攻击面管理产品市场分析报告

数说安全
CYBERSECURITY REVIEWS

2023 年 5 月 4 日

目录

法律声明

本报告版权归属于北京赛博英杰科技有限公司，报告中的文字、表格均受到中华人民共和国知识产权法律法规的保护，禁止任何商业性质的更改、报道、摘录以及引用；任何非商业性质的报道、摘录以及引用请务必注明版权来源，并获得北京赛博英杰科技有限公司的书面授权。

本报告中的调研数据均采用行业公开信息、深度访谈、实地调研、桌面研究得到。本公司不承担因使用本报告而产生的任何法律责任。

前言

“攻击面管理”是 2022 年中国网络安全产业热度上升比较快的词，过去从事网络资源探测、漏洞管理、自动渗透测试工具产品研发的公司纷纷推出自己的攻击面管理产品，或给自己打上“攻击面管理”的标签。数说安全为此分别做了供给侧、需求侧调研，试图搞清楚大家口中的攻击面管理到底是什么，攻击面管理在用户安全防线中定位是什么，其核心技术与能力是什么，各厂商的技术差别与产品定位是什么，各甲方单位的攻击面管理工作的痛点是什么，建设进度如何，以及通过数说安全商业分析平台对攻击面管理相关项目情况进行了分析，给出了攻击面管理市场的总结与展望。

最后，对从事攻击面管理的 26 家国外厂商及 21 家国内厂商做了分析和总结，并展示了其中 9 家国内厂商的解决方案与案例。

一、概述

网络攻击面是指黑客或攻击者在攻击时所能利用的网络漏洞和安全弱点的总和，对于组织而言，管理网络攻击面是保护网络安全的重要措施之一。

网络安全攻击面管理是对组织的网络资产进行全面分析，识别所有攻击者可能利用的漏洞和安全弱点，然后制定相应的防御措施和补救措施的过程。其目的是为了提高网络安全防御的有效性和韧性，以保护组织的网络资产免受各种威胁和攻击。

（一）主要发现

供给侧视角：国内攻击面管理市场厂商数量已达到 20-30 家，大多数厂商以资产测绘与管理、漏洞扫描与漏洞管理、威胁情报等作为核心能力，通过叠加微创新，参与市场竞争。

需求侧视角：客户侧目前最大的驱动力来源于实网攻防，通过产品或服务减小风险暴露面。最新发布的《信息安全技术 关键信息基础设施安全保护要求》中也提出了收敛暴露面等主动防御要求，未来或将推动需求由事件型驱动向合规驱动转变。

技术视角 1：EASM 和 DRPS 从产品技术、客户需求和应用场景来看具备一定的共通性和互补性，当前大部分 EASM 厂商通过自研或外购的形式整合了 DRPS 能力来提升产品竞争力，EASM 和 DRPS 的融合已经在市场中体现。

技术视角 2：EASM 可以作为 CAASM 在暴露面发现阶段的能力进行补充，同时完善内外网资产关联分析来挖掘更深层次的攻击面风险。随着厂商的技术能力增强，客户的需求度提高，CAASM 和 EASM 未来发展趋势将融合为一个平台来应对不同的应用场景。

技术视角 3：目前企业安全建设仍以内网安全为第一优先级，随着数据要素市场发展，

企业数据使用与流通加速，对于企业外部 IT 资产与数据风险，特别是针对敏感信息泄漏等情况，EASM 将是很好的能力补充。

资本视角 1（并购）：最近 3 年国外攻击面管理市场并购交易保持活跃，IT 巨头（IBM、Micrsoft、Google）和安全巨头（Palo Alto、CrowdStrike）通过收购 EASM 厂商，在现有产品上快速扩展对企业外部攻击面发现与管理的能力。但近 3 年还没有看到 CAASM 方向的并购。国内攻击面管理市场并购交易发生过两起：1、360 并购数字观星，将后者的企业网络资源测绘系统观星台与内部产品团队融合，共同打造攻击面管理产品线；2、联软科技并购魔方安全，补充外部攻击面管理解决方案。

资本视角 2（投融资）：从近五年的投融资数据统计看，攻击面管理赛道内公司融资进程提速明显。2022 年，海外的攻击面管理赛道一级市场的融资总额 9.98 亿美金，为 2018 年的 11.48 倍；融资公司数达到 11 家，共发生 13 轮融资。国内 2022 年攻击面管理赛道融资企业 5 家，共发生 5 轮融资，相较于 2018 年的 2 家公司共进行 3 轮融资，活跃度明显提升。从融资企业所处阶段看，有处于创业中期的华顺信安及华云安，但多数为初创企业（未岚科技、云科安信、零零信安等），赛道整体仍处于爬升期。

市场视角：狭义的攻击面管理市场主要指客户采购明确的攻击面排查、网络资产测绘及管理、威胁情报获取等攻击面管理产品及服务形成的市场，目前我国狭义攻击面管理市场正处于起步阶段。广义的攻击面管理市场应包含可纳入该领域的所有安全产品及服务，例如漏洞发现与管理、网络资产测绘及管理、威胁行为检测、攻击链路绘制、风险评估、优先级评估及排序、响应处置等领域，2022 年广义攻击面管理市场规模约 26 亿元。

（二）推荐

甲方单位网络安全与风险管理负责人应当：

- 考虑采用攻击者视角重新审视自己的网络安全防御方案，发现防御的盲区，重新调整防御的优先级；
- 攻击面管理的部署顺序考虑 EASM 与 DRPS 服务先行，CAASM 跟上；
- 中小企业考虑采用相对低成本的 EASM，大型企业应考虑 EASM、CAASM、DRPS 整合解决方案；

网络安全公司产品负责人应当：

- 投入研发资源解决客户对资产管理能力满意度低的问题，在数字资产发现、整合方面提升用户可用性；
- 解决客户已有资产管理系统、漏洞管理系统的能力整合问题，而不是简单替代；
- 关注自动化、AI 能力加持，减少对企业网络安全运营人员的要求；
- 建议加强云上资产发现与攻击面管理能力；

二、市场定义

（一）攻击面管理的起源

2018 年，Gartner 敦促安全领导者开始减少、监控和管理他们的攻击面，作为整体网络安全风险管理计划的一部分，并且在 2021 年发布的《Hyper Cycle for Security Operations，2021》中将攻击面管理（ASM，Attack Surface Management)相关技术定义为新兴技术，这被大家公认为是“攻击面管理”这个名词做为一种网络安全产品类别的起源。

（二）攻击面是什么？

美国国家标准与技术研究院（NIST）对攻击面的定义是：“位于系统、系统组件或环境的边界上的一组入口，攻击者可以从这些入口尝试进入、产生影响或从中提取数据。”（The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.）。

攻击面是所有可从 Internet 访问的处理或存储数据的硬件、软件、SaaS 和云资产，将其视为网络犯罪分子可用于操纵网络或系统以提取数据的攻击媒介的总数。 攻击面包括：

- 安全或不安全的资产
- 已知或未知资产
- 影子 IT

- 活动或非活动资产
- 托管和非托管设备
- 硬件
- 软件
- 软件即服务（SaaS）
- 云资产和资源
- 物联网设备
- 供应商管理的资产：攻击者不会由于跨越组织边界而停止攻击，恰恰相反，通过供应链进行攻击是当今攻击者常用的手段。
- 流氓资产：包括恶意软件、错误域名或仿冒组织域名的网站或移动应用程序等由攻击者建立的 IT 资产。

每天有数百万的此类资产出现在 Internet 上，并且完全不在防火墙和端点保护服务的范围内。其他名称包括外部攻击面和数字攻击面。

攻击面=可被攻击利用的暴露面
可被攻击利用=可利用的机会 × 攻击能力

来源：未岚科技

图 1：攻击面的组成

（三）攻击面管理是什么？

不同机构对攻击面管理的定义略有区别，但大同小异。

IBM 对攻击面管理的定义：攻击面管理（ASM）是对构成组织攻击面的网络安全漏洞和潜在攻击向量的持续发现、分析、修复和监控。

Michael Cobb 对攻击面管理的定义：攻击面管理是对组织的 IT 基础设施的持续发现、清点、分类和监控。

Cycongnito 对攻击面管理的定义：攻击面管理是发现、分类和评估组织所有资产安全性的持续过程。

CrowdStrike 对攻击面管理的定义：攻击面管理是对组织 IT 基础架构内的攻击媒介进行持续发现、监控、评估、优先排序和补救。

Mandiant 对攻击面管理的定义：在当今的动态、分布式和共享环境中发现和分析互联网资产，持续监控已发现资产的风险敞口，并使情报和红队能够实施风险管理并为风险管理提供信息。

Palo Alto Networks 对攻击面管理的定义：攻击面管理（ASM）是持续识别、监控和管理所有内部和外部互联网连接资产以发现潜在攻击向量、暴露和风险的过程。

国内的赛迪顾问在《中国攻击面管理市场研究报告，2022》中将攻击面管理定义为：攻击面管理是一种从攻击者的角度对企业数字资产攻击面进行检测发现、分析研判、情报预警、响应处置和持续监控的资产安全性管理方法。

数说安全综合以上各方的定义，结合对攻击面管理工作的要点，对攻击面管理的定义为：**攻击面管理（ASM）**是持续发现、分析、监控和评估内部和外部资产以发现潜在暴露面、攻击向量和风险，并进行优先排序、响应处置的过程。

《信息安全技术 关键信息基础设施安全保护要求》中的“收敛暴露面”就是攻击面管理的目的之一。

（四）攻击面管理解决的主要问题是什么？

帮助防御者发现自己的盲区：由于思维方式和所拥有的技术技能的不同，攻击者与防御者往往会存在视角上的重大不同，人不可能对自己认知范围之外的事情做出有效应对，引入攻击者视角，将会很大程度上帮助防御者发现自己所忽略的，或视野之外的安全威胁。

帮助防御者合理排定工作的优先级：防御者的工作是纷繁复杂的，所拥有的资源也是有限的，需要对防御工作进行优先级排定、做出取舍与折衷，攻击者视角可以帮助防御者有针对性的防御，提高资源利用效率。

三、核心能力

攻击面管理是一个多能力交叉的复合型领域，涵盖了资产、漏洞、攻防、情报、大数据分析等多个维度，这些特性之间存在较强的依赖关系，因此每个能力的缺失或薄弱都会对产品实际效果产生影响。举例来说，如果不能全面获得资产的可见性，攻击面的发现与收敛就会存在盲区，而如果兼顾了资产，但攻击者视角不够真实，风险评估的结论也会存在局限性，导致防御资源调配不合理甚至错误。

从技术角度看，一个优秀的攻击面管理方案需要多维深厚能力的加持，而对于上面这些能力项，放在当前国内市场中无一不可撑起一条单独的赛道，需要的是长时间的技术打磨与积累。因此，对于在国内尚处于技术萌芽期的攻击面管理领域来说，无论 CAASM、EASM 还是 DRPS，国内供给端厂商大部分呈现出能力分散、各有所长的局面。

从技术角度分析，攻击面管理的核心能力，至少应该包含以下 6 个方面：

1. 资产管理能力：通过主动式扫描、网络流量解析、第三方应用集成、数据爬取、主机代理等多种方式，识别企业 IT 资产和数字资产的过程。良好的资产管理能力将有助于企业管理者获得对资产全面的可见性，是攻击面发现与收敛的重要前提。资产管理的主要特性包括：

- 资产发现能力：通过多种手段发现企业内、外部的 IT 资产与数字资产。
  - 互联网资产发现能力：通过网络空间测绘、数据爬取等技术发现企业在互联网上存在的资产，包括但不限于 IP、域名、Web 应用、云应用、移动应用、物联网等已知和未知资产；
  - 内网资产发现能力：通过主动式扫描、网络流量解析、第三方应用集成等技术发现企业内部的资产，包括但不限于已使用的 IP/端口/服务/证书、主机、服务器、网络与安全基础设施、IT 应用与业务系统、开源组件、API 应用、BYOD 设备、供应链等已知和未知资产；
  - 恶意资产发现能力：对网络钓鱼、应用仿冒、品牌侵权等恶意资产欺诈风险的监测能力；
- 资产信息整合能力：通过对多种来源的资产信息进行聚合分析（信息来源可信度比较、信息去重、信息富化、唯一性判定、资产标签化等），构建资产间和资产与业务间的关联关系，形成可视化视图，并对资产状态（上下线、权属变更）进行监控；

2. 脆弱性管理能力：通过漏洞扫描、对接第三方扫描器、自动化渗透测试/BAS、基线扫描等多种方式，对企业的暴露面进行脆弱性检测，找到企业暴露面中的弱点，发现潜

在的攻击路径，并对风险的优先级进行排序，推动防御体系的优化。脆弱性管理的主要特性包括：

- 基于指纹的漏洞发现能力：对匹配到指纹特征的资产进行漏洞扫描，而不是全网探测方式，提高漏洞检出效率，进一步达到无损扫描效果；
- 基于 POC 的漏洞发现能力：基于 POC（漏洞验证程序）或者 EXP（漏洞利用程序）等方式去发现漏洞的能力，保证漏洞检测的准确性和真实性，减少系统资源消耗和带宽占用；
- 敏感信息泄露发现能力：通过对互联网邮件、网盘、文库、github、深网暗网等渠道的数据获取，识别出企业泄露的敏感信息，并发出警报；
- 威胁评估能力：通过不同的攻击向量探测资产可能面临的威胁，主要以漏洞为主，并结合弱口令、配置错误、网络钓鱼、不当权限等其它弱点识别方式；
- 威胁优先级评定能力：全面评估威胁风险后结合 CVSS 或 VPT 技术，以攻击者视角推演潜在的攻击路径，给出高优先级的风险清单；
- 补丁管理能力：提供从漏洞发现到处置的闭环管理机制；

3. 情报能力：通过引入威胁情报、漏洞情报以及数字情报等能力，扩大对企业风险面的识别；

4. 渗透测试能力：组织能够对自身网络资产进行渗透测试，模拟攻击者的攻击行为，识别和评估网络安全防御的有效性和韧性；

5. 攻击防护与缓解能力：通过对外交互接口，实现攻击面风险闭环管理，包括但不限于与 SOC/SIEM/SOAR/XDR 等系统集成或提供可被调用的 API 接口；

6. 安全意识和培训能力：社会工程学攻击的对象是组织中的人，组织为员工提供相

关的网络安全培训和意识提升，帮助员工提高对网络安全的认识和防范能力。

图 2：攻击面管理核心能力代表性厂商

四、市场方向

（一）技术维度

攻击面管理与零信任的技术互通性

零信任是当今网络安全市场最热的领域之一，零信任的核心是基于访问者/设备的维度，对其身份进行持续多维度认证，对其访问资源的权限进行细粒度的、动态的控制。

由于零信任策略的部署只能在已知存在的资产上实施，因此攻击面管理在资产测绘、资产映射梳理、终端监控、威胁情报监测等方面的覆盖度和完善度，有助于零信任的有效落地。同时零信任核心技术之一的 SDP（软件定义边界），使访问需要先授信后认证再连接，业务被完全隐藏到代理网关后端，从而实现网络、应用、业务攻击面收敛。

攻击面管理在整体防御体系中的定位与核心价值

结合滑动标尺模型和网络防御矩阵 CDM 模型(https://cyberdefensematrix.com),综合分析攻击面管理（CAASM/EASM/DRPS）的定位与价值:

CAASM 技术处于滑动标尺模型的“积极防御”阶段，其建设优先级与 SOC、SIEM、XDR 等运营平台相同。加入人工参与，对网络内部威胁进行监控、响应、知识总结与沉淀，对防御体系进行持续完善。

EASM、DRPS 技术处于“威胁情报”阶段，基于积极防御阶段的运营平台建设，加入组织面向互联网的资产数据和可在攻击发生期间被利用的缺陷情报总和。

安全团队对自身攻击面的可见性反应了机构整体安全状态的成熟度，被美国政府写进网络安全战略的零信任解决方案将攻击面管理中的资产可见性视作整体防御体系的基石——NIST 在《零信任架构》迁移步骤的首要任务就是：“迁移到零信任架构需要组织对其资产（物理和虚拟）、用户（包括用户权限）和业务流程有详细的了解。”

攻击面管理技术通过对设备、应用、网络、数据及用户五类资产进行实时的全面识别、监测和关联分析，联动“基础架构”及“纵深防御”阶段的技术工具对攻击实施防护。以往的“积极防御”阶段，通过安全编排、自动化和响应与其他工具的驱动，在威胁检测和事件响应方面取得了进步。在处理较熟悉的已知攻击过程中，有助于降低平均检测时长（MTTD）和平均响应率（MTTR）。但在面对复杂或者未知攻击过程中，因为缺少业务访问的上下文关系或剧本编排，安全运营中心下的团队及工具不会自动响应及处置，将任由流量穿行在网络当中。理想的攻击面管理技术通过对环境变化的自动跟踪和评估，可以了解环境的全面、准确、最新的视图。有了对资产、上下文以及它们之间关系的细粒度的理解，组织可以利用自动化运营，进一步降低 MTTD 和 MTTR。

（二）市场维度

CAASM 与 EASM 的整合

从技术角度来看，CAASM 与 EASM 的主要区别在于暴露面发现（资产识别方式和资产识别类型）及产品形态（私有化和 SAAS）。CAASM 的资产识别方式主要以对接第三方资产系统+主动扫描，资产识别类型主要以内部资产为主，产品形态主要为私有化部署。而 EASM 的资产识别方式主要是主动扫描和数据爬取，资产识别类型主要以互联网资产为主，产品形态主要为 SAAS 部署。在脆弱性检测、攻击面分析和风险处置等攻击面管理阶段，两者在技术上具备一定的相同性。从市场需求来看，CAASM 当前主要面向大中型安全成熟度较高的客户对自身内部资产的攻击面管理，而 EASM 可面向大中小微型客户对自身互联网资产的攻击面管理，两者在市场需求方面具备一定的互补性。

综上分析，从 CAASM 和 EASM 的产品技术发展和客户市场需求方面来看，短期内，两种形态的产品仍会在市场上并存一段时间，即使当前有部分厂商可同时提供这两种攻击面管理能力，多数也会定义为不同的产品进行销售，来应对客户的不同需求。但从产品和技术的发展趋势来看，平台化技术融合在攻击面管理领域同样势在必行。未来，随着攻击面管理厂商的技术能力增强，客户的需求度提高，EASM 可以作为 CAASM 在暴露面发现阶段的能力进行补充，同时完善内外网资产关联分析来挖掘更深层次的攻击面风险，CAASM 和 EASM 将会融合为一个平台来应对不同的应用场景。

EASM 与 DRPS 的融合

无论从产品技术、客户需求和应用场景来看，EASM 和 DRPS 都具备一定的共通性和互补性。当前大部分 EASM 厂商通过自研或外购的形式也都已经整合了 DRPS 能力来

补足产品的竞争力，适应更广泛的客户需求。EASM 和 DRPS 的平台化融合已经在市场应用中逐步体现。

（三）产业维度

国内网安产业现状对攻击面管理技术发展的影响

从我国网安产业发展历程来看，等保制度实施 16 年+，网络安全法实施 6 年+，大多数企业已经完成了以合规为驱动的安全体系建设，将逐步进入到深耕细作、持续安全运营的阶段，平台化产品成为市场新的供需热点。攻击面管理作为定位于积极防御阶段下的平台化产品，将成为继 SOC、态势感知、XDR 之后，市场上新的热点方向。由于国内攻击面管理市场处于起步阶段，市场规模和客户认知度有限，对于产品定义、能力边界以及各厂商对 CAASM、EASM、DRPS 方向的布局还在不断演变的过程中。

从国外的情况看，因为有可观的市场底量做基础，国外厂商在 CAASM、EASM、DRPS 方向的把握上会更聚焦，通常只专注于单一方向，并且得益于成熟的产业基础，国外厂商会充分利用开放的生态优势，通过投资并购、应用集成、数据对接等方式，完成产品的快速研发与迭代升级，既保证了产品的创新性与全面性，也避免陷入到低 ROI 困境。从产品具体细节的对比来看，例如在资产数据采集中，国外产品大多采用第三方应用集成的方式，而国内则多以主被动扫描为主，虽然从产品部署的灵活性、对资产识别的精细度和有利于技术长远发展的角度来看，应用集成是更经济的方式，但受限于国内封闭的生态环境，各厂商不得已只能将其作为一种辅助手段，只是在项目需要时被动实施。仅从应用集成的数量对比来看，国外主打 CAASM 方向的 Axonius 宣称已集成了

