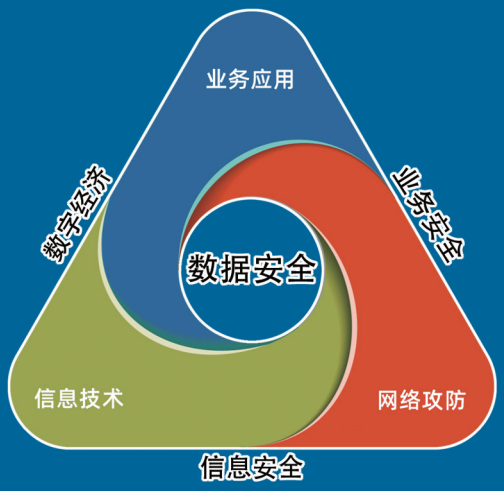
数世咨询
Digital World Consulting

攻击面收敛能力指南

数世咨询
Digital World Consulting

攻击面收敛能力指南



信息技术 + 业务应用 ➡ 数字经济

信息技术 + 网络攻防 ➡ 信息安全

网络攻防 + 业务应用 ➡ 业务安全

2020 年，数世咨询首创网络安全三元论，后进化为“数字安全三元论”，该理论由信息技术、网络攻防、业务应用三个支点与数据安全这个核心构成，其中：

- 信息技术是数字安全工作开展的基础，不清楚资产，何谈保护？没有网络，就没有网络安全；
- 网络安全的伴生、服务和对抗本质，决定了它将永远的场景化、碎片化和动态化；
- 业务应用既是信息技术与网络攻防的成本来源，也是两者最终的价值所在。

数字世界 以网络连接为基础，以数据流动释放价值，以人工智能塑造未来。
数字安全 以网络安全为基本手段，以数据安全为核心目的，支撑数字经济的健康发展和国家社会的和谐稳定。
数字世界，安全共生！

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构、网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

主笔分析师 **刘宸宇**
首席分析师 **李少鹏**
分析团队：**数世智库** 数字安全能力研究院

版权声明

目　录

目　录

前 言

继以色列安全初创公司 Axonius 作为一家专门从事网络安全资产管理的安全企业夺得 2019 年 RSAC 创新沙盒的冠军后，老生常谈的“网络空间测绘”、“资产管理”等概念重新走进安全从业者的视野并逐渐火热起来，Gartner 于 2021、2022 连续两年在 Hype Cycle for Security Operations 中收录 CAASM（网络资产攻击面管理）后，“攻击面管理”时代正式到来。

国内的安全供应商也是如此，无论较早成立的以“资产测绘”或“资产管理”为主要技术路线的企业，还是近两年如雨后春笋般新成立的定位“攻击面管理“的初创团队，都在积极向攻击面管理 ASM 这个赛道靠拢。

然而与西方不同的是，近年来国内安全市场在这一领域的驱动力仍主要来自于逐渐常态化的实战化攻防演练。

这就导致了一方面我们的攻击面管理基础较为薄弱，从机房的老旧设备到云端的新业务，潜在的攻击暴露面始终存在，另一方面我们针对这些攻击暴露面的动作仍然是周期性、运动式的。

这就决定了国内“攻击面管理”产品与解决方案在落地时，单纯的“管理”并不能完全满足需求，还需要重点关注“收敛”这一动作。

但与此同时国内的 CSO 岗位制度尚未健全，安全团队话语权普遍较弱，“收敛”往往会涉及到网络、运维、研发甚至业务等兄弟部门的沟通协作，技术外的成本一直很高，因此如何借助实战化攻防演练这一绝好机会，对攻击面进行集中式专项“收敛”成为突出的现实需求。

基于上述现状，数世咨询认为业内缺少一篇中立客观的横向调研报告，以

“攻击面收敛”为视角，对国内该细分市场做出梳理与论述。鉴于此，我们对国内具备“攻击面收敛”相关能力的安全企业开展了为期数月的调研工作，并在保护隐私不泄露任何调研原始数据的基础上，将调研成果整理成为各位读者看到的《攻击面收敛能力指南》。

报告结合国内现状，首先对攻击面收敛进行了定义及描述，之后对国内该赛道的市场规模进行了统计与概述，并针对主要能力企业画具了“攻击面收敛能力点阵图”，在关键能力部分，报告从 CAASM、EASM 视角分别进行了简述，并针对国内需求，重点描述了三个专项收敛能力，最后报告收录了该领域具有代表性的案例最佳实践，供各位读者参考。

鉴于时间紧迫，调研对象样本有限，报告中难免有遗漏、偏颇之处，请各位读者不吝指正。

关键发现

●国内“攻击面管理”产品与解决方案在落地时，单纯的“管理”并不能完全满足需求，还需要重点关注“收敛”这一动作。

●攻击暴露面指潜在攻击者对行业用户机构开展网络安全攻击时可能利用的所有数字资产、外部信息、脆弱性风险等数据的集合，称为该用户机构的攻击暴露面。

●攻击面收敛指行业用户针对机构自身及下属分支机构的攻击暴露面进行发现、判别、确认、管理，并协调内、外第三方对攻击面进行持续收敛的解决方案。

●据此次调研，2022 年国内攻击面收敛市场收入约为 6.24 亿元，同比增长 127.23%。高增长率来源于近几年国家与地方各级攻防演练的直接推动，以及用户侧对攻击面收敛概念的普遍认可。

●按照 60% 增长率的谨慎乐观估计，攻击面收敛这一领域 2023 年市场规模可达 9 亿元，2024 年市场收入可达到 15 亿元。

●对于潜在攻击者来说，攻击暴露面并不严格以 CAASM 和 EASM 作为区分，任何可被利用的外部信息、内部资产、脆弱性，都是最终用户应当关注覆盖的。

●目前国内常见的三个攻击面专项收敛能力主要有：漏洞风险资产快速定位与下线、外部信息攻击面收敛、办公网资产整体收敛等。

●攻击面收敛方案的交付将以“平台+服务”结合为主要方式，同时作为行业共识，攻击面收敛将成为安全运营必选项。

●攻击面收敛将从“安全事件驱动”向“风险量化驱动”转变。

1 攻击面收敛定义及描述

攻击暴露面

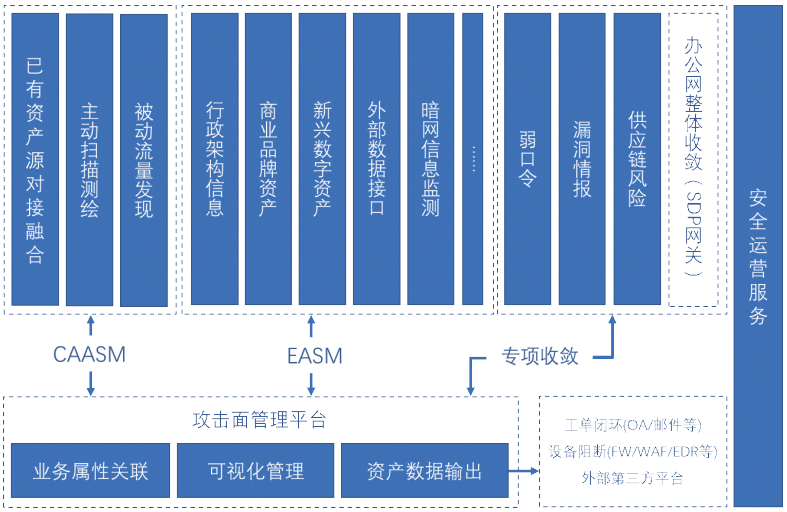
本报告中的攻击暴露面指潜在攻击者对行业用户机构开展网络安全攻击时可能利用的所有数字资产、外部信息、脆弱性风险等数据的集合，称为该用户机构的攻击暴露面。

网络空间资产

本报告中的资产指赛博空间中某机构所拥有的一切可能被潜在攻击者利用的设备、信息、应用等数字资产。具体对象包括但不限于硬件设备、云主机、操作系统、IP 地址、端口、证书、域名、Web 应用、业务应用、中间件、框架、机构公众号、小程序、App、API、源代码等。概括来说，只要是可操作的对象，不管是实体还是属性，都可以称之为“网络空间资产”。

