AhnLab

白皮书

最优勒索软件应对的综合安全策略

从近期发生的勒索软件感染事件可见，网络攻击已进入全新阶段。过去仅限于文件加密或勒索金钱的勒索软件攻击，如今已演变为伴随数据泄露、服务中断、声誉损害的复合型攻击。其影响范围也不再局限于单一企业，攻击者已从“感染后制造恐慌的存在” 转变为“渗透后潜伏的存在”。

尽管这些高度复杂的勒索软件攻击看似难以预测，但其背后存在着明确的发展脉络。因此，即便无法预知攻击发生，仍可实现可预测的应对策略。这一理念正是安博士（AhnLab）“勒索软件综合安全战略”的出发点。

勒索软件安全面临的挑战

不断进化的勒索软件攻击给企业带来了新的挑战。这些挑战虽多种多样，但主要可归纳为以下三点：

#1. 新型/变种勒索软件应对：勒索软件不断涌现的新型与变种版本令防御者束手无策。要有效应对这类威胁，必须超越单一解决方案的阻断能力，建立基于平台的战略体系——通过分析勒索软件引发的恶意行为，实现解决方案间的协同联动。

#2. 多维度防护：新型勒索软件攻击会同时出现在终端、网络、邮件等多重维度。经验丰富的攻击者为达成目的并最大化破坏，常在不同维度间穿梭实施攻击。若企业仅保护单一维度，攻击者可能绕过该区域的安全防护，或通过其他维度侵入造成损失。

#3. 建立防复发机制：勒索软件攻击并非一次拦截就能终结。类似攻击随时可能卷土重来，尤其在潜伏技术日益成熟的近期攻击中，这种趋势尤为显著。为预防勒索软件引发的连锁损害，企业必须构建超越检测拦截的安全体系，实现对威胁的追踪与预防。

安全不是通过“产品”完成，而是通过“流程”实现

为应对新型勒索软件安全挑战，企业普遍采取的应对策略是增加安全解决方案的“数量”。这一趋势不仅出现在韩国，更在全球范围内蔓延。

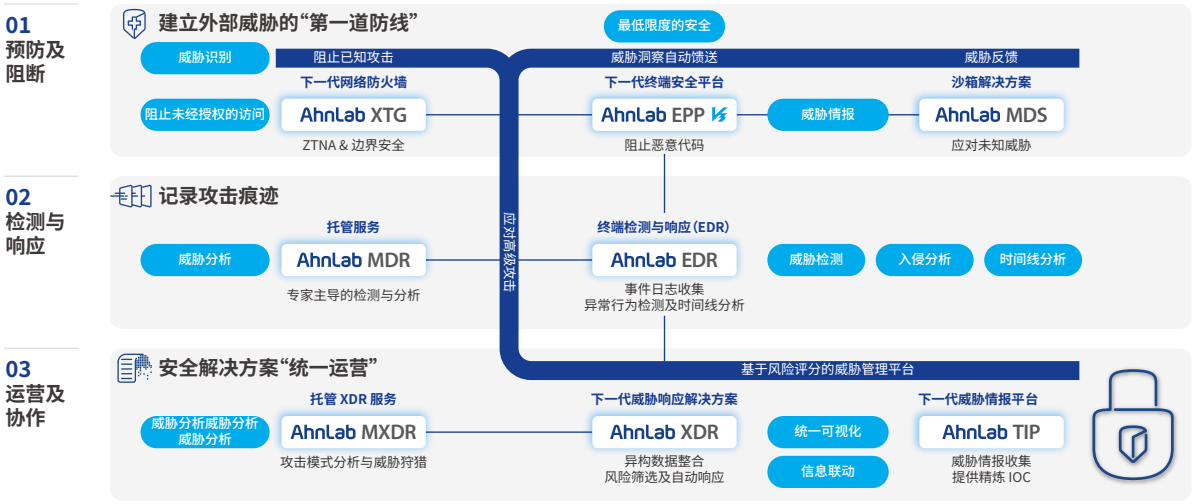
市场研究机构 Gartner 在 2024 年对全球 162 家大型企业进行的调查显示，受访者平均运行着 45 种网络安全解决方案。这一数字与 2023 年的平均值 43 个相差无几，且半数受访者坦言“未能充分利用现有解决方案”。

虽然安全解决方案的数量因企业规模、行业和国家而异，但运营困难的普遍性却是一致的。AhnLab 对实际遭受入侵的企业案例分析显示，相比于安全解决方案的“缺失”，更多企业是因“利用不足”而遭受损失。

网络安全专家布鲁斯·施奈尔曾提出“安全是过程而非产品”的经典论断。这意味着企业需突破仅导入安全解决方案进行片面功能使用的静态状态，转而投入动态努力，使安全解决方案有机协同运作，与人员形成协同效应。

