AhnLab

White Paper

Unified Security for Optimal Ransomware Protection

Recent incidents of ransomware infection show that cyber attacks have entered a new phase. Ransomware attacks that were previously limited to simple file encryption or monetary demands have now evolved into complex attacks involving data breaches, service disruptions, and reputational damage. The impact is no longer limited to a single company, and threat actors have changed from being "entities that instill fear after infection" to "entities that infiltrate and lie dormant".

Even advanced ransomware attacks like these may appear unpredictable on the surface, but in fact, there is a clear pattern within them. Therefore, even if accidents cannot be predicted, responses can be made predictable. This philosophy is precisely the starting point of AhnLab's "integrated ransomware security strategy".

Challenges

Ever-evolving ransomware attacks pose new challenges to companies. There are several challenges, but they can be broadly summarized into the following three.

#1. Response to New Ransomware and Variants: New ransomware and their variants continuously emerge, making it challenging for defenders. To effectively respond to such ransomware, it is necessary to go beyond blocking with a single solution. A platform-first strategy that analyzes the malicious behavior caused by ransomware and supports integration of multiple solutions is needed.

#2. Protection Across Various Domains: Recent ransomware attacks occur in different domains such as endpoints, networks, and emails. Skilled threat actors carry out campaigns across various attack vectors to achieve their goals and maximize damage. If a company protects only one area, it becomes vulnerable to attacks that bypass the security solution of that domain or enter through other vectors.

#3. Establishing a Recurrence Prevention System: Ransomware attacks do not end with just one block. Similar attacks can be carried out again at any time, and this trend is particularly noticeable when looking at recent attacks with advanced stealth techniques. To prevent the cascading damage caused by ransomware, a security system capable of hunting cyber threats, beyond just detection and blocking, is needed.

It is about a "Process," not a Product

To address new challenges, organizations generally increase the "number" of security solutions. This trend is appearing across the world.

According to a survey by Gartner in 2024, respondents from 162 global large enterprises reported operating an average of 45 cybersecurity solutions. In the previous year, 2023, the average was 43, which was not significantly different, and half of the respondents said they were not properly utilizing all products.

The number of security solutions varies by company size, industry, and country, but the complaints about operational complexities are the same. Whenever we analyze breach cases, there are far more cases of damage due to "insufficient utilization" rather than the "absence" of security solutions.

Cybersecurity expert Bruce Schneier left the famous quote, "Security is a process, not a product." It means moving beyond the static state of adopting security solutions and using their features in a fragmented manner, to making dynamic efforts to enable them to operate organically and collaborate with people.

Unified Security for Optimal Ransomware Protection

AhnLab provides a platform-based offering optimized for ransomware protection, in consideration of the sophistication of ransomware attacks, the challenges companies face in the field, and the importance of unified security. The solutions that make up our ransomware security offering perform their respective roles but are flexibly integrated, operating as a single security ecosystem where the "detection-analysis-response" cycle organically circulates. This enables customers to create a dynamic security structure that addresses cyber attacks from the beginning to the end.

