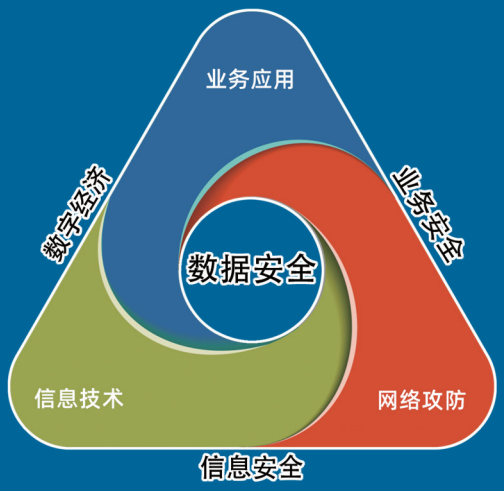
数世咨询
Digital World Consulting

2022 中国金融行业
攻击面管理白皮书

数世咨询
Digital World Consulting

2022 中国金融行业攻击面管理白皮书



信息技术 + 业务应用 ➡ 数字经济

信息技术 + 网络攻防 ➡ 数字安全

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

目 录

前 言

金融行业具有关键基础设施属性，是国家与社会生活正常运转的基础与核心。金融行业具有领先的科技属性，AI、区块链、云计算、大数据、5G 等新技术都能在金融行业中找到优秀的最佳实践。同时，金融行业还具有极高的安全属性，从信息安全到网络安全再到数据安全，金融行业的安全需求始终以“强合规、高要求”走在各行业前列，由这些新需求带来的供给侧安全技术创新，也具有很强的示范性与可复制性。

在关基属性、科技属性、安全属性等三个属性背景下，金融行业安全建设与运营，最首要场景需求是梳理潜在的攻击暴露面并有效缩小这个攻击面，使其收敛至可视、可查、可控的程度。这成为了金融行业中安全从业者要面对的第一个，也是最基本的一个问题。

面对这一需求，供给侧情况如何呢？我们先看国外，继“网络空间测绘”、“资产管理”等概念之后，Gartner 于 2021、2022 连续两年在 Hype Cycle for Security Operations 中提出了 CAASM（网络资产攻击面管理），开启了“攻击面管理”时代。我们用以色列安全公司 Axonius 为例，作为一家专门从事网络安全资产管理的安全企业，它夺得了 2019 年 RSAC 创新沙盒的冠军，在夺冠当年，它的 slogan 是这样说的：

You can’t secure what you can’t see.

三年后，它则明确提出了：

From assets management to assets intelligence: crossing the CAASM

此为一证。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“资产安全管理”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。

然而与国外环境不同的是，国内金融行业虽然相比其他行业已经大多设立了首席安全官 CSO 或有专门的安全团队，但话语权普遍不高。近年来国内安全市场很大一部分驱动力，来自于监管机构的合规要求和逐渐常态化的实网攻防演练，导致在应对潜在的攻击暴露面时，有很多不同于国外的“独特”管理手段，例如，发现风险资产后收敛的难度更大，常常需要借助安全重保与攻防演练的机会，对其进行收敛。

综上所述，数世咨询认为在突出的现实需求与供给能力之间，始终缺少一个以行业用户访谈为基础，以金融行业为代表的“攻击面管理”报告对其做出梳理与阐述。鉴于此，我们协同国内攻击面管理领域安全厂商魔方安全对银行、证券、基金、资管及互联网金融等数几十家金融行业典型客户开展了为期一个多月的调研工作，并在保护用户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《2022 中国金融行业攻击面管理白皮书》。

报告同时还收录了该领域具有代表性的一些国际、国内能力企业，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

●金融行业安全强合规，但与“攻击面管理”直接相关的合规要求始终缺少可落地的指导细则。

●金融行业攻击面管理“同业参考”是一个伪命题。

●金融行业业务变化快，攻击面管理更加注重资产生命周期的多标签动态管理。

●金融行业的收敛响应时效要求更高，攻击面管理平台应具备较强的可观测（可视、可查、可控、可度量）能力。

●金融行业攻击面的收敛效果主要依赖于资产数据的完整性、可观测性，以及与漏洞等脆弱性情报的关联性，这些也都同时与机构的安全策略管理与安全有效性验证存在正相关。

●攻击面管理作为行业共识，将成为安全运营必选项。

●金融行业攻击面管理将向“大集中”靠拢。

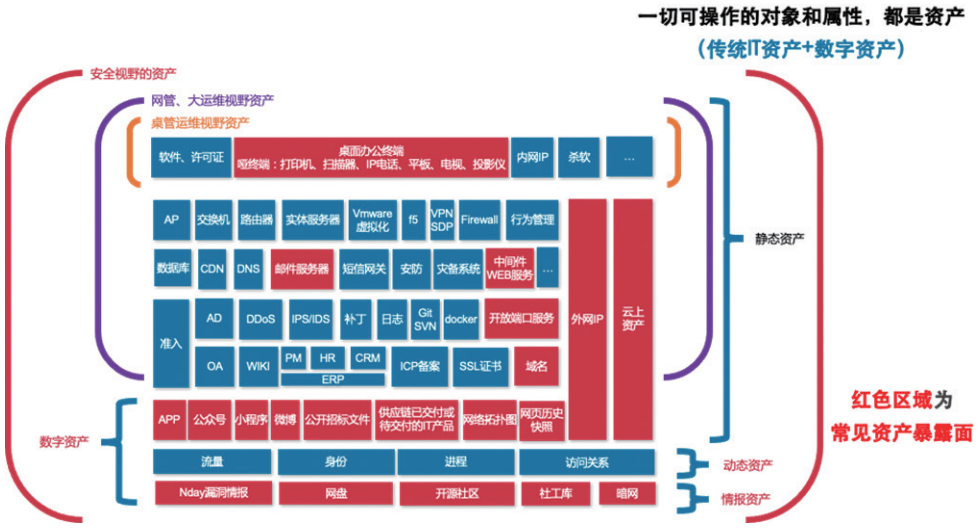
●金融行业攻击面管理方案的交付形态，以“平台 + 服务”相结合的方式为主。

1 定义及描述

1.1 攻击暴露面

本报告中的“攻击暴露面”指潜在攻击者对金融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。

资产的定义：首先明确网络空间资产的定义，这里的资产是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”。

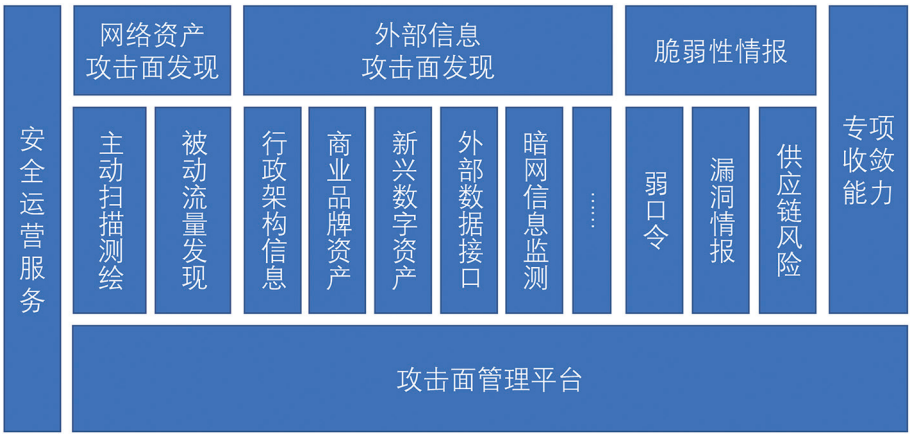


图例 1：常见攻击暴露面数据纬度（本图例由魔方安全提供）

1.2 攻击面管理

如无特别说明，本报告中的“攻击面管理”特指金融行业用户依托攻击面管理平台，结合安全运营服务，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，并协调内、外部第三方对攻击面进行持续收敛的解决方案。