最优勒索软件应对的综合安全策略

AhnLab 考虑到勒索软件攻击的高度复杂化、企业现场面临的挑战以及流程视角下集成安全的重要性，正提供基于平台的优化解决方案以应对勒索软件威胁。构成AhnLab勒索软件安全解决方案的各产品虽各自承担特定职能，但通过灵活协同运作，在流程层面形成“检测-分析-响应”的有机循环安全生态系统。该体系助力客户构建贯穿“事前防范（Prevention）- 事中检测（Detection）- 事后响应（Response）”的闭环防御体系。



[图1] AhnLab 基于平台的勒索软件安全解决方案

为此，AhnLab构建了由“下一代防火墙（ZTNA）– 防病毒（EPP）– 沙箱 – EDR – MDR – XDR – MXDR – 威胁情报（TI）”组成的联动体系。下一代防火墙通过用户与设备验证在访问阶段保障可信度，EPP与沙箱负责恶意行为检测及预先拦截，EDR与MDR承担终端行为追踪与专业分析，XDR与MXDR则负责全组织范围的统一可视化与自动响应。结合最新威胁情报，由此构建完整的安全体系。

阶段	解决方案	角色
1. 预防与拦截	AhnLab XTG	基于用户/设备验证的访问控制（ZTNA）
	AhnLab EPP (V3)	已知恶意软件检测与拦截
	AhnLab MDS	基于沙箱分析——未知恶意软件检测与拦截
2. 检测与响应	AhnLab EDR	终端事件收集、分析与响应
	MDR 服务	专家主导的终端威胁检测、分析与响应
3. 运营与协作	AhnLab XDR	基于风险评分的统一威胁管理
	MXDR 服务	跨安全层面的专家级攻击模式分析与威胁狩猎
	AhnLab TIP	提供包含入侵指标（IOC）的威胁情报

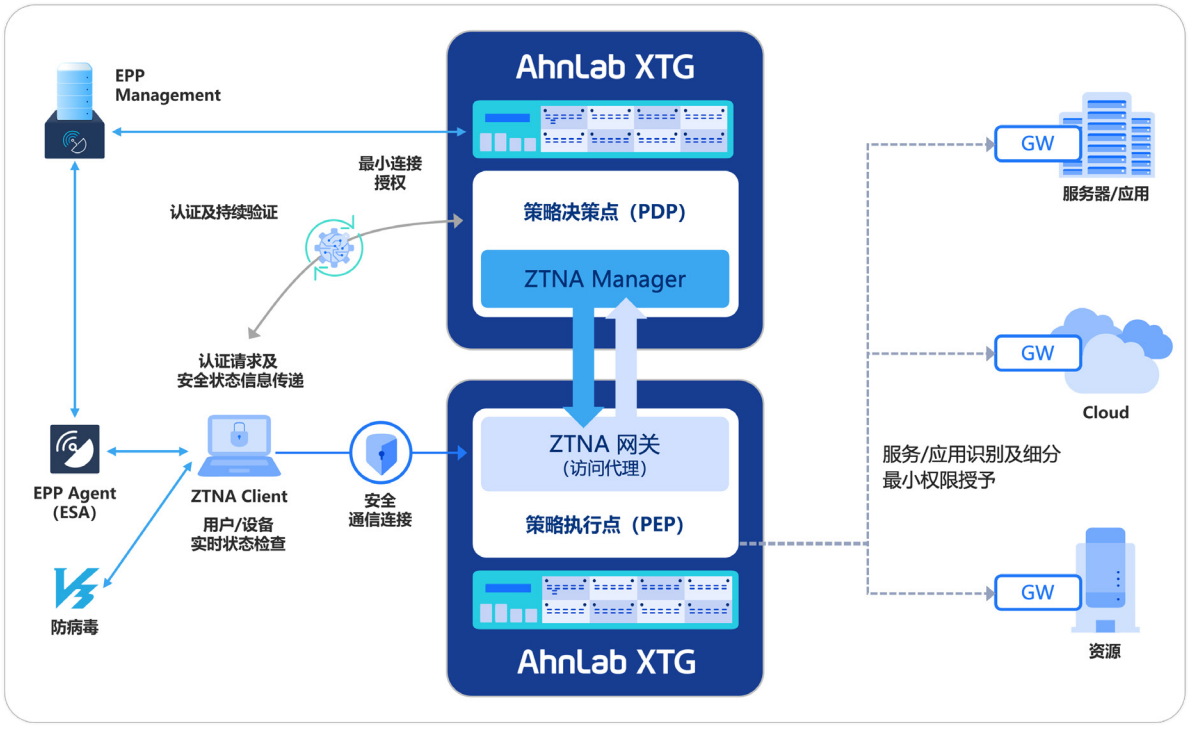
[表1] 解决方案角色分布

安全解决方案具体承担的角色如下：

第一阶段：预防与阻断——“在威胁到来之前阻止它”

① AhnLab XTG – 基于 ZTNA 的信任验证与访问控制

下一代防火墙 AhnLab XTG 是将 ZTNA（零信任网络访问）落地于实际网络运营环境的解决方案。通过与 AhnLab EPP、AhnLab V3 等终端安全解决方案联动，持续验证用户与设备身份，实现“不信任任何主体”的零信任安全模型。



