2022年中国安全技术成熟度曲线

Published 9 November 2022 - ID G00780794 - 6 min read

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

Initiatives: Identity and Access Management and Fraud Detection

> 中国安全市场的技术成熟度、产品和供应商与国际市场存在差异，国内企业机构很难做出最佳选择。安全和风险管理领导者应参考这篇技术成熟度曲线，从国内视角更好地把握创新趋势、增强安全控制。

分析

企业需要了解什么

国内法规日趋严格，安全的重要性更甚以往，而随着国内数字化转型的推进，尤其是云计算、大数据、人工智能、物联网和电子商务的发展，企业机构数字资产保护已成为安全和风险管理领导者的关键任务。一方面，各类法规的涌现要求国内企业机构迅速采取行动；但另一方面，安全技术人才有限，而一系列新技术又需要采用零信任的部署方式来确保安全，这是传统部署方式无法保障的。另外，很多企业机构过度关注数据的位置，使得安全工具本地部署的比例非常高。这些产品互相捆绑，而且与其在国际市场上的交付方式不同。中国安全和风险管理领导者应参考这篇技术成熟度曲线，从本地视角了解创新趋势，更好地改进安全战略，提高安全控制力。

技术成熟度曲线

这篇报告是全新的中国安全创新领域技术成熟度曲线。中国安全技术与市场，在技术成熟度、产品、供应商等方面与国际市场存在差异，因此本文针对国内特点筛选了一批创新安全技术和服务。

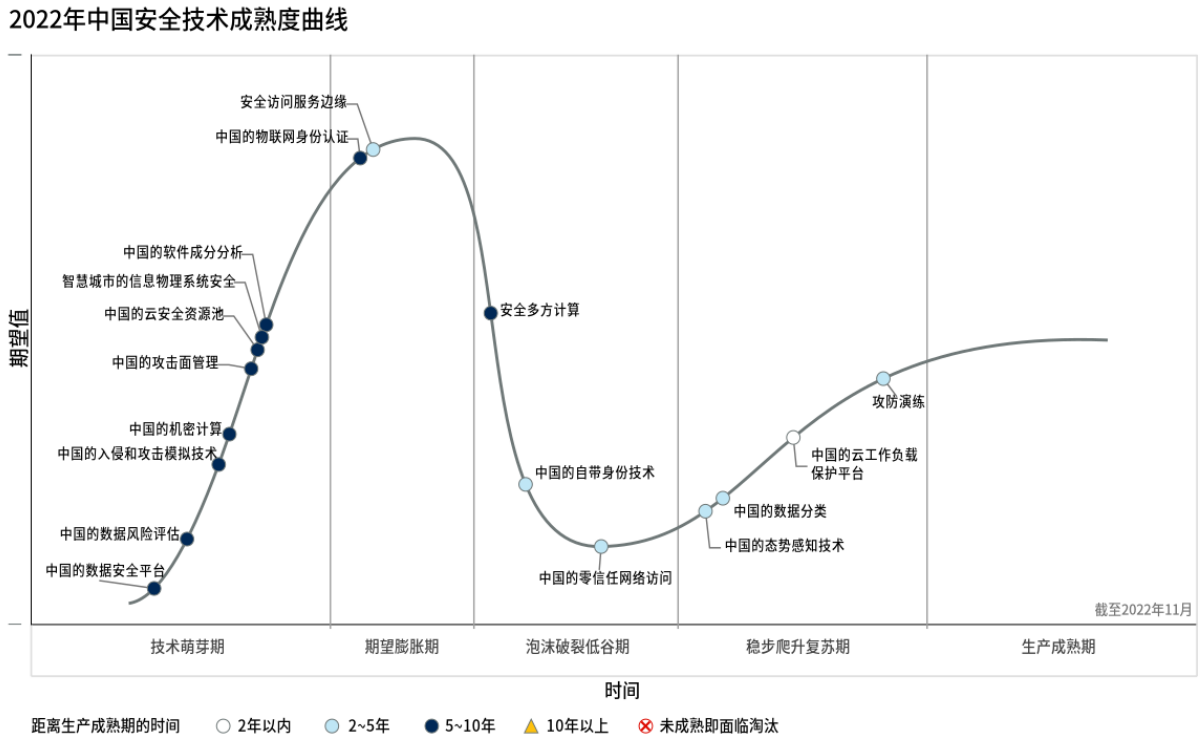
安全访问服务边缘（SASE）和物联网（IoT）身份认证，已进入期望膨胀期。SASE可针对多种边缘访问情景，提供融合型广域网边缘和安全访问能力；物联网身份认证则有助于大量IoT设备与国内各机构建立信任。

《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》的出台，让人们更加关注有关数据安全和隐私的各种新兴技术和方法。部分萌芽期创新针对的即是国内日益增多、日益碎片化的资产管理保护需求，例如智慧城市的信息物理系统（CPS）安全，攻击面管理，以及云安全资源池。

即将滑落到低谷期的一批技术，在经历过热炒后，仍未得到广泛采用。安全多方计算（SMPC）已在中国市场发展多年，但尚未普及，因为其使用场景是高度定制化的。

相对成熟的创新，例如自带身份、攻防演练、零信任网络访问、态势感知、数据分类和云工作负载保护平台等，已在国内普及，出现了多家供应商。由于国内用户基数大，网络巨头也建立了先进的数字生态系统，有大量企业机构在客户身份与访问管理场景中采用了自带身份。中国政府每年组织国家级攻防演练，因此很多国内企业机构需要组织攻防团队，为演练做好准备。

Figure 1: 2022年中国安全技术成熟度曲线



优先级矩阵

优先级矩阵表格，标明了各项安全技术和服务在中国的影响力及其走向成熟所需的时间。在这篇全新的技术成熟度曲线中，各项入选创新技术和服务均能为国内企业机构带来积极影响，而且是安全和风险管理领导者在问询中最关心的内容，相关安全话题包括：应用安全、云安全、数据安全、身份与访问管理，以及安全运营。

由于国内的云技术采用趋势发展正盛，云工作负载保护平台有望在未来两年内走向成熟并迅速扩大采用面，但多数其他技术需要2~5年或5~10年才能发展成熟。推动攻防演练和数据分类发展的，是国内的法规要求；而推动SASE、零信任网络访问等方面发展的，则是疫情期间的远程办公需求。各类影响因素会加快相关技术的成熟，例如国内的数字化转型在快速推进，需要一些技术来保护日益增多的数据和设备。

与全球市场相似的一点是，技术融合与组合也推高了SASE、数据安全等平台在中国的采用率，此类平台可代替单点产品，更好地完成任务。国内独特的安全产品，例如态势感知和云安全资源池，采用率也在提高。

Table 1: 2022年中国安全技术优先级矩阵

(Enlarged table in Appendix)

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		中国的自带身份技术 安全访问服务边缘	中国的数据风险评估 中国的软件成分分析 安全多方计算	
较高		中国的数据分类 攻防演练	中国的入侵和攻击模拟技术 中国的数据安全平台 中国的物联网身份认证 智慧城市的信息物理系统安全	
中等	中国的云工作负载保护平台	中国的态势感知技术 中国的零信任网络访问	中国的云安全资源池 中国的攻击面管理 中国的机密计算	
较低				

来源：Gartner（2022年10月）

萌芽期技术

中国的数据安全平台

分析师: Anson Chen

影响力评级: 较高

市场渗透率: 目标受众覆盖率低于1%

成熟度: 发展阶段

定义:

数据安全平台（DSP）以数据发现和数据分类为起点，整合了针对不同类型、存储孤岛和生态系统的数据保护要求。DSP通过使用后置绑定的访问控制——如数据脱敏、格式保留加密（FPE）或令牌化——来实现数据保护。成熟的DSP还可以进行数据活动监测或数据风险评估。