图例 2：金融行业攻击面管理示意简图

1.3 EASM 与 CAASM

攻击面管理分为外部攻击面（External Attack Surface Management，缩写为 EASM）和网络资产攻击面（Cyber Asset Attack Surface Management，缩写为 CAASM）。EASM 强调外部攻击者视角，针对暴露在公网的资产（包括互联网、云、物联网、智慧城市等环境下的资产与风险），主要通过黑客探测的手法与情报来进行分析。CAASM 则强调内外部全局视角，通过 API 与其他系统集成的方式来解决持续的资产可见性和漏洞风险。

1.4 与现有安全解决方案的区别

对比项	渗透测试	漏洞扫描	攻击面管理
服务对象	指定的业务系统	指定的IP范围	暴露在互联网上全部的资产与风险：IP、域名、端口、登陆入口等常规资产及POC漏洞扫描、供应链、下属单位资产、影子资产、数字资产（App、公众号、小程序等）、敏感信息泄漏（网盘、文库、开源社区）、情报（暗网、社交媒体）
周期/频次	季度/次或更久	月度/次或更久	攻击面管理以平台化方式可高频次 特殊时期能24或72小时/次（重保/攻防）
交付特征	工具+人工服务 数据结果人工维护，依赖于人员能力及工作状态	扫描报告	平台+人工服务 历史数据留存平台，可追溯、可复查、可维护，将安全经验，持续转化为平台检测能力，基于数据与情报驱动的安全运营
安全策略有效性保障	低频检测，部分检测、延迟感知	低频检测，部分检测、延迟感知	高频检测，全量检测 动态监测、及时感知
检测全面性	模拟黑客进行指定系统的缺陷发现	只关注指定系统的漏洞，基于漏洞库匹配指定资产是否存在漏洞	建立互联网资产档案库，关注资产变化动态 暴露面视角，提供资产详情，延伸到数字资产、数据资产全面风险检测，颗粒度细致
检测颗粒度	颗粒度较粗，缺少资产作为底座 对指定系统的漏洞挖掘较深	颗粒度较粗，缺少资产作为底座	颗粒度细致，资产覆盖硬件、系统、服务、支撑和应用层 可实现"资产-风险-责任人"的关联 可整合、调度各漏洞扫描工具
成效	快照式安全，投入高 结果依赖于人，偶然性强	缺失上下文和关联信息 数据噪音大 安全团队需要进行大量分析工作	全量资产及风险监测，持续完善攻击面情报 最新漏洞预警与响应处置 数据与情报驱动持续、动态的安全运营管理

图例 3：与现有解决方案的区别

攻击面管理与传统漏洞扫描及渗透测试服务的对比

漏洞扫描和漏洞管理是网络安全运营工作的基础，从防御者视角出发，聚焦现有的 IP 资产台账，进行常规的巡检与通报。但金融行业的业务具有多样复杂、快速迭代的属性，与之相伴的是企业的网络边界变得模糊，大量开源组件被广泛应用，并衍生出 App、小程序和 API 等数字资产新形态，这些变化让安全管理员遭遇巨大的挑战，传统的漏扫工具和专项渗透测试均不能很好地应对，从而出现更多的影子资产（Shadow IT）。

漏洞扫描类产品会根据 CVSS 评分体系对漏洞进行风险评级，方便安全管理员开展收敛工作。但对攻击者而言，更关注能被有效利用的价值漏洞，这种视角差、信息差令安全管理员的精力无法投放到更有价值的工作当中。

综上所述，快照式、长间歇的工作方式无法满足数字化业务和资产不断变化的要求。相对传统的渗透测试等安全服务手段，攻击面管理在广度、频度和数据驱动响应与运营方面的实践更优，也避免了高度依赖于人而导致的产出质量不稳定、资源投入大等问题。

攻击面管理与资产测绘及资产安全管理的区别

“网络空间测绘”的定义：**针对赛博空间中的数字化资产，通过扫描探测、流量监听、主机代理、特征匹配等方式，动态发现、汇集资产数据，并进行关联分析与展现，以快速感知安全风险，把握安全态势，从而辅助用户进行指挥决策，支撑预测、保护、检测、响应等安全体系的能力，即为网络空间资产测绘（CAM）。**测绘是一种技术手段，用于获取空间的数据实体，基本面向 IP 对象，端口与服务。

对比网络空间测绘，资产安全管理更进一步：更聚焦资产全生命周期安全管理，包括资产梳理、登记和上下线管理，强化工单与流程（登记、变更、资源分配、审核、通报），借助资产测绘等技术手段，建立风险治理机制和形成联动管控模式。清晰完整的资产台账、分类分级、边界和责任、资产多维属性

关联分析、风险管理、资产全景态势可视化分析，满足不同角色使用的（高层领导、信息化、安全管理、安全分析、安全运营、业务部门）的统一视角，让资产数据可管理、可运营。资产测绘是基础手段，全面且清晰的资产台账，是安全建设的必答题，也是迈向高水平安全运营的必经之路。

攻击面管理聚焦在攻击者视角，是一种比网络空间测绘和资产安全管理更高维的资产安全管理的方法，融入了更多威胁因素，以保护组织数字资产安全为出发点，聚焦在攻击者视角去审视网络空间内不同形态种类的资产所组成的攻击暴露面，同时特别强调“可观测性”、“可运营”，这意味着资产的全面性可度量、风险可度量、响应处置可度量。

2 金融行业攻击面管理需求现状分析

在调研访谈中，我们与多位金融行业安全团队负责人进行了沟通，梳理出金融行业攻击面管理需求现状的以下八大特点：

2.1 安全强合规，但缺少可落地的指导细则

《网络安全法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施保护条例》等“三法一条例”中都对“金融”行业有明确的安全合规要求，银保监会、证监会等行业监管机构出具了多项行业规定及要求，对行业机构提出更为具体的安全要求。不仅如此，《证券公司分类监管规定》（俗称证券机构分类评级）中，更是将“网络安全”列入“重大负面事项”，上升到“一票否决”的高度。因此相比其他行业，金融行业在强合规驱动下有较高的安全投入。

本次调研发现，在行业合规要求中专门针对网络安全资产管理、攻击面管理的相关指导细则并不多，这就导致整个金融行业的攻击面管理现状水平参差不齐且差距很大。

对于安全预算较少的用户，安全团队倾向于优先满足有明确条文的合规要求，间接降低了攻击面管理的建设优先级，因此很多机构仍然以 excel 表格作为资产台账的管理手段；对于为数不多的安全预算较为充足的用户，专门为攻击面管理设立了专项预算；剩余大部分安全团队为满足这方面需求，往往需要参考年度整体安全规划，结合其它安全需求，将攻击面管理的建设一并落地。

2.2 金融机构安全团队往往面临多个监管方的扫描与通报

金融机构行业主体往往受到多个行业监管单位的交叉辖制。除了网信办、工信部、公安部等网络安全监管机构外，银保监会、证监会等金融行业监管机

构也会对下辖行业机构进行攻击暴露面的扫描与通报。除此以外，个别央国企下属的银行，还会同时面临国资委的安全监管要求。

多个监管方的合规要求不尽相同，监管手段也有差异，有的是从合规角度，以行政手段提出要求，有的是从攻击者角度以技术手段进行扫描通报。在这样的监管态势下，各金融行业机构的安全团队，随时会有被多家监管单位通报的几率，因此就需要先行自发进行攻击暴露面的梳理排查与收敛。一旦被通报，也需要及时做出响应，形成整改说明材料进行上报。