[图2] AhnLab XTG - 基于 ZTNA 的网络访问控制架构

AhnLab XTG 实时管控未经授权的用户、安全状态不健全的设备以及权限超限的内部访问。在网络段落中彻底封堵内部入侵的首道关口，构建贯通网络与终端的统一访问控制体系。

简而言之，AhnLab XTG 是以“认证-权限-行为”为核心的零信任安全平台，作为“信任验证的核心枢纽”，为组织提供无视内外边界的新型威胁防御能力。

② AhnLab V3——统一安全体系的“终端第一道防线”

AhnLab V3 是企业及机构信赖逾30年的防病毒（AV）解决方案。该产品不仅具备卓越性能与技术实力，其防护能力更取决于用户操作细节——从实时防护启用、扫描周期管理到例外策略检查，远非单纯“是否安装”所能决定。即使使用相同版本的 V3，配置精细度与运维水平将直接影响安全效果。

AhnLab V3 围绕以下核心功能，精准检测并拦截勒索软件等恶意行为：

A. 基于特征码的检测

AhnLab V3 的基本检测体系由基于特征码的实时扫描（Real-time Scan）和深度扫描（Smart Scan）构成。已知恶意程序可即时拦截，可疑对象则通过追加检测判定安全状态。签名数据库持续更新，能快速应对最新威胁。

B. 勒索软件安全文件夹

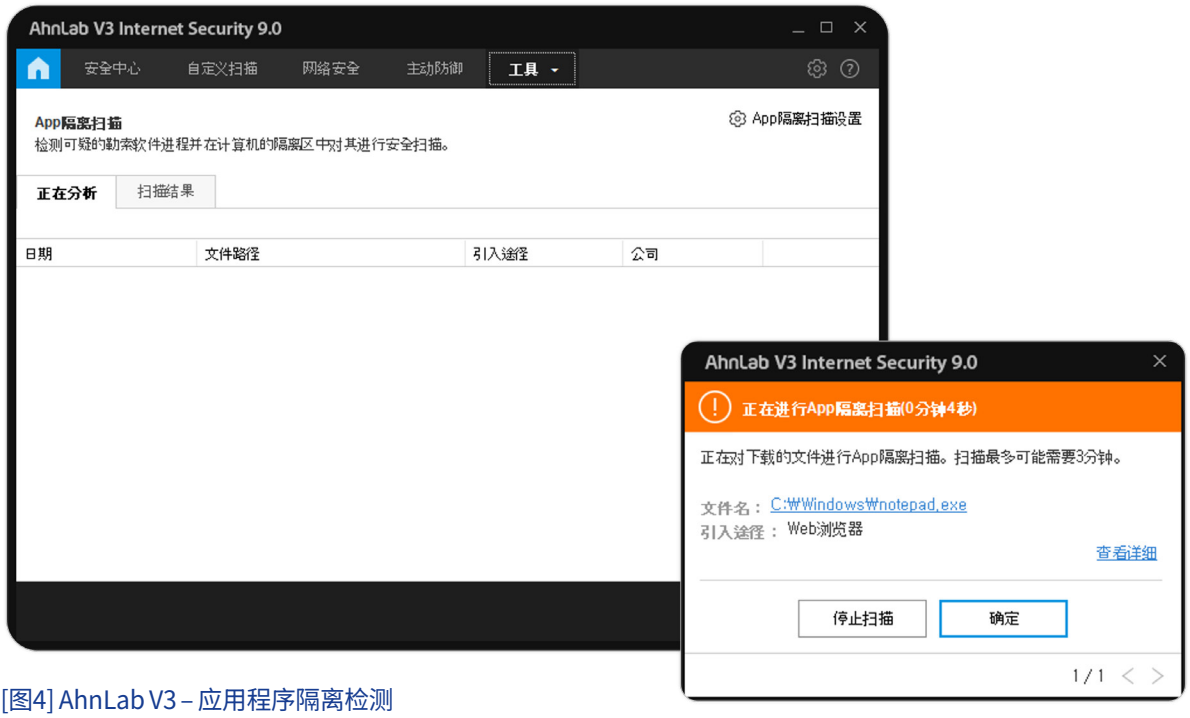
V3 用户可将必须保护的文件夹（如防勒索软件等网络攻击）设置为“勒索软件安全文件夹”。被指定为勒索软件安全文件夹的区域仅允许“受信任进程”访问。例如，若仅允许 PowerPoint 或 Excel 等正常应用程序访问，勒索软件便无法影响该文件夹。

AhnLab 观察客户的安全运营及勒索软件入侵案例发现，许多用户虽已部署 V3，却未启用勒索软件安全文件夹功能。需强调的是，该功能可在系统遭遇勒索软件感染时，有效保护重要/敏感数据的安全。

[图3] AhnLab V3 – 勒索软件安全文件夹设置

C. 应用隔离扫描

AhnLab V3 提供“应用程序隔离扫描”功能，该功能可在PC内独立虚拟环境中运行疑似勒索软件的文件，并基于行为监控技术进行检查。利用此功能，即使勒索软件侵入系统，也能在行为表现前实施检查，从而防止损害扩散。