550 个常见应用，而国内在这方面比较突出的厂商，包括 360 数字安全、华云安、魔方安全、雾帜智能，其集成的应用数量不超过 100 个。

综上，国内攻击面管理市场的发展离不开网安产业和生态的进步。在合规时期，单打独斗或许是一种常态，但进入到主动防御、动态防御、体系化防御的新时代，无论是攻击面管理、还是 XDR、SOC/SIEM、零信任这类对底层能力广度和深度有较高要求的技术整合型领域，单一厂商很难做到面面俱到，只有坚持共创共享的发展理念，推动生态环境开放，引导产业协同创新，才会使各厂商更专注在自身核心竞争力的打造上，而对于不擅长的领域，可以通过开放的生态体系相互赋能、取长补短，这样在能力规划上做到主次分明，实现缩短技术革新周期的同时，保障业务全面均衡的成长，最终促进行业整体水平进步，加速网安产业高质量的发展。

攻击面管理与数字经济和数据安全的关系

数字经济是支撑未来全球经济发展的重要推动力，数据资产作为助力企业数字化转型、创造经济利益的新生产资料，也同样成为了黑产的首要目标。2022 年 12 月，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》，明确了加快构建我国数据基础制度，激活数据要素潜能，做强做优做大数字经济，增强经济发展动能的新目标。意见印发不到一个月后，工业和信息化部、国家互联网信息办公室等十六部门联合印发了《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》，明确指出了数据安全产业的发展任务，即从供给侧为保障国家数据安全提供技术、产品和服务支持，助力数据要素市场培育和价值释放，夯实数字中国建设与数字经济发展。通过以上不难看出，数据安全已经不再像网络安全那样孤立存在，对于未来数字经济的长期发展来说，数据安全已成为了促发展、保发展的必要基础之一。

传统的数据安全技术主要包括了数据库安全相关、数据泄漏防护、数据脱敏，新技术包括了数据分类分级、隐私计算、数据安全管控平台。这些技术主要面向企业内部管理者视角，即在清楚企业内部有哪些数据应用和数据资产的前提下，对其进行加固和防护，对于未知或不可见的数据应用与资产则无法起到保护作用。如果数据流转到企业外部以后，数据可见性和可控性的问题可能会变得更糟糕，特别在互联网风险面中，涉及企业敏感信息、源代码数据、机密文档、个人隐私信息等数据的泄漏，很难通过传统内网的数据安全手段进行监测和管理，这也是目前企业数据安全建设中容易被忽视的问题。如何构建内外兼顾的数据安全整体方案，攻击面管理可以做相应能力的补充，其价值可凸显在下述 3 个方面：

- 通过 EASM、DRPS 方案，补充企业外部互联网数据风险监测的能力，对邮件、网盘/文库、github 代码平台、深网暗网等渠道泄漏的企业敏感信息、业务账号、源代码等数据资产进行识别；
- 通过 CAASM 提升企业管理者对内部数据应用与资产的风险识别能力，进一步加强对承载数据资产的 API 资产、移动资产、业务资产、未知和隐藏资产的发现和防护能力，提高数据安全防护体系的健壮性；
- 提高企业数据安全整体能力，改变被动防御和静态防御的态势，通过引入攻击者视角和辅助对抗手段，推动安全关口前移，向积极防御、动态防御模式转变。

五、市场分析

我国的攻击面管理市场还处于早期阶段，大多数用户的注意力仍然停留在漏洞发现与管理、资产发现与管理、威胁情报、攻击模拟等单体能力建设与完善方面，只有少量客户将这些领域综合起来，形成相对全面的攻击面防护与管理建设。长期来看，随着用户需求和厂商技术、产品的不断提高，漏洞扫描和管理、网络资产测绘与管理市场、威胁情报、模拟攻击等市场将不断汇集融合，纳入到攻击面管理领域。

我国攻击面管理的热度不断提升，2022 年受疫情影响，相关项目的采购数量与上年基本持平，但项目的采购平均规模明显提升，专项项目的比重也从 2021 年的 10.3%增长至 2022 年的 12.7%，用户对攻击面管理的重视程度不断提升。

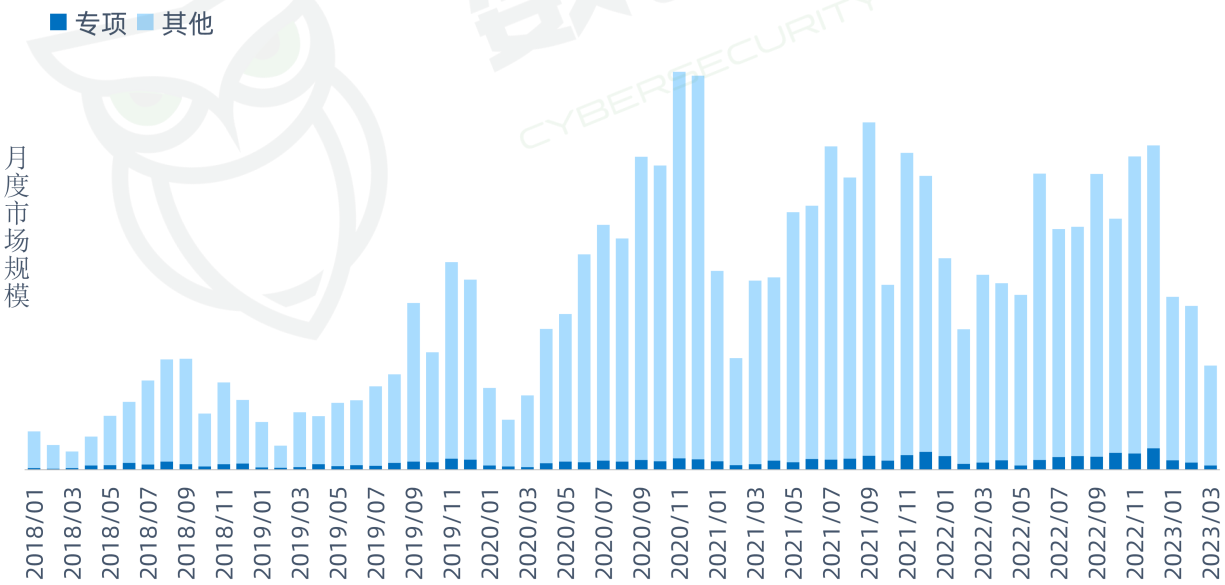


图 3：2018 年-2023 年 3 月攻击面管理采购热度趋势

攻击面管理客户近三年的行业分布中，TOP5 行业占整体比重的 81.3%，分别是政府、教育、医疗卫生、公检法司和电信（见图 2020-2022 年攻击面管理项目分布）；但在专项项目采购的行业分布中，金融和电信行业占比明显提升（见图 2020-2022 年攻击

面管理项目分布（专项）），说明这两个行业对攻击面管理的重视程度较高，以攻击面单独立项的项目占比较多；而政府、教育、医疗卫生、公检法司行业中的大部分客户对攻击面管理，采购网络安全产品仍是主要形式，对运营工作的重视程度仍有待提高。

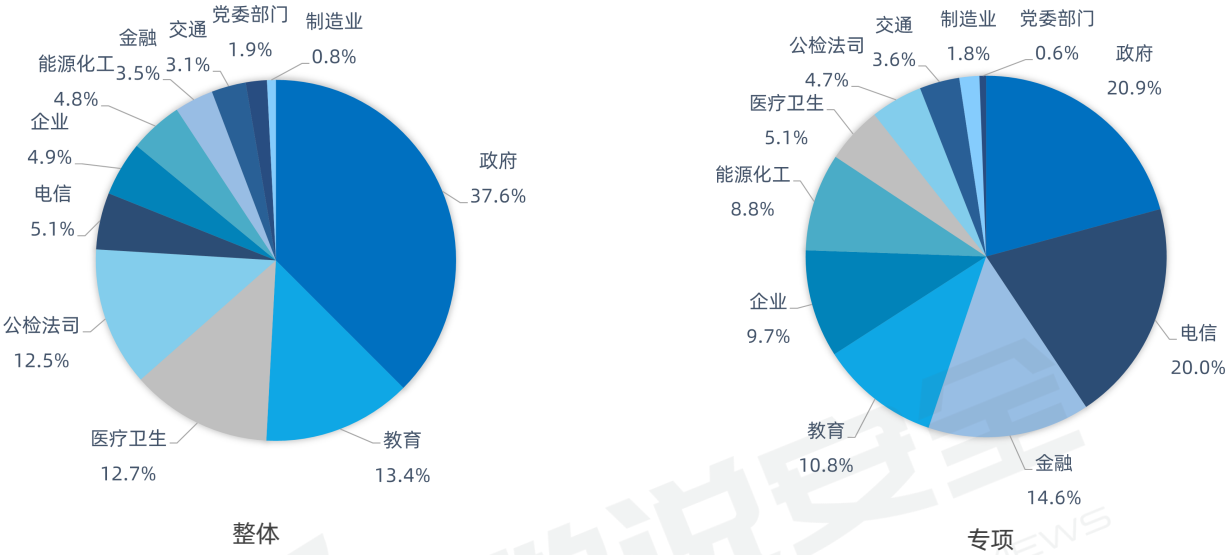


图 4：2020-2022 年攻击面管理项目行业分布

2020-2022 年攻击面管理项目采购的 TOP20 关键客户如下图所示：

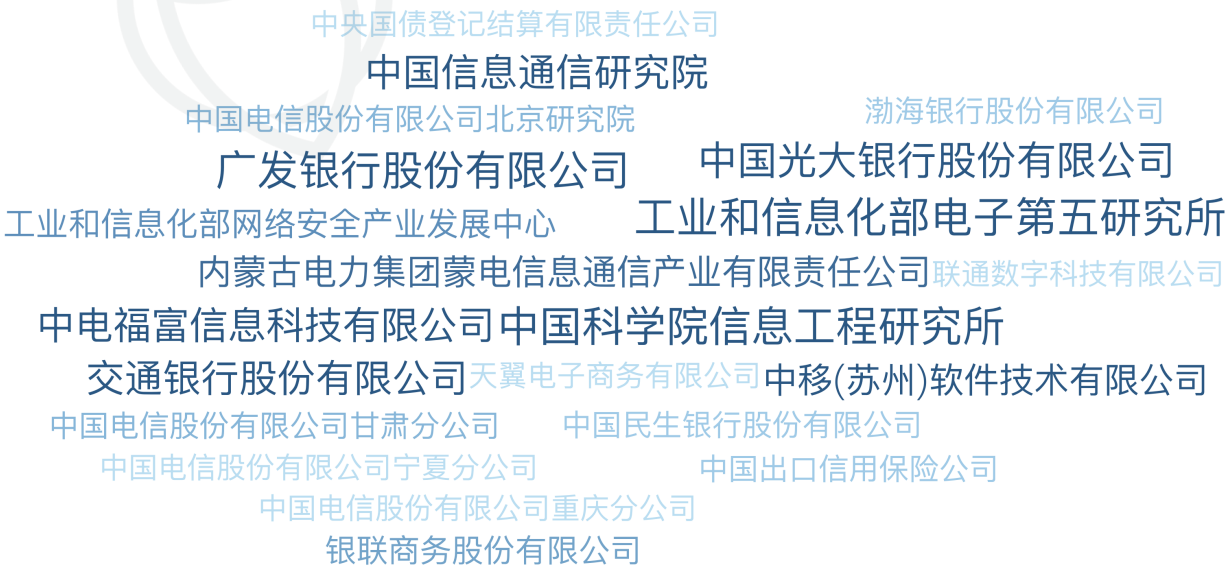
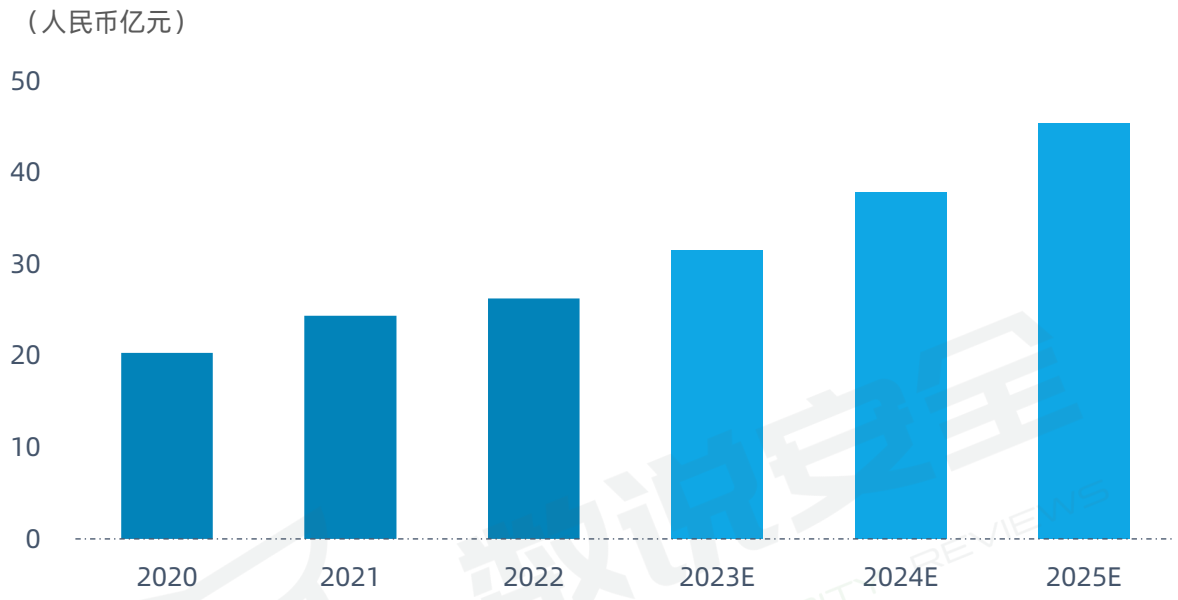


图 5：2020-2022 年攻击面管理项目 TOP20 客户词云

目前采购攻击面管理相关产品的年采购客户数量不足一万，随着用户对网络安全运营的更加重视，攻击面管理市场的不断融合汇聚，客户采购数量和单价不断增加，作为网络安全运营平台重要组成部分的网络安全攻击面管理市场将会持续快速增长。



数据来源： 数说安全 CSRadar 商业分析平台

图 6：2020-2025 年中国网络攻击面管理市场规模及预测（亿元）

根据数说安全 CSRadar 商业分析平台对上述市场的综合数据统计，广义口径上，2022 年我国攻击面管理市场规模约 26 亿人民币，同比增长约 8%，随着网络安全运营的兴起以及对攻击面管理的认知，未来三年的年均增速预计会到 20%左右，2025 年广义的攻击面管理产品和服务的市场规模有望达到 45 亿元人民币。

六、用户调研

数说安全联合安在新媒体做了《2023 中国网络安全市场攻击面管理产品用户调研报告》，针对国内近百家甲方企业，从企业背景、企业自身 IT 与网络安全管理现状、攻击面管理产品与用户需求匹配度、攻击面管理产品用户实际使用情况、攻击面管理产品未来投入等多个方面进行了调研，最终得到结果如下：

（一） 关键发现

- 漏洞扫描、漏洞与补丁管理、网络资产管理仍是作为目前企业发现与管理自身攻击面的最主要产品，采购专业 CAASM 和 EASM 产品的用户比例仅为 11%和 15%，市场渗透率远低于传统安全产品。
- 不同于传统安全产品以合规导向为主，攻击面管理产品由技术与合规双轮驱动，现有能力无法持续监测攻击面的变化、符合监管或审计要求是目前企业实施攻击面管理的两大最主要因素。
- 超过 50%以上的企业认为 IT 资产管理和未知资产发现上存在不足，而认为满意的企业比例仅为 15%和 11%，良好的资产发现与管理仍是企业目前亟待解决的核心问题。
- 办公网、数据中心、公有云、私有云是企业 IT 资产分布最主要的区域，并且有 60%的企业认为目前攻击面扩大的首要原因是将数据和资产转移到云端，因此，未来云上资产识别与管理将成为企业 IT 风险管理中新的关注重点。

- 全面的资产可见性与动态管理、漏洞发现与优先级管理，这两项能力，既是产品功能层面用户最关注的两个主要特性，也是用户认为现有产品最主要的两个不足。
- 对于攻击面管理产品来说，94%的企业选择将预算投入控制在百万以内，而在这部分企业中，有 70%认为预算将不超过五十万。

