数世咨询
Digital World Consulting

主机检测与响应
Host Detection and Response (HDR)
能力指南

数世咨询
Digital World Consulting

主机检测与响应
Host Detection and Response (HDR)
能力指南

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

综合分析师 刘宸宇
首席分析师 李少鹏
统计分析师 牛爱民

版权声明

目　录

目　录

前 言

主机上的安全防护手段，多年来一直以HIDS为主，但随着金融、制造、能源等传统行业的数字化转型，到科技互联网等新兴行业的创新业务，数字经济的背后最重要基础设施之一是海量的云主机，目前大部分的主机安全场景都已经来到云端。

针对云主机安全，目前现有的体系只有2016年Gartner提出的CWPP体系，但其目标是主机、虚拟机、容器，无服务器（serverless）等工作负载，没有任何一家单一厂商能够真正将其完整落地。除了CWPP，还有针对端点（Endpoint）的EDR，但与CWPP一样，EDR中虽然也包含主机，但国内的EDR实际落地时，主要集中在PC端，无论是业务场景还是系统层面，EDR所需的安全能力与主机侧有很大不同。单纯针对主机侧的安全检测与响应，始终缺少一个“DR”对其做出体系化的描述；

与此同时，无论是红蓝对抗演练，还是日常安全运营，主机侧的安全检测与响应又实实在在不断涌现着新的实战化需求。有需求就会有市场。越来越多的安全企业开始进入主机安全这一细分领域，实际上，做主机侧安全检测与响应的企业已经有一批优秀产品及服务。在本报告持续调研的一年多期间，仍有新的能力“玩家”进入到这个赛道中来。

综上所述，在这样的背景下，理论与现实之间的空白，需要一个适宜的新赛道，对其做出定义与描述。数世咨询撰写本能力指南，旨在梳理“主机检测与响应”这一细分领域的用户需求、市场现状，盘点能力企业的技术能力与典型案例，于用户和能力企业之间，建立指南性质的纽带，供各方参考。如有错误，欢迎不吝批评与指正。

关键发现

●主机检测与响应（Host Detection and Response - HDR）是指，以主机侧为目标，以探针 agent 为基础技术手段，采集网络、文件、进程等多种维度的数据并上传至管理平台，辅助威胁情报关联分析后，以自动化策略或人工响应处置安全事件的解决方案。

● HDR 细分领域的市场规模（2021 年）为 21.56 亿元人民币，相比较 2020 年 12.8 亿，增长率为 68.44%。新冠疫情第二年，客观上加快了国内云计算的进程，伴生的主机安全需求也随之增长；近年来持续的红蓝对抗实网攻防，对主机安全提供了有力的刚需支撑。

● HDR 的四大需求场景：合规驱动、技术驱动、效率驱动以及场景驱动。

● HDR 关键四大能力：agent、安全视角的资产发现、安全检测能力、安全响应能力。

●用户业务连续性与 agent 的接受程度负相关。

●主机侧的安全响应，一定要能够通过 HDR 产品与业务、网络、运维等兄弟团队进行同步、协同，这是 HDR 响应能力的重点。

●未来发展趋势， HDR 的未来会呈现需求与投入双增长的态势，内存安全能力将成为标配，实战化对抗场景仍将是主流，HDR 将与 EDR 趋于整合。

第一章　市场情况

参与本次调研的企业共11家，分别为青藤云安全、奇安信、安全狗、阿里云、绿盟科技、天融信、安芯网盾、长亭科技、微步在线、杰思安全、云弈科技。数世咨询以市场执行力与应用创新力为主要维度，HDR 能力指南点阵图如下所示：

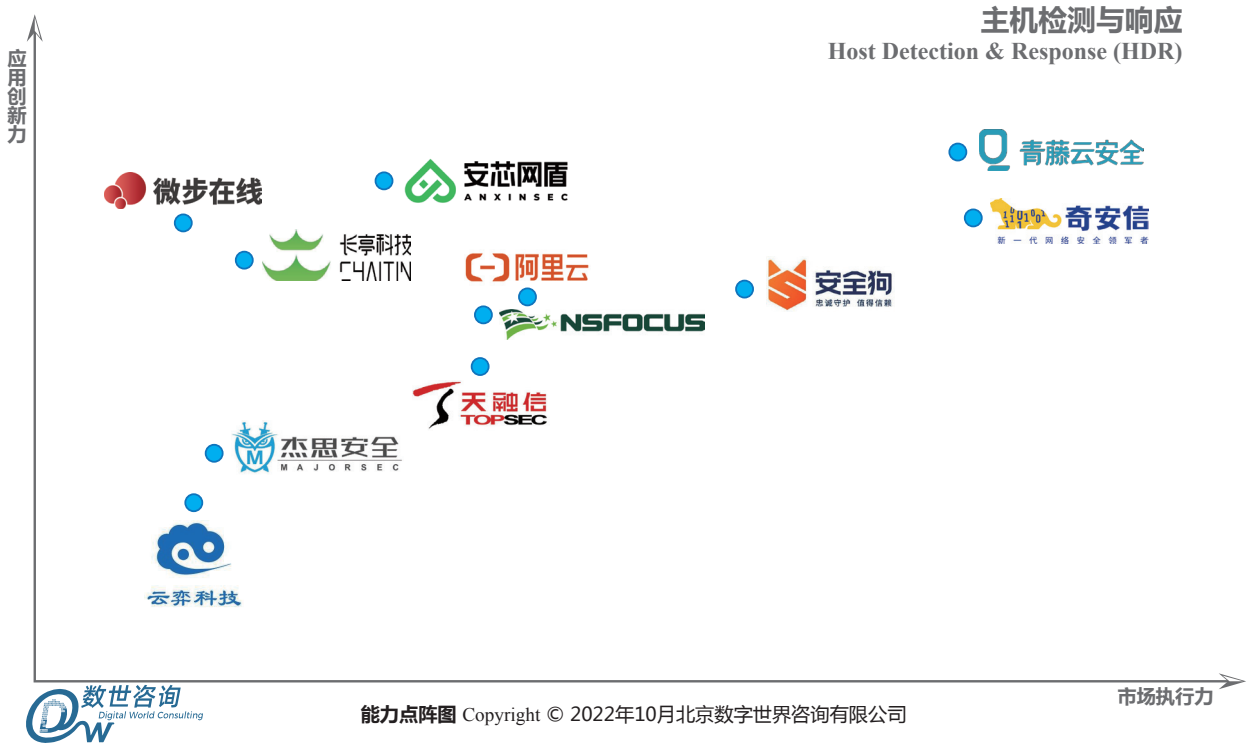

图 1　主机检测与响应能力点阵图

据不完全统计，HDR 细分领域的市场规模（2021 年）为 21.56 亿元人民币，相比较 2020 年 12.8 亿，增长率为 68.44%，显著高于 2021 年整个网络安全行业的年复合增长率 18.6%（数据来源《中国数字安全产业统计与分析报告 2022》，数世咨询，2022 年 8 月）。

“主机安全”高增长的主要驱动力有二。一是新冠疫情第二年，客观上加

快了国内云计算的进程，伴生的主机安全需求也随之增长；二是近年来持续的红蓝对抗实网攻防，对主机安全提供了有力的刚需支撑。再则基于前两点，用户对主机安全的接受度越来越高，同时不断有新的能力“玩家”加入这个细分领域。

第二章　能力定义

一、HDR

本报告中的主机检测与响应(Host Detection and Response - HDR)是指，以主机侧为目标，以探针（agent）为基础技术手段，采集网络、文件、进程等多种维度的数据并上传至管理平台，辅助威胁情报关联分析后，以自动化策略或人工响应处置安全事件的解决方案。

二、含义与区别

根据定义，同时具备主机、agent 探针、检测、响应以及管理平台等关键要素的产品才属于HDR。本报告中的“主机”，若无特殊说明，均指服务器——即传统物理主机——以及虚拟机和容器的统称。