[图4] AhnLab V3 – 应用程序隔离检测

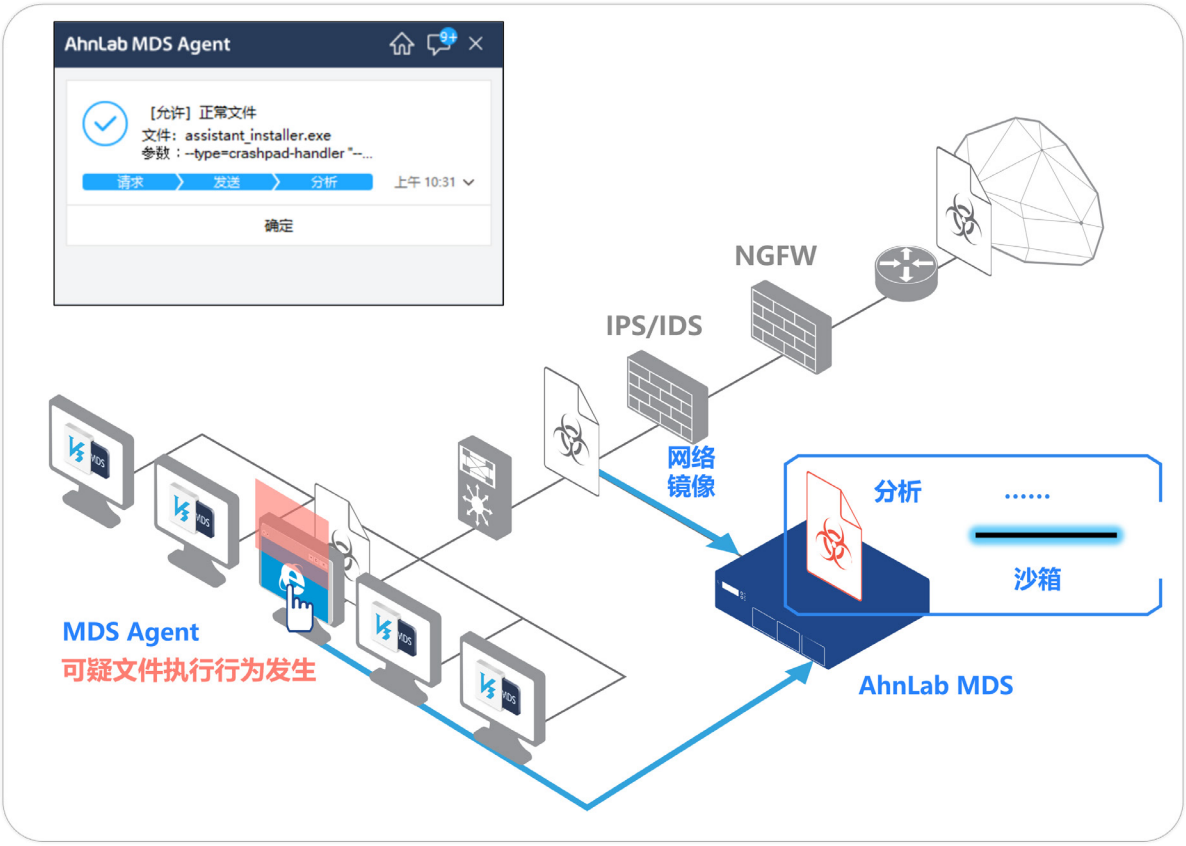
此外，若将 V3 与终端安全平台 AhnLab EPP 协同使用，可实现检测状态、策略及事件的统一管理，从而加速响应速度。EPP 不仅能监控单台 PC 或服务器，更能整合组织内所有终端的安全状态并批量部署策略。通过该平台，安全管理员可将各终端的检测事件整合为统一流程，实现策略管理、补丁状态检查、设备控制等多项安全功能的联动响应。

尤其近期 Linux 服务器环境中的漏洞与恶意软件激增，通过 EPP 实现跨操作系统统一安全管理的重要性日益凸显。同时部署 AhnLab V3 与 AhnLab EPP，既能强化终端检测/拦截能力，又能提升集中管理的效率。

③ AhnLab MDS——通过沙箱分析实现“勒索软件执行前拦截”