攻击面收敛

如无特别说明，本报告中的“攻击面收敛”特指行业用户针对机构自身及下属分支机构的攻击暴露面进行发现、判别、确认、管理，并协调内、外第三方对攻击面进行持续收敛的解决方案。



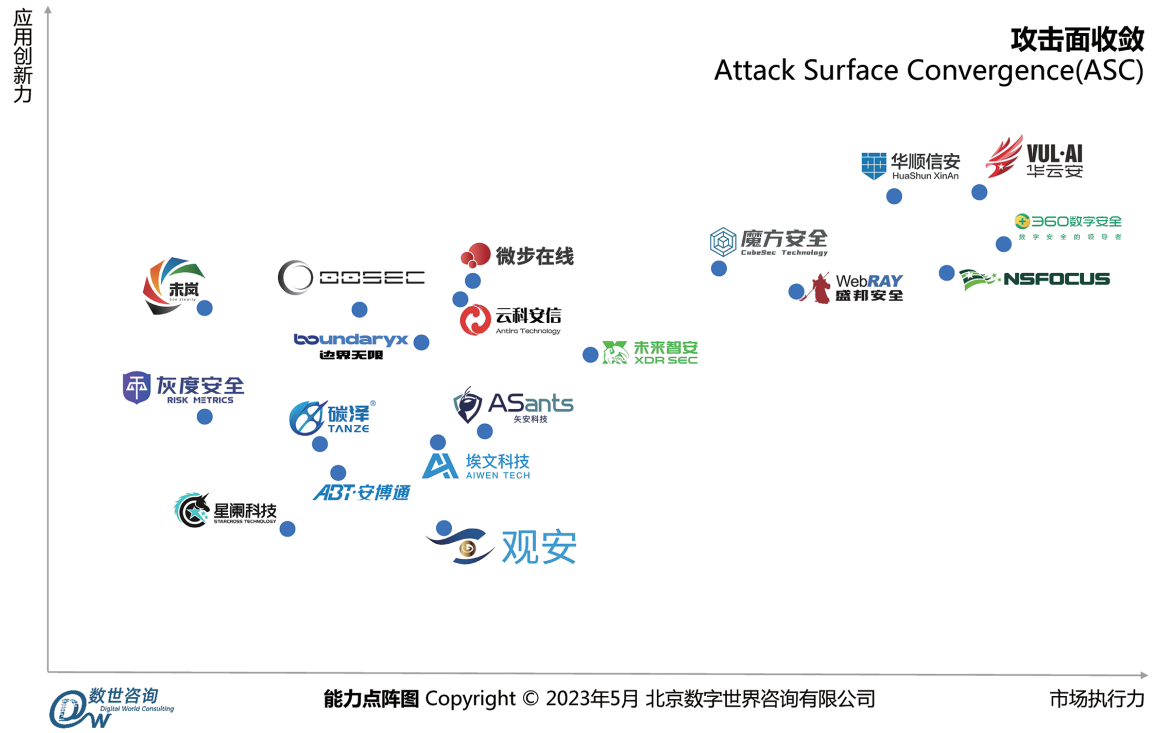
2 攻击面收敛市场情况

本次调研广泛征集能力企业参与，截至报告发布，共回收调研表30余家（以企业简称首字母排序）：

360数字安全、安博通、埃文科技、边界无限、白山云、长亭科技、长扬科技、烽台科技、观安信息、灰度科技、华顺信安、华云安、零零信安、绿盟科技、魔方安全、奇安信、矢安科技、盛邦安全、上海碳泽、天防安全、天懋信息、探真科技、微步在线、未岚科技、未来智安、雾帜智能、亿格云、云科安信、星阑科技、指掌易等。

能力点阵图

本次能力指南点阵图仍然以市场执行力、应用创新力分别为横、纵坐标轴，对企业进行展示。鉴于攻击面管理/收敛涉及行业、场景、技术实现方式多且杂，上述参与调研的企业并未全部在点阵图中展示：



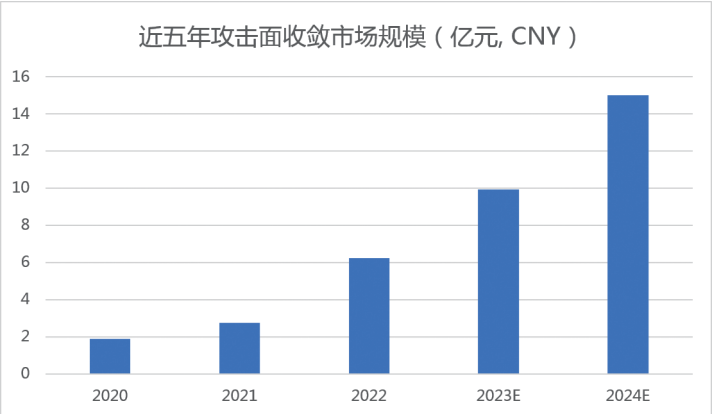
攻击面收敛能力点阵图

除点阵图中企业外，另有一些非典型攻击面管理/收敛赛道的企业，如烽台科技、长扬科技、天防安全、天懋信息等，具备典型的行业属性；又如亿格云、白山云、指掌易等利用零信任等新的理念或技术同样实现了“攻击面收敛”目的；部分未列入点阵图的能力企业，在后文中会另有叙述。

市场概况

根据此次调研，2022 年国内攻击面收敛市场收入约为 6.24 亿元，同比增长 127.23%。高增长率来源于近几年国家与地方各级攻防演练的直接推动，以及用户侧对攻击面收敛概念的普遍认可。

结合各家被调研企业对 2023 年用户预算的了解及整个市场预期，我们预计增长率会有较明显的回调，但相比其他细分领域，仍属高位。按照 60% 增长率的谨慎乐观估计，攻击面收敛这一领域 2023 年市场规模可达 9 亿元，2024 年市场收入可达到 15 亿元。