（二） 企业背景

被调研企业所属 TOP3 行业分别是：金融（21%）、互联网公司（19%）、商业企业（15%）。

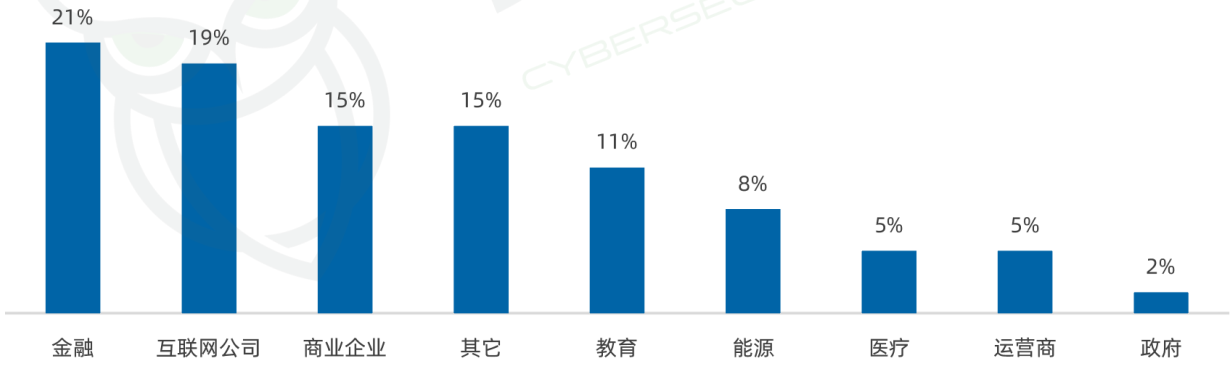


图 7：被调研企业所属行业

被调研企业的 TOP3 类型分别是：私营企业（48%）、央国企（29%）、外资企业（13%）。

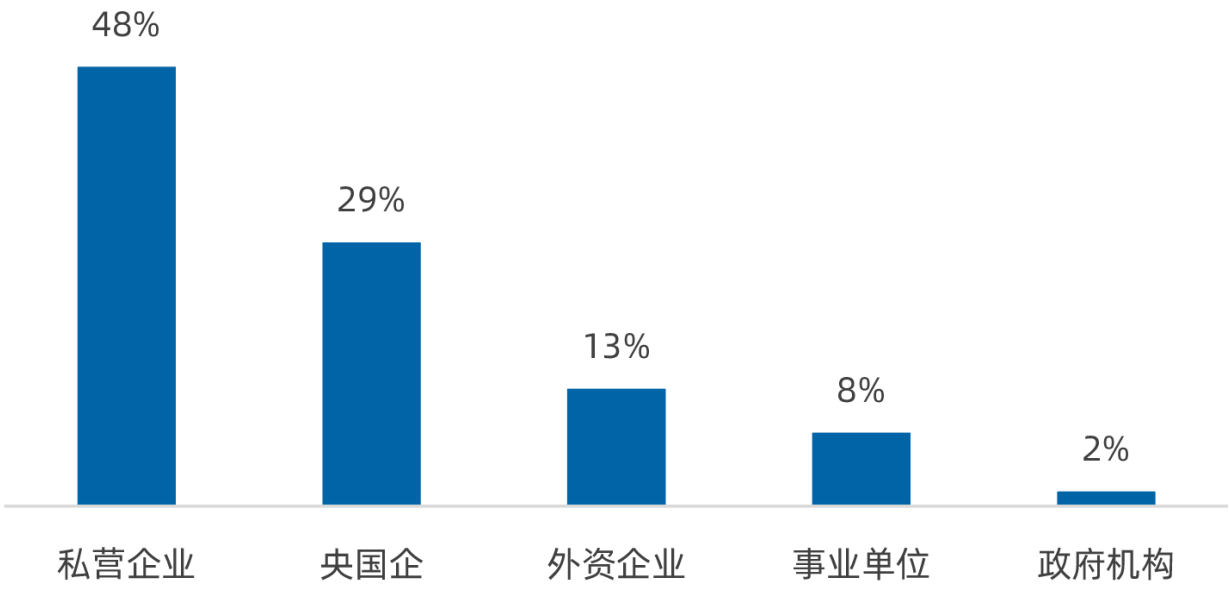


图 8：被调研企业类型

被调研企业安全管理团队 TOP3 规模分别是：5 人以下（34%）、6-10 人（27%）、11-20 人（16%），另外有 8%的企业无专职网络安全人员。

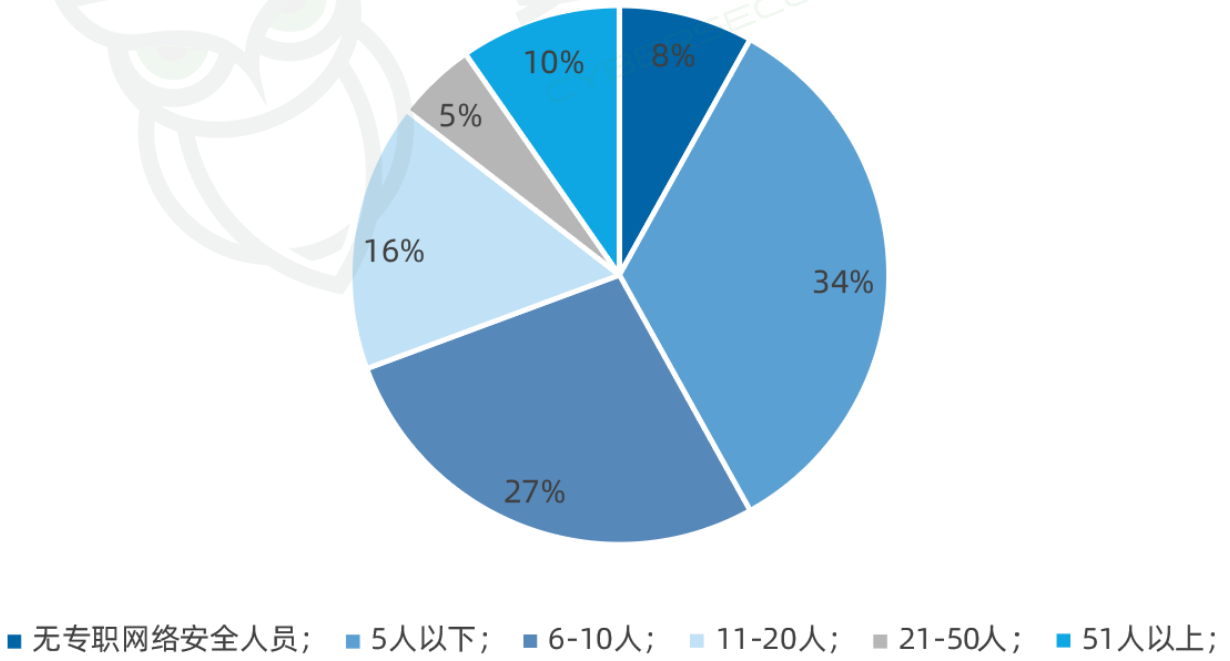


图 9：被调研企业安全管理团队规模

(三) 企业自身 IT 与网络安全现状

企业 IT 资产分布最多的 3 个区域分别是：办公网、数据中心、公有云。

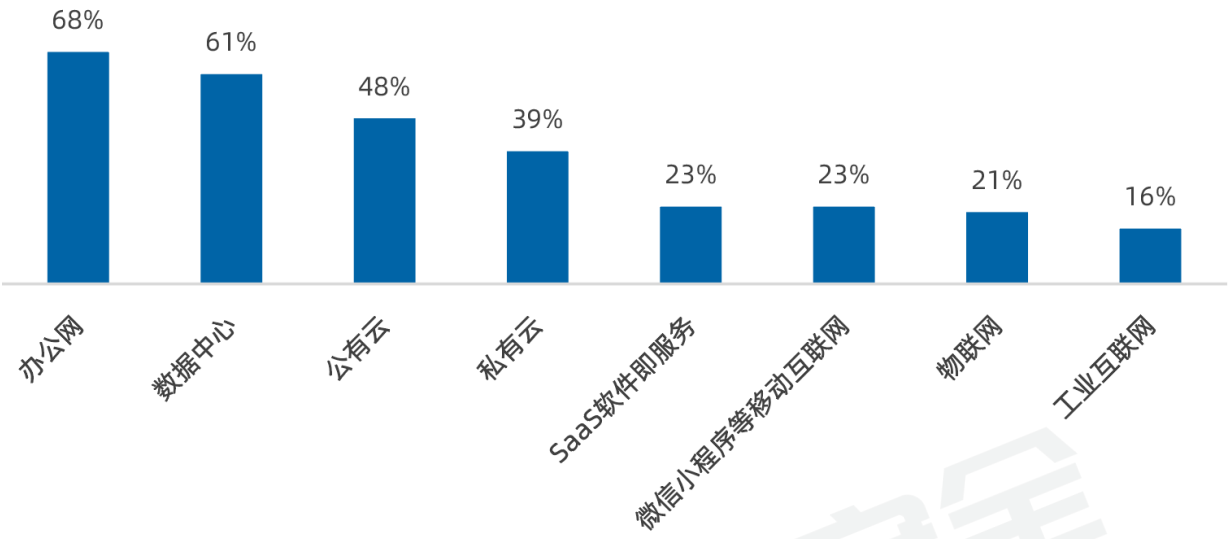


图 10：被调研企业 IT 资产区域分布

企业 IT 资产管理能力：有 52%的企业认为没有或只有较弱的资产管理能力；只有 15%的企业认为可以将资产管理系统与 SOC/SIEM/SOAR 系统进行有效整合，赋能安全运营。

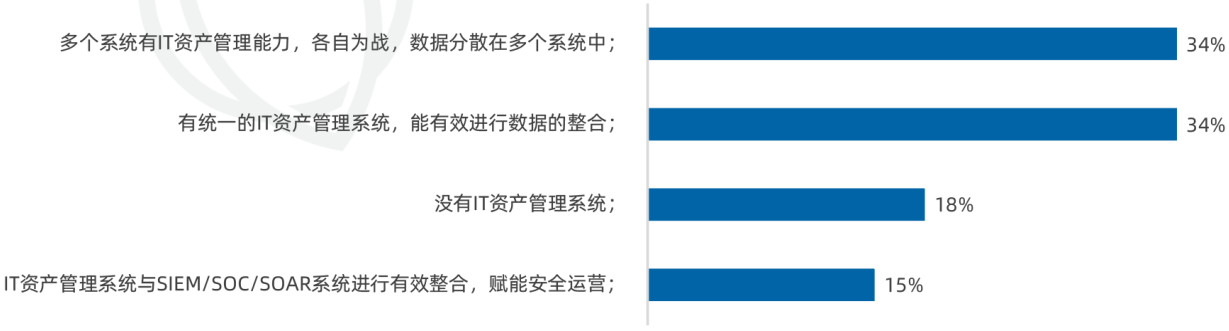


图 11：被调研企业 IT 资产管理能力自我评价

企业未知资产发现能力：有 58%的企业认为存在较大不足；只有 11%的企业认为可以很好的发现未知资产。

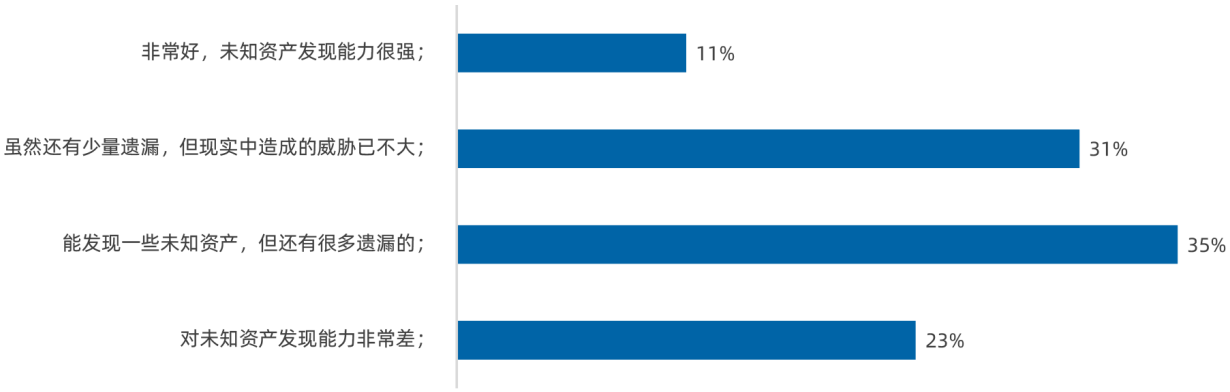


图 12：被调研企业未知资产发现能力自我评价

组织攻击面不断扩大，企业认为最主要的 3 个原因是：将更多的数据和资产转移到云端、组织中影子 IT 的增加、更多设备被添加到需要资产管理的组织；

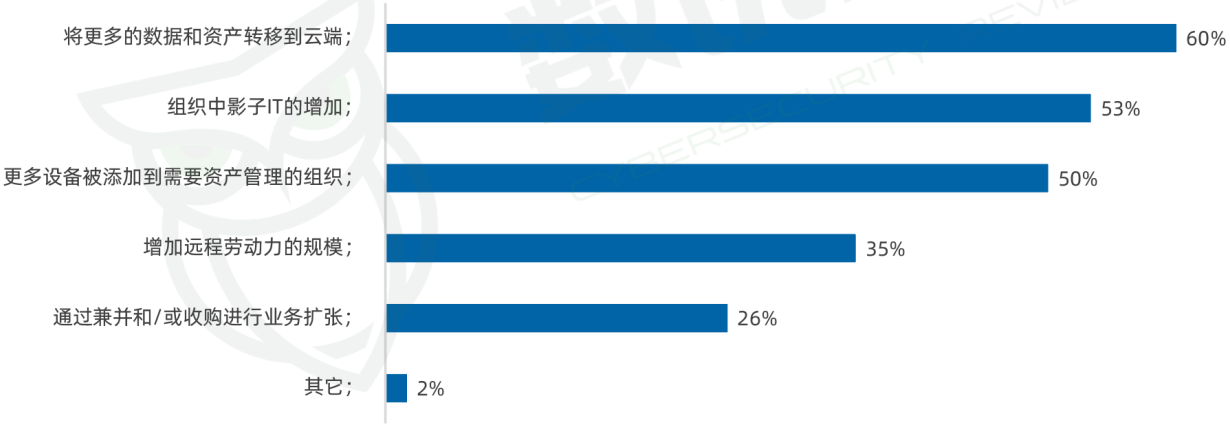


图 13：被调研企业攻击面扩大的原因

企业通过资产识别与漏洞发现，实现攻击面管理，购买最多的 3 个产品是：漏洞扫描产品（79%）、漏洞与补丁管理系统（60%）、网络资产管理系统（47%）。而对于 CAASM 和 EASM，已购买的比例仅有 11%和 15%。

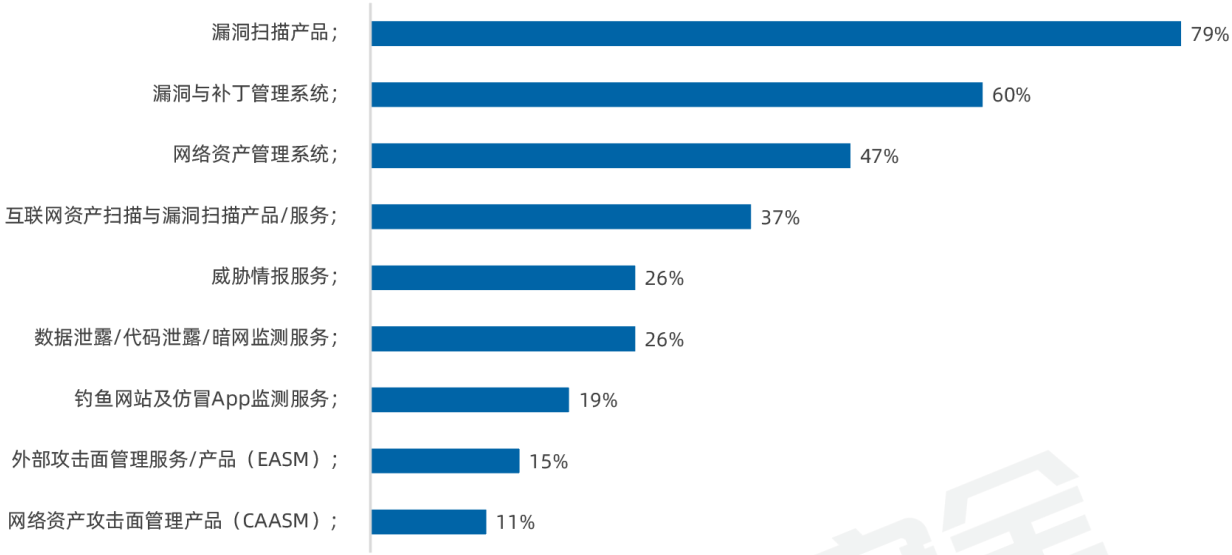


图 14：被调研企业管理攻击面的主要产品

（四） 攻击面管理产品与用户需求的匹配度

驱动企业实施攻击面管理的最主要 3 个原因是：现有能力无法持续监测攻击面的变化（68%）、符合监管和/或审计要求（65%）、难以发现企业外部的新 IT 资产（55%）；

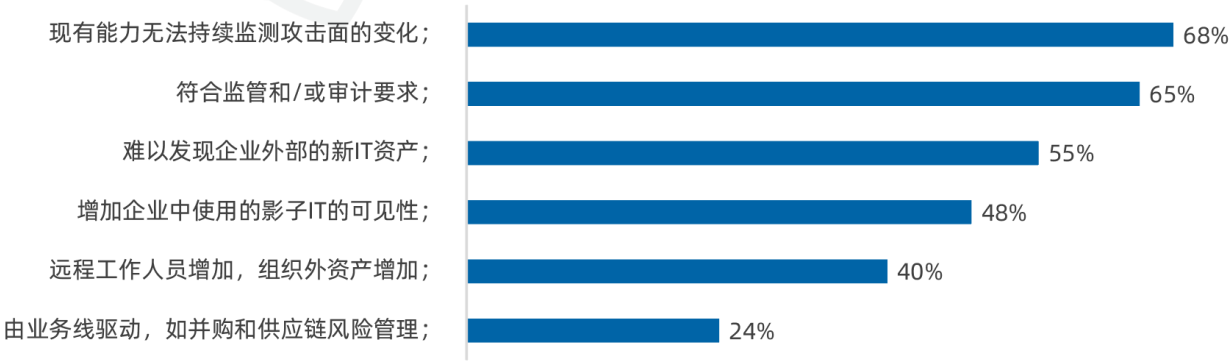


图 15：被调研企业实施攻击面管理的驱动力

如果选购攻击面管理产品，企业最关注的 3 个功能特性是：动态监控和警报 IT 资产状态的变化（58%）、整个企业 IT 资产盘点、整合和分类（53%）、集成漏洞管理和优先级（45%）。

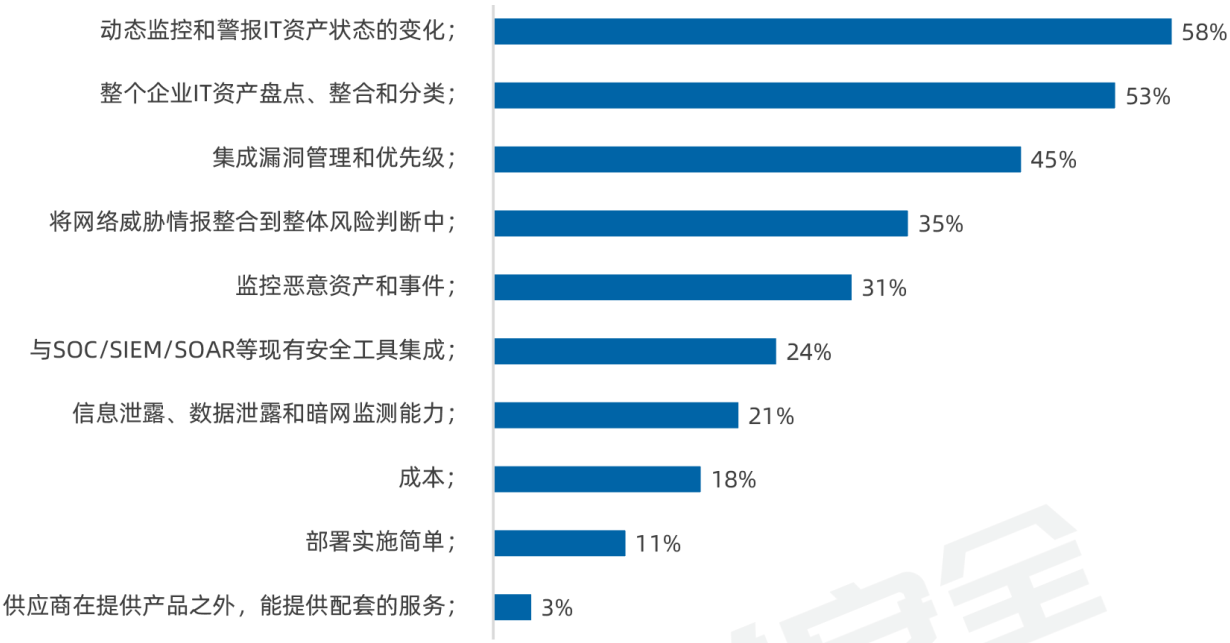


图 16：被调研企业关注攻击面管理产品的主要功能特性

(五) 攻击面管理产品实际使用情况

企业对现有 CAASM 产品的满意度：有 47%的企业对已购买的 CAASM 产品不满意，主要原因是资产管理、漏洞发现、漏洞优先级排序方面不能满足企业要求。仅有 13%的企业对已购买的 CAASM 产品满意，而另有 40%的企业还没有购买 CAASM 产品；

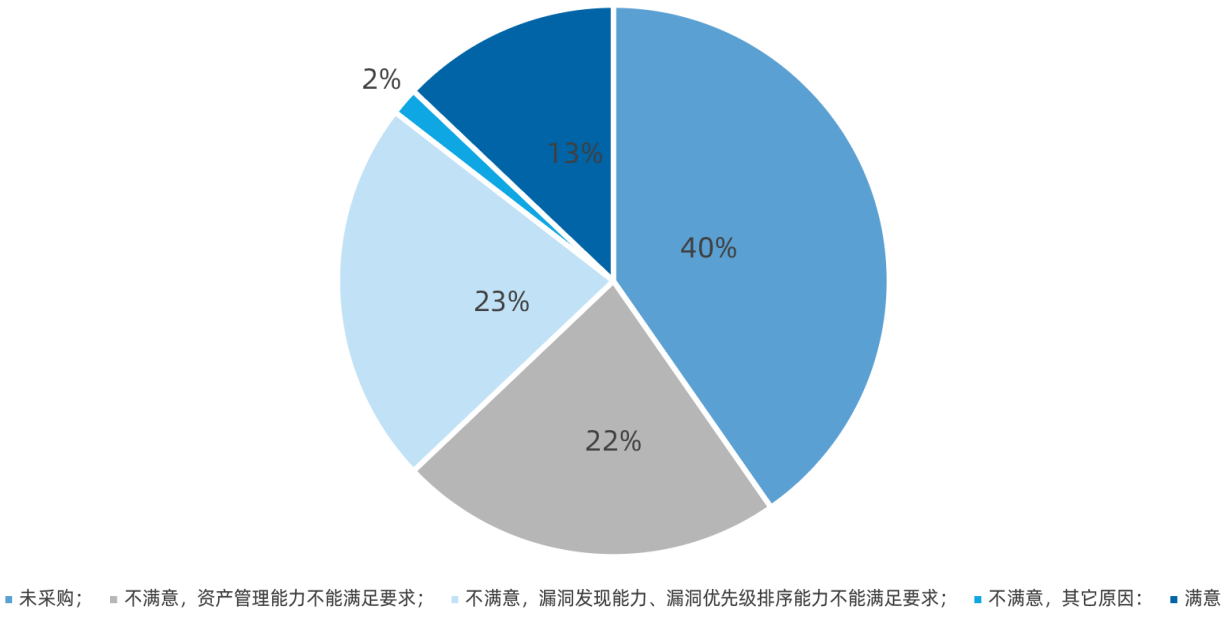


图 17：被调研企业对现有 CAASM 产品的满意度

企业对现有 EASM 产品的满意度：有 40%的企业对已购买的 EASM 服务不满意，主要原因在于较多的漏报和误报，有 23%的企业对购买的 EASM 服务满意，而另有 37%的企业还没有购买 EASM 服务；

