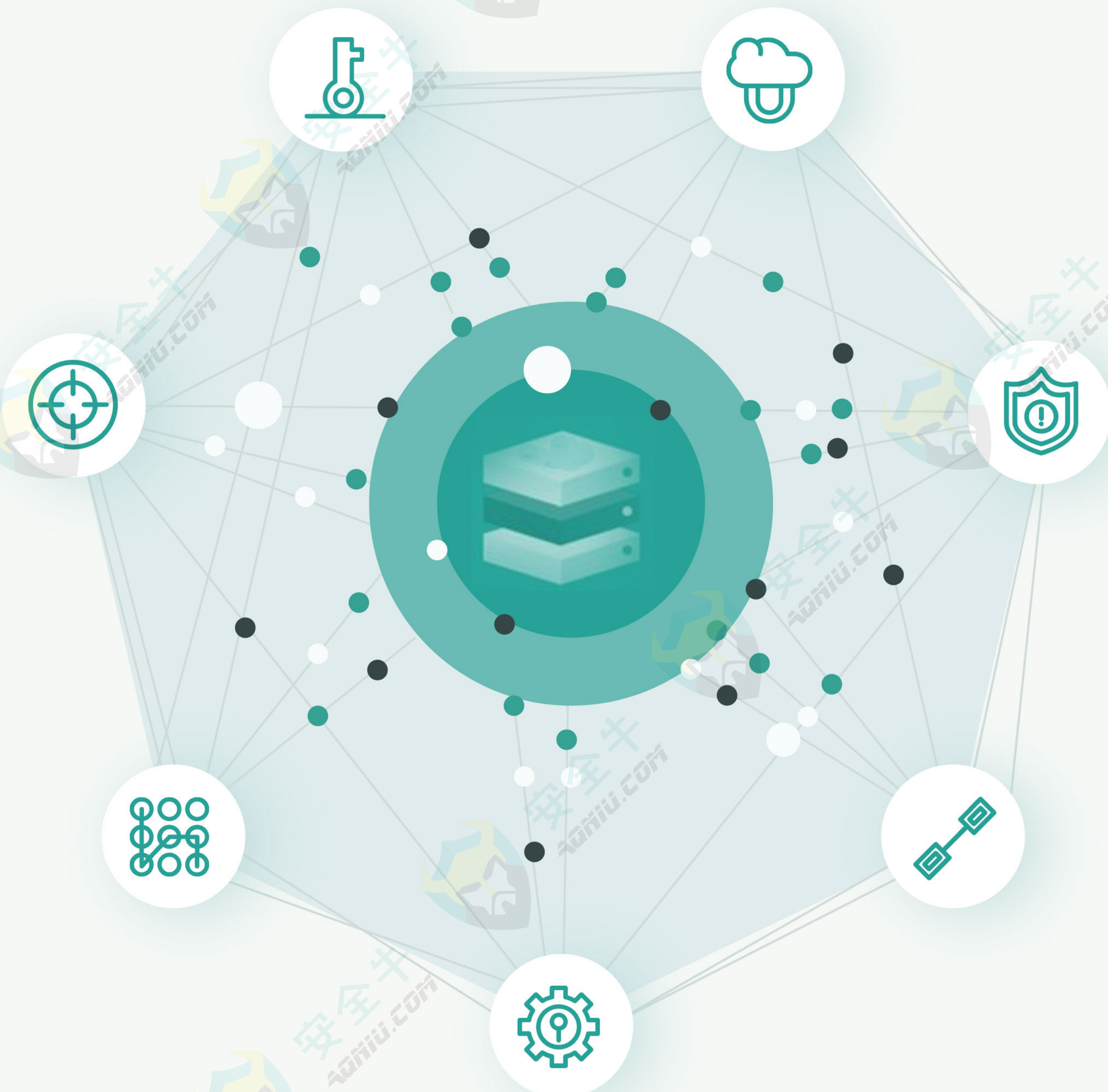
《攻击面管理技术应用指南》

（2024版）



版权声明

免责声明

本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。 任何非本公司发布的有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司发布的本报告完整版本为准。

本报告中的行业数据主要为分析师市场调研、行业访谈及其他研究方法估算得来，仅供参考。因调研方法及样本、调查资料收集范围等的限制，本报告中的数据仅服务于当前报告。本公司以勤勉的态度、专业的研究方法，使用合法合规的信息，独立、客观地出具本报告，但不保证数据的准确性和完整性，本公司不对本报告的数据和观点承担任何法律责任。同时，本公司不保证本报告中的观点或陈述不会发生任何变更。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的行为建议，也没有考虑到个别客户特殊的目的或需求。客户应考虑本报告中的任何意见是否符合其特定状况，若有必要应寻求专家意见。任何出现在本报告中的包括但不限于评论、预测、图表、指标、指标、理论、陈述均为市场和客户提供基本参考，您须对您自主决定的行为负责。本公司不对因本报告资料全部或部分内容产生的，或因依赖本报告而引致的任何损失承担任何责任，不对任何因本报告提供的资料不充分、不完整或未能提供特定资料产生的任何损失承担任何责任。

目 录

引言

随着数字经济的蓬勃发展和全球网络安全形势的日益严峻，网络安全已经成为企业和组织发展的重要基石。传统的安全防御手段面对不断演变的网络威胁，越来越无法满足企业和组织的安全需求。攻击面管理（ASM）应运而生，作为一种新兴的安全理念，它通过持续监控和分析企业网络资产和暴露面，识别潜在的安全风险，并采取相应的措施进行缓解和处置，从而帮助企业更好地应对网络攻击，保障业务安全和数据安全。

近年来，攻击面管理在国内外市场都得到了快速发展和广泛应用。在国外，Gartner、Forrester 等权威研究机构纷纷将攻击面管理列为重要的安全趋势，并对其发展前景给予了高度评价。在国内，随着《中华人民共和国网络安全法》等一系列法律法规的出台，以及关键信息基础设施安全保护条例的实施，企业和组织对网络安全的重视程度不断提高，对攻击面管理的需求也日益增长。

当前，攻击面管理技术发展迅速，市场规模不断扩大。根据 Gartner 的预测，到 2026 年，全球攻击面管理市场规模将达到 187 亿美元。越来越多的企业开始意识到攻击面管理的重要性，并将其作为网络安全建设的关键环节。

为了帮助企业更好地理解和应用攻击面管理技术，安全牛在 2023 年发布了《攻击面管理技术应用指南 2023 版》，受到了广大读者的欢迎和好评。今年，安全牛延续去年的工作，再次推出《攻击面管理技术应用指南 2024 版》。本报告的研究方法包括文献研究、用户调研、厂商调研等，

本报告将重点关注攻击面管理的概念发展、技术应用，深入分析国内市场需求和应用场景，探讨攻击面管理的能力框架和关键技术，并对国内外市场发展趋势进行研究。此外，本报告还将新增一章对 AI 攻击面进行探讨，分析 AI 技术带来的新的安全挑战和应对策略，从而帮助企业和组织更好地应对网络攻击，保障业务安全和数据安全。

报告关键发现

- 攻击面管理需要管理和技术并重。攻击面管理不仅是技术，更需要管理支撑，制定相应的管理标准和规范，推动安全团队与 IT 运维团队的深度协作，才能实现更高效、更精确的攻击面管控。

- 适用于较高成熟度阶段的企业实践。实施攻击面管理需要企业具备一定的基础设施与技术能力，与基础设施深度集成与联动的条件下，攻击面管理才能更有效的为企业的安全运营提供有力支撑。

- 国内市场的初级发展与资产数据挑战。当前国内攻击面管理仍处于发展早期阶段。核心难点在于企业普遍面临资产数据质量参差不齐、数据冗余与缺失的问题，亟需加强数据治理与质量管控，数据质量直接影响了攻击风险的发现与分析。

- 需求增长与政策驱动。随着数字化转型加速，企业外部暴露面随之增多，对攻击面管理的需求持续上升。同时，国家对网络安全监管与实战化要求不断提高，从政策与合规层面推动了市场对更完备的攻击面管理能力的强烈需求。

- 平台化与融合方向。攻击面管理平台正从单点工具转向与其他安全技术有机融合。一方面，CAASM、EASM 与 BAS 正逐步整合为统一平台，实现数据共享与功能互补；另一方面，与其他安全平台的循环交互与数据联动正在形成新的生态，使整体安全防御体系更为完善、敏捷与高效。

- 关注重点从外部扩展至内部。国内用户正从关注外部攻击面（EASM）转向内部攻击面（CAASM）。用户意识到内网资产通常比外网资产更加敏感，在此趋势下，将外部与内部攻击面管理有机融合，为企业提供更全面的资产视图与风险画像，成为新的关注焦点。

- 资产数据质量的核心地位与治理需求。企业已积累大量资产数据，但数据质量参差不齐是当前痛点。企业期望通过资产数据治理技术与方法，获得高精度、高关联性的资产数据，为后续攻击面分析和防护策略制定奠定坚实基础。

- 从资产到风险的价值转移。攻击面管理的价值正从传统的资产管理拓展到风险管理层面。用户不仅期望通过攻击面管理提升资产可见性，更希望实现对整体安全态势的动态、可量化管控，提高攻击风险的检测和响应能力。

- 开始关注全链路威胁展示与溯源。用户不再满足于对孤立风险点的识别，而是希望通过跨设备、跨系统的数据关联和分析，实现完整的攻击链路可视化。精准定位真正的攻击路径与风险源，更好地支持事前预防与事中响应。

- AI 技术应用初步尝试，成效有限。尽管厂商积极探索利用人工智能（AI）技术实现自动资产发现、漏洞识别与风险评估，然而当前成果仍然有限。技术应用仍处于初级阶段，有待进一步优化算法模型、提升数据训练质量与增强应用场景适配度。

- 行业定制与深耕趋势。国内攻击面管理正在走向行业化应用，针对不同行业的需求与业务场景提供差异化方案。通过贴合行业特性与业务流程的深度定制，攻击面管理厂商正逐步构建行业生态，提升客户满意度与实际防护效果。

- 安全验证需求崛起。目前大多数用户已经完成基础安全建设阶段，进入攻防演练等验证阶段，需要利用攻击面管理技术从攻击者视角检验现有安全防御能力的有效性，确保安全投入的实战价值。

第一章 攻击面管理背景概述

在数字化时代，网络威胁正在快速演变和升级，对全球企业和组织的安全防护体系构成了前所未有的挑战。勒索软件、供应链攻击、APT 攻击等新型网络威胁层出不穷，其复杂性和破坏力不断增强。此外，随着人工智能技术的快速发展和广泛应用，AI 攻击面也逐渐成为网络安全的新焦点。AI 技术不仅可能被攻击者用来发起更复杂的攻击，而且其自身也可能存在安全漏洞和风险。

为了应对日益严峻的网络安全形势，各国政府和行业组织纷纷出台了相关的安全合规要求和标准。例如，美国国家标准与技术研究院（NIST）的网络安全框架、欧盟的通用数据保护条例（GDPR），以及中国的数据安全法、个人信息保护法、关键信息基础设施安全保护条例等。这些政策法规和标准不仅对企业和组织的安全管理提出了更高的要求，也促进了攻击面管理技术的应用和发展。

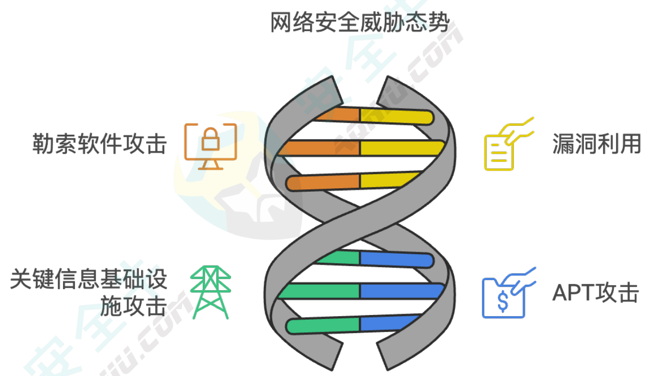
攻击面管理作为一种主动防御策略，通过持续监控与分析网络资产及其暴露面，可以及时发现潜在安全风险，并迅速采取缓解与应对措施，不仅能有效降低安全事件的发生概率与影响范围，更可全面保障业务连续性与数据安全性。因此，攻击面管理引起了业内的普遍重视，并得到了快速发展。

1.1 攻击面管理威胁态势分析

近年来，随着网络攻击技术的不断发展，安全漏洞频出，攻击手段翻新，黑灰产猖獗，企业面临的攻击面风险日趋严峻。攻击者利用各种手段，包括勒索软件、供应链攻击、APT 攻击，以及 AI 技术等，对企业的数据安全、业务安全和声誉造成严重威胁。以下对国内外攻击面管理的威胁态势现状进行分析。

1.1.1 全球网络攻击威胁态势

随着网络技术的快速发展，攻击手段也在不断进化。网络攻击者利用先进的技术手段，来提高攻击的精准度和隐蔽性。



全球网络攻击威胁态势

全球网络攻击威胁态势有以下特点：

- 勒索软件攻击持续高发。勒索软件攻击在全球范围内持续高发，攻击目标也更加广泛，包括政府、金融、医疗、教育等关键领域。攻击者通常采用加密数据、破坏系统等手段，勒索高额赎金，给受害者带来巨大的经济损失和业务中断。如在 2023 年 10 月，美国波音公司遭受勒索软件攻击，2023 年勒索软件索求金额达 2 亿美元，由于未支付赎金，43GB 的公司数据被发布到网上，导致波音公司受到起诉。

- 漏洞利用攻击仍是主流。攻击者利用各种漏洞和弱点，例如零日漏洞、供应链漏洞、社会工程学等，对目标系统进行渗透和破坏。漏洞利用攻击的成本低、效率高，攻击者可以轻易地利用自动化工具和技术对大量目标进行攻击。2020 年美国联邦政府数据泄露事件，导致全球包括美国各级政府部门、北约、英国政府、欧洲议会、微软等至少 200 个政府单位、组织或公司受到影响，并且组织数据遭到了泄露，该事件就是利用了微软和 SolarWinds 漏洞。

- 针对关键信息基础设施的攻击日益增多。关键信息基础设施是国家安全和社会稳定的重要支撑，攻击者针对关键信息基础设施的攻击日益增多，例如能源、交通、医疗等领域。这些攻击可能导致关键服务的瘫痪和社会秩序的混乱。

- APT 攻击持续活跃。APT 攻击通常由国家或组织支持，目标是窃取敏感数据、破坏关键基础设施或进行长期潜伏和渗透。APT 攻击手段复杂、技术高超，对安全防护体系构成了严峻挑战。例如，2022 年 1 月 14 日，在 2021 年—2022 年俄乌危机期间，乌克兰十多个政府网站遭到网络攻击后瘫痪，据乌克兰官员称，大约有 70 个政府网站受到攻击，包括外交部、部长内阁和国家安全与国防事务委员会。

1.1.2 国内网络攻击威胁态势

近年来，国内网络攻击手段也层出不穷，攻击目标广泛，攻击方式多样化且日趋高级，对我国各行各业的企业和组织都带来了巨大的安全挑战。

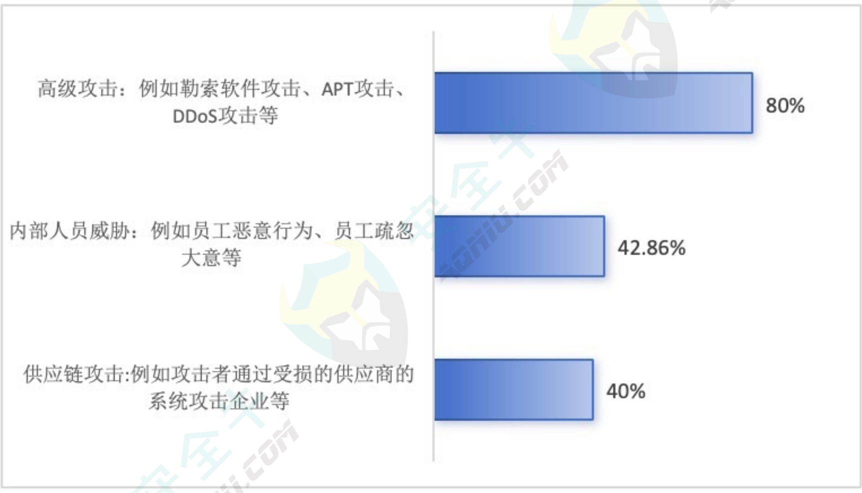
国内网络攻击威胁态势

国内网络攻击威胁态势有以下特点：

- 勒索软件攻击快速增长，目标更具针对性。勒索软件攻击在国内呈高发态势，攻击目标涵盖了政府、金融、医疗、教育等多个行业。攻击者通常采用加密数据、破坏系统等手段，勒索高额赎金，给受害者带来巨大的经济损失和业务中断。攻击者不再仅仅满足于加密数据勒索赎金，而是更倾向于攻击关键信息基础设施、大型企业等高价值目标，窃取数据并威胁公开，以增加受害者支付赎金的压力
- APT 攻击持续活跃，趋于长期化和隐蔽化。APT 攻击通常由国家或组织支持，目标是窃取敏感数据、破坏关键基础设施或进行长期潜伏和渗透。APT 攻击手段复杂、技术高超，对安全防护体系构成了严峻挑战。攻击者潜伏期更长，攻击手段更加隐蔽，攻击目标更加精准，对安全防护体系的威胁更大
- 内部人员威胁不容忽视。内部人员泄露数据、破坏系统的事件时有发生，企业应加强内部人员的安全管理和安全意识教育。
- 供应链攻击成为新兴威胁。攻击者利用供应链中的薄弱环节，例如软件漏洞、第三方服务、人员疏忽等，对目标企业进行渗透和攻击。供应链攻击的隐蔽性和破坏性极强，一旦成功，将会对整个供应链造成严重的安全风险和经济损失。

数据泄露事件频发。近年来，国内数据泄露事件频发，例如 2023 年，某高校因 3 万余条师生个人信息数据泄露被罚款 80 万元。数据泄露的原因包括系统漏洞、人为错误、网络攻击等，给企业和个人都带来了巨大的损失和风险。

根据安全牛 2024 年企业用户调研结果显示，用户对外部高级攻击的担忧程度最高（80%），其次是内部人员安全风险（42.86%）和供应链攻击风险（40%）。用户担心的网络安全风险主要原因中，系统漏洞占比最高（68.57%），其次是网络钓鱼（48.57%）、弱密码（48.57%）、数据安全（42.86%）。

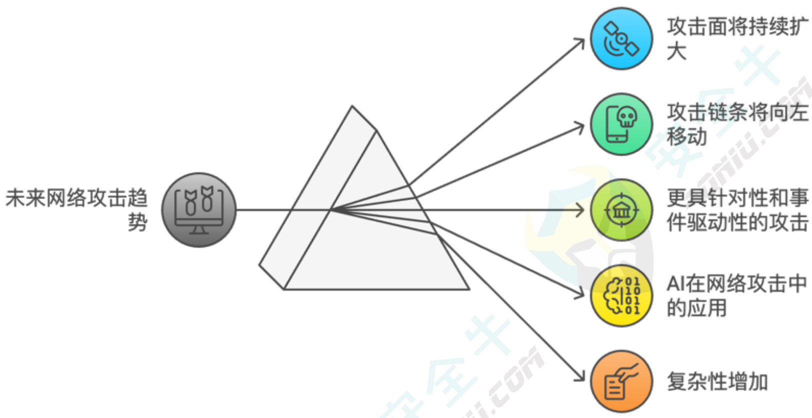


企业担心的网络攻击风险

企业认为网络攻击风险的原因

1.1.3 未来威胁总体态势

安全牛认为，未来网络攻击主要有以下趋势：攻击面将持续扩大，攻击链条将向左移动，攻击将更具针对性和事件驱动性，AI 将被更广泛地用于攻击，网络攻击将更加复杂和难以预测，网络安全威胁将更加严峻。



未来威胁总体态势

网络攻击面未来总体态势如下：

- 攻击面将持续扩大。随着物联网、5G/6G、卫星通信等技术的发展，越来越多的设备接入网络，攻击面将不断扩大。例如，近地轨道卫星空间的设备连接数量增加，为攻击者提供了更多入侵机会。

- 攻击链条将向左移动。攻击者将更多地利用攻击链左侧的战术，例如社工、钓鱼等，以获取初始访问权限。利用 AI 技术，攻击者可以更轻松地获取个人信息、伪造身份，甚至可能出现“招募即服务”的模式，帮助攻击者从目

标组织内部招募人员。

- 攻击将更具针对性和事件驱动性。攻击者将聚焦更具针对性和事件驱动性的攻击机遇，例如大型体育赛事、地缘政治事件等。借助 AI 等新工具，攻击者可以更有效地针对特定目标和事件发动攻击。
- AI 将被更广泛地用于攻击。从生成式分析到自动化攻击，AI 将被攻击者用于攻击的各个阶段。攻击者可以利用 AI 技术进行更精准的目标研究、自动化攻击执行，甚至开发新的攻击工具和技术。
- 网络攻击将更加复杂和难以预测。随着攻击技术和工具的不断发展，网络攻击将更加复杂和难以预测。攻击者将利用各种手段，例如 AI 技术、社会工程学、漏洞利用等，对目标系统进行攻击，给安全防护带来更大的挑战。

1.2 攻击面管理防护要求与标准

随着网络安全威胁的日益严峻和攻击面的不断扩大，各国政府和行业组织都加大了对网络安全的监管力度，出台了一系列安全合规要求和标准，强调了攻击面管理的重要性，要求企业和组织应识别和评估其所有攻击面，并采取相应的措施进行保护和监控。攻击面管理已经成为网络安全的重要组成部分，是企业和组织保障网络安全、数据安全和业务安全的重要手段。

1.2.1 国外安全合规要求

在国际范围内，尽管“攻击面管理”这一概念并未在多数政策、法规和标准中以独立名词的形式明确提出，但许多国外的网络安全法规、标准和指导原则已对与攻击面管理密切相关的实践（如资产识别、脆弱性管理、持续监控、风险评估与处置等）提出了要求。这些政策和标准为组织构建和完善攻击面管理体系提供了监管和合规层面的依据。以下是一些主要的国外政策、法规及标准示例：

◈ **美国（U.S.）相关法规、政策与框架**

联邦信息安全管理法案（FISMA）。要求美国联邦机构建立全面的网络安全计划，包括持续监控、资产识别及风险管理，这为攻击面管理奠定了基础。

✓ NIST 网络安全框架（NISTCybersecurityFramework，CSF）。由美国国家标准与技术研究院（NIST）推出的自愿性框架，为识别、保护、检测、响应和恢复安全能力提供指导。其中资产管理（ID.AM）和漏洞管理（PR.IP）相关措施为攻击面管理实践提供直接参照。

✓ NIST 特别出版物系列（如 NISTSP800-53、NISTSP800-37）。对信息系统及组织层面的安全与隐私控制、风险管理流程进行标准化。SP800-53 中对持续监控、资产配置管理、脆弱性评估的要求可辅助建立系统化的攻击面管控策略。

