AhnLab

White Paper

"Response Beyond Detection" Security Strategy Leveraging EDR

Contents

Understanding EDR

Endpoints are the ultimate targets for cyber threat actors. Tens of thousands of endpoint vulnerabilities appear every year, and hundreds of thousands of new types of malware are discovered daily. More sophisticated attack techniques have recently emerged, such as evading detection by existing security solutions, breaching servers via lateral movement, and deleting infiltration traces. To address this, the security paradigm has shifted towards establishing a continuous monitoring and post-incident investigation system, leading to the emergence of Endpoint Detection and Response (EDR).

Introduced by Gartner in 2013, EDR is a security solution that secures visibility and enhances response capabilities to threats by continuously monitoring, collecting, and analyzing threat information at the endpoint. Its goal is to minimize the dwell time of threats and prevent potential damage. Additionally, according to Gartner, EDR must provide the following four features: ▲Detect security incidents, ▲Investigate security incidents, ▲Contain the incident at the endpoint, and ▲Provide remediation guidance.

Simply put, EDR functions similarly to a surveillance camera. It strengthens endpoint logging by detecting all activities occurring at the endpoint and continuously collects the information necessary for investigating security incidents. Based on the collected behavioral information, it actively tracks and analyzes threats, contributing to the establishment of a long-term threat response system.

The Key Point of EDR:
A next-generation endpoint security solution that goes beyond protection to actively detect, respond to, and prevent the recurrence of threats

It should be noted that EDR is a tool to complement endpoint security and is not a perfect solution that creates a completely secure environment. It is important to understand this point and use it in conjunction with existing security products such as anti-malware products.

Necessity of Implementing EDR

EDR is based on the following premise: what cannot be collected cannot be analyzed; what cannot be analyzed cannot be determined as malicious; if malware cannot be identified, it cannot be responded to.

To meet this premise, EDR continuously monitors and visualizes all activities occurring at the endpoint, aiming to minimize threat dwell time through integrating with existing solutions. Threat dwell time refers to the time taken from the detection of an external threat's infiltration to its sampling and analysis, and engine registration and update. EDR can be utilized to address security vulnerabilities that may occur during this period.

The primary routes for threat actors to distribute malware are email or web. They secure specific PCs with vulnerabilities to execute their attacks. After doing so, they install backdoors and download additional malicious files via external C&C servers. They also search for internally accessible servers and perform lateral movement to PCs that can connect to those servers. This process allows them to exfiltrate server data and erase all traces.

This type of attacks cannot be traced by traditional security solutions. To counter these attacks, implementing EDR is essential. EDR proactively hunts for threats by tracking endpoint activities and logging the behavior history of files and processes on a timeline.

Additionally, EDR provides various response measures to prevent threat propagation such as network quarantine, process execution blocking, and file collection and restoration, thereby helping organizations establish robust preventive measures and prevent incident recurrence.

Why EDR Is Necessary:

- Limitations in responding to unknown threats
- Need for high-level forensic analysis capabilities
- Deriving recurrence prevention strategies via analysis of breach causes

Applying the MITRE ATT&CK framework to EDR helps it to detect and identify various attack techniques more effectively. By referencing specific stages of attacks and the technologies used, it becomes possible to determine where the threats originated, how they progressed, and even predict future attack methods. Therefore, the security team can better understand threats, respond swiftly, and enhance their organization's overall security posture.

Previously, threat responses were one-off, with limitations in analyzing and responding to advanced threats. Now, with EDR, it is possible to comprehensively manage and respond to unknown threats, identify their causes through holistic analysis, and develop strategies to prevent their recurrence.