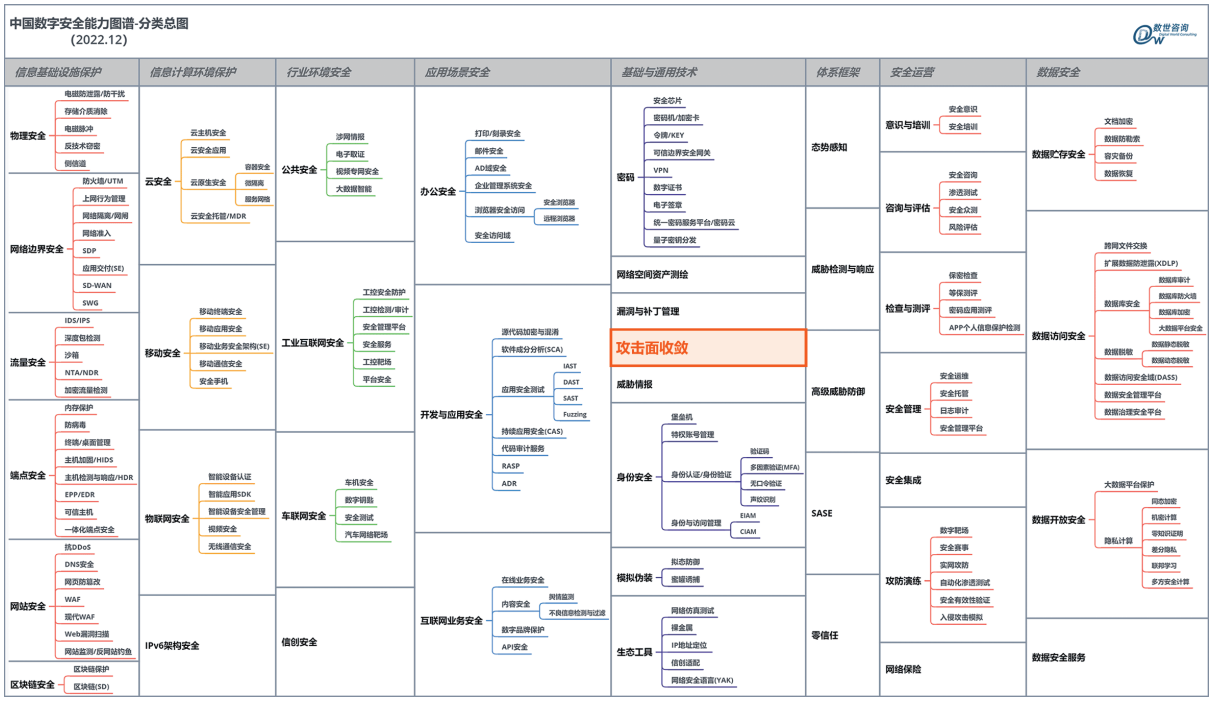


统计口径说明：

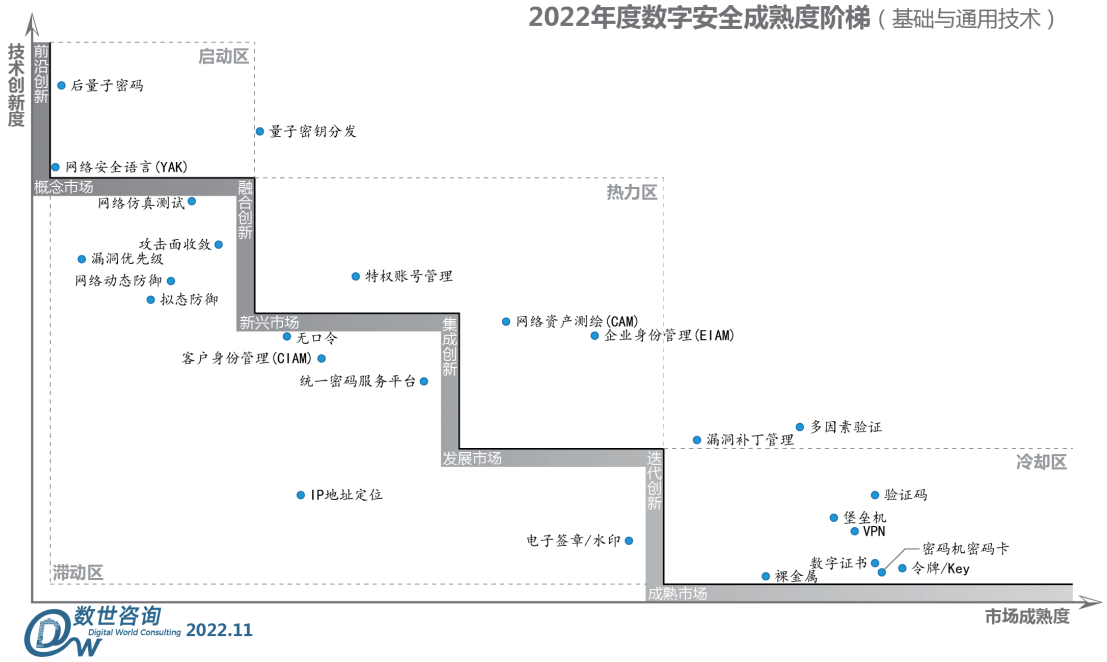
这里要格外说明的是，鉴于几乎所有行业所有场景下的安全工作，首先都会涉及到攻击面的发现、管理与收敛，因此若单纯以产品功能或解决方案模块等为市场统计依据，会重复纳入相当多其他安全领域的收入。因此本报告采用相对狭义的统计口径，仅以最终用户安全团队明确的攻击面收敛需求驱动的项目立项或采购为依据，将相关收入纳入统计。诸如传统的漏洞扫描、漏洞补丁管理产品，以及工业互联网、物联网等行业的相关营收，均并未计入此次调研

数据。特此说明。

在 2022 年底，数世咨询发布的《中国数字安全能力图谱》中，攻击面收敛属于“基础与通用技术“领域。



2022 年度《中国数字安全能力图谱》



2022 年度数字安全成熟度阶梯（基础与通用技术）

在“数字安全成熟度阶梯”中，攻击面收敛位于“热力区”，处于“融合创新”的“新兴市场“阶段。

3 攻击面收敛主要场景

攻击面资产纳管

对于传统网络协议环境，集团总部对各地分子公司、营业网点等分支机构的资产进行全面排查，将分支机构的潜在攻击暴露面资产纳入管辖范围，掌握集团整体攻击暴露面情况；分支机构也可以自行采购或建设攻击面收敛解决方案开展自查，然后将收敛后的资产信息上报给集团总部或监管机构，从而掌握主动权。

对于视频专网、工业互联网、以及 IoT 设备网络等专网环境，安全团队借助攻击面收敛能力对测试设备（影子资产）与更新换代后的老旧设备（僵尸资产）等进行纳管或下线处置。鉴于其行业场景特殊性，本报告将报名参与本调研的该领域能力企业在此单独列出，供有此类场景需求的用户参考：

- **烽台科技** —— 工业互联网攻击面收敛解决方案
- **长扬科技** —— 工控网络攻击面管理解决方案
- **天防安全** —— 视频网络攻击面管理解决方案
- **天懋信息** —— 特种行业专网攻击面管理解决方案

实网攻防演练

国家级、地市级、行业级实网攻防演练活动逐步趋于常态化。演练开始前，防守队对自身潜在的攻击暴露面进行提前发现和收敛；演练开始后，防守队快速定位失陷资产、精准下线失陷资产，第一时间做出收敛响应。

数据泄露溯源取证

安全应急团队将暗网、黑市中贩卖的样本数据等外部攻击面，与内部数据

对照相互印证，进而定位失陷设备、资产乃至人员，形成攻击证据链。一方面为下一步诉诸法律手段提供法律依据，另一方面对同类资产横向排查同类攻击行为，避免再发生类似泄露事件。

安全运营基础设施

安全运营建设初期,以攻击面暴露面作为其他各项安全投入的依据和基础;安全运营建设过程中，以接口化攻击面管理平台作为SOC、SIEM等平台的底座;安全运营能力形成后，结合安全有效性验证与量化评估进一步收敛攻击面，持续提升整体安全运营水平。

4 攻击面收敛关键能力

为方便读者与业内已有概念对照，本报告以大家所熟知的CAASM、EASM与专项收敛三个方面来描述攻击面收敛的关键能力。然对于潜在攻击者来说，攻击暴露面并不严格区分内外，因此，下面这些关键能力点虽然分别描述，但并非相互割裂，而是互为补充。任何可被利用的外部信息、内部资产、脆弱性，都是最终用户应当关注覆盖的。

CAASM

CAASM直译为网络资产攻击面管理，对应到国内市场这里的资产主要指位于机构内部、数据中心或云环境中等可直接管辖范畴内的资产。对这一部分攻击面的收敛，要重点关注与已有资产源的对接适配、主/被动资产发现、管理与可视化等关键能力。

与已有资产源的对接融合

首先CAASM应当具备多源资产数据接入能力。包括但不限于CMDB、终端管理平台、AD域等运维数据，以及NDR、EDR、HDR（含HIDS）等具备资产发现能力的安全产品及解决方案。

其次，多源资产数据接入汇总后，并非简单叠加，而是要进行持续交叉验证、去重 / 扩充、属性补全、标记等操作。具体需要结合业务数据流、网络流量、访问拓扑等多个维度，综合描绘出资产之间的关系链，将原本不同部门的资产台账融合为统一的资产视图。

主 / 被动资产发现

在与各资产源对接形成攻击面管理的基础后，可通过主动扫描探测与被动流量发现结合发现更多潜在的攻击暴露面。

主动扫描测绘有两点要说明，第一，结合目前的国际形势，我们不建议使用 Shodan、Censys 等非国内工具进行扫描探测；第二，主动探测不能影响用户的业务连续性与稳定性，应当结合用户的业务运行时间、IT 设备承受强度，综合考虑资产指纹库、节点分布、扫描时间等情况，以合理策略发起扫描。

被动流量发现可以不受业务时段限制，在金融行业交易等不便于使用主动扫描探测方式的时段持续提供资产发现能力。对于加密流量，可以通过资产指纹加密流量建模等方式，通过一段时间的机器学习，做到部分账外资产的准确发现。在实际调研中，笔者也了解到在一些资产变化频率较快的行业（如教育行业），这一能力已经产品化且形成了落地的最佳实践。

管理与可视化

经过多源资产对接、主 / 被动资产发现后的各类资产数据，最终统一聚合到管理平台。管理平台应当具备以下能力：

一是基于业务视角的资产属性完善与关联。例如根据业务架构，通过“标签”对资产所属的业务线、系统应用、相关负责人等属性进行关联补充，目的是体现出资产的业务价值等级、业务连续性要求等重要属性。