AhnLab MDS 是一款沙箱解决方案，能够在网络、终端和邮件环节防御未知恶意代码，并最大限度减少检测后的响应空白。

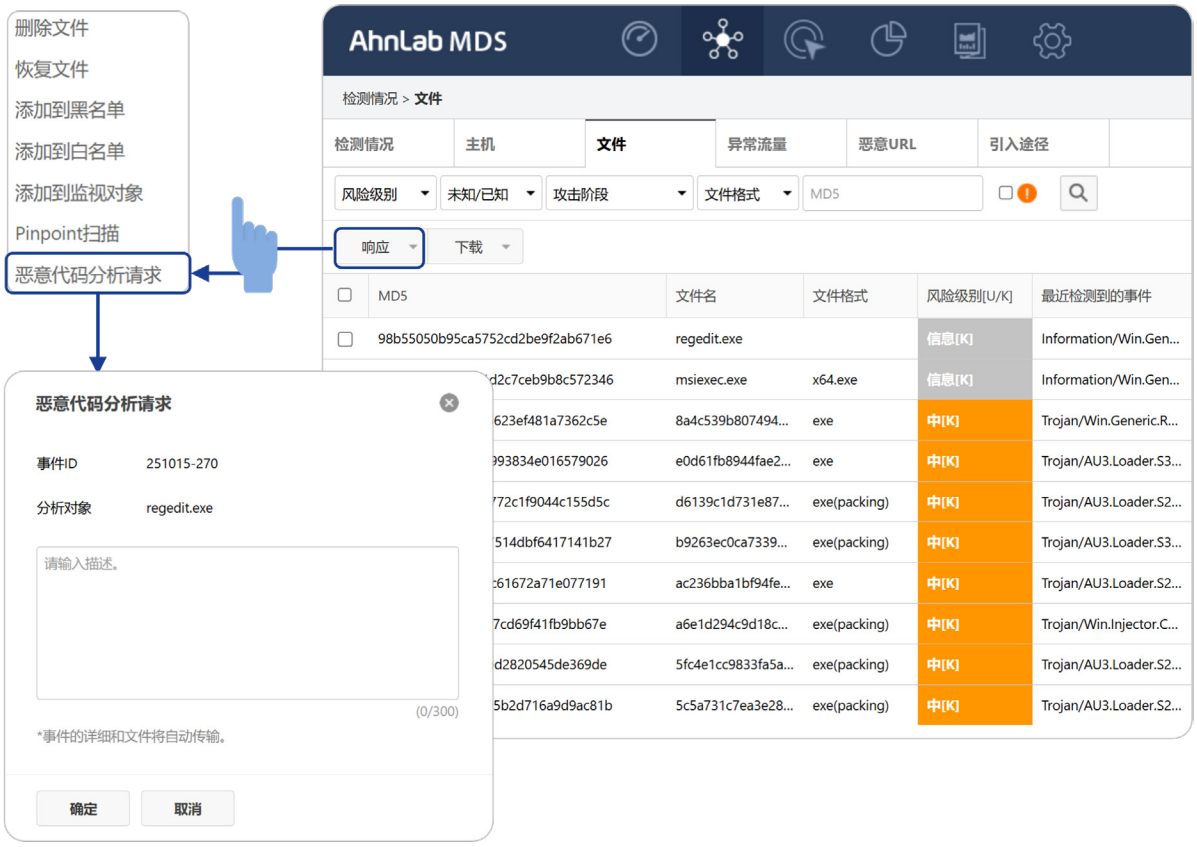
首先，AhnLab MDS 通过在沙箱虚拟环境（VM）中分析网络传输的文件和流量，执行“运行前保留（execution holding）”、“行为分析（behavior analysis）”等操作。在终端侧，如果用户 PC 检测到可疑文件，AhnLab MDS 会自动收集并在沙箱环境中观察其实际行为。如果在设定时间内发现加密、删除、未经授权访问等异常行为，将立即阻止执行。同时，分析结果会传送至管理控制台，以追踪可能受感染的其他终端并防止内部扩散。



[图5] AhnLab MDS - 基于沙箱的行为分析及执行前拦截

在邮件处理环节，AhnLab MDS 的邮件传输代理（MTA）会对邮件的标题、正文、URL及附件进行综合检测。对于正文中的 URL，系统会直接访问以判断是否存在异常；附件则在沙箱环境中进行分析。恶意邮件将被隔离处理，防止其流入系统。

此外，AhnLab MDS 还提供“恶意代码分析请求”功能，支持将内部发现的可疑文件发送至 AhnLab 专业分析师团队进行检测。管理员可通过分析报告确认威胁类型、感染路径及扩散情况，从而迅速采取应对措施。



[图6] AhnLab MDS – 恶意代码分析请求

第二阶段：检测与响应——“即使允许渗透，也要阻止扩散”

