅限某一组指定实体的访问，从而将横向移动限制在网络内部。

为何重要

ZTNA通过信任代理，实现用户到应用的动态分段访问。这一技术采用的安全策略，使企业机构能够隐藏专有应用和服务，并要求应用使用最小特权访问模型。在中国，此项技术通过创建个性化的“虚拟边界”来缩小攻击面。该“虚拟边界”不仅涵盖用户、设备和应用，还包含数据。

业务影响

ZTNA从逻辑上将源用户/设备与目标应用分隔开，以减少对网络的完全访问，以及企业机构内部的攻击面。采用这种方法，可以改善用户体验（UX），提升远程访问灵活性，同时通过简化的策略管理来实现动态、细化的用户到应用分段。在中国，ZTNA可取代虚拟专用网络（VPN），在日益严格的安全监管环境中，为远程工作提供更好的安全态势和数据安全保障。

推动因素

- 企业机构内部零信任方式采用的增加，带来了对本地和云应用更精确的访问和会话控制的需要。
- 企业对传统VPN部署进行现代化升级和简化的需求日益增加。这些VPN部署针对连接到数据中心环境的静态用户位置进行优化，而不是面向企业外的应用、服务或数据。
- 中国的数据监管要求，促使企业机构寻求更安全的用户数据访问解决方案，尤其是在混合工作环境中。

- 某些受到高度监管的场景，例如访问中国监管系统，需要使用与外界隔离的网络，而用户并不希望为此单独设立终端。
- 在实施精细化控制之前，一些企业机构需要具备查看应用访问模式的能力。
- 企业机构需要采用安全的方式，将供应商、厂商和承包商等第三方连接到应用，无需通过VPN暴露其整个网络，或者将应用连接到互联网才能访问。

阻碍因素

- 成本：ZTNA的许可证通常按年度授予每个指定用户，价格约为传统VPN的两到三倍。
- 身份与访问管理（IAM）能力较弱：IAM能力较弱的企业机构难以部署ZTNA，最终可能使用另一个VPN，或者长期同时使用ZTNA与VPN。
- 对数据物理位置的担忧：出于对数据安全性的担忧，中国的企业机构并不青睐使用在中国境外运营的基于云服务的信任代理，而仅在本地部署的ZTNA无法充分发挥其高可用性和可快速扩展的优势。
- 缺乏数据丢失防护（DLP）能力：数据安全是中国企业机构最为关心的问题，但多数供应商缺乏DLP能力，数据安全能力非常薄弱，导致客户缺乏采用ZTNA的兴趣。
- 访问策略颗粒度：企业机构必须为用户设定应用访问规则，但很多企业机构对此缺乏了解，导致最终的访问规则要么过于细化，要么颗粒度不够。

使用建议

- 优先选择软件即服务（SaaS）型ZTNA，仅在有监管要求时才采用本地ZTNA。
- 保证中国大陆接入点（POP）的数量，以确保SaaS型ZTNA供应商的冗余度，并避免数据出境。
- 仅在特定用户场景（例如开发或满足监管要求）中才使用设备应用沙箱。
- 评估ZTNA产品时应重点关注DLP，因为多数供应商缺乏DLP功能，尤其针对中国内容的DLP。
- 推动ZTNA供应商的选择与安全服务边缘（SSE）供应商的选择保持一致，以支持混合办公人员和远程分支机构采用统一的安全控制，并确保ZTNA策略与企业机构的零信任策略相协调。使用成果驱动型指标来衡量风险减少程度。

- 要求提供安全远程访问的供应商提供通用ZTNA功能，通过添加物联网（IoT）支持功能来统一本地和场外访问控制策略，以取代传统网络访问控制（NAC）或软件定义网络（SDN）部署。

厂商示例

阿里云、持安科技、缔盟云、苏州云至深、数篷科技、绿盟科技、派拉软件、腾讯云、天融信

Gartner相关推荐阅读

Market Guide for Zero Trust Network Access

How to Select the Right ZTNA Offering

7 Effective Steps for Implementing Zero Trust Network Access

2023 Strategic Roadmap for Zero Trust Security Program Implementation

2022 Strategic Roadmap for SASE Convergence

数据分类

分析师: Anson Chen

影响力评级: 较高

市场渗透率: 目标受众覆盖率为5%~20%

成熟度: 主流采用起步阶段

定义:

数据分类是根据约定的编目方法、分类法或本体论来组织信息资产的过程，包括给数据对象进行标记或打上标签，以提高数据使用和治理的便利度，也包括在数据生命周期中采取控制措施或使用数据编织来激活元数据。通常，数据分类会形成一个大型存储库，内含大量有用的元数据，供决策者使用，以做出知情决策。

为何重要

数据分类有助于在涉及价值、访问、隐私、存储、伦理、质量和留存的数据治理和数据安全项目中，采用有效且高效的方式确定数据优先级。根据 中国的数据监管要求，数据分类应成为安全、数据治理和合规项目中的重要一环，用于帮助企业机构区分数据的敏感度，并提高数据保护控制措施的有效性。

业务影响

数据分类增强了企业机构对数据集的分析能力，使企业机构能够在存储库中构建数据，并对数据资产的使用进行即时控制。各类安全控制措施，例如数据丢失防护（DLP）和数据访问治理（DAG），都可极大受益于数据分类或数据标签。数据分类使企业机构能够更轻松地查找和验证数据，同时避免过度保护和留存，从而经济高效地履行监管合规义务。

推动因素

- 当前的法律和地缘政治局势增加了人们对数据驻留和主权的担忧，尤其是在涉及重要数据和个人信息时。然而，当前这种“出问题后再解决”的安全治理实践十分低效，因此从数据分类入手以简化和自动化这些流程的需求越来越多。
- 数据分类方法日趋成熟，可按类型、所有者、监管要求、敏感度和留存要求进行分类，使企业机构能够将安全、隐私和分析工作的重点放在重要数据集及其分类上。
- 预先定义了行业特定分类（如金融、电信、医疗和政府）的自动化数据分类工具的出现，降低了启动数据分类项目时对业务知识和安全知识的要求。

阻碍因素

- 由于缺乏充分的培训并且依赖于用户自行分类，传统的数据分类计划经常以失败告终。
- 数据分类工作的思路往往是以安全为中心，没有使用业务语言向用户解释分类的目的，导致用户参与度不高。
- 尽管许多供应商提供了自动化数据分类工具，可以更准确地进行数据分类，同时最大限度地减少用户工作量，但分类结果的准确性仍未达到预期，特别是需要对模型进行长期训练的机器学习或人工智能算法。
- 从合规角度来看，如果企业机构所在的行业未受严格监管，或行业监管机构未发布分类标准，那么企业机构可能很难衡量或验证数据分类的效果。

使用建议

- 全面评估企业机构内部数据类型和敏感度，并与业务部门和数据分析团队合作，识别对数据分类至关重要的具体用例，从而确定企业机构范围内的数据分类用例和需要开展的工作。
- 在数据安全治理项目中，将用户自行分类和自动化数据分类相结合，并安排用户培训。
- 分析行业监管机构或国家标准委员会发布的数据分类指南和标准，制定符合监管要求的数据分类方案。
- 优先考虑能够与其他数据安全技术，如匿名化、加密、DLP和数据安全平台（DSP）等更好地集成和互操作的数据分类工具。同时也要考虑其他方面，例如更丰富的内置分类模板和灵活的自定义标签。

厂商示例

安恒信息、观安信息、美创科技、绿盟科技、全知科技、天融信、明朝万达

Gartner相关推荐阅读

Still a Moving Target — What to Do With the Chinese Data Security Law

Building Effective Data Classification and Handling Documents

Case Study: An Active Metadata Augmented Data Classification System to Boost Analytics Efficiency

Improving Unstructured Data Security With Classification

How to Succeed With Data Classification Using Modern Approaches

态势感知

分析师: Angela Zhao

影响力评级: 中等

市场渗透率: 目标受众覆盖率为20%~50%

成熟度: 主流采用起步阶段

定义:

中国的态势感知技术衍生自安全信息和事件管理平台（SIEM），是其现代化与集中化的形态，能够与其他安全工具集成，并收集资产、网络流量、日志、漏洞、用户行为和威胁等数据。态势感知技术通过收集和分析数据，展示企业机构的安全状况，同时预测未来趋势。

为何重要

安全项目有效实施的核心要素之一，是将安全数据进行汇总和标准化处理，并以可视化方式集中展示企业机构的安全状况。态势感知技术可以支持安全运营中心（SOC）对安全事件进行识别、优先级排序和调查。广泛的可见性是SOC在日常安全运营工作中做出决策的基础。