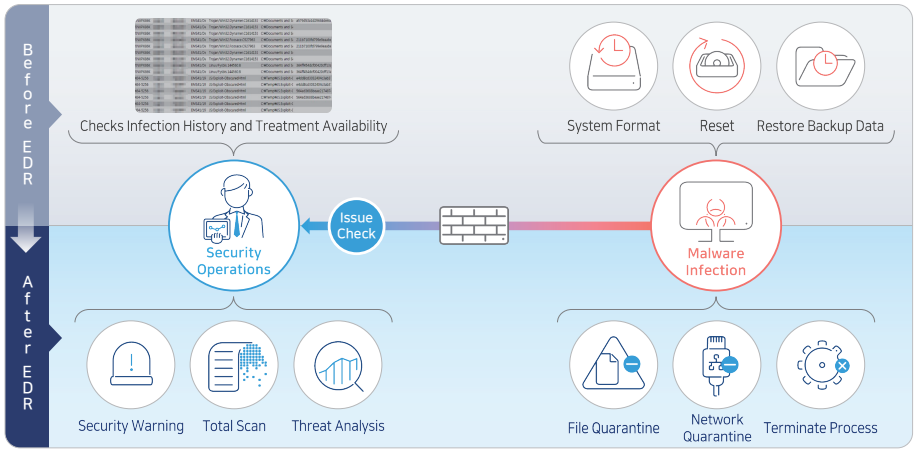

Figure 1. Comparison of Before and After EDR Implementation

AhnLab first released AhnLab EDR in 2018. In 2022, the company also announced an upgraded version, AhnLab EDR 2.0, with enhanced usability and threat visibility.

AhnLab EDR Key Feature (1):
Provides threat information through diagram and timeline analysis

AhnLab EDR Key Feature (2):
Supports a dedicated console integrated with the threat intelligence platform

AhnLab EDR's Attack Response Methods

AhnLab EDR responds to endpoint threats based on the following 7 key features.

(1) Diagram and Timeline Analysis

AhnLab EDR provides analyses on 16 types of threats based on MITRE ATT&CK along with threat entry paths, key behaviors, relationships, severity, and threat information links. It also offers detailed information on processes, files, systems, registry, and network targets and responds in real time.

Additionally, it provides filters to pre-classify detected threat analysis information by major activities (object type/severity), general activities (object type), and artifacts. These filters can be combined with their prerequisites to provide information on a timeline basis.

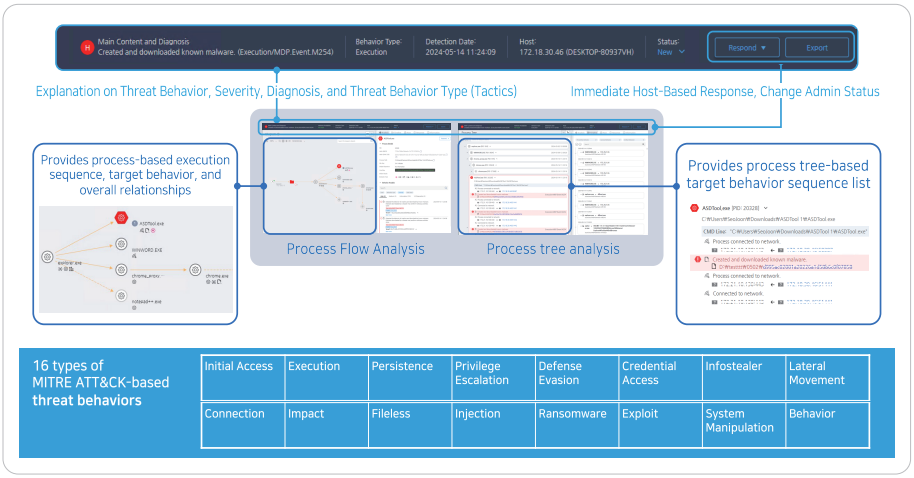

Figure 2. Diagram Analysis

(2) Providing Threat Information and Statistics via Dedicated Console

AhnLab EDR provides a dedicated console called EDR Analyzer, which is designed for ease of use and backed by AhnLab's technical expertise. The EDR Analyzer dashboard allows users to accurately identify threats from detection, analysis, and response perspectives and configure security settings accordingly. AhnLab EDR continuously collects information on suspicious behavior types and stores it on the central server of EDR Analyzer. It also optimizes management and reduces the storage burden by adjusting the behavior collection level according to the importance of the client's environment and monitoring group.