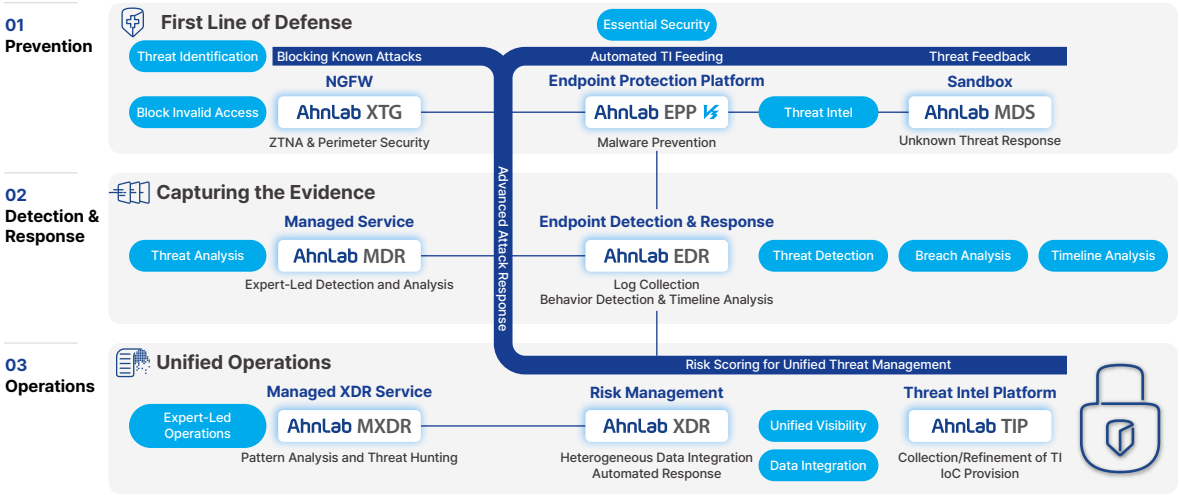

Figure 1. Our platform-based ransomware security offering

AhnLab has established an integrated system connecting next-generation firewall (ZTNA), antivirus (EPP), sandbox, EDR, MDR, XDR, MXDR, and threat intelligence (TI). The next-generation firewall ensures trust at the access stage through user and device verification, while EPP and sandbox detect and block malicious activities in advance. EDR and MDR track endpoint events and provide expert analysis, and XDR and MXDR deliver integrated visibility and automated response. All of them are fueled by the latest threat intelligence.

Stage	Solution	Role
1. Prevention	AhnLab XTG	Access control through user/device verification (ZTNA)
	AhnLab EPP (V3)	Detection and prevention of known malware
	AhnLab MDS	Sandbox analysis – detection & prevention of unknown malware
2. Detection and Response	AhnLab EDR	Collection, analysis, and response to endpoint events
	MDR service	Expert-led endpoint threat detection, analysis, and response
3. Operations	AhnLab XDR	Risk scoring-based unified threat management
	MXDR service	Expert-led cross-domain pattern analysis and threat hunting
	AhnLab TIP	Provision of threat intelligence including IoCs

Table 1. Roles of each solution

The detailed information regarding the roles of security solutions is as follows.

Stage 1: Prevention - Stop Ransomware Before They Arrive

① AhnLab XTG – ZTNA-Based Verification and Access Control

The next-generation firewall AhnLab XTG is a solution that implements zero trust network access (ZTNA) in real network environments. Integrating with endpoint security solutions like AhnLab EPP and AhnLab V3, it continuously verifies the identity of users and devices, realizing the zero trust security model that "trusts no one by default."