2.3 攻击面管理的建设与运营，仍然需要事件驱动和推动

虽然攻击面管理在金融行业中已经得到了大范围的普及和接受，但具体到安全建设与安全运营中，仍然需要借助各级实网攻防演练或是偶然发生的安全事件的“帮助”。

一方面，安全团队在上一年底做预算时，撰写采购方案时，这些事件都是“借力”的重点，另一方面，安全团队在资产摸排、漏洞修复、安全整改等攻击面的收敛环节，也需要“借力”这些安全事件，将一些遗留问题加以集中解决。目前在缺少指导细则的合规背景下，仍有不少分管安全的领导对安全并不了解，重视程度也不够，所以这一需求现状还会持续相当长一段时间。

2.4 业务变化快，更注重资产生命周期的多标签动态管理

金融行业始终走在业务创新的前沿，业务创新带动信息基础设施环境的变化，金融机构的资产数量、资产属性、资产状态等攻击暴露面始终处在动态多变之中，因此金融行业的攻击面管理解决方案不能简单被动“拴”在 CMDB 的人工维护上，而是要将有限的人力资源投入到资产的分类分级和多标签管理等动态管理工作中，好钢用在刀刃上。

具体来说，在资产的生命周期中，安全运营团队可根据资产的业务相关属性、合规审计要求、潜在威胁风险等，对资产进行多维度的识别判断、多标签

的动态管理。例如，一个开源组件可能涉及到多个工程项目、系统应用、业务服务器等，安全运营团队应当在该组件评审通过允许上线时起，就将其纳入资产管理平台，然后分别从威胁狩猎的角度、从攻击向量的角度，通过多标签和知识图谱工具，对其资产状态持续完善持续更新，实现资产从上线到下线全生命周期的动态管理。

2.5 业务属性差异大，要完全实现“同业参考”是一个伪命题

在调研中我们发现，即便金融业务和规模都很相近的两家机构，攻击暴露面存在如：组织架构、IT 架构、业务层级等多种不同的业务属性，而这些业务属性又是“收敛”的重要依据，必须梳理清楚。业务部门的参与度决定了属性梳理工作的效率、完整性与准确性，这就导致两家机构各自梳理后的资产业务属性差异很大。

此外，“家丑不可外扬”和同业竞争关系等技术之外的壁垒，也让同业参考很难大范围公开推行，只在关系较近的个人或小群体间沟通。这就导致目前金融行业内不同机构间的攻击面管理水平参差不齐，差距很大，加之合规方面“缺少落地指导细则”的现状短时间内亦很难有所改变，金融机构仍然需要利用实战攻防演练等运动式场景，通过“平台 + 服务”的方式，提升攻击面管理的相关能力。

因此，攻击面管理的业务属性很难参考复制，甚至可以说，要想完全实现攻击面管理的“同业参考”是一个伪命题。

2.6 响应时效要求高，需要兼顾可观测性与安全有效性

相比其他行业，金融行业要求更高的业务连续性、数据完整性、安全保密性，因此在发现潜在的攻击暴露面后，其收敛的应急响应时效要求也更高。这就要求金融行业攻击面管理解决方案要具备较高的可观测性。

可观测性是指在攻击暴露面信息丰富、准确的基础上，安全运营团队通过

可视、可查、可控、可度量的攻击面管理平台，对内外网资产进行类似“上帝视角”的实时观测与管理，当发现攻击暴露面时，第一时间可以收敛响应。

当然，这只是一个理想状态，现实安全运营中，不可能百分百实现。漏报、误报等准确性问题都会对安全运营工作带来阻力。因此，团队还需要对现有安全建设的整体有效性进行持续验证。安全有效性验证能力越强，攻击暴露面的可观测性就越强。再者，通过提高可观测性，也能够帮助审视现有安全能力体系中的有效性问题。两者是正相关的关系。可观测性是过程，安全有效性是结果。两者兼顾，找到两者的平衡点，攻击面收敛的响应时效就会持续提高。

2.7 攻击面收敛难，需要专业技术与服务意识相结合

访谈中我们发现，处在不同安全建设阶段的各类金融机构安全团队，手里多少都具备一定的攻击面管理工具或平台产品。但在漏洞修复等收敛环节，经常会遇到研发部门不配合、个别领导不重视等现实问题。针对这一情况，安全团队除了要具备适用于本机构的技术工具，还需要在与其他部门沟通过程中具备主动服务的意识，两者结合，才有可能做好攻击面管理。

如何结合呢？还以漏洞修复为例。安全团队日常会通过攻击面管理产品从攻击者视角做持续的的资产摸排，当某个漏洞事件爆发时，安全团队第一时间将潜在收到漏洞威胁的资产列表筛选出来后，直接连同漏洞影响和修复建议，指定给相关的资产负责人。如此一来一方面省去了其他部门同事突击资产排查的工作量，另一方面，安全团队基于攻击者视角给出的漏洞影响和修复建议，降低了相关领导和其他非安全部门同事对此类安全事件的理解门槛。

调研中我们看到，在这方面做的较好的安全团队，其统一的攻击面视图甚至成为了网络部门、运维部门甚至业务部门经常会来“求助”的重要资产台账。如此通过专业技术与服务意识的结合，既能提升攻击面收敛的时效，还能体现出安全团队的工作价值。

2.8 共同成长，金融机构与安全厂商形成攻击面管理的共生互助关系

在调研中我们还看到一种值得欣慰的现状，多个金融机构的攻击面管理经过几年的建设后，与攻击面管理安全企业形成了共同成长的局面。一方面用户的新需求，通过安全企业的人工服务得到解决和验证，之后这些新需求转化为安全企业产品中的新功能；另一方面不断升级迭代的安全产品和服务又帮助用户覆盖着越来越多的资产维度和攻击面，提升攻击面管理的水平与时效。总体来看，双方不断磨合，一起提升着攻击面管理的自动化、可视化、智能化程度。这一需求现状，主要取决于攻击面管理与用户业务的强关联性。少了任何一方，攻击暴露面的梳理排查和收敛，都难以顺畅的落地，因此双方才会形成攻击面管理的共生互助关系，后续随着合规要求的进一步细化与技术发展，这一需求现状还会持续下去。

3 行业用户场景

经调研，金融行业用户在采用攻击面管理解决方案时，有分支机构资产纳管、实网攻防演练、数据泄露溯源取证、安全运营基础设施、后疫情时代攻击面管理等五个典型场景。

3.1 分支机构资产纳管

金融行业监管机构对辖区内所有单位组成的攻击暴露面开展管理工作，就是第一个典型场景——分支机构资产纳管。

金融行业监管机构明确要求分支机构上报关键信息基础设施资产，然而分支机构上报的资产信息普遍存在漏报、错报或信息滞后的情况，因此，如银保监会、证监会以及各金融业务机构的集团总部通过攻击面管理解决方案将分支机构的潜在攻击暴露面资产纳入管辖范围。

具体到不同的使用主体：监管机构对下辖被监管各单位上报的资产进行核查、补充，以满足后续的合规评级、安全通报、应急响应等需求；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，掌握集团整体攻击暴露面情况；当然，分支机构也可以自行采购或建设攻击面管理解决方案进行自查，然后将收敛后的资产信息上报给监管或集团总部，从而掌握主动权。

3.2 实网攻防演练

近年来，随着国家级、地市级、行业级实网攻防演练活动逐步趋于常态化，作为重点关键基础设施行业之一的金融行业，需要在各级攻防演练活动开始前对自身潜在的攻击暴露面进行提前发现和收敛。

常见的可能被攻击者利用的暴露在互联网上的新型数字资产有 GitHub、

网盘文库、公众号小程序等；此外可以帮助防守方发现软件供应链、合作伙伴等更深层次的攻击暴露面，例如开源组件、合作商 API 接口等。

演练开始后，高危漏洞事件集中式爆发，攻击面管理解决方案可在情报披露时对业务影响范围和暴露面进行预判，提前做好防护加固措施；当利用细节公开时，对外部攻击面进行全面摸排，协助防守方第一时间做出收敛响应，及快速定位、处置失陷资产。