AhnLab EDR Key Feature (3):
Advanced detection and analysis based on machine learning

AhnLab EDR Key Feature (4):
User-defined rules and automated response settings

By integrating EDR Analyzer with AhnLab's threat intelligence platform AhnLab TIP, it provides the latest IoC (files, IPs, and URLs) status information and the latest security advisories, allowing users to check the reputation of events detected by the client's EDR.

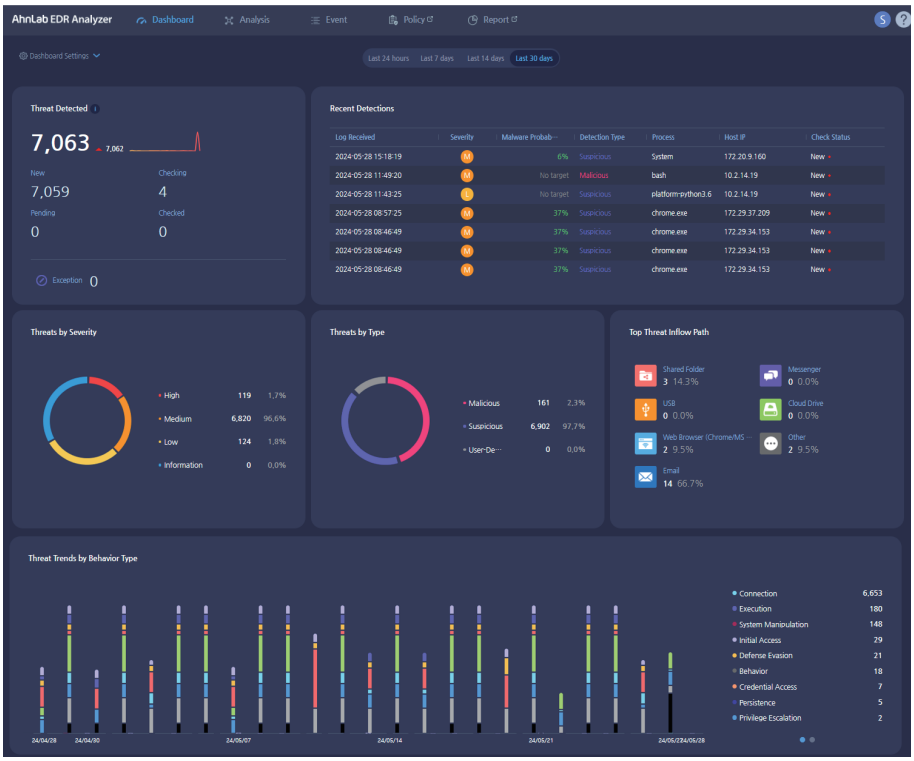

Figure 3. EDR Analyzer Dashboard

(3) Severity Analysis Based on Machine Learning (ML)

AhnLab EDR uses supervised ML, trained on billions of large-scale data collected by AhnLab's cloud server, AhnLab Smart Defense (ASD). More than 10 models are used during training, and the optimized model is selected for the product. The ML in EDR provides the probability of malware for suspicious and threat activities detected by EDR, helping the security team determine the priority and importance of EDR's analysis results.

(4) Automated Responses via User-defined Rules

AhnLab EDR offers various types of user-defined rules (IoC/YARA/behavior-based rules) and automated response settings such as network and file quarantine, and process blocking. Behavior-based custom rules enable users to define suspicious activities that require close monitoring based on the organizational environment, supporting threat management tailored to the organization's needs.

AhnLab EDR Key Feature (5):
Recovery of important data from PCs infected with ransomware

AhnLab EDR Key Feature (6):
Detailed analysis of breach incidents and collection of additional evidence

AhnLab EDR Key Feature (7):
MDR service is provided by default to assist with EDR operation and usage.

(5) Rollback Feature

The rollback feature is also one of the key features of AhnLab EDR. AhnLab EDR utilizes Windows' VSS technology to restore files encrypted by ransomware to their previous state. It also blocks malicious behaviors, the disabling of VSS functions and the deletion of snapshots. This allows users to safely restore their PC data to a state prior to any damage.