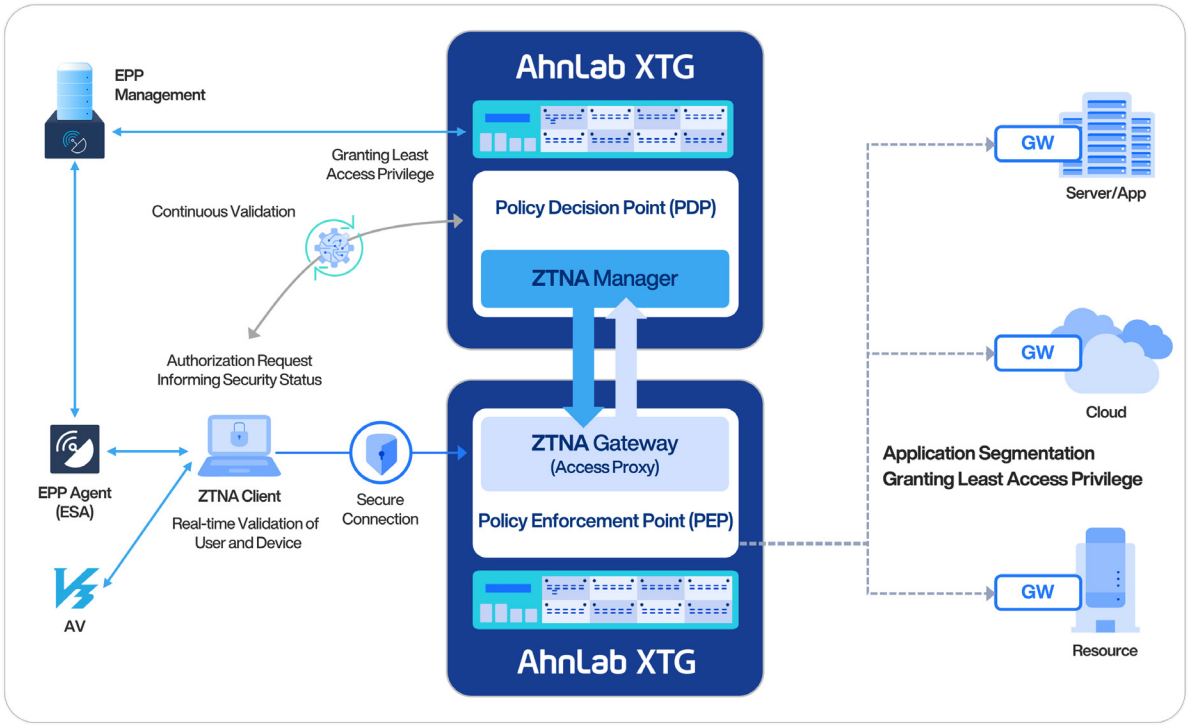

Figure 2. AhnLab XTG – ZTNA architecture

AhnLab XTG controls unauthorized users and devices with insufficient security, and internal access beyond permissions in real-time. In the network domain, it completely blocks the first gateway of internal intrusion and completes an integrated access control from the network to the endpoint.

In summary, AhnLab XTG delivers a zero trust security as the "central axis of verification" to defend against the latest threats that traverse internal and external boundaries of the organization.

② AhnLab V3 – The First Line of Defense at the Endpoint

AhnLab V3 is an antivirus (AV) solution that has been trusted by businesses and organizations for over 30 years. It is a product with excellent performance and technology, and it provides tailored defense capabilities, such as real-time prevention, scan management, and exception policy management based on the user environment. Even when using the same V3, the security depends on how properly it is managed.

AhnLab V3 centers around the following key features to detect and prevent ransomware.

A. Signature-Based Detection

AhnLab V3's fundamental detection consists of signature-based "Real-Time Scan" and "Smart Scan." It immediately blocks known malware and performs additional inspection on suspicious objects. The signature database is constantly updated so that the product can address the latest cyber threats.

B. Ransomware Security Folder

V3 users can configure the folder that must be protected from ransomware. It is called "Ransomware Security Folder" and it can only be accessed by allowed processes. For example, if you specify that only legitimate apps like PowerPoint or Excel can access, ransomware cannot affect the folder.

When AhnLab examines customers' ransomware incidents, we often find that although V3 has been implemented, the ransomware security folder is not used. The folder is one of the most crucial features for protecting critical business data when the system is infected with ransomware.

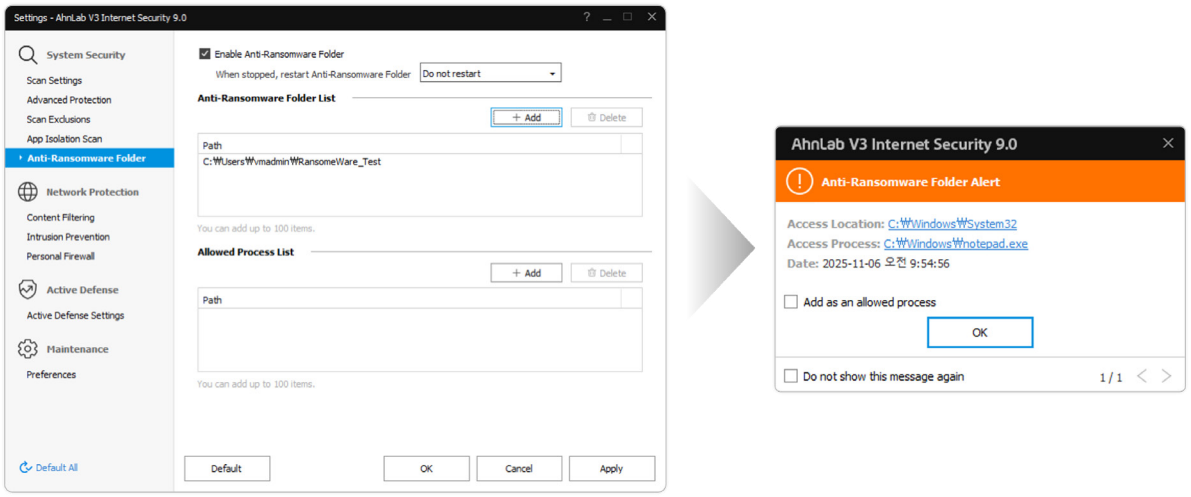

Figure 3. AhnLab V3 – ransomware security folder

C. App Isolation Scan

AhnLab V3 provides the app isolation scan, which executes suspicious files in a virtual environment on the desktop and scans them based on behavioral detection technology. By utilizing this feature, users can scan threats before they occur to prevent the spread of damage even if ransomware infiltrates the system.