3.3 数据泄露溯源取证

由于行业特殊性，金融行业用户数据往往是网络犯罪者优先关注的对象。在日常安全运营中，若不幸发生了数据泄露，金融机构可以通过攻击面管理解决方案从泄露数据（例如暗网、黑市中的样本数据）向上溯源，还原攻击链，进而找到最早的攻击入口。

一方面将相关设备、资产乃至人员信息作为举证材料纳入证据链，为下一步诉诸法律提供依据；另一方面，对其他同类资产进行横向排查，避免遗漏尚未检出的同类攻击行为，确保泄露途径已排查完整。最后，将所有符合此类攻击链特征的攻击暴露面统一进行收敛，避免再发生同类数据泄露事件。

3.4 安全运营基础设施

相比其他行业，金融行业具备更高的安全投入和安全建设水平，建有数量更多、成熟度更高的安全运营平台或安全运营中心。自动化、接口化、可视化的攻击暴露面发现与管理能力，是安全运营最重要的基础设施。

安全运营建设初期，自动化的攻击面管理能力是安全运营的基础能力之一，同时全面准确的攻击暴露面也是其他各项安全投入的依据；安全运营建设过程中，接口化的攻击面管理平台能够成为 SOC、SIEM 等平台的底座；安全运营能力形成后的安全有效性验证阶段，攻击面管理更是必不可少的基础设施，安全团队对设备、工具、人员、以及管理流程等内容进行安全有效性验证和量化评

估时，都需要用到可视化的攻击面管理能力。

3.5 后疫情时代的攻击面管理

新冠疫情给全球经济和金融行业带来的影响是显著的，为了支撑远程办公，金融互联网攻击面不断增加，更多的业务系统需要对互联网开放，无论是通过端口映射将业务系统直接开放公网访问，还是使用 VPN 打通远程网络通道，都是在原本脆弱的网络防护边界增加更多暴露面。接入网络的人员、设备、系统、应用的多样性呈指数型增加，企业的业务数据在复杂的人员、设备、系统、应用间频繁流动，数据流动的复杂性、数据泄露和滥用的风险均大幅增加。

因此，后疫情时代的攻击面管理及收敛能力，关注的重点就不再仅仅是传统中心化的 IT 资产，而是扩大到更大范围更多维度的数字资产。满足的是数字资产无处不在，攻击暴露面无处不在的安全需求。

4 关键能力

针对金融行业的关基属性、科技属性、安全属性等行业特点，数世咨询认为，其攻击面管理关键能力主要包括攻击暴露面发现、攻击面数据融合、攻击面管理平台、攻击面专项收敛等四大能力。

4.1 攻击暴露面发现能力

如前文定义部分所述，攻击暴露面的发现要以攻击者视角为主，涵盖网络资产、外部信息、脆弱性风险等维度，下面针对这三个维度分别阐述其能力要点。

对于潜在攻击者来说，“信息收集”是发起攻击前必做的功课，而且从时间角度来看，占据了攻击者大部分的时间精力。因此，对安全团队而言，除了直接管控范围内的网络资产,外部信息是另一个需要重点要关注的攻击暴露面。为便于阐述，本报告将金融行业用户的外部攻击暴露面以外部信息、网络资产、脆弱性风险评估等维度进行分类，并分别讨论其关键能力点。

4.1.1 外部信息攻击面覆盖

机构信息收集（如行政架构、品牌、邮箱、网盘、文档文库等）

潜在攻击者首先会搜集用户的机构信息，搜集维度包括但不限于总部及分支机构名称、品牌、安全管理制度、业务运行时间、集团行政架构、各分支机构间的关系等等；针对高权限的 IT 管理人员，重点搜集姓名、邮箱、手机号、VPN 账户、昵称、社会关系等等；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，安全团队可以通过外部攻击面发现平台，对此类信息做持续周期性的发现。先于攻击者发现此类资产，为响应收敛争取时间。

源代码监测（如 Github、码云等）

代码共享平台存在隐匿的攻击暴露面，例如管理后台 URL、VPN 账户密码等，开发运维人员因缺乏安全意识，无意中将此类敏感信息上传至 GitHub、Gitee 等代码共享平台，为信息安全事故埋下导火索。攻击者主要是以用户机构的业务关键字、品牌名称、公司名称、IT 人员的个人 GitHub 账户等渠道搜集这类信息，因此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。

外部接口（如 API、公众号、小程序接口等）

除了代码平台，还有一类常被忽视的攻击暴露面是外部接口，如与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，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。同代码平台监测一样，安全团队应当以“技术 + 管理”相结合的方式，对此进行持续发现、收敛。

暗网监测（社工库、泄漏数据）

金融行业用户数据与“钱”直接强相关，具有非常高的“黑灰产价值”，因此在黑市（特别是暗网中的黑市）十分抢手。攻击者针对金融行业机构的网络攻击其目的也往往正是这些高价值的用户数据。因此，针对暗网实行持续的社工库、泄露数据等监测，能够为用户机构的攻击暴露面监测提供非常有价值的参考。例如，对暗网交易市场中的样例数据进行抽样比对，除了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（例如用户数据分属于某个支行网点），更能帮助安全团队进而梳理出攻击暴露面中的薄弱环节。

4.1.2 网络资产攻击面覆盖

主动扫描探测

对于存在总部和分支机构的场景，特别是营业网点众多的银行、证券等用户，主动扫描测绘是部署成本相对较低、效果明显的管理工具与手段，可以获取绝大部分在互联网侧对外提供服务的资产信息，维度主要包括：IP 地址、DNS、域名、URL、端口服务、Web 应用等。在实网攻防演练等场景中，可以帮助集团安全团队发现分支机构私自上线的网络资产。

值得一提的是，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

在用户机构的出入口网关、内部核心路由等关键部位，旁路部署流量分析设备，实现被动的资产发现需求。

被动流量发现的资产指纹信息相比主动扫描探测，可发现资产的种类数量相对少一些，但指纹匹配的准确度相对更高。即便对于加密流量而言，仍然可以通过资产指纹加密流量建模等方式，做到部分资产的准确发现。

此外，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；此外还可以发现主动扫描测绘不易发现的台账外资产，例如主动扫描节点触达不到的内网资产、相对偶发的测试资产等。

云资产发现

金融行业科技属性加持下，业务的云化始终走在前列，但云的敏捷、灵活反而成为攻击面管理中的难题：弹性公网 IP 临时分配必然会引发“资产漂移”的现象，应用动态水平扩展会导致暴露面无法采用静态评估的方式有效完成，多云异构也进一步考验攻击面管理平台的兼容能力。

因此，云资产的发现，可以通过对接云管平台 API，对虚拟化实例、域名解析记录、弹性公网 IP、负载均衡、WAF 防护目标等实例对象进行高频同步，实现跨供应商的云端资产纳管，从云端视角提高攻击暴露面的可见性。

影子资产发现

大部分安全隐患与风险来自于未知，Shadow IT（影子资产），一般是指在 IT 组织所有权之外的 IT 设备、系统和应用。它是相对于上述“主动扫描探测”、“被动流量发现”、“云资产发现”之外的资产来说的。例如分子机构私自上线的接口或站点、“碰瓷”式的合作伙伴站点、钓鱼网站等仿冒站点，都属于这类资产。

因此，对于影子资产，攻击面管理的解决方案，将在上述三种资产覆盖的基础上，通过“资产线索”（关键字线索、logo 图形线索）持续检索整个互联网空间或第三方数据仓库，逐一比对现在有的台账记录，从而发现台账中未被记录的疑似资产数据，实现对 Shadow IT（影子资产）的持续发现。用户进行内部核查，研判后，最后再行决定是纳管或是沟通、举报、甚至诉诸法律等其他手段将其下线。

4.1.3 脆弱性风险评估

弱口令

弱口令 (weak password) 没有严格和准确的定义，通常认为容易被别人猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等。