为何重要

传统上，数据安全是通过截然不同的产品来实现的，运行效率较低，无法支持数据风险评估、开放数据、商务数据，以及涉及数据的内部创新与协作等需求。DSP支持本地和云端的数据存储，也可以将原本分散的数据安全控制与功能连接起来，降低集成成本，减少人工任务与损耗。

业务影响

DSP增加了数据的可见性和使用范围，也改进了数据控制方式，例如未知行为。它不仅可以让企业的目标更具有针对性——如专注于隐私相关的合规，而且可以让企业机构充分保护自身数据安全。同时，数据可见性和控制力的提升，实现了数据在个人、企业机构和政府之间的安全流动。DSP可帮助企业机构做出更明智的决策，为自身业务和社会创造更好的成果。

推动因素

- 从遵守中国数据安全和隐私相关法律法规的角度来看，数据安全治理（DSG）是保证合规的关键部分。企业机构需要一个集成平台来全面了解数据的驻留、流通和使用情况，也要能够更轻松地为所有不同的产品实施一致的安全策略，简化数据风险和合规评估流程。
- 围绕DevSecOps方法、旨在加强数据安全和隐私的各个企业议程，相互竞争日趋激烈。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。

- 企业机构数据越来越多地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。数据很可能会通过基于基础设施、平台或软件即服务（SaaS）的各类公有云服务进行处理和存储。这一现状要求企业机构大幅提升数据安全管理的效率。

阻碍因素

- DSP技术对于中国大多数最终用户来说，仍处于初级阶段。企业机构只有在发现传统控制无法满足需求或不能很好地同步时，才会意识到DSP的意义。然而，用集成平台替代单一功能产品需要强有力的业务论证、长年的过渡计划以及大量精力和成本的投入。
- 大多数DSP可以很好地与同一供应商原产的安全产品进行协同。如果买方现有的产品组合主要来自其他供应商的异构产品，则实施起来会有困难。
- DSP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，即便是领先的DSP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也进展缓慢。

使用建议

- 为DSP投资设置优先级排序时，应评估DSP对新的数据安全项目的支持程度，例如技术实施可否支持DSG、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DSP，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。DSP使用了当下流行的后置绑定访问控制。这是一项加密转换技术，可将明文转换为加密或不易识别的格式，例如令牌化和格式保留加密（FPE）、动态数据脱敏（DDM）以及专有连接器和代理。
- 鉴于DSP的发展尚未成熟，预计在很长一段时间之内，DSP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DSP产品，例如一组基于互操作性标准的API，有助于弥合DSP覆盖面之间的差距。

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、天融信、明朝万达

Gartner相关推荐阅读

Innovation Insight for Data Security Platforms

2022 Strategic Roadmap for Data Security Platform Convergence

Predicts 2022: Consolidated Security Platforms Are the Future

Quick Answer: How Do Other Organizations Deploy Data and Analytics Security Governance in the Cloud?

Develop an Enterprisewide Encryption Key Management Strategy or Lose the Data

Market Guide for Data Masking

Market Guide for Data Loss Prevention

中国的数据风险评估

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1%~5%

成熟度: 发展阶段

定义:

数据风险评估（DRA）流程，目的是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。该流程旨在降低业务风险，减少不合规、隐私侵权和数据泄漏等问题。

为何重要

随着中国数字业务的不断扩展，数据安全治理（DSG）方面的监管规定也在不断加强。因此，在有关降低业务风险水平的评估中，数据风险评估成为必不可少的一部分。数据安全、隐私保护和身份认证管理产品应用不同的控制措施，因此会出现不同的DSG策略，而DRA流程会分析多种策略之间的差别和不一致性。DRA流程是成功实施DSG并确保其符合法律法规和行业规定的基础。

业务影响

DRA流程为安全和风险管理（SRM）领导者提供了洞察，有助于其根据企业机构的风险偏好完成数据风险排序。DRA流程可识别出已实施的数据安全策略是否出现偏离，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的合规要求，包括数据处理相关的法律以及（金融、电信和汽车等）行业规定。

推动因素

- 中国的法律和监管要求，促使企业机构在衡量数据风险评估的影响时考虑国家安全和公共利益，特别是在企业机构所处理的数据涉及重要数据、大量个人信息和跨境传输的情况下。
- 当务之急，是增加业务领导者对DRA流程的支持。为降低业务风险、优化业务成果，各企业机构应重点关注数据风险，从而识别和评估业务用户的数据访问要求。
- 业务部门需要增加风险优先级排序流程，以确定数据安全预算。财务数据风险评估（FinDRA）流程会根据预算和业务成果影响来评估业务所受到的经济影响，确定风险降低力度。
- 使用数据安全态势管理（DSPM）产品创建数据地图并进行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，必须通过执行DRA流程和实施以数据为中心的安全架构（DCSA）方法。登记表会记录数据安全控制措施之间的漏洞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有差异，因此DRA流程需要考量的风险因素也多种多样，包括全面数据安全风险、数据出境传输风险、隐私风险、数据生命周期管理风险、技术漏洞，等等。在这些风险的影响下，DRA流程实施的复杂性提高了，需要专家人才来完成。
- 数据处理活动随着业务流程的变化而发展。基于特定时点执行的DRA流程，不足以迅速识别并减轻数据安全风险。
- 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，特别是那些可能对各个项目或服务的业务成果产生影响的数据安全控制。
- 在数据流路径中，各产品通常会使用源自特定数据存储的特定控制措施。这就意味着需要对很多既没有集成也无法共享策略执行的产品进行调查，难免会导致控制中的漏洞和不一致性。

使用建议

- 采用流程自动化来简化DRA的监督流程，同时生成报告模板以满足各种DRA合规要求。
- 评估现有的数据安全平台（DSP）供应商在企业当前使用的平台中纳入DRA功能模块的能力。
- 通过DSP启用DRA流程，将其作为日常数据安全运营的一部分。
- 与业务领导者共同支持DRA流程，从中直接获取信息和洞察，清晰把握业务成果、业务项目对数据集处理的要求以及业务事故的影响。
- 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——并评估其可能带来的业务风险。
- 通过DSG框架传达您的发现，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

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

Select the Best Approach for Capturing and Communicating the Value of Cybersecurity

中国的入侵和攻击模拟技术

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）技术通过自动模拟内外部威胁、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可对企业机构检测各类模拟攻击的能力进行测试，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

- 企业机构可利用BAS技术，自动对威胁向量进行统一的评估。
- BAS有助于企业机构发现针对其重要资产的攻击路径，确定实战能力建设的优先任务，并在中国国家级攻防演练的背景下，为企业机构的攻防演练做好准备。
- BAS有助于企业机构评估其检测并阻止模拟攻击的安全控制及能力。

业务影响

利用BAS技术，企业机构能够：

- 验证自身安全态势。
- 审查安全控制的配置和短板。
- 从攻击者的角度发现攻击路径。
- 定量评估现有安全工具的防御效果，从而在真正的攻击发生之前，更好地了解自身安全能力，并且强化防御措施。
- 利用模拟测试，确保测试质量在不同时间和地点的可控性和一致性。

推动因素

中国的安全和风险管理（SRM）领导者应在采购BAS技术时对其进行深入了解，因为该技术：

- 有助于确保在不同时间和地点保持安全态势的一致性。
- 在生产环境中运行，不会对数据或业务造成影响。BAS测试仍然需要审批，但启动较快，因此能够更直接地了解当前的安全管控情况。
- 能够可视化展示所有潜在攻击路径，是渗透测试和攻防演练的有效补充。渗透测试通常聚焦于一个特定目标，而攻防演练更关注整个环境中更复杂的场景。
- 有助于企业机构在现有的渗透测试和攻防演练的基础上，更频繁地开展安全评估，并且进一步评估即将进行的安全投资的优先级。
- 能够在中国国家级攻防演练之前，帮助企业机构发现威胁和攻击路径，从而为攻防演练做更充分的准备。

