AhnLab

白皮书

“从检测到响应”利用 EDR 的安全策略

目录

EDR是什么

端点是网络攻击者的最终目标。每年有数万例端点漏洞被发现，每天发现的新恶意代码数量多达数十万。此外，近期还出现了高级攻击类型，如绕过现有安全解决方案检测、通过内部移动劫持服务器、删除入侵痕迹等。为了解决这些问题，安全范式发生了变化，转向建立持续监控和事后调查体系，于是出现了“EDR（Endpoint Detection and Response）”。

EDR于2013年由Gartner首次提出，是一种通过在端点进行持续监控、收集和分析威胁信息，以确保对威胁的适当可见性，并增强响应能力的安全解决方案。其目的是将威胁的潜伏期（Dwell Time）最小化并防止潜在的损害。此外，根据Gartner的定义，EDR必须提供以下四项功能：▲检测安全事件（Detect security incident）、▲调查安全事件（Investigate Security incident）、▲在端点遏制事件（Contain the incident at the endpoint）、▲提供修复指导（Provide remediation guidance）。

简而言之，EDR的作用类似于闭路电视（CCTV）。它通过检测端点上发生的所有行为来加强端点日志记录，并持续收集调查安全事件所需的信息。基于收集的行为信息，主动追踪和分析威胁，并有助于建立长期的威胁响应体系。

EDR的核心：下一代端点安全解决方案，不仅限于保护，还执行主动检测和响应、全面预防再发

EDR是一种增强端点安全的工具，而非能够完全确保安全环境的万能解决方案。理解这一点后，与防病毒软件（Anti-Virus, AV）等传统安全产品结合使用更为理想。

EDR引入的必要性

EDR的基本前提是：“无法收集的对象就无法分析，无法分析就无法确定其是否为恶意，未确定为恶意的对象就无法做出响应”。

为了满足这一前提，EDR持续监控和可视化终端设备上发生的所有行为，并通过与现有解决方案链接，旨在最小化威胁潜伏期。威胁潜伏期是指从确认外部威胁到样本分析和分析、引擎注册和更新所需的时间。通过EDR可以应对在此期间可能出现的安全漏洞。

攻击者通常通过电子邮件或Web传递恶意代码。利用存在漏洞的特定计算机进行攻击，然后安装后门并通过外部C&C服务器下载其他恶意文件。此外，攻击者还会寻找可以访问内部服务器的计算机，进行横向移动（Lateral Movement）。通过这些步骤，泄露服务器数据并消除所有痕迹。

这类攻击是传统安全解决方案无法追踪的。因此，引入EDR是必要的。EDR可以基于时间线记录端点上发生的文件或进程等行为的历史，在必要时执行威胁捕获（Threat Hunting），主动追踪威胁。

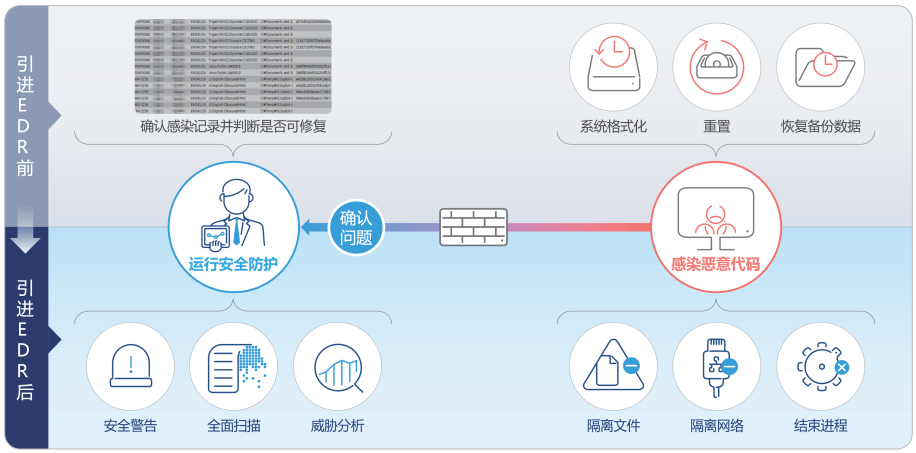
此外，还提供多种应对措施，如网络隔离、进程运行拦截、文件收集和恢复等，有助于企业建立预防和防止再次发生的体系。