近年来，账户密码的不断泄露导致暗网的密码数据库不断增加，日益开放的网络环境降低了边界的可防御性，远程设备的迅速涌入使互联网络上的用户和终端身份的安全管理更加复杂。可以说 金融行业的弱口令攻击面仍然是在不断扩大的。因此，攻击面发现能力中，对攻击面脆弱性的评估，首先还是要

关注弱口令。

发现方式相对也并不复杂，在发现管理后台页面、口令认证接口等类型资产时，相关产品或工具能够进一步辅以口令字典进行测试即可。这里的字典要支持用户上传进行自定义，同时针对不同的资产发现场景和任务，修改不同级别的弱口令测试强度，不影响业务。

漏洞风险

以金融行业机构为目标的潜在攻击者，往往更加依赖于新爆出的 0day 或 1day 漏洞。这就决定了在新的漏洞威胁出现后，安全团队需要抢在攻击者之前，更快、更全、更准地定位潜在受漏洞威胁的风险资产。近几年无论是心脏滴血、永恒之蓝还是 Log4j2 等漏洞的大范围爆发，都让金融机构的安全团队度过一个又一个不眠之夜。

面对这样的情况，攻击面管理首先要做到在漏洞爆发之前，就对资产台账中的所有资产信息按照业务优先级进行标记，同时对所使用的系统、应用、中间件及资产的版本号等关键信息做到精细管理、持续更新。如此一来，在漏洞爆发时，才能第一时间做到资产快速筛选、PoC 快速分发、漏洞精准匹配、虚拟补丁临时修复等快速检测与响应，赶在攻击者行动之前完成风险收敛。

安全团队需要通过工单、OA 等流程系统将该漏洞信息推送至业务及 IT 运维等部门，之后定期或不定期对包含漏洞风险的资产进行精准复测。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。

软件供应链风险

经过近几年的攻防对抗演练，行业单位安全运营能力普遍得到提升，常规的攻击路径得到有效的暴露与封堵。攻击者开始转换思路，将目光瞄准了上游——供应链。例如金融机构所使用的办公软件、有合作的软件应用开发商、

可能用到的开源代码，甚至是金融行业经常使用的安全产品等等。

对此，攻击面管理解决方案可通过持续应用安全（CAS）等“安全左移”的方式，将上游的攻击暴露面也纳入收敛范围。

持续应用安全（CAS）是基于我国软件供应链安全现状所诞生的一种理念，主要解决软件供应链中数字化应用的开发以及运行方面的安全问题，覆盖应用的源代码开发、构建部署、上线运行等多个阶段，保障数字化应用的全流程安全状态，是安全能力原子化（离散式制造、集中式交付、统一式管理、智能式应用）在软件供应链安全上的应用。因此在应用的开发阶段，攻击面管理能够与 CAS 形成资产数据的关联和融合，并经由统一调度管理形成体系化的解决方案，以达到帮助用户整合资产数据、提升攻击面管理效率的目的。

4.2 攻击面数据融合能力

4.2.1 多源资产数据接入

从 2019 年的 RSAC 创新沙盒冠军 Axonius，到今年（2022 年）的 RSAC 创新沙盒十强 Sevco Security，这两家都是从事网络资产管理的优秀创新企业，他们有一个共同点——对接多源资产数据并进行交叉比对融合。由此可见，无论用户的单独一个部门亦或是单独某一家供应商，不可能覆盖所有资产，因此，攻击面管理解决方案一定要具备的能力是“多源资产数据接入”能力。

对接的多源资产数据，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。这里要注意的是，由于金融行业产品迭代速度较快、金融科技创新程度较高等特点，多源资产数据对接的接口应当避免项目定制化，而是尽量采用标准化产品接口实现。接口应当是通用且可扩展的，当需要对接新的资产数据来源时，其接口仍然能够支持。

要做到这一点并不容易，需要攻击面管理供应商在金融行业有多年积累，

既熟悉金融业务特点，又熟悉金融 IT 环境、软件应用供应商，才可能在产品或解决方案的后端始终做好资产对接接口的适配，跟上用户的需求迭代速度。

4.2.2 数据融合与分析

多源资产数据接入汇总后，并非简单的叠加，而是要进行持续的交叉验证、去重 / 扩充、属性补全、标记等操作。

举一个较常见的例子，同一台边界设备资产，同时具备内外网两套资产属性，有可能这台设备在业务部门（内网）和安全团队（外网）各自的资产台账中，看起来是完全不相关的两个资产。

类似这种情况，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。回到例子中，攻击面管理产品或解决方案，要能够描绘出从域名 / 公网 IP 到内网主机，再从内网主机到内网 IP/ 域名的资产关系链。如此将原本不同部门的资产台账融合为统一的资产视图，在面对新爆发漏洞或攻击溯源时，可以对该资产进行一体响应，避免习惯上的“先外网后内网”导致的潜在风险。

4.3 攻击面管理平台能力

经过网络资产发现、外部信息搜集、多源资产对接后的各类资产数据，最终统一聚合到攻击面管理平台。管理平台应当至少具备以下三个能力：一是信息完善与关联，二是可观测性管理、三是数据输出。

4.3.1 基于业务视角的资产属性

无论是监管机构还是金融机构自身，都需要掌握资产的全局数据，以满足“强监管、强合规”的需求。因此，管理平台应当支持用户以行政管理视角，对资产所属的分支机构和部门进行分配与登记；同时还要根据业务架构，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，最终体现出资

产的业务价值等级、业务连续性要求等等重要属性。

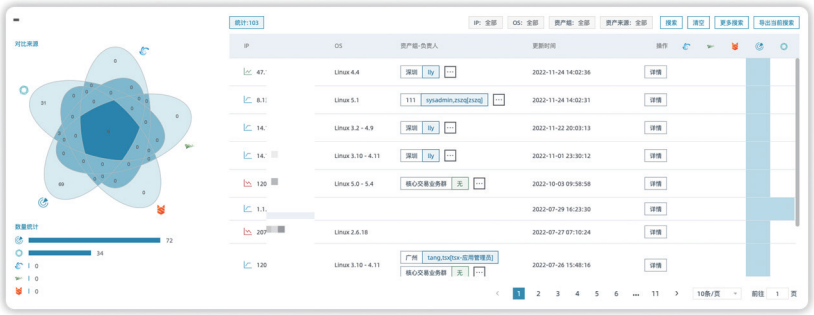
对安全团队来说，管理平台还应当具备一定程度智能化的“标签”能力。所谓智能化，是指管理平台支持以业务、部门、IP 范围等维度，给资产批量化自动化打标签，目的是减少平台自身的数据维护工作量，提高安全运营效率。

4.3.2 可观测性

攻击面管理平台的“可观测性”是指经过海量数据聚合后，根据专业经验对数据进行消化解析，多维分析呈现的一种洞察能力。当攻击者在突破边界时，执行突破的动作可被观测；攻击者开始横向移动时，活动范围、细节过程可被观测；攻击者获得靶标后，整个行动过程和细节可被重放，所有攻击向量和路径均可被观测。

若让攻击面具备“可观测性”，前提是需要先解决资产和风险的“可见性”。通过 4.1 ～ 4.2 章节描述的发现与融合能力，已经为“可见性”奠定基础。不同资产来源，通过比对数据集，客观描述不同安全工具下，自身对暴露面的覆盖范围。CMDB、主动扫描测绘、HIDS 等单一技术手段，只能获得到部分暴露面视野，并不能代表真实、客观的攻击暴露面。只有多者结合，才能更好的获得更佳的“可见性”。

在差集数据中，检索“CMDB 尚未覆盖的无主资产”、“DMZ 中未部署 HIDS 探针的脱管资产”、“下线未下架的僵尸资产”，“主动测绘发现的影子资产”等等。以上罗列的场景，便是安全管理覆盖面的间隙，在求证暴露面可见性时，体现的“可观测性”。