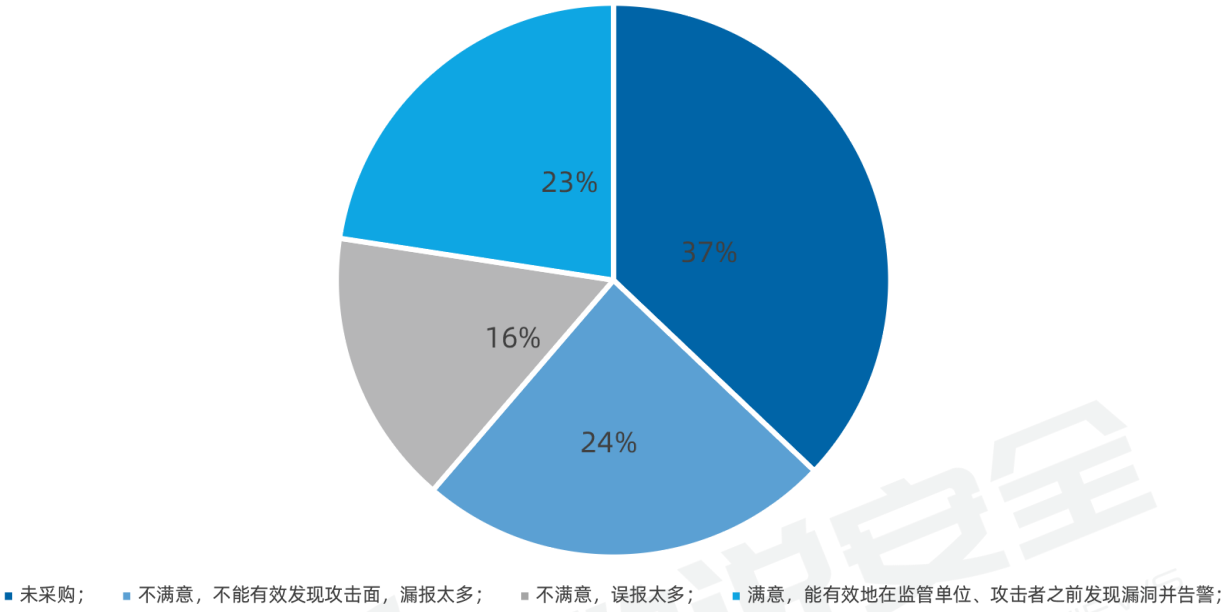


图 18：被调研企业对现有 EASM 产品的满意度

企业对攻击面管理产品集成威胁情报的满意度：有 52%的企业对攻击面管理产品集成威胁情报的效果不满意；

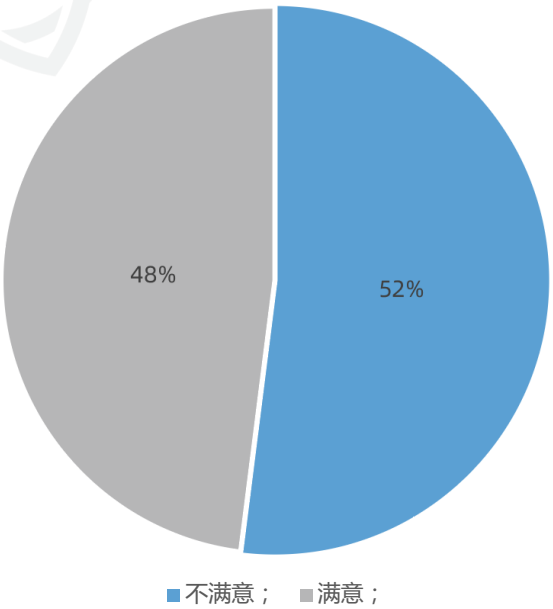


图 19：被调研企业对攻击面管理产品集成威胁情报的满意度

企业对攻击面管理产品与安全运营平台集成的满意度：有 52%的企业认为不满意，难以将攻击面管理产品集成到企业安全运营平台中，有 19%的企业认为可以完美集成，而有 29%的企业则认为没有将两者集成的需求；

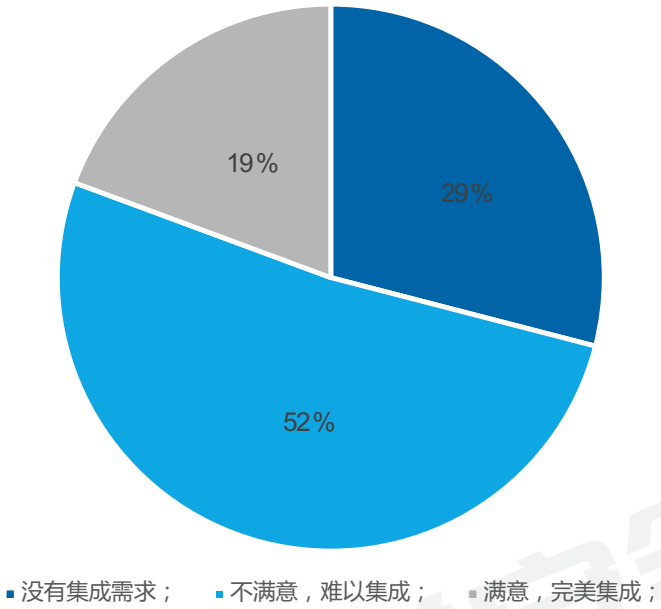


图 20：被调研企业对攻击面管理产品与安全运维平台集成的满意度

企业认为目前使用的攻击面管理产品，最主要的 5 个不足分别：漏洞发现能力(58%)、缺乏对某些资产(如 OT、物联网、云等)的可见性（48%）、漏洞扫描或 POC 验证对业务系统产生的负面影响（脏数据、系统停服等）（39%）、风险评级的科学性（37%）、无法获得 IT 资产的实时或动态视图（35%）。

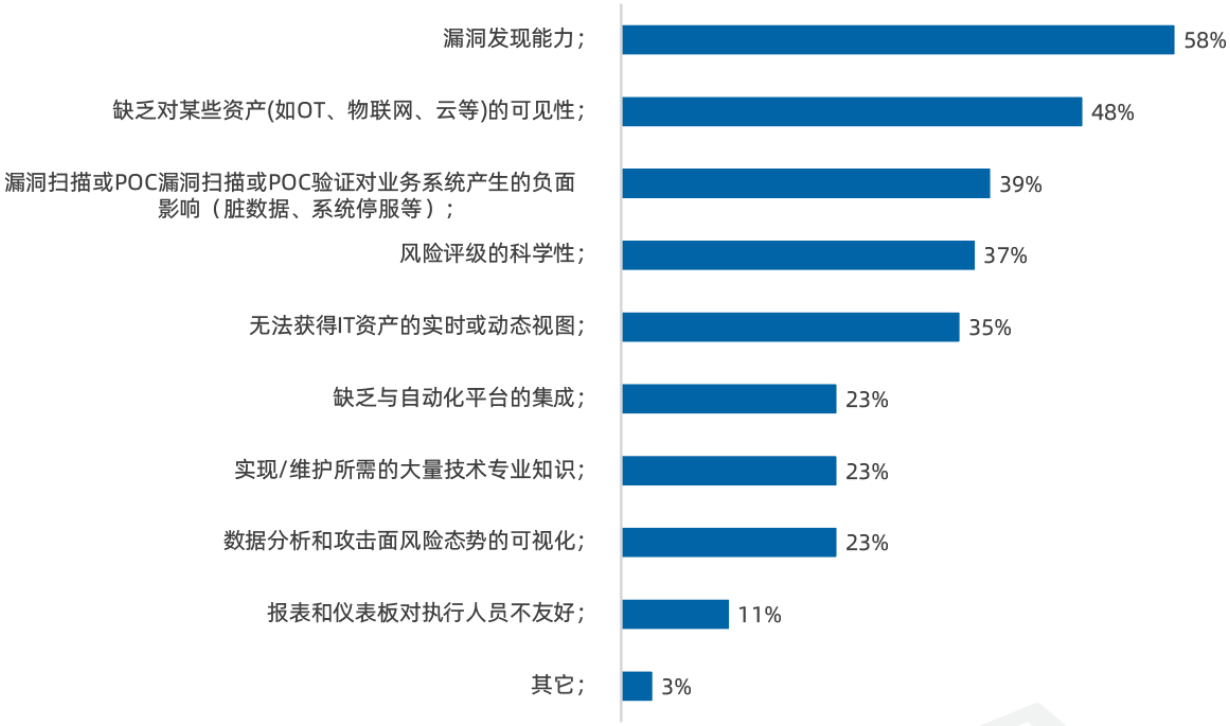


图 21：被调研企业认为现有攻击面管理产品的主要不足

（六） 攻击面管理产品未来投入

企业采购攻击面管理产品的时间周期：有 24%的企业表示将在一年内采购攻击面管理产品，有 42%的企业表示虽在关注产品但未列入当年预算，有 15%的企业则表示尚未考虑；

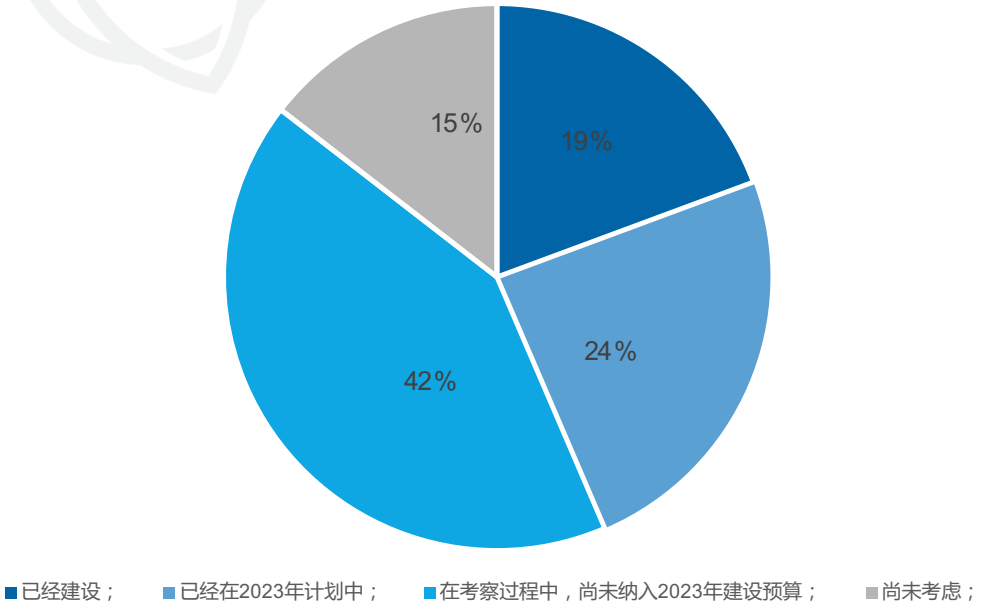


图 22：被调研企业采购攻击面管理产品的时间周期

企业建立攻击面管理体系的技术路线：有 35%的企业希望建立 CAASM+EASM 一体化的攻击面管理系统，有 35%的企业认为应该先从 CAASM 入手，而有 24%的企业认为先从 EASM 开始。

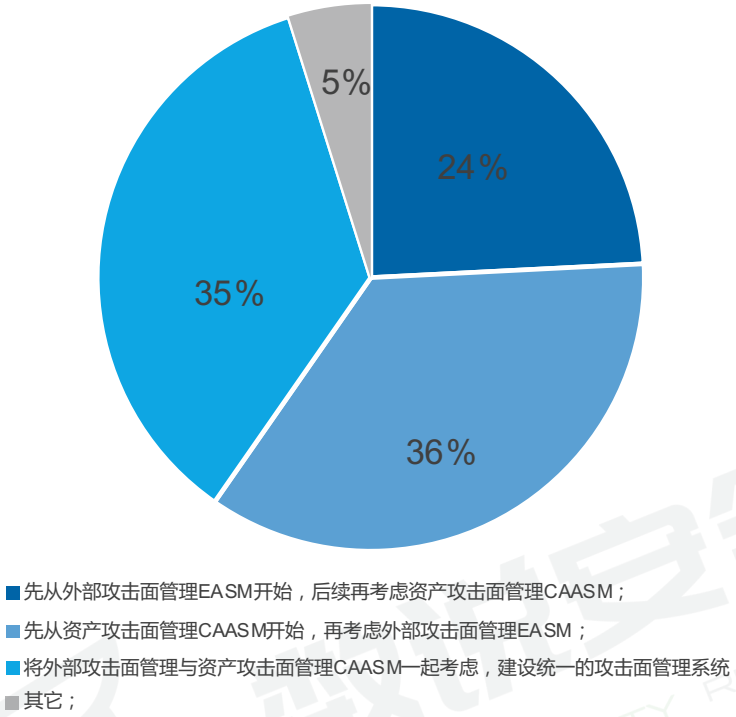


图 23：被调研企业建立攻击面管理体系的技术路线

企业购买攻击面管理产品的预算投入：每年可用于攻击面管理产品的预算范围，有近 70%的企业选择了 50 万人民币以下，24%的企业表示可以在 50 万-100 万人民币，只有 6%的企业认为可以在 100 万人民币以上。

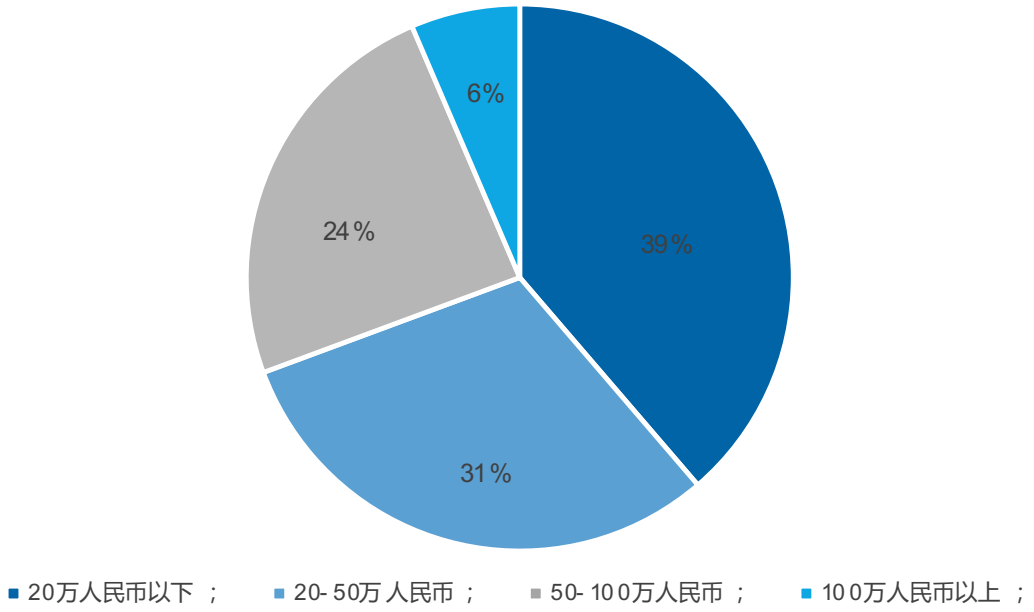


图 24：被调研企业购买攻击面管理产品的预算投入

七、国外攻击面管理赛道投融资状况分析

近三年，国外攻击面管理市场的主要并购项目如下表。从并购方情况看，既有 IT 巨头，包括 Microsoft、IBM、Google（已收购的 Mandiant 在 2021 年收购攻击面管理厂商 Intrigue），也有网络安全巨头，包括 Palo Alto、CrowdStrike。从被并购方的情况看，业务类型非常一致，全部为 EASM 和 TI 方向。目前还没有看到 CAASM 方向的并购。

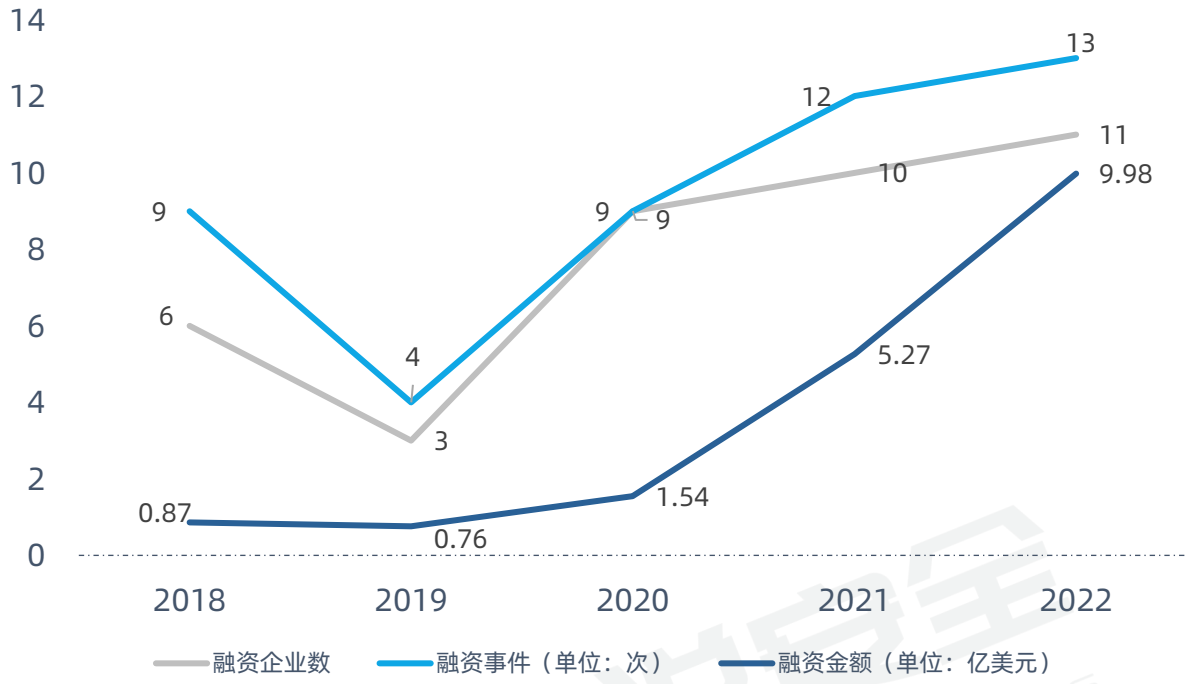
结合并购的具体内容可以看出，头部厂商通过对 EASM 厂商的收购，将外部攻击面管理技术与现有安全产品进行集成，在传统安全，例如：端点安全、XDR、威胁情报、电子邮件安全等产品上，扩展对企业外部攻击面风险发现与监测的功能。

并购时间	项目名称	创立时间	业务类型	并购方	金额	并购背景说明
2022.11	SpiderFoot	2005	TI EASM	Intel 471	未披露	Intel 471 TITAN 平台可为全球网络安全企业和专业人员提供专业的网络犯罪情报，SpiderFoot 是 github 上一个开源网络情报工具，通过整合大量 OSINT 数据源，采集互联网 ip、域名、电子邮件、电话号码等信息，形成对企业外部攻击面的监测。收购 SpiderFoot 可以对 Intel 471 情报方案形成互补和增强。
2022.10	Hardenize	2016	EASM	Red Sift	未披露	Red Sift 专注于电子邮件和品牌保护，Red Sift 平台提供入站和出站电子邮件保护，阻止钓鱼邮件等风险。Hardenize 外部攻击面管理技术可以帮助 Red Sift 不断扩展识别其它互联网资产的风险，将 Red Sift 现有解决方案扩展到保护电子邮件之外。
2022.9	Reposify, Ltd.	2016	EASM	CrowdStrike	1890 万美元	Reposify 平台扫描互联网以查找组织暴露的资产，以在攻击者利用它们之前检测并消除易受攻击和未知资产的风险。CrowdStrike 将 Reposify 作为其威胁情报的一部分，为客户提供差异化的 EASM 体验套件，将对端点和 IT 环境的深入洞察与互联网扫描功能相结合，提供跨内部和外部攻击面的企业风险对抗视图。
2022.6	Randori	2018	EASM	IBM	未披露	IBM 计划将 Randori 的攻击面管理软件与 IBM Security QRadar 的扩展检测和响应 (XDR) 功能相集成。通过将 Randori 的洞察力输入 QRadar XDR，安全团队将能够利用实时攻击面可见性进行智能警报分类、威胁搜寻和事件响应。
2022.1	SecurityTrails	2017	EASM	Recorded Future	6500 万美元	SecurityTrails 收集、存储、维护当前和历史的互联网记录，包括域名记录、注册数据和 DNS 信息等，可为 Recorded Future 威胁情报平台提供数据，两家公司从 2018 开始成为技术合作伙伴。

