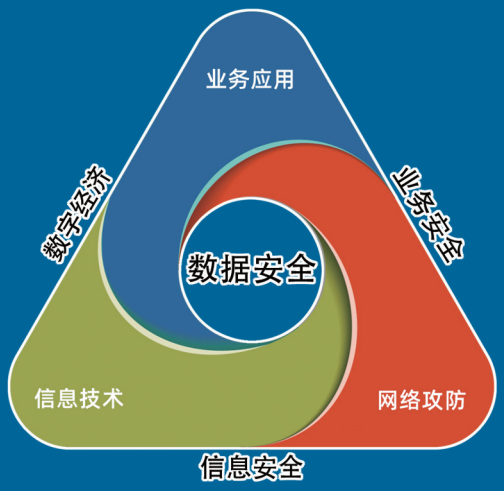
数世咨询
Digital World Consulting

精准 EDR 能力白皮书

数世咨询
Digital World Consulting

精准 EDR 能力白皮书



信息技术 + 业务应用 ➡ 数字经济

信息技术 + 网络攻防 ➡ 网络安全

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

经过近 30 年的攻防博弈，国内传统终端安全的需求从最初的防病毒、终端管理、安全审计等，逐步升级为端点防护平台 EPP、终端数据防泄漏等综合解决方案，随着近年来国际形势的变化、国内安全演练活动的举办、机构主管安全意识的普遍提升，端点侧的安全能力需求更加侧重对安全威胁的检测与响应。

由此，端点检测与响应（EDR）应需而生。然而，国内目前大部分 EDR 产品及解决方案都是基于传统 PC 防病毒或终端管理产品发展演化而来，核心能力并非原生满足检测与响应的需求。例如，防病毒引擎主要基于病毒特征检测威胁攻击行为，不具备实时威胁情报的支持，同时也缺少上下文关联分析的能力；终端管理产品则重在管理，虽然在应急响应场景中具备一定的批量处置能力，但是对威胁的检出率较弱，安全响应的效能化智能化水平也都无法满足安全团队的需求。

与此同时，国际上如 CrowdStrike 此类以威胁情报为基础具备云原生优势的安全企业已经经过了市场的验证，受到用户、投资人、同行的多方认可。国内有哪些新兴安全企业也具备这样的能力特点，各界莫衷一是。

基于上述现状,数世咨询认为在传统终端安全能力与检测响应新需求之间，始终缺少一个以行业调研为基础的 EDR 报告对其做出梳理与阐述。鉴于此，我们协同国内 EDR 领域安全厂商微步在线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《精准 EDR 能力白皮书》。

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

●精准 EDR 是指基于海量威胁情报与终端行为分析，以高级威胁攻击行为为应对目标，具备精准威胁发现、快速溯源分析、智能响应闭环的 EDR 解决方案。

●精准 EDR 重在精准，关键能力主要有攻击检测能力、数据采集能力、攻击溯源分析能力、安全响应能力等四个维度。

●要构建满足用户需求的检测准确度，目前在多种可选技术路线中以“上下文关联”最具落地实践效果。

●对威胁检测的覆盖主要包括基于特征的恶意软件、覆盖 ATT&CK 的 IoA、以及包含 APT 组织在内的高质量 IoC 情报等。

● agent 采集的数据需要在终端侧进行去重、重组、筛选、标签等操作，以最小化原则回传。

●精准 EDR 进行溯源分析的两个基础能力：底层事件的上下文关联、基于图的可视化。

●精准EDR的安全响应以一定程度的智能化溯源分析作为前置能力，以“单点隔离，阻断横移”为基本原则。

●未来 EDR 将向精准化、一体化、智能化等方向发展。

1 定义及描述

1.1 EDR

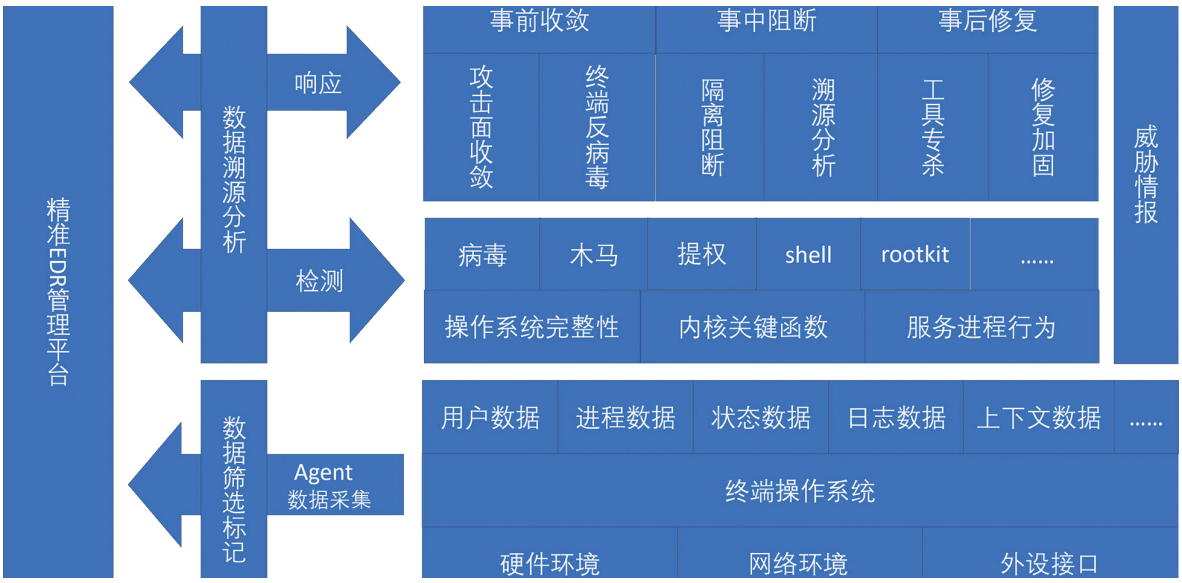
端点检测与防护（Endpoint Detection and Response，EDR）是一种采集、记录并存储数字空间中机构所拥有的各端点状态数据与行为数据，并对数据进行关联分析，以应对威胁的安全能力。具体包括，分析端点数据，检测发现威胁，进行隔离、查杀等安全响应；对正在发生或已发生的安全事件进行追踪溯源；针对潜在的风险（如二次攻击、未修复漏洞等），基于客户业务需求提供修复与保护建议；最终，实现整个数字环境中对未知威胁与高级可持续威胁的检测与响应。（注：本定义取自《数世咨询：EDR 能力指南 2021》，有修改）