业务影响

态势感知平台可以帮助SOC实时或近乎实时地识别和处理信息，并将企业机构的整体安全态势进行可视化展示。此外，内置的威胁情报和威胁狩猎功能可以帮助SOC预测可能发生的情况并制定有效的保护措施。SOC可以将安全信息统一集中到态势感知平台的单个控制台上，而无须切换登录不同的工具。

推动因素

- 大型企业机构的系统具有扩展性，而且处理的敏感数据价值较高，因此更容易成为网络攻击的目标。 因此，这些企业机构迫切需要将态势感知解决方案作为基础技术应用于SOC中。
- 2023年，中国出台了国家标准 《信息安全技术 网络安全态势感知通用技术要求》，为标准化市场和提升技术成熟度发挥了关键作用。
- 网络安全风险的多样性、可扩展性、复杂性和连续性都在不断演进，而对数字领域的日益依赖大大增加了对态势感知技术的需求，因为可以使用这一技术对潜在网络安全威胁进行风险评估并主动响应。
- 现代化的SOC团队需要一个集中式平台来整合来自不同工具的实时信息，以便有效地协调安全流程并分配资源。

阻碍因素

- 不同的态势感知解决方案可能会有不同的名称、功能和能力，这通常会让用户在购买时难以抉择。
- 有些产品只能提供态势感知技术的部分功能，会使买方更加困惑。
- 要使态势感知解决方案发挥出色的攻击检测能力，需要足够的人员和技能储备，而中国许多企业机构资源短缺，无法支持全天候的监控、分析和事件处理。
- 态势感知技术的效果不仅取决于其自身的功能和配置，还取决于前端遥测数据。目前，当态势感知解决方案需要与其他供应商提供的第三方工具集成时，会产生额外成本。

使用建议

- 定义和规划最能满足企业机构需求的监控目标，并基于这些需求来明确合适的购买标准，例如分析方法、性能、规模和数据留存时间。
- 评估态势感知解决方案是否可以缓解现有技术栈的差距，并要求进行现场演示、案例研究和概念验证。
- 分配专职人员来使用态势感知解决方案进行安全检测和响应，以实现企业机构的目标。或者，也可以将安全服务提供商作为内部团队的延伸，进行共同管理。
- 如果现有的安全技术栈很复杂，请选择支持开放式API和无缝集成的态势感知解决方案。明确与集成工作和成本相关的条款，以最大程度地减少意外费用。

厂商示例

360数字安全、新华三、山石网科、华为、绿盟科技、奇安信、深信服、腾讯、天融信、启明星辰

Gartner相关推荐阅读

Magic Quadrant for Security Information and Event Management

Critical Capabilities for Security Information and Event Management

云工作负载保护平台

分析师: Feng Gao, Neil MacDonald

影响力评级: 中等

市场渗透率: 目标受众覆盖率为20%~50%

成熟度: 主流采用成熟阶段

定义:

云工作负载保护平台（CWPP）可以保护混合部署和云部署中的工作负载，并对位于任何地点的物理机、虚拟机、容器和无服务器工作负载提供同等的可见性和统一的控制。CWPP产品融合了多种功能，包括系统完整性保护、应用控制、行为监控、入侵预防，以及恶意软件防护（可选），对工作负载实施保护。

为何重要

中国的企业机构更倾向于使用混合云或私有云，因而对支持公有云、私有云以及本地数据中心的工作负载保护工具的需求水涨船高。单单使用专为本地数据中心或终端用户端点设计的解决方案，无法适应多种多样的工作负载。云工作负载保护平台可维护运行时工作负载的可见性、控制和完整性，而且可与工作负载创建工具链相集成。

业务影响

云服务在中国企业机构的数字化进程中发挥着重要作用。同时，云托管保护也成为一项关键策略，可帮助企业机构满足中国独特的云安全要求，例如私有云和混合云的高度采用。因此，CWPP与终端用户系统存在很大差异，可针对容器、无服务器工作负载以及传统数据中心和基础设施即服务（IaaS）提供统一的云保护。

