

Case Study

Securing Visibility is Key: Company R's EDR Success Story

Industry

Specialized Credit Finance Business

Benefits

- Quick identification of ransomware and malware inflow paths
- Detection of previously unknown threats
- Enhanced behavior-based visibility for internal users and devices
- Blocking C2 (Command & Control) traffic to minimize additional damage
- Acquisition of foundational data to improve internal security policies and operational procedures
- Strengthened response capabilities through visibility across all stages (before, during, and after an attack)

Solution

AhnLab EDR

Overview

Company R is a leading financial institution that offers a wide range of credit card products and services supported by one of the largest distribution and service networks in South Korea. Due to the nature of the financial industry, maintaining a high level of security is essential, and a stable security framework is critical for preserving customer trust.

However, Company R recently suffered repeated ransomware attacks that caused significant operational disruptions. There were difficulties in securing the files necessary for attack analysis, delaying the identification of the infection source. As a result, both response and recovery processes were slowed even further. Facing these challenges, Company R recognized the need for a new solution that could bolster security without compromising operational efficiency.

The company already operates a multi-layered security architecture that aligns with financial-sector standards, including firewalls, intrusion prevention systems (IPS), and malware-response solutions. However, threat actors have recently been masking their malicious behavior as normal activity or exploiting legitimate tools to evade detection. As abnormal outbound communication attempts from internal endpoints continue to rise, securing visibility that allows teams to identify and analyze suspicious behavior itself—beyond simply determining whether something is malicious—has become an essential task.

Facing this shift in the security landscape, Company R recognized the need for a solution capable of closely analyzing threats based on a wide range of endpoint activities. To address these challenges, Company R adopted AhnLab EDR. By collecting and analyzing endpoint behavior in real time, and combining this capability with AhnLab's threat analysis expertise, the company established a foundation that allows it to effectively detect and respond to even previously unknown threats.

Challenge

- Limited ability to analyze recurring ransomware infection causes and entry vectors
- Burden of detecting unknown threats while maintaining operational efficiency
- Existing systems have limitations in behavior-based analysis and recurrence prevention
- Lack of visibility into internal user behavior makes it difficult to improve security policies

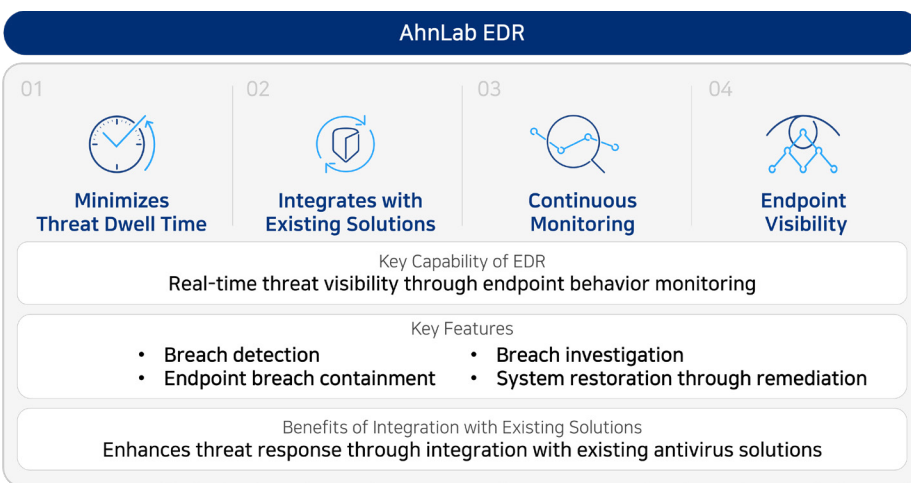


Figure 1. Key Benefits and Features of AhnLab EDR

Challenge

1) Repeated ransomware infections from relying solely on known threat detection

Company R was finding it difficult to block modern ransomware using only signature-based and policy-based detection. Actual user PCs continued to be reinfected, leading to interruptions in daily operations. The core issue was the lack of behavior-based visibility needed to analyze how ransomware was entering the environment and what was causing the infections.

2) Growing need to detect unknown threats without disrupting productivity

As ransomware attacks became more sophisticated, Company R needed more than simple blocking measures. They required the ability to detect missed threats, check attack paths, and build a system that could prevent recurrence.