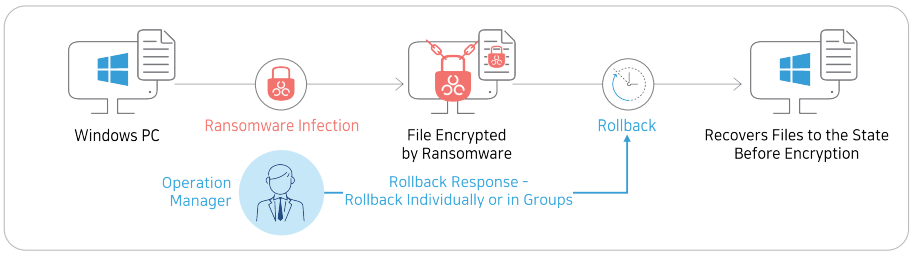

Figure 4. Rollback Feature Application Process

(6) Evidence Collection and Response to Data Breaches

AhnLab EDR collects additional evidence information for endpoints that require detailed analysis and responds accordingly. It collects and analyzes artifact information based on basic and user-defined conditions and conducts comprehensive file scans. Afterward, detailed analysis and search of the data breach are performed based on the information collected from multiple endpoints.

(7) Providing MDR Service for EDR Operation and Usage

AhnLab EDR offers the MDR service as a standard feature, where AhnLab's security experts assist with the operation and usage of EDR. Tickets are generated for threats using the EDR deployed in the organization and are systematically processed according to AhnLab's threat response procedures, including reputation information and malware behavior analysis. It also provides threat analysis reports, monthly statistical reports, and guidance for threat mitigation and recovery measures.

Organizations seeking more specialized and tailored MDR services can opt for EDR Premium for an additional cost, which includes monitoring, analysis, and response services for comprehensive threat coverage, along with quarterly review reports containing expert insights.

Practical Usage of AhnLab EDR (1): Achieving unified endpoint security through integrating with EP (V3/MDS/EPP) solutions

Figure 5. MDR Service Overview

Practical Usage of AhnLab EDR

AhnLab EDR cannot fully demonstrate its capabilities when deployed independently. The device must be integrated with other security products to achieve a unified security system for more robust protection.

AhnLab EDR can seamlessly integrate with various systems, including AhnLab's anti-malware V3 product line, sandbox solution MDS, and endpoint protection platform (EPP), as well as remote monitoring systems such as SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response). Through these integrations, AhnLab EDR significantly enhances security by leveraging synergistic effects.

(1) EP Solution Integration - Achieving Unified Endpoint Security

AhnLab EDR can achieve unified endpoint security by seamlessly integrating with AhnLab V3 and AhnLab MDS. When integrated with V3, it classifies detected and suspicious threats into Malicious, Warning, and Caution levels and provides their analysis information. Integration with MDS enables additional dynamic and static analysis of suspicious files.

To elaborate further, deploying AhnLab MDS and AhnLab EDR alongside AhnLab V3 on servers allows the issuing of response commands such as deleting malicious files, quarantining PCs, and sending notifications through agents, effectively detecting and responding to unknown threats such as APT attacks using threat detection capabilities based on ML and big data. Moreover, AhnLab EDR provides detailed behavior analysis reports from file execution to termination and supports users in determining malicious nature through integration with VirusTotal.

Integration Effects Between AhnLab EDR, V3, and MDS: Achieving comprehensive security capabilities through known/unknown malware detection, sandbox-based dynamic analysis, and behavior information collection and monitoring

AhnLab EDR not only blocks unknown threats but also prevents attacks that bypass AhnLab V3 and AhnLab MDS. It collects and monitors all processes, files, network activities, registry changes, and system behaviors occurring on endpoints, and detects threats using detection patterns and rules based on AhnLab's expertise and the MITRE ATT&CK framework. Additionally, it enables customized threat detection and response through the creation of IoCs, YARA rules, and behavioral rules tailored to each client's environment.

It also provides various analysis information that enables preemptive defense against potential future threats of the same kind, including infection paths of malware diagnosed by V3, key behaviors from MITRE ATT&CK, process event flow diagrams, process trees, and timeline information. Suspicious processes or files collected by EDR can undergo sandbox analysis through MDS, allowing analysis results and additional evidence to be checked.