阻碍因素

- 目前，多数BAS技术是依靠代理来运行测试的。企业机构希望该技术能够轻松适应环境和拓扑变化来执行测试并上报问题。因此，BAS解决方案须克服部署和维护方面的挑战。
- 中国企业机构已经采用了太多来自监管机构、审计、漏洞管理、应用安全测试和渗透测试的安全检测方法。BAS工具不应仅仅作为又一种诊断方法，而应为现有的安全评估提供方向性指导和补充。
- BAS解决方案还处于成熟初期，因此还不为中国企业机构所熟知。此外，向企业利益相关者解释BAS与渗透测试之间的细微差别也并非易事。
- BAS无法检测到利用业务流程漏洞而实施的威胁和攻击，而渗透测试则在该领域具有一定优势。

使用建议

- 对企业机构的安全用例进行优先级排序，并且评估BAS解决方案的能力。BAS技术需根据企业机构的环境变化，定期增添并调整新能力，从而提供更多价值。
- 与合规团队和审计人员合作，判断BAS技术是否可用于验证现有安全控制措施的有效性。判断的结果可用于其他诊断方法。
- 确保业务、安全运营中心（SOC）分析人员以及渗透测试人员等所有利益相关者，对BAS技术的特性和收益达成一致意见，以避免内部阻力和误解。
- BAS技术并不是万能的，不能代替所有手动工作或其他类型的安全测试，企业机构仍然需要安全专家根据自身环境配置攻击模拟，以及执行其他类型的验证。与依赖单一方法相比，将BAS技术与更有深度和复杂性的人工渗透测试相结合，可提供更多价值。

厂商示例

360数字安全集团、墨云科技、华云安、悬镜安全

Gartner相关推荐阅读

Implement a Continuous Threat Exposure Management (CTEM) Program

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

Using Security Testing to Grow and Evolve Your Security Operation

中国的机密计算

分析师: Feng Gao, Anson Chen

影响力评级: 中等

市场渗透率: 目标受众覆盖率低于1%

成熟度: 发展阶段

定义:

机密计算是在基于硬件的可信执行环境（TEE，也被称作Enclave）中执行代码的安全机制。这些Enclave将代码和数据与主机系统及主机系统所有者隔离，保护代码和数据的安全，同时确保代码完整性并进行证明。

为何重要

- 中国于2020年将数据定义为一种生产要素，希望通过数据交换和处理的方法来激活数据价值。《数据安全法》和《个人信息保护法》在中国的实施也促使企业寻求数据保护。
- 机密计算将芯片级TEE与传统密钥管理与加密协议相结合，以实现不可读取的计算，支持多个项目在无需数据或IP共享的情况下实现重要的合作。

业务影响

机密计算可以解决公有云数据使用中未经授权的第三方数据访问问题，这是被严格监管的企业对于云采用的一个重要顾虑。利用机密计算，竞争企业、数据处理人员和数据分析者可利用传统密码学无法实现的方式，从硬件层面上加强使用中数据的保护。将机密计算应用于物联网（IoT）/边缘服务器或节点，可保护更靠近数据源的数据和企业应用。

推动因素

- 中国的《数据安全法》和《个人信息保护法》已于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的安全规范和技术测试方法。通过CAITC评估的商业化TEE平台逐渐增加（2021年之前已超过15个平台）。
- 在商业智能（BI）和分析方面，中国企业越来越多地寻求通过第三方进行数据交换和处理，从而实现数据的最大价值。这就推动了机密计算的采用，以便为数据交换和处理营造安全的计算环境（如数据净室）。
- 中国的用户越来越青睐于软硬件结合的解决方案（隐私保护计算集成平台）。隐私增强计算（PEC）供应商将此类解决方案视为解决性能问题的良方，同时通过采用机密计算来确保达到承诺的安全水平。
- 对于个人数据和知识产权等竞争性问题的顾虑，也推动了机密计算的采用。对于第三方访问机密性与保护的需求也是推动因素之一。
- 中国的"十四五"规划（2021年至2025年）鼓励本土企业在前沿技术（如芯片、生物技术和AI）方面进行自主创新。因此，越来越多的本土芯片制造商推出了支持以X86或TrustZone平台为基础的TEE的CPU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、飞腾和兆信）。

阻碍因素

- 技术的复杂性，以及缺少训练有素的员工和对最佳实施方式的理解，都可能不利于这项技术的采用并/或削弱其部署（如，密钥管理/处理方式不当，或者侧信道漏洞未解决）。
- 建立信任很难，但破坏它只需一瞬间，特别是当机密计算这类尚未成熟的技术存在硬件漏洞时。
- 机密计算通常并不是拿来即用的，更适合用于高风险用例。根据所选择的不同供应商，这项技术可能需要较高的投入，但与传输层安全（TLS）、多重认证（MFA）、客户管控的密钥管理服务等普通控制方式相比，其提供较低的安全改进效益。

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。执行数据集处理工作，确定机密计算对应用性能的影响，并尽力将负面影响降至最低。这里的数据集代表企业机构在实际生产工作负载中可能遇到的敏感信息的类型和数量。
- 选择的厂商产品应具备CAITC等可信的第三方认证。
- 根据用例类型和安全性要求，审核能够为使用中的敏感数据提供相似保护的替代产品，例如多方加密或同态加密。
- 分析机密计算对于多方项目的适用性。此类项目中，各方可能缺乏对彼此的信任，但需要处理（但不访问）敏感数据，最终各方都能从所输出的共同成果中获益。在这一场景下，任何一方都不应控制TEE。

厂商示例

阿里云、蚂蚁集团、百度、华为云、冲量在线、腾讯云

Gartner相关推荐阅读

Quick Answer: What Is Confidential Computing?

Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Achieving Data Security Through Privacy-Enhanced Computation Techniques

How to Make Cloud More Secure Than Your Own Data Center

中国的攻击面管理

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:

企业机构的数字资产包括内部资产和外部资产，这些资产均有可能带来数字风险。攻击面管理（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问题。ASM通过合理配置人员、流程、技术和服务，持续实现企业资产的发现、存储和管理。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，中国的数字化转型使其网络资产的数量和复杂性陡增。因此，企业不仅要知道网络资产的存在，也要了解其漏洞和可能被利用的方式。ASM技术可帮助安全运营分析人员不断明确已知和未知的资产，评估并减少暴露，并且提供威胁预警。

业务影响

企业机构可利用ASM技术，从内部管理和外部攻击者的角度，克服资产可见性和漏洞挑战等长期问题。在缓解或修复最有可能被攻击者利用的问题方面，ASM有助于对资源进行优先级排序。此外，ASM可支持安全和风险管理（SRM）团队发现攻击路径，调整并改进安全管控措施，同时强化安全态势和业务韧性。

推动因素

- 在中国每年进行的国家级攻防演练中，首要工作是通过识别、分类和去除不必要的资产，从而减少攻击面。企业机构需要高效的跨部门资产管理流程，尽可能地发现资产并实现流程自动化。
- ASM技术主要分为三类：网络资产攻击面管理（CAASM）、外部攻击面管理（EASM）和数字风险保护服务（DRPS）。每类技术均针对安全团队的具体目标，帮助其在内外部IT资产、第三方资产、“影子IT”系统和数字风险方面，提升可见性、治理和管控。
- 伴随着智能制造、智慧医疗和智慧城市的发展，ASM需要从单纯的IT场景，扩展到各类信息物理资产和新兴技术领域。
- ASM不仅是一种数据平台，也是一种分析和协作资源，有助于对企业机构的资产信息和数字风险进行有效地规范和整合。此外，ASM可帮助安全团队变革工作模式，打破不同资产所有者之间的壁垒，并紧跟数字化转型步伐。
- ASM提供的一系列资产可见性，有助于企业机构针对资产信息作出规划，为众多网络安全项目奠定基础。