✓ 美国网络安全与基础设施安全局（CISA）相关指令。CISA 发布的绑定操作指令（BOD），如 BOD23-01，要求美国联邦民用部门执行持续漏洞扫描与清点资产，以减少可被利用的攻击面。

✓ 行政命令（EO14028）“提升国家网络安全”。强调软件供应链安全及持续安全监测，与攻击面管理中常涉及的供应链资产识别、验证及风险管理直接相关。

✓ CMMC（CybersecurityMaturityModelCertification）。美国国防部推出的供应链安全成熟度模型，要求承包商明确资产清单、持续评估网络脆弱性，这一要求与攻击面管理的基础环节高度契合。

◈ **欧盟（EU）及欧洲相关法规与标准**

✓ 网络与信息安全指令（NISDirective）及 NIS2。要求成员国关键基础设施提供商与数字服务商加强网络安全风险管理，包括风险识别、持续监控与漏洞管理，这实际推动了攻击面管理相关实践的落地。

✓ 欧洲网络安全法（EUCybersecurityAct）及欧洲网络与信息安全局（ENISA）指导文件。ENISA 发布的网络威胁分析报告和最佳实践指南涵盖了资产识别、风险识别及缓解策略，为攻击面管理提供参考。

✓ 通用数据保护条例（GDPR）。尽管 GDPR 重点关注个人数据保护，但其对数据处理安全性的要求鼓励企业重视对攻击面的识别与保护，从而减少潜在数据泄露风险。

✓ ISO/IEC27001 与 27002 系列国际标准。这些标准为信息安全管理体系（ISMS）提供整体框架，对资产管理、漏洞管理、持续监控及风险评估均有明确要求。尤其是 ISO/IEC27002 中细化了安全控制措施，对攻击面管理实践给予方向性指导。

◈ **英国及其他欧洲国家措施**

✓ 英国国家网络安全中心（NCSC）最佳实践与指南。NCSC 的指导文件（如“TenStepstoCyberSecurity”）强调资产可见性、漏洞管理与持续监控，对于建立攻击面管理机制具有借鉴意义。

✓ 英国“网络安全基础认证 (CyberEssentials)”。要求组织具备基础的安全防护措施，包括安全配置、持续补丁和风险处理，为小型企业实施初级的攻击面管理能力提供参考。

◈ **行业标准与框架**

✓ CIS 控制（CISControls）。由国际非营利组织 CenterforInternetSecurity 发布的安全控制指南在最新版本中强调准确的资产清点、持续漏洞扫描和风险优先级管理，为企业构建攻击面管理体系提供可操作的参考控制项。

✓ PCI-DSS（PaymentCardIndustryDataSecurityStandard）。对支付行业组织提出严格的数据安全要求，包括定期扫描、漏洞修复与风险管理，这些要求在本质上也是对攻击面的持续管理与收敛。

✓ MITREATT&CK 框架。虽然不是法规，但该知识库为组织理解攻击者技术和策略提供结构化参考，有助于组织识别潜在攻击路径，进而辅助组织优化攻击面管理策略。

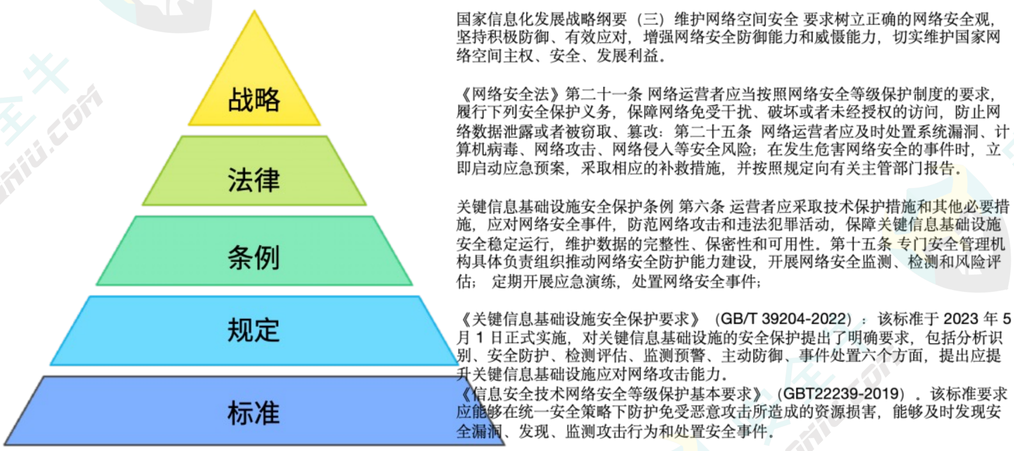
◈ **云与供应链安全相关标准与准则**

✓ CloudSecurityAlliance（CSA）指南。CSA 对云计算环境下的安全控制提出标准化建议，涵盖持续监测、资产识别与配置管理，为云环境中的攻击面管理提供参考模型。

✓ 供应链安全标准与法规（如美国 EO14028 中对软件供应链安全的强调）。要求组织在供应链层面做到资产和组件清单的透明化，进而减小供应链攻击面。

1.2.2 国内安全合规要求

国内在网络安全和数据安全方面，从战略、法律、条例、规定和标准等多个层面提出了明确的要求，并强调了积极防御、主动发现、及时处置和持续改进的重要性。



国内安全合规要求

国内相关网络安全政策法规如下：

- 国家信息化政策。我国 2016 年发布了国家信息化发展战略纲要，作为规范和指导未来 10 年国家信息化发展的纲领性文件，要求树立正确的网络安全观，坚持积极防御、有效应对，增强网络安全防御能力和威慑能力，切实维护国家网络空间主权、安全、发展利益。

- 网络安全相关法律。《中华人民共和国网络安全法》《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》等法律推动了网络安全风险防控的重视，要求企业不仅要保护关键信息基础设施，还要保护个人信息和数据安全，减少因资产暴露面过大而带来的安全风险。如《中华人民共和国网络安全法》第二十一条要求网络运营者应保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；第二十五条 网络运

营者应及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。如《中华人民共和国数据安全法》要求数据处理者采取必要措施保障数据安全，防止数据泄露、篡改和破坏。如《中华人民共和国个人信息保护法》要求个人信息处理者采取必要措施保护个人信息安全，防止个人信息泄露、滥用和非法交易。

- 《关键信息基础设施安全保护条例》。该条例于 2021 年 9 月生效，要求关键信息基础设施运营者采取必要措施保障关键信息基础设施安全，包括识别和管理关键信息基础设施攻击面，防止网络攻击和数据泄露。

- 《关键信息基础设施安全保护要求》（GB/T39204-2022）。该标准于 2023 年 5 月 1 日正式实施，对关键信息基础设施的安全保护提出了明确要求，包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置六个方面，提出应提升关键信息基础设施应对网络攻击能力。如针对发生的网络安全事件或发现的网络安全威胁，提前或及时发出安全警示。建立威胁情报和信息共享机制，落实相关措施，提高主动发现攻击能力。以应对攻击行为的监测发现为基础，主动采取收敛暴露面、捕获、溯源、干扰和阻断等措施，开展攻防演习和威胁情报工作，提升对网络威胁与攻击行为的识别、分析和主动防御能力。

- 《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）。该标准提出应能够在统一安全策略下防护免受恶意攻击所造成的资源损害，能够及时发现安全漏洞、发现、监测攻击行为和处置安全事件。 如应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

1.2.3 国内行业合规要求

工业和信息化部、公安部等主管部门根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国国家安全法》等法律法规，陆续发布了一系列数据安全的管理办法、细则等要求。

- 2022 年 12 月 8 日，工业和信息化部印发《工业和信息化领域数据安全管理办法（试行）》，对数据安全管理，保障数据安全进行了明确的要求，如第三十四条，行业监管部门及其委托的数据安全评估机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露或者非法向他人提供。

- 2023 年 11 月 30 日，公安机关强调要高度重视“两高一弱”的问题，即高度重视高危漏洞和高危端口，这是“两高”“一弱”就是弱口令这样的问题，加强防火墙和安全软件管理，合理分配员工权限，升级多层次的密码保护，加强软件和设备防护，防止黑客入侵系统。

- 2023 年 11 月 23 日，工业和信息化部网络安全管理局发布《工业和信息化领域数据安全行政处罚裁量指引（试行）》（征求意见稿），制定了数据处理活动监管处罚的规定。

- 2024 年 5 月 10 日，工业和信息化部发布了《工业和信息化领域数据安全风险评估实施细则（试行）》，要求开展数据安全风险评估，重点评估以下内容：（六）发生数据遭到篡改、破坏、泄露、丢失或者被非法获取、非法利用等安全事件，对国家安全、公共利益的影响范围、程度等风险。
- 2024 年 10 月 29 日，工业和信息化部印发《工业和信息化领域数据安全事件应急预案（试行）》，要求建立健全数据安全事件应急组织体系和工作机制，提高数据安全事件综合应对能力，确保及时有效地控制、减轻和消除数据安全事件造成的危害和损失。

1.2.4 标准与技术规范体系

国内网络安全技术规范标准虽未对“攻击面管理”进行专门定义，但其核心理念和要求已在多个标准中有所体现。

◈ **信息安全管理体系相关标准**

✓ GB/T22080（等同采用 ISO/IEC27001）及 GB/T22081（等同采用 ISO/IEC27002）中对资产管理、风险评估、漏洞管理、持续改进有明确要求。这些要求与攻击面管理在识别、分析和处置安全风险的流程中有高度重合。

✓ 风险评估与漏洞管理标准：GB/T20984《信息安全技术信息安全风险评估规范》：提供风险识别与评估的方法论，其中资产清点与脆弱点识别是实现攻击面可视化与管控的核心环节。

✓ GB/T30284《信息安全技术漏洞管理要求》：强调对系统、应用等进行持续性漏洞监测、分析与修复，是对攻击面中脆弱节点的直接管理手段。

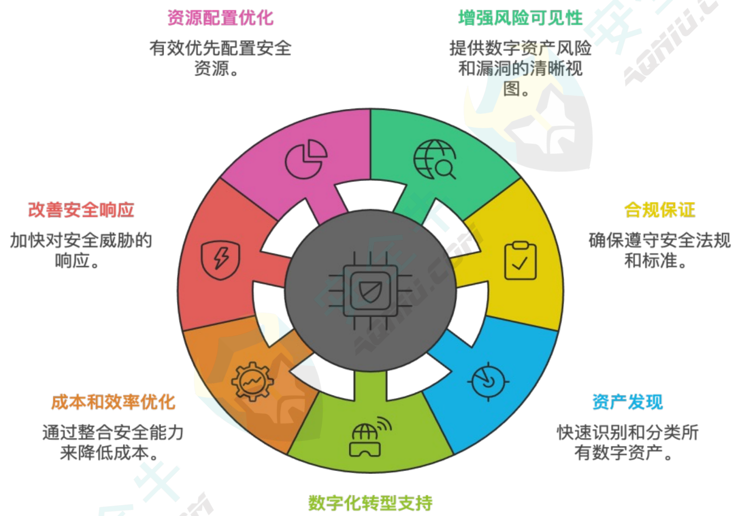
◈ **安全运营与应急响应相关标准**

✓ GB/T29246《信息安全技术信息安全能力成熟度模型》：鼓励组织持续提升安全管理与技术能力，包括对资产及弱点进行动态监测与改进。

✓ GB/T20988《信息安全技术网络安全应急处置指南》：要求对网络安全事件进行有效检测与快速响应，而有效的攻击面管理能帮助提前发现潜在攻击路径，减少应急响应难度。

1.3 攻击面管理应用必要性分析

通过实施攻击面管理，企业不仅能够更好地识别、评估和管理其攻击面，还能够满足国内外最新的安全合规要求和标准，以帮助企业降低安全风险，提升安全事件响应能力，从而提升整体安全防护能力，并降低安全运营成本。



攻击面管理应用必要性分析

（1）增强企业的风险可见性。随着数字化转型的深入，企业的数字资产分布变得更加广泛和复杂，包括内部网络、云服务、移动设备等。攻击面管理平台能够全面梳理这些资产，帮助企业清晰了解自身的风险状况，及时发现潜在的安全隐患。

（2）满足合规要求。在严格的法规环境下，企业需要确保其网络安全措施符合相关法律法规。攻击面管理平台能够提供详细的安全审计报告，帮助企业证明其合规性，避免因违规而遭受处罚。

（3）全面、快速的资产发现能力。攻击面管理产品应具备全面、快速的资产发现能力，包括网络空间测绘（CAM）、多类型扫描器调度和多维度漏洞评估，以及漏洞情报和智能优先级排序

（4）应对数字化转型带来的挑战。数字化转型导致 IT 架构重塑，大多数组织的网络资产数量和复杂性增加，攻击面急剧扩大。攻击面管理能够帮助企业在攻击者发现风险之前消除或管理风险。

（5）能力融合降本提效。将攻击面管理需要的各类能力整合到一个平台上，提升速度和准确性，减少频繁切换安全平台或工具的需要，降低复杂性和成本。

（6）提升安全响应速度。攻击面管理平台能够迅速发出预警，并提供详细的攻击路径和相关信息，协助企业能够快速采取措施进行应对，有效降低损失。

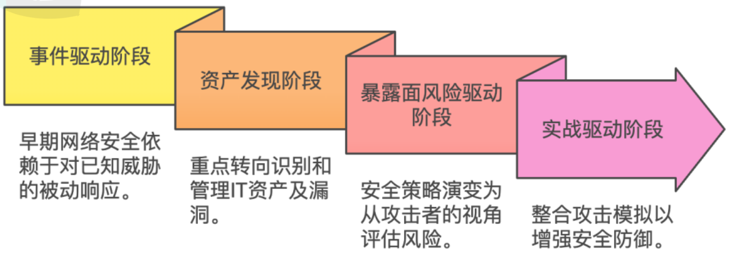
（7）优化安全资源配置。通过对攻击面的评估和分析，企业可以明确安全工作的重点和优先级，将有限的安全资源投入最关键的领域，提高安全防护的效率和效果。

第二章 攻击面管理能力框架

新一代攻击面管理防护理念强调持续监控、主动防御、风险导向和智能化。攻击面管理能够帮助企业提升资产管理效率与安全可见性、风险管理与安全控制、合规性保障与安全运营效率。企业应明确攻击面管理目标，构建人员、流程和技术三方面的能力框架，并掌握新一代攻击面管理关键技术，如自动化工具和平台、AI 驱动的资产发现和漏洞识别、攻击面建模与可视化等。

2.1 攻击面管理发展历程

攻击面管理的发展历程体现了网络安全防护理念的不断演进过程，包括从被动响应到主动防御，从静态分析到动态分析，从孤立的安全产品到全面的安全解决方案。未来，攻击面管理将继续朝着更加智能化、自动化和一体化的方向发展，为企业提供更加有效的安全防护。



攻击面管理发展历程

1. 事件驱动（被动）阶段（约 2000 年以前）

早期网络安全防护以被动响应为主，安全人员主要依靠安全信息和事件管理（SIEM）等工具来被动地收集和分析安全事件，并进行事件响应。安全防护的重点是识别和响应已知的攻击，对未知威胁的防护能力不足。例如，早期的防火墙主要用于拦截已知的攻击流量，对于新型的攻击手段经常无法有效防御。

2. 资产发现阶段（约 2000 年 -2010 年）

随着 IT 环境的日益复杂，企业开始重视资产的识别和管理，并使用漏洞扫描、配置检查等工具来发现和评估资产的安全风险。安全防护的重点是识别和管理资产，对攻击路径和攻击面的分析还不够深入。例如，企业开始使用漏洞扫描器来发现系统和应用中的漏洞，并进行修复。

3. 暴露面风险驱动阶段（约 2010 年 -2018 年）

企业开始从攻击者的视角来审视自身的安全防御体系，并使用攻击面管理工具来识别和评估暴露面风险。安全防护的

重点是识别和管理暴露面风险，对内部攻击面和动态攻击面的关注还不够。例如，企业开始使用攻击面管理平台来识别和管理暴露在互联网上的资产和漏洞。

4. 实战驱动阶段（2018 年至今）

Gartner 于 2018 年正式提出攻击面管理的概念，并将其定义为“持续发现、识别、清点和评估实体 IT 资产风险的过程”。企业开始将攻击面管理与实战攻防相结合，使用入侵和攻击模拟（BAS）等技术来验证安全防御体系的有效性，并进行持续改进。安全防护的重点是主动地识别和管理安全风险，并持续提升安全防御能力。例如，企业开始使用 BAS 平台来模拟攻击者的行为，并评估安全防御体系的有效性。

2.2 攻击面管理概念的改变

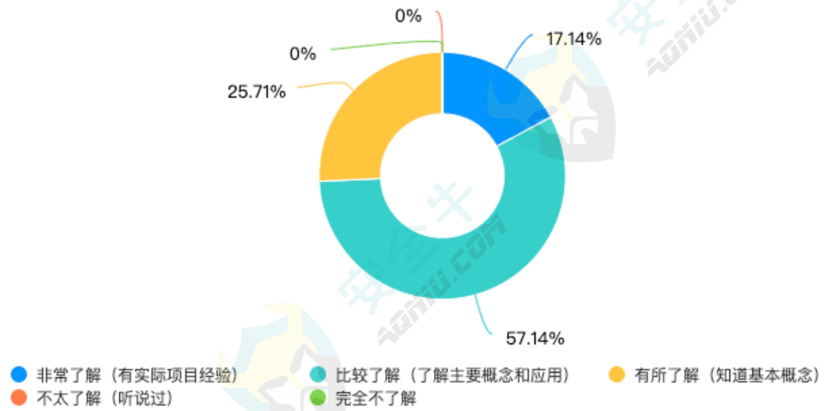
根据 2023 年安全牛研究报告《攻击面管理应用指南 2023 版》，攻击面管理是利用攻击者视角进行风险管理的方法，通过持续识别发现企业的攻击面，并对整体攻击风险进行收敛和验证，实现有效控制攻击风险的管理方法。攻击面是指从攻击者的视角开展网络安全的风险管理，类型包括外部攻击面管理（EASM）、网络资产攻击面管理（CAASM）、数字风险保护服务（DRPS），能力包括资产识别、攻击面识别、攻击面分析、收敛与验证和持续监控，详情请参考《攻击面管理应用指南 2023 版》。

攻击面管理框架 2023 版

2.2.1 攻击面管理需求场景的变化

2023 年的攻击面管理研究报告中，用户则对攻击面的概念理解并不充分，还存在很多问题与困惑；大部分厂商的攻击面管理还是以互联网资产识别加漏洞管理组成的产品为主，并且，其主要能力体现在互联网资产的发现。

经过一年多的实践，企业用户对攻击面的理解更加清晰，已经能够准确地了解攻击面主动防御的概念，其应用场景也开始贴合结合实战需求而应用落地。**根据 2024 年安全牛用户调研显示，**目前 74.28% 的用户表示比较或非常了解攻击面管理的概念。



用户对攻击面的理解

随着用户需求和理解的不断深入，攻击面管理的概念和内涵在不断丰富与演变，更加适应当前的网络安全威胁和技术发展趋势。

攻击面管理的概念变化

攻击面管理的主要变化趋势如下：

- **从关注外部攻击面到关注内部攻击面。**用户逐渐意识到内部攻击面的重要性，开始关注 CASSM 与 EASM 的融合能力。例如识别和管理未纳管内外部资产、分析外部资产与内部业务之间的连接关系、识别潜在的攻击路径等。
- **从资产梳理转向资产治理优化。**用户的资产数据已经基本建立，用户更加关注资产的质量，例如资产的数据的资产重复、属性等数据缺失、数据冲突等，并希望利用健全的一张图作为基础，实现攻击链路的可视化。**根据安全牛调研数据，**77.14% 的用户希望攻击面可以实现资产关联分类，自动归属，重要性标签，并资产全景图。并且 45.71% 的用户希望可以得到准确的风险报告。

- **从面向设备资产到面向风险管理。**攻击面管理从之前的资产发现能力转向面向风险的发现。根据安全牛调研数据，51.43% 的用户希望攻击面可以协助威胁的检测和响应，51.43% 的用户希望攻击面可以进行弱密码、配置错误核查，48.573% 的用户希望攻击面可以协助漏洞管理。

- **从单点资产管理到全链路风险防护。**用户更加关注全链路风险防护，更加关注攻击者可能利用的攻击路径和攻击目标，进行跨设备的数据关联分析，识别完整的攻击链路。**根据安全牛调研数据，**40% 的用户希望攻击面可以实现展示真实攻击路径。

- **从合规检查到有效性验证。**随着用户安全建设能力的提高，用户从合规检查转向安全有效性验证，并且更关注检验安全防御体系是否能够抵御真实的攻击，而不是单个安全设备的防护能力。

- **持续监控。**攻击面管理需要持续监控攻击面的变化，例如新增资产、变更资产、退役资产、新的漏洞、新的攻击技术等，以便及时调整安全防护策略。

2.2.2 攻击面管理能力目标的变化

随着用户对攻击面管理的深入理解和应用场景的不断增加，其需求也在不断增多。原有的攻击面管理目标正转化为以下新的目标：

- **资产治理优化。**大部分企业已经通过各种设备获取到相当数量的资产数据，如 HIS、EDR、WAF、CMDB 等，但是这些数据普遍问题存在数据重复、缺失、冲突等问题，需要对不同资产设备进行对接、融合和核对，实现资产管理“一张图”。

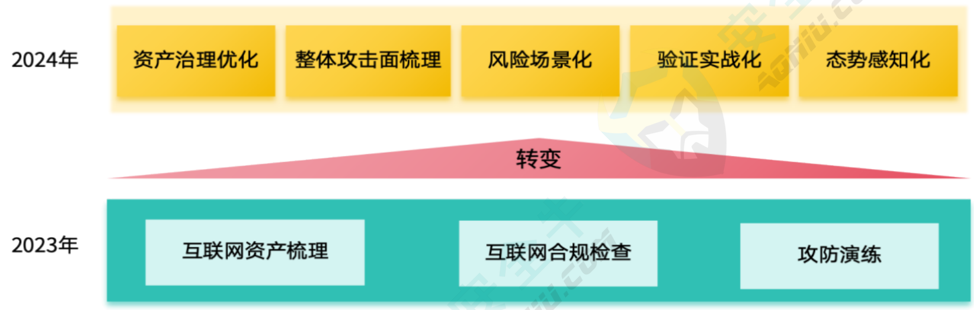
- **整体攻击面梳理。**攻击面管理需要将 CAASM 与 EASM 的数据进行融合，打破内外网边界，实现对企业整体攻击面的全面管理。

- **风险场景化。**随着用户对攻击面的深入理解，不同行业的用户开始根据自身的安全需求和风险特点，提出实际需求，厂商也正朝着行业深耕的方向发展，针对金融、能源、政府等不同行业提供差异化的解决方案。