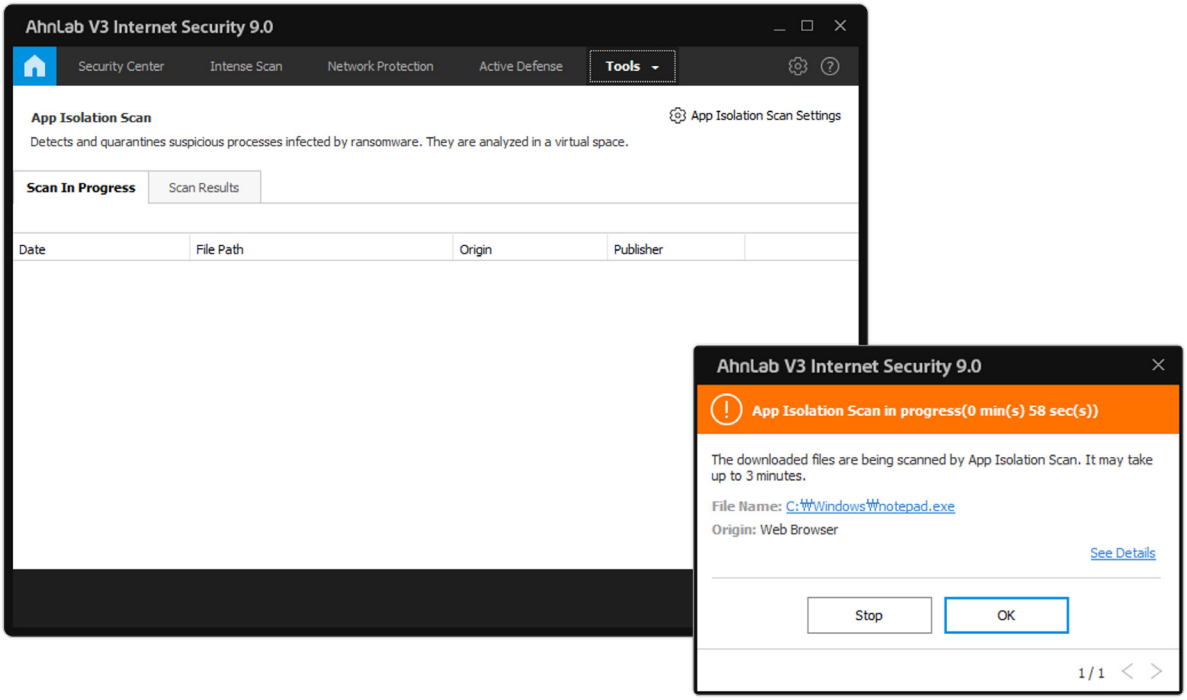

Figure 4. AhnLab V3 – app isolation scan

Additionally, using V3 with AhnLab EPP allows for the integrated management of detection status, policies, and events, enabling a faster response. EPP goes beyond protecting a single desktop or server by providing centralized monitoring of the security status of all endpoints in an organization. A security manager can understand detection events of individual devices and perform unified responses utilizing various security features, such as patch management, and device control.

Recently, with the increase in vulnerabilities and malware in Linux servers, the importance of the EPP-powered central security management is growing. By operating AhnLab V3 and AhnLab EPP together, users can secure both endpoint protection capabilities and operational efficiency.

③ AhnLab MDS – Sandbox Analysis for Blocking Ransomware Before Executed

AhnLab MDS is a sandbox solution that defends against unknown malware across network, endpoint, and email, minimizing the response gap after detection.

First, AhnLab MDS analyzes files and traffic moving across network domains in a virtual machine (VM) to perform execution holding and behavior analysis. When the agent detects suspicious file on the user's desktop even at the endpoint level, AhnLab MDS automatically collects it and monitors its behavior in a sandbox. If it detects abnormal activities, such as encryption, deletion, or unauthorized access within a certain timeframe, it immediately blocks execution. Additionally, AhnLab MDS tracks devices with potential infection and prevents internal spread by delivering the analysis results to the admin console.