They evaluated several products, including DRM, document-centralization tools, and traditional ransomware-response solutions. However, these products made it difficult to meet both security and productivity needs because they caused ▲ additional login and document-handling steps ▲ limited visibility into threats beyond ransomware ▲ insufficient behavioral data for analyzing infection causes ▲ and limited recovery and resilience capabilities.

3) Lack of visibility into internal user behavior, leaving no foundation for improving security policies

A ransomware attack does not end with a single file download. It unfolds through a combination of user actions and the threat actor's preparatory steps. However, with the existing system, it was difficult to understand basic user behavior, such as why a file was accessed or downloaded, what websites were visited, or whether the user had been exposed to spear phishing.

As a result, there was not enough objective evidence to improve firewall and IPS policies. At the same time, the lack of visibility into endpoint behavior meant threat actors could still establish footholds inside the network.

Solution & Results

Company R operates a network-segmented environment that separates devices with Internet access from devices that connect to internal business systems. However, due to the nature of their work, they often need to bring externally collected information into the internal network, and because of this, it is structurally difficult to completely isolate core business systems and related servers from the outside.

Solution & Results

• Internet Network Monitoring

Monitoring malware entry paths, RDP access, browser connections, and data leakage

• Business Network Monitoring

Monitoring suspicious activity events, inbound and outbound flows between networks, and server SSH and RDP connections

AhnLab EDR provides behavior-based detection capabilities for various malware including ransomware, and collects diverse activity information occurring before and after infection on endpoints to comprehensively analyze user behavior. Through this, it becomes possible to visualize not only the simple inflow and execution of malware but also the threat actor's early breach attempts to establish a foothold, actions taken to evade security solution detection, and the full activity flow across all stages of the attack.

Company R applied AhnLab EDR to both Internet-connected devices and internal business network devices, and performed behavior-based analysis focusing on the following points in each area:

1) Internet network

- Tracking entry paths when malware detection occurs and linking with AhnLab V3
- Monitoring abnormal RDP access attempts targeting Internet-connected devices
- Analyzing user browser access behavior
- Checking whether internal business data is leaked externally

2) Business network

- Comprehensive monitoring of suspicious activities through AhnLab EDR
- Analyzing inbound and outbound events between the business network and the Internet network
- Checking SSH and RDP access activities from internal devices toward servers

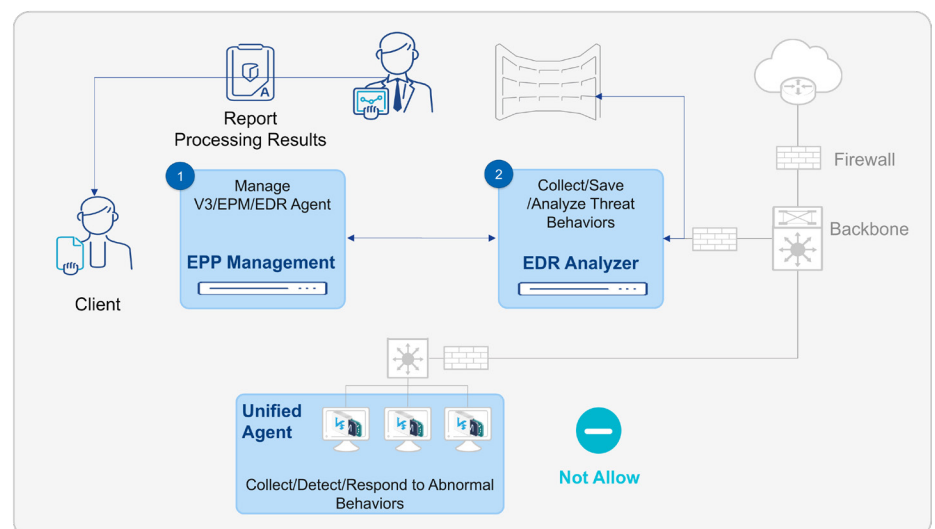


Figure 2. Company R's AhnLab EDR Deployment Status

Benefits

1) Easy identification of malware entry paths and recovery

In the past, when ransomware or other malware infections occurred, it was difficult to identify the entry path, and formatting the device or deploying a replacement PC was practically the only response. Even after formatting and reinstallation several times to trace the entry path, downtime only grew longer, and it was structurally difficult to secure analysis data that could be used for preventing recurrence.