- **验证实战化。**攻击面管理要更加贴近实战，能够帮助用户模拟真实的攻击场景，并验证安全防御体系的有效性。

- **自动化和智能化。**攻击面管理需要自动化和智能化的工具来提高效率和效果，例如自动化资产发现、自动化漏洞扫描、智能化风险评估、自动化的安全防护等。

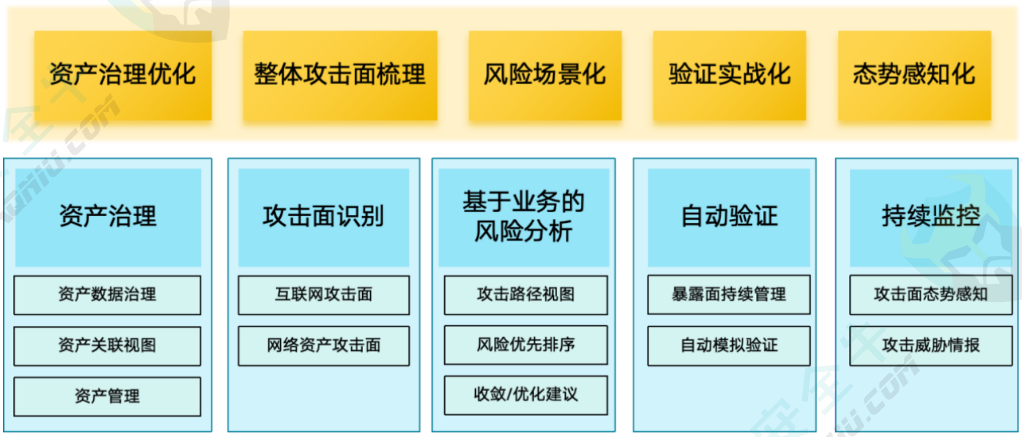
- **产品服务化。**攻击面管理功能要能提供相应的产品服务和专家服务的形式提供，用户可以借助专家能力，以及便捷灵活地获取攻击面管理能力，降低部署和维护成本。



攻击面管理能力目标

2.3 攻击面管理的能力框架

攻击面管理目标从之前主要针对 IT 资产和互联网资产识别，转变为整体攻击面的持续可视化，对攻击面风险开展常态化监控和管理，实现降低风险暴露，提升安全防护能力。



攻击面管理的能力框架

◎ **攻击面管理成功的关键因素：**

- **资产数据和关联要全和准。**攻击面管理的首要任务是全面、准确地识别和管理企业的所有资产，需要攻击面管理系统具备强大的资产发现能力，并准确识别资产的属性信息，同时，攻击面管理系统还需要能够识别资产之间的关联关系，以便于进行攻击路径的识别。
- **攻击面需要“管理 + 技术”。**攻击面管理不仅仅是技术问题，也需要管理手段的配合。企业需要建立明确的攻击面管理策略和标准，例如影子资产 / 违规资产的定义、风险评估标准、安全加固标准等。
- **攻击面需要安全与运维协同。**攻击面管理需要安全团队和 IT 运维团队的协同配合，才能有效地进行资产管理、攻击面闭环管理等。

- **企业需要有一定的基础设施基础。**攻击面管理的实施需要企业具备一定的基础设施基础，攻击面管理系统需要能够与这些基础设施进行集成，才能发挥最大的价值。

◎ **攻击面管理能力之一“资产治理”的特点：**

- **互联网资产识别更全面。**攻击面管理应能够识别企业所有面向互联网的资产，包括组织架构、域名、IP 地址、子域名、SSL 证书、Web 应用程序、API 接口、数字资产、仿冒资产等，并能够持续监控这些资产的变化，及时发现新增资产、失效资产和变更资产等。

- **网络资产数据更完整。**攻击面管理应能够识别企业内部网络中的所有资产，包括互联网资产、IT 影子资产、设备、中间件、应用系统等，并能够识别资产之间的关联关系，例如网络拓扑结构、版本号、供应商等。

- **资产数据更准确。**攻击面管理应能够准确识别资产的属性信息，例如 IP 地址、MAC 地址、操作系统、开放端口、服务版本等，并能够及时更新资产信息，确保资产信息的准确性和完整性。

- **资产与业务关联更清晰。**攻击面管理应能够将资产与业务系统进行关联，例如识别某个 Web 应用程序属于哪个业务系统，某个服务器承载了哪些业务应用等，以便于进行风险评估和安全防护。

◎ **攻击面管理能力之二“攻击面识别”的特点：**

- **全面覆盖各种攻击向量。**攻击面管理应能够识别所有可能的攻击向量，包括漏洞、配置缺陷、弱口令、身份和访问管理缺陷、社会工程学攻击等。

- **攻击面路径图。**攻击面管理应能够绘制攻击面路径图，清晰地展示攻击者可能利用的攻击路径，并评估攻击成功的可能性。

◎ **攻击面管理能力之三“基于业务的风险分析”的特点：**

- **准确评估风险。**攻击面管理应能够对攻击面进行风险评估，识别高风险资产和漏洞，并能够准确计算风险评分。

- **科学分析风险。**攻击面管理应能够对风险进行分析和优先级排序，例如识别高风险资产和漏洞，确定修复的优先级。

- **风险可视化。**攻击面管理应能够对风险进行可视化展示，例如通过攻击路径图、风险热力图等方式展示风险，以便于用户理解和分析。

◎ **攻击面管理能力之四“自动验证”的特点：**

- **持续监控暴露面变化。**攻击面管理应能够持续监控暴露面的变化，例如新增暴露面、失效暴露面、变更暴露面等，并及时发出告警。

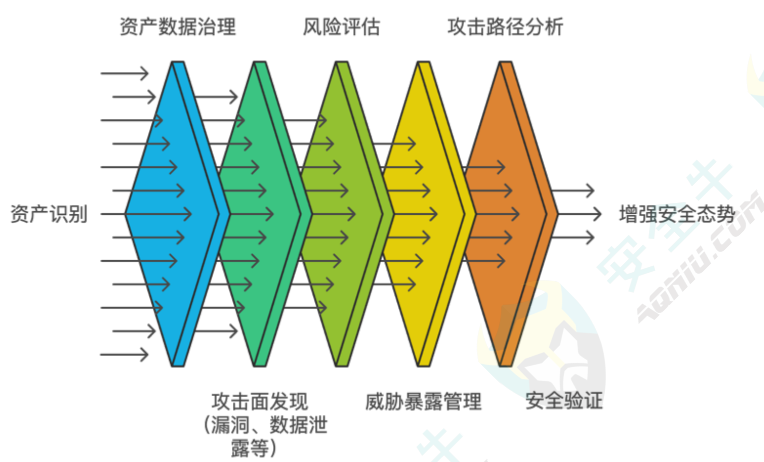
- **收敛攻击面。**攻击面管理应能够采取措施降低风险暴露，例如漏洞修复、安全加固、访问控制等，并能够验证安全控制措施的有效性，例如模拟攻击、渗透测试等。

◎ **攻击面管理能力之五“持续监控”的特点：**

- **持续验证。**攻击面管理应能够持续验证安全控制措施的有效性，并根据验证结果进行调整和改进。
- **自动化。**攻击面管理应能够自动化执行攻击面收敛和验证操作，例如自动化漏洞修复、自动化安全加固等。
- **攻击面态势感知。**应实时感知企业的攻击面态势，例如当前面临的威胁、攻击者的活动轨迹、攻击的影响范围等，并提供态势分析报告和可视化展示。

2.4 关键技术

为了支撑新的攻击面管理能力框架，攻击面管理的关键技术涵盖了资产识别、漏洞扫描、风险评估、持续威胁暴露管理、攻击路径分析、入侵和攻击模拟等多个方面。了解这些技术的实现原理，可以帮助企业更好地理解和应用攻击面管理，从而降低安全风险，提升安全防护能力。



攻击面管理关键技术

攻击面管理的关键技术有以下：

（1）资产识别技术

- **主动扫描技术。**通过发送网络探测数据包（例如 ping、TCPSYN 等），来探测目标网络中的活动主机和开放端口，并识别主机的操作系统、服务类型等信息。例如，使用 Nmap 工具扫描目标网络，可以发现网络中的主机、开放端口、操作系统、服务版本等信息。

- **被动扫描技术。**通过监听网络流量（例如 ARP 请求、DNS 查询等），来识别网络中的活动主机和开放端口，并识别主机的操作系统、服务类型等信息。例如，使用 tcpdump 工具监听网络流量，可以分析流量中的主机信息和服务信息。

- **网络空间测绘技术。**通过对互联网上的资产进行扫描和探测，例如 IP 地址、域名、网站等，来识别企业的外部资产和攻击面。例如，使用 Shodan 搜索引擎搜索企业的 IP 地址和域名，可以发现企业暴露在互联网上的资产和服务。

- **威胁情报技术。**通过收集和分析各种威胁情报，例如漏洞信息、攻击事件、恶意软件等，来识别与企业资产相关的威胁信息。例如，订阅威胁情报平台的漏洞信息，可以及时了解最新的漏洞信息，并识别企业资产中受影响的资产。

- **Agent 技术。**在终端设备上安装 Agent 程序，收集终端设备的信息，例如操作系统、硬件配置、软件安装情况等，并将其上传到攻击面管理平台。

以上具体可参见安全牛《攻击面管理应用技术指南 2023 版》中相关内容。

（2）资产数据质量治理技术

- **集成现有资产数据。**与企业现有的安全产品进行对接，例如 WAF、CMDB、EDR 等，读取其中的资产数据并集中存储。

- **融合。**采用数据融合技术，将不同来源的资产数据进行融合，例如根据资产的唯一标识符进行融合，并解决数据冲突问题，例如华云安的攻击面管理平台，支持对多种数据源的资产数据进行融合，包括 CMDB、漏洞扫描器、网络扫描器等，并能够识别和处理数据冲突，例如 IP 地址冲突、MAC 地址缺失等。

- **清洗。**对采集到的数据进行清洗，例如去除重复数据、纠正错误数据等，例如知其安的攻击面管理平台，支持对资产数据进行清洗，例如识别和删除重复资产、补充缺失的资产信息、纠正错误的资产属性等。

- **去重和异常处理。**对全部的资产数据进行清洗、去重和异常处理，形成资产清单。

（3）攻击面识别技术

攻击面发现技术用于识别和分析企业面临的各种安全风险和威胁，包括漏洞、配置缺陷、弱口令、数据泄露等。

- **漏洞扫描。**通过漏洞扫描工具对资产进行扫描，发现资产中存在的安全漏洞。例如，使用漏洞扫描器对服务器进行漏洞扫描，发现服务器中存在的漏洞，并评估漏洞的风险等级。

- **配置检查。**通过配置检查工具对资产进行检查，发现资产中存在的配置缺陷，例如，网络设备中存在的弱口令、默认账户等安全风险。

- **敏感信息识别。**通过敏感信息识别工具对资产进行扫描，发现资产中存在的敏感信息，例如机密文件、源代码、数据库密码等的存储位置和访问权限。
- **数据泄漏检测。**通过数据泄漏检测工具对网络流量进行监控，关注文件的上传、下载、邮件发送等，发现数据泄露行为，例如使用网络流量分析工具监控企业网络流量，发现是否有机密文件通过邮件发送到外部。
- **威胁情报。**通过威胁情报平台获取最新的威胁情报，例如漏洞信息、攻击事件、恶意软件等，并用于攻击面管理。例如，订阅威胁情报平台的漏洞信息，及时了解最新的漏洞信息，并识别企业资产中受影响的资产。
- **暗网监控。**通过暗网监控工具对暗网进行监控，发现是否有企业敏感信息泄露到暗网。例如，使用暗网监控工具监控暗网论坛、交易平台等，发现是否有企业机密文件、数据库密码等敏感信息在暗网流通。

（4）风险评估技术

- **定量风险评估。**使用数学模型对风险进行量化评估，例如计算风险发生的概率和损失。例如，使用 CVSS 评分模型对漏洞进行风险评估，可以计算漏洞的风险评分，并根据风险评分对漏洞进行优先级排序。
- **定性风险评估。**对风险进行定性评估，例如评估风险的影响程度和可能性。例如，安全专家可以根据漏洞的类型、攻击的复杂度、影响的范围等因素，对漏洞进行定性评估。

（5）持续威胁暴露管理（CTEM）

- **持续的攻击面监控。**持续监控企业攻击面的变化，例如新增资产、变更资产、退役资产、新的漏洞、新的攻击技术等。
- **基于风险的优先级排序。**对威胁暴露进行风险评估，并根据漏洞的 CVSS 评分、漏洞的利用难度、漏洞的实际业务的影响范围等因素进行优先级排序。
- **多维度的安全验证。**使用多维度的安全验证，例如漏洞扫描、配置检查、渗透测试、入侵和攻击模拟等，以验证安全控制措施的有效性。例如模拟各种类型的攻击，例如勒索软件攻击、APT 攻击、DDoS 攻击等，以评估企业安全防御体系的有效性。
- **自动化的安全响应。**开展自动化的安全响应，例如自动下发漏洞修复指令、自动加固安全配置等，以提高安全响应效率。
- **持续的改进。**根据新的威胁和漏洞情报，持续改进攻击面管理方案，以确保企业始终处于安全状态。

（6）攻击路径分析技术

- **基于图论的攻击路径分析。**将网络拓扑结构和资产之间的连接关系表示为图，对网络拓扑结构进行自动发现和建

模，并结合漏洞信息、威胁情报等信息，分析攻击者可能利用的攻击路径，并评估攻击成功的可能性。例如，使用攻击路径分析工具可以分析攻击者从互联网到企业内网关键服务器的攻击路径，并识别攻击路径上的未打补丁的漏洞、弱口令等薄弱环节。

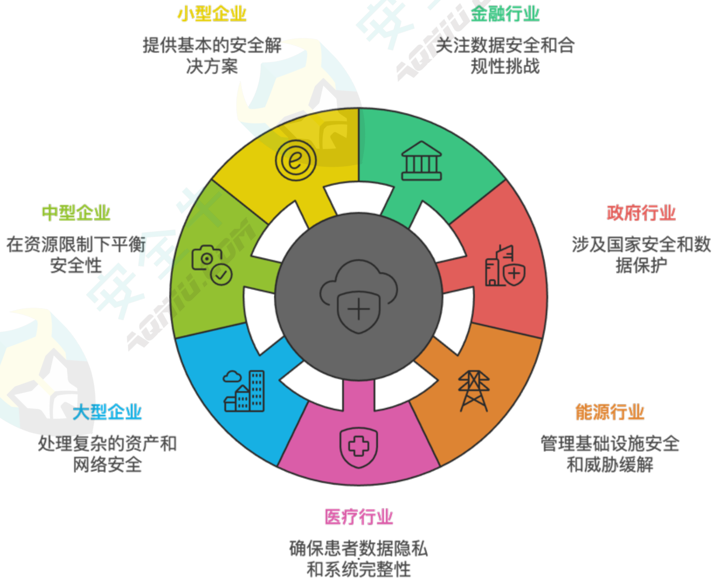
- **基于攻击链的攻击路径分析。**根据攻击链模型，分析攻击者可能采取的攻击步骤，并识别每个步骤可能利用的漏洞和攻击技术。例如，根据网络杀伤链模型（CyberKillChain），结合企业的实际情况和安全需求，分析攻击者从侦察、武器化、投递、利用、安装、指挥与控制、行动到目标的攻击步骤，并识别每个步骤可能利用的漏洞和攻击技术。
- **攻击路径可视化。**将攻击路径分析的结果以图形化的方式展示出来，例如攻击路径图、攻击树等，以便于用户理解和分析。例如，使用攻击路径图可以清晰地展示攻击者可能利用的攻击路径、攻击路径上的薄弱环节，以及攻击成功的可能性。

（7）入侵和攻击模拟（BAS）

- **模拟攻击。**模拟各种类型的攻击，例如模拟攻击者利用社会工程学手段获取初始访问权限、模拟攻击者在内网进行横向移动，以及勒索软件攻击、APT 攻击、DDoS 攻击等，以评估企业安全防御体系的有效性。
- **攻击路径分析。**分析攻击者可能利用的攻击路径，并识别薄弱环节。例如，利用 BAS 分析攻击者从互联网到企业内网重要服务器的攻击路径，并识别攻击路径上的薄弱环节，例如未打补丁的漏洞、弱口令等。
- **安全验证。**验证安全控制措施的有效性，例如防火墙、入侵检测系统等。例如，利用 BAS 模拟攻击者对防火墙进行攻击，测试防火墙是否能够有效地拦截攻击流量。
- **安全评估。**对企业的整体安全状况进行评估，并提供改进建议。例如，根据模拟攻击的结果，评估企业安全防御体系的整体安全状况，并提供改进建议，例如加强安全意识培训、优化安全策略、部署新的安全设备等。

第三章 攻击面管理应用场景分析

攻击面管理的应用场景非常广泛，不同行业和规模的用户对攻击面管理的需求存在差异，攻击面管理产品和服务需要针对用户的实际需求进行交付，才能更好地满足用户的需求，帮助用户提升安全防护能力，接下来我们将从不同的行业用户场景和企业规模进行举例说明。



攻击面管理应用场景

3.1 行业用户场景

（1）金融行业

金融行业对数据安全和合规性要求较高，并且业务系统复杂，攻击面广泛。金融行业经常面临来自外部攻击、内部威胁、数据泄露等多方面的安全挑战，具有难全面识别攻击面，难以有效地规避安全风险、满足日益严格的安全合规要求等痛点。金融行业经常遭受网络钓鱼攻击造成用户信息泄露，遭受因系统漏洞攻击而造成银行系统中断，遭受勒索软件攻击而造成数据丢失。

◆ **攻击面管理场景：**

- 敏感数据发现和保护。
- 外部攻击面管理。
- 应用系统漏洞扫描和安全加固。

- API 识别、测试和防护。

◆ **攻击面管理目标：**

- 全面识别和管理金融机构的攻击面，包括外部攻击面和内部攻击面。
- 及时发现和缓解安全风险，防止数据泄露和业务中断。
- 满足金融行业的安全合规要求等。

（2）政府行业

政府行业是国家关键信息基础设施的重要组成部分，其安全关系到国家安全和社会稳定。政府行业常拥有大量的关键信息基础设施，例如政府网站、政务系统等。存储和处理大量的敏感政府数据，例如公民个人信息、政府机密文件等。面临来自 APT 攻击、网络恐怖主义等多方面的安全挑战。可能遭受政府网站、政务系统等攻击，窃取敏感政府数据等。

◆ **攻击面管理场景：**

- 资产识别和风险评估。
- 漏洞扫描、安全加固和入侵检测。
- 数据安全和隐私保护。
- 安全合规检查。

◆ **攻击面管理目标：**

- 全面识别和管理政府部门的攻击面，包括外部攻击面和内部攻击面。
- 及时发现和缓解安全风险，防止数据泄露和业务中断。
- 满足政府行业的安全合规要求，例如等级保护制度等。

（3）能源行业

能源行业是国家关键基础设施的重要组成部分，其安全关系到国家能源安全和经济发展。能源行业拥有大量的关键信息基础设施，例如电力系统、石油管道等。并且工业控制系统（ICS）和运维技术（OT）环境复杂，安全防护难度大。常面临能源关键基础设施攻击，能源生产中断，例如攻击电力系统导致大规模停电、攻击石油管道导致石油泄漏等。

◆ **攻击面管理场景：**

- ICS 和 OT 资产的识别和风险评估。
- 漏洞扫描、安全加固和入侵检测。
- 异常行为检测和安全事件响应。
- 与工业控制系统安全防护技术的集成。

◆ **攻击面管理目标：**

- 全面识别和管理能源行业的攻击面，包括 IT 攻击面和 OT 攻击面。
- 及时发现和缓解安全风险，防止网络攻击和物理破坏。
- 保障能源生产和供应的安全稳定运行。

（4）医疗行业

医疗行业涉及大量的敏感医疗数据，例如患者个人信息、病历等，其安全和隐私保护至关重要。并且医疗设备和系统种类繁多，安全防护难度大。可能遭受医疗机构的网络系统被攻击，窃取敏感医疗数据，影响医疗服务的正常开展。

◆ **应用攻击面管理的场景：**

- 医疗数据的发现和分类。
- 数据安全和隐私保护。
- 医疗设备和系统的漏洞扫描和安全加固。
- 安全事件响应和应急处置。

◆ **攻击面管理目标：**

- 全面识别和管理医疗机构的攻击面，包括外部攻击面和内部攻击面。
- 及时发现和缓解安全风险，防止数据泄露和业务中断。
- 满足医疗行业的安全合规要求，例如 HIPAA 等。

3.2 企业规模分类

（1）大型企业

大型企业的资产数量众多，类型多样，包括传统 IT 资产、云资产、物联网设备、OT 设备等，并且网络环境复杂，包括物理网络、虚拟化网络、云网络等，同时安全防护体系较为完善，但面临的安全挑战也更大。大型企业由于资产数量众多、网络环境复杂，大型企业面临的攻击面广泛，容易成为攻击者的目标。

◆ **攻击面管理场景：**

- 全面识别和管理企业的攻击面，包括所有类型的资产和网络环境
- 对攻击面进行精细化的风险评估，并根据风险评估结果进行优先级排序
- 动化地执行攻击面收敛操作，例如自动化漏洞修复、自动化安全配置加固等
- 将攻击面管理平台与现有的安全体系进行联动，例如与 SOC、SIEM、SOAR 等平台进行集成

◆ **攻击面管理应用建设**

大型企业由于其 IT 环境和安全需求的复杂性，攻击面管理的建设需要分阶段逐步推进。

◎ **第一阶段：攻击面可视化**

◆ **应用攻击面管理的场景：**

- 全面识别和管理企业的攻击面，包括所有类型的资产和网络环境。
- 对攻击面进行初步的风险评估，识别高风险资产和漏洞。
- 将攻击面管理平台与现有的安全体系进行初步联动，例如与 SOC、SIEM 等平台进行集成。

◆ **攻击面管理目标：**

- 建立统一的攻击面视图，全面了解企业的资产状况、安全风险和攻击面暴露情况。
- 初步实现攻击面的可视化和风险的识别。

◆ **关键点：**

- 资产发现和攻击面识别能力。

- 基本的风险评估和攻击路径分析能力。
- 与其他安全产品和平台的初步集成能力。

◎ **第二阶段：攻击面风险管理**

◆ **应用攻击面管理的场景：**

- 对攻击面进行精细化的风险评估，并根据风险评估结果进行优先级排序。
- 自动化地执行部分攻击面收敛操作，例如自动化漏洞修复、自动化安全配置加固等。
- 加强与现有安全体系的联动，例如与 SOAR 等平台进行集成，实现安全事件的自动化响应。

◆ **攻击面管理目标：**

- 有效地管理安全风险，降低安全事件发生的概率。
- 提高安全运营效率，降低安全运营成本。

◆ **关键点：**

- 精细化的风险评估和攻击路径分析能力。
- 自动化的攻击面收敛和安全加固能力。
- 与其他安全产品和平台的深度集成能力。

◎ **第三阶段：攻击面持续监控与优化**

◆ **应用攻击面管理的场景：**

- 持续监控攻击面的变化，及时发现新的风险和威胁。
- 持续优化攻击面管理策略和流程，提高攻击面管理的效率和有效性。
- 将攻击面管理融入企业的整体安全体系中，实现安全运营的闭环管理。