端点的范畴：本报告中的“端点”若无特别说明，主要是指数字空间中某机构所拥有的办公电脑、个人移动终端、IoT 设备、网络设备、联网打印机、摄像头等终端设备。

需要强调的是，本报告的端点中不包含物理主机、虚拟机、容器等服务器设备，主机场景下的检测与响应，数世咨询单独以“主机检测与响应 HDR”进行了划分，详见《数世咨询：主机检测与响应 HDR 能力指南》（2022）。

1.2 精准 EDR

基于上述 EDR 定义，精准 EDR 是指基于海量威胁情报与终端行为分析，以高级威胁攻击行为为应对目标，具备精准威胁发现、快速溯源分析、智能响应闭环的 EDR 解决方案。



图例 1：精准 EDR 示意简图

1.3 与传统终端安全产品的区别

精准 EDR 与终端管理类产品相比（如终端管理、桌面管理）：

- √产品定位不同，终端管理产品为 IT 运维工程师提供管理上的便捷，而精准 EDR 关注的是黑客攻击行为，供安全管理员应对威胁使用；

- √安全能力不同，终端管理产品的安全能力较弱，一般具备弱口令扫描、漏洞扫描等基本安全能力，精准 EDR 要能够检测出高级威胁攻击行为；

- √然两者并不冲突，精准 EDR 主要角色为高级威胁检测与响应，并且其 agent 较为轻量，在终端侧的资源占用很小，再基于定位与能力上的不同，因此能够与用户原有终端管理产品并存发挥各自能力。

精准 EDR 与国内传统终端安全相比（主要以防病毒为主，包括传统的 EPP、AV 在内）：

- √应对目标不同，相对传统杀毒软件或病毒防护产品，精准 EDR 更关注端点侧的高级威胁攻击行为；

√基础架构不同，相对传统的本地化扫描引擎，精准 EDR 采用 SaaS 模式或者本地化大数据架构（SaaS 模式基于云具备更强的可扩展计算能力），状态数据行为数据的存储、溯源分析、策略分发等都在云端，且多为云原生架构，支持大规模可扩展，能够及时应对多场景下的不同需求；

√检测机制不同，相对基于特征的匹配机制，精准 EDR 基于海量威胁情报数据与多种行为方法，对威胁攻击行为的事件上下文进行关联分析，从而发现威胁；

√响应效果不同，相对传统的高级分析师判断后交由运维、网络等部门响应，精准 EDR 直接具备智能化的端点隔离、横向阻断、智能清理攻击者驻留项等闭环响应能力。

√当然新型的 EPP 中也会不断融入 EDR 能力，以国际为例目前已经出现了两种方向的厂商。一种是专业的 EDR 厂商扩展成为 EPP 厂商，以 Crowdstrike 为典型；另一种为传统 EPP 厂商通过研发或者并购整合 EDR 能力。

对比项	终端管理 桌面管理	传统终端安全 (含 EPP、AV)	精准 EDR
产品定位	IT 运维管理	以终端侧恶意软件防护为主	终端侧高级威胁检测与响应
使用人群	运维工程师	安全工程师	安全工程师
应对目标	员工终端行为	病毒/恶意软件	高级威胁攻击
基础架构	C/S、B/S 架构	C/S、B/S 架构	C/S、B/S 架构、云原生架构
关键功能	软件管控、外设管理、终端数据防泄漏、漏洞补丁管理	病毒扫描、文件实时防护、漏洞补丁管理	终端行为日志检索、威胁分析与溯源，威胁智能化处置
检测机制	基于字典或漏洞脆弱性扫描	基于恶意软件特征匹配	基于行为上下文、结合情报关联分析
响应手段	要求修改口令择期修复漏洞	查杀隔离文件，择期脆弱性修复	实时单点隔离、智能化清理驻留项并在全域横向同步阻断

图例 2：与传统终端安全产品的区别

2 EDR 需求现状分析

2.1 传统产品无法有效捕获企业终端面临的新威胁

如定义部分所述，防病毒、EPP 等传统终端安全产品基于已知特征库、通过传统签名技术实现对恶意文件的检测发现；面对未知特征恶意文件，虽逐步发展出了“云查杀”、“启发式检测”等功能，但面对内存马、无文件攻击等新型威胁时，传统安全产品已无法有效应对。

2.2 混合办公、多分支办公等场景下的统一终端安全视角缺失

新冠疫情客观上加速了业务上云、居家办公、远程协同等混合办公、多分支办公的场景，机构安全团队需要同时覆盖多类型、多属地的终端安全需求，然而在同时面对VPN、数据中心边界防护、Web 防护等多个烟囱式的安全界面时，很易出现疏漏。

与此同时，机构下辖的各分支机构安全建设投入先后有别，水平不一，人员少经验浅安全意识薄弱是普遍现象，攻击者一旦进入，横向移动内网扩散畅通无阻，因此往往成为实网攻防演练中攻击队最常突破的目标。面对这种情况，统一的终端安全视角成为最迫切需求之一。

2.3 EDR 缺乏全面有效的监控记录数据支持

要想具备统一的终端安全视角，需要对终端进行监控记录全覆盖。然而我们调研发现，目前行业内大部分 EDR 产品在端侧的数据采集能力都较弱。

“全量”记录终端上的所有数据并不能直接为检测或响应带来更高效助力，相反还可能会占用更多的计算资源与网络资源，影响业务连续性与用户体验。监控记录数据是否有效支撑，要看覆盖度与精准度。覆盖度与精准度要考虑机

构用户的业务特点、基础设施环境、安全需求、外部潜在威胁等，有侧重地采集所需要的监控与记录数据。后文在“关键能力”部分会有详细论述。

2.4 溯源分析定位缺少高效的技术手段与数据支撑

溯源分析定位环节也需要数据支撑，标准是“高效”，实现手段是将前面提到的端侧采集数据，与外部海量的威胁情报数据、基于行为的上下文分析检测技术三者在 EDR 平台侧进行融合，对端侧提供持续支撑。