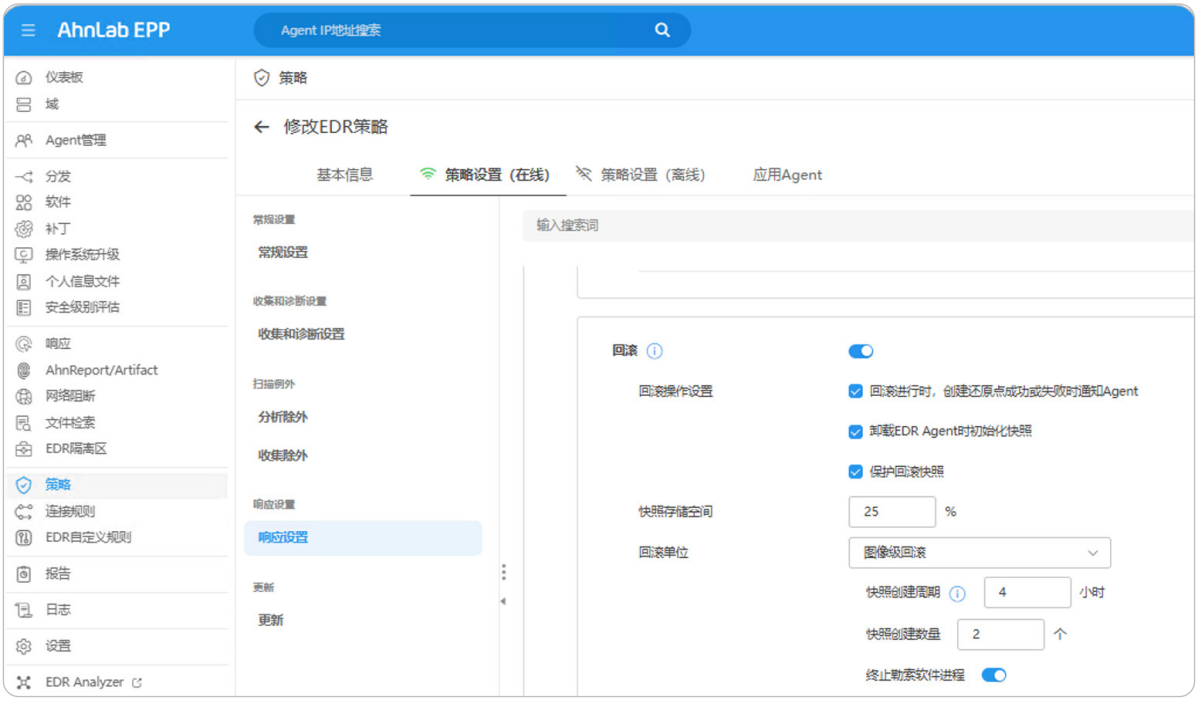
① AhnLab EDR——读取威胁“上下文”的眼睛

EDR 不只是一个简单的事件监控工具。它会以时间轴和进程链为基准，记录每个终端发生的所有行为，并通过分析攻击的上下文来重建威胁链条。也就是说，EDR 识别威胁的方式不是基于单一事件， 而是基于“行为之间的关联性” 。通过这种方式，帮助用户实现终端威胁管理，缩短未知威胁的潜伏期，并预防潜在损害及复发。

此外，EDR 还搭载了专为勒索软件防护设计的专用功能，主要功能如下：

A. 自动回滚（Auto Rollback）

该功能可将文件恢复至感染前的状态。过去需管理员手动执行回滚操作，如今通过自动选项可在检测到威胁时立即完成修复。



[图7] AhnLab EDR – 自动回滚功能界面

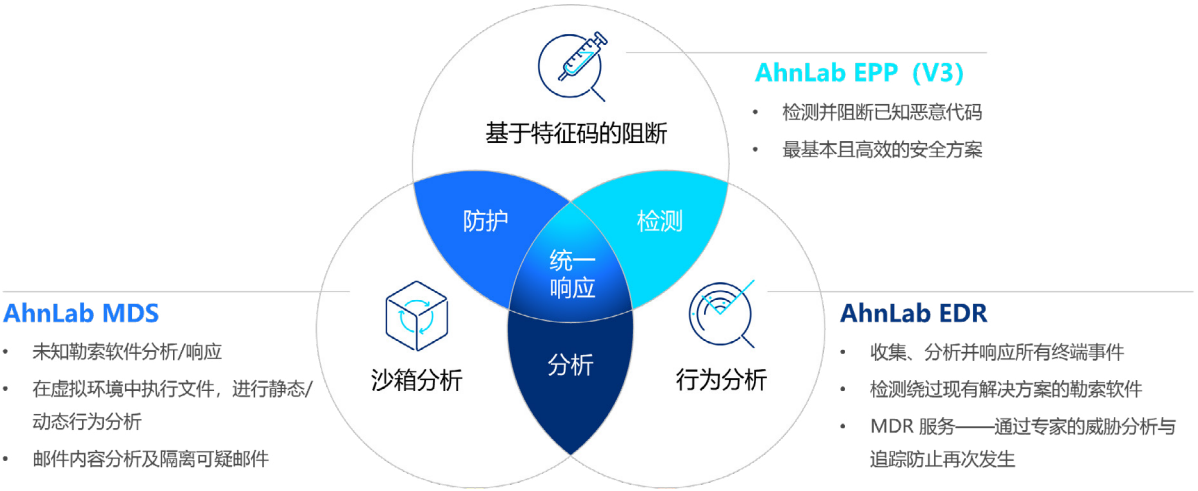
B. 安全新闻 & IOC 小组件

EDR 会自动收集 AhnLab 威胁情报平台 TIP 最新安全公告中提供的 IP、URL、哈希值等情报，并与内部日志进行比对分析。管理员可立即查看“与该新闻相关的风险终端”，从而缩短响应时间。