阻碍因素

- CAASM和EASM主要提供了内外部资产的可见性，但无法检测安全事件或预防安全风险。这两项技术需要与其他安全工具结合使用，如安全信息和事件管理（SIEM），以及扩展型检测和响应（XDR）。
- ASM与其他安全产品有所重叠，如资产和漏洞管理、入侵和攻击模拟（BAS），以及攻击路径管理（APM）。因此，从长期来看，ASM可能不会成为一个独立市场，而是可能会与其他市场相融合。
- 目前的ASM解决方案可用于IT环境，但并不完全支持信息物理系统（CPS），如物联网（IoT）和运营技术（OT）。
- 企业需要对ASM提供的可见性信息进行进一步解读和关联分析，才能从风险角度出发做出决策，并避免安全威胁。

使用建议

- 在将ASM与现有安全技术集成前，应充分了解ASM的能力。这有助于降低安全团队管理不同平台的复杂性和工作量。
- 在采购新工具前，了解现有安全解决方案在攻击面可见性方面的欠缺之处。
- 根据已确认的用例，选择ASM技术，或利用额外的ASM模块扩展当前安全解决方案。
- 优先选择对IoT、OT和IT系统能力有所了解的厂商，拥有IT资产和信息物理系统的企业机构尤其应如此。
- 评估安全团队的成熟度和能力，确保有充足的资源整合ASM输出的信息与其他安全洞察。这有助于提高安全运营的效果和效率。

厂商示例

华顺信安、零零信安、华云安

Gartner相关推荐阅读

Innovation Insight for Attack Surface Management

Quick Answer: What Is the Difference Between EASM, DRPS and SRS?

中国的云安全资源池

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。云安全资源池可与供应商生态系统中的各类安全工具相集成，并可被纳入第三方安全工具，还可实现安全资源的按需及灵活使用。

为何重要

传统的分散型安全工具交付速度慢、难以扩展，并且监控和管理效果不佳。随着中国云部署的增加，企业机构需要通过新方式来交付安全能力。此外，企业机构还面临一个主要问题，即需要通过采购不同供应商的安全工具来构建安全能力。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。
- 降低集成风险，因为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。
- 通过采用统一管理和监控，以及安全编排与自动化服务，提高效率并减轻安全人员的负担。
- 与中国监管机构要求的安全能力相符。

推动因素

- 在中国，云服务采用正不断增加，特别是私有云，因此企业机构需要一个简单的安全平台产品，以满足安全需求并保护其云资产。
- 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，并可与其他厂商工具开放集成。
- 中国的企业机构中缺乏熟练的安全专业人员，因此更加需要简化安全工具，提供统一管理和监控、安全自动化和编排服务，并减少集成工作。
- 中国对网络安全严格的监管，使得客户需要安全产品帮助他们满足合规要求。云安全资源池可提供满足网络安全等级保护制度（等保）等监管要求所需的安全能力。

阻碍因素

- 针对云安全资源池的标准尚未制定。云安全资源池多数来自供应商生态系统，并且可与其他安全工具开放集成。这些因素可能会制约其对第三方安全工具的支持。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，但由于相关标准缺失，可能会导致进一步的整合问题。
- 云安全资源池与多种技术的整合较为复杂，并且缺乏标准，因此客户实施和运营的难度很大。
- 集成解决方案会伴随着捆绑定价，这会导致退订部分服务非常困难。由于供应商声称其原始价格基于捆绑服务，因此客户可能无法做到资源节约。

使用建议

- 在甄选厂商时，应首先询问其是否支持企业所使用的云技术，以及其产品是否能够与现有安全工具集成，并且应向所有入围厂商发出征求建议书。
- 对入围厂商的产品进行概念验证，确认其产品是否能够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，并且针对供应商不具备的安全能力与特定合作伙伴开展测试，以避免供应商锁定。
- 针对折扣进行谈判，并且商讨未来放弃某一特定组件或采购更多组件时的责任条款。应留意起初看上去非常诱人的捆绑折扣，此类折扣可能会使企业长期受制于缺乏灵活性的消费模式。

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

中国云安全资源池创新洞察

中国云安全最佳实践

中国的软件成分分析

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1%~5%

成熟度: 发展阶段

定义:

软件成分分析（SCA）产品是专门的应用安全工具，用于对已知存在漏洞的开源软件（OSS）和第三方组件进行检测，还可用于识别潜在的许可证和供应链风险。SCA是确保企业机构软件供应链包含安全和可信组件的一种必备要素，为安全应用的开发和组装提供帮助。

为何重要

数字化时代，中国的软件开发通常依赖第三方软件和组件来实现成本节约和快速交付。SCA可帮助确保软件供应链的可靠性，识别已知漏洞，并确保在应用开发过程中使用的各组件已获得所需许可证。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可协助应用开发团队发布更安全的代码，使安全团队能够采取更积极的风险管理。在第三方组件和组件库与应用集成的早期阶段即进行安全评估，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，对于法律和采购团队来说，这仍是SCA的重要功能。

推动因素

- 使用开源软件是 中国《“十四五”软件和信息技术服务业发展规划》中的重要内容，这更加促使企业机构在引入第三方和开源代码时需要注意避免给软件的安全、合规或供应链带来风险。SCA根据从开源社区、私人研究和公开的安全漏洞数据库等来源获得的数据，对企业机构正在使用的代码进行分析，并报告发现的问题。
- 为满足国家网络安全相关法律法规的要求，对于许多中国本土企业机构来说，完全掌控其软件供应链的安全变得至关重要。企业机构希望利用SCA工具，积极预防由于开源组件升级造成的功能改变而导致的破坏性。
- 数十年来，针对商业和开源软件的供应链攻击一直都是令人头痛的问题。为应对这一问题，需要更好地理解开源和商业软件包所带来的风险。在多数情况下，SCA工具都包含对操作风险的评估，以帮助预防供应链攻击，并为软件物料清单（SBOM）分析和生成提供程度不等的支持。
- SCA技术帮助开发人员确保代码的使用符合合规要求以及伦理和法律标准，降低可能给企业机构的知识产权造成风险的错误或不合规代码的出现概率。

阻碍因素

- SCA的部署和使用涉及多个部门，每个部门的优先任务和风险偏好各不相同。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，部门之间缺乏整体规划和协作。
- 多数企业机构使用SCA工具对已投入生产的软件进行检测，或者将检测作为软件开发流程的专门环节。但是，该环节会导致软件交付速度放缓，因此可能导致SCA检测环节被跳过，从而将潜在安全风险带入到生产环境中。
- 在中国的安全产品市场上，并非所有SCA工具都能进行许可证评估；因此，一些企业机构无法应对由于组件问题造成的许可证风险。
- 供应链攻击中可利用的漏洞数量持续增加，却难以找到一个可覆盖所有语言和设备的完整漏洞数据库。

使用建议

- 明确决策、执行和审批各环节的角色和职责。与所有利益相关者沟通，了解企业机构对于SCA工具选型的需求，并确定优先级排序。为SCA工具开发不同的界面，供不同用户使用。
- 选择使用可集成到企业机构的持续集成/持续交付（CI/CD）管道中的SCA工具。在开源软件可供使用之前，主动对其进行评估，以避免给生产环境带来风险，或后续进行替换的麻烦。
- 确保法律专家能够对SCA就许可证问题发出的告警进行分析，解决由于组件的知识产权归属或许可证有效期导致的法律问题。
- 定期使用SCA工具对企业机构的软件和组件清单进行维护，并识别漏洞。每当第三方组件的漏洞信息被披露时，就立即检查现有清单，确定企业机构所使用的软件是否受到影响。

厂商示例

思客云、默安科技、墨云科技、奇安信、鸿渐科技、开源网安、悬镜安全

Gartner相关推荐阅读

Market Guide for Software Composition Analysis

智慧城市的信息物理系统安全

分析师: Angela Zhao, Katell Thielemann

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:

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。智慧城市的CPS安全，用于解决传感器、网络和应用系统的安全问题。这些系统会采集数据，以支持交通运输、建筑、公共事业、环境和公共服务等城市关键基础设施。

为何重要

在"数字经济"与"新基建"举措的推动下，信息物理系统已成为建设交通运输、能源、医疗、政务等智慧城市关键基础设施的重要前提。然而，目前各城市中的基础设施，要么是多年前部署的，缺乏内在安全性；要么虽然是新部署的，但同样充满漏洞。当务之急是要建立一个系统性的安全保护体系，提高信息物理系统的安全性，降低智慧城市的安全风险。

业务影响

智慧城市的CPS安全作为 中国"十四五"规划中国家安全的重要组成部分，对于经济发展和社会稳定具有重要影响。CPS的安全事件不仅会影响到市民，也会涉及市政府的财政、权威和声誉。这些安全事件包括对个人隐私的侵犯（ 《中华人民共和国个人信息保护法》），甚至关键功能的中断或故障，如交通瘫痪、停电、医疗系统故障、人身安全问题等。

推动因素

- 网络安全等级保护制度（等保2.0）和国家标准 GB/T 37971-2019 智慧城市安全体系框架将安全管理的范围从IT系统扩展到了信息物理系统。这些从政府角度提出的CPS安全相关要求和标准，进一步强调了CPS对支持智慧城市关键任务领域的重要性。
- 新加坡和中国等国家在人工智能（AI）和物联网（IoT）传感器技术领域处于领先地位。这些技术涉及大量个人和业务数据，蕴含着未知的风险。因此，希望其数据受到妥善保护的公民和合作伙伴对隐私问题产生了担忧，而企业机构就需要采用CPS安全解决方案来保护数据，或确保数据处理的安全性。
- 随着大量智能终端和传感器与智慧城市综合网络联网，CPS提供的服务无处不在，因此也成为恶意攻击的目标。
- 智慧城市CPS数量的增加提高了接入环境的复杂性和接入方式的多样性。由于终端和数据传输接口缺乏统一有效的管理，因此带来了信息泄露、数据窃听、非法劫持和篡改的风险。
- CPS对智慧城市的稳定至关重要，任何安全事件都会产生严重影响，因此安全事件的及时发现和应对成为智慧城市发展的重要任务。

阻碍因素

- 由于缺乏整体规划和跨部门协作，因此造成各类CPS管理职责孤立且分散，难以快速有效地应对大规模、高强度的紧急事件。
- 智慧城市CPS的不同技术为攻击者提供了各种机会。例如，对于交通控制系统，攻击者可能会篡改或伪造数据；而对于智能电网，分布式拒绝服务（DDoS）是最常见的攻击方式。这增加了安全监测和响应的复杂性。
- CPS安全管理在网络和物理层面上通常是孤立的。网络安全风险通常会受到关注，但降低物理安全风险有时并未获得足够的重视。
- 各企业机构和政府部门收集的部分数据会被集中存储，便于进行进一步的大数据分析和应用开发。汇聚的数据量非常庞大，因此它们具有很高的价值，并且面临数据泄露和被盗的风险。

使用建议

- 构建“纵向贯通、横向连接”的CPS安全体系，包括中心化的安全运营中心（智慧大脑），合理的组织架构，以及明确的决策、执行和监督角色和职责划分。
- 全面识别各类攻击面和威胁，为所有可能的场景制定监测和应急综合规划，以确保及时发现、响应和恢复。
- （尽可能自动化地）发现所有CPS资产，从整体上评估并降低其物理安全与网络安全风险，如违规的物理访问、资产损失、无线网络干扰等。
- 尽量减少个人信息和重要数据的收集、处理和共享，在数据使用、隐私保护和数据安全之间寻求平衡。在数据全生命周期和大数据环境中加强数据保护。

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、天融信、启明星辰

Gartner相关推荐阅读

Product Leaders Insight: Embed Cybersecurity Into Your Vertical Industry Strategies

Quick Answer: What Privacy Concerns Must Executives Prioritize With Regards to Cyber-Physical Systems?

Quick Answer: Security of Cyber-Physical Systems: Who Is In Charge?

膨胀期技术

中国的物联网身份认证

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1%~5%

成熟度: 成型阶段

定义:

物联网（IoT）身份认证是指设备、应用、云服务、网关或在物联网环境中操作的人工用户等实体在与某个单一实体（通常是设备）互动时，为该实体的身份建立信任的机制。物联网身份认证需要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

物联网解决方案，为优化流程或挖掘新的收入来源带来了新机会。工业物联网带来了更高的制造自动化水平，也推动了发展。在中国，互联汽车、智慧城市、智能家居和智能可穿戴设备等市场发展迅速。然而，这些互联互通的设备在联通网络和物理世界的同时，也引发了新的攻击威胁。为了减少网络攻击，物联网设备需要可信的身份和强大的设备认证。

业务影响

物联网身份认证降低了未经授权的物联网设备访问风险。这些风险可能会：

- 导致能效下降或停滞，进而直接影响生产力。
- 在工业物联网环境中对安全要求极高的生产区域里，影响运营或引发潜在的灾难性事件。
- 引起个人数据泄露等隐私问题，进而可能影响品牌声誉及可信度。

推动因素

- 通过构建网络-物理系统（CPS），物联网解决方案正在模糊物理世界和数字世界的边界，改变人类生活和工作的方式。物联网的爆炸式增长正在以前所未有的方式在人与机器之间建立连接。
- 对物联网身份及身份认证的投资受法规和标准的驱动，例如等保2.0对可信计算的基本要求和对物联网的其他要求。

- 无论是政府还是消费者，都将继续对安全提出更高的要求，以防止网络攻击带来的危险、高成本和不便。

- 为了提供统一的方法并巩固投资、保持可靠性和利用率，当前有一些标准，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的身份认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）以及其他消息协议而使用。

阻碍因素

- 物联网的安全环境十分复杂。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，因此某些身份认证方法并不是很好的选择。

- 对于通过物联网平台进行身份认证，目前的支持不成熟或不完整。许多用例领域（如工业物联网）的协议无法进行互操作，而且往往不能与TCP/IP等标准适配，因为现有的这些设备并不是为了连接互联网而设计。这对身份认证方法将会是持续的挑战。此外，大多数工业物联网系统都是独立的，自带专有的身份认证方式。

使用建议

- 为物联网中各个类型的设备编撰目录并让其发挥作用。使用基于设备和网络的场景信息来获取额外的安全保障。

- 评估和采用支持物联网运行的各种设备类型所应用的身份认证框架。

- 企业所筛选的供应商，应有能力克服身份认证的特殊挑战，以及解决设备资源受限或互操作性有问题的物联网设备所面临的身份认证问题。

- 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。中国的关键信息基础设施运营商（CIIO）在选择可信计算技术和供应商时，应注意中国的密码法。

厂商示例

阿里云、杭州映云科技（EMQ）、派拉软件（ParaView）、奇安信、天防安全

Gartner相关推荐阅读

Managing Machine Identities, Secrets, Keys and Certificates

Cross-Industry Insight: IoT Market Opportunities and Top Spend Use Cases

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）提供了多种融合型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）等。中国的SASE为机构网点、远程办公、互联网和云访问安全、低延迟云访问等各类用例提供支持。由于中国的企业机构在平台即服务（PaaS）和软件即服务（SaaS）方面的支出低于全球平均水平，因此在中国市场上，CASB是SASE的可选组件。

为何重要

SASE是数字业务转型的关键驱动性技术，采用平台式而非孤岛式方法来交付服务，提高了服务的可见性、敏捷性、韧性和安全性。在中国，由于市场上缺乏软件定义的云互联服务提供商，因此市场上并不常见采用即付即用定价模式来连接云上资源的低延迟网络，SASE平台就变得十分重要。