2021.8	RiskIQ	2009	EASM TI	Microsoft	5 亿美元	通过收购全球威胁情报和攻击面管理领域品牌 RiskIQ，增强 Microsoft 365 Defender、Microsoft Azure Defender 和 Microsoft Azure Sentinel 等产品对多云、混合云环境下威胁保护、检测和响应的能力。收购 RiskIQ 1 年后，微软推出 Defender 外部攻击面管理(EASM) 和 Defender 威胁情报产品。
2021.8	Intrigue	2019	EASM	Mandiant（Google 已收购）	1230 万美元	将 Intrigue 集成到 Mandiant Advantage SaaS 平台中，实现外部攻击面管理技术与 Mandiant Advantage 平台威胁情报、安全验证和自动防御功能的融合，扩展为客户提供的专业知识与情报。
2020.12	Expanse	2012	EASM	Palo Alto	8 亿美元	Palo Alto Networks Cortex™ 产品套件提供了针对企业内部可见性、威胁、检测和响应的功能，收购 Expanse 后，会将其互联网资产发现和数据归属等能力与 Cortex 集成。

表 1：近三年国外攻击面管理市场的主要并购项目

融资方面，成功融资的企业数量、融资事件近三年稳步增长，融资金额则从 2021 年起快速提升，去年已实现近 10 亿美元的融资额，说明一级市场对该领域内公司的发展前景的看好。



（说明：数据基于公开信息整理）

图 25：2018-2022 年国外攻击面管理赛道融资情况

八、代表性供应商

（一）国外厂商

1. Randori（EASM）

Randori 成立于 2018 年，是一家以黑客思维为主导的进攻型公司。Randori 攻击面管理解决方案使用了更符合现实的攻击逻辑，攻者视角在传统漏扫、POC 等方式上深度结合了 ATT&CK、BAS 和红队技术，通过使用 Randori 自有 Target Temptation 风险评分模型，将攻击方法与目标资产的业务价值、业务影响以及现有安全控制和补救措施相结合，识别出对攻击者最有吸引力的风险，从而构建实时的高优先级风险清单，同时基于双向 API

集成，Randori 可以将攻击面发现能力快速嵌入到 SIEM、SOAR 等生态系统。

2022 年 6 月，IBM 完成对 Randori 的收购，并将 Randori 攻击面管理软件与 IBM Security QRadar 扩展检测和响应（XDR）方案进行集成。

2. UpGuard（EASM）

UpGuard 成立于 2012 年，作为一家数据驱动型公司，UpGuard 提供外部攻击面管理和轻量级数字风险保护 SaaS 服务。通过每天 8000 亿次数据采集，UpGuard 可以识别出企业外部六大类安全风险，包括：网站风险、电子邮件安全风险、网络安全风险、网络钓鱼和恶意软件风险、企业品牌与声誉风险。UpGuard 使用经过实战考验的风险评分与安全评级系统，针对漏洞和数据泄漏等行为进行识别，在漏洞风险评估中采用 CVSS 匹配，在数据泄漏上实现对深网暗网的覆盖，除此外，UpGuard 提供对第三方、第四方供应商事件与安全风险的监控，以及对企业域名仿冒、抢注等风险的识别。

3. Axonius（CAASM）

Axonius 成立于 2017 年，2019 年夺得 RSA 创新沙盒冠军。Axonius 定位于 CAASM 方向，目标是要解决一个看似普通但确一直无法完美解决的问题，即如何全面获得企业资产的可见性视图，因此 Axonius 并未走大而全的解决方案路线，而是聚焦在资产清点、资产运行及安全状态的监控。

做为一个行业性平台，Axonius 在无需部署任何代理的情况下，通过与包括网络、端点、身份、漏洞、云管理平台等不同类型超过 550+Adapter 信息源的对接来获取资产信息，实现细粒度的资产类型识别与唯一性标识，帮助企业完成资产可视化与资产运行状态

的安全监控。同时，针对已识别的资产漏洞风险，Axonius 会依据资产重要性、漏洞潜在影响和已识别的威胁来确定漏洞修复的优先级，并与多种安全节点进行深层的动作调用以实现风险处置。

2022 年 3 月，Axonius 以 26 亿美元估值获得了 2 亿美元的 E 轮融资，历史融资额达到 6.65 亿美元。

4. Balbix（CAASM）

Balbix 成立于 2015 年，产品定位为网络安全态势自动化平台（CAASM 方向），使用 AI 实现自动化网络风险发现、优先级排序、安全缓解与风险量化。Balbix 通过探针、Agent、第三方数据源集成采集资产数据，在风险发现中，通过分析漏洞工具、BAS 工具、安全控制工具的结果和多种威胁数据源，结合自有风险度量模型进行体系化综合的风险量化分析并进行后续安全编排与缓解工作。Balbix 基于“风险=可能性（脆弱性、暴露面、威胁、缓解控制）*影响（业务关键度）”模型，将网络安全风险量化为数据指标，可以快速帮助安全运营团队做出防御决策。

Balbix 在 2022 年 3 月完成 C 轮 7000 万美元融资，历史融资额超过 1 亿美元。

5. CTM360（DRPS、EASM）

CTM360 成立于 2014 年，总部位于巴林，作为老牌数字风险保护品牌，CTM360 在 2021 年推出 EASM SaaS 服务，并与 DRPS 进行整合，可以为企业提供外部攻击面管理、安全评级、网络威胁情报、深网暗网监控、品牌保护和反网络钓鱼、第三方风险监控、社交媒体欺诈监控、数据泄漏保护、Takedown 等服务。CTM360 提供了开箱即用、配置灵

活的交互系统，并在数据可视化和威胁风险分析展示上提供一流的用户体验。

6. Cycognito（EASM）

Cycognito 成立于 2017 年，是攻击面管理领域初创公司，旗下 CyCognito 平台强调以攻击者角度为设计原则，通过将市场上先进的 EASM 功能与自动化测试/BAS 相结合来提供攻击面保护，以发现攻击者最有可能用来危害组织的最小攻击路径。平台在业务上下文关联阶段使用了机器学习、自然语言处理和图形数据模型等创新技术；在响应修复阶段支持与 SIEM、ITSM、CMDB 和通信软件进行联动；平台支持常见的安全框架和安全合规等方面的检查及有效性验证能力。整体来看，平台在 EASM 领域能力覆盖较全面，但在对于暗网、深网和数据泄露等方面的监控能力没有体现，同时产品技术及运营方面的成熟度有待考验。

7. Tenable（CAASM 和 EASM）

Tenable 成立于 2002 年，属于漏洞技术驱动型公司，作为老牌的漏洞管理厂商，旗下 Tenable One 漏洞管理平台整合漏洞管理、web 应用安全、云安全、身份安全及外部攻击面管理等功能模块，把资产、漏洞和风险进行关联分析，一定程度上实现 CAASM 功能。产品在漏洞可视化及攻击路径分析等方面具备一定优势，但在资产和漏洞发现阶段，主要还是以主动扫描方式获取，没有明确可集成其他产品适配器的功能。此外，Tenable.asm 作为 Tenable One 功能模块聚焦在 EASM 方向，是业界首个完全集成到漏洞管理平台中的外部攻击面管理（EASM）解决方案；产品可无缝启动对未评估资产的新扫描，以扫描盲点并全面覆盖整个外部攻击面。

8. Palo Alto Networks（EASM）

Palo Alto Networks 成立于 2005 年，作为老牌综合型网络安全厂商，在 2020 年以 8 亿美金收购网络安全服务商 Expanse 后，将其互联网资产发现和数据归属等功能与 Cortex 产品套件集成。旗下攻击面管理产品 Cortex Xpanse 产品推出较早，无论在品牌知名度、客户认可度、技术和方案成熟度方面都具备一定优势。核心优势主要在全球互联网资产与漏洞发现的全面性及实效性，以及风险关联分析方面，同时产品作为 PaloAlto 旗下 Cortex 系列，可与 Cortex Soar、Cortex XDR 联动，提供威胁检测分析和自动化响应能力。在云资产安全方面，通过 CortexXpanse + Prisma Cloud（云原生应用保护）可实现云资产风险发现及安全管理。

9. JupiterOne（CAASM）

JupiterOne 成立于 2018 年，属于资产识别驱动型公司，产品以云原生网络资产攻击面管理（CAASM）为核心，以集成 180+的适配器为资产发现为基础，通过资产、漏洞、业务上下文等关联融合技术，进行攻击面管理分析，可覆盖内部网络资产、多云资产、身份和访问资产、资产安全合规等方面能力。同时，JupiterOne 支持与客户现网中的 XDR、SOAR、SIEM 等产品联动，以获得风险和优先级的综合视图，实现统一平台威胁态势管理。

10. SOCRadar（EASM 和 DRPS）

SOCRadar 成立于 2018 年，属于威胁情报驱动型公司，旗下产品扩展威胁情报平台结合了外部攻击面管理（AttackMapper）、数字风险保护服务（RiskPrime)和网络威胁情报（ThreatFusion)功能模块，实现一站式解决方案。借助威胁情报技术优势，产品在 DRPS

方面具备一定优势，特别是针对暗网、深网及数据泄露等方面的覆盖较全面。在 EASM 方向，主要针对 WEB 和 DNS 监控方向较为深入，资产上下文关联及攻击路径可视化等方面的特性有待增强。

11. CrowdStrike（EASM）

CrowdStrike 是全球知名的网络安全龙头厂商，主打的云原生终端安全产品是近年来终端类安全产品用户数增长最快的产品之一。公司的 Falcon 云原生架构，具有可扩展性和适应性，迭代升级迅速；通过 SaaS 订阅方式集成 8 大类别(22 个云模块)：包括端点安全、云安全、托管服务、安全&IT 运营、威胁情报、身份保护、日志管理，且推出 PaaS 安全平台 CrowdStrike Store，让第三方合作伙伴能够快速创新，构建和部署新的云模块，实现 SaaS+PaaS 的完整生态。这不断冲击传统安全厂商的市场份额。

2022 年，crowdStrike 收购以色列安全厂商 Reposify Ltd.，补充外部攻击面管理及威胁情报能力。于 2022 年 9 月 20 日推出外部攻击面管理功能产品，作为 Falcon 平台的重要补充。CrowdStrike 认为 EASM 是企业实施零信任策略的基础，在数字资产发现、企业上云、跟踪下属公司安全状态等场景下帮助客户。功能包括持续的暴露面监测、风险优先级排序及修复指引。为客户实现 7*24 小时持续暴露面监测，结合资产类别、CVE 评分等因子做综合优先级排序，最后结合行业最佳实践生成处置建议手册，帮助客户处置风险。

12. Noetic Cyber（CAASM）

Noetic Cyber 公司成立于 2020 年，2021 年 7 月获得 A 轮 2000 万美元融资。产品架构开放，接收 IT 系统管理中心和 CMDB，云平台，容器和 VM 基础设施，等系统数据信

息构建一个持续更新的来源，通过图形数据库呈现给客户。通过实时分析，帮助客户完善端点安全、漏洞管理、IT 系统管理等工作流程。提供完整的资产可见性，实时的安全风险洞察，并给出自动化补救措施建议。

13. Sevco Security（CAASM）

Sevco Security 成立于 2020 年，产品以云原生网络资产攻击面管理（CAASM）为核心，同 Axonius 和 JupiterOne 的设计理念相似，Sevcon 攻击面管理平台不做主动式资产发现，其通过本地 API 与现有资产相关系统集成，获取客户资产信息清单。其优势在于基于 API 的集成只需几分钟，不需要安装代理或部署扫描设备，也不需要对客户的环境进行任何特殊访问。同时，Sevco 平台具备独创的资产关联引擎可识别源系统资产的关键属性，自动创建并持续处理重复的资产信息，通过分析和汇集不同的资产数据源来构建实时资产视图。此外，平台支持资产遥测功能来实时监控资产状态并生成资产和属性更改事件，对事后调查溯源至关重要。

14. Brinqa（CAASM）

Brinqa 公司创立于 2008 年，总部位于德克萨斯州奥斯汀，他的统一风险管理平台有本地和 Saas 两种形式为客户提供服务，平台对数百个业务及数据源开放了接口，通过建立智能分析引擎实现对大量数据的收集、关联、分析、响应，并建立了风险图谱模型，可实现资产发现、业务上下文关联、风险分析管理、风险优先级排序、风险处置等全流程风险监管工作，为客户提供实时风险分析、自动化风险评估、优先补救和可行的见解和改进建议。

15. Reflectiz（EASM）

Reflectiz 成立于 2017 年，为填补应用程序安全和第三方风险管理工具方面的空白而创立，公司旨在通过开发一个映射整个数字供应链并分析每个组件的“WWW（哪些、什么、在哪里）”的解决方案来确保 Web 应用程序的安全。

Reflectiz 并于 2019 年发布攻击面管理平台产品。攻击面管理平台以应用程序安全和第三方风险管理为切入点，通过创新的远程沙箱，模拟用户和攻击者行为以监控客户网站，并对客户的数字生态系统进行深入分析。核心能力包括资产映射及发现、应用程序安全及可用性的监控验证、供应链安全、告警收敛和数字资产报告等。

16. Censys（EASM）

Censys 公司以资产发现为核心，主要以资产发现、风险优先级管理、威胁情报和红蓝对抗为能力，通过对端口、证书、协议、配置、上下文关系、历史风险记录等帮助客户实现风险监控，并可提供消除风险的建议。

17. DigitalShadows（EASM）

DigitalShadows 主要为客户提供威胁情报服务，推出“探照灯”产品，该产品提供可操作的威胁情报，可适应特定风险状况和偏好；并通过数据分析，结合超过 1000 条规则和分析师的专业知识，以确保检测与不断变化的威胁景观保持同步。“探照灯”还能将情报与资产联系起来，在风险评估中使用资产价值，并提供透明的风险评分，以快速识别重要内容，更快地做出更好的决策。

18. CyberInt（DRPS）

CyberInt 公司提供较为全面综合的解决方案，ArgosEdgeM 攻击面监控和高级威胁情报平台协同工作，提供持续的发现和监控，提供对组织面临的恶意行为者的威胁的完全可见性。

核心功能包括攻击面管理：资产发现、漏洞扫描、风险优先级管理；威胁情报：包括暗网、社交媒体及品牌监控；取证画布：通过广泛的 ioc 上下文链接，将多个服务集成到统一的调查平台中，以支持各种类型的连接，包括威胁情报、WHois 服务、被动 DNS、社交发现、恶意代码检测等，来识别和分析威胁行为者；钓鱼检测：通过发现网络钓鱼目标列表、攻击中使用的电子邮件模板和其他暴露的数据来检测针对员工的攻击，并通过 AP、SOAR 或票务平台集成这些结构化警报，已启动补救和删除功能；专家服务：攻击者分析、网络调查、态势分析、攻击模拟、删除补救、三方风险管理等。

19. NetSPI（ASM）

NetSPI 是一家美国的网络安全公司，成立于 2001 年，其 2023 年人员规模在 400 人上下。公司主营业务是攻击面管理及渗透测试等，其他业务涉及金融服务信息安全、漏洞管理、应用程序代码审查、应用程序安全、红队、应用程序安全程序开发、Web 安全、信息安全等。其在攻击面管理方面的核心优势是可以将 20 多年的渗透测试经验，和全球的专家团队的技术能力融入到攻击面管理技术平台。

20. Cyberpion（EASM）

Cyberpion 是一家以色列的网络安全公司，成立于 2016 年，其 2023 年人员规模在

60 人上下。其主营业务是外部攻击面管理，其他业务还涉及生态系统安全、供应链风险评估、第三方风险评估、云安全、在线安全威胁管理、网络安全威胁管理、网络安全风险管理和 Web 应用安全管理等。

21. ImmuniWeb（EASM）

ImmuniWeb 是一家瑞士的网络安全公司，成立于 2019 年，其 2023 年人员规模在 30 人上下。其主营业务是攻击面管理，其他业务还涉及 Web 应用程序安全、渗透测试和审计、Web 应用程序的 PCI DSS 合规性、动态应用程序安全测试 （DAST）、静态应用程序安全测试 （SAST）、移动应用程序安全、应用程序安全、应用程序安全测试、软件组成分析、网络威胁情报、第三方风险管理、Web 渗透测试和移动渗透测试等。

22. Bishop Fox（EASM）

Bishop Fox 是一家美国的网络安全公司，成立于 2005 年，其 2023 年人员规模在 420 人上下。其主营业务是 Offensive Security，其他业务还涉及风险评估、架构安全、应用程序安全、移动安全、网络安全、应用程序评估、产品安全审查、移动应用程序评估、攻击面测试、云安全、攻击面管理和威胁建模等。

23. Coalfire（EASM）

Coalfire 是一家美国的网络安全公司，成立于 2001 年，其 2023 年人员规模在 1100 人上下。其主营业务为合规服务、云安全、渗透测试、应用安全、托管服务、脆弱性管理以及战略、隐私和风险服务。

24. LookingGlass（EASM）

LookingGlass 是一家美国的网络安全公司，成立于 2009 年，其 2023 年人员规模在 160 人上下。其主营业务是威胁情报和威胁防御，其他业务还涉及高级恶意软件、DNS 安全、开放安全平台和 APT 研究等。

25. RunZero（CAASM）

RunZero 是一家美国的网络安全公司，成立于 2018 年，其 2023 年人员规模在 80 人上下。其主营业务是资产清单和网络可视性解决方案。

26. BrandDefense（DRPS）

BrandDefense 是一家美国的网络安全公司，成立于 2019 年，其 2023 年人员规模在 50 人上下。其主营业务是综合防御和网络威胁情报，其他业务涉及漏洞管理和攻击面。

（二）国内厂商

1. 360 数字安全集团

360 有多条产品线和能力线与攻击面管理相关：360 所收购的数字观星团队的企业网络资源测绘系统观星台、360 自身研发的 Quake 网络空间资源测绘系统以及 360 漏洞研究团队。

360 对攻击面管理产品的理念是，将外部攻击面管理与内部攻击面管理二者结合，从企业内、外网双重视角查看企业资产、掌握资产的暴露情况、风险情况、访问路径、保护措施，从而支撑安全运营工作的有效开展。

产品的实现方案也是围绕内外部攻击面一体化展开：首先有一个探针层和采集层，通过主动的资产扫描、漏洞扫描，以及对接 CMDB、其它安全软件/设备采集资产与漏洞信息，然后将数据存储和进行标准化融合加工处理，在数据分析层完成资产变更感知监控、未知资产分析加工、资产/漏洞标签、资产漏洞重要性评价、业务/应用重要性评价、资产/应用/业务/组织风险评价、资漏碰撞、漏洞真实性验证、访问关系挖掘。在数据分析能力支撑下，形成资产管理、漏洞管理、风险管理能力，支撑更上层的攻击面管理动作：业务资产逻辑拓扑、攻击路径推断、攻击面资产图谱、攻击面风险分析。这些能力可以支持用户的一些专项行动，如资产盘点、外部攻击面排查、攻击面资产图谱、攻击面风险分析等。

在外部攻击面上，采用 360 云端大脑的数据，对外部攻击面做整体的测绘，然后再把这个数据落到本地。所有的资产的模板和风险的模板是可配置的，不同的模板适用于不同的管理场景。

以看见为中心，建立攻击面的运营体系：看见资产，看见漏洞，看见风险，，把资产、漏洞和风险统一生成攻击面，然后去有效评估攻击防护措施。

目前 360 攻击面管理产品共有 4 条产品线：

- 销量最大，从数字观星 2016 年开始研发的“观星台”演进而来的“360 资产与漏洞检测管理系统（天相-标准版）”；
- 面向集团型企业客户的“360 信息资产安全统一管理平台（天相-旗舰版）”；
- 面向中大型金融、央企、政府客户的“360 漏洞管理系统（星规）”，天相旗舰版和星规的技术底层是相同的。
- 定位于中型客户的“360 互联网攻击面监控系统（天相-SaaS 版）”。

360 自身研发的网络资源测绘系统 Quake、360 的漏洞研究团队在其中都是作为能

力提供者贡献资产测绘能力、漏洞能力、威胁情报能力。

360 的特长是拥有丰富的资产情报（包括 DNS 情报、Quake 互联网测绘情报、数据泄露情报及暗网检测情报等）、资产指纹信息、大量的 POC/漏洞情报，尤其是信创的漏洞情报，历年实网攻防演习的漏洞，以及在移动应用侧的微信资产测绘能力。在实施模式上，可以为用户提供安全运营服务支持。

2. 华顺信安

华顺信安是国内互联网测绘的领军企业，旗下有白帽汇、FOFA、Goby 等安全品牌，创始人赵武黑客出身，曾开发著名的渗透测试工具 Pangolin。FOFA 是互联网资产测绘平台，白帽汇是安全众测平台，Goby 是一款渗透测试工具，“互联网资产测绘”与“漏洞”是华顺信安的两大标签。华顺信安的兴起与 2016 年开始进行的实网攻防演习有很大关系，其开发的互联网资产测绘产品成为“实网攻防演习必备”产品之一。