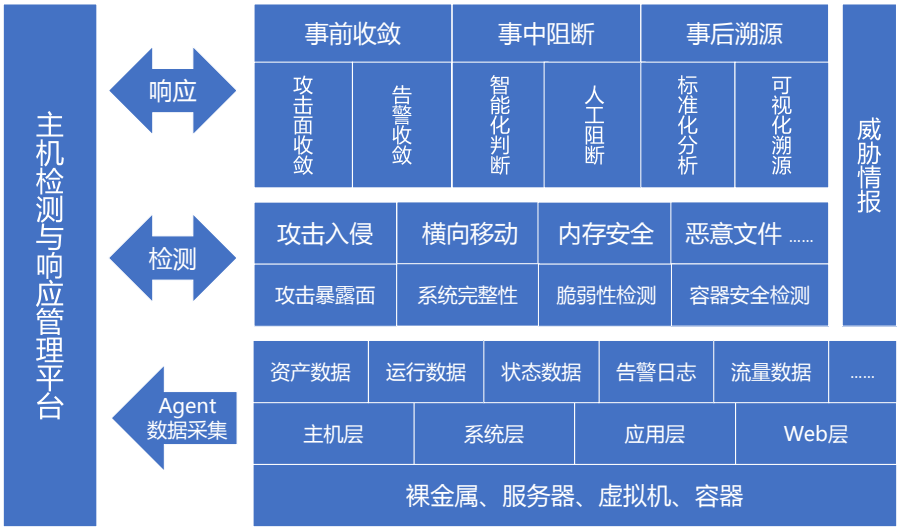

图 2　主机检测与响应

与 EDR 的区别

HDR 看似与 EDR 很相似，但不同于 EDR 以 PC 终端为主要目标，HDR 主要针对的是主机侧，其特点主要为：

性能角度，重服务端，轻客户端；重稳定兼容，忌资源占用；
功能角度，重基线监测，轻突击检测；重采集分析，慎自动响应；
效能角度，重精准告警，忌大量疑似；重聚合可视，忌单点孤岛；
价值角度，重业务连续，轻安全防护；重管理协调，忌草率加固。

与 HIDS 的区别

传统的主机入侵检测（HIDS）是孤岛式的，基于相对固化的恶意特征和行为规则，缺少数据关联分析与响应。与之相比，HDR 强调与攻击暴露面、威胁情报等内外部数据的联动，强调基于安全运行基线的精准检测告警及人工快速响应。

与 CWPP 的区别

Gartner 提出的 CWPP 是一个理念，对工作负载涉及到的安全技术做了完整覆盖。虽然全，但是没有一家能够凭借一己之力做到全部落地。同时，CWPP 中所包含的微隔离、HIPS、漏洞利用防护、内存防护、文件防篡改等侧重“防护”的能力要求，本报告并不涉及。本报告作为 HDR 能力指南，对“防护”的描述较少，主要关注主机层、系统层、应用层等各层的检测与响应能力，此外，CWPP 涉及到的 AD 域安全、容器安全等赛道能力，本报告虽有提及，但并不打算进一步展开，未来会有其他报告详细讨论，在此也一并说明，后不再赘述。

三、能力标准

接下来，在讨论具体的关键能力前，首先要明确能力的标准，数世咨询认为，HDR 的主要能力标准包括检出率与漏报率、MTTD 与 MTTR（平均检测时间与平均响应时间）等指标。

检出率与误报率主要针对 HDR 类产品的威胁检测环节，重点考量对漏洞、木马、弱口令等潜在威胁的发现能力。在主机侧业务场景中，HDR 产品的检出率与误报率要综合考虑对运维效率的影响，保证检出率的同时，优先降低误报

率。

MTTD 与 MTTR 主要衡量的是安全团队综合利用安全工具、产品、平台进行体系化威胁检测与事件响应的能力。

MTTD - Mean Time To Detect 平均检测时间，指从系统故障到检测或告警所需的平均时间。MTTD = 故障与检测之间的总时间 / 事件数量。例如：某主机系统在 12:00 发生故障，但直到 12:10 才有人收到 HDR 产品的提醒或告警，那么此时 MTTD 是 10 分钟。

MTTR - Mean time to respond 平均响应时间,指从第一次收到告警时起，直到主机或主机上的系统、应用等从故障中恢复所需的平均时间。MTTR = 检测告警与服务恢复之间的总时间 / 事件数量。例如：本周工作时间内（40 个小时）一共发生了四起事件，安全团队在这些事件上总共花了一个小时（从告警到恢复），那么本周的 MTTR 就是 15 分钟。

值得一提的是，对于主机侧来说，由于优先保障业务连续性等原因，目前上述各项指标中短板主要在 MTTR。“自动化响应”能够有效缩短 MTTR，但应当注意结合主机侧所属行业，区分红蓝对抗演练与实战等不同场景，在业务等安全之外的因素允许的情况下，通过内存实时防护阻断等较高可靠性的分析与判断能力，实现一定程度的自动化阻断。

第三章　需求场景

数世咨询本次调研，访谈了十余家用户，分布于金融、运营商、科技互联网等行业。各行业主机数量庞大，形成了庞大的主机安全需求。以金融为例，头部大金融机构，其虚机数量超过百万台量级，以 6 家国有银行、12 家股份制银行，数百家城商行统计，共计私有云数量上百个，粗略估计，全行业主机数量（虚机）超过 5000 万台。

这其中，除云厂商之外，HDR 厂商部署的云环境中，私有云占比约为 80%，大型金融机构为代表的用户不会将核心业务（大型机、小型机等核心交易系统，暂时还没办法资源池化的业务）放在公有云上。公有云自带的主机防护产品作为云的附加值即可基本满足安全需求。主机安全的自主建设需求，主要来源于私有云或本地数据中心。

基于此，数世咨询梳理总结出 HDR 产品的需求：合规需求驱动、安全技术驱动、提升安全运维效率、实战攻防演练等四大场景。

满足合规要求

不仅“等保 2.0”对主机安全有明确要求，各行业如工信部、人民银行等监管机构，每年对下辖各行业机构的安全审计中，对主机安全也都有明确的能力要求，且非常严格，审计考核结果都会列入年底的绩效，甚至“一票否决”，主机安全能力成为必修课，此为 HDR 的第一需求。

安全技术驱动

运营商、金融、电力等行业用户主机数量动辄百万台数量级，主机侧的安全需求仅仅依靠边界防护早已无法满足。主机侧的资产发现与管理、安全检测

与应急响应，若直接套用PC终端的安全能力，又并不适用，因此迫切需要专门的主机侧的产品及技术解决方案，作为最后一道防线，主机检测与响应成为技术发展的必然。

提升安全运行效率

第三个需求，安全团队希望通过HDR产品及相关解决方案，加强与各兄弟团队的沟通，提升安全运行效率。以漏扫为例，面对物理服务器、虚拟机、容器等多种形式的主机，真实的资产情况并不清楚，于是首先借助主机安全产品，以安全视角盘点资产摸清家底，并充分获取相关安全运行数据。在此基础上，借用agent进行漏洞的版本匹配式扫描，并将扫描结果与网络、运维等各兄弟部门对接，进行后续漏洞的修复以及修复后的复测效率。总之，安全团队需要通过HDR与各部门共同修补短板，提升主机安全运行的整体效率。

实战攻防演练

实战化攻防演练这几年带动了诸多安全需求，客观上也从实战化角度促进了各行业用户对主机安全需求的提升。以金融行业为例，在金融科技转型要求的背景下，除了公有云上的互联网金融业务，更多业务迁移到了私有云为主的一朵朵金融云中，且疫情之后，这个迁移速度还在加快。业务上云与实战化攻防演练的双重背景下，大量的主机资产暴露在攻击者面前，成为潜在的攻击目标，若仍采用传统的内网防御方式是明显滞后不足的。**因此，HDR需要的不再是基于特征匹配的传统HIDS，而是结合安全基线与外部情报的有效检测能力，以及基于精准告警的快速响应能力。**基于此，主机侧的脆弱性检测、攻击入侵检测、内存安全等实战化能力，都成为近两年实战攻防演练中取得好成绩的必备技能。

上述各类需求只是简单分类，不同行业用户对不同场景的需求程度是不同的，几类需求之间也并非完全割裂开。例如资产盘点在红蓝对抗攻防演练前一定会再进行2-3轮排查。相对而言，能力强的用户更关注HDR的安全检测能力、风险发现能力，侧重发现威胁的全面性；能力相对较弱的客户，还希望在发现