◆ **攻击面管理目标：**

- 持续降低风险暴露，提升安全防护能力。

- 实现安全与业务的平衡发展。
- 满足安全合规要求，提升企业安全形象。

◆ **关键点：**

- 持续监控和攻击面态势感知能力。
- 安全运营和自动化响应能力。
- 与其他安全产品和平台的深度融合能力。

（2）中型企业

中型企业的资产数量适中，类型多样，一般包括传统 IT 资产、云资产等，但是网络环境较为复杂，包括物理网络、虚拟化网络等。安全防护体系处于建设阶段，安全防护能力有待提升。安全预算和人力资源有限，通常没有专门的安全团队，安全人员需要兼顾多种安全工作。由于安全防护能力相对薄弱，缺乏专业的安全管理工具和平台，安全人员缺乏专业的安全知识和技能，中型企业容易成为攻击者的目标。可能遭受勒索软件、钓鱼邮件等攻击。并难以对攻击面进行全面、有效的管理，难以应对复杂的网络安全威胁。

◆ **应用场景：**

- 覆盖关键的资产和攻击面，例如面向互联网的资产、关键业务系统等。
- 对关键攻击面进行风险评估，并能够根据风险评估结果进行优先级排序。
- 自动化地执行安全加固操作，例如漏洞修复、安全配置加固等。
- 选择易于使用的攻击面管理平台，以便于安全团队快速上手和操作。

◆ **攻击面管理目标：**

- 降低安全风险，提高安全防护能力。
- 提高安全运营效率，降低安全运营成本。
- 满足基本的安全合规要求。

◆ **关键点：**

- 实用性和易用性。

- 成本效益。
- 自动化的安全加固能力。
- 基本的风险评估和攻击面可视化能力。

（3）小型企业

小型企业的资产数量较少，类型相对单一，主要包括传统 IT 资产和一些基础的云服务。安全防护能力薄弱，通常只部署了一些基础的安全设备，例如防火墙、杀毒软件等。缺乏专业的安全团队和充足的安全预算，安全意识和安全投入不足。

◆ **应用场景：**

- 对企业的基本攻击面进行可视化，例如面向互联网的资产、主要的网络设备等。
- 对主要的攻击面进行风险评估，并能够识别主要的风险。
- 获得安全加固建议，例如漏洞修复建议、安全配置建议等。
- 得外部的安全服务，例如漏洞扫描服务、渗透测试服务等。

◆ **攻击面管理目标：**

- 降低安全风险，提高基本的安全防护能力。
- 满足基本的安全合规要求。

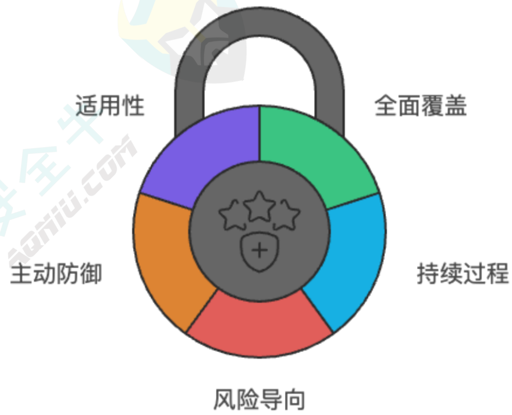
◆ **关键点：**

- 使用易用和低成本的 Saas 在线自助服务
- 利用第三方专家安全服务。

第四章 攻击面管理应用实施方法

4.1 攻击面管理实施原则

在构建攻击面管理体系的过程中，企业需要遵循一些关键原则，才能确保攻击面管理体系的有效性和可持续性。以下是一些建议的攻击面管理实施建设原则：

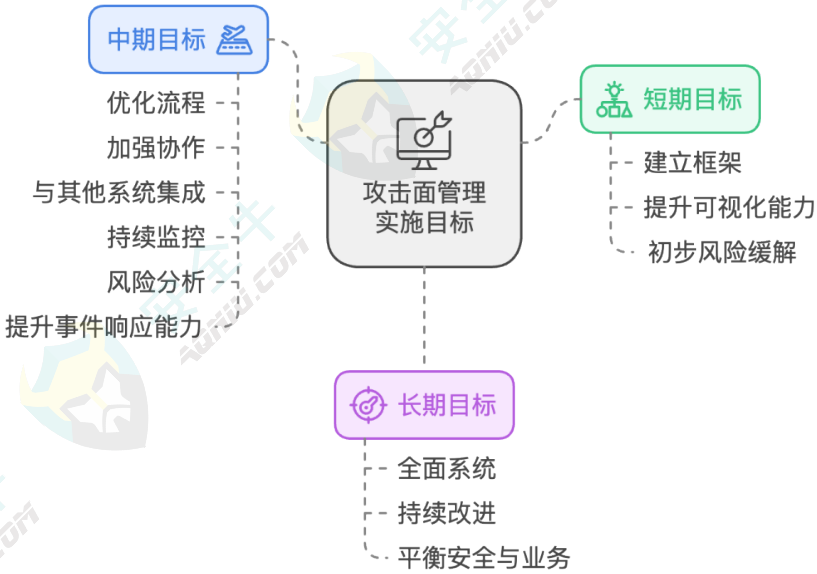


攻击面管理实施原则

- 全面性原则。应覆盖所有的攻击面，包括内部和外部攻击面、传统 IT 资产和新兴 IT 资产（如云资产、物联网设备、OT 设备等），以及第三方攻击面（如供应链、合作伙伴等）。
- 持续性原则。攻击面管理应是一个持续的过程，而不是一次性的活动。
- 风险导向原则。攻击面管理应以风险管理为核心，识别、评估和控制网络安全风险。应将有限的资源集中到高风险的攻击面上。
- 主动防御原则。攻击面管理应强调主动发现和防御，例如通过模拟攻击、漏洞验证、威胁情报等手段来识别和降低风险。
- 适应性原则。应根据企业的具体情况进行调整和优化，例如企业的规模、行业、安全需求等。
- 自动化原则。应尽可能地自动化攻击面管理流程，例如自动化资产发现、自动化漏洞扫描、自动化风险评估等。
- 智能化原则。应积极探索人工智能（AI）技术在攻击面管理中的应用，例如自动化资产发现、智能化风险评估、自动化的安全防护等。
-

4.2 攻击面管理实施目标

攻击面管理实施建设的目标应根据企业的实际情况和安全需求进行制定，并分解为短期、中期和长期目标，逐步推进，最终实现降低风险暴露，提升安全防护能力的目标，攻击面管理实施建设的目标应与企业的整体安全战略和业务目标相一致。一般来说，攻击面管理实施建设的目标可以分解为以下几个层次：



攻击面管理实施目标

1. 短期目标

（1）建立攻击面管理体系框架：

- 明确攻击面管理的范围、职责和流程。
- 建立攻击面管理的组织架构和人员配备。
- 选择合适的攻击面管理工具和平台。

（2）提升攻击面可视化能力：

- 全面识别和梳理企业所有资产，包括 IT 资产、OT 资产、云资产、IoT 设备等。
- 识别所有可能的攻击向量，包括漏洞、配置缺陷、弱口令等。
- 对攻击面进行风险评估，识别高风险资产和漏洞。

（3）初步实现攻击面风险的收敛：

- 针对高风险资产和漏洞，采取措施进行缓解和处置，例如漏洞修复、攻击面收敛、访问控制等。
- 验证安全控制措施的有效性，例如模拟攻击、渗透测试等。

2. 中期目标

（1）完善攻击面管理体系：

- 优化攻击面管理流程，提高效率和准确性。
- 加强跨部门的沟通和协作，例如安全团队、IT 运维团队、业务部门等之间的协作。
- 将攻击面管理与其他安全技术和平台进行集成，例如与漏洞管理、威胁情报、安全运营中心（SOC）等平台进行集成和联动。

（2）提升攻击面风险的管理水平：

- 持续监控攻击面的变化，例如新增资产、变更资产、退役资产、新的漏洞、新的攻击技术等。
- 对风险进行分析和优先级排序，例如识别高风险资产和漏洞，确定修复的优先级。
- 对风险进行可视化展示，例如通过攻击路径图、风险热力图等方式展示风险。

（3）提升安全事件响应能力：

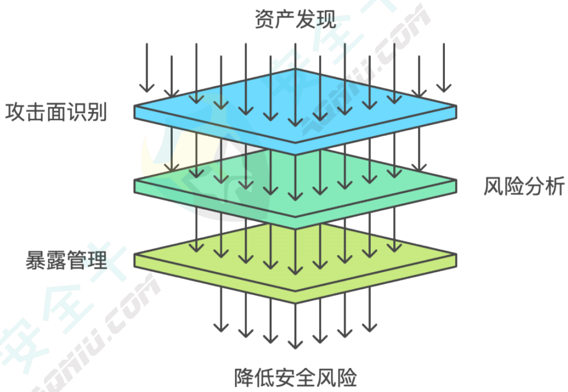
- 对安全事件进行响应和处置，例如安全事件的识别、分析、响应和恢复等。
- 对安全事件进行溯源和分析，例如识别攻击源、攻击路径、攻击目标等。

3. 长期目标

- 构建全面、持续、有效、主动、协同、自动化、智能化和适应性的攻击面管理体系。
- 持续降低风险暴露，提升安全防护能力。
- 实现安全与业务的平衡发展。
- 满足安全合规要求，提升企业安全形象。

4.3 攻击面管理实施思路与方法

构建一个完善的攻击面管理平台架构，可以帮助企业有效地实施攻击面管理，降低安全风险，提升安全防护能力。以下是一个建议的攻击面管理系统架构，以及每个部分应实现的功能：



攻击面管理主要功能

（1）资产发现

资产发现可以通过主动扫描发现、被动流量发现和集成数据等方式。

◎ 主动发现：配置扫描的 IP 地址范围、端口范围、协议等。

- 建议进行全面的资产发现，包括所有网络区域和设备类型。
- 例如，可以将企业的整个内网 IP 地址段配置为扫描范围，并扫描所有常见的端口，例如 80、443、3389 等。

◎ 被动发现：配置网络流量镜像，将网络设备的流量镜像到攻击面管理平台。

- 被动发现可以发现主动扫描无法发现的资产，例如隐藏在 NAT 后面的资产。
- 例如，可以将核心交换机的流量镜像到攻击面管理平台，以便于平台收集和分析网络流量，识别网络中的资产。
- 集成现有安全产品数据：集成现有安全产品数据，融合处理形成资产清单
- 与企业现有的安全产品进行对接，例如 WAF、CMDB、EDR 等，读取其中的资产数据并集中存储。
- 对全部的资产数据进行清洗、去重和异常处理，形成资产清单。
- 针对资产清单实现资产之间、资产与业务的关联，根据业务的重要性进行责任人和重要性标记。

◆ **关键点：**

- 资产发现的全面性和准确性：应尽可能地发现所有资产，并准确识别资产的类型、属性、位置等信息。
- 资产数据的融合和清洗：对收集的资产数据进行融合、清洗，以形成没有数据错误、完整的资产列表。
- 资产分类和标记的合理性：根据企业的实际情况和安全需求，对资产进行合理的分类和标记，以便于后续的风险评估和安全防护。
- 资产管理的自动化和智能化：尽可能地自动化资产管理流程，例如自动化资产发现、自动化资产分类、自动化资产变更管理等。

（2）攻击面识别

攻击面识别是指识别所有可能被攻击者利用的攻击向量，例如漏洞、配置缺陷、弱口令、身份和访问管理缺陷等。攻击面识别是攻击面管理的重要环节，只有识别出所有可能的攻击向量，才能有效地进行风险评估和安全防护。

◎ 漏洞扫描：对资产进行漏洞扫描，发现资产中存在的安全漏洞，例如 Web 漏洞、操作系统漏洞、数据库漏洞等。

- 配置漏洞扫描策略，例如扫描的频率、漏洞库、扫描插件等。
- 对漏洞扫描结果进行分析和评估，例如识别高危漏洞、分析漏洞趋势等。
- 例如，可以使用 Nessus 漏洞扫描器对服务器进行漏洞扫描，发现服务器中存在的漏洞，并评估漏洞的风险等级。

◎ 配置检查：对资产进行配置检查，发现资产中存在的配置缺陷，例如弱口令、未授权访问等。

- 配置检查策略，例如检查的规则、检查的频率等。
- 对配置检查结果进行分析和评估，例如识别不安全的配置、分析配置缺陷趋势等。
- 例如，可以使用漏洞扫描器对网络设备进行配置检查，发现网络设备中存在的弱口令、默认账户等安全风险。

◎ 数字风险识别：通过威胁情报分析、数据泄露监测、网络爬虫等技术手段，识别和评估数字风险，例如钓鱼攻击、数据泄露、品牌仿冒等。

- 配置数字风险识别策略，例如监控的渠道、监控的频率等。
- 对数字风险识别结果进行分析和评估，例如识别高风险的数字风险、分析数字风险趋势等。
- 例如，使用数据泄露监测平台监控暗网、社交媒体等渠道，发现是否有企业敏感数据泄露。

◎ 第三方风险识别：通过收集和分析第三方的安全信息，识别和评估第三方风险，例如供应链攻击、合作伙伴安全

风险等。

- 配置第三方风险识别策略，例如评估的指标、评估的频率等。
- 对第三方风险识别结果进行分析和评估，例如识别高风险的第三方、分析第三方风险趋势等。
- 例如，对供应商进行安全评估，了解供应商的安全状况，并识别潜在的供应链安全风险。

◆ **关键点：**

- 识别方法的全面性和有效性：攻击面识别应采用多种方法，例如漏洞扫描、配置检查、威胁情报分析等，并确保方法的有效性。
- 识别结果的准确性和及时性：攻击面识别应尽可能准确识别所有可能的攻击向量，并及时发现新的攻击向量。
- 识别结果的可视化和易用性：攻击面识别结果应易于理解和使用。

（3）攻击面风险分析

攻击面风险分析是指对攻击面进行风险评估，识别高风险资产和漏洞，并进行优先级排序。风险分析是攻击面管理的核心环节，只有准确地评估风险，才能有效地进行安全防护。

◎ 风险评估：对资产和漏洞进行风险评估，例如根据资产的重要性、漏洞的严重程度、威胁情报等因素进行评估，并计算风险评分。

- 选择合适的风险评估模型，例如 CVSS 评分模型、DREAD 模型等。
- 配置风险评估参数，例如资产的重要性权重、漏洞的严重程度权重等。
- 例如，可以使用风险评估模型对服务器和漏洞进行风险评估，例如根据 CVSS 评分模型，评估服务器中存在的漏洞的风险等级。

◎ 风险优先级排序：根据风险评分、资产的重要性、业务影响等因素，对风险进行优先级排序，以便于企业进行风险处置。

- 配置风险优先级排序规则，例如根据风险评分、资产的重要性、业务影响等因素进行排序。
- 例如，将风险评分较高的漏洞优先进行修复，将影响关键业务系统的漏洞优先进行处理。

◎ 风险可视化：对风险进行可视化展示，例如通过攻击路径图、风险热力图等方式展示风险，以便于用户理解和分析。

- 选择合适的风险可视化工具，例如攻击路径图、风险热力图等。
- 配置风险可视化参数，例如显示的指标、颜色等。
- 例如，使用攻击路径图展示攻击者可能利用的攻击路径，使用风险热力图展示企业网络中风险资产的分布情况。

◆ **关键点：**

- 风险评估的准确性和全面性：应尽可能准确评估风险，并考虑各种因素，例如资产的重要性、漏洞的严重程度、威胁情报等。
- 风险分析的科学性和有效性：应采用科学的风险分析方法，例如定量分析、定性分析等，并能够有效地识别高风险资产和漏洞。
- 风险可视化的直观性和易用性：风险可视化应易于理解和使用，并能够帮助用户快速了解企业的风险信息。

（4）暴露面管理

暴露面管理应识别和管理企业所有面向互联网的暴露面，例如域名、IP 地址、Web 应用程序、API 接口等，并对暴露面进行风险评估和安全加固。

◆ **功能：**

- 自动发现和识别企业的互联网暴露面，例如域名、IP 地址、Web 应用程序、API 接口等。
- 对暴露面进行风险评估，例如识别暴露面中存在的漏洞、配置缺陷、弱口令等。
- 对暴露面进行安全加固，例如修复漏洞、改进安全配置、加强访问控制等。
- 持续监控暴露面的变化，例如新增暴露面、失效暴露面、变更暴露面等。

◆ **关键点：**

- 暴露面发现的全面性和准确性：应尽可能地发现所有暴露面，并准确识别暴露面的类型、属性、位置等信息。
- 风险评估的准确性和及时性：应尽可能准确评估暴露面的风险，并及时发现新的风险。
- 安全加固的有效性和及时性：应采取有效的措施对暴露面进行安全加固，并及时修复新的漏洞和安全隐患。
- 监控的实时性和全面性：应实时监控暴露面的变化，并及时发现新增暴露面、失效暴露面、变更暴露面等。

（5）攻击面验证

攻击面验证应验证企业安全防御体系的有效性，例如通过模拟攻击、渗透测试等方式，发现企业网络中存在的安全漏洞和风险。

◆ **功能：**

- 支持多种攻击面验证方法，例如模拟攻击、渗透测试、漏洞扫描等。
- 提供攻击面验证报告，例如安全评估报告、渗透测试报告等。
- 支持对攻击面验证结果进行分析和评估，例如识别仍然存在的安全风险，并提出改进建议。

◆ **关键点：**

- 验证方法的科学性和有效性：应采用科学的验证方法，例如模拟攻击、渗透测试、漏洞扫描等，并能够有效地评估安全防御体系的有效性。
- 验证结果的准确性和全面性：应尽可能准确评估安全防御体系的有效性，并覆盖所有关键资产和攻击面。
- 验证流程的自动化和智能化：尽可能地自动化验证流程，例如自动化模拟攻击、自动化漏洞扫描等。

（6）攻击面监控

监控建设应实时监控企业的攻击面信息，例如资产的变化情况、漏洞的变化情况、网络流量的异常情况等，并及时发出告警。

- 实时采集和分析企业的攻击面信息，例如资产信息、漏洞信息、网络流量信息等。
- 支持自定义监控指标和告警规则，例如可以根据企业的实际情况和安全需求，自定义监控的指标和告警的阈值。
- 提供多种告警方式，例如邮件告警、短信告警、微信告警等。
- 提供监控报表和趋势分析，例如可以查看资产的变化趋势、漏洞的变化趋势、网络攻击的趋势等。

◆ **关键点：**

- 监控的全面性和实时性：应尽可能地监控所有攻击面信息，并实时采集和分析数据。
- 告警的准确性和及时性：应尽可能地避免误报和漏报，并及时发出告警。
- 监控报表的直观性和易用性：监控报表应易于理解和使用，并能够帮助用户快速了解企业的攻击面态势。

（7）攻击态势感知的建设

攻击态势感知应实时感知企业的攻击面态势，例如当前面临的威胁、攻击者的活动轨迹、攻击的影响范围等，并提供态势分析报告和可视化展示。

- 实时采集和分析企业的攻击面信息，例如资产信息、漏洞信息、网络流量信息、威胁情报信息等。
- 关联分析不同来源的数据，例如将漏洞信息与资产信息进行关联，将威胁情报信息与网络流量信息进行关联等。
- 识别攻击者的活动轨迹，例如识别攻击者的 IP 地址、攻击手法、攻击目标等。
- 评估攻击的影响范围，例如评估攻击可能造成的损失、影响的业务系统等。
- 提供态势分析报告和可视化展示，例如攻击面态势图、攻击路径图、攻击事件时间线等。

◆ **关键点：**

- 态势感知的准确性和实时性：应尽可能准确感知企业的攻击面态势，并实时更新态势信息。
- 态势分析的科学性和有效性：应采用科学的态势分析方法，例如攻击链分析、威胁情报分析等，并能够有效地识别安全威胁和风险。
- 态势展示的直观性和易用性：态势展示应易于理解和使用，并能够帮助用户快速了解企业的攻击面态势。

4.4 攻击面管理应用挑战与建议

组织在实施攻击面管理时常面临多方面挑战，包括对底层资产数据的准确收集与持续更新难题、不同安全工具与平台之间数据孤岛与整合困难、无法准确全面地识别攻击面，以及攻击面风险评价不准确等。针对这些问题，安全牛根据调研结果和研究发现，将给出相关参考建议。

（1）挑战：企业已经有 CMDB、SOC 了，那么是否还需要攻击面管理呢？

安全牛建议：攻击面管理与 CMDB、SOC 等不同，CMDB 侧重于 IT 资产的管理，SOC 侧重于安全事件的监控和响应，而攻击面管理则侧重于从攻击者的视角来识别、评估和管理安全风险，三者共同构成了企业安全防护体系的重要组成部分。

- CMDB vs CAASM：CMDB（配置管理数据库）侧重于 IT 资产的管理，记录和跟踪资产的配置信息、生命周期等，主要用于 IT 运维管理。而 CAASM（网络资产攻击面管理）则侧重于 IT 资产的安全属性，例如漏洞、配置缺陷、风险等级等，主要用于安全风险管理。
- 资产风险运营 vs SOC：资产风险运营是通过检查来提前发现潜在的安全隐患，并及时采取措施进行管理。而 SOC（安全运营中心）是通过实时监控和分析来发现正在发生的安全事件和响应安全威胁。

（2）挑战：对接其他安全产品（如 WAF、CMDB、EDR 等）进行资产数据的收集时，资产数据的多源异构和数据冲突。例如 IP 地址不一样、MAC 地址缺失等。

安全牛建议，造成的原因主要是不同安全产品采集资产信息的维度和方式不同，导致数据存在差异和冲突，企业应：

- 数据标准化：建立统一的资产数据标准，对不同来源的数据进行标准化处理，例如统一 IP 地址的格式、MAC 地址的格式等。
- 数据融合：采用数据融合技术，将不同来源的资产数据进行融合，例如根据资产的唯一标识符进行融合，并解决数据冲突问题。
- 数据质量控制：对资产数据进行质量控制，例如识别和处理重复资产、缺失资产、数据冲突等问题。

（3）挑战：无法准确全面地识别攻击面，例如未授权的访问路径等。

安全牛建议：造成的原因主要是攻击面的复杂性和动态性，以及用户对攻击面缺乏了解等因素，导致攻击面识别的准确性和全面性不足，企业应：

- 采用多种攻击面识别技术：结合多种攻击面识别技术，例如漏洞扫描、配置检查、威胁情报分析、攻击路径分析等，以提高攻击面识别的准确性和全面性。
- 持续监控攻击面变化：持续监控攻击面的变化，例如新增资产、变更资产、退役资产、新的漏洞、新的攻击技术等，并及时更新攻击面信息。
- 加强安全意识培训：加强对员工的安全意识培训，提高员工对攻击面的认识和防范意识。