业务影响

SASE可提供：

- 在广域网（WAN）和安全访问基础设施上采用单一管理和运营界面的平台方法。
- 可覆盖全国的SASE服务平台提供到云、数据中心和边缘设施的低延迟访问。
- 加强对传统企业数据中心之外的云和边缘资源的安全保护和治理。
- 利用SASE提供商的SD-WAN基础设施来显著减少WAN基础设施成本。

推动因素

- SASE由企业数字业务转型推动，而中国的企业正越来越多地采用分布式数据中心和多云架构，可覆盖全国的SASE平台因此更受青睐，因为可以满足客户安全访问和互联互通要求。
- 由于企业对于身份安全和高昂的WAN基础设施成本的担忧，零信任网络访问和SD-WAN成为中国企业最常提及的两个SASE服务。
- SASE可提供“即服务”基础设施，缩短客户采购和部署所需时间，还可以提高安全保护水平、缩短修复时间，从而大大提升了基于云和边缘的资源的可观测性。
- 为无关联的云平台和基础设施平台提供统一的管理和访问服务，从而减少支付给由多个服务提供商提供的、功能大量重叠的产品的费用。
- 以数据中心外围安全性为基础的网络安全模型，无法应对现代化数字业务以及分散的数字化劳动力的动态需求，迫使传统的数据中心外围转型为一组基于云的融合能力，仅在企业需要时才在合适地点创建，即一个动态创建的、基于规则的安全访问服务边缘。
- 中国政府已针对网络安全、消费者隐私和任务关键型基础设施颁布了多项法律法规，例如“网络安全等级保护制度2.0”（简称“等保2.0”）和《中华人民共和国网络安全法》等。SASE为协助客户更好地遵守这些法律法规提供了一个平台。
- 疫情加速了中国企业机构对于远程办公的采用。企业机构需要融合型边缘保护解决方案，以获得更好的客户体验，使用户能够安全地访问内外部数据资源。

阻碍因素

- 企业机构孤岛，以及现有投资和技能缺口：SASE的全面执行，需要网络安全和网络建设团队协调一致，通力合作。
- 企业机构的偏见和监管要求，促使企业机构继续采用本地部署的形式：一些客户排斥使用云服务，希望维持对数据的掌控。
- 提供商仍需时间来完善其为中国市场提供的SASE套件。例如，多数中国提供商采取共同开发的方式来研发SASE套件，但不同提供商的产品整合仍亟待加强；中国市场上也有厂商独立开发SASE套件，但多数产品未能与控制平面集成，无法提供对各功能组件的统一管理。
- 海外提供商在中国推出其SASE产品仍尚待时日，因为SASE涉及安全和SaaS服务，而在中国提供此类服务需要获得相关证书和许可证。

使用建议

- 邀请首席信息安全官和网络架构师参与评估主导及新兴厂商的产品和路线图，确保集成方法的采用。
- 利用WAN、防火墙、虚拟专用网络（VPN）或SD-WAN来升级网络以及网络安全架构。
- 对于在中国使用的SASE套件的核心服务，选择的提供商尽量不要超过两个，以尽可能减少复杂性并提高性能。
- 对提供商的SASE产品进行审核，确认是否能对SASE套件中的各项服务提供统一管理和运营。目前，中国市场上的单一厂商SASE解决方案数量十分有限。
- 为中国开发SASE用例，从而在进行厂商选择时，能够对核心功能进行优先级排序。
- 在单一部署中结合机构网点和远程访问的需求，确保策略的一致性，并尽可能地减少所需提供商的数量。部署ZTNA来增强或取代传统VPN。
- 在续签合同时，整合WAN和安全服务边缘提供商，以降低复杂性和成本。

厂商示例

阿里巴巴、华为、奇安信、深信服科技、天融信

Gartner相关推荐阅读

Magic Quadrant for WAN Edge Infrastructure

Critical Capabilities for WAN Edge Infrastructure

Overcome the Challenges of Cross-Border Data Communication Over Internet With China

Product Manager Insight: China Presents Growing Opportunities for SASE Providers

低谷期技术

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

中国政府出台了新的数据相关法律法规，如《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》）和《中华人民共和国数据安全法》（以下简称《数据安全法》），而在中国运营的企业机构也需要实现其业务目标；因此，处理个人数据时面临的复杂性增加，需要应对平衡数据安全和隐私保护这一挑战。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。这是一种安全方法新范式，是传统安全策略的增强版。

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。SMPC适用于多种应用场景，如检测信贷风险、联合营销和客户画像、情报共享和联合医学研究等。

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）获得越来越多成功案例，SMPC的实际应用部署也在不断增多：金融领域的联合风控和联合营销；医疗卫生领域的跨机构医学研究；公用部门的跨机构数据共享和开放政府数据。
- 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算法对延迟敏感；在有些情况下，其表现可能达不到客户要求或预期。
- 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。高度定制化增加了采用SMPC的工作量和成本，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。

使用建议

- 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，如云计算等。
- 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、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

Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation

中国的自带身份技术

分析师: Mia Yu

影响力评级: 颠覆

市场渗透率: 目标受众覆盖率高于50%

成熟度: 主流采用起步阶段

定义:

自带身份（BYOI）技术能够帮助用户在使用多种数字业务时，选择并采用第三方数字身份，如社交媒体身份或具有更高保障的身份。

为何重要

腾讯和阿里巴巴等中国互联网巨头拥有庞大的用户群。服务提供商和相关业务方可利用此类外部数字社交身份，而不必要求用户创建用于认证和访问的新身份。数字政务身份的应用不断扩展。例如，在一些城市中，人们可获得数字驾照和数字社保身份，这提高了数字政务和商业服务的可信度。

业务影响

采用BYOI技术的企业机构可获得以下优势：

- 减少用户数字旅程摩擦，用户体验得以提升。
- 在客户注册（包括身份属性共享）时采用具备更高可信度的BYOI，降低或消除身份证明或客户身份审核（KYC）流程的成本。
- 采用高可信度的身份提供商（IdP）开展适当的风险评估和认证，可减少需要更高级别身份保障的新业务模式的实施阻碍。

推动因素

推动BYOI发展的因素包括且不限于：

- IdP投资和允许服务提供商使用IdP的身份和认证服务（例如，微信、支付宝和新浪微博都提供了此类服务）。
- 中国的身份与访问管理（IAM）供应商（如Authing、竹云科技、派拉软件）为第三方IdP提供了全方位支持，尤其是为中国互联网巨头的主要社交身份提供支持。这些社交身份的使用有益于其庞大的用户群，并在企业机构与其终端客户互动方面产生强大的生态系统效应。
- 由于BYOI能够减少消费者和用户在注册和登录时的摩擦（消费者选择一个自带身份与服务提供商开展互动），因此对客户和整个市场产生了吸引力。同时，服务的使用率和品牌忠诚度也得到了提升。用户在持续使用IdP数字身份时，可定期接触到IdP品牌，使其对IdP的忠诚度得以提升。
- 2022年初，中国国务院办公厅发布了相关政策，推进电子证照在获取政府服务方面的应用，增加电子证照的社会化用例（更多信息，参见北京大学法制信息中心网页：国务院办公厅关于加快推进电子证照扩大应用领域和全国互通互认的意见[现行有效]，或 中国政府网相关网页）。

阻碍因素

- 社交身份无法满足很多企业机构对安全和信任标准的要求，受严格监管的行业（如金融）尤其如此。隐私问题仍然存在，许多IdP都能够追踪用户的登录地点。
- 高风险用例缺乏高可信度的身份认证方法。例如，公民使用政府税务服务等高风险用例时，可使用第三方的高可信度身份认证，如网上银行凭证，以减少注册和登录的摩擦。
- 存在潜在风险（服务提供商可能会失去客户可见度，甚至失去对客户关系的管控）。
- 如果社交身份丢失，并且无法恢复账户，就可能会导致用户无法获取利用该社交身份注册的、或与该社交身份相关联的其他数字服务。如果企业机构失去了对社交媒体提供商身份的访问权（如出现毁约或监管限制），就可能会造成使用这些社交身份的客户的流失。