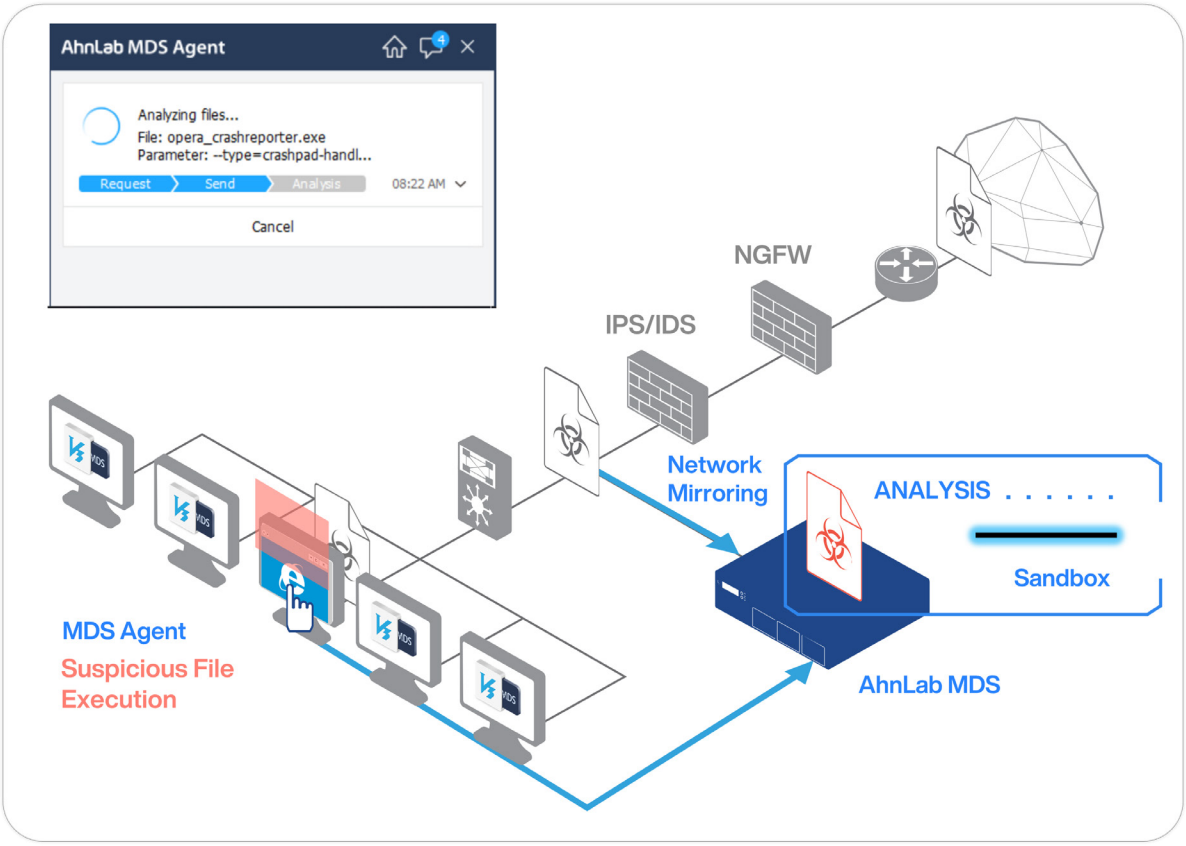

Figure 5. AhnLab MDS - sandbox analysis and prevention before execution

In the email domain, AhnLab MDS's Mail Transfer Agent (MTA) performs a comprehensive scan of the email header, body, URLs, and attachments. It directly accesses URLs included in the body to scan potential threats and analyzes attachments in a virtual environment. Malicious emails are quarantined to prevent them from entering the system.

In addition, AhnLab MDS provides a "malware analysis request" feature, supporting the sending and reporting of suspicious files to AhnLab's expert analysts. Administrators can use the analysis report to identify the threat type, infection path, and whether it has spread, allowing them to take swift action.