二是资产数据的统计与汇总等可视化管理，这里要结合业务权重、告警可信度、漏洞优先级等维度，对整体视图以知识图谱等方式进行呈现，目标是迅

速发现攻击暴露面中需要优先收敛的部分。

三是完备精准的资产数据输出。资产数据除了为撰写报告与汇报材料提供有力支持，还可以对接给漏洞管理平台与工单系统，形成漏洞管理闭环，也可以支撑 FW、WAF、EDR 等设备，形成实时阻断响应能力；此外，还可以作为后续长期安全建设的基础性数据，输出给安全运营中心等大型项目或平台，为其提供丰富且精准的资产数据支撑。

EASM

从攻击者视角来看，“信息收集”是发起攻击前必做的功课，且会占据攻击者大部分的时间精力。因此对安全团队而言，除了要关注直接管控的“内部”资产，还有机构外的攻击暴露面，即 EASM，这里分为机构数字资产与对应的脆弱性风险两个方面进行讨论。

资产类别	常见资产
IT 资产	• 服务器、云主机、存储设备、网络设备、安全设备、物联网设备、终端设备... • IP 地址、域名、子域名、端口、api、应用系统、证书...
软件资产	• 操作系统、数据库、中间件、邮件系统、办公软件、安全软件...
移动资产	• APP、公众号、生活号、小程序.....
数字资产	• 源代码、文档、账号、客户数据、业务数据.....
脆弱性风险	• 漏洞、弱口令、配置核查、供应链安全、非法数据贩卖.....

常见资产与脆弱性风险，本图例由 360 数字安全提供

数字资产发现

首先，潜在攻击者首先会搜集用户的机构信息，搜集渠道主要有各大搜索引擎、天眼查类平台、网盘文库、官网、公众号、钉钉群、微信群、代码共享平台等。因此，安全团队要先于攻击者发现此类资产，为响应收敛争取时间。

其次， GitHub、码云等代码共享平台是需要重点关注的外部攻击暴露面。安全团队应以技术监测手段与内部行政管理相结合的方式，对此类攻击暴露面进行持续发现、收敛。

除了代码平台，还有合作伙伴或第三方平台的 API 数据接口，与微信公众号菜单对接的 URL、小程序或 H5 中隐含的数据接口等。这类外部接口在开发测试使用过后即随着项目结束而被遗忘，极易成为潜在的攻击暴露面。

最后一个值得重点关注的是针对暗网进行持续的社工库、泄露数据监测。对暗网交易市场中的样例数据进行抽样比对，能够直接判断泄露数据真实性，还能够为梳理数据泄露的路径提供依据与证据，帮助安全团队进而梳理出攻击暴露面中的薄弱环节。

脆弱性风险

在通过上述各渠道发现机构相关的数字资产后，安全管理员还应当关注自身潜在面临的弱口令、漏洞、供应链等脆弱性风险。这里重点关注与各类资产相关的漏洞威胁。

用户可实时关注国际国内主要的漏洞库、漏洞共享平台、社区，有条件的用户还可以直接采购漏洞情报，或对暗网中的漏洞交易平台进行监测。在漏洞描述中，用户可重点关注受漏洞影响的系统、应用、版本号、影响范围等与资产直接相关的关键信息。

主要目的是能够在 0.5day/1day 漏洞爆发时，第一时间根据漏洞关键信息，匹配定位到潜在受威胁的资产后进行收敛，下面的专项收敛部分会详细叙述。

专项收敛能力

攻击面的“收敛”目前仍然处于管理手段为主、技术手段为辅的阶段。在这样的背景下，本报告将攻击面的收敛能力以三个主要场景来阐述。

漏洞风险资产快速定位与下线

为应对 0.5day 或 1day 漏洞而进行的风险资产快速定位与下线，安全团队首先要在漏洞爆发前，对资产台账按照业务优先级进行标记，对系统、应用、中间件及版本号等关键信息精细管理、持续更新。

接下来，当漏洞爆发时，使用这些关键信息筛选定位出风险资产，快速分发 PoC 进行漏洞的精准匹配，并根据资产的业务优先级下发不同的响应策略。在不影响业务连续性的前提下，可协调业务、运维等部门，对部分资产做临时下线处理；对于受业务连续性要求既不能下线又不能修复的资产，则通过“虚拟补丁 / 透明补丁”的方式临时加固，待将来允许时，再行修复。

快速应急之后，安全团队将该漏洞信息通过工单、OA 等流程推送至业务及 IT 运维等部门，对包含漏洞风险的资产进行周期性精准复测。此外，还需要对漏洞响应之后新加入台账的资产进行漏洞 PoC 测试，杜绝“新资产、老漏洞”的情况发生，以此实现漏洞风险的攻击面持续收敛。

外部信息攻击面收敛

对于外部信息攻击暴露面，针对外部信息所在平台不同，需要采取不同的收敛策略。

对于外部接口类信息，例如公众号小程序，要从机构内部找到相关 API 接口关闭；对于共享平台类的外部信息攻击面，例如代码共享、文档文库共享等平台，可以通过举证申诉等方式，联系平台方进行信息下线处置；对于不具备举证申诉条件的平台，例如暗网交易市场等，则需要首先通过泄露样本数据等进行攻击路径溯源，将外部信息攻击面关联至内部网络资产攻击面，亦或是某个内部员工，然后再做进一步的收敛处置。

需要强调的是，无论采用上述哪种收敛策略，对于此类外部信息攻击暴露面，重点是先于潜在利用这些信息的攻击者进行自查。抢得先机才有足够的时

间进行收敛。。

办公网资产整体收敛

有条件大幅调整网络架构的用户，还可以利用基于零信任理念的“单包敲门”方式，对攻击面资产进行整体收敛。

所谓“单包敲门”，即单包授权 Single Packet Authorization 的一种通俗说法，是 Software Defined Perimeter 软件定义边界的关键特征。这一方法可以将办公网等互联网业务以外的资产隐藏在零信任安全网关后面,实现“批量”收敛内网资产的效果。

严格来说，这一方式不属于业内“攻击面管理“的技术赛道，但同样可以起到攻击面收敛的效果。其局限性在于对原有网络架构的改动较大，对钓鱼攻击的防护效果也很有限，需要结合其他收敛方式以及安全意识教育等手段，以达到更好的立体收敛效果。

下面列出了部分报名参与本调研并具备该项能力的企业，有条件对网络架构进行较大调整的用户可以参考：

- **亿格云** —— 零信任安全访问解决方案
- **白山云** —— 零信任安全访问
- **指掌易** —— 灵犀 SDP 安全网关

5 攻击面收敛未来展望

攻击面收敛作为行业共识，将成为安全运营必选项

在笔者去年年底进行的金融行业攻击面管理调研中，多家金融机构安全负责人都提到，除了各级实网攻防演练外，近两年的日常安全运营中都发现境外IP对境内金融机构的扫描明显增多，虽然没有产生真实的攻击，但是有明显的扫描动作。由此可见，攻击面收敛已成为金融客户在内各行业的普遍共识。团队的安全运营工作，有条件的将以专项收敛推进，条件暂不成熟的，也会以“商业秘密保护”等方式，与审计、合规、法务等部门联合推进。攻击面收敛将成为安全运营的必选项。

攻击面收敛方案的交付将以“平台 + 服务”结合为主要方式

目前行业内攻击面收敛项目普遍以平台的产品形式进行交付。未来一段时间，攻击面收敛的落地方案将由标准化平台产品负责大部分常见的数字资产，再结合人的服务解决业务差异性，从而覆盖更为完整的攻击暴露面。这里的“服务”部分，将多由相对初创阶段的外部团队负责，“服务”积累下来的资产指纹和收敛经验，会逐渐固话到攻击面收敛产品中，在用户与厂商的共同成长中，攻击面收敛的成效也会越来越显著。