为什么需要EDR：

- 面对未知威胁的响应局限
- 需要高水平的取证分析技术
- 通过分析入侵原因，制定预防复发策略

另外，将MITRE ATT&CK框架应用于EDR可以更有效地检测和识别各种攻击技术。通过参考攻击的特定阶段和所使用的技术，可以确认威胁的起源、进行情况并预测未来可能发生的攻击方式。因此，安全负责人可以更好地了解威胁并快速做出响应，从而加强组织的整体安全态势。

以前，对威胁的响应往往是一次性的，并且随着威胁的复杂化，分析和响应存在限制。然而，现在可以利用EDR全面管理和响应未知威胁，并通过综合分析找出原因，从而制定预防复发的策略。



[图1] EDR引入前后比较

AhnLab于2018年首次推出了“AhnLab EDR”。2022年，发布了进一步增强可用性和威胁可见性的升级版本——“AhnLab EDR 2.0”。

AhnLab EDR的攻击响应方法

AhnLab EDR基于以下七个核心功能来响应端点威胁：

(1)图表和时间线分析

AhnLab EDR基于MITRE ATT&CK框架，分析包括16种威胁类型、威胁引入途径、主要行为、相关关系、风险级别、威胁情报信息链接等的内容，提供按进程、文件、系统、注册表、网络的行为和详细信息，并实时响应。此外，根据检测到的威胁分析信息，按主要行为（对象类型/风险级别）、一般行为（对象类型）和Artifacts信息进行预分类，通过组合筛选器和必要条件，在时间线上提供信息。

AhnLab EDR主要功能(1)：
通过图表和时间线分析，提供威胁信息

AhnLab EDR主要功能(2)：
支持与威胁情报平台联动的专用控制台

[图2] 图表分析

(2)基于专用控制台，提供威胁信息和统计数据

AhnLab EDR提供了操作便捷且搭载了AhnLab专业技术的专用控制台“EDR Analyzer”。EDR Analyzer从检测和分析、响应的角度出发，帮助用户准确识别威胁并设置条件。AhnLab EDR持续收集与可疑行为相关的各类型的信息，并将其存储在EDR Analyzer的中央服务器上。根据客户公司环境和监控组的重要程度，调整行为收集级别，从而优化管理并减轻容量负担。

此外，EDR Analyzer与AhnLab的威胁情报平台（AhnLab TIP）联动，提供最新的IoC（文件、IP、URL）统计信息和最新的安全建议，还可查询在客户EDR中检测到的事件的信誉度。

AhnLab EDR主要功能(3)：
基于机器学习的高级检测和分析

AhnLab EDR主要功能(4)：
设置用户自定义规则和自动响应

AhnLab EDR主要功能(5)：
恢复感染勒索软件的计算机的重要数据

[图3] EDR Analyzer仪表板

(3)基于机器学习（ML）的风险级别分析

AhnLab EDR应用了“监督学习ML”，基于AhnLab云服务器ASD（AhnLab Smart Defense）收集到的数百亿条大数据进行学习。学习过程中使用超过10个模型，从中选择最佳模型并应用于产品中。应用于EDR的ML提供对EDR检测到的可疑行为和威胁行为的恶意概率分析，帮助安全负责人确定EDR分析结果的优先级和重要程度。

(4)通过设置用户自定义规则，进行自动响应

AhnLab EDR提供多种类型的用户自定义规则（IoC/Yara/基于行为的规则）以及网络和文件隔离、进程拦截等自动响应设置功能。特别是，基于行为的用户自定义规则可以根据组织环境定义需要重点监控的可疑行为，支持针对组织环境的威胁管理。

(5)回滚（Roll back）功能

回滚功能也是AhnLab EDR的重要功能之一。AhnLab EDR运用Windows的VSS技术，将被勒索软件加密的文件恢复到之前的状态。此外，还可以全面阻断恶意行为、VSS功能失效，和快照删除行为。通过这些功能，用户可以安全地将计算机数据恢复到受损之前的状态。

AhnLab EDR主要功能(6)：
详细分析安全事件并额外取证

AhnLab EDR主要功能(7)：
默认提供MDR服务，有效地管理和应用EDR

[图4] 应用回滚功能的流程

(6)安全事件取证和响应

AhnLab EDR针对需要详细分析的终端设备进行额外的证据收集并做出响应。根据默认和用户自定义条件收集和分析Artifacts信息，执行文件全面扫描。然后，基于从多个终端设备收集的详细信息，通过综合搜索系统进行安全事件详细分析和搜索。