这里的价值在于，溯源分析的过程目前大多依赖于有经验的安全事件分析师，在安全重保、实网攻防演练、或个别重大高危漏洞爆发时，人工分析是有必要的，但在日常安全运营的“告警风暴”中，如何通过技术手段实现一定程度自动化的溯源分析定位，这是安全运营团队的另一个迫切需求。

2.5 仅靠流量安全产品的威胁定位和响应无法闭环

IPS、NGFW、UTM 等流量检测类安全产品在应对办公网中动态 IP、NAT 等场景时，无法获取真实 IP，进而找到对应的终端，也无法关联到对应的员工。即便定位到终端，也无法第一时间定位到威胁进程，常常需要有经验的安全工程师进一步人工排查，排查到威胁进程后，如何在不影响业务的情况下进行溯源、清除，更加依赖安全工程师的经验水平。

整个排查工作下来，很可能攻击者已经完成了横向移动、后门植入等动作，入侵踪迹也已经删除完毕。因此流量安全产品要与 EDR 联动才可能形成有效的威胁定位、响应闭环。

3 行业用户场景

3.1 攻防演练中的攻击检测与快速响应

应对攻击队的渗透入侵行为，EDR 能够提供快速的检测定位与响应阻断能力。

EDR 的检测定位能力可以发现内网中爆破、提权等常见攻击工具，此外还可以用于发现凭据获取、权限维持和提升、防御绕过、内网信息收集、隐藏命令控制通信等高级攻击手法，另外还可以对内网横移手段中常用的域控攻击、漏洞利用、远程服务爆破等方式进行检测。

EDR 的响应阻断能力可以对失陷终端进行快速隔离，同时将失陷情报上报后同步至机构所有关联终端，第一时间做到全网响应。失陷终端上的攻击过程、攻击手法、具体的攻击动作、攻击进程链等上下文信息，可用于溯源分析报告的快速产出。

3.2 APT 攻击的检测与溯源

不同于一般的网络攻击，APT 攻击具备团伙化、专业化、武器化等特点。团伙化体现在分工明确、团队协同；专业化体现在杀伤链的每个环节都有针对性的专业工具，甚至会为单次攻击专门开发专用工具；武器化体现在大量使用从未公开过的 0day 漏洞，或是在黑市上大肆收购网络攻击工具，具备军火买卖的特征；此外，APT 组织一旦成功入侵，反而会低调蛰伏下来，轻易不做任何动作，这也为日常排查带来了极大的难度。

在这样的场景中，EDR 能够从终端上抓取 APT 攻击检测所需的多种行为数据，包括进程注入、Playload 反射加载、进程挖空等 APT 相关的高阶行为事件；

此外依托 EDR 平台侧的威胁情报能力，可以主动将 APT 组织在其他同类目标的攻击线索、攻击手法、攻击技巧等转为检测脚本，实现反客为主式的检测与溯源。

3.3 高危安全事件的终端定位与分析

“永恒之蓝”之后的每个周五晚上，安全团队负责人收到安全漏洞预警时都会心有余悸。因此，应对高危安全事件，第一时间对潜在受到影响的终端进行定位与分析，是 EDR 发挥作用的另一个主要场景。

对其他安全设备上发现的告警，或者 EDR 本身发现的潜在风险，EDR 都可以快速通过终端行为定位到威胁的进程源头，进而通过终端间的网络访问关系确定其关联影响的其他终端。安全管理者可据此快速下发响应策略，如隔离或修复。

3.4 混合办公、多分支办公等场景下的威胁感知

EDR 能够为混合办公、多分支办公等场景提供统一的终端安全视角。具体来说，包括对不同场景下的办公终端都能实现“随时随地”的接入和保护，保证勒索软件、钓鱼邮件、APT 攻击、木马外联、恶意软件等在内的多种攻击手法，都能通过 EDR 实现统一的安全检测与响应。基于此，EDR 能够持续采集终端行为数据，为远程终端和分支机构环境提供持续的安全评估，并通过 API 和 VPN/零信任网关联动，及时阻断高风险终端入网，从而以统一视角实现统一检测、统一响应。

4 关键能力

相比传统终端安全，精准 EDR 重在精准，因此，精准背后的关键能力主要有攻击检测能力、数据采集能力、攻击溯源分析能力、安全响应能力等四个维度。

4.1 攻击检测能力

所谓“精准”，攻击检测要准，威胁覆盖要全。

4.1.1 检测准确度

数世调研调研发现，在基于特征的匹配检测能力之外，想要构建更能满足用户需求的检测准确度，目前在多种可选技术路线中以“上下文关联”最具落地实践效果。

其逻辑步骤：首先全面记录终端产生的行为事件，之后将事件按照文件或进程上下文的方式进行关联，构建完整的事件关系链 / 网，然后对链 / 网中的每个节点进行判定，确定其行为标签，当新增事件或关系链时，对所有标签进行关联分析，从而判断该事件是否恶意。

这里要说明的是，事件涉及到的对象不局限于文件或进程，从系统进程、服务、接口、消息、命令行、注册表、日志等都应当加以覆盖（后面在“数据采集能力”部分会详细阐述）。

此外，大量关联分析的工作要在端侧和服务侧分工协作并加以平衡。端侧的数据采集与传输不能影响终端与网络性能；服务侧的标签判定、关联分析工作以人机结合的方式——例如基于图论等理论应用与机器学习算法等——自动化完成。

关于检测准确度的标准，用户需求场景不同，准确度的标准也不同。实网攻防演练场景下用户终端上的准确度更侧重高检出率，允许一定的误报率；对于金融、运营商等关基行业业务连续性要求更高的用户终端场景，准确度的要求则更高，检出即要求准确无误；其他日常安全运营场景，根据实际情况调整策略。

4.1.2 威胁覆盖度

除了检测准确度，另一个衡量检测能力的维度是威胁覆盖度。覆盖的威胁主要包括基于特征的恶意软件、覆盖 ATT&CK 的 IoA、以及包含 APT 组织在内的高质量 IoC 情报等。