使用建议

- 仔细判断采用传统方法产生的摩擦会对客户体验（CX）乃至客户留存带来的负面影响。
- 利用账户注册和登录等常见的BYOI用例，重点关注减少摩擦。打造良好的客户体验，这有助于抵消品牌稀释和无法掌握客户旅程的风险。
- 确保IdP提供的信任水平与风险水平相匹配，或者IdP能够提供更高的信任水平来弥补差距。
- 提供与多个社交身份提供商的集成，降低单一社交身份访问失败的风险。为失去社交身份访问权的用户构建强有力的账户恢复机制。

厂商示例

阿里巴巴、Authing、竹云科技、派拉软件、新浪、腾讯

Gartner相关推荐阅读

Top Trends in Government for 2022: Digital Identity Ecosystems

中国的零信任网络访问

分析师: Neil MacDonald, Nat Smith, Jie Zhang, Kevin Ji, Feng Gao, Uko Tian

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:

零信任网络访问（ZTNA）可以为应用提供基于身份和情景的逻辑访问边界。应用可以隐藏起来，无法在检索中发现，仅允许部分指定实体通过信任代理访问。信任代理在允许用户访问前，会先验证用户身份、访问情景以及指定人员和设备是否遵循规定，并禁止网络中的横向移动，从而避免应用对公众曝光，大幅缩小攻击面。

为何重要

ZTNA通过信任代理，实现用户到应用的分段访问。这是一项重要技术，使企业机构能够隐藏专有应用和服务，并要求所有应用实施最小特权访问模型，通过创建仅包含用户、设备和应用的个性化"虚拟外围"来缩小攻击面。在中国，终端用户对于使用ZTNA来保护企业机构的数据兴趣渐浓。

业务影响

ZTNA保护服务免受攻击者的攻击，可产生立竿见影的效果。与基础版虚拟专用网络（VPN）产品不同，ZTNA取消了全网接入，改善了用户体验、灵活性和适应性。ZTNA简化了策略管理，可实现更精细的用户到应用分段，使中国的企业机构能够利用ZTNA取代其他不够安全的远程访问方式，缩小外部攻击面，并且提高数据安全性。

推动因素

- 传统VPN部署需要进行现代化升级改造，使用针对静态用户位置进行优化的简化网络架构连接至数据中心环境，而不是位于企业外的应用、服务或数据。
- 企业机构内部零信任方式采用增多，带来了对本地和云应用更精确的访问和会话控制的需要。
- 大型企业集团旗下不同实体的第三方（如供应商、厂商和承包商）和/或者用户，需要在不将整个网络暴露于外网的条件下，与应用安全连接。
- 为并购赋能，在并购完成前将应用的访问权限扩展至被收购的企业，无须另外部署端点或将企业网络互联；在并购完成后，简化网络合并流程，缩短所需时间。
- 随着包括ZTNA组件在内的安全服务边缘（SSE）市场兴起，企业机构愈发希望通过一个单一平台和终端代理来获得安全的专有应用、网络和云服务。
- 中国的大型企业或企业联盟的治理结构通常十分复杂，旗下存在多个大型子公司或关联公司，这些公司都对基于使用和基于实体的安全访问策略有着强烈需求。

阻碍因素

- 成本：ZTNA通常以用户或年度为单位来为每个许可证的指定用户授权；与以会话为单位的传统VPN相比，这一方式花费较多。
- 弱身份与访问管理（IAM）：弱IAM的企业机构不方便部署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基于云服务的信任代理，而仅部署在本地的ZTNA无法充分发挥其高可用性和可快速扩展的优势。
- 策略的复杂性： 为使ZTNA的效益得到充分发挥，企业机构必须提前规划正确的应用访问，但从运营的角度来看，建立人员与资源的大规模映射，会导致建模、部署和管理过于复杂。
- 市场营销混乱： 厂商将“VPN即服务（VPNaaS）”或“安全套接字层VPN（SSL VPN）”作为ZTNA来营销，这会使买方感到困惑，因为VPNaaS或SSL VPN通常缺乏某些零信任态势能力。

使用建议

- 理解ZTNA与传统VPN技术在业务上的不同之处，更好地为ZTNA的部署分配适当的投资。
- 无论用户是否使用企业网络来访问应用，都为其提供标准化的用户体验（UX）。
- 基于角色而非个人来部署特定应用的访问，并与业务部门合作，确保部署的成功。
- 减少对完全自带设备（BYOD）的管理要求，允许个人设备访问，实现更加安全的应用直接访问。
- 对敌对网络（例如，暴露于互联网上的传统VPN集成商和协作系统）隐藏系统。
- 如果物联网（IoT）设备支持IoT网络段上的轻量级代理或虚拟应用连接器，则应确保对IoT设备enclave的安全访问。
- 在最终确定ZTNA提供商时，应注意其安全访问服务边缘（SASE）或SSE产品的未来路线图，因为这事关企业机构安全访问路线图的未来发展。

厂商示例

阿里云、缔盟云、云深互联、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

复苏期技术

中国的态势感知技术

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。此外，态势感知技术还可根据收集到的数据，对安全态势进行分析和展示，据此预测安全态势趋势。

为何重要

- 中国政府从2016年开始使用网络安全态势感知这一概念。安全和风险管理（SRM）领导者必须了解这个概念，并将其融入技术选型和部署战略中。
- 态势感知（SA）技术可支持安全运营中心（SOC）实现安全数据（比如，数据资产、漏洞等级和日志详情等）收集、分析、决策、执行和验证的闭环管理。

业务影响

态势感知技术可为安全和风险管理领导者赋能，使其能够：

- 实时或近实时地确定流程并理解信息。
- 提前预测系统可能遇到的问题，在此基础上制定和创建有效的主动安全防护措施。
- 轻松、高效地集成安全工具。例如，SOC可以使用单一控制台来统一汇总安全信息，无须登录不同平台。

推动因素

- 企业机构如果使用等保2.0三级和三级以上的系统，由于其系统和数据重要性较高，因此更有可能成为网络攻击的目标。此类机构对于采用SA解决方案作为其SOC的核心技术有着强烈需求。

- 网络安全风险在多样性、可扩展性、复杂性和持续性等方面不断发展演进。对于网络空间依赖度的提升，带来了对于SA技术需求的大幅增加——尤其是可为潜在网络安全问题提供可见性、风险评分和响应。
- 现代SOC团队需要一个集中化的平台来集成各个工具提供的实时信息，并对安全流程和资源进行编排。

阻碍因素

- 态势感知通用技术要求的国家标准征求意见稿目前已发布（更多信息，请参阅 全国信息安全标准化技术委员会官方网页），但市面上的SA解决方案和产品在命名、能力和功能等方面都存在差异，有待统一。
- 云技术的采用使IT环境的边界扩大，安全运营的范围也因此拓展，复杂性也随之增强。
- 随着安全工具和日志的不断集成，安全数据的体量在急剧增长。因此，一些SA解决方案难以做到减少告警噪音，以帮助SOC团队集中精力应对最重要的事件和风险。
- 由于SA解决方案要兼顾各方面的功能，因此不是每个方面都能配备充足的预算和资源，例如合格的安全分析师、安全用例和剧本开发者。