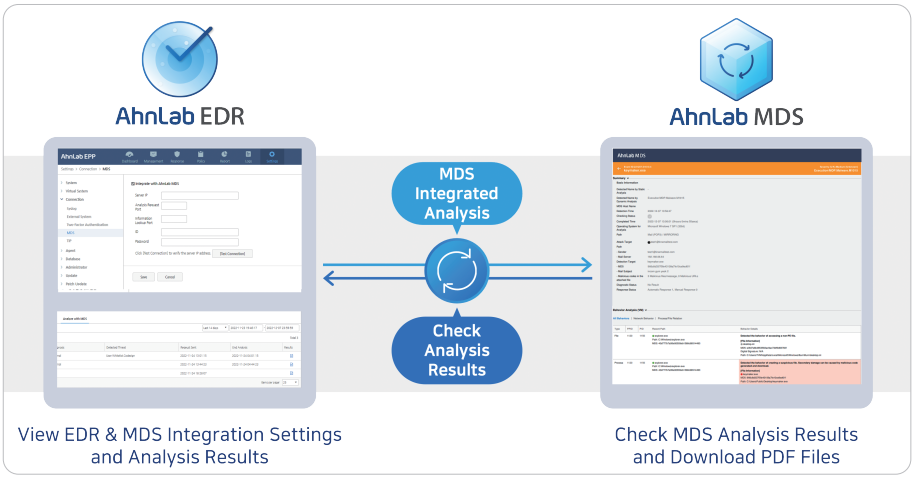

Figure 6. Integrating AhnLab EDR with AhnLab MDS

In summary, AhnLab V3 performs preventive measures such as signature and pattern-based malware detection, as well as blocking, deleting, and remediating malicious files or URLs. AhnLab MDS accurately detects unknown threats using sandbox technology. AhnLab EDR ultimately performs more advanced functions by monitoring and detecting all potentially threatening behaviors on endpoints, then tracking and analyzing these threats. By integrating these three solutions, complex and multi-layered endpoint system environments can be securely protected.

Integration of AhnLab EDR and EPP: Enabling faster threat detection and automated response compared to traditional endpoint products

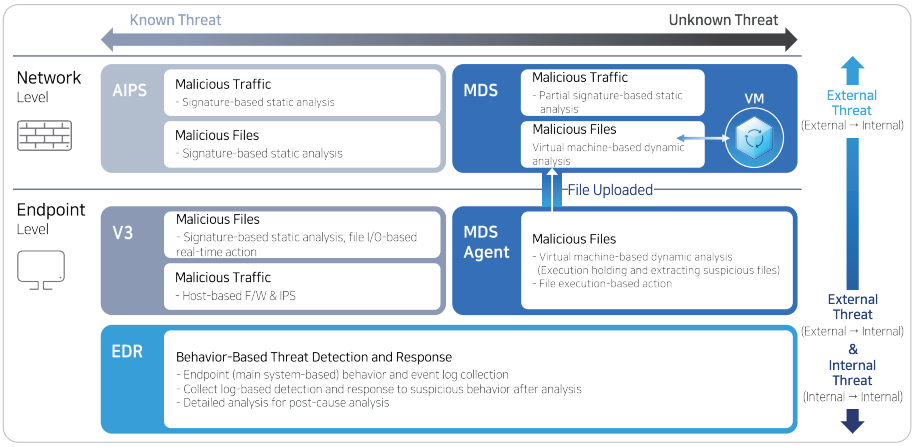

Figure 7. Threat Response Architecture Based on Unified Endpoint Agent

Moreover, AhnLab EDR integrates with AhnLab EPP to detect and respond to threats more swiftly. While the solutions within EPP provide security features for endpoint hardening* and directly detect and respond to threats, EDR analyzes the detection and response results from EPP and provides insights to the security team about breach incidents, their progress, and the urgency of required actions.

* Endpoint hardening: Minimizing the attack surface in endpoint domain through various protective measures

AhnLab EDR integrated with EPP provides individual and integrated policy settings for endpoint vulnerability status, suspicious activities, and more, allowing security administrators to proactively and actively take measures such as issuing alerts, quarantining networks, remediating malware, and applying patches to systems that violate security policies.