对恶意软件的检测，可以依靠多引擎交叉检测进行覆盖，技术上不难实现，对于甲方用户和乙方企业来讲，主要考虑成本和生态合作；

对于 ATT&CK，需要对框架中的组织、战术、技术、步骤、工具软件等进行体系化的覆盖，形成针对性的 IoA 检测能力。对于高阶威胁场景需要重点覆盖，例如不同的远控框架、钓鱼场景、白加黑利用等，形成 APT 攻击手法的 IoA 检测能力；

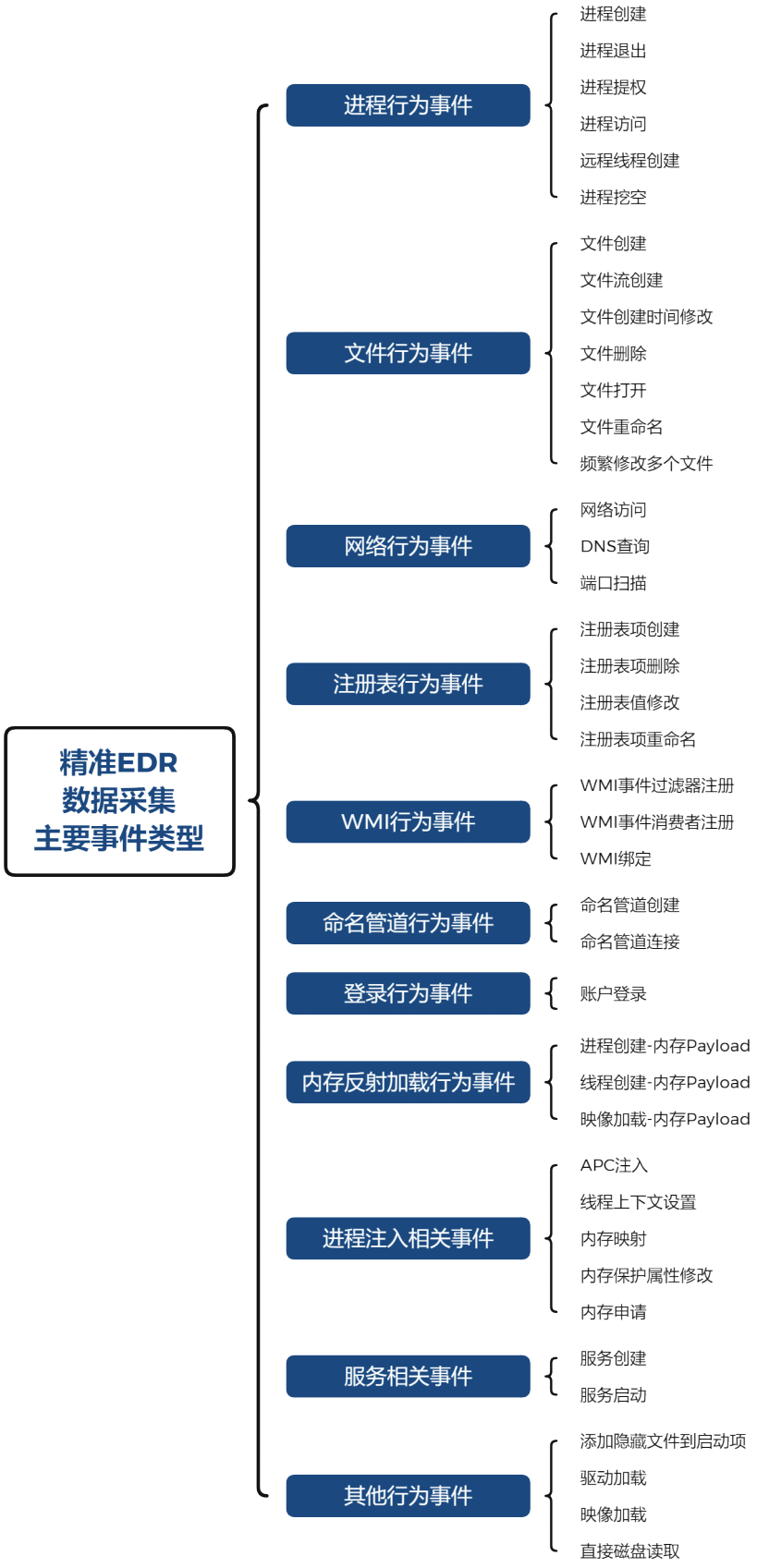
此外，海量、准确的威胁情报能力要能覆盖痛苦金字塔模型中哈希、IP、域名、网络 / 主机部件、工具等多个维度，高质量的 IoC 威胁情报是捕获 TTPs 的基础和保障。

4.2 数据采集能力

数据采集要全，一方面覆盖足够多的事件类型，如前面提到的进程、服务、接口、消息、命令行、注册表、日志等，另一方面每个事件所采集的属性也要尽量丰富，为溯源分析研判打基础。

数据采集的过程中要考虑到，不同用户态、内核态下不同权限所接触到的

数据有所差别。例如驱动的加载要避免遗漏，对内存马等高级威胁攻击要注意采集内存状态、内存活动等行为，避免被绕过。



图例 3：精准 EDR 数据采集

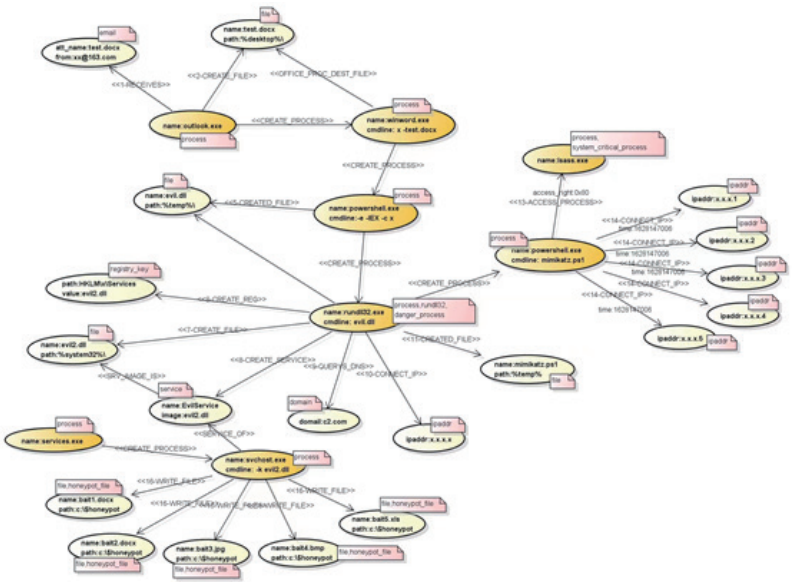
值得一提的是，采集的数据并非全部都要回传，绝大部分数据属于重复数据、静态数据，它们对于研判是无用的，回传会占用大量的 agent 性能与网络资源，因此需要在终端侧对采集到的数据进行去重、重组、筛选、标签等操作，以最小化原则回传。