攻击入侵后，HDR 能够第一时间自行判断后加以阻断，具备一定的自动化响应能力帮其抵御住威胁。后面会详细阐述 HDR 的各项关键能力。

第四章　关键能力

一、Agent

首先，本次能力指南调研过程中，无论用户还是能力企业，讨论最多的就是 agent。HDR 实时的安全监测数据采集来源主要来源于 agent，HDR 产品的定价模式也是以单台主机 agent 为定价单元。

从用户角度来说，对 agent 的衡量标准主要有三点：业务连续性、资源占用率、功能效率。

业务连续性

用户对 agent 的要求中，排在首位的一定是业务连续性。agent 要安装在用户的主机上，这就代表所有的业务应用、运维系统都要在 agent 的潜在影响下运转，理论上，如果 agent 出现问题，是可能会影响到业务的连续性的，哪怕这个可能性非常非常小。

安全产品的目的是提高业务安全稳定运行的上限，但是安全产品本身一定不能影响到业务正常运行这条底线。一直以来，agent 在对业务连续性要求极高的行业中，始终会面临较难的接受度，正是基于这个原因。因此，对于金融、运营商等行业用户的主机来说，agent 类安全产品会十分触动业务部门与运维部门的神经。

这里有一个小小的区别，当用户的安全团队尝试协调各部门，将“侵入式”agent 安装到主机上时，往往会受到更大阻力，同事们会担心对主机驱

动或配置的修改，更可能导致业务连续性受到影响。与“侵入式”类似，当agent 运行在“内核态”，即需要 root 权限时，也可能会导致类似的来自于相关部门同事的阻力。

这里并不是说，相比“侵入式”、“内核态”而言，“接管式”、“用户态”的 agent 会更好，没有绝对的好与坏，只有是否适合，这个要根据用户的实际情况而定。当用户的安全部门具备较高的地位或更强势的话语权时，agent 如果具备更充分的运行资源、更高级别的运行权限，探针的能效会发挥到最大，对于数据的获取、主机运行的安全监测一定会收到更好的效果。相反，如果用户的安全部门相对弱势，退而求其次相对“温柔”的 agent 形态才是一个合理选择。不论以哪种权限、哪种身份运行，对 agent 的兼容性测试就很重要，公有云、私有云、混合云各种云环境，主机、虚拟机、容器以及对古老硬件与操作系统的适配都要考虑到，底线都是不能影响业务连续性。

资源占用率

对 agent 的第二个衡量标准是资源占用率。例如 CPU 占用率、内存、吞吐、磁盘 IO 等。数世咨询建议从两个维度来考量，首先是模拟主机资源有限情况下的 agent 资源占用率，例如中低端性能的主机场景下，agent 可能会占用的资源。如果 agent 占用资源过高，就可能导致宕机，影响业务系统的运转。

其次是压力测试下的 agent 稳定性，即模拟真实业务环境下，全量策略运转起来后 agent 的稳定性，如果不能稳定运行在某个资源占用率区间内，例如 agent 一开始内存占用只有几十 MB，但随着全量策略下运转时间不断延长，内存占用可能会逐渐升高，当超过某个阈值（例如 200MB）时，会被服务器的自保护机制 kill 掉，这样一来，威胁因此反而得以入侵。

应对这种情况，不同的能力企业应对方式也不一样。有的 agent 会定期检测自己的资源占用情况，当超过某个预先设定好的阈值时，会自我 kill 并立即重启，避免上述情况。还有的 agent 会以接口轮询的方式，避免资源的持续占用，只有检测触发到威胁时才会有新的资源调用。总之，采用哪种应对方法，

还是要根据用户的实际应用场景来决定。

功能效率

为了应对上述种种可能的情况，市面上的主机安全产品均带有较为 灵活的配置接口，供用户根据实际需求，对 agent 的功能、运行效率进行设置。在此基础上，不少能力企业会为 agent 加入更丰富的功能，例如除了采集进程、网络连接等实时数据外，有的 agent 会内置 WAF 探针模块，支持监测加密流量，还有的 agent 加入了阻断能力，使其在安全监测的角色之外，具备了一定的响应能力。

功能效率也会体现在客单价上，功能更多、同时资源占用更少的 agent，客单价会更高。当然，从用户的角度来说，价格并非首要的考量因素，功能的专与多，也并非绝对，要看不同的用户需求。对于金融、运营商这样自有安全团队能力较强的行业客户，倾向于功能更“专”的专一型 agent，相对的，安全团队人员较少、能力较弱的行业用户则倾向于功能更“多”的综合型 agent。

此外值得一提的是，有些企业还为用户提供无 agent 模式的主机安全产品，以并行虚拟机的方式实现，主要用在 IaaS 或 PaaS 上不便于直接在租户主机安装 agent 的场景中，例如运营商或电子政务云等。

总之，对于用户来说，选用何种类型的 HDR 产品，应当对 agent 的业务连续性影响、资源占用率、功能效率、价格等因素综合考虑，再根据实际 PoC 测试后确定。

二、安全视角的资产发现

基于安全视角的资产发现与管理，是有效检测与响应的前提。对于主机侧的资产，安全团队应当重点考虑不同云环境下的服务器、虚拟机、容器等资产台账的盘点与统计。针对这些入账资产，要进行主机层、系统层、应用层乃至

Web 层等各细化层级的资产清点，为后面做到安全基线梳理、快速精准检测、快速发现威胁、快速做出响应打好基础。

这里要强调的是，所谓“基于安全视角”，不能只从攻防角度来考虑资产重要性，还应当结合业务优先级、强合规等要求，从更高的安全敏感度考虑资产重要性，对发现的资产进行分类分级、统一管理。例如，哪些是对外提供服务的资产，哪些是机构内部员工可以横向移动访问到的资产，哪些是核心业务系统相关的资产，以此为基础，在诸如红蓝对抗攻防演练等场景下，提前关闭不必要的业务、服务、端口等，收敛靶标系统相关资产，极大减少潜在的攻击暴露面，并逐渐形成常态化标准。

除了这些内部资产，还应当关注可能存在的相关外部资产，例如主机上业务应用相关的源代码、运维文档等是否被员工私自上传到了 GitHub、百度文库上，相关运维人员的邮箱账户等个人信息是否被其他泄露事件牵连，存在潜在的撞库风险等等。外部资产的发现能力，严格来讲不属于 HDR，大都需要其他产品或情报能力相配合，但“收敛潜在的攻击暴露面”这一思路，在资产发现关键环节应当贯穿始终。

三、检测能力

传统的 HIDS 主机安全产品，其检测重在防病毒、主机加固、白名单等“预防性”的能力，在这些传统能力的基础上，HDR 产品需要在攻防演练与日常安全运营中满足用户逐渐产生的新需求，例如结合情报的脆弱性检测、基于基线的攻击入侵检测等、内存安全检测、容器安全检测等。

1、结合情报的脆弱性检测

脆弱性检测针对的是可能被威胁所利用的资产或若干资产的薄弱环节，就 HDR 而言，主机侧的脆弱性检测一般不采用 PoC 类的检测，而是以版本匹配为主，因此，针对漏洞、弱口令等脆弱性检测应当与外部威胁情报重点结合来开展。

举例来说，当出现类似 Struts2、Log4j 等影响范围较大、危害较为严重的漏洞时，HDR 产品如果得到及时准确的漏洞情报赋能，精准匹配并检测出潜在受到最新漏洞威胁的主机资产，就能先于潜在攻击者对风险资产做出处置。

当然，主机侧对脆弱点的处置，特别是漏洞的修复，会业务系统的连续性、稳定性等为重要前提，因此，在主机侧，HDR 产品也需要漏洞白名单、虚拟补丁、热补丁等能力。

近年来不断升级的攻防演练场景中，脆弱性检测是红蓝双方在演练开始前就已重点关注的战场。不夸张的说，演练结果如何，在这个阶段就已经能够决定。

此外，HDR 的脆弱性检测还应当注意检测的策略、强度、时间周期等。虽然相比网络侧发起的脆弱性检测，主机侧的脆弱性检测本身精准度更高，对网络性能的影响更小，但考虑到扫描行为对资源占用、对业务的影响，仍应采用较低频度、较低资源占用的策略配置。