攻击面收敛将从“安全事件驱动”向“风险量化驱动”转变

伴随传统技术栈的升级，容器化、DevOps（CI/CD）、微服务等云原生技术的应用，数据的获取、分析、处置，都会有很大改善。安全团队相比以前可以实现更全面的数据（特别是业务相关数据）的采集，这就为攻击面风险的可视化 / 量化提供了更为有利的技术基础与数据基础。由此我们预见，攻击面的收敛也将从过去的安全事件驱动逐步向风险量化驱动转变。安全运营团队的工作价值得以量化体现，用户机构“一把手”也得以最大限度规避因为突发安全事件被问责的风险。

6 攻击面收敛案例收录

某金融行业用户案例

本案例由华顺信安提供

场景介绍

随着金融机构稳妥发展，金融科技和数字化转型不断加深，导致相应的资产数量和资产种类也日趋增多，资产暴露面越来越大，同时数据密度和网络资产价值凸显，系统的关联性和复杂度不断增强，相应的攻击手段也在不断变化，传统资产安全管理方式难以为继。当前网络安全已经是金融科技发展的重要保障，金融机构所面临的网络空间安全环境在发生剧烈变化。因此，收敛金融行业互联网暴露面、明确需要保护的网络空间资产、保护核心资产免受各类安全威胁，开展有效的资产安全运营成为金融机构亟待解决的问题。

客户需求

随着金融监管部门对金融企业网络安全的重视不断加强，某大型金融机构已经将开展资产管理及安全风险管控作为安全运营的首要工作。华顺信安通过多次与该客户深入沟通，明确了客户的资产安全管理需求，主要包括以下内容：

●全网 IT 资产的集中管理和可视化

底数清则态势明，该金融机构网络资产繁多且归属复杂，包括云主机、网络设备、办公终端、安全设备、业务系统、IOT 终端、容器、API，并且不同种类的 IT 资产信息散布在不同类型的设备中。

●互联网暴露面及其风险管理

具备互联网暴露面监测能力，该金融机构的数字化转型带来的互联网暴露

面不断扩大，如果不对暴露面进行收敛，将成为整个网络安全体系的重大短板，包括未知资产、僵尸资产、违规资产、钓鱼网站、仿冒资产等，其次还需要具备公众号、小程序、APP 等数字资产的发现、互联网数据泄露风险监测能力。

●安全指标度量能力

该金融机构的资产安全运营的目标之一是提高各类安全工具或安全策略的覆盖率，需要直观展现各类资产安全指标。包括客户端覆盖率、安全管控覆盖率、安全风险整改率，并通过构建全面的在线资产库，快速定位未纳入安全管控的资产信息，如：未安装防病毒的 windows 服务器、未安装 HIDS 的服务器，消除资产安全管理盲区，还需要建立各个条线、团队或业务系统的安全指标动态变化曲线，跟踪各类安全指标变化情况。

●资产赋能能力

需要具备丰富资产数据接口，通过将多维资产数据，可供第三方平台消费使用，可对接给态势感知，实现关联安全告警日志和资产信息，实现告警事件的快速定位、跟踪、处置；可对接 SOAR 实现多种安全告警事件的自动化处置，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。

解决方案

整体方案设计思路以华顺信安 FOBrain 网络资产攻击面管理平台、FORadar 互联网资产攻击面管理平台（外网资产测绘探针）、FOEYE 网络资产测绘及风险分析系统（内网资产测绘探针）为基础，全面对接该客户多个资产数据源、漏洞数据源，对资产、漏洞等信息做清洗、去重、归一、关联等分析工作，实现资产画像和各类关联分析。能够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

通过 FOBrain 调用 FOEYE 和 FORadar 实现资产测绘的同时，还接入客户侧的 CMDB、HIDS、堡垒机、TDP 等十多个数据源，建立了可视化的数据模型，支持字段级的数据源优先级配置，解决了数据源字段冲突的问题，帮助该客户梳理了已知资产、数字资产，识别了未知资产、仿冒资产、违规资产，形成了精准的资产库，并通过将多个来源的 IT 资产碎片化数据进行关联分析，实现对资产属性的多维度画像。

●实现漏洞智能化管理

FOBrain 现已积累了数十万的漏洞情报库，首先通过对接多源异构的漏洞扫描工具，实现调度漏洞扫描工具，将多个漏洞扫描工具的漏洞数据基于漏洞情报库进行标准化处理，解决漏洞数据格式不统一的问题。同时，基于 CVE、CNVD、CNNVD 进行归一化去重处理，通过对相同的漏洞做了去重合并，有效降低漏洞数量，降低数据噪音。

基于 FOBrain 创新漏洞优先级排序技术，重新定义了漏洞优先级，漏洞优先级不仅基于 CVSS，还从漏洞是否存在 POC、EXP、漏洞是否多次出现、漏洞是否可以远程利用、漏洞关联资产的重要性、所属区域、互联网暴露情况、FOFA 引擎热力值等多个加权值，计算漏洞优先级，该客户的安全运营人员只需关注归一化之后的漏洞数据，且漏洞处置顺序更加有的放矢。同时，通过关联分析，可以直观的看到漏洞对应的责任人、内外网资产映射关系，并有多种漏洞状态：未处理 、待修复、待核查、已修复、忽略、误报、复现等，极大的提升了漏洞安全运营工作效率。

●实现安全指标度量管理

基于精准全面的资产库，解决了资产的唯一性识别问题，通过与 EDR、WAF、数据库审计进行对接，能够直观展示各类资产安全指标，包括 CMDB 覆盖率、防病毒客户端覆盖率、WAF 覆盖率、漏洞修复率等多个指标，快速定位未

纳入安全管控的资产信息，同时帮助该客户绘制了安全指标动态变化曲线，能够跟踪各类指标变化情况，反馈安全运营治理效果。

客户价值

●摸清全网资产底数和风险敞口

通过华顺信安强大的资产测绘能力，统筹该金融机构互联网资产和内网资产，建立了精准化的资产信息库，打破了客户现有的资产数据孤岛，摸清了资产底数和资产暴露面及攻击面，有效弥补当前的资产管理短板，帮助该金融机构落实资产责任到人，时时掌握资产安全态势，为网络安全管理奠定了基础。

●健全金融机构安全风险响应机制

通过全面、深入以及持续高效的资产安全监测和漏洞智能化管理，实现了“业务系统－互联网资产－内网资产－风险－部门－责任人”的自动关联分析，帮助该金融机构建立了基于资产多场景化的自动化处置流程，实现风险资产通报机制，通过闭环式的监督、管理、检查，帮助该客户总部履行监管协查、责任通报、结果复核的监督管理职能，摆脱以往依赖人工处置的困境，缩减修复窗口期，从而降低资产安全风险，实现可落地的预警与风险整改督促。

●实现资产的安全指标度量，助力资产安全运营

基于为该金融机构构建的全量精准资产库,实现了对资产安全指标的度量，通过各类覆盖率的分析与展示，快速定位未纳入安全管控的资产信息，同时提供安全指标动态变化曲线，能够实时跟踪安全指标的变化，助力实现资产安全运营。

某大型国有集团用户案例

本案例由 360 数字安全提供

场景介绍

随着数字化转型、互联网业务的不断发展，某大型国有集团由于经营范围广泛，分支公司众多，信息化业务已经具备较大规模，为了保障信息化业务安全，支撑上层安全运营、统一监管等各项安全措施开展，该大型国有集团建设了资产与脆弱性子系统，将网络中运行的各类信息化业务及其风险统一管理，提升安全管理基础能力，并面向数量众多的分支机构开放自服务，形成了整体化的攻击面管理能力。

