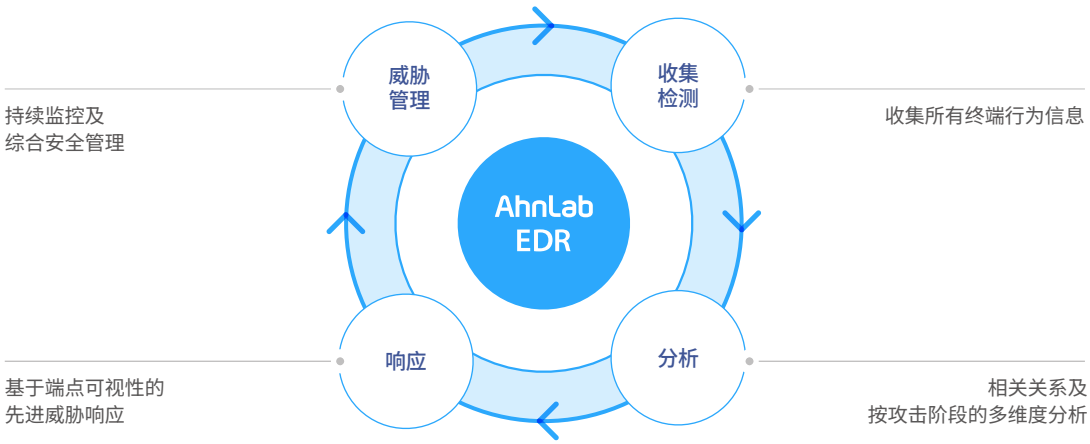
AhnLab EDR

精确检测、专业的分析与响应、主动的威胁狩猎

AhnLab EDR 基于通过 MITRE ATT&CK 评估验证的检测、分析和响应能力，
主动追踪威胁，帮助企业建立强大的安全体系。

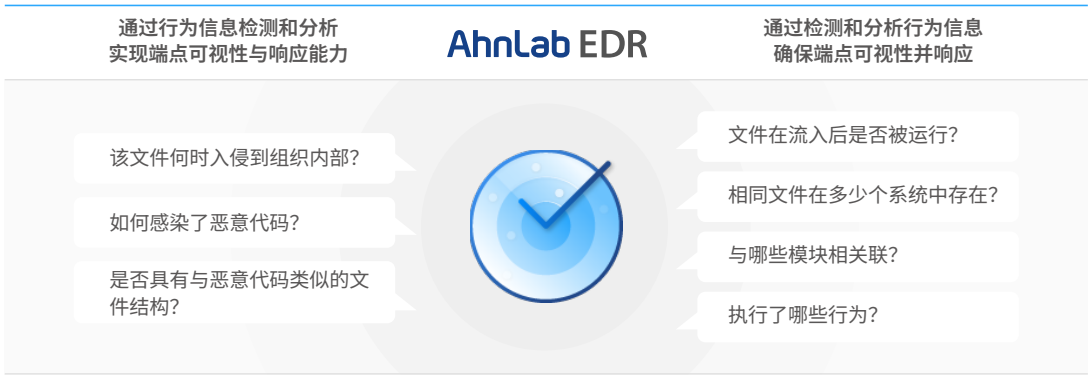
产品概要

AhnLab EDR 是一款下一代端点威胁检测与响应解决方案，基于韩国唯一的行为分析引擎，专为端点领域提供强大的威胁监控、分析与响应能力。AhnLab EDR 在 MITRE ATT&CK 评估中取得了优异的成绩，与 MDR（托管检测和响应，Managed Detection & Response）服务相结合，进一步增强了整个威胁检测与响应流程的专业性。



AhnLab EDR 的必要性

针对端点的攻击日益复杂，每天都有大量新种和变种恶意代码出现，预先阻断所有威胁几乎是不可能的。因此，必须建立能够全天候监控并快速感知安全事件的安全体系，以尽量减少威胁的影响。AhnLab EDR 通过检测和分析行为信息，提供广泛的端点可视性，并通过简便的部署和运维实现更有效的威胁检测与响应。此外，EDR 能够主动追踪威胁，帮助企业构建预防和防止再发的安全机制。



特点和优势

运营便捷性

AhnLab EDR 支持凝聚了 AhnLab 的专业技术与专业性的专用控制台“EDR Analyzer”。EDR Analyzer 从检测、分析和响应的角度帮助用户准确识别威胁并设置条件。AhnLab EDR 持续收集有关可疑行为的分类信息，并将其存储在 EDR Analyzer 中央服务器中。根据客户的环境，行为收集的级别可进行灵活调整，从而优化管理并减轻容量负担。