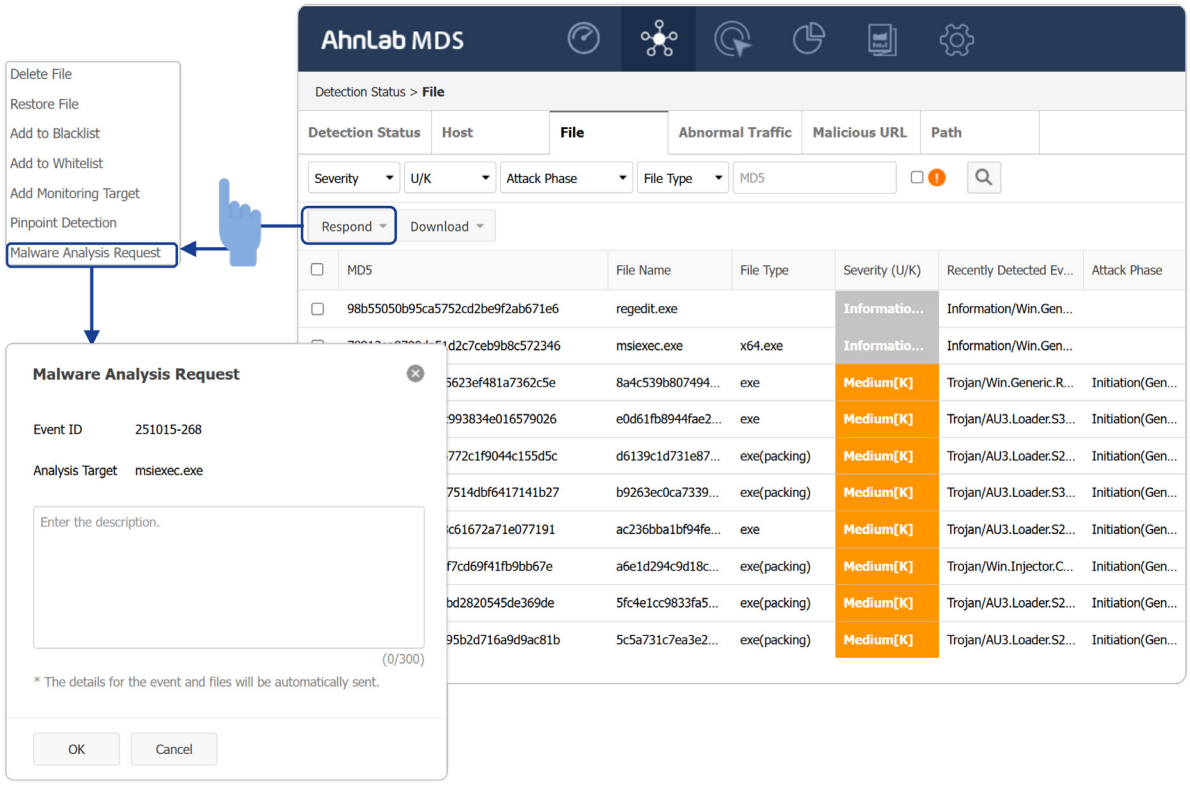

Figure 6. AhnLab MDS – malware analysis request

Stage 2: Detection & Response – Contain Cyber Threats

① AhnLab EDR – A Deep Understanding of Context

AhnLab EDR is not just a simple event monitoring tool. It records all activities occurring at each endpoint by time and process and analyzes the context of attacks to reconstruct the flow of threats. In other words, it recognizes threats based on the "correlation between behaviors," rather than on a single event. Through this, it supports the user's endpoint threat management, minimizing the dwell time of unknown threats, and preventing potential damage and recurrence.

AhnLab EDR also has features specialized for ransomware security. The major features are as follows:

A. Auto Roll Back

It restores files to their state before the point of infection. In the past, administrators had to perform rollbacks manually, but this features enables automated recovery immediately upon ransomware detection.