(7)提供MDR服务以有效地管理和应用EDR

AhnLab EDR默认提供作为核心服务的托管检测与响应（MDR），该服务由AhnLab安全专家提供支持。企业通过安装和运营的EDR，创建对威胁的工单（Ticket），并根据AhnLab的威胁响应流程系统地处理，包括信誉信息和恶意代码行为分析。此外，还提供威胁分析报告、每月统计报告以及威胁缓解和恢复的操作指南。

希望获得更高级和定制型MDR服务的企业可以选择额外付费的“EDR Premium”，该服务包括对所有威胁的监控、分析和响应服务，以及每季度的专家审查意见。

[图5] MDR服务概要

AhnLab EDR实际运用方案(1)：
通过联动EP（V3/MDS/EPP）
解决方案，实现端点集成安全

AhnLab EDR实际应用方案

独立构建AhnLab EDR时，无法充分展现其真正价值。需要与其他安全产品进行链接，实现集成安全，才能打造更强大的安全体系。

AhnLab EDR不仅与AhnLab的AV解决方案V3产品群、沙箱解决方案MDS、端点集成安全平台EPP（Endpoint Protection Platform）等EP专用解决方案集成，还可以与SIEM（安全信息和事件管理，Security Information and Event Management）、SOAR（安全编排、自动化与响应，Security Orchestration, Automation, and Response）等远程控制系统及各种关联系统配合使用，以发挥安全增强的协同效应。

(1)结合EP解决方案，实现端点集成安全

首先，AhnLab EDR可以与AhnLab V3、AhnLab MDS有机地结合，实现对端点领域的集成安全。与V3结合，可将已发生的威胁和可疑威胁分为恶意/警告/注意三个级别进行分类，并提供分析信息。与MDS结合，可对可疑文件执行额外的动态分析和静态分析。

具体来说，将AhnLab MDS和AhnLab EDR添加到安装了AhnLab V3的服务器上，可以通过Agent执行恶意文件删除、系统隔离、发送通知等响应命令，并通过基于机器学习和大数据的威胁检测功能，有效检测并响应APT攻击等未知威胁。此外，还提供从文件运行至终止的详细行为分析结果报告，并支持与VirusTotal链接，以帮助用户判断是否为恶意。

AhnLab EDR不仅能够应对未知威胁，还可以阻止绕过AhnLab V3和AhnLab MDS的攻击。收集端点上发生的所有进程、文件、网络、注册表和系统行为，并利用AhnLab专业知识和MITRE ATT&CK框架的检测模式和规则来监控和检测威胁。此外，还支持根据客户环境定制的IoC、YARA和行为规则，检测和响应威胁。

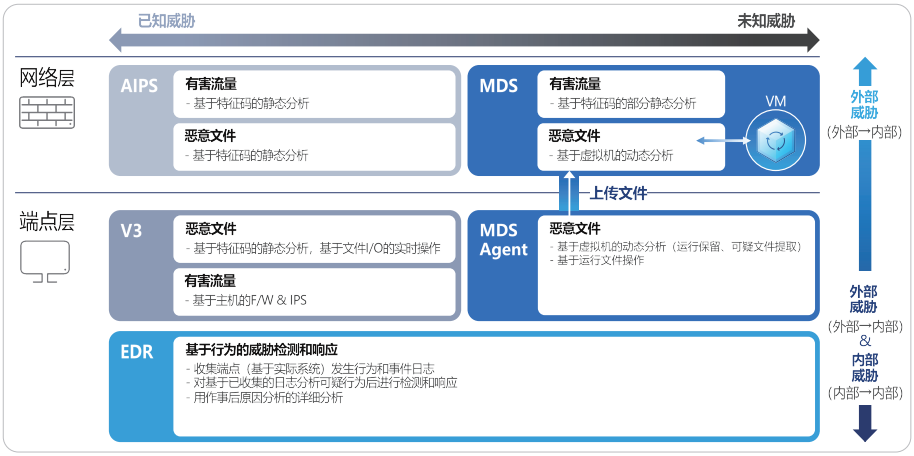
另外，还提供由V3诊断的恶意代码引入途径、主要行为、MITRE ATT&CK信息、进程事件流程图、进程树、时间线信息等各种分析信息，以预防可能发生的同类威胁。通过MDS，可以对EDR收集到的可疑进程或文件进行沙箱分析，并查看分析结果和额外证据。