【AhnLab EDR Analyzer 仪表板】

精确的威胁检测与分类

AhnLab EDR 通过基于行为的引擎自主分析国内外攻击集团，并创建检测模式和规则，以精确检测威胁。此外，根据 MITRE ATT&CK 框架，将威胁分为 16 种行为类别，帮助用户能够直观地识别威胁。除此之外，还利用机器学习技术，提供有关每种威胁的风险级别和恶意风险概率的信息。

专业分析与响应

AhnLab EDR 针对检测到的威胁，基于 MITRE ATT&CK 框架提供信息的分析信息，包括威胁情报、引入途径、主要行为、相关关系、风险级别、威胁情报链接等。分析信息以▲图表、▲时间线、▲进程树的形式呈现，帮助用户轻松理解整体攻击流程。还支持对主要行为进行按需（On-Demand）扫描，并通过与 AhnLab TIP 和 AhnLab MDS 的联动进行进一步分析。

强化可靠性的基础服务

对于检测到的高风险事件中，AhnLab EDR 提供初步和二次报告，以及基于统计的报告，帮助客户更有效地使用 EDR。此外，还会在与客户事先协商的情况下进行威胁响应。

** 此服务在部署 AhnLab EDR 时默认提供，但如果无法将 EDR 检测日志传输到外部，则不支持此服务。*

MITRE ATT&CK 评估验证

AhnLab EDR 在最近进行的 MITRE ATT&CK Evaluation Round 4 中，模拟执行了攻击集团“Wizard Spider”和“Sandworm”使用的最新技术。在 90 个攻击步骤中成功检测到了 83 个，达到了 92% 的检测率，证明了其对高级威胁的出色的检测能力。

主要功能

AhnLab EDR 根据检测类型对威胁进行分类，支持从威胁识别到分析和响应的快速工作流程。此外，通过与各种解决方案联动，最大化响应能力，并通过 AhnLab EPP 产品之间的连接规则设置，实现针对企业环境进行优化的端点安全运营。

高级威胁检测 · 分类 · 分析 · 响应

- 收集并存储所有行为信息 – 可以随时查看与事件相关的整体威胁信息
  - 收集进程、文件、注册表、网络、系统等行为信息
- 按信息单位（Agent、文件、行为）进行详细条件搜索和查询
- 支持通过用户定义规则（IoC、Yara、静态 / 动态行为规则）进行检测和自动响应
- 在检测到威胁时能够立即响应（拦截网络、结束进程、回滚、收集 / 搜索 / 删除 / 恢复文件等）
- 通过用户设置实现自动响应（用户定义规则、连接规则、基于黑名单哈希值的进程预先拦截）
- 生成用户（安全管理员）定义报告 - 提供 CSV、XLS、PDF 等多种格式
- 通过按需（On-Demand）扫描，分析主要行为和 V3 诊断的恶意代码行为
- 基于 MITRE ATT&CK 战术划分 16 个威胁类别分类
- 提供勒索软件、注入、网络连接、C&C 访问、系统设置更改、权限提升、无文件攻击、窃取信息等主要恶意行为的监控文件信息
- 可收集用于入侵响应分析的附加资料（AhnReport、Artifacts、Windows 事件日志）

基于平台的集成安全运营和管理

- 基于下一代端点安全平台 AhnLab EPP，构建强大的威胁响应体系
  - 基于单一管理和单一 Agent 实现高效的安全运营和管理
- 通过灵活的连接策略设置，支持有机的威胁响应和修复功能
- 基于扩展的端点可视性，最小化威胁检测和响应时间

通过灵活的联动确保威胁情报并提高响应能力

- 通过与第三方解决方案的联动，确保丰富的威胁情报
- 支持与 SIEM、SOAR、综合日志等通过 API 和 Syslog 的联动
  - 通过控制台轻松设置联动，并提供各种协议支持（UDP/TCP/TCP over SSL 等）

EDR Premium

EDR Premium 是与 AhnLab EDR 结合提供专业威胁检测和响应能力的“MDR（托管检测和响应，Managed Detection & Response）”服务组合产品。使用 EDR Premium 时，AhnLab 专家将对已知威胁或可疑行为进行监控、分析和判断，并主动响应。

EDR Premium 的背景是 AhnLab 长期积累的无与伦比的威胁响应能力。EDR Premium 为客户端点环境中发生的威胁生成工单（Ticket）票证，并利用信誉信息和恶意代码行为信息等，基于 AhnLab 的威胁响应流程进行系统化处理。

此外，AhnLab 通过将入侵事件分析服务、恶意代码专家分析服务、可疑系统诊断服务等各种专业服务与 EDR Premium 链接，为提高安全威胁分析和响应能力提供多种选项。