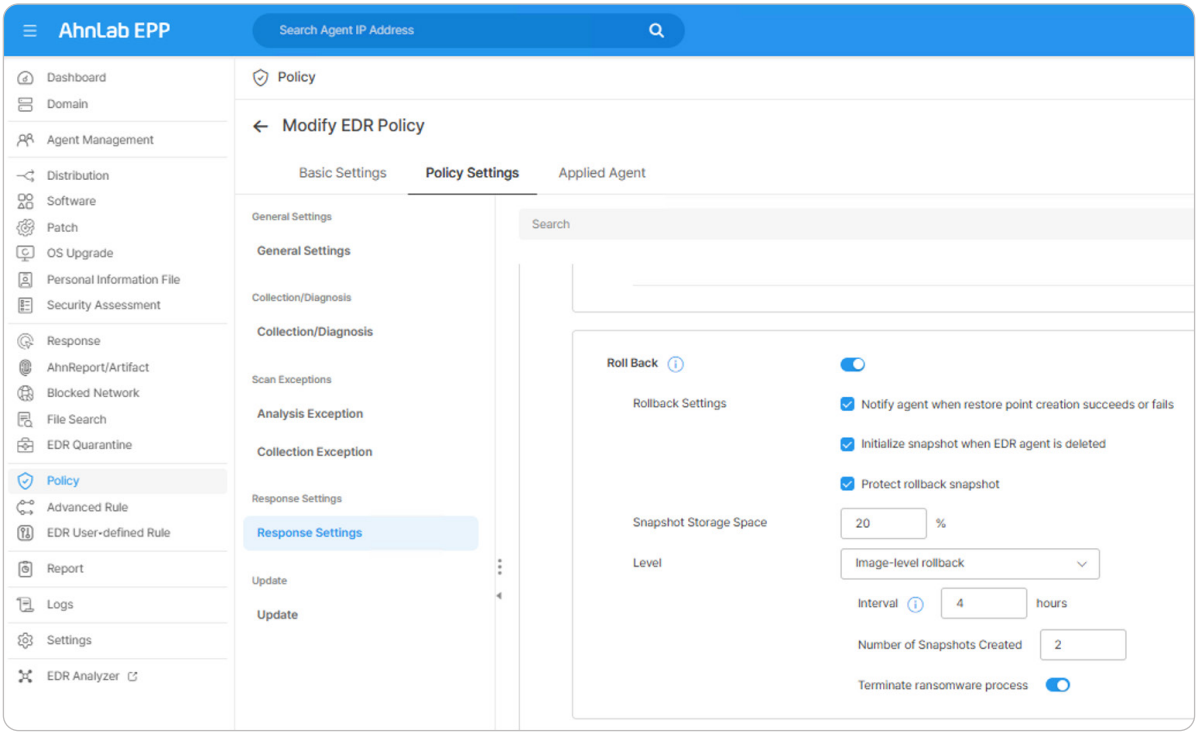

Figure 7. AhnLab EDR – automatic roll back feature

B. Security News & IoC Widget

AhnLab EDR automatically collects IPs, URLs, hash values, etc., provided in the latest security advisories from AhnLab TIP, and compares and analyzes them with EDR logs. Admins can immediately identify "at-risk devices" related to the news, allowing them to reduce the MTTR (Mean Time To Respond).

AhnLab EPP (V3), MDS, and EDR, as explained so far, play a key role in our ransomware security offerings. EPP (V3) provides primary endpoint protection, MDS analyzes and blocks abnormal network-endpoint-email behaviors, and EDR analyzes and responds to all endpoint events. These three solutions flexibly interoperate to establish a multi-layered security architecture that delivers dynamic threat detection, analysis, and response.

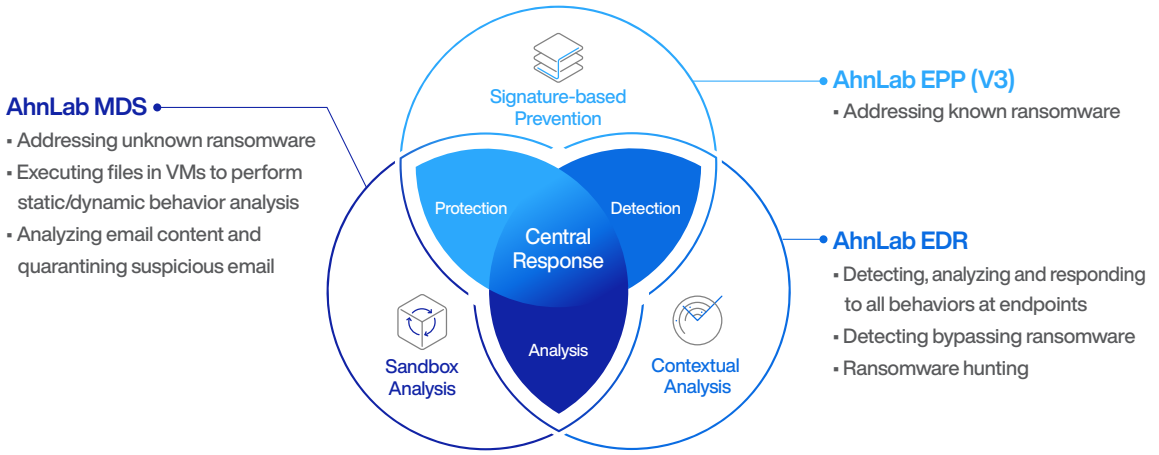

Figure 8. Integrated security framework (V3-MDS-EDR)

② MDR – Human-Centric Endpoint Detection and Response

MDR (Managed Detection & Response) enables a threat response process enhanced by human expertise. Our security experts monitor cyber threats detected by AhnLab EDR 24/7 and proactively hunt for signs of intrusion. When an anomaly is detected, we perform rapid detection and response based on established processes to keep our customers safe in real time.