2、基于基线的攻击入侵检测

作为攻击入侵检测的最后一道防线，主机上的 HIDS 能力虽传统但不可或缺，对于安全团队能力较强的甲方用户而言，HIDS 是分析诊断、应急响应等后续其他能力发挥价值的前提。因此，HIDS 除了要具备深入理解操作系统，监测隐蔽攻击行为等能力外，还应当与安全运行基线相结合。

数世咨询在调研中发现，无论是自建较强安全团队的甲方用户，亦或是在攻防演练对抗中协助甲方取得较好成绩的乙方团队，其攻击入侵检测之所以能够实现精准告警，共同点都是提前进行了至少一个月的安全基线梳理工作，进而通过 HDR 产品或其他自动化手段，有效降低“噪音”减少了误报，显著缩短了安全团队的 MTTD/MTTR。

在实现安全运行基线梳理的基础上，HDR 攻击入侵检测的相关能力中，用

户应当重点考察：

（1）系统完整性监测

基于已形成的安全基线，对关键进程、核心数据、证书文件、高权限账户等重要目标进行重点监测，一旦发现异常行为，立刻告警通知相关人员。

（2）横向移动检测

如果攻击者通过个别盲点资产或分支机构资产，成功“打点”进入内网，入侵行为开始由典型的“侵入者”转变为横向移动的“潜行者”。隐蔽与仿冒，是横向移动时的典型特征。此时的入侵检测，应当重点关注 RDP、SMB、DCOM、哈希传递、票据传递等行为，此外，对会话劫持、文件共享攻击、软件升级分发等相对较容易忽略的潜在风险点也要关注到。

（3）兼容性与可扩展性

以上各项能力，都需要针对业务环境中不同操作系统的不同版本，通过大量的兼容性测试，保证其兼容性，同时应当拥有成熟的 API 接口，能与 CMDB 等其他系统进行联动，从而满足稳定运行、自动协同等需求。

3、内存安全检测

如果说主机安全是网络安全的最后一道防线，那么内存安全就是主机安全的最后一道防线。近两年在红蓝对抗攻防演练中，0day、内存马、无文件攻击等威胁越来越多，HDR 能力企业先后开始在产品中加入内存安全能力。

内存安全检测，即通过对内存写入、内存读取、内存执行、操作系统 API 等行为的监控，重点发现内存篡改、内存漏洞利用、恶意代码执行等内存攻击行为。同时，用户业务场景允许的情况下，还应对 MBR 引导扇区、内核完整性等进行校验，对内核隐藏进程进行监测。

值得一提的是，内存马等无文件攻击行为，顾名思义，文件不落盘，我们必须在系统运行时，将内存中细粒度的异常程序行为点关联结合，形成攻击链，

才有可能有效发现内存中的威胁。这就需要 agent 在多个关键行为采集点实时采集系统行为数据，并以此为基础，结合攻击行为模型，实现对已知威胁与未知威胁同等的检测能力。

4、容器安全检测

容器的安全检测重点关注容器镜像完整性与运行时状态的监测，主要覆盖容器构建、容器部署以及容器运行三个阶段。

对于前两个阶段，容器的构建与部署，主要通过镜像安全扫描、镜像签名、安全配置基线检查等等方式解决。第三个阶段——容器运行时的威胁检测与防护，首先要关注容器运行环境的安全，例如宿主机安全、容器应用、负载均衡等；其次关注运行时容器本身的安全检测。

目前行业内主流的实现方案有两种：特权平行容器方案与宿主机 agent 监控方案。平行容器方案能够充分利用容器天然的隔离性与良好的资源控制能力等特点；宿主机 agent 监控方案则类似于“上帝视角”，以更高的维度对容器行为进行监控。

两者针对恶意镜像启动、容器恶意程序、容器入侵行为、容器逃逸行为、异常特权容器等行为均有不错的监控效果。用户可以针对自身实际需求，选用不同的方案。如果是已经部署了主机安全 agent 的用户，且供应商 agent 具备容器监控能力的情况下，自然可以选用后者即宿主机 agent 监控方案。

容器安全并非本报告的重点，未来数世咨询也会专门撰写容器安全相关内容，更多详细能力这里不再赘述。

四、响应能力

基于主机侧的安全响应与终端不同，其难点并不在于传统的攻防技术或安全服务，而在于保证业务连续性的前提下，**结合威胁情报进行准确分析与判断，**

利用 HDR 产品与各团队的协同，将传统被动应急，转变为主动安全运营。

1、结合威胁情报的分析与诊断

如前所述，agent 采集来的数据，首先要根据之前建立的主机侧安全运行基线，将占绝大多数的正常数据与噪音筛选掉。之后对于疑似异常数据，结合威胁情报，进行初步的自动化分析。对于较为典型的恶意行为，结合既定策略，可直接转入 HDR 产品处置。对于更高复杂度、需要人工进一步分析的，则应当在最短时间内定位到可能失陷的主机，连同相关数据与处置建议，交给安全运营人员。

这个过程中，提升“自动化分析”的检测准确率（缩短 MTTD），能够为后续提升响应时效（缩短 MTTR）带来非常大的助力。因此需要在前期进行精准的资产清点，有效收敛攻击暴露面，其次要结合资产的业务线、优先级、所属相关部门及责任人，为一定程度的自动化分析与响应提供扎实的判断依据。此外，对于核心业务主机，自动化分析之后，仍然要交由人工进行最终研判。目的还是为了即不影响业务连续性，同时又能尽量快速稳妥的做出响应。

就 HDR 所需的威胁情报而言，在调研中，我们发现几乎所有厂商都在努力扩充自己的威胁情报来源，构建海量、优质的多源威胁情报能力。此外，企业除了自建、商业合作以及从开源渠道广泛收集外，一个重要方面是来源于用户，特别是当百万台级别的海量主机同时采集数据时，主机本身就成为了有效的威胁情报来源。一旦确定情报无误，用户就能够实现快速情报分发、快速响应。

这里额外要提到的是，在实网攻防演练场景中，云蜜罐、微蜜罐等欺骗诱捕类产品，也是主机安全所需的重要情报来源。蜜罐中捕获的攻击行为及相关日志信息，能够有效提升分析诊断的准确度与可信度，如果蜜罐中具备一定的反制功能，还能为溯源提供有力帮助。

2、HDR 产品与各团队的协同

主机侧的安全响应有其特殊性——不影响业务连续性，这一点在本报告中已经不厌其烦多次提及——因此，主机侧的安全响应，一定要能够通过 HDR 产品与业务、网络、运维等兄弟团队进行同步、协同，这是 HDR 响应能力的重点。

可视化

可视化是主机侧安全响应的基础，资产清单、网络拓扑、攻击暴露面等都需要直观、动态的可视化，与安全、网络、运维乃至业务等各部门进行同步。例如，通过网络拓扑可视化，可以将主机、系统、应用、服务之间的沟通关系描绘清楚，使网络与业务间的对应关系充分可见，这是后期安全响应能不能做、如何做、是否能守住不影响业务连续性这条底线的基础工作。

核心业务

以可见性为基础，优先对核心业务关键应用，特别是核心业务主机涉及到的虚机、容器、系统、应用等安全策略设置最高优先级，后续有任何涉及核心业务的疑似攻击、甚至策略变化请求，都应当以高优先级告警自动触达业务负责人、运维负责人、网络负责人、安全负责人共同研判后进行响应。

灵活维护策略

基于前面两点，随着业务变化或 IT 环境的变化，HDR 产品应当能够自适应调整发布到主机的策略。灵活自适应的策略维护能力能够减少各部门间的沟通成本，减少人工疏漏及犯错的可能。各团队只需要在策略配置初期达成共识，后期的策略自适应调整始终遵循共识即可。

丰富的报告

HDR 产品要能够自动化生成内容丰富的报告，成为事前、事中、事后各项工作特别是文档方面工作的加分项。如果报告能够体现出与业务的结合，那就更好了。如果没有一个与业务充分结合且通俗易懂的报告，挖再多的漏洞，抓再多的木马，也难以体现出安全的价值，更难获得其他部门的认可与配合。