推动因素

- 中国企业机构云采用率的提升，推动了对不断增加的云工作负载进行保护的需求。此外，由于企业机构大量采用混合云和私有云，因此工作负载保护工具需要能够覆盖公有云、私有云和本地数据中心。
- 云工作负载保护工具需要解决速度、规模和复杂性问题，从而与云工具链相集成。
- 工作负载的跨平台部署越来越多，而且不再只部署于企业机构的传统物理范围内，这就增加了对所有类型和位置工作负载的运行时可见性需求。
- 单单使用专为本地数据中心或终端用户端点保护设计的解决方案，并不是最优解。因此，许多供应商——包括初创公司和成熟的终端保护平台（EPP）供应商——都明确瞄准了CWPP市场。
- 云服务器工作负载保护策略必须基于坚实的规范操作，包括适当的管理控制、补丁规则和工作负载配置管理，而CWPP工具可以实现这一点。

- 工作负载不再是远程同构的。工具必须保护容器、虚拟机和无服务器工作负载，并且为每个容器提供适度的可见性和安全性。
- 与终端用户端点不同，服务器工作负载通常不会遇到或执行未知的任意代码，因此适合于默认拒绝、基于零信任的保护策略，而经过精心设计的CWPP正是为了支持该策略。
- 对Gartner客户而言，供应商融合仍然十分重要。因此，将CWPP和云安全态势管理（CSPM）集成到云原生应用保护平台（CNAPP）中，可以整合之前各自孤立的产品，并且创造相同或更大的价值。

阻碍因素

- 在中国，一些CWPP工具只是终端保护工具的改版，并不符合云工作负载保护的要求。
- 由于云工作负载保护技术较为复杂，并且缺乏具备相关技能的员工，因此企业机构很难选出合适的云工作负载保护终端工具，比如终端探测和响应（EDR）或终端保护平台（EPP）。
- 并非所有供应商都会提供全种类的云工作负载保护能力，有些供应商仅提供一种或两种相关能力。
- 有些企业机构正在完善其云保护方法；有些尚未确定其对云原生安全工具集的需求；还有些更愿意继续使用现有的端点工具，尽管其与云部署并不适配。这类企业机构通常仍希望将本地控件和控制模式扩展到云，无论适用性如何。

使用建议

- 避免使用终端用户EDR或EPP解决方案来保护云主机工作负载。
- 选择支持当前及未来平台以及不同工作负载类型的CWPP工具。
- 为不同位置和规模的所有工作负载提供一致的可见性和控制，无论其位置或规模如何。
- 将工作负载扫描及合规工作延伸到DevSecOps中，尤其针对容器和无服务器功能。首选支持容器和无服务器环境的平台。
- 要求CWPP产品能够通过应用编程接口（API）展示所有功能。
- 要求CWPP供应商提供集成的云安全态势管理（CSPM）功能，以识别有风险的配置。

厂商示例

阿里云、亚信安全、长亭科技、山石网科、华为、默安科技、绿盟科技、奇安信、安全狗、腾讯云

Gartner相关推荐阅读

Market Guide for Cloud-Native Application Protection Platforms

How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB

Magic Quadrant for Endpoint Protection Platforms

成熟期技术

攻防演练

分析师: Angela Zhao

影响力评级: 较高

市场渗透率: 目标受众覆盖率高于50%

成熟度: 主流采用成熟阶段

定义:

在攻防演练中，攻击团队（红队）的任务是，利用攻击者可以采用的一切手段对企业机构系统成功实施攻击。这些手段包括网络钓鱼、社会工程、物理渗透、潜伏和突袭。与之相对的防守团队（蓝队）则负责检测并应对来自红队的攻击。

为何重要

为了确保业务的连续性，攻防演练通过有组织的攻击行动尽可能模拟真实的网络攻击，以测试企业机构的实际安全态势和应急响应能力，并弥补技术、人员和流程方面的缺陷。攻防演练作为一种网络安全验证方法，还可以为安全投资的持续优化提供指导。

业务影响

通过攻防演练，中国的企业机构能够：

- 识别企业机构系统和流程中的暴露面，从而实施有针对性的风险缓解策略。
- 测试安全运营中心（SOC）对真实攻击的检测能力，以及所有利益相关者在安全事件发生时可采用的协作模式。
- 培养安全意识文化，并鼓励所有员工积极主动地发现和报告潜在威胁。

推动因素

- 国家级攻防演练是中国许多企业机构需要完成的合规任务。有远见的企业机构并不止步于满足合规要求，而是希望能够对其安全态势进行持续验证。
- 中国的企业机构在逐渐改变以往受合规要求驱动的被动响应模式，向积极对抗攻击的模式发展。如果能够从攻击者的角度来看待威胁，企业机构就能够更主动地发现迫在眉睫的风险，从而推动开展至关重要的修复工作。