客户需求

●全网资产发现能力建设

发现在企业网络中活跃的各类设备，包括私有云主机、终端、服务器、网络设备、安全设备等，并通过多种手段那堆资产进行细粒度的识别和监控，获取实时、详细的资产信息。

● 1day 漏洞快速定位和评估

当出现 1day 漏洞时，能够基于详细的资产维护信息，快速定位 1day 漏洞所影响的资产以及他们关联的业务情况，从而评估 1day 漏洞的影响范围。

●集团化资产运营体系建设

为分子公司提供资产上报、确认、梳理的途径，建设全集团的资产运营管理机制，保障资产的业务归属、人员归属等信息详细、准确。

●风险汇聚和全生命周期管理

汇聚多个来源的漏洞数据，包含扫描器、HIDS、情报平台等，对多个来源的漏洞进行加工归并、风险评价，并基于平台跟踪漏洞和弱口令的修复情况。

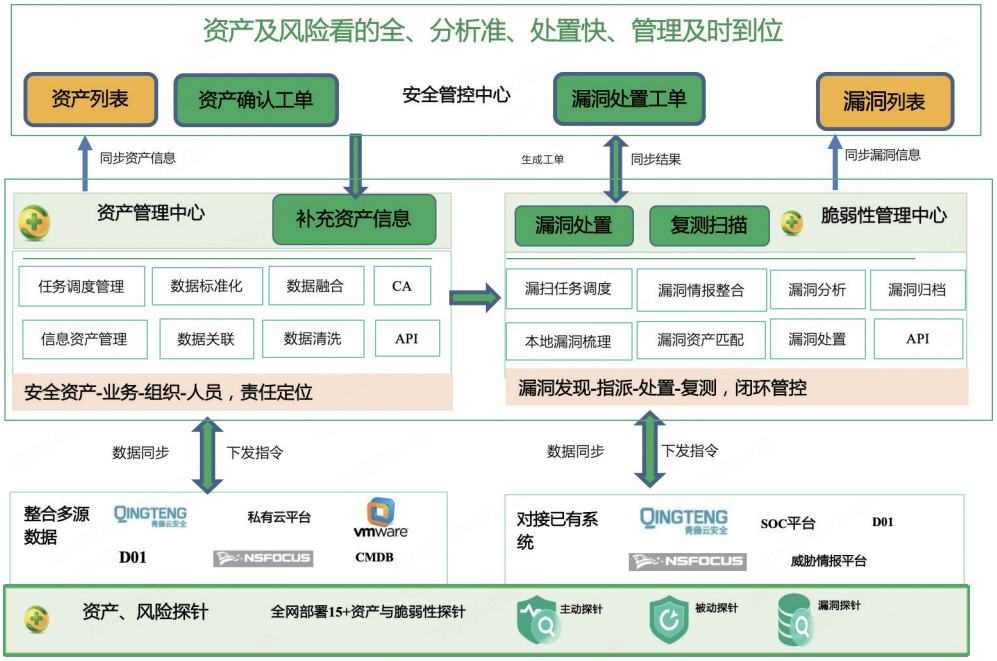
建设方案

根据该大型国有集团客户的建设需求和实际业务场景，为客户设计建设了资产与脆弱性管理子系统。该系统功能包含资产发现、资产管理、漏洞检测、漏洞管理、生命周期跟踪、任务管理等多个模块。

在本项目中，资产与脆弱性子系统共计对接整合了十余个资产系统、6 类漏洞检测工具，对接范围包含 CMDB、私有云、HIDS、漏扫工具、情报平台、SOC 等，有效将原有建设的各类安全平台中分散的资产、脆弱性数据进行了整合加工。

同时该项目也从资产、脆弱性检测维度，为客户提升了整体资产与风险发现呢能力，根据业务实际需求，为客户在多个子网中建设主动资产探测、被动流量识别、漏洞扫描三类探针共计 15 个，实现了全网资产发现能力建设，能够持续化监控并发现企业内网资产。

子系统整体与上层安全运营平台进行对接，为安全运营工作提供资产与风险数据支撑，同时联动工单能力，形成资产与风险全生命周期管理，并为子公司提供数百个账号，面向子公司提供了资产、风险上报与处置能力。
整体建设方案示意图如下：



客户价值

●建设全网资产识别监控机制，从而形成集团化资产管理体系

通过建设主动、被动资产发现能力，发现在网络中存在的未知资产和“僵尸”资产，同时对接已有资产来源，融合加工后形成权威资产库，为分子公司提供资产确认、上报、业务登记途径，最终形成集团化资产运营管理体系。

●多来源漏洞去重后统一纳管，降低漏洞处置工作量

对接各类漏扫、HIDS、SOC 平台、威胁情报平台等六个漏洞来源，纳管 20w+ 漏洞，并对漏洞数据进行去重和缩减，合并多来源漏洞避免重复工作量。

●分子公司漏洞全流程线上管理，全面掌握漏洞加固进展

支持漏洞自动化复测，根据漏洞来源任务自动化下发复测任务并获取复测结果，降低原本复测工作量，同时对漏洞处置工作进展的平均时长、当前进展状态等维度进行统计，帮助客户全面掌握漏洞处置工作进展情况。

●漏洞优先级推荐，快速定位优先修复漏洞，降低响应时长

系统根据资产重要性、漏洞情报、漏洞等级等维度，对漏洞的加固优先级进行评价，快速定位需要优先修复的漏洞，帮助客户降低重大漏洞的响应时长

某运营商用户案例

本案例由探真科技提供

背景介绍

某运营商单位在早期搭建好容器云 PaaS 平台，采用传统的针对物理机、与虚拟机的安全防护模式，但不管从实现方式、规模、防护方式等方面均一定程度上不适用于容器云 PaaS 平台，无法针对容器场景下的安全威胁做到很好的发现与拦截。正值单位内部组织针对集团自身的 HW 活动，借此机会梳理当前容器化场景下内部网络的安全脆弱性，希望能在 HW 期间实现收敛攻击面，并建设自身针对容器平台的安全防护能力。

客户需求

探真科技通过与客户紧密沟通，包括结合客户的实际环境，明确在此次 HW 行动中客户所关注和面临的问题主要如下：

●云原生化衍生了一些新的安全问题，如：逃逸难度降低，利用组件 API 暴露提权等，传统安全产品在这类场景下防御能力不足，需要针对这类新型攻击方式具备较好的发现能力。

● HW 中攻击队会使用 0day、1day 等攻击手段，导致普通防御方式失效，很难被检测到，希望能针对这类未知攻击具备发现能力。

●大量的无效告警极大的消耗了运维人员的精力，希望能根据条件筛查一

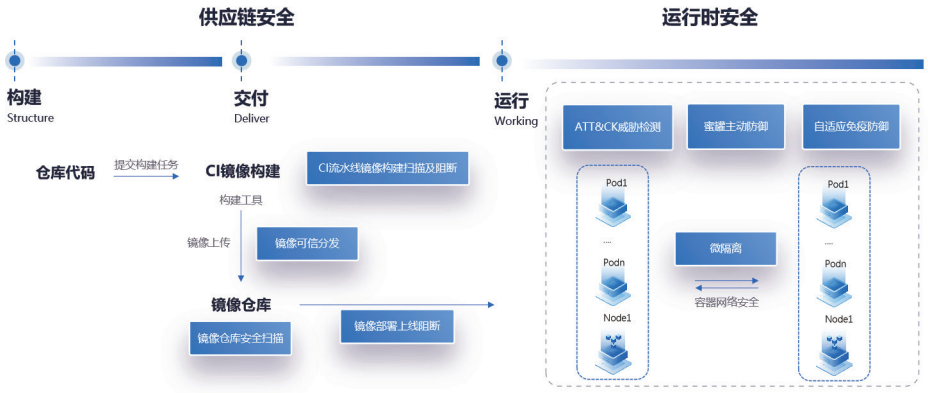
些准确的、实际的威胁，快速定位攻击发生位置、攻击时间、攻击方式等。

●希望对目前仓库中的镜像进行一个全面检查，发现目前镜像中存在的一些恶意文件、敏感信息、病毒木马等，同时筛选出存在高危漏洞的镜像，客户将针对这些镜像进行修复。

●客户目前已具备有 WAF 等南北向流量的防御能力，普通攻击队想从外网攻入难度较大，但客户自身攻击队对内网结构及企业账号相关较为熟悉，每年 HW 从内网发动攻击的情况较多，有较多的逃逸及提权实践，因此比较关注逃逸相关的安全问题，同时希望能通过微隔离有效限制攻击范围。

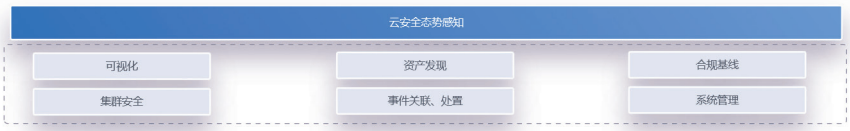
建设方案

根据以上问题，探真科技结合 HW 场景以及客户容器安全能力构建需求，提出了针对运行时安全检测以及镜像安全的完整解决方案，其中具体包含了“镜像扫描、流水线扫描与阻断、运行时攻击检测、主动防御、偏移防御、微隔离”等安全能力，并辅以“容器资产梳理、精细化告警筛查、攻击事件关联”等能力，帮助客户在 HW 及容器安全能力构建中发挥作用。