本身的安全性

主机安全产品链接所有服务器，自身的安全风险是最高的，因此，主机安全产品本身的安全性是一个必须要重视的能力点：

（1）agent 安全性

除了前面提到的稳定性、资源占用率外，用户还应当测试 agent 能否被绕过，模拟高权限账户能不能把它干掉，agent 所采集数据的存储、传输等环节的安全性也要充分考虑。

（2）服务端安全性

管理平台一侧，除了对管理界面、访问接口等关键点进行重点漏洞挖掘测试外，有条件的话，应当对管理平台与 agent 的通信过程全程加密。在调研过程中，数世咨询也看到有的能力企业通过 ORM 数据库框架、MVVM 前端框架、OSS 对象存储框架，从实现机制上避免 SQL 注入、XSS、目录遍历、任意文件上传、下载等常见安全问题。另有企业会在服务端使用容器化部署，由系统沙箱提供基础的隔离机制，满足资源隔离需求，有效控制服务端代码的权限范围。以上都是针对管理平台的有效安全手段。

总之，自身足够“硬”，兄弟部门才会放心。

3、基于主机侧的安全运营

从威胁检测到应急响应，从分析诊断到部门协同，前述各项产品能力要结合“人”形成安全运营能力。基于主机侧相对稳定的业务、运维、网络环境，本报告建议以主机资产为核心，以事前收敛、事中控制、事后追溯为原则，结合威胁情报能力，实现一定程度标准化的预防、检测、响应闭环。

事前收敛，攻击面收敛与告警收敛相结合。攻击面收敛前面已经讲过，这里不再赘述，只说告警收敛。告警收敛是指在做好主机侧资产发现与管理的基础上，通过一段时间（一般至少一个月以上）的运行梳理形成安全基线，同时将各告警信息源进行识别归类，结合业务优先级、安全基线、告警日志等，以

事件的角度对不同的告警信息进行聚合判断，过滤掉无效告警，只留下有效告警。目的是为后面的事中、事后步骤去除掉大量的噪音，让安全运营人员只集中精力处置有效告警事件，不必手动在海量告警信息中进行溯源。

事中控制， 智能化判断与人工阻断相结合。前面提到过，目前 HDR 各个能力点中相对的短板是响应，而响应的短板就在阻断。综合大厂有实力通过多个专家团队对告警信息进行分析判断，继而做出响应阻断。而初创团队则尝试以人工智能的方式，结合多点多维度多引擎的检测数据，对恶意行为做出智能化判断后，再交由少量人工进行阻断，从而帮助用户有效提升 MTTR 的时效。值得一提的是，对于部分“重安全轻业务”的行业或红蓝对抗演练场景，用户正逐渐接受一定程度的自动化阻断，方式是通过能力企业的“内存实时防护”等具备较高可靠性的恶意行为检测、分析与判断能力来实现。

事后追溯，标准化分析与可视化溯源相结合。在发现威胁并进行阻断后，溯源工作主要依靠各类日志、流量，辅以威胁情报综合分析进行溯源。相比多样化的 PC 机环境，主机侧的溯源有更大的标准化空间，例如对于相对更加稳定的数据中心等场景，可以根据前期形成的基线环境，结合资产视图、拓扑访问关系、异常流量等可视化手段，进行快速溯源。这样一来，无需专业的安全分析团队，只需要相对基本的网络知识与安全知识，即可形成标准、高效的事后分析溯源能力。

安全运营，形成熟练的威胁检测与响应流程机制。对于主机资产数量庞大、安全团队能力较强的用户，可以依托用户的自建平台，建立“平台、工具、人”相结合的运营流程。对安全团队规模不大、能力较为有限的用户来说，ROI 较高且行之有效的方法是参照 ATT&CK 等标准化框架，根据自身实际业务情况，结合目标系统或目标数据所在的主机环境，确定检测、分析、阻断、留证等动作与所需的安全工具包，并指定相关负责人，建立检测与响应的流程机制。然后就是反复演练、优化、完善，并不断重复循环这个过程。无论哪一类用户，采用哪种工具、平台或框架，事中控制的关键是让整个流程真正跑起来，最理想的状态是形成团队的“肌肉记忆”，才能在与攻击者拼时间的对抗中不断缩小差距。

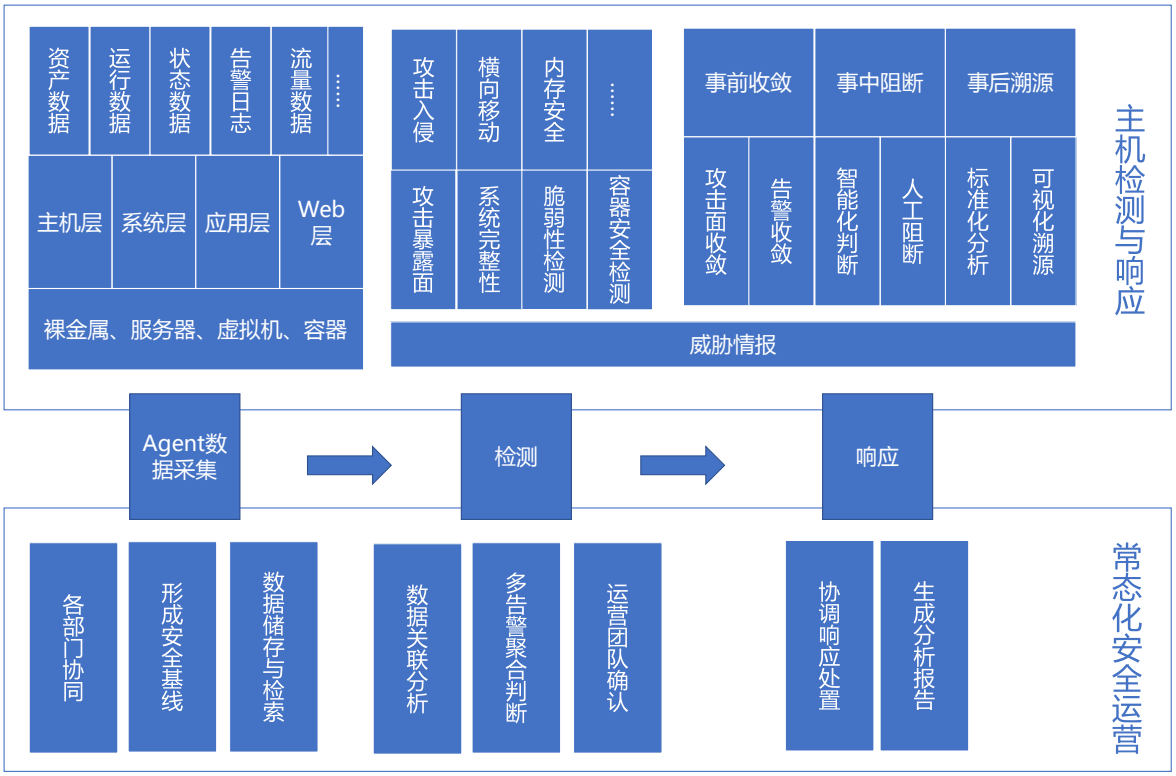

图 3 主机检测与响应（HDR）形成常态化运营能力

第五章　落地难点

用户业务连续性与 agent 的接受程度负相关。ToC 业务（互联网业务）技术开放较前沿，对 agent 这种形式相对比较好接受；ToG 业务（政府业务）受等保合规要求驱动，只要合规需要，直接就能装；相比之下，占大多数的 ToB 业务（行业应用）最担心业务受影响，对 agent 最不好接受，始终都心存较大疑虑。虽然经过近几年红蓝对抗攻防演练的实战化市场教育，这方面有所改善，但是业务、运维等兄弟部门的阻力与质疑始终是存在的。

主机侧的自动化响应还难以在各行业大规模实现。除了对安全格外重视的用户、以及短时间的红蓝对抗演练场景外，主机侧始终都是以重点保障业务连续性为第一要求的。因此，即便近年来，不少初创团队以人工智能、内存安全等不同维度为抓手，有效推进了自动化响应的落地，但在相当一段时间内，仍然很难推广到全行业，特别是运营商、金融、电力等对业务连续性要求极高的行业。安全与效率将始终是一对“冤家”。