- 攻防团队通常会根据每个企业机构的环境和架构实施演练，因此能够有针对性地改善企业机构安全态势。
- 由于攻防演练的持续时间较长，因此获得的结果通常会比其他类型的网络安全验证方式（如渗透测试、入侵和攻击模拟[BAS]）的结果更详尽，并能够从更多角度提供洞察。
- 攻击团队可在规定的窗口期内使用任何方法开展攻击，包括但不限于渗透、漏洞利用、弱口令利用、暴力破解、网络钓鱼和社会工程。采用这种方法，中国的企业机构不仅可以提高SOC的安全意识，还可以提高IT团队和业务部门的安全意识。
- 随着各类工具逐渐涌现，一些活动实现了自动化，攻防团队的效率也因此得以提高。例如，有些工具可以为攻击团队自动收集网络资产和漏洞信息，还有一种审计平台可以记录攻防双方的活动并监控测试的实施情况。

阻碍因素

- 全面的攻防演练需要大量的时间、专业知识和资源支持，因此中国的许多企业机构难以频繁进行测试。
- 一些企业机构没有充分利用这种做法来测试其安全团队的能力，而是采用关闭系统以减少攻击面这种简单而极端的补救措施。
- 因为所有测试场景都是为各个企业机构量身定制的，因此没有普遍适用的方法来衡量攻防演练的有效性和成果。
- 采用临时的第三方服务可增强企业机构SOC攻防演练的人员配置，但却存在数据泄露、系统中断等风险。
- 由人力主导的攻防演练高度依赖于攻防双方专家的能力。但在目前的中国安全市场中，此类人才仍然稀缺，而且内部培养成本高昂。

使用建议

- 将攻防演练纳入企业机构的长期安全框架中，并优先对关键资产和高风险领域进行测试。
- 分析测试结果并从中学习，从而了解企业机构的安全态势概况，并在此基础上，有针对性地实施补救措施。
- 在进行演练之前定义明确的目标和成功指标。从小规模的测试和补救措施着手，展示积极的成果。

- 在聘请第三方服务提供商之前进行概念验证和尽职调查。考虑使用审计平台来管理访问权限并记录所有测试活动。
- 综合使用多种测试方式，例如渗透测试和BAS。人员和预算充足的成熟企业机构，可以考虑投资于现有员工的培训和认证计划。

厂商示例

360数字安全集团、安天、安恒信息、新华三、山石网科、绿盟科技、奇安信、深信服科技、天融信、启明星辰

Gartner相关推荐阅读

Top Practices for Security Operations in China

Using Security Testing to Grow and Evolve Your Security Operations

附录

请参阅上一篇技术成熟度曲线：Hype Cycle for Security in China, 2022。

技术成熟度曲线的各个阶段、影响力评级和成熟度等级

Table 2: 技术成熟度曲线的各个阶段

(Enlarged table in Appendix)

阶段 ↓	定义 ↓
技术萌芽期	某一创新的突破进展、公开展示、产品发布等事件，引起了媒体与行业的极大兴趣。
期望膨胀期	外界对某一创新寄予过高的热情和不切实际的期待。技术领先企业大力宣传的项目多以失败告终，只有一小部分取得成功。在此过程中，会展公司和媒体是仅有的获利者。
泡沫破裂低谷期	创新未能满足人们的过高期待，迅速褪去热度。媒体报道的兴趣逐渐降低，只余下几个令人警醒的故事。
稳步爬升复苏期	有针对性的试验和扎实的工作，使人们真正了解到一项创新的适用性、风险点和影响力。商业化的现成方法和工具，使开发流程得到简化。
生产成熟期	某一创新的现实影响得到展示和认可，相关工具和方法不断完善，出现第二代、第三代版本，效果日趋稳定，风险亦逐渐降低，因此接受度也得到提高，开启了采用率快速增长的新阶段。大约20%的目标受众在此阶段已采用或开始采用相关技术。
距离主流采用的时间	一项创新进入生产成熟期所需的时间。