图例 4：资产可见性示意简图（本图例由魔方安全网络资产安全管理平台提供）

此外，结合业务权重、告警可信度、漏洞优先级等维度，对整体视图进行呈现，方便安全团队负责人在把握整体资产安全态势的同时，迅速发现攻击暴露面中需要优先收敛的部分。

可视化资产信息在持续完善关联的过程中，数据复杂度也在增加。目前业内通行的做法是以知识图谱的方式进行可视化呈现。每个图谱节点即是一个资产单元，每个资产单元可以以颜色深浅、节点大小等可视化方式进行区分，表明该资产的不同属性与状态。可视化视图应当支持属性筛选、无限下钻等功能，以满足风险资产快速定位、攻击路径溯源等场景。

这里值得一提的是，对于少部分无需二次确认即可收敛的资产，管理平台可通过“一件下线”功能直接将其收敛，对于大部分需要内、外部相关部门二次确认的资产，应当提供接口与工单系统对接。后面的专项收敛能力部分还会有详细阐述。

最后，对上述所有资产数据以及工单中的修复时长、跟进复测次数等，还应当具备量化统计功能，以实现对攻击面收敛的可度量能力。

4.3.3 资产数据输出

经过交叉融合、信息完善、聚类关联后的资产数据，能够对外输出提供数据支持。

首先，完备精准的资产数据，可以用于安全团队上报给上级监管部门，满足资产报备等合规要求。在告警通报、实网攻防演练等场景中，还可以用于快速定位风险资产，为撰写相关报告提供有力的资产数据支持，使安全团队避免被动，掌握主动权，始终做到心中有数。

其次，经过与资产关联确认后的外部威胁信息，可以对接给漏洞管理平台、HIDS 等，提升现有安全设备的价值，甚至输出给 WAF、EDR 等安全产品，形成实时的阻断响应能力。经过与资产关联确认后的漏洞信息，还可以对接工单系统，推送至业务、网络、运维等兄弟部门，督促相关负责人定期修复，通过后期不定期的漏洞复测，进而形成漏洞管理的闭环。

最后，资产数据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。

4.4 攻击面专项收敛能力

关于攻击暴露面的“收敛”，本次调研访谈的金融行业用户中，大部分安全负责人都反馈，需要与风险资产相关的部门同事、风险应用相关的软件开发供应商等进行大量的沟通、协调、研判、持续跟进等等安全技术之外的工作，这表明，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。

4.4.1 互联网风险资产快速定位与下线

在实网攻防演练和日常安全运营中，最常见的“收敛”场景是为应对 1day 漏洞而进行的风险资产快速定位与下线。此专项收敛需要具备漏洞预警、攻击面管理平台两个基本能力。

漏洞预警是便于用户第一时间掌握 0.5day 或 1day 的漏洞关键信息。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对暗网中的漏洞交易平台进行监测。在第一时间收到漏洞预警后，用户重点

关注漏洞描述中受漏洞影响的系统、应用、版本号、影响范围等关键信息。

接下来在攻击面管理平台中，使用这些关键信息筛选定位出所有潜在威胁的风险资产，然后根据资产的业务优先级、所属部门，下发不同的响应策略。在不影响业务连续性的前提下，确定漏洞修复方案前，也可通过工单系统，协调业务、运维等部门，对部分资产做临时下线处理。最后一小部分受业务连续性要求，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。

4.4.2 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，收敛方式最为简单，直接从机构内部关闭相关 API 接口即可；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。

4.4.3 办公网资产整体收敛

采用零信任“单包敲门”的方式，用户也可以实现攻击暴露面收敛。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。

这一方法有效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。在调研中，有证券行业用户就是采用的这种方式。当然，这一方法也有其局限性，例如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。

4.5 能力建设建议：阶梯式建设

以上各项能力，并不要求一蹴而就一步完成，建议有能力的用户分阶段完成：

第一阶段目标是解决“可见性”这一行业痛点，即基于攻击者视角进行内外网的攻击暴露面排查，达到“有效观测”这一阶段性目标，因为“你无法保护你看不见的东西”。

第二阶段洞察安全管理策略覆盖度。进行根据资产的来源标签挖掘安全策略间隙，如DMZ的HIDS覆盖情况，深化资产的管理颗粒度（组件、容器、API等），多维资产数据梳理与关联。

第三阶段聚焦有效管控、指标化运营。针对各类资产安全场景进行补强，制定度量指标结合内部流程，管对治好。

第四阶段强调联动，融入机构内部生态。与CMDB+OA配合，实现全生命周期的安全管理，对上线下线的资产进行有效管控。

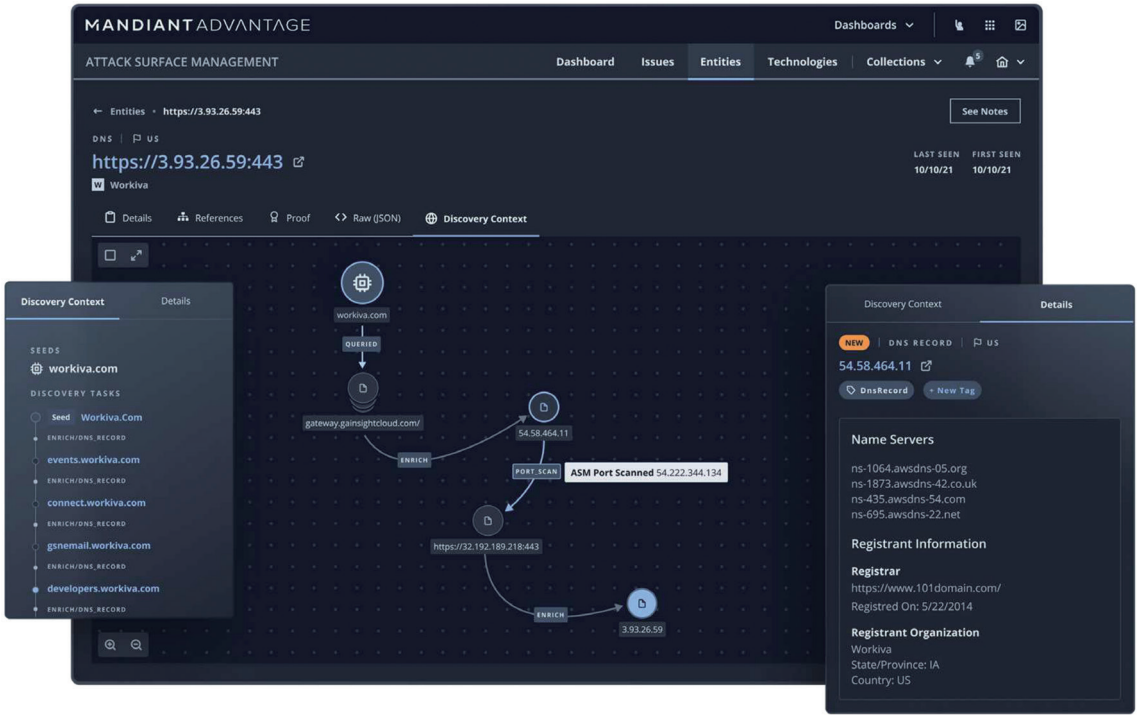
最后阶段增强“可观测性”。在对资产安全治理与运营的基础上，“从实战中来，往实战中去”，通过网络仿真、知识图谱与攻击预测算法，实现攻击面的可视化管理，完成“平战一体化”的理念升维，以支撑各类常态化的攻防演练活动。