用户的定制化需求较多，且难以满足。由于主机与几乎所有业务相链接，因此主机环境的变化非常大，哪怕同一行业，甚至同一用户的不同分支机构，对主机安全的要求都会有区别。例如，分子公司较多时，不同的分支机构业务特点，需要出具各种不同的报表，有些报表是给其他部门的运维工程师沟通用的，然而目前各家企业普遍的报表能力从时效性、业务贴合度来说都较弱。

除了业务区别，技术上也有些难以落地的定制化需求，例如安全团队能力较强的用户会参考 CWPP 体系，在主机侧使用 HDR，在办公网 PC 环境中用 EPP/EDR，两者是分开的。但对于能力相对较弱的用户，可能会想把这两类产品“合二为一”，例如在主机上加入 EDR 类似“自动化修复”这样的功能。这种将 HDR 与 EDR“合二为一”的定制化需求目前来看都是难以落地的。

第六章　未来发展趋势

市场供需方面，HDR 的未来会呈现需求与投入双增长的态势。

如前所述，行业用户采购主机安全产品及解决方案的三大驱动力：第一合规，网络安全法、等保及关基条例中，均对主机安全有明确要求；第二上云，新冠疫情等客观因素加速了业务上云后，多形态云主机安全能力提升的需求；第三实战化红蓝对抗攻防演练中，主机安全成为最后一道有效防线。因此，从需求角度来说，这三大驱动力决定着安全体系中，主机安全成为必备，而传统的主机安全需求正向虚拟机、容器等云环境转化，需求还会大幅增加。

以金额行业为例，除了传统清算、核心系统，暂不能安装 agent 外，应普惠金融要求，农业贷款业务、中小企业贷款等业务现在都往线上迁移，因此，未来的一大趋势就是增加互联网业务，降低网点比例。预计 3 年内，国有六大行 50% 的业务，12 家股份制银行 60-70% 的业务要上云。计划 8 年后，全部都上云，包括非金融交易业务、客户系统等，也都上私有云。目前保守估计全行业主机安全的 agent 装机量还不到三分之一，因此数世咨询认为，HDR 的需求会大幅增加。

另据本次调研，金融行业中，头部金融机构每年的 IT 预算占其年营收的 2%-3.5%，安全预算占 IT 预算的比例则 5% 左右，这其中主机安全投入占整个安全投入的 10% 左右。假设以年营收 1000 亿人民币、IT 预算占比 2% 为基数计算，该机构在主机安全方面的投入即可达到 1000 万人民币。当然，并非所有的金融机构年营收都能够千亿以上，且 1000 万的主机安全投入也多以 2-3 期分期建设完成，但足以从用户侧显示出该细分领域市场的火热。同时，疫情之后的远程办公、远程服务、智能客服等业务都大幅度增长，因此数世咨询认为，主机安全的投入增长占比还会进一步升高。

技术能力方面，内存安全能力将成为标配。

对于主机数量庞大的用户群体，若要实现一定程度的自动化阻断能力，需要检出率、准确率更高的恶意攻击行为发现能力，以及可信度更高的攻击行为判别能力。结合前文提到的 HDR 的各项能力，再辅以内存安全的实时检测与阻断能力，这一需求已经能够在部分“重安全轻业务”类型用户中得到有效落地。例如，对内存中的内存马、无文件攻击等新的攻击形式，内存安全检测成为近两年实网攻防演练中的必备能力；同时，疑似攻击行为在内存中一旦形成攻击链条，会具备更高的可信度。因此我们说，内存安全能力将逐渐成为 HDR 中的标配。

应用场景方面，实战化对抗场景仍将是主流。

随着红蓝对抗实网攻防在用户侧常态化演练越来越多，业务、运维等兄弟部门对 agent 接受程度也会越来越高；主机侧的自动化响应能力逐渐增强，特别对安全格外重视的行业，一定程度的自动化响应能力会越来越多得到应用；威胁情报的作用与地位会进一步凸显；最后，各类框架体系中不同安全产品与技术融合的趋势也会逐渐明朗，例如面对越来越多的 0day 攻击，HDR 与入侵攻击模拟、安全有效性验证等新赛道技术手段的融合将在未来 1-2 年内迅速兴起。

总体来看，HDR 将与 EDR 趋于整合。

现在的落地难点就是未来的发展趋势。用户侧对 HDR 提出的自动化响应等类似 EDR 的需求虽然暂时无法得到满足，但代表了未来 HDR 发展的某些技术可能性。也就是说，主机外其他类型端点的安全能力，将会大大促进 HDR 的能力提升，进而推进 HDR 的普及与落地。不远的将来，各类端点侧的安全能力，都将整合为一体化的端点安全能力。

综上所述，数世咨询会持续关注 HDR 主机检测与响应。

第七章　应用案例

一、某大型企业主机检测与响应平台建设项目

本案例由青藤云安全提供

1、场景介绍

在数字化转型的背景下，大型企业业务上云加速，但是也打破了原来相对封闭的业务网络，业务变得更加开放和灵活。主机承载了企业越来越多的业务资产，成为攻击者的主要目标，企业安全对抗和管理核心逐渐从边界转移至主机系统内，攻击者通过各类工具利用系统脆弱性突破企业防线，入侵主机内部完成攻击目的。因此，大型企业对主机的持续检测和响应能力需求迫切。
本项目打造了一套符合大型企业需求的主机安全检测和响应体系，构建与现有安全工具协同工作的防御体系架构，以降低入侵成功可能性，缩短恢复和处置时间，提升企业的主机安全能力。

2、客户需求

全面细粒度的资产可视化

企业信息化业务发展迅速、资产剧增。因此客户需要持续进行系统监控和分析，获得实时详细的资产信息，从而更精准地进行风险评估和威胁预测。

入侵威胁的持续检测能力

传统基于报警或已存在的威胁特征的检测技术，在应对未知威胁过程中存在检测技术单一、缺乏持续检测、无法进行联动等不足，因此客户需要持续检测分析服务器上的各种行为，打造全面立体的防御体系，及时发现外部和内部的各种入侵攻击行为。