来源：Gartner（2023年10月）

Table 3: 影响力评级

影响力评级 ↓	*定义* ↓
颠覆	催生出跨行业开展业务的新方式，可引发行业重大转变。
较高	催生出执行横向或纵向流程的新方法，可为企业显著增加营收或大幅降低成本。
中等	逐步改进现有流程，可为企业增加营收或降低成本。
较低	小幅改进部分流程（例如提升用户体验），难以真正增加营收或降低成本。

来源：Gartner（2023年10月）

Table 4: 成熟度等级

成熟度等级 ↓	*状态* ↓	*产品/厂商* ↓
孵化阶段	实验室阶段	无
发展阶段	商业化阶段 行业领军企业进行试点和部署	第一代 价格高昂 高度定制化
成型阶段	*技术能力和流程理解趋向成熟* 运用范围扩大，不再局限于早期采用者	第二代 轻度定制化
主流采用起步阶段	技术得到验证 厂商和技术快速发展，采用率快速提高	第三代 开箱即用方法增多
主流采用成熟阶段	技术稳定可靠 厂商和技术鲜有变化	数家厂商占据主导地位
延续阶段	不适用于开发新项目 替换受到迁移成本制约	维护营收成为重点
淘汰阶段	极少使用	仅在二手/转售市场可见

来源：Gartner（2023年10月）

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Top Cybersecurity Trends in China for 2024 and Beyond

Table 1: 2023年中国安全技术优先级矩阵

影响力 ↓	*距离主流采用的时间*			
	2年以内 ↓	***2~5年*** ↓	***5~10年*** ↓	***10年以上*** ↓
颠覆		安全服务边缘 安全访问服务边缘	安全多方计算 数据安全治理 数据风险评估 暴露面管理 软件成分分析	
较高	攻防演练	中国的隐私保护 数据分类 物联网身份验证	中国的信息物理系统安全 入侵和攻击模拟 数据安全平台	
中等	云工作负载保护平台	态势感知 零信任网络访问	云安全资源池 攻击面管理 机密计算	
较低				

来源：Gartner（2023年10月）

Table 2: 技术成熟度曲线的各个阶段

阶段 ↓	*定义* ↓
技术萌芽期	某一创新的突破进展、公开展示、产品发布等事件，引起了媒体与行业的极大兴趣。
期望膨胀期	外界对某一创新寄予过高的热情和不切实际的期待。技术领先企业大力宣传的项目多以失败告终，只有一小部分取得成功。在此过程中，会展公司和媒体是仅有的获利者。
泡沫破裂低谷期	创新未能满足人们的过高期待，迅速褪去热度。媒体报道的兴趣逐渐降低，只余下几个令人警醒的故事。
稳步爬升复苏期	有针对性的试验和扎实的工作，使人们真正了解到一项创新的适用性、风险点和影响力。商业化的现成方法和工具，使开发流程得到简化。
生产成熟期	某一创新的现实影响得到展示和认可，相关工具和方法不断完善，出现第二代、第三代版本，效果日趋稳定，风险亦逐渐降低，因此接受度也得到提高，开启了采用率快速增长的新阶段。大约20%的目标受众在此阶段已采用或开始采用相关技术。
距离主流采用的时间	一项创新进入生产成熟期所需的时间。

来源：Gartner（2023年10月）

Table 3: 影响力评级

影响力评级 ↓	*定义* ↓
颠覆	催生出跨行业开展业务的新方式，可引发行业重大转变。
较高	催生出执行横向或纵向流程的新方法，可为企业显著增加营收或大幅降低成本。
中等	逐步改进现有流程，可为企业增加营收或降低成本。
较低	小幅改进部分流程（例如提升用户体验），难以真正增加营收或降低成本。

来源：Gartner（2023年10月）

Table 4: 成熟度等级

成熟度等级 ↓	*状态* ↓	*产品/厂商* ↓
孵化阶段	实验室阶段	无
发展阶段	商业化阶段 行业领军企业进行试点和部署	第一代 价格高昂 高度定制化
成型阶段	*技术能力和流程理解趋向成熟* 运用范围扩大，不再局限于早期采用者	第二代 轻度定制化
主流采用起步阶段	技术得到验证 厂商和技术快速发展，采用率快速提高	第三代 开箱即用方法增多
主流采用成熟阶段	技术稳定可靠 厂商和技术鲜有变化	数家厂商占据主导地位
延续阶段	不适用于开发新项目 替换受到迁移成本制约	维护营收成为重点
淘汰阶段	极少使用	仅在二手/转售市场可见

来源：Gartner（2023年10月）