探真科技将容器侧风险分为了两个部分，一部分是供应链风险，攻击方可能利用镜像投毒、容器后门、镜像漏洞等方式发动入侵，因此在镜像构建及入库阶段，通过对镜像构建进行快速扫描，即时发现并解决存在的各种系统漏洞、软件漏洞、病毒木马等问题，可保证业务基础环境的安全，同时可在多个阶段设置卡点，对不合规的容器禁止其入库或部署。

另一部分则是运行时风险，攻击者可能通过多种手段入侵，因此也需要更加全面的检测能力。针对逃逸、提权、容器后门等，检测引擎通过基于 ebpf 的内核态检测能力，可以及时发现攻击并无视攻击者的绕过手段；针对横向攻击，通过微隔离等手段进行细粒度隔离防止攻击扩散；针对 0day 等未知攻击，主动防御通过诱导攻击进而捕获入侵行为；另外，基于容器不可变性，偏移防御通过固化容器内二进制，并拒绝一切其它有害工具的引入，可实现强防御。



除产品的安全检测能力外，辅以人工值守，在整个攻防演练期间，针对客户的业务环境，定制开关部分规则以降低干扰，并通过持续的日志分析确认攻击事件的有效性，同时针对有效攻击进行溯源，协助客户共同处理。

客户价值

●构建完整云原生防护能力

通过供应链安全能力实现 CI/CD 阶段的基础镜像安全，通过基于 ATT&CK 的多重检测能力保障运行时安全，结合事件关联、资产可视化等多重安全能力，覆盖各个云原生场景下的各个安全风险点，全面收敛安全攻击影响范围，为客户构建了完整的云原生安全防护体系。

●攻击告警与拦截

在演练过程中，除了帮助客户发现与修复多个镜像漏洞外，产品通过运行时安全检测能力，发现多起针对容器的逃逸、恶意工具执行、端口扫描等攻击行为，并进行了及时上报与处置，同时主动防御模块也捕获了多起攻击者的内网横向移动，保障了客户在整个演练期间容器业务 0 失分。

●运营成本降低

通过自定义安全筛查条件，对告警事件实现了精细到具体进程、端口的过滤，剔除大量无效攻击事件，极大的缩减了运营人员针对攻击事件的筛查成本。

某证券行业用户案例

本案例由魔方安全提供

背景介绍

证券公司业务场景走向互联网金融化已成未来发展趋势，互联网 + 新业态 + 新生态发展成为各证券实现业务快速拓展的必经之路，此背景下监管侧、券商侧、消费者侧都在时刻关注其网络安全水平及风险防范能力，而互联网攻击面治理又为常态化安全运营中最重要的一环，当前各证券公司的互联网受攻击面正在不断增长，暴露在攻击者视角下的企业攻击面更趋复杂化，随着网络攻击技术的持续演进，各证券公司在攻击面治理领域面临严重的压力与挑战，如何发现并高效管理互联网攻击面，持续治理并收敛风险，更好地管理组织数字资产、防止各类安全事件及数据泄漏事件发生，护航业务安全，是网络安全工作中的重中之重及决定整体网络安全体系建设是否达标的关键一环。

客户需求

新业态场景下，数字资产形态变化快、管理难度大，如何精准护航业务穿透式发展？

由于当前业务竞争的压力大，新互联网金融线上业务“野蛮发展”，业务驱动 IT 场景下带来的资产形态、资产数量、资产属性、资产状态动态多变，组织需要关注的数字资产类型复杂，除传统的互联网域名、业务系统外，微信公众号、小程序、APP、支付宝生活号、业务第三方生态合作系统已成为需要持续跟踪管理的组织新型数字资产攻击面，如何统一纳管，提升安全团队、运维管队管理效率，为整体安全运营提供有力支撑，助力业务开拓，成为互联网攻击面管理的第一必答题。

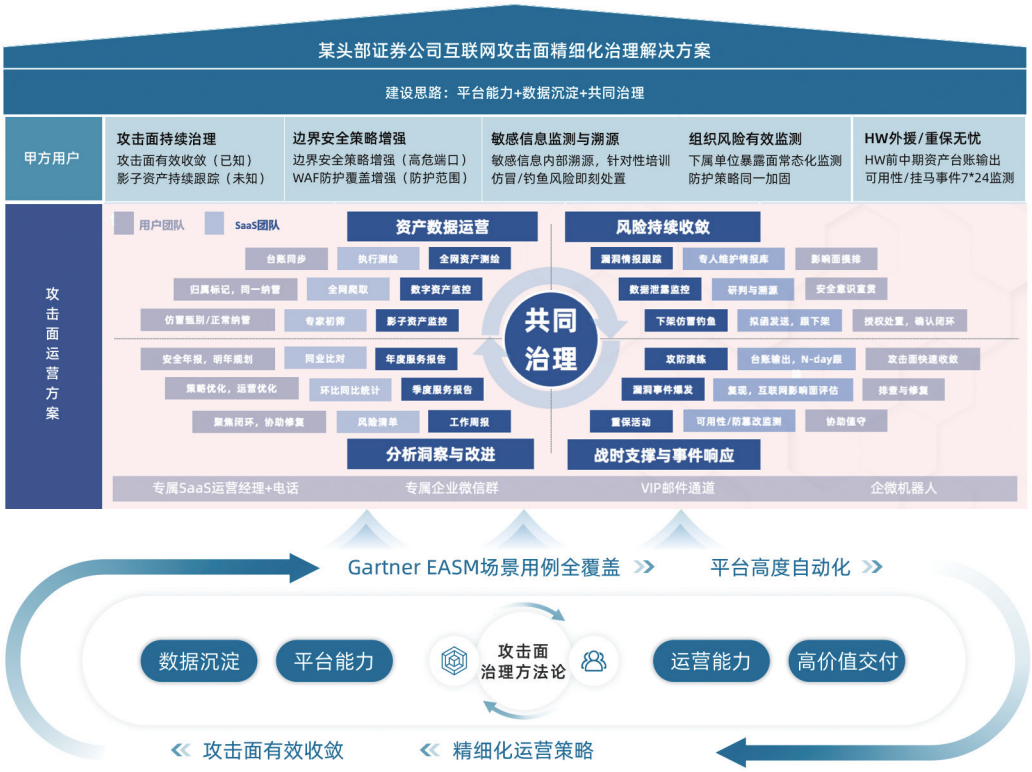
实战型导向已成为监管新趋势，如何抢在监管之前发现、闭环互联网侧风险事件？

当前证券公司面临着多个行业主管单位的交叉监管，当前各监管力度趋向于实战型问题检查，影子资产、仿冒网站、高危漏洞、数据泄漏首当其冲成为其攻击暴露面扫描与通报的重点关注场景，安全团队需要构建常态化安全运营能力，建立高时效性的攻击面收敛响应能力。

敏感数据泄漏逐步强合规，但缺乏多源监测能力及运营能力。

证券行业机构及用户数据资产由于其行业特殊性，成为攻击者重点关注对象，随着《数据安全法》、《个人信息保护法》等政策法规的实施推行，当前组织敏感数据泄露监测能力及排查收敛成为当前重点需要弥补的短板能力，一方面外部攻击形势日益严峻，攻击者持续挖掘证券公司内部数据进而流入非法平台获利，如用户信息、交易信息等，另一方面内部员工、第三方合作商缺乏安全意识及有效管理，在工作中有意无意将业务系统核心代码上传至GitHub、Gitee等第三方代码托管平台，重要文档、文件共享至第三方网盘文库、文档共享平台，造成安全威胁。