未知威胁的快速响应能力

从攻防实战演习可以看出，无法保证系统完全不被攻击，入侵后的快速响应能力才是关键。客户需要提高风险事件的研判、溯源和响应处置的效率。

3、解决方案

根据大型企业客户的安全建设需求和实际业务现状，解决方案重点要满足以下三个需求：

（1）解决大型企业资产数量大、变化快、结构复杂情况下的资产清点难题

对客户网络环境内的主机资产进行有效清点和管理，提高大规模集群主机的管理效率、清点细粒度、自动化程度，减少人工介入。

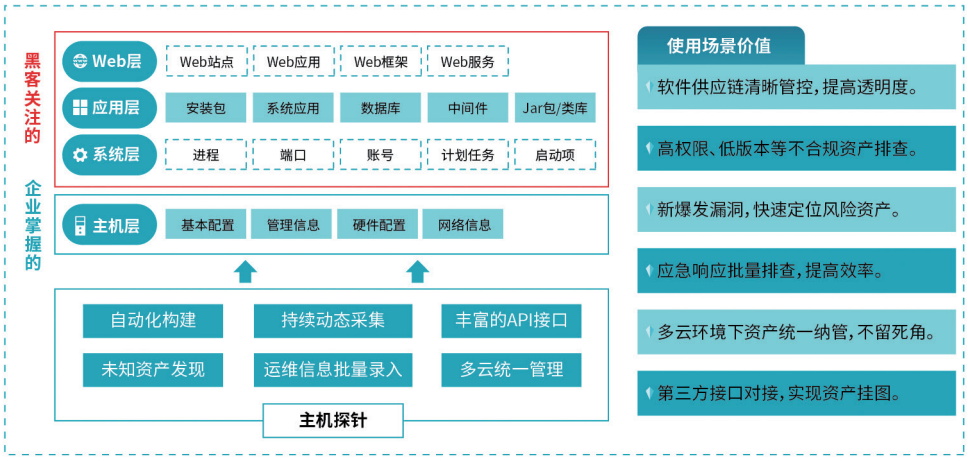

图 4　基于主机的资产清点能力

该方案帮助客户从安全角度自动化构建细粒度资产信息，让保护对象清晰可见。

- 15 秒内自动化构建资产信息。
- 资产变化实时通知，并支持灵活快速检索定位。
- 支持本地环境、云环境等混合业务架构下的资产清点。

（2）建立集防御、检测、响应和预测于一体的主机自适应安全防御体系

通过细粒度、多角度、持续地监控和分析，以智能、集成和联动的方式应对各类攻击，实现持续监控、持续防护威胁的安全运营。

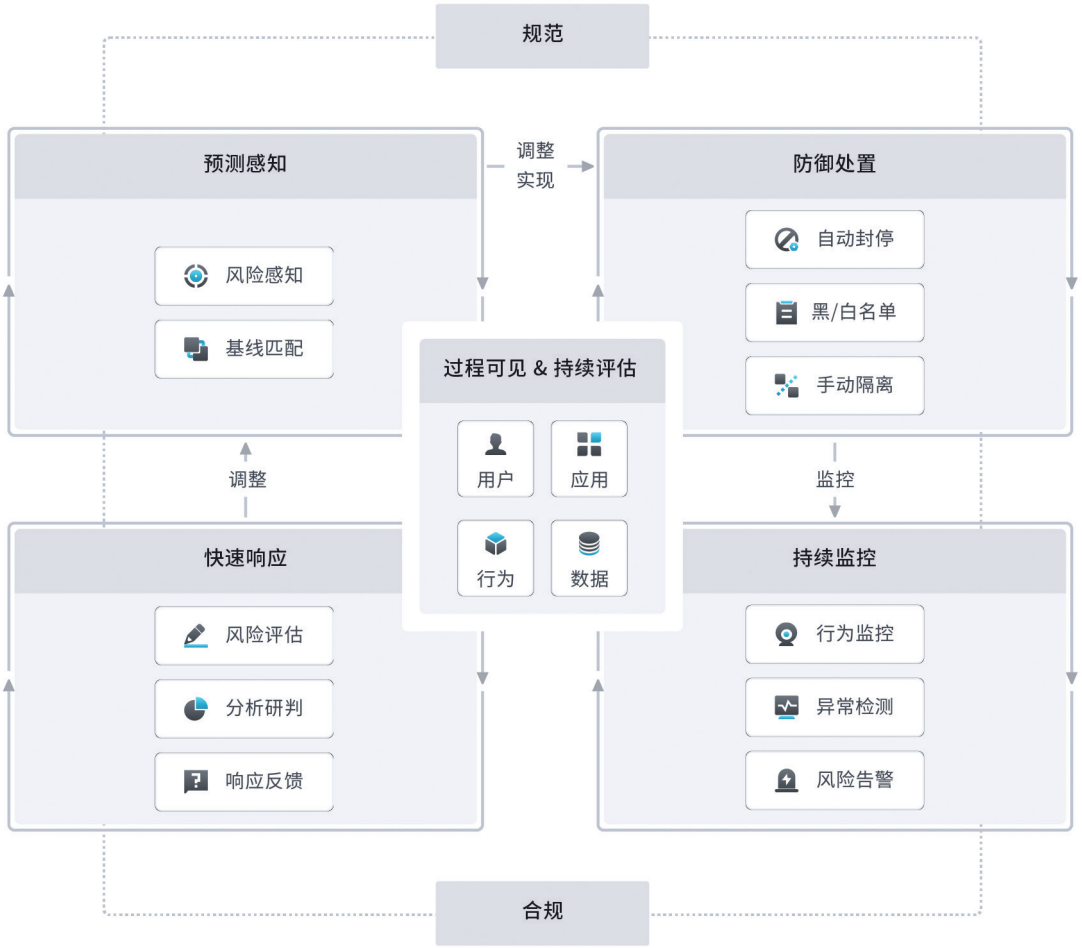

图 5　基于主机的多锚点入侵检测能力

该方案提供多锚点的检测能力，并提供对入侵事件的响应手段，对业务系统＂零＂影响。

- ◆ 对攻击路径的每个节点都进行监控，实时发现并响应威胁。
- ◆ 基于异常行为持续监控分析，有效应对各种未知黑客攻击。
- ◆ 通过攻击行为分析提高检测能力，降低误报率。

（3）加强威胁研判、溯源、分析、响应能力

通过威胁狩猎快速发现、确认、处置入侵威胁，实现威胁闭环管理，提高

威胁处置效率，提升主动防御能力，达到安全的可管、可控、可视、可调度、可持续。

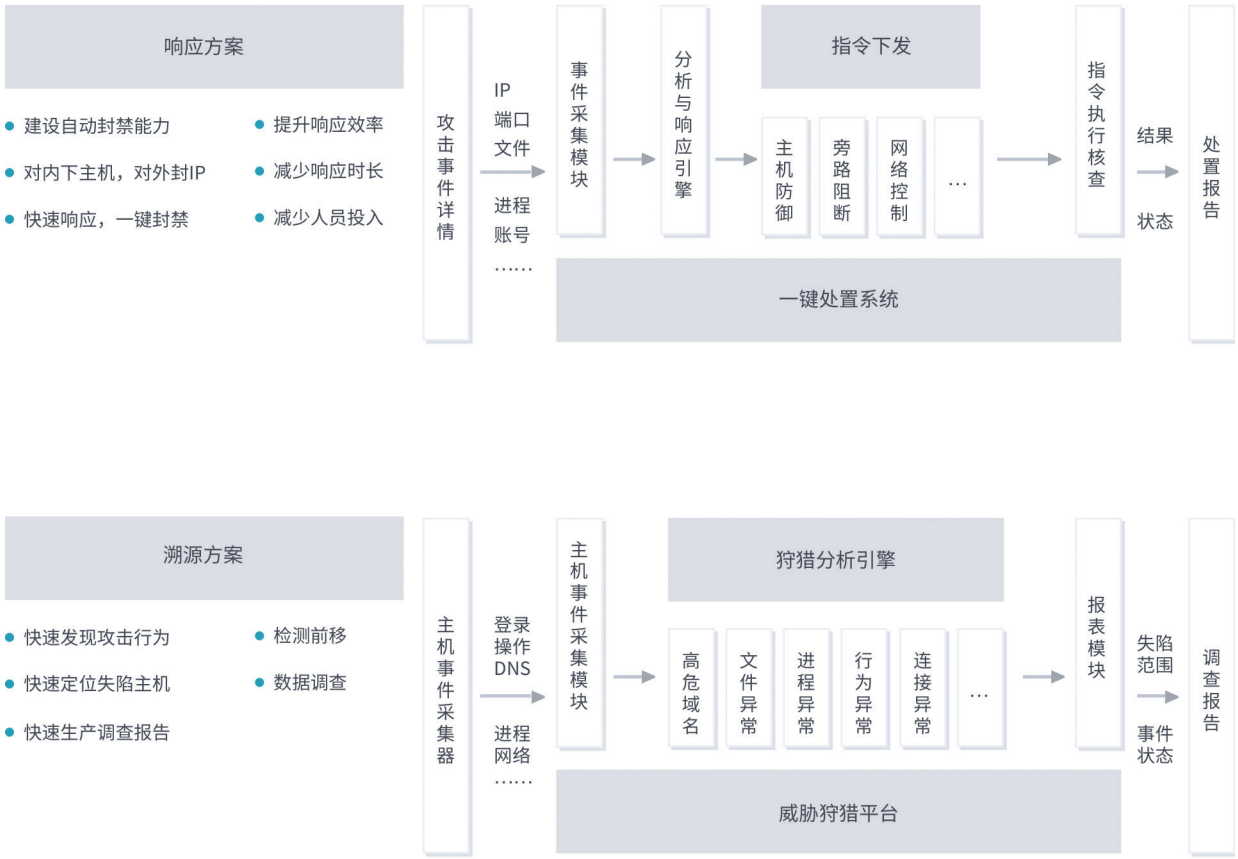

图 6　基于主机的主动防御能力

该方案能够及时发布安全事件和处置指令，做到监控告警、分析研判、安全处置一体化快速响应。

- ◆ 深度检测分析发现潜在的高级攻击行为。
- ◆ 实现威胁告警的快速、准确地研判。
- ◆ 对攻击及时响应处置，缩小影响范围。

4、客户价值

提高实时智能的资产可视化分析和风险发现能力

实现自动化构建并快速定位资产信息，获得重要资产实时变化通知，让客

户资产清晰可见，并与风险和入侵事件自动关联，提供灵活高效的回溯能力。

补齐大型企业主机持续检测和响应的能力短板

构建基于主机侧的持续检测和响应安全能力，补齐企业基于边界和流量侧的主机安全保障方式的能力短板，通过主机细粒度、多角度、持续化的实时动态检测分析，构建网络安全 2.0 时代新防御体系。