前面介绍的 AhnLab EPP（V3）、MDS、EDR 构成 AhnLab 勒索软件防护安全产品组合中的核心支柱：

- EPP（V3）：负责终端初级防护，
- MDS：负责“网络 - 终端 - 邮件”的行为分析与阻断，
- EDR：负责终端全事件分析与响应。

这三款解决方案灵活协同，构建了检测 - 分析 - 响应有机结合的多层安全体系。

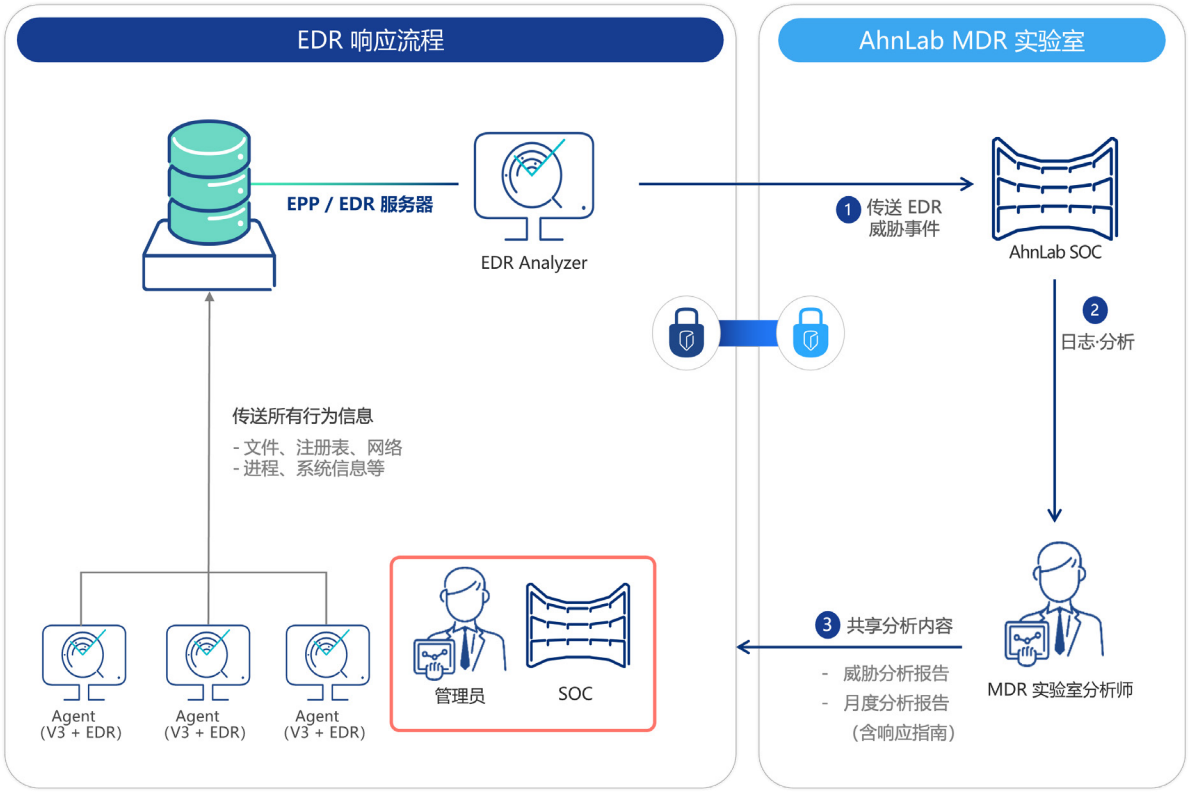


[图8] AhnLab V3-MDS-EDR联动安全体系

② MDR——检测与“以人为本的响应”

若说 EDR 是技术基础，那么 MDR（托管检测与响应）便是融入人类经验的威胁应对流程。AhnLab 的安全专家全天候监控 AhnLab EDR 检测到的威胁，主动追踪（hunting）入侵迹象。一旦发现异常征兆，便通过专业运营流程实施快速响应与深度检测，持续分析客户面临的威胁事件。

MDR 的核心优势在于实时分析能力与协同沟通。其不仅能解析日志数据，更能判断“该事件是孤立行为还是连锁攻击的开端”，并综合考量风险等级、传播可能性及业务影响提出应对方案。这使安全人力不足的企业也能构建卓越的威胁检测与响应体系。



[图9] MDR 服务——运营流程

综上所述，EDR 与 MDR 的结合构建了人机协同运作的实时威胁响应体系。这标志着技术层面实现了“即便无法阻止攻击，也必须遏制其扩散”的防御哲学。

第三阶段：运营与协作——“安全的终点是统一管理”

包括勒索软件在内的最新威胁已不在局限于终端、邮件、云端或网络等安全环节。因此，实现覆盖所有安全领域的统一可视性已成为首要任务。

① AhnLab XDR——连接数据的“安全枢纽”