**EDR Premium 为付费服务，请另行咨询服务费用和具体内容。*

威胁检测
实时检测
各种威胁

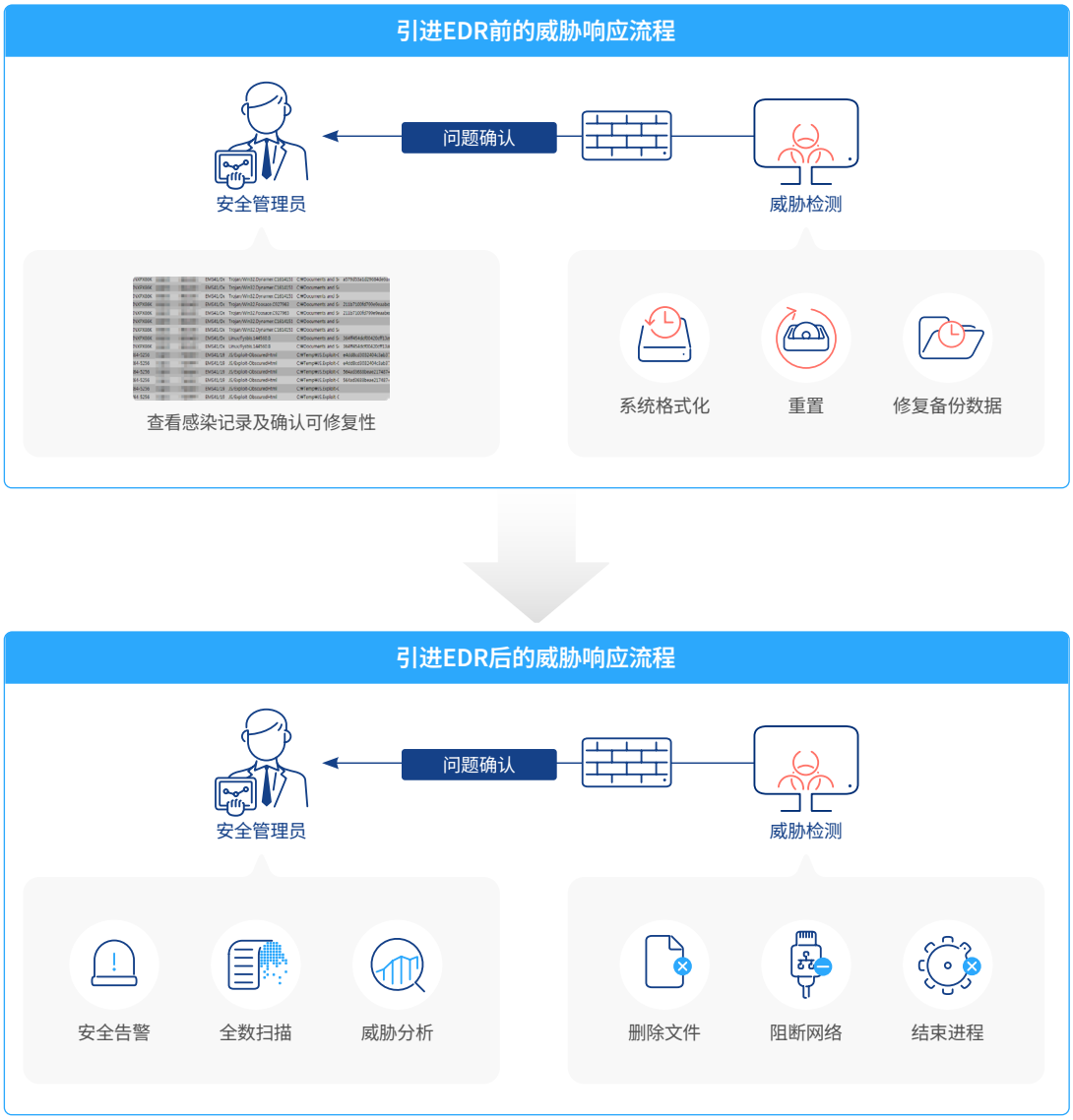
专家分析与响应
通过主动分析与响应
实现威胁缓解和恢复

报告
提供报告以强化
威胁检测与响应流程

引进效果

未使用 AhnLab EDR 的情况下，一旦发现恶意代码感染记录，通常需要对系统进行格式化或重置，然后恢复备份数据以继续工作。在防病毒软件管理服务器中，用户计算机可能存在恶意代码感染记录，但具体感染路径无法确定，导致威胁响应仅为一次性措施，难以制定有效的预防复发方案。

然而，引进 AhnLab EDR 后，可以通过综合分析来查明原因，制定适当的响应和防范流程。当发生安全事件时，管理员会收到告警通知，并基于预定义规则进行威胁分析和全公司范围的扫描。从而可以采取正确措施，如收集可疑文件、结束相关进程、阻断网络等。此外，通过检查漏洞和感染记录，不仅可以实现积极的提前响应，还可以进行事后管理。



北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
http://cn.ahnlab.com | cn.sales@ahnlab.com
电话：+86 10 8260 0932（北京）| +86 21 6095 6780（上海）

AhnLab