（4）挑战：攻击面风险评价不准确，例如难以评估风险的严重程度、难以确定风险的优先级等。

安全牛建议，造成的原因主要是风险评估的因素众多、数据来源分散、分析方法复杂等因素，以及用户缺乏风险评估的经验和知识等，导致风险评估的准确性和有效性不足，企业应：

- 建立科学的风险评估模型：根据企业的实际情况和安全需求，建立科学的风险评估模型，并选择合适的风险评估方法，例如定量风险评估、定性风险评估等。
- 采用威胁情报：采用威胁情报平台，例如威胁情报平台、安全运营中心（SOC）等，获取最新的威胁情报，并用于风险评估和分析。
- 风险可视化：对风险进行可视化展示，例如通过攻击路径图、风险热力图等方式展示风险，以便于用户理解和分析。

（5）挑战：用暴露面管理的处置效率低下。

安全牛建议，造成的原因主要是用户在处置暴露面风险时，只能依赖人工操作，效率低下，难以满足及时响应的需求，企业应：

- 采用具有自动化处置能力的平台处置暴露面风险，通过自动化、智能化、可视化的方式，帮助企业更好地掌控风险，有效解决暴露面风险处置效率低下的问题，提高企业的安全防护水平。例如绿盟科技的 CTEM 暴露面管理方案，可以提供自动化发现和识别资产、自动化风险评估和验证、智能化风险处置建议、自动化工单流转和协作和可视化风险管理和运营等功能。

第五章 人工智能攻击面应对初探

随着人工智能（AI）技术的快速发展和普及，AI 攻击面逐渐成为网络安全的新焦点。AI 技术不仅可以被攻击者利用来发起更复杂的攻击，也可能自身存在安全漏洞和风险。人工智能技术的发展带来了新的攻击面安全风险，包括 AI 模型、数据、应用和基础设施等方面。企业需要加强 AI 模型安全防护，保障 AI 数据安全，提升 AI 应用安全，加强 AI 基础设施安全，以应对 AI 攻击的威胁。

5.1 AI 攻击面威胁分析

AI 攻击面是网络安全的新兴领域，企业和组织需要充分认识 AI 攻击面的威胁风险，并采取相应的策略和措施进行防护，以保障 AI 系统的安全性和可靠性，AI 攻击面可以分为以下几个方面：

AI 攻击面威胁分析

5.1.1 AI 模型攻击面

AI 模型是智能化系统的核心，攻击者可以通过各种手段攻击 AI 模型，例如：

- **预训练模型污染：**攻击者在预训练模型中注入恶意数据或代码，导致模型在使用过程中出现错误或偏差，甚至被攻击者控制。例如，攻击者通过污染一个图像识别模型，使其将恶意软件识别为正常文件。
- **依赖库投毒：**攻击者在 AI 模型依赖的库中注入恶意代码，导致模型在调用库时执行恶意代码。例如，攻击者通过投毒一个 Python 库，导致所有使用该库的 AI 模型都被攻击。
- **数据投毒：**攻击者在训练数据中注入恶意数据，导致模型学习到错误的模式，从而在使用过程中出现错误或偏差。例如，攻击者可以向一个垃圾邮件过滤模型的训练数据中注入大量的正常邮件，导致模型将垃圾邮件识别为正常邮件。

- **对抗样本攻击：**攻击者通过对输入数据进行微小的修改，生成对抗样本，导致模型对对抗样本的识别出现错误。例如，攻击者可以对一张图片进行微小的修改，使其被一个图像识别模型识别为完全不同的物体。
- **模型窃取：**攻击者通过对模型进行逆向工程，窃取模型的结构和参数，从而复制模型或进行对抗样本攻击。例如，攻击者可以通过 API 访问一个 AI 模型，并收集模型的输入和输出数据，然后利用这些数据训练一个与目标模型功能相同的模型。

5.1.2 AI 数据攻击面

AI 系统依赖于大量的数据进行训练和推理，攻击者可以通过各种手段攻击 AI 数据，例如：

- **数据泄露：**攻击者窃取 AI 系统的训练数据或推理数据，例如个人信息、商业机密等，导致数据泄露和隐私侵犯。
- **数据污染：**攻击者篡改或破坏 AI 系统的训练数据或推理数据，导致模型的准确性和可靠性下降，甚至出现错误或偏差。
- **数据滥用：**攻击者利用 AI 系统的推理能力，对数据进行滥用，例如生成虚假信息、进行网络钓鱼攻击等。

5.1.3 AI 应用攻击面

AI 应用是 AI 技术的具体应用形式，攻击者可以通过各种手段攻击 AI 应用，例如：

- **提示词注入：**攻击者向 AI 应用的输入框中注入恶意提示词，导致应用执行恶意操作或泄露敏感信息。例如，攻击者可以向一个聊天机器人注入提示词，使其泄露用户的个人信息。
- **越权访问：**攻击者利用 AI 应用的漏洞，获取未经授权的访问权限，例如访问用户的账户信息、修改应用的配置等。
- **隐私泄露：**攻击者利用 AI 应用的漏洞，窃取用户的隐私数据，例如用户的搜索记录、聊天记录、位置信息等。
- **恶意代码注入：**攻击者向 AI 应用中注入恶意代码，导致应用执行恶意操作或被攻击者控制。
- **拒绝服务攻击：**攻击者向 AI 应用发送大量的请求，导致应用无法正常处理用户的请求，从而造成拒绝服务。

5.1.4 AI 基础设施攻击面

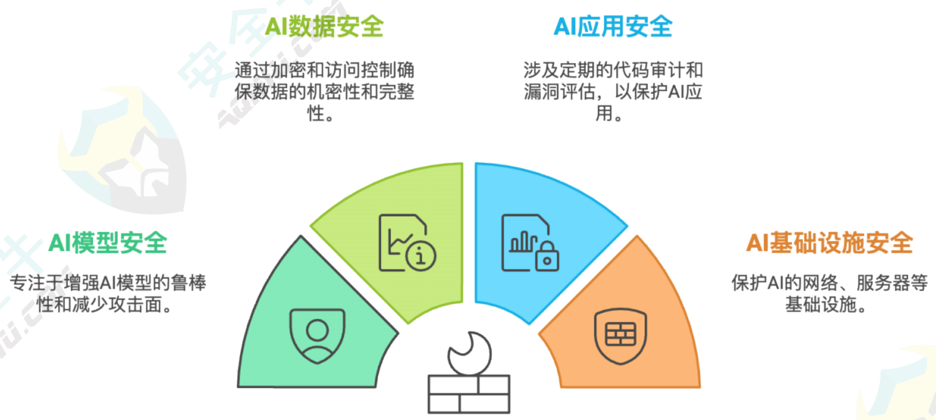
AI 基础设施是支撑 AI 系统运行的基础环境，攻击者可以通过各种手段攻击 AI 基础设施，例如：

- **算力资源滥用：**攻击者利用 AI 系统的算力资源进行挖矿、DDoS 攻击等恶意活动。
- **API 滥用：**攻击者利用 AI 系统的 API 漏洞，进行未经授权的访问或恶意操作。

- **服务器攻击：**攻击者攻击 AI 系统的服务器，例如利用漏洞获取服务器的控制权、窃取服务器上的数据等。
- **网络攻击：**攻击者攻击 AI 系统的网络，例如进行 DDoS 攻击、窃取网络流量等。
- **硬件攻击：**攻击者攻击 AI 系统的硬件设备，例如篡改硬件设备、植入恶意代码等。

5.2 应对 AI 攻击面威胁的策略和建议

为了应对 AI 攻击面威胁，企业和组织需要采取多层次的安全防护措施，加强 AI 模型、数据、应用和基础设施的安全防护，以保障 AI 系统的安全性和可靠性



加强 AI 安全

5.2.1 加强 AI 模型安全防护

（1）模型鲁棒性测试：对 AI 模型进行鲁棒性测试，评估模型在各种攻击下的稳定性和可靠性，例如对抗样本攻击、数据投毒攻击等。

- 操作建议：选择合适的对抗样本生成技术：根据模型的类型和应用场景，选择合适的对抗样本生成技术，例如 FGSM、JSMA、DeepFool 等。
- 生成对抗样本：使用选择的对抗样本生成技术，生成针对模型的对抗样本。
- 测试模型：使用生成的对抗样本对模型进行测试，评估模型在对抗样本攻击下的准确率和鲁棒性。
- 分析测试结果：分析测试结果，识别模型的薄弱环节，并采取相应的措施进行改进，例如增加训练数据、改进模型结构、使用对抗训练等。
- 持续测试：定期对模型进行鲁棒性测试，并持续改进模型的鲁棒性。

例如，针对图像识别模型，可以使用 FGSM 方法生成对抗样本，例如对一张熊猫图片添加微小的扰动，使其被模型识别为长臂猿。通过测试模型在对抗样本攻击下的准确率，可以评估模型的鲁棒性，并针对性地进行改进，例如使用对抗训练增强模型对对抗样本的抵抗能力。

（2）模型攻击面收敛：减少 AI 模型的攻击面，例如限制模型的访问权限、对模型进行代码混淆等。

- 操作建议：最小化模型暴露：仅将必要的模型功能暴露给用户，例如通过 API 接口提供模型访问，而不是直接暴露模型的代码或参数。
- 访问控制：对模型的访问进行严格的权限控制，仅允许授权用户访问模型。
- 代码混淆：对模型的代码进行混淆，增加攻击者进行逆向工程的难度。
- 模型加密：对模型进行加密，防止攻击者直接访问模型的代码或参数。
- 模型签名：对模型进行签名，验证模型的完整性和真实性。

例如，对于一个在线翻译模型，可以通过 API 接口提供翻译服务，并对 API 接口进行身份验证和授权，限制访问模型的用户和权限。同时，可以对模型的代码进行混淆，例如使用代码混淆工具对代码进行重命名、替换、插入等操作，增加攻击者进行逆向工程的难度。

（3）模型安全审计：定期对 AI 模型进行安全审计，发现和修复模型中存在的安全漏洞和风险。

- 操作建议：制定审计计划：制定详细的模型安全审计计划，明确审计的目标、范围、方法和时间安排。
- 选择审计工具：选择合适的模型安全审计工具，例如静态代码分析工具、动态测试工具等。
- 执行审计：按照审计计划执行审计，并记录审计发现的问题和风险。
- 分析审计结果：分析审计结果，识别模型中存在的安全漏洞和风险，并提出相应的改进建议。
- 修复安全问题：根据审计结果，修复模型中存在的安全问题。
- 复查：对修复后的模型进行复查，确保安全问题得到有效解决。

例如，对一个推荐系统模型进行安全审计，可以使用静态代码分析工具扫描模型代码，发现代码中存在的安全漏洞，例如 SQL 注入漏洞、跨站脚本攻击漏洞等。同时，可以使用动态测试工具模拟用户行为，测试模型是否存在逻辑错误或安全缺陷，例如用户是否可以通过输入特定的参数获取未经授权的信息。

5.2.2 保障 AI 数据安全

（1）数据加密：对 AI 系统的训练数据和推理数据进行加密存储，防止数据泄露。

- 操作建议：选择合适的加密算法：根据数据的敏感程度和安全需求，选择合适的加密算法，例如 AES、RSA 等。
- 密钥管理：妥善保管密钥，例如使用密钥管理系统、硬件安全模块等。
- 加密存储：对数据进行加密存储，例如加密数据库、加密文件系统等。
- 加密传输：对数据传输进行加密，例如使用 HTTPS 协议、VPN 等。

例如，对于用户的个人信息数据，可以使用 AES 算法进行加密存储，并使用密钥管理系统对密钥进行管理。在数据传输过程中，可以使用 HTTPS 协议对数据进行加密，防止数据被窃取或篡改。

（2）访问控制：对 AI 数据的访问进行权限控制，仅允许授权用户访问数据。

- 操作建议：身份验证：对用户进行身份验证，例如使用用户名密码、多因素认证等。
- 授权：根据用户的角色和职责，设置不同的数据访问权限。
- 审计：对数据访问进行审计，记录用户的访问行为。

例如，对于 AI 模型的训练数据，可以设置访问权限，仅允许数据科学家和模型训练工程师访问数据。同时，可以对数据访问进行审计，记录用户的访问时间、访问内容等信息，以便于追溯和问责。

（3）数据脱敏：对 AI 数据进行脱敏处理，例如去除敏感信息、添加噪声等，防止数据滥用。

- 操作建议：识别敏感数据：识别数据中的敏感信息，例如个人信息、商业机密等。
- 选择脱敏方法：根据数据的类型和应用场景，选择合适的脱敏方法，例如假名化、匿名化、泛化等。
- 脱敏处理：对敏感数据进行脱敏处理，例如使用假名化技术替换敏感信息，或对数据添加噪声，使其难以被识别。
- 验证：对脱敏后的数据进行验证，确保数据仍然可用，并且敏感信息得到有效保护。

例如，对于包含用户姓名、地址、电话号码等个人信息的训练数据，可以使用假名化技术对敏感信息进行替换，例如使用随机生成的 ID 替换用户的真实姓名，使用虚拟地址替换用户的真实地址，从而保护用户的隐私信息。

5.2.3 提升 AI 应用安全

（1）代码安全审计：对 AI 应用的代码进行安全审计，发现和修复代码中存在的安全漏洞和风险。

- 操作建议：制定审计计划：制定详细的代码安全审计计划，明确审计的目标、范围、方法和时间安排。

- 选择审计工具：选择合适的代码安全审计工具，例如静态代码分析工具、动态测试工具等。
- 执行审计：按照审计计划执行审计，并记录审计发现的问题和风险。
- 分析审计结果：分析审计结果，识别代码中存在的安全漏洞和风险，并提出相应的改进建议。
- 修复安全问题：根据审计结果，修复代码中存在的安全问题。
- 复查：对修复后的代码进行复查，确保安全问题得到有效解决。

例如，对一个 AI 驱动的聊天机器人应用进行代码安全审计，可以使用静态代码分析工具扫描应用代码，发现代码中存在的安全漏洞，例如跨站脚本攻击漏洞、SQL 注入漏洞等。同时，可以使用动态测试工具模拟用户行为，测试应用是否存在逻辑错误或安全缺陷，例如用户是否可以通过输入特定的语句获取未经授权的信息。

（2）漏洞扫描：对 AI 应用进行漏洞扫描，发现应用中存在的安全漏洞和风险。

- 操作建议：选择合适的漏洞扫描工具：根据应用的类型和技术架构，选择合适的漏洞扫描工具，例如 Web 漏洞扫描器、移动应用漏洞扫描器等。
- 配置扫描规则：根据应用的安全需求，配置扫描规则，例如扫描的范围、深度、频率等。
- 执行扫描：定期对应用进行漏洞扫描，并记录扫描结果。
- 分析扫描结果：分析扫描结果，识别应用中存在的安全漏洞和风险，并提出相应的改进建议。
- 修复漏洞：根据扫描结果，修复应用中存在的安全漏洞。
- 复查：对修复后的应用进行复查，确保安全漏洞得到有效解决。

例如，对一个 AI 驱动的在线客服系统进行漏洞扫描，可以使用 Web 漏洞扫描器扫描应用的网页界面，发现网页中存在的安全漏洞，例如跨站脚本攻击漏洞、SQL 注入漏洞等。同时，可以对应用的 API 接口进行扫描，发现 API 接口中存在的安全漏洞，例如身份验证绕过漏洞、数据泄露漏洞等。

（3）安全测试：对 AI 应用进行安全测试，例如渗透测试、模糊测试等，评估应用的安全性。

- 操作建议：制定测试计划：制定详细的安全测试计划，明确测试的目标、范围、方法和时间安排。
- 选择测试方法：根据应用的安全需求，选择合适的安全测试方法，例如渗透测试、模糊测试、代码审计等。
- 执行测试：按照测试计划执行测试，并记录测试发现的问题和风险。

- 分析测试结果：分析测试结果，识别应用中存在的安全漏洞和风险，并提出相应的改进建议。
- 修复安全问题：根据测试结果，修复应用中存在的安全问题。

复查：对修复后的应用进行复查，确保安全问题得到有效解决。

例如，对一个 AI 驱动的自动驾驶系统进行安全测试，可以进行渗透测试，模拟攻击者对系统进行攻击，例如尝试控制车辆的方向盘、刹车等，以发现系统中存在的安全漏洞。同时，可以进行模糊测试，向系统发送大量的随机数据，测试系统在异常输入情况下的稳定性和安全性。

5.2.4 加强 AI 基础设施安全

（1）网络安全防护：对 AI 基础设施的网络进行安全防护，例如部署防火墙、入侵检测系统等安全设备。

- 操作建议：网络隔离：将 AI 基础设施与其他网络进行隔离，例如使用 VLAN、VPN 等技术。
- 访问控制：对 AI 基础设施的访问进行严格的权限控制，仅允许授权用户访问。
- 入侵检测：部署入侵检测系统，实时监控网络流量，并及时发现异常情况。
- 安全审计：对网络访问进行审计，记录用户的访问行为。

例如，将 AI 模型训练服务器与企业内网进行隔离，可以使用 VLAN 技术将服务器划分到一个独立的网络区域，并通过防火墙限制对该区域的访问权限。同时，可以部署入侵检测系统，监控服务器的网络流量，并及时发现异常情况，例如 DDoS 攻击、端口扫描等。

（2）服务器攻击面收敛：减少 AI 服务器的攻击面，例如关闭不必要的端口、禁用不必要的服务等。

- 操作建议：关闭不必要的端口和服务：关闭服务器上不必要的端口和服务，减少攻击面。
- 安全配置：对服务器进行安全配置，例如禁用不必要的账户、设置强密码等。
- 漏洞修复：及时修复服务器上发现的安全漏洞。
- 安全加固：对服务器进行安全加固，例如安装安全补丁、部署安全软件等。

例如，对 AI 模型训练服务器进行攻击面收敛，可以关闭服务器上不必要的端口，例如 Telnet、FTP 等。同时，可以禁用服务器上不必要的服务，例如远程桌面服务、文件共享服务等。

（3）安全监控：对 AI 基础设施进行安全监控，例如监控服务器的运行状态、网络流量等，及时发现异常情况。

- 操作建议: 监控服务器运行状态: 监控服务器的CPU使用率、内存使用率、磁盘空间等运行状态，及时发现异常情况。
- 监控网络流量：监控服务器的网络流量，及时发现异常流量，例如 DDoS 攻击、恶意扫描等。
- 监控安全事件：监控服务器上的安全事件，例如登录失败、文件修改等，及时发现异常行为。
- 告警：及时告警异常情况，并采取相应的措施进行处理。

例如，使用安全监控工具监控 AI 模型训练服务器的运行状态，例如 CPU 使用率、内存使用率等。当服务器的 CPU 使用率或内存使用率超过设定的阈值时，及时发出告警，并通知管理员进行处理。

第六章 攻击面管理成功案例分析

案例一：某城商行统一安全管理平台运营项目（绿盟科技提供）

(1) 案例背景

某银行属于国内大型城商行，20 余家分行和 400 多家对外营业机构，该银行的 IT 环境复杂且多元化，不仅涵盖了传统的本地数据中心、虚拟化平台以及部分云服务，也包括多种形式的互联网服务。随着业务的快速发展和数字化转型的推进，该银行的 IT 资产规模不断扩大，安全风险也随之增加。

该银行为落实有关安全规划建设目标，进一步满足监管相关要求，提升资产安全管理水平，完善安全策略有效性验证工作机制，增强互联网安全监测及处置质效。拟开展信息安全管理体系建设，建立统一安全管理中心，并开展持续安全风险治理运营工作。

(2) 用户问题、痛点和挑战

该银行在项目开展前，在终端安全方面遇到了以下问题和挑战：

- 资产管控难：缺乏互联网资产暴露发现和管理手段，风险视角下现有科技资产的安全底账覆盖面不全，不能快速掌握资产的动态变化，例如互联网数据资产泄露，内网违规业务系统上线等。
- 漏洞管理复杂：没有建立实时漏洞信息获取和响应机制，热点漏洞与现有资产难以快速进行关联，未建立漏洞处置优先级技术手段和机制，导致漏洞管理效率低下。
- 安全风险分散：不同工具和服务发现的安全风险、问题等分布在不同平台，无法做到统一管理，导致安全风险难以全面掌控和及时处置。

(3) 案例实施

项目目标和需求：

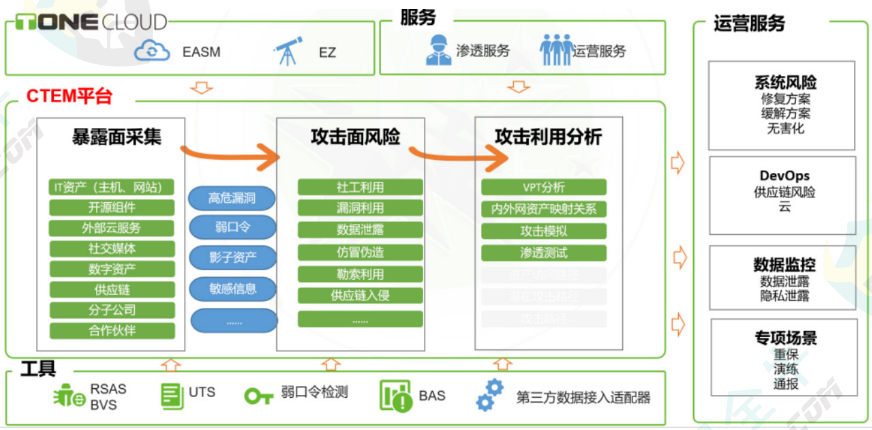
- 知家底：建设内外网 IT 资产、新媒体应用服务、数字资产等多维度多数据来源的资产数据采集能力，建设安全视角的资产台账。
- 常态化：建立持续的威胁评估手段，结合情报和资产指纹对企业敏感服务、仿冒投毒、数据泄露、安全漏洞、配置缺陷等威胁进行持续评估。
- 重闭环：打通统一安全管理平台与工单平台的流程对接，形成处置流程，并且对处置结果与持续监测 / 复测结果进行比对验证，确保问题闭环。

（4）项目实施思路和方法论：

- 采用攻击面管理的思路，从攻击者的视角来审视和管理企业的安全风险。
- 构建统一的安全管理平台，整合多种安全数据和工具，实现对攻击面的全面管理。
- 增加日常安全策略有效性验证工作，确保安全风险处置及时有效。
- 建立安全运营机制，实现对安全风险的持续监控和及时响应。