正是因为在网络资产测绘与漏洞方面的积累，华顺信安推出攻击面管理产品是水到渠成的事情。2019-2020 年开始，用户将 FOFA 用于互联网资产暴露面梳理，2021 年公司开始做外部攻击面管理 EASM 产品 FORadar，由于用户有外部、内部资产的关联问题，产生对 CAASM 的需求，为满足用户需求而进入内部攻击面管理 CAASM 市场，推出 FOBrain。但华顺信安一直对自身的产品边界保持比较谨慎的态度，依旧避免进入对安全事件收集、响应功能，聚焦在资产与漏洞相关。

产品的部署形态，FORadar 可以支持 SaaS 服务与本地化部署两种形态，FOBrain 则是本地部署。

3. 华云安

华云安是 2019 年 7 月才创立的公司，初期定位于漏洞研究、开发漏洞管理产品、人工智能赋能的攻防对抗。从 2021 年 9 月份开始转攻击面管理，依靠基于知识图谱的情报协同技术的 EASM 产品“灵知 Ai-Radar”，基于云原生技术做的 CAASM 产品“灵洞 Ai-Vul”，以及自动化渗透测试 BAS 产品“灵刃 Ai-Bot”。三款产品采用“灵洞”的云原生平台构架，统一的开发平台不仅可以减少公司的技术管理开销，可以容器化部署更带来的领先的灵活性。

华云安的技术优势主要在做为国家漏洞库支撑单位而获得的漏洞情报能力、攻防能力、知识图谱与人工智能能力。在竞争策略方面，对国防安全客户，通过情报和作战对抗，在漏洞库和战机捕获方面建立竞争优势；对关基保护客户，主动防御和溯源预警方面建立竞争优势；在企业安全方面，通过未知资产梳理、漏洞扫描。

产品的交付模式上，灵洞与灵刃采用本地交付，灵知是 SaaS 方式交付，因为采用统一的云原生架构，三款产品都实现了通过许可证即可简单交付的方式。

4. 魔方安全

2015 年，魔方安全由 Cubesec 团队在深圳创立，成立 1 年后，魔方安全便推出了基于 SaaS 模式的互联网安全监控平台，并为某 TOP 级金融客户提供互联网暴露面风险监控服务。

成立 7 年来魔方安全始终专注于攻击面管理领域的产品研究与技术创新，目前可以提供 EASM 和 CAASM 两种产品。魔方安全 2020 年首创数字资产测绘理念，实现对移动端公众号、小程序、网盘文库、暗网、github 敏感代码等数字资产的识别和监控，并以此打

造基于 SaaS 模式、且自动化程度较高的 EASM 产品，在金融行业具有较高的客户覆盖和口碑。在 CAASM 产品上，魔方安全融合了国外厂商 Axonius 和 Sevco 的开放性理念，通过对数十种资产信息数据源的对接，实现对资产可见性和安全风险的全面观测，在资产信息整合与关联分析、攻击路径分析与可视化方面具有比较扎实的技术积累。

5. 盛邦安全

盛邦安全从 web 应用安全领域出发，目前已成为聚焦漏洞及脆弱性检测、应用安全防御、溯源管理及网络空间地图领域的综合型厂商。在攻击面管理领域，盛邦安全是国内为数不多可以提供 CAASM、EASM、DRPS 三类解决方案的供应商。

盛邦安全 EASM 方案以 SaaS 为主，其平台底层能力由盛邦安全知名产品网络空间测绘系统 RaySpace 和大数据分析系统 RayBA 构成，通过 RaySpace 实现对企业互联网资产暴露面数据的全面测绘（包括规模领先的 IPv6 测绘数据库以及业内首创对互联网安防或代理节点后隐藏资产的识别），RayBA 则通过多种维度（包括基于 IP、域名、证书、子孙公司、威胁情报、VPT 等）分析并绘制企业可能存在攻击面，进而形成对企业外部漏洞、攻击面以及供应链安全的风险评估。在 CAASM 方面，盛邦安全在 2017 年便推出了网络安全资产治理平台 RayGate，目前采用主、被动测绘技术可以实现对企业内部 IT 资产、API 资产、开源组件、僵尸资产以及合规资产外连的识别，达成企业内部资产的快速盘点与收敛。在 DRPS 方面，依托于自身互联网敏感信息监测系统 RaySIN，通过 SaaS 订阅模式，盛邦安全可以为企业提供针对敏感信息泄漏、代码泄漏、钓鱼网站、移动端 APP/公众号/小程序、暗网、个人隐私信息等多维度数字资产的风险监测服务，并且盛邦安全认为 DRPS 对于国内的市场环境来说，如果仅定位于包装成独立的产品放手给客户使用，将

无法真正体现其产品价值，只有产品+服务的结合才会达成更好的客户体验。

目前盛邦安全攻击面管理产品的客户数量已达到数百家，特别在教育、能源、运营商以及某特殊行业，产品与客户实际业务场景已形成深度的融合。

6. 长亭科技

长亭科技在 2022 年 9 月发布了定位于 EASM 方向的云图（Cloud Atlas）攻击面管理运营平台。该产品由猪猪侠（王昱）主导研发，做为前乌云网排名第一的白帽子、阿里云先知平台的领航者、阿里云整体云平台与产品安全负责人、长亭科技安全技术副总裁，猪猪侠对攻击面收敛和自动化安全运营方面具有非常丰富的经验。

立足于长期在攻防渗透领域的投入与累积，长亭云图平台在攻击者视角的确立和运用上有着比较深刻理解和体现，并基于漏洞攻击面、数字资产攻击面、社会工程攻击面 3 个维度进行风险研判与管理。特别在漏洞风险中，通过整合其它多产品底层数据、自动化以及社区情报能力，并结合多年渗透测试经验，构建了面向实战视角、符合真实攻击逻辑的风险分析方法。除此外，长亭在攻击面管理整体方案中也可以提供面向内网资产攻击面管理（CAASM）的产品洞鉴（X-Ray）。

云图产品发布至今不足半年，已试用于数十家大中型客户，产品未来的目标客户将定位于参与实网攻防或资产规模较大的客户。长亭科技认为没有实战需求或资产规模小将无法凸显其产品价值。

7. 云科安信

云科安信公司是一家创立之初就定位于外部攻击面管理的公司，创始人金飞是做网络

攻防背景，曾在 HP、F5 等外企工作。公司有攻防实验室做漏洞 POC 研究支撑，推出的“白泽”攻击面管理产品，以 EASM SaaS 服务为主，借助运营商合作渠道，已获得上千家客户，以中小企业为主。

与业内厂商比拼 POC 数量的竞争路线不同，云科安信认为保持 1000 个左右的 POC 就可以满足攻击面管理的需求，维护更多数量的 POC 并无太大必要。

云科安信目前主要通过和运营商合作，以运营商的品牌为用户提供攻击面管理及攻击防护服务，目前已服务数千家企业，以中小企业为主，公司也已经开始组建销售队伍，开始云科安信品牌的攻击面管理服务与产品的销售工作。

8. 斗象科技

斗象科技是国家信息安全漏洞库（CNNVD）和国家信息安全漏洞共享平台（CNVD）重要支撑单位，2022 年漏洞报送数量位于 CNNVD 和 CNVD 首位。斗象科技旗下业务品牌包括：安全数据分析与安全运营产品体系“斗象智能安全”，安全众测与安全运营服务平台“漏洞盒子”，网络安全行业门户“FreeBuf”及“FreeBuf 咨询”。

斗象科技在 2022 年末发布了面向企业攻击面检测与管理的安全平台 APTP，APTP 平台是目前市场中为数不多的将网络资产攻击面管理（CAASM）与外部攻击面管理（EASM）整合的产品。在资产梳理上，APTP 平台可以识别比较丰富的企业内外网资产信息，包括传统 IT 资产、云资产、物联网资产、移动端资产、API 资产、企业及员工的数字资产等，并支持打通内外网资产映射关系，除此外，APTP 还以动态爬虫和辅助对抗手段，对不同环境中运行的应用程序、服务组件、API 等应用级资产进行更细粒度的识别，提取到包括支付卡信息（PCI）、个人身份信息（PII）、健康信息（ePHI）以及 GDPR 等信息。在风

险分析方面，APTP 平台提供针对漏洞风险、数据泄漏风险、供应链风险、证书风险、配置错误风险、钓鱼风险等多维度风险分析策略，并结合多种渗透测试方法与自动化策略编排，对风险与业务的重要性进行综合分析与风险优先级排序，最终形成攻击路径推演与攻击面可视化呈现。依托于漏洞盒子，APTP 平台在漏洞情报和 POC 方面也具有一定数据基础。

APTP 目前客户主要涉及金融和新零售行业，斗象科技认为从目前市场沟通和 POC 情况来看，未来 APTP 在客户行业与应用场景上将具备广泛的适用性。

9. 绿盟科技

绿盟攻击面管理平台以网络空间测绘平台、测绘探针、攻击面管理服务和 MDR 服务组成，方案主要针对企业互联网资产暴露面和敏感信息泄漏情况进行风险监测，定位于 EASM 方向。通过持续 7 年在网络空间测绘方面的研究与数据积累，并结合自身在攻防对抗方面的经验，绿盟攻击面管理平台可以帮助客户掌握外部资产信息，包括识别企业高危主机、恶意行为主机、幽灵资产等异常资产，全面实现企业互联网资产风险监测与暴露面收敛。同时，该方案也可以对企业在网盘、文库、Github 代码平台、暗网中泄漏的敏感信息以及移动端 APP、小程序、微信公众号等资产进行稽查。

该平台可以 SaaS 和私有化方式部署，目标客户定位于重保单位、监管机构以及企业级客户，使用场景包括资产风险态势监测、挖矿专项治理、资产归属识别以及风险资产定位。

10. 未岚科技

未岚科技是一家以攻击面管理为创业方向的初创网络安全公司，创始人王金成有从事

SIEM/SOC 类产品开发背景，有较强的大数据系统的应用开发经验，同时具备甲方、乙方的工作经验。

未岚科技同时提供 CAASM、EASM 和 DRPS 的能力，产品通过 API 接口可与数十种资产相关系统/设备的数据进行对接和采集。特长在多源资产信息的融合及资产上下文分析，底层采用图数据库支撑，并发明了 ASQL 语言，可实现复杂的资产查询。同时，在资产关联分析、攻击路径分析与可视化方面具备一定的成熟度。客户主要定位为安全成熟度较高的企业，目前还是聚焦在 CAASM 领域，提供一体化的攻击面管理平台，并不刻意区分内部攻击面与外部攻击面，因此在内外网资产的映射上比较重视。

11. 螣龙安科

螣龙安科成立于 2020 年，创始人王昊天曾有十几年网络安全从业经验，多次负责如 Google、Yahoo、AOL、新华工控等安全项目。

螣龙安科以 BAS 起家，并在 2022 年发布潮汐攻击面管理平台进军攻击面管理领域，公司定位在 DRPS，同时具备 EASM 和 CAASM 能力，在政府机构、金融、电信都已树立起标杆案例。

在 CAASM 领域，公司支持多种识别方式，主要通过种子录入方式对资产（IP、域名、端口、协议、操作系统、指纹等）进行快速的自动化探测识别，并可进行高效精确的时序指纹识别，同时可通过绘制资产拓扑图、概览图、图库等方式全面展示资产情况。由于以 BAS 起家，在漏洞方面螣龙安科支持较多的 1day 漏洞的 POC，大幅降低了新漏洞的可被利用性，而 BAS 系统也支持多攻击向量的安全性模拟检测及漏洞优先级评估，并提供漏洞修复指南。在 EASM 方面，螣龙安科通过爬虫抓取的方式，及支持文档平台、暗网平台、

数据泄露论坛、代码仓库、搜索引擎等方式监测用户的外部攻击面情况。腾龙安科在 2021 年启动了全球化的安全社区，目前有近万名白帽黑客在持续和公司进行高频交互，帮助进一步完善产品。

12. 零零信安

零零信安是一家从暗网信息监测切入攻击面管理市场的厂商，创始人王宇曾任知道创宇 Zoom Eye 产品的负责人。

零零信安提供暗网信息监测服务，通过 0.zone 网站为客户提供自己组织或目标组织所泄露在暗网上的数据、身份等可用来进行对组织 IT 设施进行攻击的信息。除了直接为最终客户提供服务外，零零信安还与其它安全公司提供威胁情报服务，为其它安全公司的攻击面管理产品赋能。

13. 知道创宇

知道创宇的创始人赵伟与杨冀龙都是著名的黑客，公司也以网络攻防见长，在漏洞挖掘利用、渗透测试服务、Web 云抗 D、Web 云防护等方面在都曾引领过国内的潮流，其推出的 Zoom Eye（钟馗之眼）是国内第一个提供服务的网络空间资源测绘平台，非常有影响力。

知道创宇在 10 多年的发展过程中形成了政府、电信运营商、金融、电商、教育、新闻媒体、直播、棋牌游戏、大型企业、中小型企业等多个行业的安全解决方案，公司也拥有较齐全的资质。

网络资源测绘与漏洞，是攻击面管理的两个基础能力，知道创宇有做攻击面管理的良

好的基础，但近年来公司在产品的创新能力上有所下降，但依然是攻击面管理方面的玩家之一。

14. 墨云科技

墨云科技是主打网络智能攻防的厂商，主要产品是虚拟黑客机器人（VackBot）。VackBot 从攻击者的视角出发，通过融合 AI 引擎与黑客攻击技术，实现用机器程序自动化模拟黑客攻击行为，自主规划攻击路径和攻击方法，为用户提供针对各类 IT 资产的资产发现、漏洞挖掘、漏洞验证以及利用漏洞进行扩展等攻击行为。

墨云推出的入侵和攻击模拟系统 VackBAS，内置 2000 多个模拟黑客攻击和入侵行为的剧本，对数据安全、端点安全、口站安全、容器安全、邮件安全、边界安全、云安全等网络安全防护能力、安全配置和策略的有效性进行测试和验证。VackBAS 还可提供基于实战和攻击者视角构建的 MITRE ATT&CK 对抗能力仿真测试，能够更有通过攻击模拟、优先级排序、修复提升帮助企业提升网络安全防护效能和降低业务风险。

VackBot 与 VackBAS 两款产品同时支持云平台服务模式与本地部署模式，云平台服务模式可以通过 VPN 通道连入企业内网提供服务。

墨云的攻击面与漏洞优先级管理平台 MagiBot 是一个框架，可以把资产，攻击面发现，漏扫归一化，自动化渗透和攻击模拟等产品集成到了一起，除了墨云自己的产品，还可以集成其它安全公司的漏扫产品和资产管理平台，产品采用本地部署方式。

墨云的 AI 引擎除了逻辑调度外还引入多种机器学习算法，包括图像识别类算法（如 CNN，KNN 等）、特征识别与分类算法（如 NB，CNN，A3C，KMeans 等）、决策类算法（如 NB，DNN）等等。

AI 技术在网络攻防中的应用一直是人们努力的方向，目前还有许多问题有待解决，离成熟还有很一定距，但在提高工作效率、提升响应的速度方面已经在金融、运营商和关基行业得到了验证，相信随着技术进步，会有更好的价值体现。

15. 灰度安全

灰度安全是一家以 BAS 和 VPT 为创业方向的公司，其开发的产品先知-智能风险评估系统是一款聚焦风险度量的专家级平台，是一款聚焦风险度量，持续验证防御措施有效性的平台，通过攻击场景构造和攻击向量编排技术，实现控制措施及过程的验证和风险态势的度量，并且可以对接外部态势感知、作战指挥等系统实现风险度量集中可视化呈现、风险协同响应处置与统一作战指挥。

产品思路是在用户现网中部署一些探针，然后去接收灰度安全自己打的攻击包，通过接收到的攻击包与安全告警情况判断已经部署的安全防护系统、安全监测系统是否在正常工作，其工作原理与自动化渗透测试完全不一样。可视化风险度量是系统的亮点之一。

攻击面管理与 BAS、VPT 产品在底层技术上有共同之处，也是灰度安全要拓展的产品方向之一，重点需要丰富资产探测能力。

16. 微步在线

微步在线凭借多年来在情报生态领域积累的数据基础打造了 OneRisk 外部攻击面管理 SaaS 平台，定位于 EASM 方向。做为数据驱动型平台，OneRisk 以网络空间测绘数据、威胁情报和漏洞情报数据、全站爬虫数据为基础，对企业互联网资产和数字资产进行全面梳理和风险排查，在资产漏洞风险发现中，OneRisk 坚持聚焦 0day 和 1day 等高可利用

漏洞，提供针对最新高危漏洞的快速检测与响应能力。除此外，OneRisk 可以针对互联网文库、代码平台、邮箱、暗网中的数字资产提供数据泄漏风险管理与人工应急处置服务。

17. 天际友盟

天际友盟是 2015 年 6 月成立的威胁情报供应商，同年 10 月作为创始成员单位之一成立烽火台安全威胁情报联盟，陆续发布 RedQueen 安全智能服务平台、Alice 威助溯源平台、SIC 安全情报中心、Leon 威胁情报网关，于 2019 年开始进入数字风险防护领域，发布 DBP 数字品牌保护平台，2020 年发布 DRP 数字风险防护体系，但其实在 2017-2018 年就已经有客户提出这方面的需求，只是那时候 DRP 的名词还没有被提出。

天际友盟的 DRP 数字风险防护体系提供钓鱼欺诈与仿冒、品牌侵权、版权盗版、数据泄露、代码泄露、威胁误报的监测服务。其中钓鱼欺诈与仿冒、数据泄露、代码泄露是攻击面管理的重要内容。

天际友盟除了直接为最终客户提供服务外，还与其它网络安全公司建立了合作关系，为网络安全公司提供数据情报服务。

从业务规模上，2022 年天际友盟 DRP 服务的收入已经超过威胁情报的数据订阅服务收入（未包括 TIP/TIG 类威胁情报产品收入）。

18. 雾帜智能

雾帜智能自 2019 年成立以来始终聚焦于安全运营领域技术和产品的研发，公司成立后首先推出了安全编排自动化与响应（SOAR）产品 HoneyGuide，AssetWise 实时资产治理系统则是雾帜智能发布的第二个平台型产品，定位于 CAASM 方向。在资产识别中，

AssetWise 除了主动探测外，还可以 API 对接和日志方式采集第三方 HIDS、EDR、桌面管理系统、CMDB、AD 域以及交换机、日志审计、网络准入等数据源的资产信息，力求对企业内网的全量资产进行发现和关联分析。在资产漏洞风险评估上，AssetWise 会结合自身与第三方扫描器结果综合判断。AssetWise 提供了丰富的资产类型自定义功能，并在风险处置流程中采用低代码、拖拽形式实现灵活、易用的自动化响应工作流。

19. 迪普科技

基于多来年在实网攻防、重保服务、行业专项安全服务项目中沉淀的技术与经验，迪普科技推出了以人+工具+平台三要素相结合的攻击面管理整体解决方案。方案以多层次、体系化的全局视角，全面梳理企业内外网暴露面和与之存在的攻击面风险，并针对不同客户的需求以服务、服务（为主）+平台、平台（为主）+服务等多种灵活的形式对企业安全运营建设赋能。

通过实现资产与漏洞风险管理平台、API 数据安全风险管控平台、网络威胁管理平台、安全运营管理平台这 4 个自有平台的能力汇聚与数据贯通，迪普科技可以提供攻击面风险预判，事中积极防御、事后快速响应的完整闭环。同时，依靠自身服务能力与生态链的结合，迪普科技也可以提供面向企业互联网风险监控与暴露面收敛服务。

迪普科技在攻击面管理解决方案上积累了比较丰富的客户案例，并在公安政法、运营商、电力等行业实现了深度应用。

20. 天防安全

北京天防安全科技有限公司成立于 2017 年，是物联网安全行业的新兴厂商，创始人

段伟恒先生曾任启明星辰集团公安业务副总经理、集团副总裁，有十五年以上的的网络安全从业经验。

天防安全以视频监控系统安全防护为物联网安全的切入点，深耕全国公安视频监控安全领域，积累了大量的视频监控领域 IoT 设备指纹库和 IoT 设备漏洞库，并以此为基础推出相应产品，并提供攻击面管理中的 CAASM 能力，包括视频设备资产盘查、弱口令发现及管理、漏洞扫描及补丁修复等。

21. 万物安全

万物安全成立于 2018 年，以物联网安全为定位，产品覆盖资产监测及管理、安全准入、边界防护、泄漏防护和态势感知，并在金融、公检法司领域重点布局。

公司通过对物联网资产（PC、服务器、摄像头、IP 对讲、报警系统、门禁系统、网络打印机等）的指纹库和漏洞库的积累，先后推出了星空-网络空间资产测绘系统和银河-CAASM 系统，星空-网络空间资产测绘系统主要通过探针发现、指纹识别、流量分析、第三方系统对接等方式，实现全网物联网资产测绘，而银河-CAASM 系统则提供物联网资产的漏洞扫描、弱口令发现及管理、私接仿冒等恶意行为监测、合规检测和风险等级评估等能力。