4.3 攻击溯源分析能力

精准 EDR 对攻击事件进行溯源分析时，有两个基础能力要满足，首先要具备底层事件的上下文关联，其次要具备基于图的可视化。

所谓底层事件上下文关联，是指采集事件时诸多系统进程中的行为看似是系统进程或正常进程，如 services.eve、explorer.exe、svchost.exe、winword.exe 等，但其实是恶意文件通过系统接口、服务、消息等方式发起请求实现的。在采集到这些事件时，需要加以甄别处理，并结合上下文，判断其真实行为。

基于图的可视化，是指将攻击过程以知识图谱等方式进行可视化展示，重点突出显示高风险行为所关联的节点和边，这样即使是普通安全分析师也能快速掌握，达到精准的攻击溯源分析能力。



图例 4：基于底层事件上下文关联的图溯源（本图例由微步在线提供）

在上述两个能力的基础上，对攻击威胁进行溯源分析时，可根据用户场景，结合 ATT&CK 框架，制定出若干适用的溯源脚本；还可引入图分析和机器学习算法，从而达到一定程度的自动化、智能化水平；最后，依托云原生能力，可以将所有数据汇总形成一个基于云的、可大规模扩展的图形数据库，从而形成近乎实时的可视化、数据分析与威胁防护能力。

4.4 安全响应能力

精准 EDR 的安全响应以一定程度的智能化溯源分析作为前置能力，以“单点隔离，阻断横移”为基本原则，不同的场景响应方式略有不同。

在实网攻防演练场景中，可结合威胁情报针对疑似失陷终端做快速隔离，或者通过策略配置限定其可访问的网络范围，进行快速处置。

在 APT 攻击场景中，可对全量事件记录数据进行回放溯源分析，初步判定威胁的攻击路径及源头，然后给出针对性的处置动作建议，或者由经验丰富的安全分析专家直接从云端下发响应处置动作。

更精细的响应动作上面，除了基本的隔离终端、文件进程阻断等操作，应该支持更精细的响应动作，以支持高级威胁中的处置，这些动作包括但不限于：计划任务和启动项的删除、账号的禁用和删除、驱动的卸载、顽固病毒木马的专杀清理等。

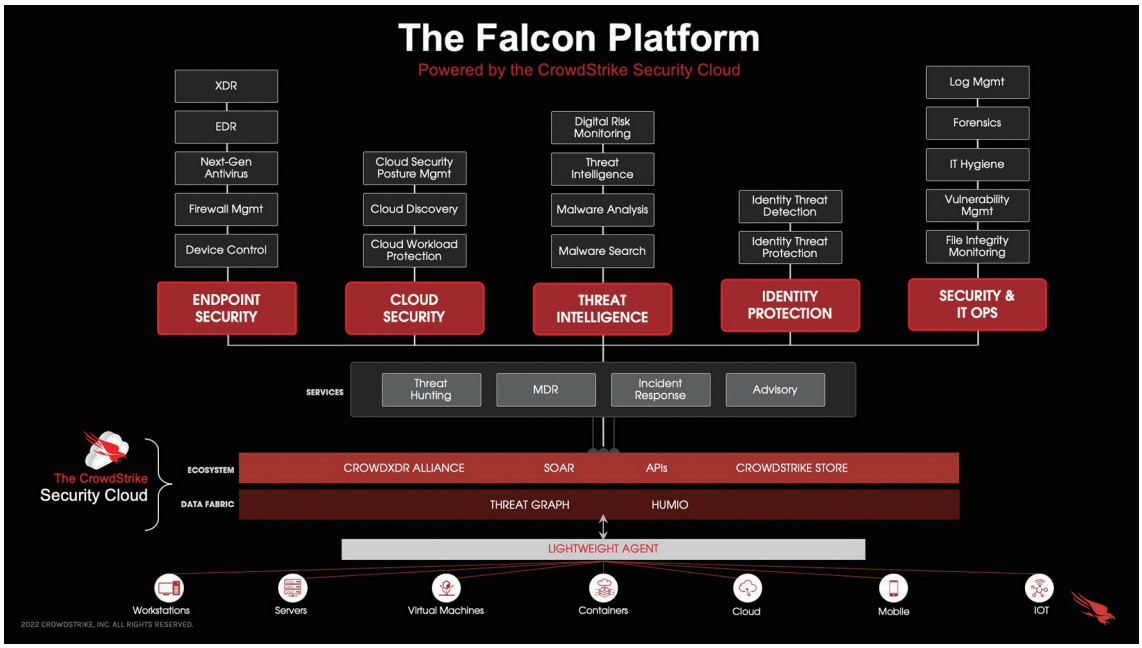
为了提升响应时效，上述响应手段建议以 SaaS 方式实现，且所有处置动作都应可记录可审计可检索。当然，这里要说明的是，调研中我们也发现，在面临重大安全事件时，用户普遍认为必要的现场应急响应目前仍然是必不可少的。

5 代表企业

5.1 CROWDSTRIKE

众所周知，CrowdStrike 作为当前终端安全厂商的先进代表，其最早期以其出众威胁情报能力打动市场，后通过 EDR 产品则使其情报能力在用户侧得到了充分的发挥和落地。