5 代表企业

5.1 MANDIANT

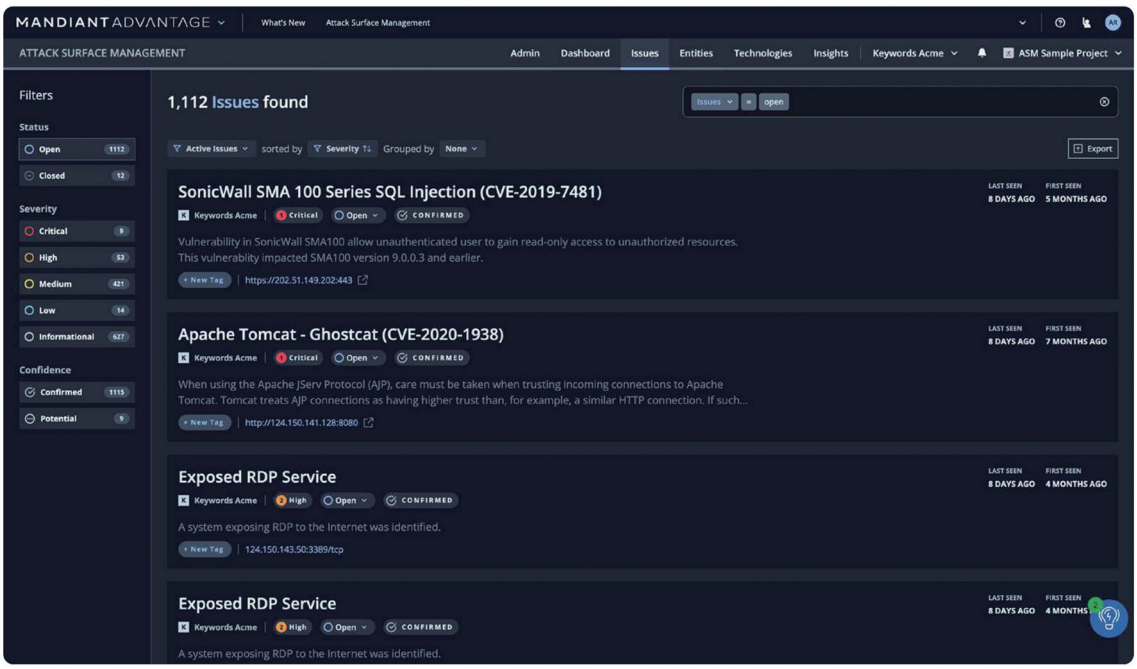
作为老牌网络安全企业之一，Mandiant 积累了多年的安全运营与威胁事件分析能力。Google Cloud 收购 Mandiant 后，为其带来了强大的数据处理、人工智能等新的能力支持。加之原本就优秀的威胁情报数据收集能力，Mandiant 将威胁监测、事件分析、安全验证、自动化防御、攻击面管理等多个能力集成在归一化 XDR 平台“Mandiant Advantage”上，用户可以获得更加闭环高效的使用效果。

其中的攻击面管理 ASM 兼具资产全面、信息深度、情报关联等特点。例如其全面、深度的资产信息详情，除了具备深度且直观的可视化页面，还包含了资产设备对应的软件应用、配置信息以及其他多种属性。如此一来，安全运营人员在对资产进行识别、分类、打标签等操作时，准确度和效率都更高。



在 Mandiant 的优势能力威胁情报方面，支持从实时更新的威胁情报

（Issues）中一键筛选关联至潜在受影响的资产，呈现时也是按照攻击威胁的严重级别进行优先排序展示的，这在安全人员第一时间需要进行攻击面收敛或事件响应时，非常高效。

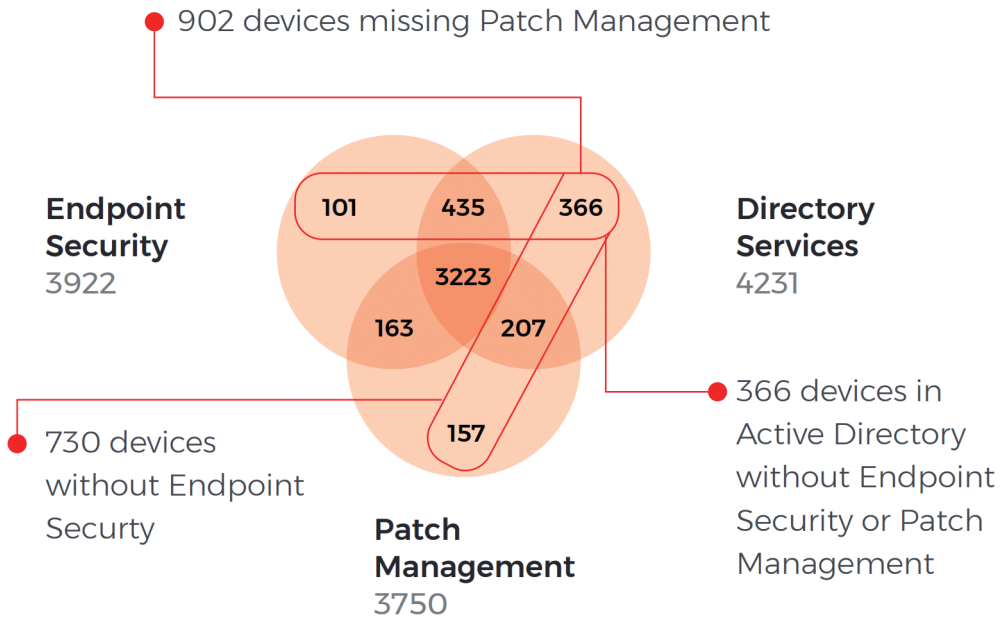


总的来说，Mandiant 的攻击面管理，依靠资产信息的深度、威胁情报的关联以及归一化平台的快速响应闭环，充分体现出了一家老牌安全公司的综合安全能力。

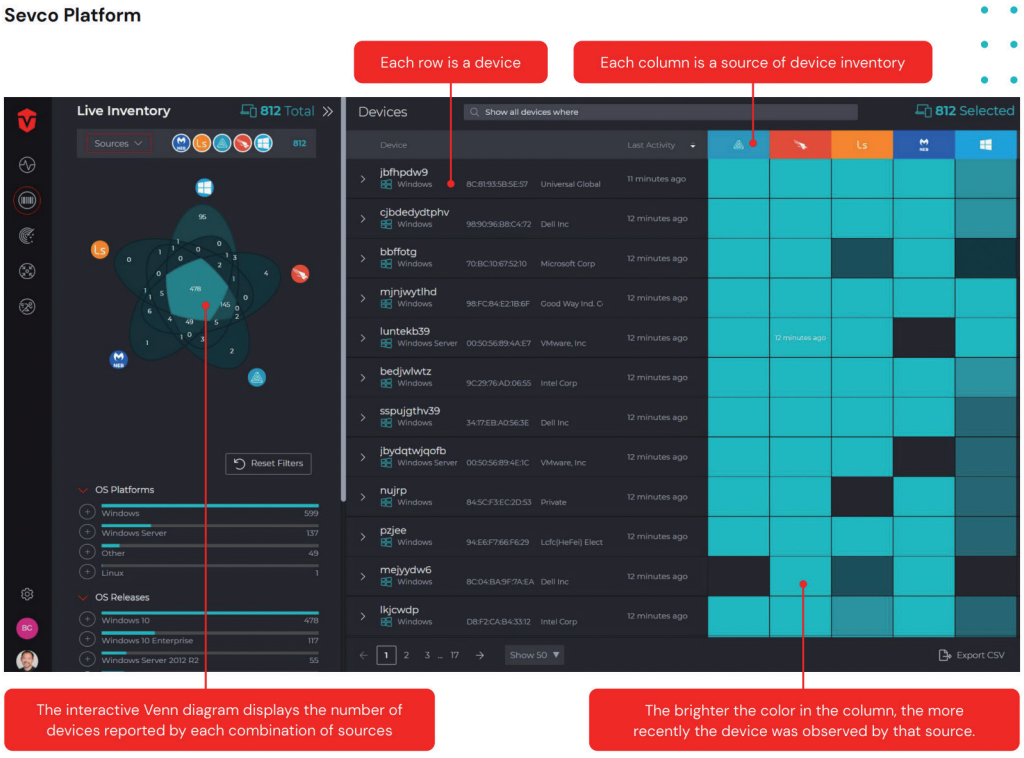
5.2 SEVCO SECURITY

Sevco Security（以下简称 Sevco）成立于 2020 年，总部位于美国。核心产品 Sevco 资产管理平台，可通过集成现有资产管理平台的资产清单，将多源资产管理软件的数据融合，建立更全面的资产库，以识别企业网络中的风险资产，进而实时跟踪资产库中的资产状态变化情况。