九、解决方案与案例

（一）三六零数字安全集团----某国有大型银行安全运营中心项目（攻击面部分）

公司简介：

360 数字安全集团(三六零数字安全科技集团有限公司)是数字安全的领导者，专注为国家、城市、大型企业、中小微企业提供数字安全服务。360 攻击面管理方面基于外部攻击者视角和内部安全运营视角，从传统 IT 资产、云资产、影子资产、新兴资产、数据资产等多个维度全面梳理企业资产与风险数据并评估应用风险，形成全网攻击面管理能力。

项目简介：

客户为国有大型银行，世界 500 强品牌。项目整体为安全运营中心建设项目，需要对内外网攻击面进行全面梳理，实现分行总行资产、风险数据集中纳管，形成攻击面管理能力，以支持各项日常安全运营工作开展，并具备突发安全事件定位能力。

项目建设情况：

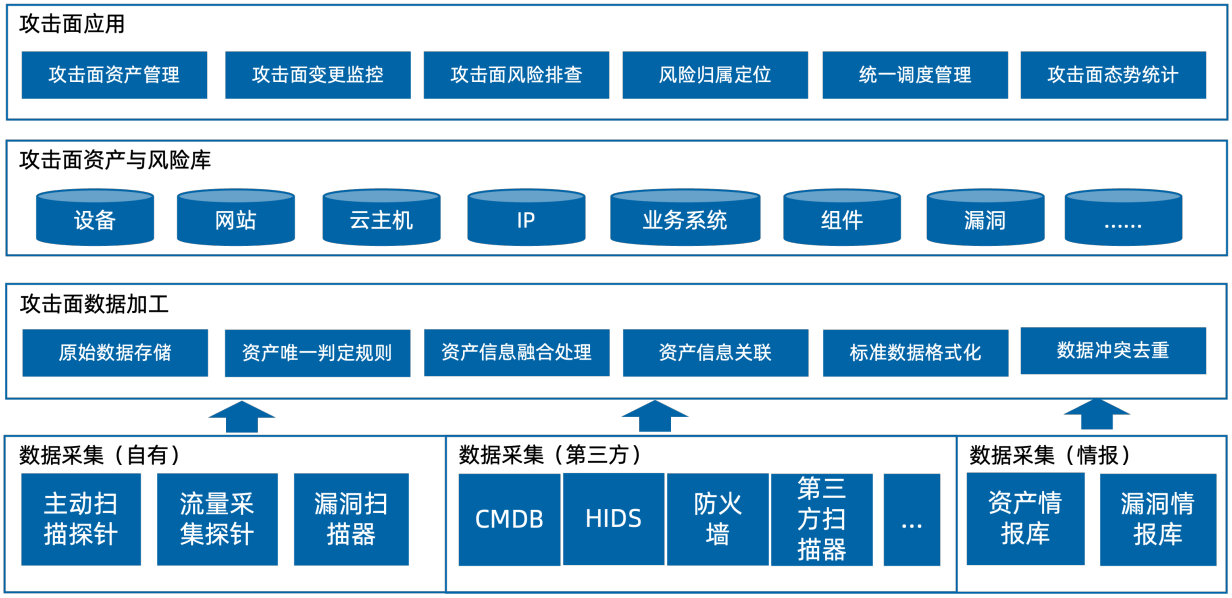


图 26：三六零数字安全——某国有大型银行安全运营中心项目（攻击面部分）建设情况

项目亮点：

- 承载百万量级资产，覆盖主机资产、网站资产、IOT 资产等多个维度。
- 根据客户实际管理场景设定资产模型，建立了近百个属性的资产精细化管理模式。
- 对接近 10 个资产与风险数据来源包含 CMDB、HIDS、网管、漏扫等，基于多来源数据进行融合加工，统一调度，归一攻击面管理工作入口。

客户价值：

- 在实现数据隔离的前提下，实现了对分行、总行资产集中纳管，并提供统一管理标准。
- 对资产分区分域管理，持续监控并发现新增资产，不断提高攻击面可见性，杜绝安全管理盲区。
- 在面临突发安全风险时，可快速进行排查，精准定位资产以及相关责任人，从而实现处置闭环，收窄攻击面风险。

（二）华云安----国网某省公司基于攻击实战场景下的攻击面管理项目

公司简介：

北京华云安信息技术有限公司，基于攻击者视角构建集主动防御、情报协同、溯源反制于一体的新一代网络安全防御体系，提供完整的攻击面管理解决方案，涵盖网络资产攻击面管理（CAASM）、外部攻击面管理（EASM）、渗透与攻击模拟（BAS），实现对企业数字化资产风险的持续检测、分析、响应和监控。通过灵洞·网络资产攻击面管理平台（Ai.Vul）、灵知·互联网情报监测预警中心（Ai.Radar）、灵刃·智能渗透与攻击模拟系统（Ai.Bot），基于攻击者视角从不同维度打造实战化、体系化、常态化的新一代数字安全风险管理解决方案。

项目简介：

随着国家电网数字化转型步伐加快，软件系统越来越庞大，开源组件、代码复用以及数字化应用场景等极大增加了网络攻击面；近年来攻击手法的多样化和复杂化，使重要信息系统和关键基础设施面临着较大的安全风险，如何保障电力基础设施的安全成为网络空间对抗新时代的主要挑战。

某国网省公司，面对不断增加的数字资产以及未知资产不可控带来的攻击面外溢影响企业安全防御能力，需要针对目前网络安全防御体系中安全设备防御有效性进行验证，并针对企业内外部攻击面进行管理，项目预算金额千万。

项目建设情况：

本系统聚焦“高强度网络攻击场景下的对抗防御能力”建设，通过聚合电网实战化攻防战法和网络资产攻击面情报，提供自动化网络渗透评估、网络攻击与 APT 防御评估、软件供应链安全评估、工业网络安全防护评估、敏感数据防护评估等安全场景，构建“实战

化、体系化、常态化”的新一代网络安全运营体系。

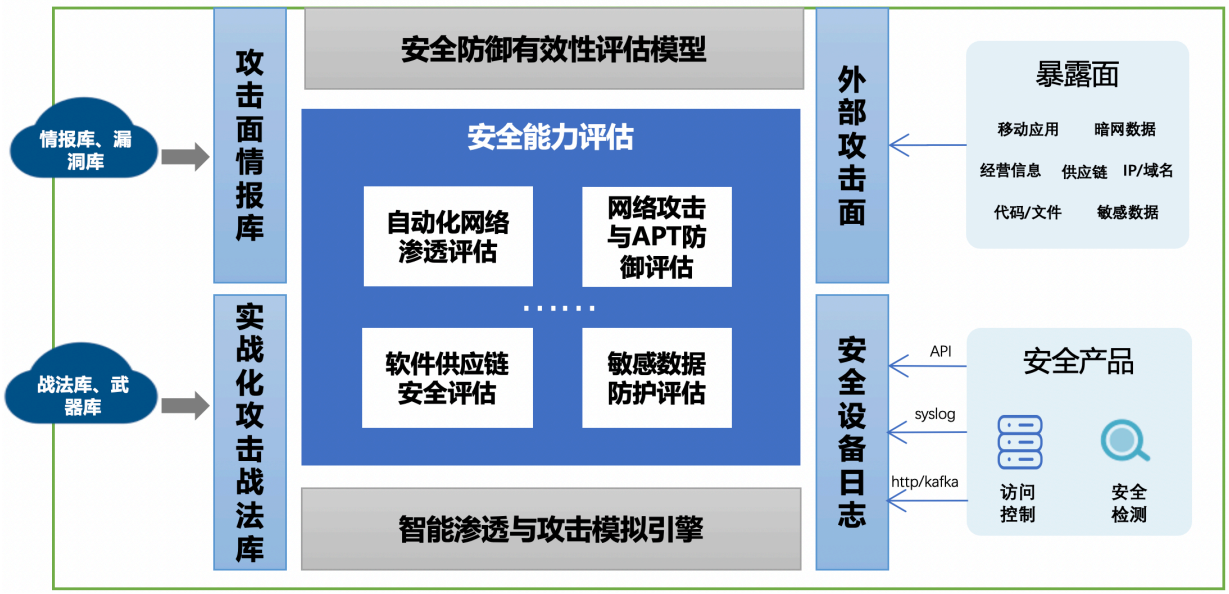


图 27：华云安——国网某省公司基于攻击实战场景下的攻击面管理项目建设情况

项目亮点：

- 系统融合华云安基于知识图谱的网络安全风险情报库，通过分布全球的节点数据采集能力，跟踪网络环境中的每个威胁行为，应用知识图谱和人工智能技术帮助客户发现高级安全威胁，提升安全体系防御能力。
- 系统融合了由实战型 PoC/Exp/武器/工具等组成网络安全攻防战法库，对用户整体安全防御能力进行验证评估。
- 系统采用了华云安智能渗透及攻击模拟引擎，以攻击者视角，通过多种攻击手段对用户网络安全防御体系有效性进行验证评估。

客户价值：

- 建立起一套以攻击面管理为思想，安全防御有效性评估为能力的安全运营体系。
- 优化安全防御策略 50%以上，安全设备防御能力有效性提升 90%以上。

- 对于企业暴露在互联网的数字资产进行攻击面收敛，帮助企业快速自动化规避安全风险。
- 为企业提供攻防实战演练及重大保障活动的防御有效性检验，将演习成果固定化、深度防御常态化。

（三）盛邦安全----某运营商互联网资产暴露面发现与安全治理方案

公司介绍：

远江盛邦（北京）网络安全科技股份有限公司（简称：盛邦安全）成立于 2010 年，专注于网络空间安全领域，以“让网络空间更有序”为使命，为客户提供网络安全基础类、业务场景安全类、网络空间地图类安全产品及服务。盛邦安全倡导“安全有道，治理先行”的发展理念，秉持精准识别、精确防御、深入业务场景的“两精一深”的研发战略，聚焦漏洞及脆弱性检测、应用安全防御、溯源管理及网络空间地图等技术领域，致力于从网络空间视角剖析数字世界，构建数字世界的网络空间地图，赋能各行业客户的数字化转型，护航国家网络空间安全战略的实施落地。

项目介绍：

该运营商客户需要建立企业集团网络空间资产暴露面全量数据仓库，绘制资产全息指纹画像信息；健全资产备案管控措施，助力企业完成各级单位资产备案稽查核验工作，发现漏报、瞒报、未知、违规等资产威胁风险；对高危漏洞、0Day/1Day 漏洞快速资产普查和定位风险资产，及时处置修复，减少网络资产漏洞风险暴露面。

项目建设情况：

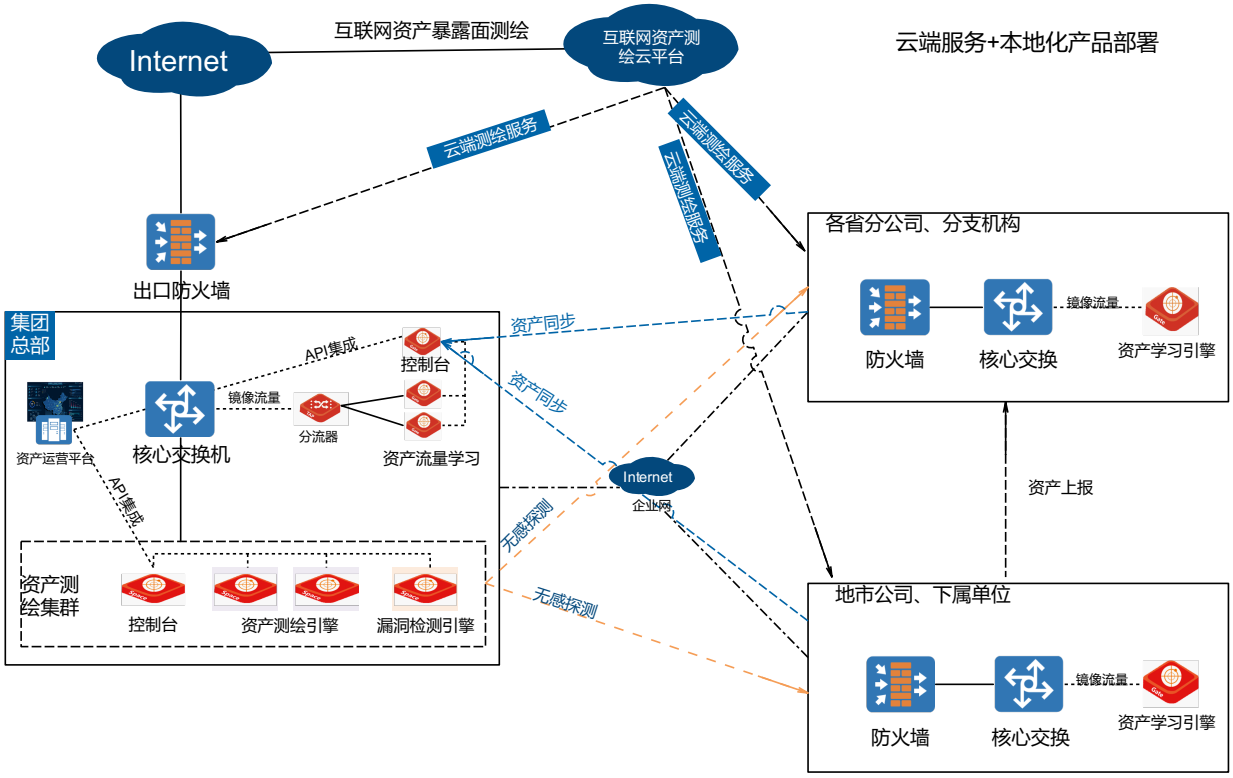


图 28：盛邦安全—某运营商互联网资产暴露面发现与安全治理项目建设情况

项目亮点：

- 建立“云+地”协同模式，在集团总部和各省市机构本地部署资产测绘和流量学习设备，并结合云端资产测绘服务，实现企业互联网全网资产暴露面普查，建立全网数据仓库；
- 通过与集团资产运管平台 API 集成，实现对集团全网各省市分公司所属资产暴露面测绘普查，逐级核查资产备案及上报的真实性、合规性和完整性；
- 通过调用资产安全漏洞检测引擎，快速完成企业互联网资产漏洞普查和 PoC 漏洞验证，及时发现资产高危漏洞，快速定位资产，主动通报处置，降低资产风险暴露面；

客户价值：

- 全面梳理企业网络资产全景图，实现互联网资产清单可知可控，降低企业互联

网资产暴露面风险；

- 绘制网络资产指纹图谱，动态更新资产台账，实现资产、机构、人员、供应链等信息关联绑定，定位责任主体，快速响应处置，落实企业资产备案管理要求，提升资产安全管控能力；
- 开展网络资产安全漏洞监测，快速定位查询并及时预警通报；快速修复漏洞并加固处置，贯彻网络安全相关法律法规要求，主动收敛资产攻击面风险，提升企业安全防护能力。

（四）魔方安全----某股份制银行攻击面管理最佳实践

公司简介：

魔方安全专注于攻击面管理和网络空间资产安全相关技术研究、产品研发和运营服务，包括：外部攻击面管理（EASM）、网络资产攻击面管理（CAASM）、漏洞管理（CVM）、安全攻防服务，并推出业内首个攻击面可视化（VASM）解决方案。凭借多年金融客户的服务经验，总结《金融攻击面管理方法论》，配套精细化攻击面运营服务，协助用户构建攻击面高阶运营能力。以下案例为魔方安全与某股份制银行在攻击面治理领域七年的的实践与创新，实现攻击面管理的指标化运营。

项目建设情况：

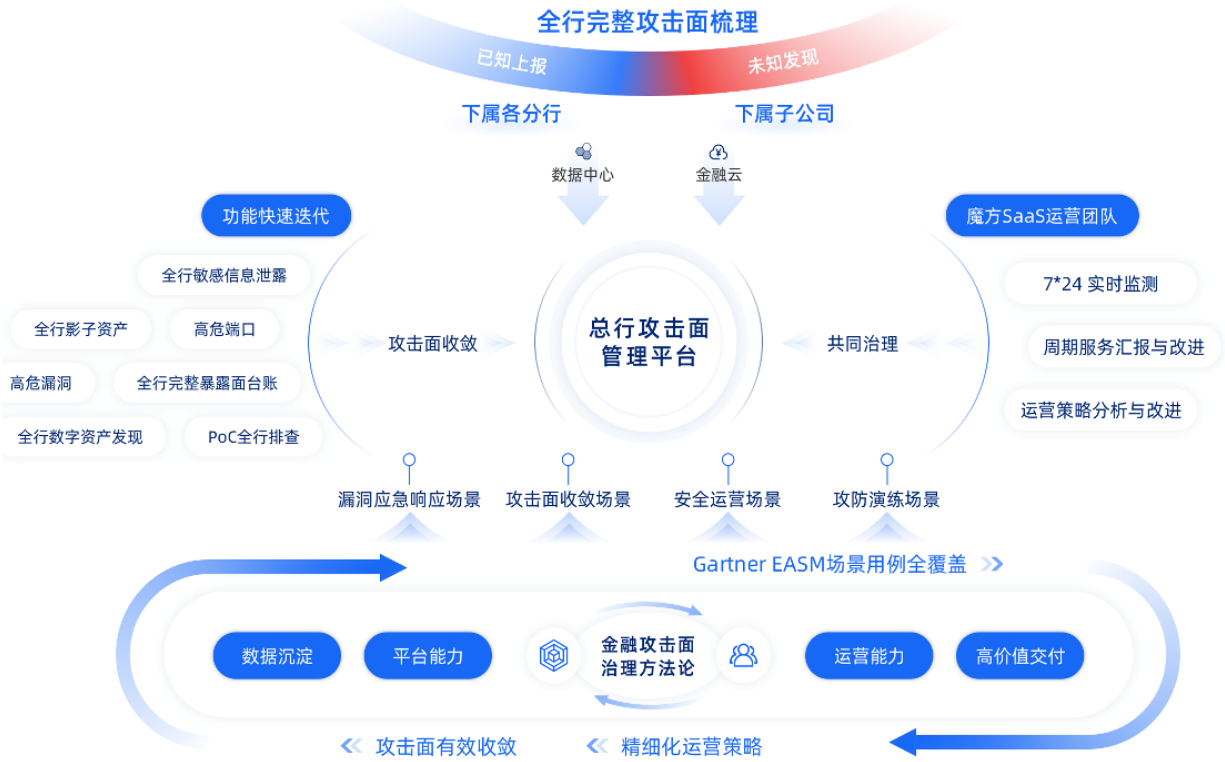


图 29：魔方安全——某股份制银行攻击面管理最佳实践项目建设情况

项目亮点：

- 精细化的攻击面运营：依照阶段式、抓重点的攻击面治理方法论，以产品+情报+运营能力持续交付，区分于传统的产品交付及数据情报交付，为其它金融行业客户提供高价值实践参考。
- 有效提升安全运营效率：平台能力高度自动化，实现 Gartner EASM 场景用例全覆盖，持续化监控互联网侧攻击面风险并有效收敛，将攻击面治理融入常态化运营工作，实时赋能安全运营体系。

客户价值：

- 构建攻击者视角的资产全景视图：传统的 IT 信息资产 + 新型的数字化资产一本账，持续监测影子资产，全面覆盖新业态数字化资产。

- 敏感信息泄露全掌握，可下架：依托平台化的大网数字风险搜索引擎，先于攻击者发现开源社区、网盘、文库、暗网等泄漏信息，学习引擎上下文验证，提供验证与告警，并可协助下架处理，有效避免网络入侵、数据泄露、监管问责等风险
- 风险持续监测，快速收敛：结合魔方持续更新的 POC、漏洞情报库，当高危漏洞事件爆发，第一时间知晓并定位、闭环。

（五）长亭科技----互联网攻击面管理建设项目

公司介绍：

长亭科技是国际顶尖的技术驱动型安全公司之一，全球首发基于智能语义分析的下一代 Web 应用防火墙产品；目前，公司已发布 10 余款自研技术驱动产品服务，形成以攻（安全评估系统）、防（下一代 Web 应用防火墙、高级威胁分析预警系统）、知（安全分析与管理平台、攻击面管理运营平台）、查（主机安全管理平台）、抓（伪装欺骗系统）为核心的新一代安全防护体系，并提供优质的安全测试及咨询服务，为企业级客户带来智能的全新安全防护思路。