After deploying AhnLab EDR, even when AhnLab V3 does not directly detect the malware, it becomes possible to estimate a significant portion of the entry path by checking suspicious activity events such as large-scale file extension changes together with user actions at that time.

Benefits

- Significant reduction in time required to track malware entry paths and restore systems
- Visibility into internal user behavior and grounds for policy improvement strengthened
- Prevention of additional damage and spread suppression through blocking C2 communication
- Identification of unknown threats that are difficult to detect with existing systems and behavior-based detection strengthened.
- Snapshot-based remote restoration improves business continuity and minimizes device downtime

In addition, based on C2 connection information occurring on the device, it becomes possible to take further action such as immediately blocking external communication through the firewall.

Furthermore, through AhnLab EDR's snapshot restoration function, remote restoration to a point before the ransomware infection can be performed, greatly reducing the time needed to normalize devices and quickly restoring business continuity.

2) Expanded visibility into internal user behavior

AhnLab EDR provides visibility not only into malware detection but also into overall internal user behavior. Through this, it becomes possible to check not only unauthorized SSH and RDP access attempts to internal servers but also abnormal behavioral patterns from internal systems and solutions that previously could not be captured.

In particular, such unauthorized access or abnormal execution and registration match the typical signs that appear when a threat actor plants a backdoor or registers malicious scripts in the Windows Task Scheduler or registry. If the same type of behavior leads to an actual attack, AhnLab EDR detects it and alerts security teams, supporting early blocking.

Based on this, Company R secured a basis for improving internal security policies and operational processes, such as supplementing configuration deficiencies and reorganizing access policies and business procedures. In this way, Company R secured visibility and analysis capabilities that spanned not only devices but also internal user behavior through AhnLab EDR.

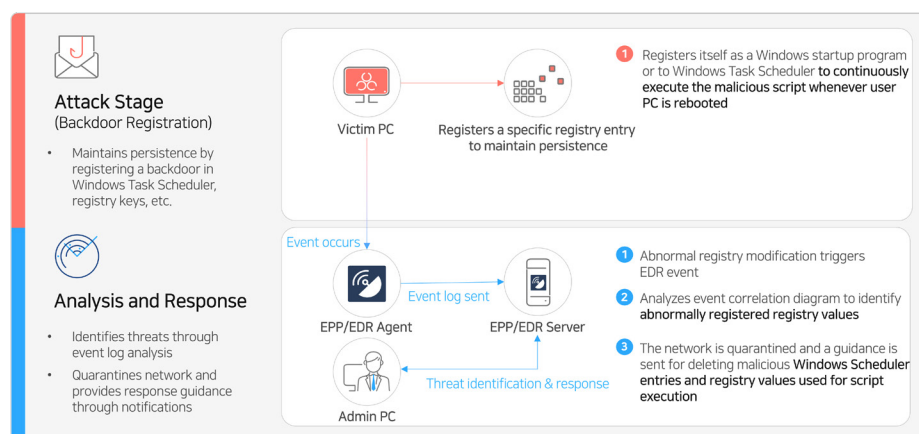


Figure 3. Registry-Based Persistence Attack and AhnLab EDR Response

Conclusion

In this way, Company R has steadily responded to known threats, but repeated ransomware infections and increasingly sophisticated attack methods placed clear limitations on relying solely on their existing response framework. By deploying AhnLab EDR and securing broad behavior-based information at the endpoint level, the company established a foundation that allowed it to clearly identify malware entry paths and abnormal activities occurring before and after an attack, information that had previously been difficult to determine. Through this, the company was able to clearly trace the causes of repeated infections, minimize downtime, and strengthen their root cause analysis system for preventing recurrence.

In addition, AhnLab EDR provided visibility into internal user behavior, enabling early identification and response to various risk factors such as unauthorized access, abnormal communication, and abnormal activity within internal systems, areas that were difficult to control with existing security measures alone. As a result, Company R built a practical security framework that not only blocked malware but also strengthened business continuity and enabled comprehensive improvement of internal operational processes and security policies.