使用建议

- 对企业机构的安全监控目标和用例进行定义。
- 评估SA解决方案能否弥补已经部署的技术的差距。
- 记录网络和系统拓扑结构（包括本地和云端基础设施），以及部署安全控制措施的位置。
- 根据企业机构的“上云”计划，选择并设置最适合的SA解决方案对云环境进行监控。
- 通过应用编程接口（API），使用嵌入SA解决方案中的相关功能，快速减少误报并提高效率。这些功能包括关联分析、漏洞和威胁情报，以及安全编排、自动化和响应（SOAR）等在内的技术方法，对告警进行分类，并自动处理及关闭简单告警。
- 分配数量充足的专门人员负责实现SA解决方案中的监测和响应用例；或者，也可以考虑将安全服务提供商作为内部团队的延伸，与其共同管理。

厂商示例

360数字安全集团、亚信安全、安恒信息、新华三、华为、绿盟科技、奇安信、深信服科技、天融信、启明星辰

Gartner相关阅读推荐

快问快答：态势感知解决方案在中国的两种常见用例是什么？

What You Need to Know About China's Cybersecurity Protection Classification Framework

中国的数据分类

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归类、分类法或本体论来组织信息资产的过程，包括给数据对象打标签，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，包含大量有用的元数据，可为决策者提供洞察力。

为何重要

数据分类可以对数据治理项目里的数据进行高效的优先级排序，其依据包括数据价值、安全、访问、使用、复用性、隐私、存储、伦理、质量和留存等各个方面。根据中国的法律法规，数据分类对于数据安全、数据治理以及合规都至关重要。同时，它也有助于企业机构了解其处理的数据的敏感程度及相关业务场景。

业务影响

数据分类增强了企业机构对数据集的分析，能够在数据存储中构建数据，而且允许对数据资产使用即时控制。数据预分类或数据标签，会给各种安全控制——例如数据丢失防护（DLP）和数据访问治理（DAG）——带来极大的便利。数据分类使企业机构能够更轻松地查找和检查数据，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

- 市场上成熟和标准化的数据分类方法越来越多，包括按照类型、所有者、法规、敏感度和留存要求进行分类。这使企业机构可以将其安全、隐私和分析工作的重点放在重要的数据集上。
- 当前地缘政治形势的变动增加了人们对数据驻留和数据主权的担忧，特别是对于重要数据和个人信息。然而，当前这种出问题后再解决的安全治理实践十分低效，因此从数据分类开始简化和自动化这些流程的需求越来越多。
- 具有行业特定分类定义（如金融、电信、医疗和政府）的自动化数据分类工具的出现，降低了数据分类项目启动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。
- 分类工作的思路往往是以安全为中心，没有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，但结果的准确性仍未达到预期，特别是需要长期训练模型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

- 明确企业机构范围内的数据分类用例和工作。
- 将相关情况同步给所有利益相关者——包括业务、安全、隐私及合规领导者。
- 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）——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。
- 部署与数据编织相关的功能，例如主动的元数据实践和数据可观测性，以简化和自动化数据分类流程。

厂商示例

安恒信息、观安信息、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

Toolkit: Sensitive Data Classification and Handling Documents

Improving Unstructured Data Security With Classification

How to Succeed With Data Classification Using Modern Approaches

中国的云工作负载保护平台

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）是以工作负载为中心的安全产品，可以为混合云和多云数据中心的服务器工作负载提供保护。CWPP可对任何地点的物理机、虚拟机、容器和无服务器工作负载提供持续的可见性和管控。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

中国的云服务采用率不断提高，而且许多中国企业机构更青睐采用混合云和私有云。这两个因素推升了对工作负载保护工具的需求，此类工具可为公有云、私有云和本地数据中心提供支持。云工作负载保护平台可维护运行时工作负载的可见性、管控和完整性，并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。因此，CWPP与终端用户系统存在很大差异，可为容器和无服务器工作负载，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，从而与云工具链和软件开发流程相集成。
- 工作负载的跨平台部署越来越多，而不再局限于企业机构的传统物理范围，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。
- 采用本地数据中心或终端用户终端保护平台（EPP）无法为云工作负载提供充分保护。服务器工作负载通常不会出现并执行未知任意代码，这与终端用户的端点有所差异。因此，此类工作负载适合采用默认拒绝、基于应用控制的保护策略。

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。
- 中国的许多CWPP工具对容器的支持有限，并未覆盖无服务器功能和平台即服务（PaaS）要求。此外，无服务器功能和PaaS安全保护能力的实施不应借助代理或容器特权模式。
- 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适当的云工作负载保护终端工具。
- 一些企业机构的云保护方法仍不成熟，并且未能明确对云原生安全工具集的真正需求。
- 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。

使用建议

- 在保护云主机工作负载时，避免使用终端用户终端检测和响应（EDR）或EPP解决方案。
- 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。
- 要求CWPP产品的所有功能具有应用编程接口（API）。
- 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。
- 要求提供云原生应用保护平台（CNAPP）工具发展路线图。

厂商示例

阿里云、亚信安全、山石网科、华为、默安科技、绿盟科技、奇安信、安全狗、腾讯

Gartner相关推荐阅读

Market Guide for Cloud Workload Protection Platforms

How to Make Cloud More Secure Than Your Own Data Center

中国云安全最佳实践

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实施攻击，以展示攻击成功带来的影响。这些手段包括网络钓鱼、社会工程、物理渗透、潜伏和突袭。与之相对的是，防守团队（蓝队）负责检测并应对来自红队的攻击。

为何重要

中国政府每年都会组织国家级攻防演练，不可预测的恶意攻击也日益增多，这些都促使企业机构主动实施攻防演练。安全服务提供商可能会在演练中担任攻击队的角色，帮助企业安全团队在接近真实的场景下查漏补缺。

业务影响

攻防演练具有重要的业务影响，例如：

- 可提供企业机构当前安全状态的信息和修复需求。
- 可评估安全运营中心（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。
- 可判断安全响应流程的设计和执行是否恰当。
- 可促进SOC攻防团队之间的良性竞争，有助于保持SOC的警惕性和互动性。

推动因素

- 对于应要求参与国家级攻防演练的企业机构来说，攻防演练已成为一项合规需求。这些企业机构涉及的行业包括金融、交通、能源、电信和公共服务行业等。监管机构可基于演练结果，判断这些企业机构是否严格实施了相关安全法规和国家标准中的安全基线。
- 由于威胁环境发生变化，攻击也变得更为复杂。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。企业机构如果从攻击者的角度来看待威胁，就能够更主动地发现迫在眉睫的风险，从而推动最重要的修复工作。
- 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。
- 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。这种方法有助于提高SOC、其他IT团队和业务部门的安全意识。
- 各类工具逐渐涌现，有助于提高攻防团队的效率。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执行情况。

阻碍因素

- 许多企业机构将攻防演练视为特定时间的特定活动，并未将其与日常的安全运营紧密结合起来。
- 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。
- 制定常规演练与应急响应相结合的安全运营战略。
- 在选用第三方服务提供商之前，对其开展概念验证和尽职调查，对其可使用的设备、访问权限、活动记录和监控进行详尽的规划。
- 组合使用多种适合企业具体情况和需求的测试方法，对安全态势进行更全面的了解。例如，对每个系统进行渗透测试，以及利用入侵和攻击模拟（BAS）实现重复任务的自动化，为攻击团队提供支持。人员配置和预算充足且成熟度高的企业机构，可考虑聘用安全人员或培养现有人员，自建内部攻击团队。

厂商示例

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

Gartner相关推荐阅读

中国安全运营最佳实践

附录

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（2022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（2022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（2022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

Table 1: 2022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		中国的自带身份技术 安全访问服务边缘	中国的数据风险评估 中国的软件成分分析 安全多方计算	
较高		中国的数据分类 攻防演练	中国的入侵和攻击模拟技术 中国的数据安全平台 中国的物联网身份认证 智慧城市的信息物理系统安全	
中等	中国的云工作负载保护平台	中国的态势感知技术 中国的零信任网络访问	中国的云安全资源池 中国的攻击面管理 中国的机密计算	
较低				

来源：Gartner（2022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（2022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（2022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（2022年10月）