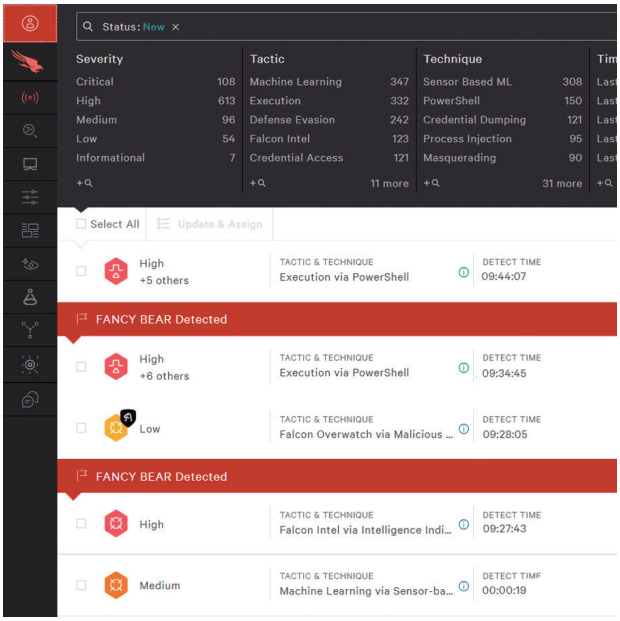
具体到产品和解决方案层面，不同于传统基于规则和签名的杀毒软件公司（如 Symantec 和 McAfee），CrowdStrike 的 EDR 解决方案 Falcon Insight 是一款 SaaS 模式的终端安全平台，无需重新启动系统和网络，轻量级 agent 就可以在终端和工作负载上大规模部署，也无需本地硬件与数据库，管理和配置均通过云端实现。

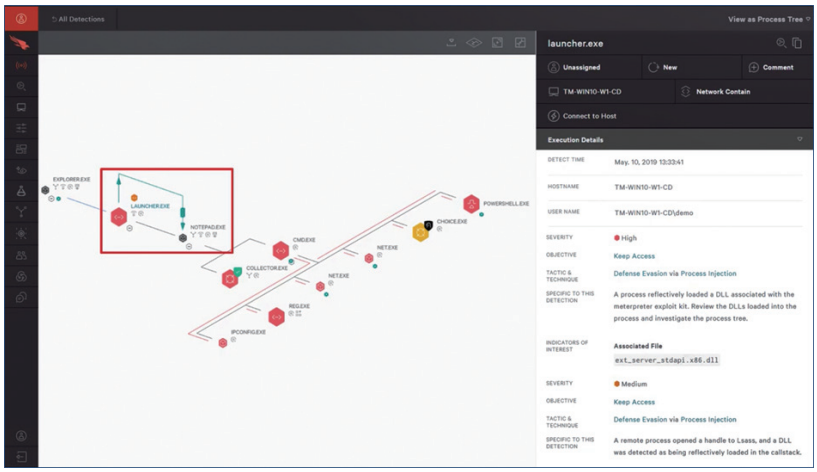


这些便捷性，是由 100% 的云原生架构带来的，如上图所示。

通过安装在客户终端上的单一轻量级 agent 将收集来的数据传输至云端统一数据库 Threat Graph，基于 Threat Graph，Falcon 持续地收集、处理和实时分析所有客户终端所面临的的威胁。

功能方面，通过智能优先排序、上下文关联、快速搜索等功能，Falcon Insight 能够带来显著的效率提升，如下图所示：





同时在多年的威胁情报积累与出色的数据溯源分析能力形成的“CrowdStrike 安全云”的支持下，其在可视化、智能化等方面做的也很出色，

一个显著指标是，据称其能够减少 90% 以上的无效预警，避免告警风暴；再加上完备生态带来的响应闭环能力，安全运营团队的整体效率可以得到进一步提升。

市面上对 CrowdStrike 产品能力的介绍有很多，本报告不多做赘述。总之，以优异的威胁情报能力为基础，CrowdStrike 又充分利用了云和 AI 的能力特性，如轻量快速部署、大规模可扩展、单事件 - 全平台学习与更新等，使其能够在海量威胁事件中快速精准发现会真正影响用户的真实潜在威胁，这让它在终端侧的快速检测与响应场景中获得了普遍高于同行的客户评价。

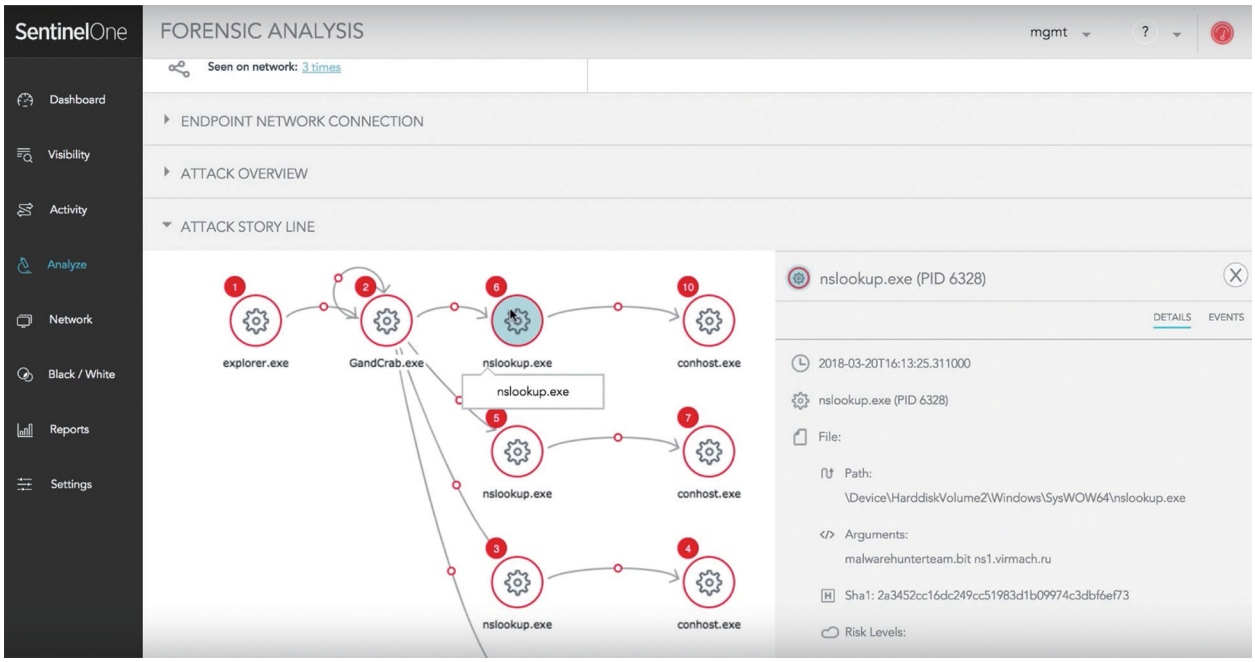
5.2 SENTINELONE

SentinelOne 公司成立于 2013 年，总部位于美国加州的帕洛阿尔托市，公司的产品使用人工智能技术自动化识别企业网络中的异常行为，保护用户终端设备免受网络安全漏洞的侵害。