增强未知威胁、高级持续攻击的溯源响应处置能力

发生威胁告警后，对攻击事件进行快速溯源，还原整个攻击链路，做到监控告警、分析研判、安全处置一体化快速响应。同时通过异构数据统一分析，解决了单一产品能力不足的问题。

二、某政府单位主机检测与响应能力建设实践

本案例由安芯网盾提供

1、场景介绍

某政府单位经过多年发展建设，信息化业务已经具备一定规模，同时，客户十分重视系统安全性，不断完善安全防护体系建设，形成了运行状况可视、运维操作可控、安全事件可预警、威胁情报可追踪的格局，保障信息化业务安全稳定运行。安芯网盾通过实网攻防演习活动与该单位客户建立业务合作关系，客户对安芯神甲的能力验证效果非常满意，并在其业务网络主机系统部署本产品，提升业务服务器应对未知恶意代码攻击、0day 漏洞利用等高级威胁的能力。

2、客户需求

安芯网盾通过与客户紧密沟通，明确出客户在服务器安全检测与响应能力方面主要关注以下问题：

（1）传统恶意代码检测工具需要持续升级特征库，检测能力存在滞后性，难以应对新型恶意代码，**需要提升新型恶意代码检测能力。**

（2）大量难以修复的 Nday 漏洞以及可能存在的 0day 漏洞给用户单位安全防守带来较大压力，**需要补充对漏洞利用防护的能力。**

（3）内存 Webshell 基于无文件攻击形式实现，且对通信流量进行加密，现有应用安全防护手段无法有效应对，**需要加强内存 Webshell 防护能力。**

（4）客户目前运维人员有限，需要**加强精准防护和实时防护**，减少运维负担。

（5）需要**加强联动分析与溯源处置**能力，发现威胁后能够与现有的安全检测手段进行联动分析，并对攻击详细信息进行记录溯源，做到有据可查。

3、建设方案

安芯网盾团队基于多年未知威胁检测技术实践经验，结合用户实际需求，从全局出发，**构建内存层、系统层、应用层一体化的全栈主机检测与响应防护体系**，形成对全局的行为感知和关联，帮助客户在主机侧建立威胁实时检测和响应能力。

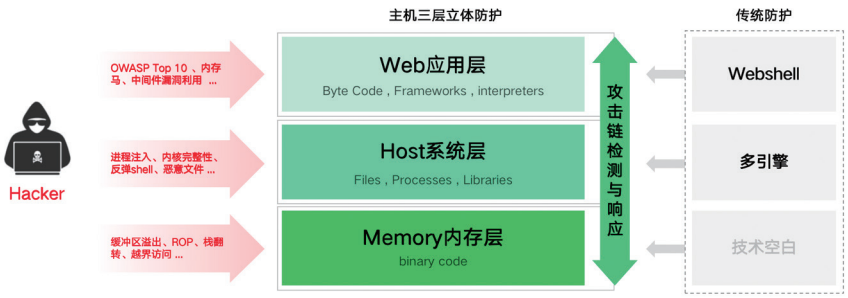

图 7　主机全栈保护能力图

客户已经对业务网络做了区域划分，并在各网络区域边界部署防火墙，通

过细粒度的访问控制策略来实现对网络和区域边界的访问控制。业务服务器主要分布于三级业务区和二级业务区，少部分服务器位于 DMZ 区。安芯神甲由控制中端和客户端组成，控制中心部署在安全管理区，客户端覆盖全部网络安全等级保护定级在三级以上的业务系统服务器以及部分二级业务系统服务器。

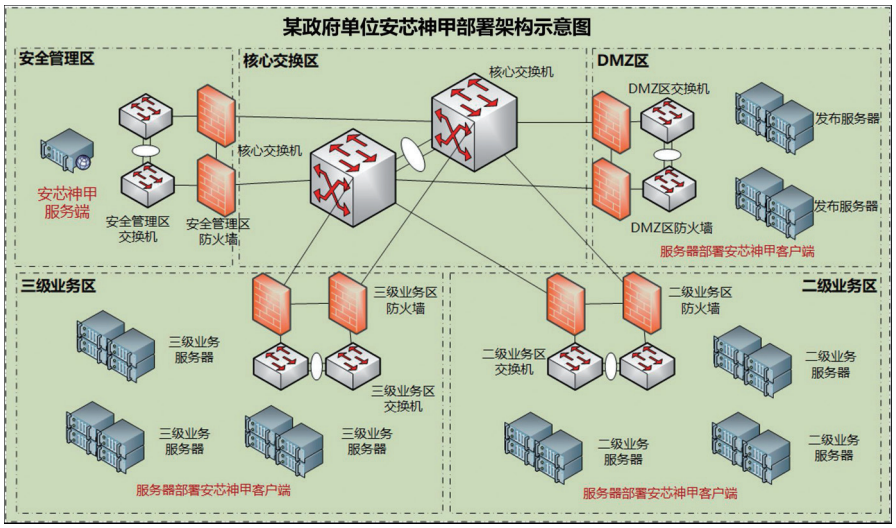

图 8　部署架构图

通过详细调研用户信息系统的业务特点及重要程度，结合用户实际工作要求，对服务器进行分组分类，也制定了不同的安全防护策略，实现不同要求的安全保护。

核心业务系统：核心业务系统防护策略以检测能力作为重点，告警信息以人工研判处置为主，最大程度保障业务系统的安全性和稳定性。

重点业务系统：采用检测和拦截相结合的策略组合模式，由检测缓慢向拦截过度。对外提供服务的 Web 应用系统开启 RASP 功能重点保护。

一般业务系统：系统使用频率较低，服务短时间不可用不会造成较大影响，对于这类系统，在检测模式下自学习后完全开启拦截策略模式，降低安全运维工作压力。

4、客户价值

与传统的主机安全防护手段相比，本方案具有以下价值：

（1）打造主机立体防护理念

构建覆盖内核层、系统层和应用层有机结合的立体防护体系，通过对内存访问行为、程序运行行为进行细粒度的监控，检测异常行为，有效识别内存破坏攻击、内存马攻击等高级威胁，构建系统运行时安全防护。

（2）有效防护未知威胁攻击

以内存保护技术为底座，以行为分析技术为核心理念，通过检测内存异常行为，结合攻击链检测与响应技术、混合感知技术，实现对已知威胁和未知威胁的无差别检测和防御能力，摆脱对特征签名、网络流量、系统日志等静态特征的重度依赖。

（3）降低安全运维运营成本

基于系统底层技术能有效提升威胁检测精确度，降低误报率，同时，系统的拦截能力也显著提升威胁事件自动化响应和处置能力,促进安全运维敏捷化、自动化、智能化建设，降低安全运维运营成本，提升运维效率。

（4）加快企业数字化转型进度

安芯神甲通过运行在系统底层和应用程序内部,获取详细的攻击行为信息，为开发人员提供更多的情报信息来改进代码，加快产品迭代效率，从而更好地推进用户单位数字化转型。

运营期间，安芯网盾践行“构建主机安全最后一道防线”的安全理念，成功帮助客户发现 OA 0day 漏洞利用攻击、哥斯拉魔改工具利用等高级威胁，有力保障用户业务主机安全稳定运行，助力用户信息化业务有序开展，获得用户的充分肯定和赞誉。

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