AhnLab EDR与V3、MDS的联动效果：通过检测已知/未知恶意代码以及基于沙箱的动态分析、收集和监控行为信息，确保全方位的安全能力解决方案，实现端点集成安全

AhnLab EDR与EPP的集成：与现有端点产品相比，可实现快速威胁检测和自动响应

[图6] AhnLab EDR与AhnLab MDS的联动

总结来说，AhnLab V3负责基于特征码和模式恶意代码检测，以及对恶意文件或URL的拦截、删除和修复等主动响应。AhnLab MDS基于沙箱技术，精确检测未知威胁。而AhnLab EDR最终在端点上监控和检测所有潜在威胁行为，跟踪并分析威胁，负责更高层次的功能。将这三种解决方案结合起来，可以安全地保护复杂多变的端点系统环境。



[图7] 基于端点统一Agent的威胁响应架构

此外，AhnLab EDR与AhnLab EPP集成，可以更快地检测和响应威胁。EPP中包含的解决方案提供端点强化（Endpoint Hardening）的安全功能，并直接检测和响应威胁，而EDR则分析EPP检测和响应的结果，通知安全负责人，并提供关于是否发生和进行安全事件以及是否需要响应的见解。

端点强化：通过多种保护措施，最大限度地减少端点领域的攻击面。

AhnLab EDR实际运用方案(2)：
通过与SIEM和SOAR联动，实现安全威胁响应自动化

此外，与EPP链接的AhnLab EDR提供了针对端点漏洞状态、可疑行为的单独以及连接策略设置，并支持安全管理员对违反安全策略的系统进行主动和积极地措施，如通知、网络隔离、修复恶意代码、应用补丁等。

[图8] 与AhnLab EPP产品群的互补运用

(2)SIEM & SOAR链接，最大化安全托管（SOC）运营效果

AhnLab EDR提供与SIEM、SOAR、Syslog和API链接功能。因此，安全管理员可以选择性地指定威胁检测类型、风险级别和行为类型等联动信息来确认威胁，并通过链接的API实现自动响应，包括网络隔离或解除、文件隔离和恢复、发送通知、结束进程、运行Artifacts和运行AhnReport。此外，还提供了主机信息和数据库（DB）信息查询（Query）。

[图9] AhnLab EDR与SIEM、SOAR链接

AhnLab EDR实际运用方案(3)：通过与AhnLab专业服务链接，分析安全事件并制定威胁响应方案

SIEM仅基于网络信息或简单的防病毒软件诊断信息设置警报条件，因此在与端点的各种信息进行关联分析和建立链接条件方面存在局限。然而，将AhnLab EDR与SIEM链接后，可以多样化问题事件警报条件，细化严重级别标准，便于判断威胁和响应的优先级，能够实时响应端点威胁，减少平均响应时间（MTTR）和运营资源。

(3)链接AhnLab专家服务 - 提供最佳响应方案

将AhnLab EDR与MDR服务以及“AhnLab专业服务”结合使用时，韩国顶级的恶意软件专家将详细分析企业和机构中进入的恶意代码（文件）的下载、复制、生成及网络活动，并根据可疑行为信息快速提供应对方案。另外，还提供内部引入的恶意代码的基本信息、是否恶意和行为信息的详细分析报告，有助于预防安全事故并缩短响应时间。

此外，还通过数字取证技术分析安全事件的影响程度和引入途径，从而有效管理风险，并预防APT攻击等安全事件的再次发生。

结语

AhnLab EDR对于所有需要技术保护措施来预防恶意代码感染或安全事件的所有企业和机构不可或缺的安全解决方案。然而，在引进AhnLab EDR时，不应从单一的角度来考虑。由于EDR本身是一种功能强大且信息量大的解决方案，因此需要考虑当前组织的规模、IT基础设施状况、成本以及具体的应用方式等多方面因素。此外，需要牢记与与其他产品结合使用能够提供更大的安全价值。积极评估通过EDR可以补充改进的领域，并相应地定制化部署EDR是明智之举。如有需要，建议利用AhnLab等专业公司咨询服务。

有关AhnLab EDR的更多信息，请访问AhnLab官方网站（www.ahnlab.com）。

▶前往AhnLab EDR产品介绍页面

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 (邮编: 100102) | 上海市闵行区万源路2158号 泓毅大厦1201室 (邮编: 201113)
https://www.ahnlab.com/cn
cn.sales@ahnlab.com
电话： +86 10 8260 0935/8（北京）| +86 21 6095 6780（上海）