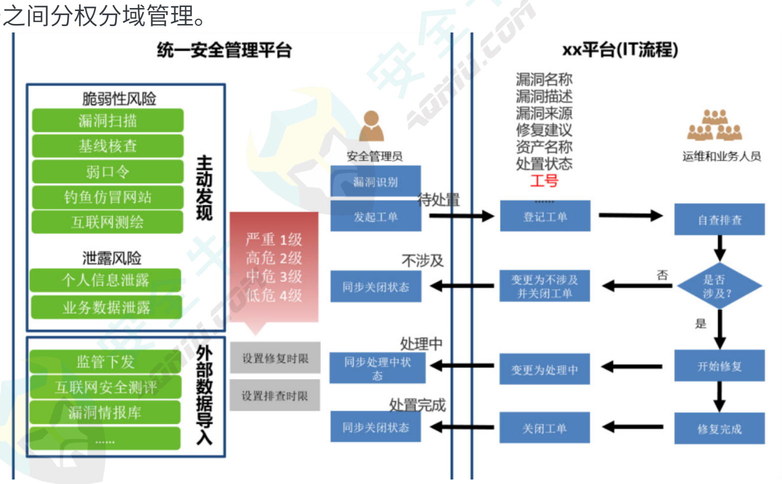
项目实施内容：

- 在运维管理区部署统一安全管理平台，接入已有的漏洞扫描设备、被动流量设备，接入互联网攻击面服务数据，接入行内已有的第三方 CMDB、OA 数据、终端管控平台数据，以及云控制器和 SIME 管理平台等，建立安全视角的资产风险台账模型，进行资产数据融合与统一管理。



统一安全管理平台

- 通过适配器实现对本地多种数据来源的轻量化识别和有效利用，通过搭建反向代理，可以安全地获取云端 SaaS 服务数据；优化现有风险管理流程，开展风险生命周期统一管理运营，实现风险问题流转、转派、验证，以及不同部门、账号之间分权分域管理。



(4) 关键成功因素

- 统一的安全管理平台：该项目中通过平台整合了行内多种安全数据和工具，并补充了安全策略有效性验证环节工作，实现了对攻击面的全面和有效管理，提高了安全运营效率。
- 攻击面管理方法论：从攻击者的视角来审视和管理企业的安全风险，指导安全运营人员聚焦关键风险，及时处置和阻断潜在攻击途径，更加有效。
- 安全运营机制：优化行内现有风险管理流程，建立了依托统一安全管理平台的安全风险运营机制，实现了对安全风险的持续监控和及时响应。
- 与现有安全产品的集成：将统一安全管理平台与现有的安全产品进行集成，例如漏洞扫描设备、CMDB、终端管控平台等，实现了数据共享和联动响应。

(5) 实施收益

- 多维度资产台账打好风险管理基础：项目实施过程，协助客户建立了多维度、符合该银行实际资产管理工作的台账，实现了对 IT 资产、新媒体应用服务、数字资产等多种类型资产的统一管理。
- 攻击视角管理方法提升风险管理水平：通过汇总 CMDB、终端平台、互联网测绘平台、漏洞扫描工具多维度的风险数据，进行数据融合和分析，实现了持续风险运营数据支撑能力，发现单一工具无法覆盖的安全风险死角。
- 持续安全风险运营落实监管合规要求：建立持续安全风险运营工作机制，实时监控安全风险变化，及时响应处置，确保满足国家和行业安全风险监管要求。
- 统一安全管理平台提高安全运营效率：实现风险处置优先级自动化评估能力，统一平台进行安全风险优先级推荐，重点关注高风险和优先级的漏洞，减轻了运维人员工作量。
- 策略有效验证提升安全防护能力：实现了多种维度实时风险发现的安全能力，快速响应并处置潜在的安全风险；结合业务现状，配置合理的策略，形成风险优先级修复的最优解，以最低的修复成本，达到最优的安全效果；对安全修复工作进行有效性验证，确保修复工作达到预期；实现对数据资产泄露风险的监控能力，提供关停和下架闭环管理，保护自身的数字资产和业务运行不受损害。

■ **安全牛评价：**

金融行业作为数字化转型的先锋，其 IT 架构日趋复杂，混合云、移动应用、开放 API 等新技术应用广泛，导致资产类型激增、边界日益模糊，安全管理难度加大。同时，金融行业对数据安全和合规性要求极高，面临的网络攻击也更加复杂和有针对性，任何安全漏洞和风险都可能导致严重的损失，例如资金损失、客户信息泄露、监管处罚等。

该方案的关键能力在于整合多种安全数据和工具，构建统一的安全管理平台，并采用攻击面管理的思路，从攻击者的视角来审视和管理企业的安全风险，实现对企业 IT 资产、新媒体应用服务、数字资产等多维度资产的全面覆盖和持续监控。方案的优势在于其针对性、创新性和可落地性。针对金融行业的需求和痛点，实现了对多维度资产的全面覆盖、持续监控和闭环管理，并从攻击者的视角来审视和管理企业的安全风险，更加有效。

该案例为其他金融机构提供了参考经验，特别是对于面临类似挑战的城商行和其他中小型金融机构，具有一定借鉴意义。

案例二：某新能源汽车控股集团攻击面管理案例（魔方安全提供）

(1) 案例背景

某新能源汽车控股集团是全球汽车品牌组合价值排名前十的企业之一，致力于成为具有全球竞争力和影响力的智能电动出行和能源服务科技公司。其业务涵盖汽车及上下游产业链、智能出行服务、绿色运力、数字科技等，业务板块已覆盖汽车、金融、科技、教育等领域，并拥有大量的下属公司。

(2) 用户问题、痛点和挑战

- 用户信息和车联网敏感数据泄露风险高：新能源汽车行业拥有大量的用户信息和车联网敏感数据，这些数据极易成为网络攻击者的目标。由于数据体量庞大、分布广泛，传统安全工具难以有效防护，导致数据泄露风险居高不下。
- 监管压力大: 国家和行业监管部门对网络安全的要求日益严格，HW演练、重大活动安全保障、网络安全检查常态化，集团面临巨大的合规压力。
- 影子资产缺乏纳管能力：业务快速发展和扩张导致影子资产数量激增，安全团队难以全面掌握和管理这些资产，存在安全盲区。
- 业务资产上线变更频繁，缺乏有效监测手段：频繁的业务上线和变更导致互联网资产风险暴露面不断变化，安全团队缺乏有效手段进行持续监测，难以及时发现和应对安全风险。
- 新业态数字资产缺乏统一监控和管理手段：小程序、API等新业态数字资产的兴起，使得资产的数字化特征更加明显，分布更加泛化，传统安全工具难以有效监控和管理。
- 安全漏洞情报预警能力不足：难以将漏洞情报与资产信息有效关联，无法快速定位受影响资产，导致漏洞修复效率低下，增加了安全风险。
- 下属机构的风险难以综合掌控：下属机构众多，安全管理水平参差不齐，集团难以全面掌控其安全风险，存在安全管理盲区。
- 资产碎片化严重，安全运营缺乏统一平台：多种安全工具和运维工具并存，导致资产数据碎片化严重，安全运营效率低下。

（3）建设方案

项目目标：

- 建立统一的攻击面管理平台，实现对全网资产的全面监控和管理。

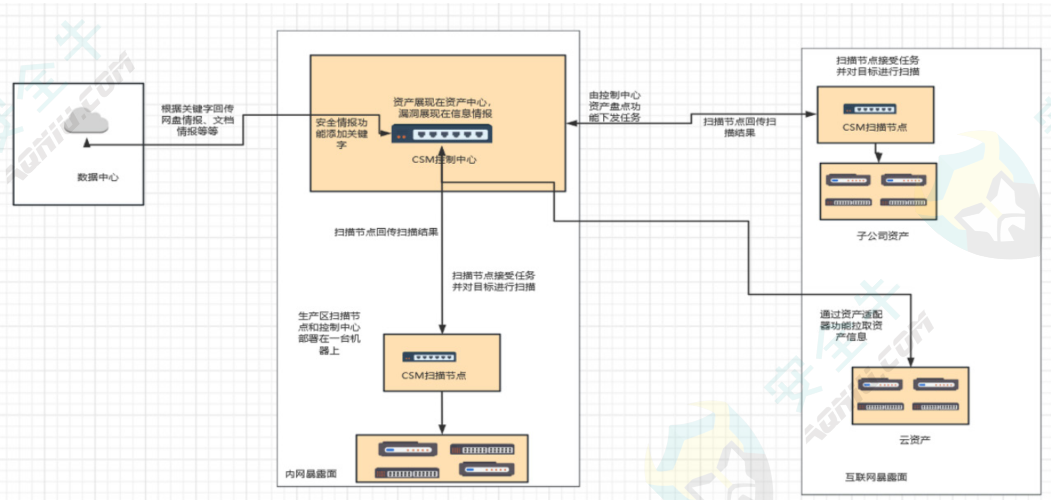
- 提升安全风险发现和响应能力，降低安全风险。
- 满足监管合规要求，保障业务安全稳定运行。

项目需求：

- 能够全面发现和识别各种类型的资产，包括传统 IT 资产、影子资产和新业态数字资产。
- 能够持续监控资产风险暴露面，及时发现安全漏洞和威胁。
- 能够整合现有安全工具和平台，实现资产数据的统一管理和分析。
- 能够提供可视化的资产安全态势，帮助安全团队快速了解和应对安全风险。

项目实施内容：

该集团部署了魔方网络资产攻击面管理系统（CAASM），实现互联网与内网网络资产一体化安全管理。



A.EASM 场景：

- 主动资产发现和模糊关联：平台利用主动扫描和模糊关联技术，全面识别集团及其子公司的互联网资产，并进行持续的漏洞扫描和风险监测。
- 影子资产监测：通过关键字特征和关键图案识别，平台能够自动发现未知资产，并监测仿冒、假冒和钓鱼资产。
- 新型数字资产风险监控：平台能够监控公众号、小程序、APP、网盘、开源社区等新型数字资产的敏感信息泄露风险。
- 数据下架服务：魔方安全针对真实的敏感泄露事件提供数据下架服务，实现敏感信息泄露事件全生命周期的闭环管理。

- 漏洞通报预警：通过微信群等方式进行漏洞通报预警，及时响应该集团相关问题。

B.CAASM 场景：

- 全网资产安全运营中心：平台作为全网资产安全运营中心，通过扫描探针、流量探针和资产适配器，快速对接第三方系统，聚合全网资产数据。
- 资产数据汇总和提纯：平台利用关联清洗算法，实现全网资产信息的汇总和提纯，并打通业务属性与管理属性，构建可持续更新的资产安全台账。
- 资产标签化管理：平台自动对资产来源进行标签化管理，有效对比分析第三方产品部署覆盖度情况，洞察安全管理覆盖度。
- 漏洞扫描和风险评估：平台整合现网第三方漏洞扫描引擎，并利用强大的 PoC 插件检测能力，自动化、持续化地补全全网脆弱性数据，对资产全生命周期进行安全管理。

（4）关键成功因素

- 全面的资产发现能力：CSM 平台能够发现各种类型的资产，包括传统 IT 资产、影子资产和新业态数字资产，有效解决了资产可见性的问题。
- 高价值风险评估能力：CSM 平台自研 POC 漏洞检测引擎，能够精准、快速地发现安全漏洞，并进行风险评估。
- 灵活的集成和扩展能力：CSM 平台能够与第三方安全工具和平台无缝集成，实现资产数据的统一管理和分析。
- 可视化的安全态势感知：平台提供直观的可视化界面，帮助安全团队快速了解资产安全态势，及时发现和应对安全风险。

（5）实施收益

平台的部署为该集团带来了显著的收益：

风险控制，有助于企业自动发现全部的网络 IT 资产，梳理暴露面，形成完整、及时更新的资产数据库；网络空间资产状况清晰，资产变动及时感知；

- 持续收集外部漏洞情报、威胁情报，与资产进行关联；
- 持续对资产进行漏洞监控，先于黑客检测到攻击面暴露；
- 基于快速扫描方法，可在重大漏洞爆发时基于资产库执行全网精确扫描，精准定位受影响资产，提高应急效率；

- 业务特征指纹，识别资产滥用行为，强化公司规范和要求
- 高危漏洞爆发，基于留存资产记录，可第一时间定位、精准预警，准确响应；
- 数字资产持续监控，及时发现代码、测试数据、敏感信息的泄漏、资产防盲、未知资产，风险处置；
- 全网范围排查影子资产，让企业对整体资产及风险情况更加清晰，随之掌握动态变化。

安全牛评价：

新能源汽车行业作为新兴产业，其业务模式和 IT 架构都处于快速发展和变化之中，安全防护体系建设通常滞后于业务发展，面临着数据泄露、供应链攻击、勒索软件攻击等多种安全威胁。同时，新能源汽车行业涉及大量的敏感数据，例如用户信息、车联网数据等，一旦发生数据泄露事件，将会对企业造成巨大的经济损失和声誉损失。

该方案提供全面的攻击面管理，包括外部攻击面管理（EASM）和内部攻击面管理（CAASM），并结合威胁情报和安全运营，实现对攻击面的持续监控和及时响应。方案的优势在于针对新能源汽车行业的特殊需求和痛点，实现了对多维度资产的全面覆盖、持续监控和闭环管理，覆盖了 EASM 和 CAASM 两种场景，并结合了威胁情报和安全运营。方案的实施推动了攻击面在新能源汽车行业的应用，为其他新能源汽车企业提供参考经验，特别是对于面临类似挑战的汽车制造企业、出行服务公司等。

案例三：某科技集团网络空间风险暴露面治理实践案例（亚信安全提供）

(1) 案例背景

某科技集团企业是一家综合解决方案服务提供商，涉及软件开发、系统运维和系统集成等领域，拥有 30 余家全资控股公司。该集团主要为金融、运营商和政府客户提供综合解决方案，具有一定行业影响力。近期接监管单位通知，其备案网站被篡改为不良网站，且公共存储空间中存在大量敏感信息。该事件引起了内部高层的高度关注，迫切需要采取措施以恢复信任和保障数据安全。

(2) 用户问题、痛点和挑战

- 声誉风险：备案网站被篡改可能导致客户信任度下降，影响集团声誉。
- 敏感数据保护：公共存储空间中敏感信息的泄露对客户和业务造成严重后果，同时影响集团商誉。
- 合规性问题：金融和政府客户对数据安全有严格要求，需确保符合客户管理要求，保证客户数据不泄露。
- 数据安全工作未落实：集团早已推行数据安全管理，但是见效慢，如何快速让数据安全见效
- 长远安全策略：后续需要制定有效的安全策略，防止类似事件再次发生。

(3) 案例实施

利用亚信安全星海·外部攻击面管理平台，每月针对其自身互联网资产及数据泄露情况进行持续探测。

- 暴露面梳理：基于亚信安全外部攻击面管理服务，对主机类资产、web 类资产、公众号、小程序等暴露面进行梳理，对网盘、文库、邮箱等商业泄密风险进行检测。
- 攻击面发现：通过自动化平台风险评估 + 专家验证模式开展暴露面风险的评估，
- 针对于互联网暴露资产发现：未授权访问、测试资产暴露、弱口令、钓鱼仿冒、影子资产等大量资产风险
- 针对于数据泄露情况，在网盘、文库、代码托管平台发现大量项目信息
- 数据闭环治理：针对于异常数据，提供数据下架服务，完成数据闭环治理
- 加强员工安全意识培训：以发现风险事件为例，开展全员网络安全培训，提高员工对安全风险的认识和防范能力。同时优化安全管理政策和流程，确保全员遵守。

亚信安全星海外部攻击面管理平台

（4）客户价值

- 事前感知，以攻促防：以攻击视角，模拟黑客攻击手法，将安全左移，化被动为主动，持续收敛攻击面；
- 风险可见，持续监测：打破传统安全的局限性，降低攻防门槛，提高资产摸排及渗透测试效率，增强企业实战能力；
- 降本增效，高效高质：降低人工成本，通过自动化能力，摸清家底，发现风险，持续提升运营效率
- 管理抓手，监督机制：作为集团管理的依据，对控股公司及被管理单位进行监督和管理，保障企业的整体安全能力。

安全牛评价：

软件开发、系统运维和系统集成等科技服务行业常涉及到客户的敏感数据和机密系统，对数据安全和合规性要求极高。同时，这些企业自身的 IT 环境也较为复杂，包括大量的互联网资产、云平台、移动应用等，攻击面广泛，面临着数据泄露、网络攻击、恶意代码等多种安全威胁。

亚信安全的外部攻击面管理解决方案通过自动化风险评估和专家验证相结合的方式，不仅能够帮助企业识别和管理互联网资产，还能够检测商业泄密风险，并提供数据下架服务，并利用模拟黑客攻击方法持续收敛攻击面还通过自动化能力，降低人工成本，提高资产摸排及渗透测试效率。该案例为其他科技服务企业提供了参考经验，特别是对于面临类似挑战的软件开发公司、系统集成商等，具有一定的借鉴意义。

某全国性金融公司 EASM 联动 BAS 项目案例分析（矢安科技提供）

(1) 案例背景

某全国性金融公司，旗下拥有众多子公司和分支机构，拥有庞大的用户群体和海量交易数据，其 IT 环境复杂，安全风险较高。随着数字化转型的深入，该金融公司面临日益严峻的网络安全挑战。尤其是在近年来，外部攻击面不断扩大，高级持续性威胁 (APT) 攻击、数据泄露等安全事件频发，对公司业务的稳定运行和声誉造成了严重威胁。

(2) 用户问题、痛点和挑战

该金融公司在终端安全方面面临以下问题和挑战：

- 影子资产管理难：由于机构众多，历史遗留问题突出，存在大量未纳入管理的“影子资产”，难以全面掌握资产安全状况，增加了安全风险。
- 合规压力大：金融行业监管严格，需要满足各种安全合规要求，例如“两高一弱”、勒索软件防护等，但由于缺乏有效的工具和手段，合规检查工作繁重且效率低下。
- 人员安全意识薄弱：员工安全意识不足，容易遭受钓鱼攻击等社会工程学攻击，尤其是在当前地缘政治风险加剧的情况下，海外业务面临的钓鱼风险更加突出。
- 边界安全防护能力不足：传统的边界安全设备难以有效应对新型攻击手段，缺乏对边界安全防护能力的全面评估，存在安全盲区。
- 供应商安全风险管理难：对供应商的安全评估和管理不足，难以有效识别和控制供应链安全风险，容易遭受来自供应商的攻击或数据泄露。
- 安全运营效率低：安全人员需要处理大量的安全告警和事件，但由于缺乏有效的工具和平台，安全运营效率低下，难以及时响应和处置安全威胁。

(3) 案例实施

◎ 项目目标：

- 建立全面的外部攻击面管理体系，实现对所有资产的有效识别和管理，降低安全风险。
- 提升安全合规水平，满足监管要求。
- 增强人员安全意识，提高抵御社会工程学攻击的能力。
- 加强边界安全防护，有效应对新型攻击威胁。

- 强化供应商安全管理，降低供应链安全风险。
- 提高安全运营效率，及时响应和处置安全威胁。

◉ 项目需求：

- 能够自动发现和识别所有外部资产，包括“影子资产”。
- 能够对资产进行安全评估，识别安全漏洞和风险。
- 能够提供安全合规检查功能，满足监管要求。
- 能够进行人员安全意识评估和培训。
- 能够评估边界安全防护能力。
- 能够对供应商进行安全评估和管理。
- 能够提供安全事件告警和响应功能。

项目实施思路和方法论：

采用矢安科技的觅影 (AS EASM) 外部攻击面管理系统和攻鉴 (AS BAS) 突破与攻击模拟系统，构建一体化的外部攻击面安全管理解决方案。

◉ 项目实施内容：

- 按照组织结构统一管理子机构，绘制组织整体攻击面通过觅影平台，客户可以统一管理所有子机构的外部攻击面，设置常态化扫描任务，并下发风险整改通知。
- 内置行业合规模板，助力常态化合规检查内置多个行业合规模板，支持“两高一弱、弱口令、勒索”扫描、信创证书、国密证书、证书有效性等合规检查，并提供常态化巡检和报告下载功能。
- 联合 ASBAS 评估组织整体防护能力、防钓鱼意识水平联动攻鉴系统，评估边界安全设备的防护能力，并对泄露邮箱发送钓鱼邮件，测试员工的安全意识水平，提供有针对性的防钓鱼培训。
- 监控供应商风险情报，即时预警供应商风险通过觅影平台评估供应商风险评分，输出风险评估报告，用于供应商准入评估。同时，收集供应商风险情报，对有风险的供应商进行即时预警。
- 信息泄露多渠道监控，提供下架闭环服务针对泄露在公开文库、网盘、代码仓库的文件 / 文件夹，提供从平台下架的闭环服务（已经成功下架多家金融客户的泄露信息）。

• 结合 VPT 方法判定风险优先级，结合 AI 技术提高处置效率觅影平台支持将风险评分、资产价值、风险可利用性等维度信息综合计算风险优先级，聚焦核心风险。同时，利用 AI 技术提供修复指引、漏洞情报上下文等信息

（4）客户价值

通过实施该项目，该金融公司在终端安全方面取得了显著成效，给客户带来了以下价值：

- 组织机构整体防护

客户通过觅影平台可以查看整个组织机构每日最新的攻击面整体态势。

- 异动资产告警

客户可接收觅影平台发布的资产 / 信息 / 情报的异动通知，包括异常上线等。

- 常态化合规检查

安全团队通过内置“两高一弱、弱口令、勒索专项”合规模板，可以快速扫描，快速确定影响面并生成专业报告。也可检查信创证书、国密证书、证书有效性等合规项。

- 边界安全能力评估

安全团队通过觅影平台，可以统计集团整体边界安全设备防护水平，获取不同品牌边界安全设备的防护侧重。

- 泄露邮箱防钓鱼意识评估

安全团队根据觅影平台提供的泄露邮箱下发钓鱼邮件，评估泄露邮箱的人员安全意识水平，针对性开展防钓鱼培训及泄露邮箱收敛。

- 供应商准入评估

安全团队通过觅影平台提供的供应商风险评估报告，为准入风险评估提供数据支撑。

- 供应商管理及风险预警

欧盟的《网络弹性法案》要求供应商主动披露漏洞，但仅要求供应商向监管单位披露漏洞需要在 24 小时内，但是要求供应商向客户披露漏洞的时限在 72 小时内。这中间的 48 小时客户需要承担着该漏洞的风险，这是他们安全团队不愿看到的。