SentinelOne 的主打产品是基于人工智能的 XDR 奇点平台（Singularity Platform）。该产品将终端防护、云端安全、事件响应、攻击面管理、甚至 ITDR 等集中在一个平台中，为企业所有的互联网接入点提供保护，包括笔记本电脑和台式机，以及各种云设备、数据中心和物联网设备等，防止它们受到恶意软件、脚本攻击以及其他的危害。

就本报告所关注的 EDR 场景而言，SentinelOne 的能力特点有 AI 驱动的威胁防护与检测、实时的攻击面管理、基于 ATT&CK 的自动化快速响应等。
其能力特点与其他安全软件最大的不同之处是，其他安全软件需要把监测数据上传到云端进行分析，同时也依赖人工处理监测预警并采取应对措施，SentinelOne 则推崇用机器对抗机器，略去大量的人工判断转而采用自动化监测从而大幅度减少错误判断。

虽然效果仍需要验证，但在笔者看来，自动化监测确实可以带来至少 2 个好处：一是可以解放人工的关注度，使安全团队可以把精力集中在更为关键的风险点上；二是略去人工参与后，响应速度最快可以到毫秒级别，一旦监测到有安全威胁，平台就可以快速采取措施进行处理。



因此要达到这个目标，SentinelOne 的人工智能引擎是部署在用户的本

地化终端侧或云端平台的，能在没有云端服务器的情况下运行。看得出来，SentinelOne 相信将其设备、云服务和 AI 融合在一起，能够比现场或云原生服务更快地响应威胁（毫不避讳且有针对性地对标 CrowdStrike，其官网上甚至专门有与各个友商 EDR 的正面对比）。

除了理念上的不同，功能方面 SentinelOne 也有一些亮点，例如它支持将实时的上下文以时间线的方式进行可视化展示，再例如针对勒索软件，SentinelOne 具备“一键回滚”功能，使系统能够自动将自身重置为以前的某个状态。

总体而言，即便有市值最高的网络安全公司 CrowdStrike 在前，与之对标的这家成立于以色列的公司 SentinelOne 仍然亮点多多，鲜明地走出了自己的创新技术路线。资本市场对其也是青睐有加，2021 年 IPO 时超过 CrowdStrike 在 2019 年创下的初始估值 67 亿美元的纪录，以 88 亿美元成为历史上价值最高网络安全股 IPO。但就核心能力而言，其短板也是很明显的，即威胁情报的能力在客户侧普遍反应不如 CrowdStrike，这大大影响了 SentinelOne 在市场执行层面的表现。

因此，只有首先解决客户最在意的核心诉求——精准发现威胁，之后的自动化响应才更有价值。

5.3 微步在线

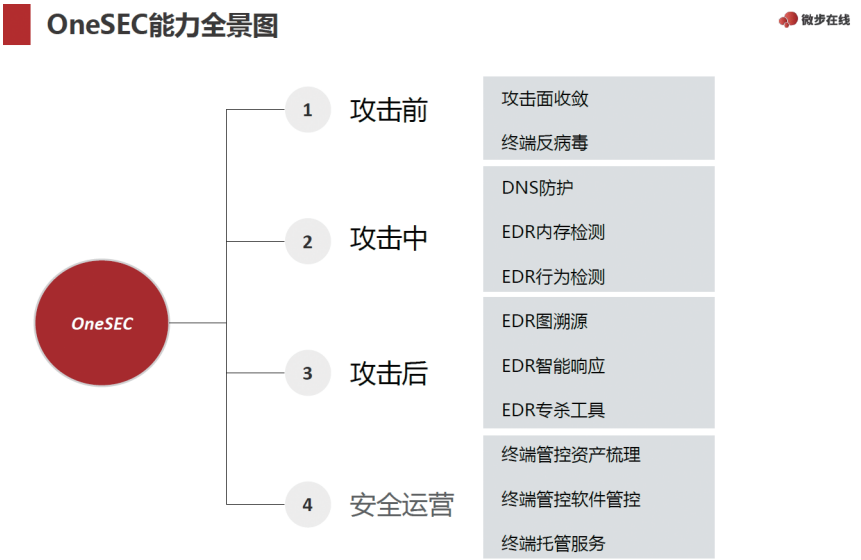
微步在线

让 安 全 没 有 边 界

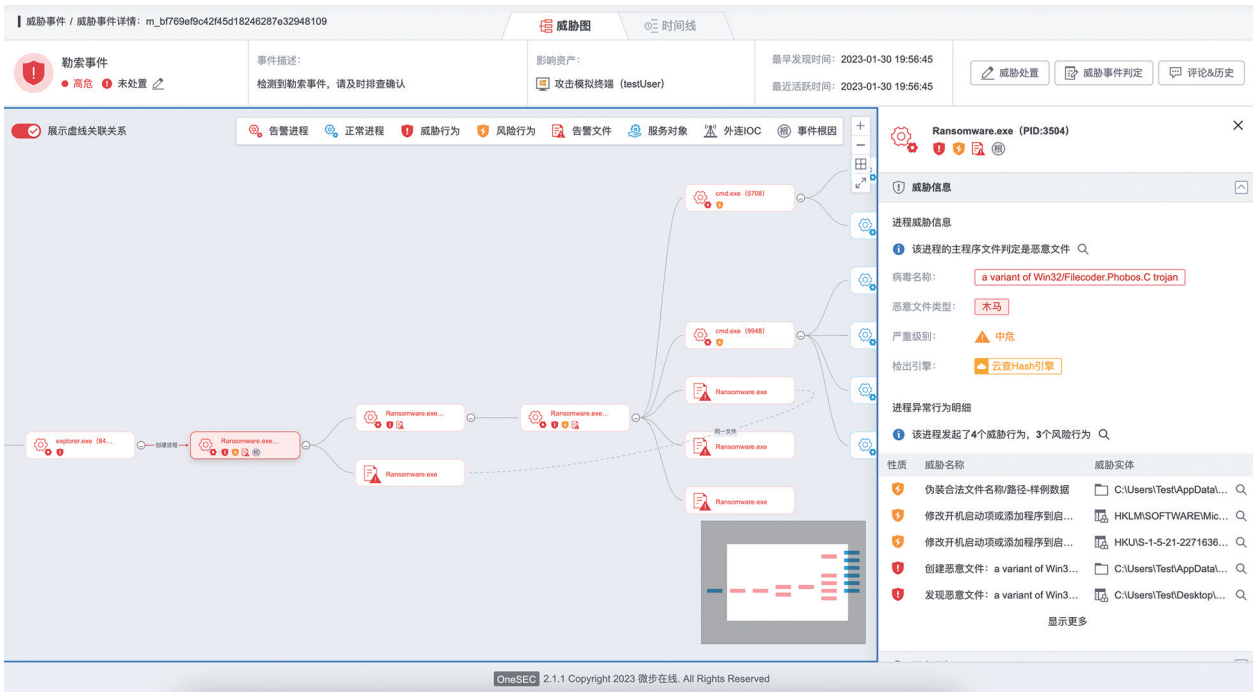
2022 年微步在线进行了品牌升级，品牌升级背后是安全能力的升级。以威胁情报为基础优势能力，全面覆盖了端点、流量、边界、云端等多个维度的安全能力。这一点与 CrowdStrike 是发展路径是相类似的。