项目介绍：

近年来，随着云平台、物联网、大数据等技术快速发展，某大型保险公司网络资产边界快速拓展，扩大了企业资产暴露面，且基于供应链的新型攻击也大大降低了攻击成本，企业面临的风险加剧。随着网络安全实战化的演进,客户希望通过切实有效的方式，对互联网攻击面进行统一的管理，寻找有效的技术手段，协助企业建立一份基于资产、脆弱性、风险管理的运营体系，提高互联网攻击面的感知能力，减少企业受攻击范围，提升企业基

于实战化背景下的安全能力。

客户要求通过 SaaS 服务,以周期性和定制化续期提供互联网资产暴露面核查服务(包括：资产基础信息、幽灵资产发现、互联网应用组件暴露面等）；公网敏感信息发现与监控服务，支持发现暴露在 Github、网盘、文库上的敏感信息；互联网主机/web 漏洞扫描，支持对网站进行 web 和系统漏洞扫描，发现系统环境潜在风险隐患，提供专业漏洞扫描报告，和对应的整改建议；互联网模拟攻击入侵，高级红队模拟攻击入侵，对客户的防护进行验证；失陷主机识别、IP 全端口监控、防护检测有效性评估、网站可用性监控、钓鱼/仿冒网站监控等服务。

项目建设情况：

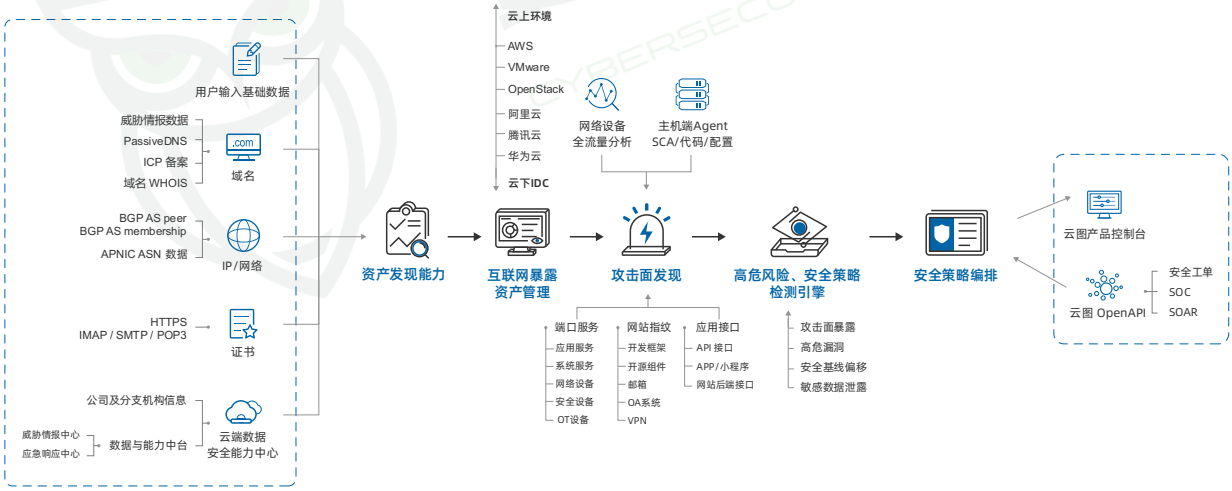


图 30：长亭科技——互联网攻击面管理建设项目建设情况

项目亮点：

- 基于长亭多年实网攻防经验设计，更贴近攻击者视角；
- SaaS 模式无需部署，无需占用客户资源；
- 自适应弹性扩容；
- 专业数据报表，为客户提供强有力的数据支撑；

- 专业的安全服务团队，协同响应；
- 攻击面 7*24 小时持续运营；

客户价值：

- 完善了在攻击视角下基于资产、脆弱性、威胁的风险管理提供重要支撑数据；
- 完善了对影子资产、未知资产的管理；
- 完善了对 Github、网盘等各类敏感数据泄漏的管理；
- 实时掌握互联网 IT 资产动态变化情况；
- 发现并整改了互联网边界存在的隐藏的高危风险隐患，提高了某大型保险公司的网络安全防护能力。

（六）未岚科技----全场景化攻击面管理建设项目

公司简介：

未岚科技是国内攻击面管理（ASM）领域创新的安全厂商，首次推出 3+3+3 全场景一体化攻击面管理平台。通过整合网络资产攻击面（CAASM）、外部互联网资产识别（EASM）、内部全网资产测绘（CAM）三大技术能力，全面、准确、细粒度地为企业理清安全数字资产，以攻击者视角自动、实时、智能地识别和管理暴露面，助力企业安全事业在未雨绸缪中稳步发展。成立至今，未岚科技已完成两轮 1000 万+融资，至今已有多个金融客户项目落地，有 20+金融、能源客户 POC。帮助企业安全部门平均发现 40%的未知资产，5 分钟内完成 1day 漏洞应急响应，提高 3 倍运营效率的同时，节省了 30%人力成本，获得客户高度认可。

项目介绍：

未岚科技「3+3+3 全场景一体化攻击面管理平台」将网络资产攻击面（CAASM）、外部互联网资产识别（EASM）、内部全网资产测绘（CAM）三大能力整合，通过 API 适配网关连接客户的各种设备和系统，全方位获取海量资产数据并对其深度分析，利用自研、独创的 VPT 智能算法过滤“误报”漏洞，识别高危、1Day 漏洞，帮助企业安全运营人员快速、高效地做出安全管理运营决策。

项目建设情况：

图 31：未岚科技——全场景化攻击面管理建设项目建设情况

项目亮点：

- 通过在客户线网中部署 CMDB、EDR、漏扫、准入、API 网关、容器安全、云平台、堡垒机、外网监测等近 10 几个厂商的 30 几个设备，对资产数据集中采集分析，形成全面、准确、细粒度的资产台账。
- 资产类型覆盖：主机、虚拟机、终端、容器、数据库、中间件、网络设备、物联网设备、API、外网 URL 等 10 几类，为客户量身定制出丰富的安全度量指标，并提供灵活的资产查询 API 接口供第三方系统消费调用。

- 同时，在客户端部署漏洞管理平台，集中采集多个异构漏洞，扫描设备数据，并对其进行泛化，去重，将资产上下文、网络访问关系上下文和漏洞情报上下文数据结合对漏洞数据进行富化，再利用未岚独创的 VPT 算法分析每个漏洞的可利用性，进而对漏洞修复优先级重新定义，最终根据漏洞所在资产或软件的运行上下文给出可自动化执行的缓解措施。

客户价值：

帮助客户覆盖 30+资产类型，提升近 30%漏扫覆盖率，并且将需要处理的漏洞数量由 10 万+降为每周 100 以内，15+安全度量指标实时输出给 CISO，1Day 漏洞响应速度所见到 1 小时以内。

（七）云科安信----某银行攻击面管理项目

公司简介：

北京云科安信科技有限公司是一家以数字风险为内核、将对风险边界的认知作为度量防御范围的尺度，与客户一起重塑安全边界，帮助客户轻量化地保有动态度量和鉴别风险的能力与权利，管理数字世界的风险的高新技术企业。云科安信聚焦防御、攻击、资产、角色、路径、攻击模拟与验证等风险场景，依托自身技术为客户重塑静态网络边界、动态网络边界、互联网络边界、数字世界边界、物联世界边界 5 大安全边界。

项目介绍：

网络攻防进入大国攻防时代，大国攻防的本质是多维度叠加下的全新安全域的对抗，任何一个维度叠加下的安全域都将使暴露面与风险呈指数级增长。银行作为国家金融基础设施，也面临越来越复杂多变的风险，需要用新的安全边界来度量风险尺度，在安全建设

的有效性和成本投入中找到平衡点，发现、验证攻击面进而收敛暴露面并作相应治理。

项目需求：

- 资产风险识别：从互联网探测和梳理银行的全部可发现资产并鉴定资产风险暴露面。
- 风险验证：在暴露面中梳理资产脆弱性，并对其可利用性进行验证，完成风险画像。
- 动态监控：以轻量化服务的方式随时随需动态监控风险的变化。
- 治理服务：提供收敛暴露面和风险管控的设计和建设方案。

项目建设情况：

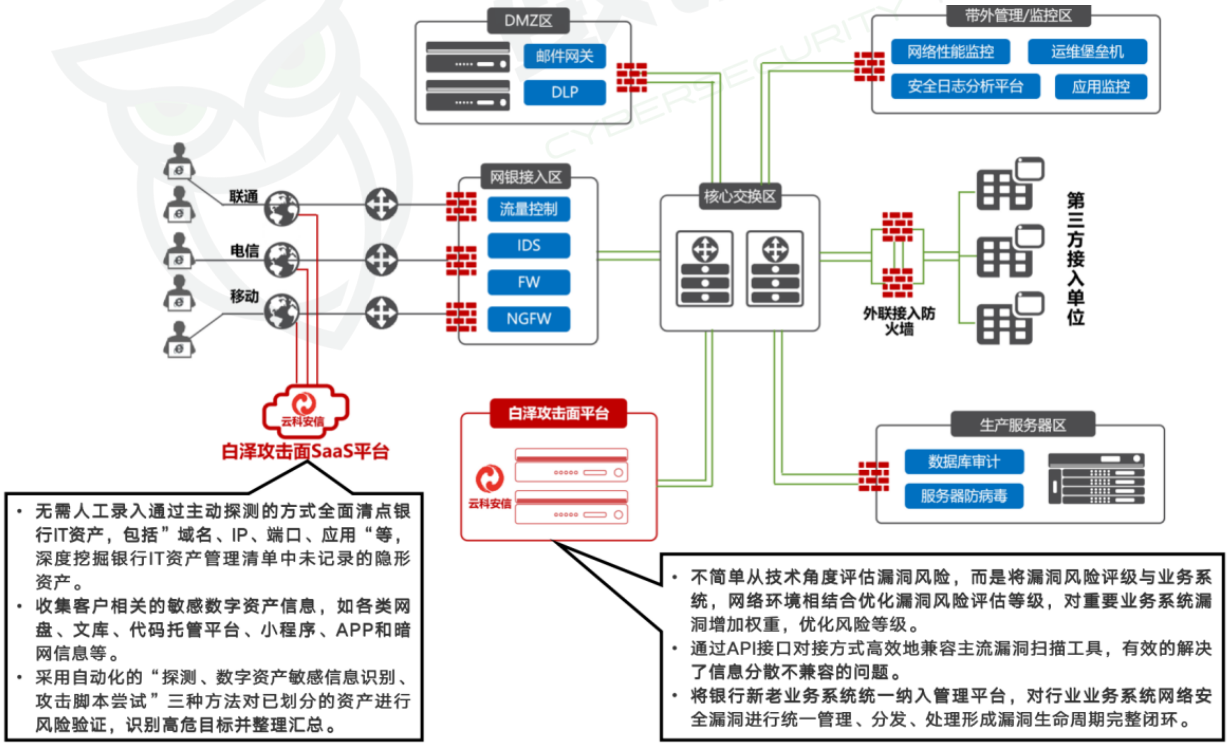


图 32：云科安信——某银行攻击面管理项目建设情况

项目亮点：

- 以风险为核心，以数字世界为视角，重新审视划分银行数字资产；

- 通过多维度叠加的方式主动探测重塑后的安全边界风险，扩宽安全防御范围和能力的尺度；
- 完成新一代安全架构的闭环管理，做到“预测、防御、验证、响应”的完整闭环；
- 降低了客户在风险探测与治理上的成本。

客户价值：

- 重新定义了安全风险边界，从全新框架弥补了过往安全防御的盲区；
- 将风险以信息图鉴的方式具象化，并随时随需动态度量其变化，实现风险可控；
- 将风险度量与验证的能力与权利以简单轻量的方式交还给客户，从完整的数字世界视角把握风险实情；
- SaaS 平台与本地化相结合，实现风险管理自动化、可持续、可追溯。

（八）螣龙安科----金融集团型企业资产测绘及管理解决方案

公司简介：

上海螣龙科技有限公司（螣龙安科）是新一代主动安全厂商，致力于实现安全自动化及安全可视化。公司核心团队来自上海交通大学网络空间安全学院，是信息安全领域的资深专家。以螣龙天眼攻击面管理系统为基座，螣龙安科为企业搭建全链条的安全验证体系，提供真实、实时、量化的“安全体检报告”，实现高度自动化的资产梳理发、风险检测，以及资产异动监控，从“主动安全”视角重新构建企业网络安全壁垒，赋能企业数字资产的高质量管理。公司客户覆盖金融、政务、能源、运营商等多个领域，且获得来自顺为资

本、名川资本等一线市场基金的资本支持。

项目简介：

某金融集团型企业在数字化转型的进程中，线上业务体量持续增长、复杂度不断提高，因此在安全建设方面遭遇以下痛点：

- 网络资产数量爆炸：集团总部及下属单位的网络资产及内外攻击面急速扩大，且资产更新周期短、速度快；
- 资产/攻击面可见性差：缺乏全面且自动的资产管理方案，无法建立起有效且全面的资产拓扑图；
- 管理方式依赖人力效率低下：下属单位遍布全国，难以实现统一管理，资产清单及漏洞检测时效性低；
- 响应速度不满足需求：资产管理的滞后，使得面对新安全风险的人工响应速度进一步低于风险通报的速度。

项目建设情况：

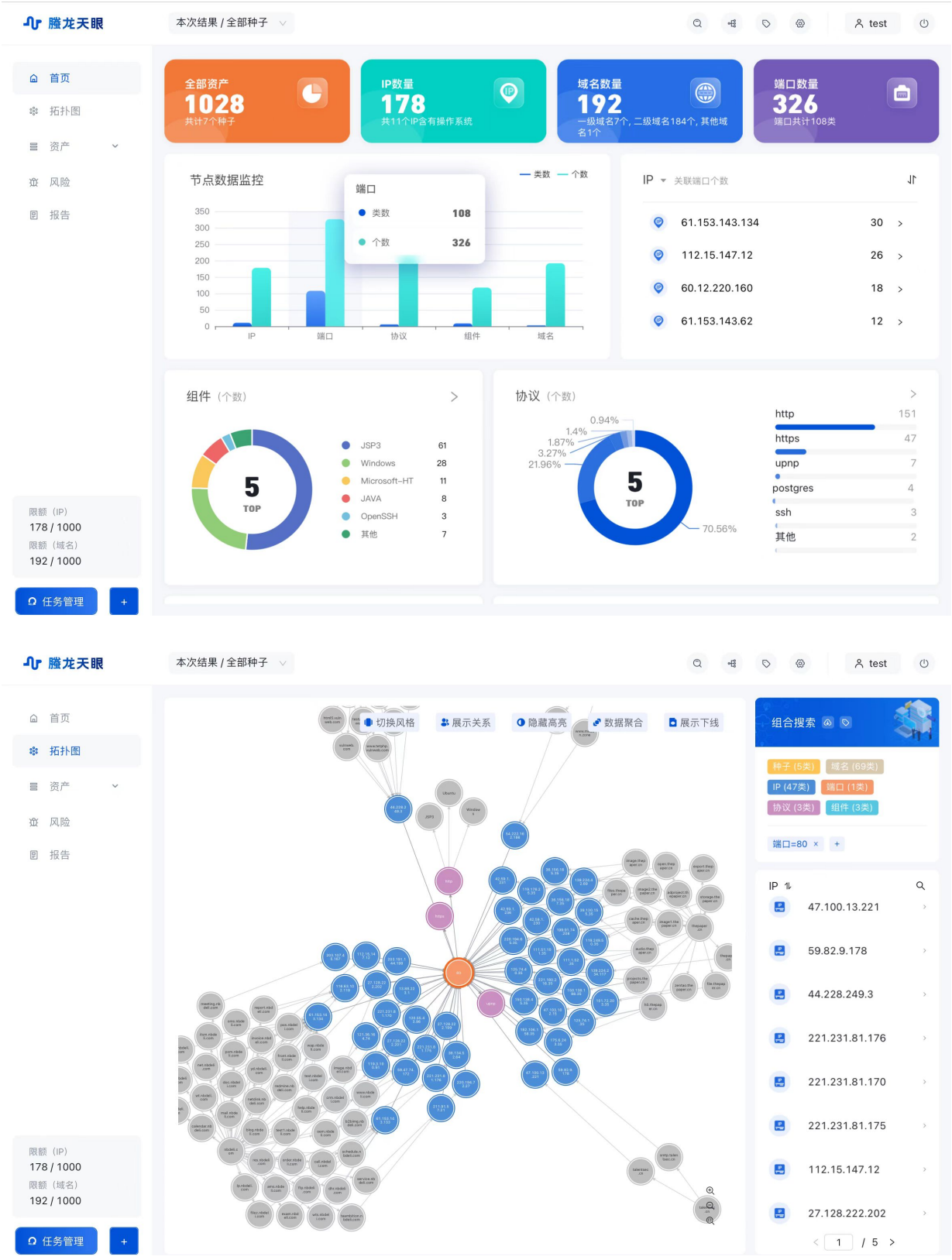


图 33：腾龙安科——金融集团型企业资产测绘及管理项目建设情况

项目亮点：

腾龙安科根据金融行业及集团单位的特性，结合产品优势，采用了以下四大技术点来解决现存的困境：

- 基于探针工作模式的分布式容器部署架构；
- 主动扫描与被动流量分析的自动化测绘；
- 动态交互式拓扑图及 3D 可视化大屏；
- 含大量 POC 及未公开 1-DAY 的漏洞库。

客户价值：

- 快速的资产测绘以降本增效：从人工到自动，资产测绘周期从数月缩短至数天，资产服务覆盖率从 35%提高至 95%；
- 高效的漏洞及安全风险响应：精准定位漏洞所在单位及资产，响应时间缩短 5 倍；
- 快速落地实施实现管理闭环：3 周内落地全国所有下属单位，实施部署对业务几乎零影响。

（九）华顺信安----某大型金融行业单位攻击面管理实践项目

公司简介：

北京华顺信安科技有限公司是一家专注网络空间资产测绘与资产安全运营管理的安全厂商，总部位于北京，并设上海、深圳、长沙、成都、武汉等多地分支机构。华顺信安将网安实战攻防作为重点研究方向，公司安全专家连续多年在各地攻防实践演练中取得优异成绩，同时公司旗下 FOFA 平台是全球安全人员频繁使用的互联网资产测绘搜索引擎，通过数年累计，华顺信安已拥有超过 51 亿条网络空间资产库数据，并以此打造出独有的

网络空间资产安全生态。华顺信安先后获评国家高新技术企业、国家级专精特新小巨人企业等。

项目简介：

在该项目中，客户提出以下需求：

- 需对散布在不同类型设备中的不同种类的全量 IT 资产信息进行集中管理和可视化；
- 金融机构因数字化转型带来的互联网暴露面不断扩大。客户需对其未知资产、僵尸资产、数字资产等互联网暴露面进行收敛及风险管理；
- 提高各类安全工具或安全策略的覆盖率，直观展现各类资产安全指标；
- 通过将多维资产数据，提升安全运营效率，形成整体防御、精准防御能力，提升该金融机构网络安全事件处置效率和应急响应速度 。

项目建设情况：

图 34：某大型金融行业单位攻击面管理实践项目

项目亮点：

基于攻击者视角全面梳理暴露面及攻击面，通过多种前沿核心技术，帮助该客户实现基于资产的安全运营，能够更快发现威胁、评估合规差距、确定风险优先级，以提升安全运营效率和网络安全防护水平。

- 实现全网 IT 资产的集中管理和可视化；
- 实现漏洞智能化管理；
- 实现安全指标度量管理。

客户价值：

- 摸清全网资产底数和风险敞口；
- 健全金融机构安全风险响应机制；
- 实现资产安全指标度量，助力资产安全运营。

DISCLAIMER
免责声明

本报告所用调研数据均采用样本调研方法获得，数据分析和相关结论因受样本来源和数量的影响，未必能够完全或唯一反映真实的行业及市场现状。所以，本报告只提供给个人或单位用于必要参考，数说安全不对任何依据本报告所作的其他分析研究和判断决策负责。

THANKS
致谢

本报告的数据采集工作得到了各界的大力支持，各项调查工作得以顺利进行，在各相关单位、调查支持网站以及媒体等的密切配合下，基础资源数据采集才能及时完成。在此，谨对他们表示最衷的感谢！

数说安全介绍

最专业的网络安全产业研究平台,以数据为基础,为网络安全监管部门、网络安全企业、网络安全产品与服务客户、网络安全资本市场等受众提供研究报告、顾问咨询、媒体传播、数字化营销工具等服务。

关注公众号

数说安全合作邮箱：ssaq@geniuscybertech.com

赛博英杰合作邮箱：connect@geniuscybertech.com