借助觅影平台，安全团队可查看供应商漏洞情报信息，24 小时内主动接收供应商风险预警，确定影响面，保证供应链安全。

- 0day 快速验证

安全团队可对觅影平台搜集到的 0day/1day 漏洞情报，快捷下发扫描任务，确定影响面并实施修复方案。

- 泄露信息下架

针对泄露在文库、网盘、代码仓库等平台的敏感信息，安全团队可以指示下架动作，并支持下架复验。

- 修复成本下降

安全团队可查看觅影平台筛选的高优先级风险，集中资源解决核心业务的严重风险。

- AI 交互指引

在执行修复、获取更多信息和深度分析时，安全团队可利用觅影平台自带的人工智能助手，扩充情报上下文、提供“手把手”修复指引、长文本关键字识别及风险降噪功能。

■ 安全牛评价：

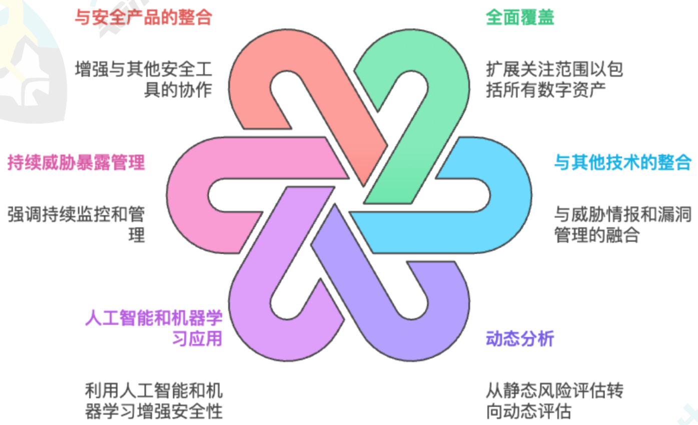
金融机构作为网络攻击的重点目标，其庞大的资产规模、复杂的 IT 环境、敏感的业务数据以及严格的合规要求，使企业在安全防护方面面临巨大压力。尤其是在“影子资产”管理、安全合规检查、人员安全意识提升、边界安全防护能力评估和供应商安全风险控制等方面，传统安全手段和工具难以有效应对，亟需有效的解决方案来解决这些痛点。方案的优势在于矢安科技提供的 EASM 联动 BAS 解决方案通过自动化技术和模拟攻击的全面性、自动化、智能化和可操作性，能够帮助金融机构有效提升安全防护能力和安全运营效率，具有较强的创新性和先进性。该案例对其他行业，特别是同样面临严格监管和复杂 IT 环境的行业，如政府、能源、医疗等，具有重要的借鉴意义。

第七章 国内外攻击面管理技术研究

国外技术发展较为成熟，产品功能完善，部分产品已融入 AI 技术并支持云原生环境。国内技术发展较晚，但近年来发展迅速，市场规模不断扩大，产品不断涌现，并与云安全、零信任架构等技术融合发展。国内企业在攻击面管理产品应用方面也呈现出行业差异化特点。

7.1 国外攻击面管理技术现状

近年来，随着云计算、移动办公、物联网等新技术的广泛应用，企业攻击面迅速扩张，传统的边界安全防御手段已不足以应对日益复杂的安全挑战。国外攻击面管理技术在这一背景下不断发展演进，以应对日益复杂的网络安全挑战。主要呈现以下趋势：



国外攻击面管理技术现状

（1）攻击面管理从外部转向全面攻击面

过去，攻击面管理主要关注外部攻击面，即面向互联网的资产和服务。例如，外部攻击面管理（EASM）工具主要用于发现未知的外部资产、评估其风险敞口并提供修复建议。然而，随着企业 IT 架构日益复杂，内部攻击面的安全问题也日益凸显。因此，攻击面管理正从外部转向全面，扩展到内部攻击面、云攻击面、物联网攻击面等，涵盖了企业所有的数字资产和系统。网络资产攻击面管理（CAASM）的兴起便是这一趋势的体现。CAASM 侧重于管理内部资产，例如服务器、数据库和应用程序，并评估其安全配置和漏洞情况。现在，EASM 和 CAASM 正在融合到统一的 ASM 理念下，以提供更全面的攻击面视图。

例如，PaloAltoNetworks 的 Expanse 平台最初专注于外部攻击面管理，但现在已扩展到涵盖内部资产和云工作负载。Microsoft 的 DefenderforCloud 平台将云安全态势管理（CSPM）和云工作负载保护平台（CWPP）功能与攻击面管理功能整合在一起。

（2）攻击面管理与威胁情报、漏洞管理等技术深度融合

为了更有效地管理攻击面，ASM 正在与其他安全技术深度融合，例如威胁情报、漏洞管理、安全信息和事件管理（SIEM）以及检测与响应（EDR）。这种融合有助于提供更全面的安全视图，并实现更精准的风险评估和修复建议。

例如，CrowdStrike 的 Falcon 平台将端点检测和响应（EDR）与攻击面管理功能结合在一起，利用其端点代理网络和威胁情报来识别和评估风险。Rapid7 的 InsightVM 平台将漏洞管理和攻击面管理功能结合在一起，利用其漏洞扫描、配置评估和威胁情报功能来识别和评估风险。Tenable 的 Nessus 和 SecurityCenter 平台将漏洞管理和攻击面管理功能结合在一起，利用其漏洞扫描、配置评估和风险评分功能来识别和评估风险。

（3）从静态分析到动态分析

早期的攻击面管理主要依赖于静态分析，例如漏洞扫描、配置检查等，例如定期对服务器进行漏洞扫描，检查系统配置是否符合安全基线等。由于高级持续性威胁（APT）攻击的增多，攻击技术和手法不断更新，静态分析方法难以发现动态环境中的安全风险，例如攻击者利用 0day 漏洞、社会工程学等手段发起的攻击。现在，攻击面管理更加注重动态分析，例如攻击路径分析、入侵和攻击模拟等，以便更全面地识别和评估风险，例如模拟攻击者对企业网络进行攻击，并分析攻击路径和攻击成功的可能性。

例如，Randori 的攻击面管理平台可以模拟攻击者的行为，对企业网络进行攻击模拟，并评估攻击成功的可能性，从而识别高风险资产和漏洞。

（4）人工智能（AI）和机器学习（ML）的应用

人工智能（AI）和机器学习（ML）正在被广泛应用于攻击面管理，以提高其效率和准确性。AI 和 ML 算法可以帮助自动发现资产、识别漏洞、评估风险和提供修复建议。它们还可以帮助识别攻击面中的异常活动，并预测潜在的攻击路径。

例如，PaloAltoNetworks 的 Expanse 平台利用机器学习算法来提供更准确的攻击面视图，并识别潜在的攻击路径。CrowdStrike 的 Falconplatform 使用 AI 技术来检测和响应安全威胁，例如识别恶意软件、检测异常行为等。

（5）攻击面管理向持续威胁暴露管理（CTEM）演进

传统的攻击面管理通常是一个静态的过程，而持续威胁暴露管理（CTEM）则强调持续监控和管理攻击面，CTEM 是一个循环的过程，包括五个阶段：范围界定、发现、优先级排序、验证和行动，CTEM 的目标是帮助组织持续改进其安全态势，并降低遭受网络攻击的风险。Gartner 将 CTEM 列为 2024 年的十大战略技术趋势之一，并指出它可以帮助组织将安全投资重点放在最关键的领域。

（6）从孤立到融合

早期的攻击面管理是孤立的，与其他安全产品和流程缺乏联动，例如攻击面管理平台与 SOC、SIEM 等平台之间的数

据没有互通。随着安全运营一体化趋势，现在，攻击面管理更加注重与其他安全产品和流程的融合，例如与 SOC、SIEM、SOAR 等平台进行集成，以构建更加完善的安全防御体系，例如将攻击面管理平台发现的漏洞信息同步到 SOC 平台，以便于 SOC 团队进行分析和响应。

例如，MicrosoftDefenderforCloud 可以与 MicrosoftSentinel、MicrosoftDefenderforEndpoint 等其他 Microsoft 安全产品进行集成，提供全面的安全防护。

7.2 国内攻击面管理技术现状

攻击面管理正在经历从外部到内外兼顾、从单点产品到平台化解决方案、从通用场景到行业深耕的转变。同时，网络资产管理更加重视数据治理和准确性，外部攻击面管理也更加注重数据的准确性和漏洞发现能力。此外，攻击面管理的驱动力也从合规驱动转向验证驱动，更加注重安全体系的有效性验证。最终，攻击面管理的核心理念正在从以资产为中心转变为以风险闭环为中心，更加强调风险的全面管理和持续监控。

（1）从外部攻击面到内外部的整体攻击面

早期的攻击面管理主要关注外部攻击面，即暴露在互联网上的资产和漏洞。由于越来越多的攻击者利用内网漏洞和弱点进行攻击，用户意识到内网资产通常比外网资产更加敏感，一旦被攻击，造成的损失更加严重。攻击面管理从关注互联网资产的暴露面，扩展到关注内网资产的攻击面，包括内网资产的识别、漏洞管理、攻击路径分析等，

例如，绿盟提供的 CTEM 解决方案，融合内外部数据对整体攻击面进行统一管理，亚信安全和知道创宇计划未来将 EASM 和 CAASM 的数据融合，提升联动防御能力。华云安通过灵洞（Ai.Vul）和灵知（Ai.Radar）实现内外部的整体风险管理，不断改进完善的安全态势。华顺信安等其他厂家则同时提供了 EASM 和 CASSM 的产品。

（2）从单点产品到整体解决方案

攻击面管理产品不再是单个工具，正在朝着平台化解决方案的方向发展，将攻击面管理平台与 SOC、SIEM、威胁情报、攻击模拟等其他安全产品进行集成，实现对风险的全面管理，未来还将提供实时监测和预警功能，帮助用户进行持续的安全运营管理。

例如，绿盟科技的攻击面管理方案可以将 EASM、TVM 脆弱性管理、BAS、云管理平台等多种安全能力整合到一个平台上，为用户提供一站式的攻击面管理解决方案。知其安网络攻击面管理平台将融合后的资产数据输出给其他安全平台进行安全业务的运营。华云安将 CAASM、EASM、BAS 等原子化安全能力通过云原生安全平台进行编排，形成攻击面管理的整体解决方案。

（3）从资产梳理转为资产数据质量治理阶段

网络资产管理 CAASM 的资产可以通过各种设备获取到较多的数据，但是数据存在数据缺失、资产无主等问题，数据的准确性已经成为用户的痛点，需要资产数据的精准度，而国内厂商也更加重视数据准确的治理工作，

例如，亚信安全的 EASM 利用 ETL 加强对多源的大网测绘数据进行重新验证，保证互联网资产的准确性。华云安聚焦资产的关联能力，实现资产与业务的关联。知其安的 CAASM 利用 ETL 增强对多源异构资产数据的接入、清洗、映射能力，实现快速对接企业现有安全设备的资产数据。知道创宇聚焦资产多维度开展资产的关联分析。

（4）外部攻击面 EASM 的资产发现方面已经较为成熟。

大部分厂商的产品都可以实现全面地发现企业未知的影子资产、泄露数据等。主要差异化现在表现为外部资产的准确度和漏洞发现，以及风险处理等服务方面。

例如，亚信安全采用重复核对，保证互联网资产数据的准确性；绿盟和亚信提供几小时内的快速下架服务，方便用户在发现泄露数据后，可以快速从百度网盘、Github 等网站快速下架。亚信利用攻击团队，提升 0day 和 1day 漏洞的挖掘能力。华顺信安提供报告的专家服务，以提高交付报告的准确性。

（5）攻击面风险运营平台初步兴起

攻击面风险运营是指以攻击者视角，持续识别、评估和管理企业网络暴露面的风险，并通过有效手段降低安全风险，提升安全防护水平。主要驱动是安全威胁态势的严峻性、网络暴露面的不断扩大、合规压力的增加等。攻击面风险运营平台通过融合 EASM、CAASM，并集成其他多种安全产品，例如漏洞扫描器、威胁情报平台、攻击模拟工具、安全运营中心（SOC）等，有效推动企业安全运营模式从被动响应向主动防御转变。未来攻击面风险运营平台将更加注重自动化和智能化，并与其他安全技术进行更深度的融合。

例如，绿盟科技利用 CTEM 理念构建攻击面风险运营中心。整合了其全面的安全产品线，并拥有专业的安全运营团队，为客户提供持续的泛资产识别、威胁评估和有效性验证、可落地的威胁管理机制、全局视角的运营度量和安全态势的攻击面风险运营一站式解决方案，并已经在金融、能源、运营商等行业落地。

（6）从合规能力到验证能力

早期的企业主要是开展合规建设，攻击面管理产品主要是面对满足合规要求的资产梳理和合规检查。随着国家对网络安全的重视程度提升，攻击演练频繁，攻击手段和攻击目标不断变化，企业的安全需要转变为以实战对抗为目标，更加注重安全体系的有效性验证，以抵御真实攻击威胁。安全厂商也更加关注安全验证能力。

例如，绿盟、华云安、亚信、矢安科技、知其安科技都提供了 BAS 功能，可以通过模拟攻击者行为，验证企业安全防御体系的有效性。

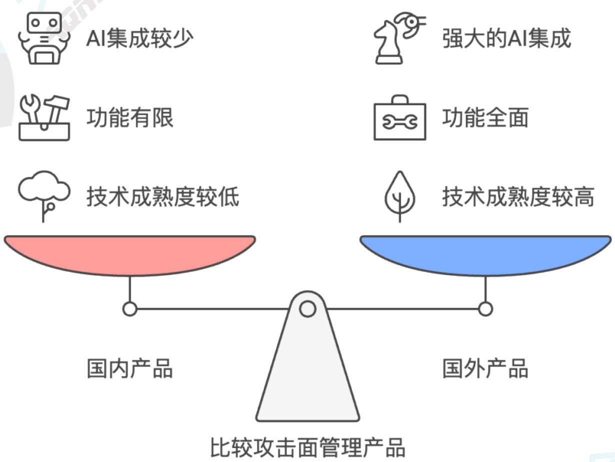
（7）供应商安全受到关注

随着全球供应链的复杂性增加，厂商开始重视厂商供应链的安全性和稳定性，有助于确保供应链的透明度和安全性，同时提高供应链的韧性和响应能力，以应对潜在的供应链打击。目前主要应用场景包括供应商准入、安全监控等场景

例如，知道创宇通过利用情报监控技术，对厂商供应链进行实时监控，以预防和应对供应链中的安全威胁。矢安科技则计划开发供应商安全监控系统，实现合作准入、供应链管理和供应链风险评估等功能。

7.3 国内外攻击面管理技术差距分析

国内攻击面管理技术与国外相比，在产品成熟度、功能完善性和智能化程度方面存在一定差距。国内厂商的产品在自动化、智能化、攻击路径分析和入侵模拟等方面还有待提升。建议国内用户选择攻击面管理产品时，优先考虑功能完善、性能稳定、技术成熟度高的产品，并关注产品是否融入了 AI 技术以提高效率。



差距分析

国内外攻击面管理产品具体差距分析及用户建议：

（1）产品技术成熟度：相比国外，国内攻击面管理技术起步较晚，技术成熟度相对较低。国外厂商如 CrowdStrike、Randori 等，其攻击面管理产品功能完善，能够提供全面的攻击面管理能力。国内厂商的攻击面管理产品在功能和性能方面与国外厂商的产品还存在一定的差距，例如部分产品的自动化程度和智能化程度还不够高，部分产品的功能还不够完善等。

用户建议：国内用户在选择攻击面管理产品时，应优先选择功能完善、性能稳定、技术成熟度较高的产品。

（2）产品功能完善度：相比国外，国内攻击面管理产品功能相对单一，部分产品的功能还不够完善。例如，国外厂商的攻击面管理产品大多能够提供更精确的攻击路径分析和入侵模拟功能，例如，Randori 的攻击面管理平台可以模拟攻击者的行为，对企业网络进行攻击模拟，并评估攻击成功的可能性，从而识别高风险资产和漏洞。而国内厂商的攻击面管理产品在这方面还有待提升。

用户建议：国内用户在选择攻击面管理产品时，应根据自身的需求，选择功能满足其需求的产品。

（3）智能化程度：国外攻击面管理产品在 AI 技术深度方面具有一定的优势，而国内攻击面管理产品在技术深度方面还有待提升。例如，CrowdStrike 的 Falconplatform 使用 AI 技术来检测和响应安全威胁，例如识别恶意软件、检测异常行为等。

用户建议：国内用户在选择攻击面管理产品时，可以关注产品是否融入了 AI 技术，可以利用 AI 技术提高效率。

7.4 国内攻击面管理未来发展趋势

安全牛预测，未来的攻击面管理将更加自动化、智能化、云原生化，并与企业的安全运营和业务风险管理流程更紧密地结合。通过采用这些先进的技术和方法，企业可以更好地了解和管理自身的安全风险，并提高抵御网络攻击的能力。

自动化和人工智能 (AI) 的深入应用。随着 AI 人工智能技术和自动化技术的发展，自动化和人工智能应用将在自动化发现和映射、AI 驱动的风险优先级排序、自动化修复建议和预测性分析等方面广泛应用。

攻击面管理的平台化和整合。企业将寻求能够提供全面攻击面管理功能的统一平台，而不是依赖多个分散的工具。未来，攻击面管理平台将与其他安全工具，进行更紧密的集成，实现安全数据的共享和协同。

基于风险的攻击面管理。攻击面管理将从单纯的资产发现和枚举，转变为基于风险的管理，更加关注对业务造成实际影响的风险。攻击面管理工具将提供更精细的风险量化功能，帮助企业评估不同攻击路径的风险等级，并制定相应的缓解措施。

主动式攻击面管理。 攻击面管理工具将提供攻击全路径模拟功能，帮助安全团队识别潜在的攻击路径，并在攻击者利用之前进行修复

供应商安全受到关注。随着全球供应链的复杂性增加，供应链攻击日益增多，给企业带来巨大风，未来供应链安全将成为攻击面管理的重要组成部分，攻击面管理产品将更加注重供应链安全风险的评估和管理。

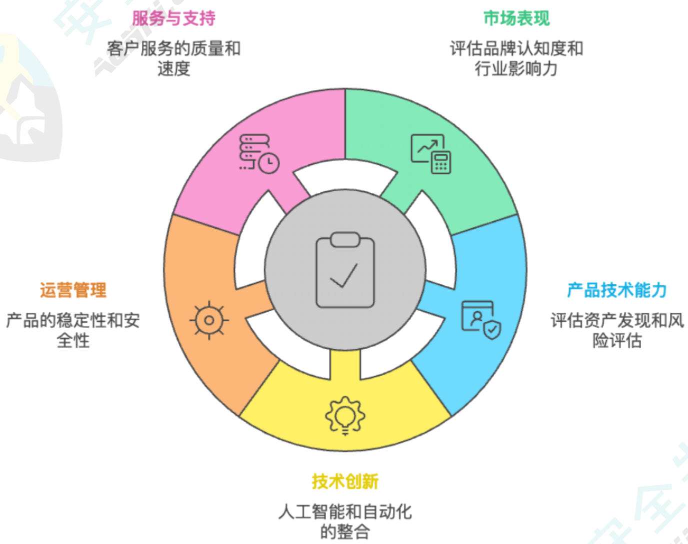
云原生攻击面管理兴起。随着云计算的普及，云原生攻击面管理技术应运而生，将更好地支持云原生环境，例如，提供云原生资产发现、云原生漏洞扫描、云原生安全策略管理等功能。

第八章 攻击面管理厂商推荐

选择合适的攻击面管理产品需要考虑市场表现、产品技术能力、技术创新能力、运营管理能力和服务与支持能力等关键指标。本报告推荐了十家具有代表性的厂商，并详细介绍了它们的产品特点、优势和推荐理由，为企业选择合适的解决方案提供参考。

8.1 选型关键指标

安全牛建议攻击面管理产品选择应考量**厂商品牌、市场表现、产品技术能力、产品创新能力、管理与服务等**多方面因素，针对企业场景明确不同建设阶段的目标和需求，从而为产品评估选择提供全面依据：



选型关键指标

8.2 十大代表性厂商推荐

报告从品牌影响力、市场表现、产品技术能力、产品创新能力、管理与服务五大能力维度，对当前国内新一代攻击面管理厂商进行了评估分析，并收录其中具有较高应用代表性的 10 家厂商（排名不分先后，按首字母序排列）

（1）推荐厂商 - 华顺信安

北京华顺信安信息技术有限公司（以下简称“华顺信安”）成立于 2015 年，北京华顺信安科技有限公司是一家以网络空间测绘技术为基础，聚焦于安全大数据和网络空间资产安全的高科技企业。华顺信安公司总部位于北京，在上海、深圳、长沙、成都、武汉等多地设有分支机构。目前研发团队规模 50+ 人，主要客户涉及政府、金融、运营商等行业。

◆ **典型产品介绍**

- 明见·FORadar，互联网资产攻击面管理平台，基于互联网资产引擎技术，动态探测客户互联网资产、数字资产、疑似资产、威胁资产、资产漏洞、数据泄露等问题，挖掘客户暴露在互联网侧的未知资产，以攻击者视角洞悉资产风险，快速精准绘制企业资产暴露面。
- FOBrain，网络资产攻击面管理平台，以攻击者视角聚焦企业网络空间资产，帮助客户全面掌握资产动态、洞察资产风险，以攻促防，从攻防实战的角度审视安全防御体系，梳理企业的攻击面，构建实战化、一体化的攻击面管理平台。

◆ **推荐理由**

- 互联网资产全面性、快速测绘
- 丰富的报告模板，成熟的资产可信度打分机制

- 报告模板和专家解读服务
- 易用性强：操作简便，自动化程度高

◆ **适合场景**

- 互联网资产梳理和未知资产探测
- 互联网资产风险评估和漏洞扫描
- 数据泄漏监控
- 安全合规检查和报告

（2）推荐厂商 - 华云安

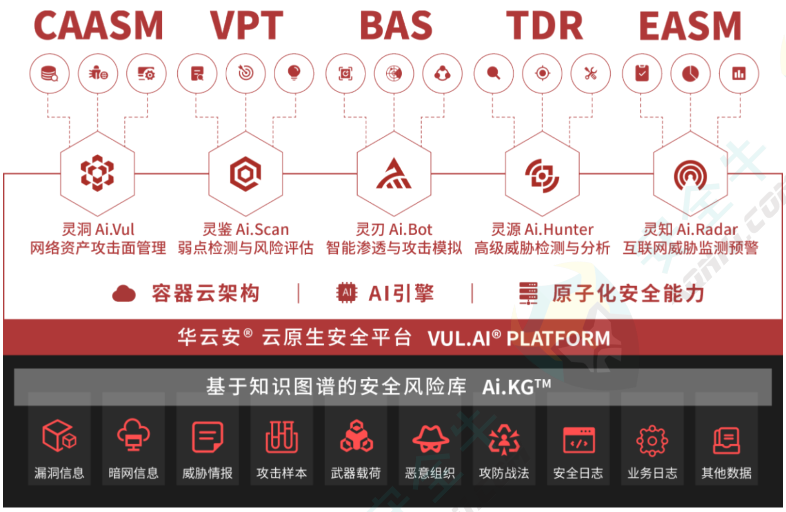
北京华云安信息技术有限公司（以下简称“华云安”）成立于 2019 年，致力于构建人工智能驱动的下一代网络安全防御体系，构建面向未来的智能化防御整体解决方案。自成立以来，陆续发布了灵洞·网络资产攻击面管理系统（Ai.Vul）、灵刃·智能渗透与攻击模拟系统（Ai.Bot）、及灵知·互联网情报监测预警中心（Ai.Radar）等核心产品；2023 年，公司继续深化安全验证产品与服务体系，构建了包括攻击面管理完整产品体系，以及围绕智能驱动的渗透测试即服务和红队服务。目前用户行业覆盖金融行业、电力行业、政府行业等。

◆ 典型产品介绍

- 灵洞·网络资产攻击面管理平台（Ai.Vul），网络资产攻击面管理平台，依托资产发现、弱点分析、情报共享、分析研判、运营响应五大环节，让客户以攻击者视角先于攻击者发现可能攻击的入口，并及时采取应对措施，一站式解决网络资产攻击面检测与管理难题。