Sevco 可通过资产的交叉查询，检索到企业内的安全防护盲点。（如上图示意图所示）不仅方便资产管理员进行查漏补缺，而且这些资产安全团队需要优先关注的对象，可以有效的收敛企业的攻击暴露面。



此外，Sevco 还会动态地对机构资产的属性变化进行监控，通过对每个报告的资产状态与之前报告的状态进行比较，实时标记资产变化情况，检测资产的变化主要包括两方面：资产库存变更和资产属性变更。资产库存变更包括：新增或删除资产、历史过时资产的监控；资产属性变更包括：IP、主机名、MAC 地址的监控。



Sevco 可以在资产管理页面查看资产的状态，通过对多方数据源的聚合分

析，最后给出资产的最近活跃状态。此外，Sevco 可以通过不同源提供的资产快照，分析资产的安全属性，比如最近一次打补丁的时间、是否安装 EDR 等信息；通过 UI 上展示的颜色深度表示上一次活跃的时间，颜色越深时间越久。

还有其他功能上的创新点，本报告就不一一列举了，文末的参考资料中有相关链接，读者可自行查阅。总之，继 2019 年 Axonius 夺冠之后，再次有安全资产管理（攻击面管理）企业入选 RSAC 创新沙盒的十强，说明这个领域无论是在用户需求侧、厂商供给侧，还是在投资机构眼中，都是一个持续受到关注的热点领域。

5.3 魔方安全

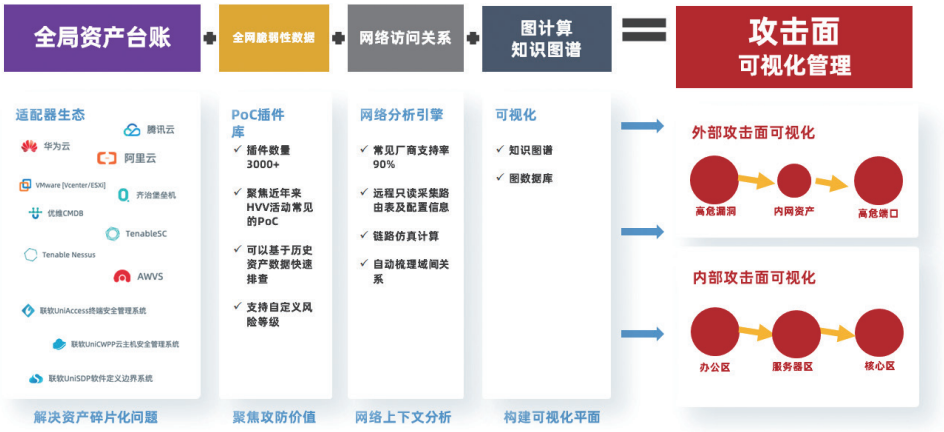
深圳市魔方安全科技有限公司（简称魔方安全）由 CubeSec 网络安全攻防团队于 2015 年 10 月创立，专注于网络空间资产安全相关的技术研究和产品研发，包括：攻击面管理（ASM）、网络空间资产测绘（CAM）、漏洞管理（VM）、安全攻防服务等。

魔方安全于 2015 年成立当年就推出了攻击者视角的“外部攻击面管理平台”并以 SaaS 化形态服务于金融、运营商、交通、教育等行业用户及大型企业。2020 年，魔方安全提出“资产测绘为起点、脆弱性管理为落脚点，安全运营为目标”的资产安全管理三阶论，并发布《资产安全管理解决方案》和“数字资产风险监控 SaaS 服务”，结合安全服务，为政企单位客户提供内外网资产安全与漏洞运营整体解决方案。

据调研，魔方安全的外部攻击面管理 EASM、攻击面可视化管理解决方案 (VASM) 符合本报告中对攻击面管理关键能力的主要描述，具备数字资产可视

化、资产脆弱性关联等特点。魔方采用的主动扫描探测 + 被动流量发现 + 资产适配器等技术，很大程度上还解决了 IP 化资产的探测覆盖率和完整性这一业内难题，同时，“SaaS 平台 + 安全代运营”的交付方式，是金融行业用户的场景优良实践。

进一步以“可视化”这一能力点来说，魔方会采集现网中所有三层网络设备的路由信息和 ACL 访问规则，通过网络仿真及智能计算、融合网络上下文信息、资产和脆弱性三要素，应用知识图谱及原生分布式图数据库，完成访问关系和攻击路径的可视化，进行自动化蔓延推理式的攻击路径演算，从而实现攻击面的可视化管理。



将用户从庞杂的表单数据中解脱出来，所见即为重点，可视化辅助决策，是安全运营的高阶形态。

再以 SaaS 平台 + 安全代运营的交付方式为例，这对金融行业客户来说——访谈中 90% 甲方表示人手不足——是解决安全资源有限的最佳实践。“平台产品 + 数据 + 甲乙方团队共同治理”或许是当前“攻击面管理”在中国市场落地生根，厂商与客户获得共赢最优雅的解法。

6 未来展望

6.1 攻击面管理作为行业共识，将成为安全运营必选项

在本次调研中，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。加之最近几次较为恶劣的数字资产泄露事件的驱动，攻击暴露面收敛已成为金融行业的普遍共识。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，攻击面管理将成为安全运营的必选项。

6.2 金融行业攻击面管理将向“大集中”靠拢

近几年由于业务发展需要以及新冠疫情带来的客观影响，很多金融机构的下属事业部、业务部都有强烈意愿自行开展新的线上业务，导致新申请域名、业务平台等数字资产“野蛮”发展，此类烟囱式的发展方式，既带来资源浪费，也带来越来越多的潜在攻击暴露面。因此，越来越多的金融机构已经开始采用“大 IT 模式”，将分支机构的业务及配套资产统一接口、统一上线、统一管理。虽然对业务的灵活程度会有一定影响，但集中到运维团队、安全团队手里后，攻击面管理的 ROI 可以得到显著提升。

6.3 攻击面管理方案的交付将以“平台 + 服务”结合为主要方式

目前行业内攻击面管理项目普遍以平台的产品形式进行交付，我们在调研过程中发现资源有限依旧是行业同性难题，访谈中 90% 甲方表示人手不足。“平台产品 + 数据 + 甲乙方团队共同治理”或许是当前“攻击面管理”在中国市场落地生根，厂商与客户获得共赢最优雅的解法。

未来一段时间，攻击面管理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，会逐渐固化到攻击面管理产品中，在用户与厂商的共同成长中，攻击面管理的成效也会越来越显著。

6.4 对攻击暴露面的实时可观测性准确度会越来越高

虽然缺少合规细则，人工服务也不可避免，但攻击面管理的实时可观测性、准确度会越来越高。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采集，这就为攻击面管理中“可观测性”的提供了更为有利的技术基础与数据基础，再辅以安全有效性验证的不断正向反馈，可见、可管、可控的准确度会越来越高。

参考资料：

https://www.mandiant.com/advantage/attack-surface-management

https://www.dwcon.cn/post/1633

https://www.cubesec.cn/

https://www.sevcosecurity.com/wp-content/uploads/2022/06/Sevco_TB-AssetCorrelationEngine.pdf

https://www.sevcosecurity.com/wp-content/uploads/2022/06/sevco_asset_intelligence_platform_datasheet_01.2.pdf

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