就本报告所关注的 EDR 场景，微步在线对应的产品为 OneSEC，功能覆盖事前、事中、事后全流程。其能力主要包括攻击面收敛、内存检测、行为检测、溯源分析、智能响应等。

与前面两家代表企业相比，微步在线 OneSEC 既具备 CrowdStrike Falcon 的云原生架构与威胁情报优势，又具备 SentinelOne 奇点平台的攻击面管理与 AI 驱动能力，因此可以同时在检测准确度、威胁覆盖度、数据采集、溯源分析、快速响应等关键能力点上满足“精准”要求。此外，结合国内重保与实网攻防演练等本土化场景，微步在线还提供了专杀工具以及资产梳理、终端托管等本地化安全运营服务。



值得一提的是，微步在线 OneSEC 具备出色的威胁狩猎能力。正如“关键能力”部分所描述的，以底层事件的上下文关联为基础，通过图的可视化能力，微步在线 OneSEC 能够显著提高威胁检测的精准度，也使普通的安全工程师能够快速溯源，找出攻击源头，实现快速响应，达到高级安全工程师的效果。



6 未来展望

6.1 EDR 向精准化、一体化等不同的方向发展

不同行业不同场景对 EDR 的差异化需求，未来会影响 EDR 向着不同的方向发展。

本报告所讨论的精准 EDR，用户群体主要为关键信息基础设施行业用户，其终端数量在数万到数百万不等，终端侧的攻击暴露面较广，且以高级威胁检测与响应为主要需求。

终端数量较多且以安全管理为主要需求，同时高级威胁检测需求相对较弱的用户，需要的是整体终端安全解决方案，在此类需求的推动下，EDR 逐渐演变为“一体化终端安全”解决方案。

6.2 EDR 从自动执行向自主决策发展

虽然多种机器学习技术都已在网络安全领域得到应用，但目前 EDR 的检测、响应都需要以积累的海量威胁情报为基础。因为一旦撞上这些签名，几乎可以确定攻击，省去大量的关联分析工作，“自动执行”阻断响应，因此威胁情报签名仍然是检测已知威胁的关键基线。

在这一基础上，接下来 EDR 将向“自主决策”发展，即通过人工智能技术将创造性思维从耗时的自动执行操作任务中解放出来，例如更多关注在检测高级威胁时的上下文关联分析、威胁处置优先级排序等，针对不同风险自主决策采用不同的控制措施（如隔离可疑文件或要求用户重新验证），逐步提高安全运营效率、降低威胁风险。

也有像 SentinelOne 这样的安全企业，把 EDR 的响应操作几乎全部交由

AI 决策，未来类似的安全企业、类似的安全领域也会也来越多。

6.3 EDR 依然是 TDR 中核心重要一环

随着 XDR 概念的提出，就开始不断有声音表示 EDR 即将走到尽头，但事实上并非如此。

EDR 只采集端点侧数据，缺乏和其他安全产品的联动（如 NDR），从而难以将关联分析更进一步扩展到整个环境。XDR 概念的提出解决了安全产品之间缺乏协同的问题，且在 XDR 中 EDR 是核心组件。与此同时，国内 XDR 要想落地，以 TDR（Threat Detection and Response）更为适合——无论是“威胁情报”，还是“威胁狩猎”服务，都是从“威胁”的角度出发，近年来的大型演练活动更突显了这一点。无论检测还是响应，都只是手段；检测和响应这两个手段的目的，是为了处理“威胁”。

因此，从“威胁”维度出发，构建数字环境的安全体系，是国内未来的安全趋势之一。在这一场景下，EDR 是直面威胁的重点区域。无论是作为独立的解决方案，还是作为 TDR 中的一个关键组件，EDR 能力必然会成为整体安全结构中的重要一环。

6.4 不断提速的信创进程需要与之匹配的 EDR 能力

关基行业大规模的国产化替代是必然趋势，三年来，信创是各项信息技术投入中屈指可数的没有受到疫情影响的领域，这给国内 EDR 市场带来了绝对的市场机会。因此不断提速的信创进程需要与之匹配的 EDR 能力跟上快速发展的步伐。

一方面目前信创操作系统、信创终端应用在研发层面更侧重于能力实现，随之产生的安全短板需要安全厂商重点从端点侧在运行阶段来补足；另一方面，信创系统的更新迭代会相对更频繁，也需要 EDR 企业需要持续投入力量做好适配，跟上信创系统的步伐。

参考资料：

https://www.dwcon.cn/post/894

https://www.dwcon.cn/post/1718

https://www.crowdstrike.co.uk/products/endpoint-security/falcon-insight-edr/

https://www.crowdstrike.com/falcon-platform/threat-graph/

https://www.sentinelone.com/

https://www.sentinelone.com/blog/sentinelone-detects-protects-gandcrab-ransomware/

https://www.threatbook.cn/

https://zhuanlan.zhihu.com/p/397782938

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