- 灵刃·智能渗透与攻击模拟系统（Ai.Bot），有效性验证系统。对目标网络持续开展无害化的智能渗透和攻击模拟验证，确保安全防护策略有效运行；验证边界突破、内网横向移动等多种攻击场景下的安全防护体系的防御、响应能力，协助用户持续优化和补齐安全防护体系，持续推动企业安全防护实战化发展。

- 灵知·互联网威胁监测预警中心（Ai.Radar），互联网攻击面管理平台，可实现企业外部攻击面管理、情报威胁预警。



◆ 推荐理由

- 资产数据质量治理和资产关联

- 攻击路径可视化

- 安全验证能力

- 易用灵活的配置和定制化功能

- 深入了解金融行业需求

◆ **适合场景**

- 云上、云下全视角的数字资产治理
- 攻击面安全验证服务
- 攻击面风险路径测绘
- 互联网风险评估

（3）推荐厂商 - 绿盟科技

绿盟科技集团股份有限公司（以下简称“绿盟科技”）成立于 2000 年 4 月，绿盟科技基于多年的安全研究，秉持智慧安全 3.0 理念，致力于推动中国网络安全产业健康良性的发展。绿盟于 2018 年发布威胁和漏洞管理平台 TVM，2021 年发布防御突破模拟与评估系统 BAS，2023 年发布外部攻击面管理 EASM，2024 年发布持续性攻击面风险管理平台 CTEM，涵盖了攻击面管理的各个关键环节，从资产识别、威胁评估、攻击模拟到风险处置和安全运营，为企业提供了一套完整的攻击面风险管理解决方案。客户涉及金融、能源、运营商等行业。

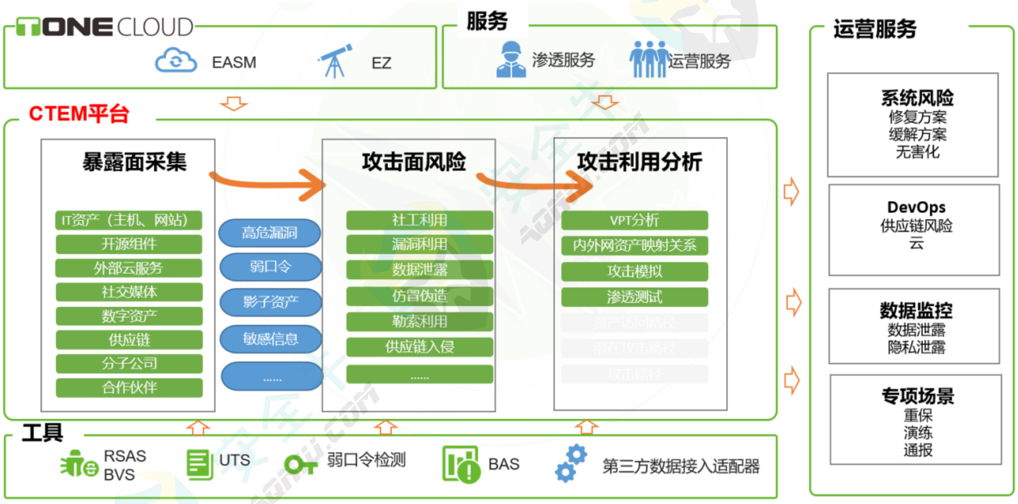
◆ **典型产品介绍**

- 绿盟 TVM 威胁和漏洞管理平台是一个全面的内网安全管理平台，整合了主动和被动探针、第三方平台数据和其他安全管理平台的数据，旨在帮助企业全面管理内网资产和风险。

- TVM 平台是发现和管理内网资产，包括主机、网络设备、数据库、中间件等，并提供漏洞扫描、修复建议和跟踪管理、弱口令检测、配置核查等功能。绿盟 BAS 防御突破模拟与评估系统通过模拟真实的攻击行为，帮助企业评估其安全防御体系的有效性。BAS 系统可以绘制网络拓扑，识别潜在攻击路径，模拟攻击者利用各种攻击技术躲避安全设备的检测，并进行 APT 攻击、勒索软件攻击、钓鱼邮件攻击等模拟，最终提供量化的评估报告和修复建议。

- 绿盟 EASM 外部攻击面管理服务是一个基于云端的安全服务，帮助企业识别和管理暴露在互联网上的资产和风险。EASM 服务通过主动和被动的方式收集互联网侧资产数据，结合情报和指纹识别技术，对企业外部攻击面进行持续监测和评估，提供风险预警、风险处置建议，并对多源数据进行治理和融合。

- 绿盟 CTEM 持续性攻击面风险管理平台整合了 TVM、EASM、BAS 等多种安全产品和能力，通过持续的泛资产识别、威胁评估和有效性验证、基于机器学习的 VPT 技术，专业的安全运营服务，建立全局视角、可落地的威胁管理机制，全局视角的运营度量和安全态势，实现对企业内外网资产全方位风险治理。



◆ 推荐理由

- 前瞻性的安全理念和风险管理方法论
- 较高的漏扫知名度和市场占有率
- 全面的安全能力和丰富的产品线
- 内外网泛资产和全方位风险治理
- 攻击路径的可视化
- 数据挖掘与分析利用

◆ 适合场景

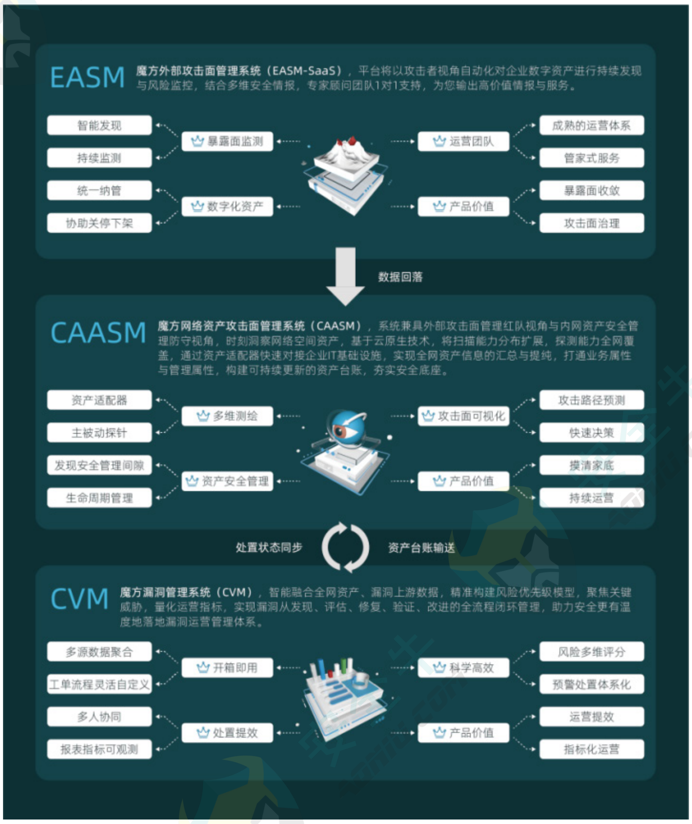
- 暴露面持续性闭环管理
- 内网与外网攻击面的综合管理
- 企业资产梳理
- 资产安全风险管理
- 漏洞验证分析和知识库运营管理

（4）推荐厂商 - 魔方安全

深圳市魔方安全科技有限公司（以下简称“魔方安全”）成立于 2015 年 10 月，由 CubeSec 网络安全攻防团队创立，是一家致力于驱动前沿科技保护数字安全的创新型公司。2015 年推出“外部攻击面管理平台”，2021 年，发布攻击面可视化管理解决方案（VASM）。已经为全国的众多客户所使用，覆盖金融、政府、交通等行业和大型企业等。

◆ 典型产品介绍

- 外部攻击面管理系统 EASM（SaaS）以攻击者的视角，自动化地对企业数字资产进行持续发现与风险监控，核心功能包括影子资产监测、漏洞情报分析、数字资产统一纳管、敏感信息下架处理，以及组织风险监测等。
- 网络资产攻击面管理系统 CAASM，实现“资产－风险－责任人”核心要素关联，建立可持续更新的资产台账，兼具外部攻击面管理的红队视角与内网资产安全管理防守方视角，洞察网络空间 IT 资产（传统 IP 化资产 + 数字化资产），主动掌控资产风险与动态。



◆ 推荐理由

- 外部攻击面精细化运营服务
- 攻击路径推演和可视化

- 基于合规模板和信创场景的检查

◆ **适合场景**

- 外部攻击面安全托管服务
- 多分支机构的大型企业的互联网安全治理
- 互联网暴露面敏感信息与数据交易监控

（5）推荐厂商－奇安信

奇安信科技集团股份有限公司（以下简称“奇安信”）成立于 2014 年，专注于为政企机构提供企业级产品、技术和服务，凭借持续的研发创新和以实战攻防为核心的安全能力，成为新一代网络安全领军者。公司愿景是成为全球第一的网络安全公司。目前客户行业涉及金融、电信、能源等行业。

◆ 典型产品介绍

- 奇安信网络资产攻击面管理系统（CAASM）是以多源资产数据融合分析为核心竞争力，基于“数据 + 运行”双核驱动模式，具备资产盘点、隐患识别、违规监测、响应处置能力的平台。基于奇安信自主研发的数据融合处理引擎，CAASM 通过 API 与安全系统、网络设备、IT 基础设施对接，对资产、风险、策略、业务、网络、组织、人员等数据进行融合和关联，构建时空动态的资产地图。通过数据碰撞，持续监测资产安全状态，精准识别高危资产和违规资产。
- 奇安信自动化渗透测试系统（EASM）是一款由奇安信自主研发的外部攻击面管理工具，拥有强大的资产发现及漏洞探测能力，以红队视角快速收集并持续监测企业暴露面脆弱性，通过底层智能算法与攻击链模型寻找可能的突破口，并通过内置 6000+POC 及 800+EXP 验证漏洞有效性及可利用性、给出漏洞修复优先级，帮助客户主动发现外部攻击面风险、真实检测系统安全防御能力。
- 奇安信网神安全有效性验证评估系统（天眼 BAS）是一款奇安信自主研发的入侵与攻击模拟系统，系统基于丰富的常态化威胁检测和预警方案，借助自动化攻击和编排能力，可对目标进行 7*24 小时的自动化多维度的攻击，从实战中找出网络与系统中存在的疏漏和失效点，发现防御体系潜在问题，对现有安全设备、人员安全意识、安全防御体系的有效性等进行量化评估，为企业提供可视化的安全运营指标，并持续性验证安全防御效果，给出真实可靠的安全评估结果，从而大幅降低安全效果评估测试对于人工的依赖，协助企业健全网络安全防护体系。

◆ 推荐理由

- 较高的知名度和市场占有率
- 聚焦安全实战，识别和评估攻击面
- 资产多源融合归一，构建时空动态的资产视图
- 数据驱动和安全运营持续提升
- 强调安全和信息化的协同管理
- 事前安全管理 + 技术视角的理念

- 人员经验赋能预置规则和知识库

◆ 适合场景

- 大型头部企业的资产攻击面管理
- 互联网暴露面监测和评估
- 攻击威胁研判告警和联动处置
- 攻击者视角发现安防机制弱点
- 专项与定制化漏洞发现与检测
- 持续自动验证安全防御有效性

（6）推荐厂商－矢安科技

上海矢安科技有限公司（以下简称“矢安科技”）成立于 2021 年，是一家创新型智能安全企业。公司提供基于攻防实战化的创新安全产品、服务及解决方案，运用 AI 及创新技术提升安全自动化、智能化程度，有效促进企业安全生产力。矢安科技致力于成为新一代智能安全的领跑者。2021 年发布 BAS 产品矢安攻鉴（AS BAS）突破与攻击模拟系统，2022 年 8 月发布矢安觅影（AS EASM）外部攻击面管理系统。目前研发团队规模 57 人，客户涉及金融、政府、能源、运营商、互联网等多个行业。

◆ **典型产品介绍**

- 觅影（AS EASM）是矢安科技的外部攻击面管理系统，可帮助企业跟踪监测各种互联网、社交媒体、暗网和深网环境，评估和分析数字资产的属性，发现和清点企业未知的面向外部的数字资产、系统、敏感数据等，系统对风险和漏洞进行优先排序和预警，并提供缓解措施或编排自动化响应流程，帮助企业快速降低风险。
- 攻鉴（AS BAS）突破与攻击模拟系统是以自动化、无害化的方式持续开展攻击模拟、验证企业安全有效性的安全产品，能够覆盖完整杀伤链的安全验证场景，包括钓鱼邮件、邮件网关、威胁情报、WAF、流量安全、终端安全、数据保护、容器安全等。并支持攻击剧本编排，允许基于真实攻击路径下的攻击模拟。

◆ **推荐理由**

- 结合 BAS 检测和提高人员安全意识
- 精细化服务和易用性
- 攻击路径推演和可视化
- AI 降噪技术深度集成
- 前瞻性的发展方向

◆ **适合场景**

- 互联网合规监管应对
- 安全防护验证
- 影子资产管理
- 分子公司资产安全
- 互联网数据安全

（7）推荐厂商 - 亚信安全

亚信安全科技股份有限公司（以下简称“亚信安全”），以护航产业互联为使命，以安全数字世界为愿景，以“懂网、懂云、懂安全”为优势基因，打造“云网安”一体的能力体系。。亚信安全于 2022 年发布攻击面管理解决方案，方案涉及星海·外部攻击面管理服务平台（EASM）、亚信安全 - 信端（TrustOne）/ 天穹 ImmunityOne、入侵与攻击模拟服务平台（BAS）、威胁情报等多款产品，涵盖 CAASM、EASM 和 BAS。服务客户分布于金融、、政府、电力等关基行业。

◆ 典型产品介绍

亚信安全攻击面管理解决方案，涵盖外部攻击面管理（EASM）、内部网络资产攻击面管理（CAASM），并结合威胁情报数据以提供更全面的安全保护。以攻击者视角来查看企业攻击面风险情况，协助企业以攻促防，常态化动态更新资产台账、收敛暴露风险，进而为企业安全运营提效。

亚信安全攻击面管理方案能力全景

◆ 推荐理由

- 红方视角，攻击视角理清数字资产
- 一键操作和攻击面排查即开即用，极具易用性
- 利用 AI 技术进行外部攻击面数据降噪和决策规则
- 提供泄露数据快速下架处置，实现风险闭环
- 内部终端的联动和丰富的虚拟补丁

◆ 适合场景

- 企业暴露面资产摸底梳理
- “两高一弱”专项检查
- 勒索风险防护联动治理
- 数据泄露风险排查和联动治理：
- 终端体检联动处置

（8）推荐厂商－知其安科技

北京知其安科技有限公司（以下简称“知其安科技”）2021 年，是一家致力于技术和产品创新驱动的新一代网络安全企业。2022 年 8 月发布陆吾网络资产攻击面管理平台，目前研发团队规模 40+ 人，产品已服务近百家金融、央企、智能制造、互联网等客户，

◆ 典型产品介绍

陆吾网络资产攻击面管理平台，网络资产攻击面管理平台，聚焦安全资产治理、资产风险治理、安全运营支撑三大类安全场景，通过对安全、运维、网络、管理侧的多来源资产数据重新融合，构建统一、全面、准确、保密的安全资产台账，帮助客户理清安全资产，梳理监管报送清单，收敛潜在攻击面，降低资产安全风险，显著提升安全运营效率。

◆ 推荐理由

- 资产数据质量治理
- BAS 平台联动实现安全验证
- 灵活和易用性
- 第三方产品快速集成能力

◆ **适合场景**

- 资产数据质量治理
- 防护度量和有效性验证
- 应急响应中心快速分析受影响资产范围
- 合规监管报送

（9）推荐厂商－知道创宇

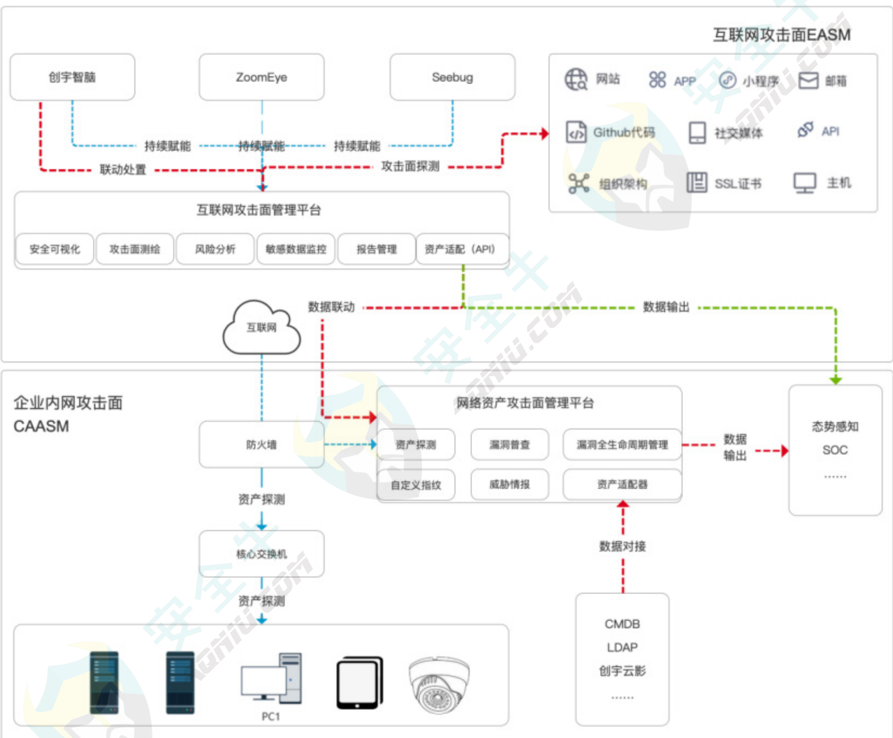
北京知道创宇信息技术股份有限公司（以下简称“知道创宇”）创立于 2007 年，由数位具有前瞻视角的安全专家创办，是一家立足攻防一线，与客户并肩战斗，拥有“实战对抗”能力，由大模型驱动的网络安全和认知域安全企业。2013 年发布 ZoomEye，全球网空资产测绘平台，2019 年发布 ZoomEye Pro、2021 年发布 ScanV 等产品，可全面覆盖外部攻击面管理和网络资产攻击面管理领域需求。目前研发团队 50+ 人，主要客户行业涉及运营商、电力、大型央企等行业。

◆ 典型产品介绍

- ZoomEye 是一个强大的网络空间搜索引擎，专注于目标和漏洞映射。它通过全端口扫描和持续探测，构建互联网安全全景观图，支持资产发现、风险分析、应急响应和网络安全保证。促进研究人员和企业迅速进行网络资产匹配，进行资产漏洞影响范围分析、应用分布统计、应用流行度排名统计等，提升网络安全能力。

- ZoomEye Pro 是一款面向企事业单位研发的网络资产扫描与管理系统，可以全面采集内外网资产并统一管理。能够快速更新高威胁漏洞插件并对全部资产进行漏洞影响面分析。具备资产发现能力快速精准、资产指纹信息丰富、资产分类清晰直观、漏洞响应能力强的特点，可以从攻击者视角持续发现内外网资产以及高风险问题，有效降低安全风险。

- ScanV 是从攻击者视角审视企事业单位互联网资产暴露面与脆弱性的 SaaS 产品，为单位提供持续全量资产发现与管理、风险监测与治理能力，实现互联网攻击面的梳理与收敛，成为网络安全合规与实战对抗中不可或缺的安全保护手段。



◆ **推荐理由**

- 基于 ZoomEye 历史数据、攻击、暗网等全面情报数据
- 攻击者角度的暴露面与脆弱性
- AI 数据挖掘和情报评估、多语言情报收集
- 内外网资产数据利用
- 供应链安全、外部暴露风险指数和动态情报表等前瞻性的发展方向

◆ **适合场景**

- 监控和治理互联网暴露面
- 资产全生命周期安全运营
- 监管合规检查
- 敏感数据泄露监控
- 供应链安全管理

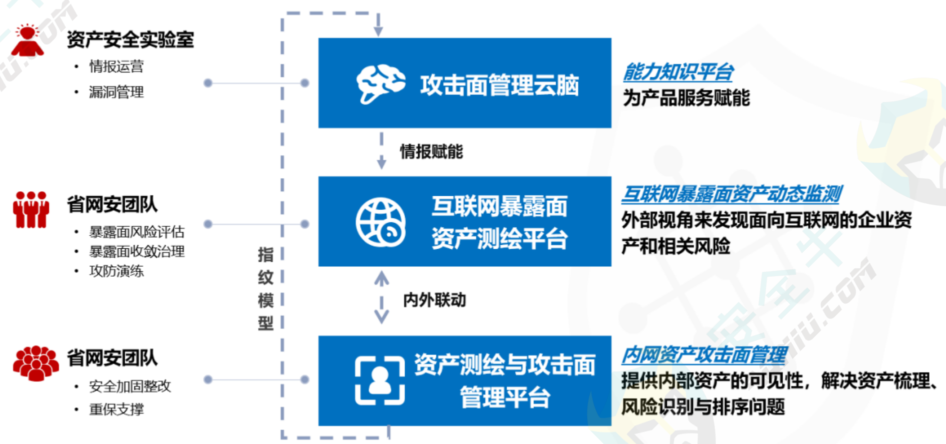
（10）推荐厂商 - 中国通服

中国通信服务（以下简称“中国通服”）成立于 2006 年，现有 22 家设计院，15 家 IT 服务公司，依托覆盖全国省、市、县三级的跨专业落地支撑体系和安全技术团队，为客户提供贯穿项目建设全生命周期（评估，咨询，设计，集成实施，涉密施工，监理，运维，应急，培训）的网络安全一体化综合服务。中国通服于 2021 年发布了资产测绘与攻击面管理平台，2022 年发布了互联网暴露面资产测绘平台，主要服务于运营商，金融，能源等行业客户。

◆ 典型产品介绍

- 资产测绘与攻击面管理平台；基于网络攻防实战的视角，采用主动和被动相结合的方式全面发现企业网络中的安全资产，通过实战化、自动化、智能化的技术手段持续探测网络资产安全风险，让资产安全可知、可见、可管、可核、可控。

- 互联网暴露面资产测绘平台；采用分布式主动扫描引擎 + 资产指纹图谱 + 漏洞检测引擎等多重核心技术手段，实现暴露面资产及攻击面从探测、识别到收敛的闭环管控，快速、准确、全面、动态的掌握全网的“暗”资产，自动绘制互联网暴露面资产动态地图，构建网络安全防护新常态，筑牢抵御攻击的第一道防线。



◆ 推荐理由

- 运营商大网资源优势
- 资产探测类型覆盖范围广，效率高
- 可应对大型企业复杂环境
- SOC 与攻击面深度融合
- 贴合产品 + 服务

- 专业的运营服务团队

◆ **适合场景**

- 内外网资产攻击面的统一发现和管理
- 互联网暴露面资产监测、评估
- 多区域大型企业资产管理
- 合规检查
- 大型关基企业的安全管理