Figure 8. Complementary Operation with AhnLab EPP Solutions

Practical Usage of AhnLab EDR (2): Automating security threat response through integration with SIEM and SOAR

(2) SIEM & SOAR Integration - Maximizing Effectiveness of SecurityOperations Center (SOC)

AhnLab EDR provides integration capabilities with SIEM and SOAR through Syslog and API. This allows security administrators to selectively specify integration information such as threat detection types, risk severity levels, and behavior types to identify threats. Automatic responses become possible by integrating APIs for network quarantine or release, file quarantine and restoration, sending notifications, terminating processes, collecting artifacts, and gathering AhnReports. AhnLab EDR also provides queries for host information and database (DB) information.

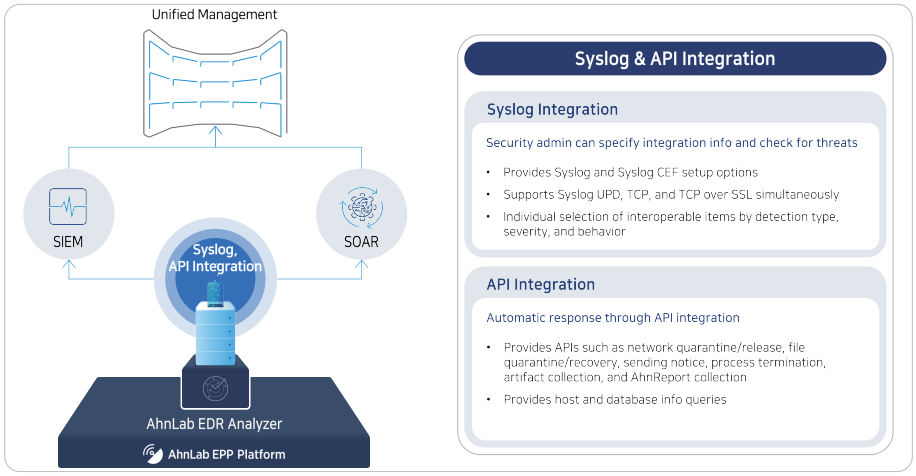

Figure 9. Integration of AhnLab EDR with SIEM & SOAR

SIEM has limitations in conducting correlation analysis and establishing connection between various endpoint information, as it sets alert conditions solely based on network information or simple anti-malware diagnostic information. However, integrating AhnLab EDR with SIEM offers multiple benefits such as diversifying issue event alert conditions, refining severity criteria, and facilitating easier assessment of threat and response priorities. This integration allows for real-time response to endpoint threats, reducing the mean time to respond (MTTR) and operational resources.

Practical Usage of AhnLab EDR (3): Deriving breach incident analysis and threat response measures through integration with AhnLab's professional services

(3) Integration with AhnLab Professional Service - Providing Optimal Response Measures

When AhnLab EDR is integrated with MDR and AhnLab Professional Service, South Korea's top malware analyst experts provide detailed analysis of the functionalities and characteristics of malware files that have entered the organizations, including download, replication, creation, and network activities. The experts then provide response measures based on the suspicious activity information. AhnLab EDR also provides analysis reports summarizing basic information about the malware, its malicious nature, and activity information.

Furthermore, digital forensic techniques are used to analyze the impact and infection paths of breach incidents, managing risks and preventing the recurrence of incidents such as APT attacks.

Conclusion

AhnLab EDR is an essential security solution for all organizations that need protection against malware infections and security breaches. However, EDR should not be implemented with a one-size-fits-all approach. Since EDR is inherently a heavy solution with extensive detection and analysis information, various factors, such as the size of the organization, current IT infrastructure, cost, and specific usage scenarios must be considered. It should also be noted that EDR offers greater security value when integrated with other products rather than operating alone. It is advisable to thoroughly review the areas within the existing IT environment that can benefit from EDR and customize the implementation accordingly. Consulting with specialized experts like AhnLab can also be highly beneficial.

For more detailed information about AhnLab EDR, please visit our website.

▶ Go to AhnLab EDR Product Introduction Page

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com/en | global.sales@ahnlab.com