解决方案



通过魔方安全外部攻击面管理EASM平台(Gartner EASM场景用例全覆盖)，

配套精细化攻击面运营服务，以产品＋情报＋运营能力持续交付，最终实现攻击面管理的指标化运营。

1、数字资产统一纳管解决方案：一本帐，已知理得清，未知全发现，安全团队可管理。

●通过对现有已知台账导入及金融云平台对接，实现现有互联网资产的掌握与同步。

●通过魔方外部攻击面管理系统 EASM 实现深度数字资产发现、云资产采集，SaaS 安全运营专家辅助业务梳理与登记，做到全资产的统一纳管，做到已知资产一本帐。

●通过对某证券公司的组织资产属性分析，生成资产线索，并根据企业名称、Logo、APP 名称、代码特征进一步拓展关联线索，通过魔方自主全球影子资产发现引擎及多方光谱 API 查询，实现影子资产监测常态化、自动化。

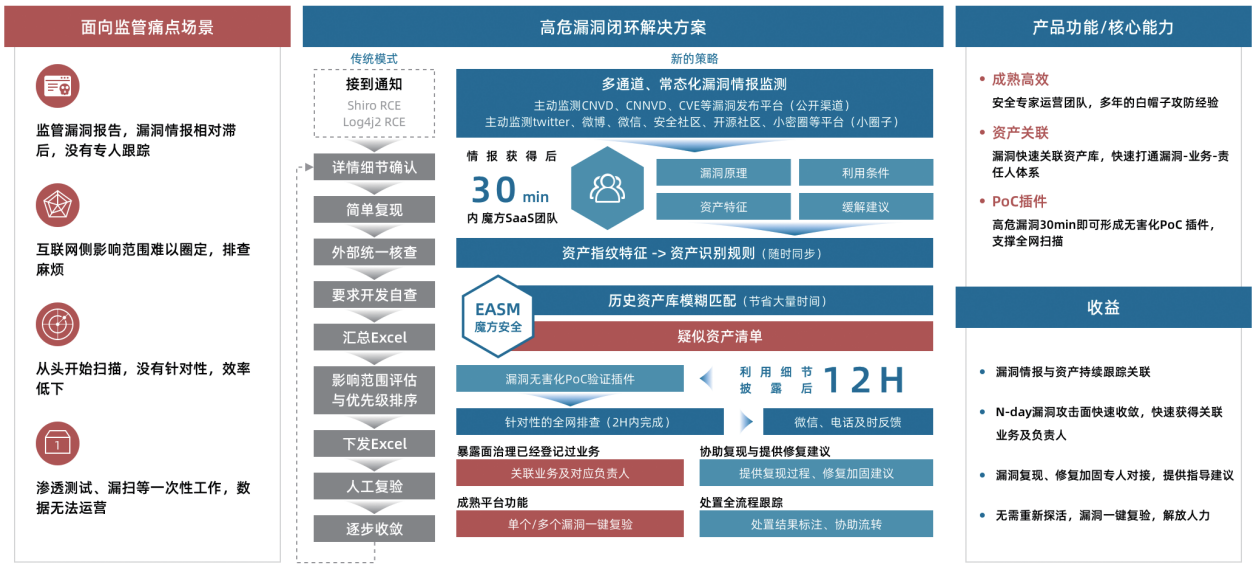
2、防微杜渐，主动、及时响应上级监管单位要求，高危漏洞快速修复。

●通过魔方安全外部攻击面管理系统 EASM 多通道监测漏洞发布平台，数

字情报实验室主动挖掘监测 twitter、微博、微信、安全社区、开源社区、小密圈等平台，并及时通过漏洞情报下发到产品

●高危漏洞 30min 内自动化预警，SaaS 安全运营专家解析漏洞形成无害化 PoC 验证插件，输出详细漏洞原理、利用条件、缓解建议，辅助客户根据资产库进行全网验证排查并进行全生命流程跟踪及过程保障，针对已修复漏洞可利用平台快速一键复验。

●联动魔方漏洞管理平台 CVM，针对漏洞事件通过深度学习学习引擎实现漏洞数据聚合、去重，通过 VPT 技术，将漏洞修复过程转化成精细指标项，结合 EASM 平台资产库快速关联业务及负责人，实现漏洞攻击面快速收敛。

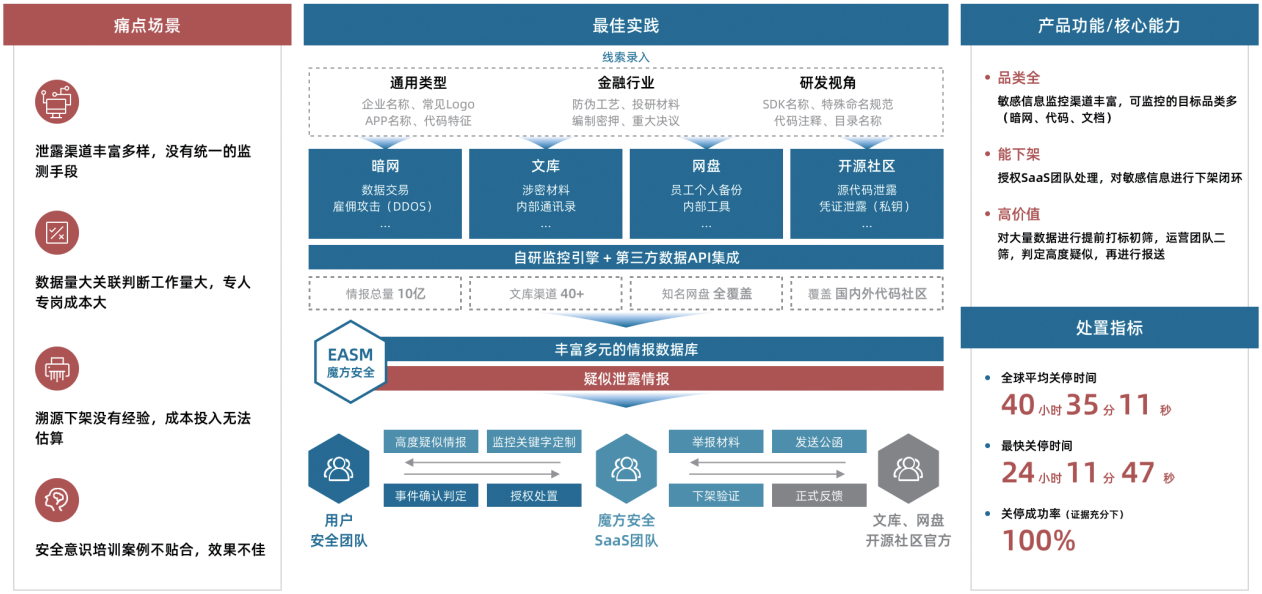


3、建立常态化、多源化数据泄漏监测能力并逐步具备数据运营能力，针对主流泄漏渠道实现全覆盖，并实现关停

●用户根据当前安全关注重点，公司当前业务特点及研发特点，协同魔方 SaaS 安全运营专家制定监测线索，针对暗网、文库、网盘、开源社区通过 EASM 平台自动化、全范围监测

●针对海量泄漏告警，通过 EASM 平台数据过滤引擎及 SaaS 安全运营专家人工干预调整数据泄漏关联规则，帮助客户梳理高价值重点泄漏事件，极大提

升安全运营效率，并针对重点泄漏信息进行下架闭环。



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。

●风险持续监测，先于监管定位问题，进快速收敛：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。

●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。

数世咨询
Digital World Consulting

第三方中立

- 完全第三方背景
- 独立分析师团队

调研对象

- 700+网络安全企业
- 年均500+深度沟通
- 年均2000+小时访谈时长

服务对象

- 国家、行业监管机构
- 行业客户及用户
- 网络安全产品&服务供应商

服务内容

- 国家、行业智库
- 细分领域等调查研究报告
- 为服务对象提供面对面咨询
- 为产业各方提供资源对接

合作方式

- 各类报告定制
- 年度企业观察列表
- 活动赞助
- 投资FA

北京数字世界咨询有限公司（以下简称数世咨询）是国内数字产业第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布过《中国网络安全大事记》、《中国数字安全能力图谱》、《中国网络安全能力100强》、《中国网络安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，并与400余家具备原厂能力的安全企业和100余家安全行业领先者企业，以及110余家有网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动，投融资对接，安全产品与企业推荐，企业资源整合等。

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区鲜鱼口街90-2号网安小酒馆
官方网站：https://dwcon.cn
联系邮箱：dw@dwcon.cn

数世咨询
Digital World Consulting

数字安全领域中立第三方调研机构