AhnLab XDR 整合端点、网络、云端、邮件等多系统日志实现可视化，通过分析事件关联性掌握攻击全流程。将分散的入侵迹象重组为统一情境，使安全人员能清晰把握威胁演变过程及影响范围。

[图10] AhnLab XDR - 基于集成数据平台的关联分析

在此过程中，威胁严重性通过风险指数实现量化，使管理员能清晰判断应对优先级。搭载生成式AI“AhnLab Annie”的XDR系统全程辅助用户的安全决策流程。同时基于开放API的Open XDR架构，可与第三方解决方案灵活联动。企业可借此构建更具扩展性的安全体系，并将其发展为有机平台。

② MXDR——由专家之手完成“统一运营”

若说XDR通过整合数据实现风险管理，MXDR则是基于整合数据由专家直接执行安全运营与响应的阶段。AhnLab的MXDR服务远程管理客户的AhnLab XDR平台，执行24小时监控、威胁狩猎及风险应对等任务。专家团队从单一事件的异常征兆到复合攻击进行全局分析，评估业务影响程度后提出最优应对方案。

[图11] AhnLab MXDR 的集成威胁响应架构（专家分析服务 + XDR 平台）

MXDR 不是单纯的监控服务，而是一种安全专家像客户安全团队成员一样持续协作的混合运营模式。它结合 XDR 的数据驱动自动检测能力与人工分析能力，将“检测–分析–响应”全过程实现为完整的流程。

③ AhnLab TIP——以情报实现主动安全

TIP 是一个预测型安全情报枢纽，整合并提供最新的入侵指标（IoC）、威胁组织分析、攻击战术与技术（TTP）信息。通过这一平台，将国内外收集的威胁信息标准化，并基于攻击者组织的战术和行为模式，实现“可预测的安全”。

此外，TIP 与 EPP、 XTG、 EDR、 XDR 等 AhnLab 的核心解决方案实时联动，将新发现的 IoC（入侵指标）自动融入各产品的检测策略中。这不仅是信息提供，更是涵盖安全事件统一可视化、自动响应及关联分析的综合安全流程的重要组成部分。

得益于这种架构，AhnLab 解决方案构建了威胁情报“收集 - 检测 - 阻断 - 响应”实时循环的自动化威胁应对体系。AhnLab TIP 作为存在于各独立解决方案之上的“安全流程核心枢纽”，帮助组织在面对看似不可预测的威胁时也能抢先一步作出响应。

全球验证的技术实力

构成 AhnLab 勒索软件安全方案的核心产品，在国际网络安全评估中屡获优异成绩，持续验证其卓越技术实力。

首先，AhnLab V3 自 2013 年起参与 AV-TEST 认证，累计获得 60 余次认证。2025 年更在“高级威胁防护测试（ATP 测试）”中斩获满分，验证了其抵御高级攻击的卓越能力。ATP 测试基于 MITRE ATT&CK 框架设计，通过 10 种网络攻击场景评估产品的检测与拦截能力。

此外，AhnLab EDR 与 AhnLab XDR 在全球最具公信力的安全产品测试之一——MITRE ATT&CK 评估中均取得优异成绩。在 2024 年第六轮测试中，针对主要勒索软件集团 CL0P 与 LockBit 在Windows 及 Linux 系统实施的真实攻击技术场景，其检测率达 95%，该成绩位居全球安全企业前列。

不仅如此，在检测到的 56 个子步骤中，有 49 个获得了最高等级的“技术”评级，这充分证明用户可通过检测信息全面理解威胁行为的“上下文”。

由此可见，AhnLab 的核心勒索软件安全解决方案正通过全球范围内的持续验证，不断提升客户信任度。

结论：可预测的安全，由人与技术的协同完成

勒索软件早已不再是单一技术的攻击形式。在成功入侵之后，还会伴随着信息窃取、内部横向扩散、对外勒索等一系列复合式威胁链。如今，企业所需要的不是单一安全产品的堆叠，而是基于可预测流程的统一响应体系。

AhnLab 的勒索软件综合安全战略正是将此类入侵应对流程具体化的模型。
其多层级结构包括：
用户及设备验证（XTG）→ 威胁检测与阻断（EPP & MDS）→ 终端行为分析与追踪（EDR）→ 专家主导终端安全（MDR）→ 综合风险管理（XDR）→ 专家主导整合威胁响应（MXDR）→ 威胁情报（TIP）
在此流程中，安全技术能够快速识别威胁，专家则负责解读攻击的上下文；再结合 AI 技术，便能实现最优且迅速的响应。

当今时代，关键在于“面对网络威胁，企业能以多块、且多准确的速度做出反应”。AhnLab 将继续深化自有解决方案与服务之间的紧密联动，以“人的洞察 + 技术自动化”的可预测安全体系，持续守护客户的业务环境。

AhnLab

AhnLab China
北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区新镇路1699弄E栋303室
http://cn.ahnlab.com | cn.sales@ahnlab.com
电话： +86 10 8260 0932（北京）| +86 21 6095 6780（上海）