The strengths of our MDR are real-time analytics and communications. We determine whether the event is a single behavior or the start of a chain attack. Then, we propose response measures considering the risk level, possibility of propagation, and business impact. Even customers with a shortage of security manpower can enjoy exceptional expert-led threat detection and response capabilities.

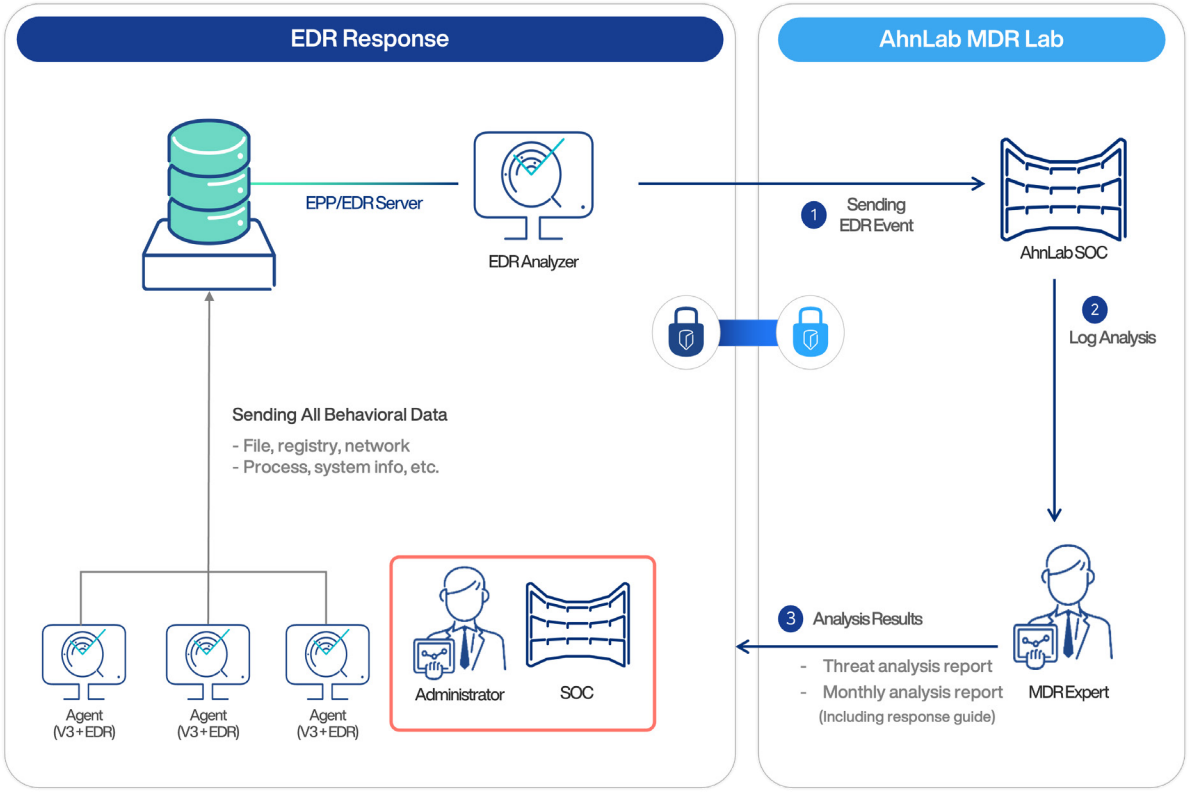

Figure 9. MDR service – operational process

In summary, the combination of EDR and MDR completes a real-time threat response workflow that people and technology work together. Even if an adversary gains access to the system, defenders can contain malicious activities in this stage.

Stage 3: Operations - Unified Management Ensuring Resilience

The latest threats, including ransomware, do not discriminate between security domains. Therefore, ensuring unified visibility across all security vectors has become the top priority.

① AhnLab XDR – A Cross-Domain Security Hub

AhnLab XDR integrates and visualizes various logs from different domains, including endpoints, networks, clouds, and emails, and analyzes the correlation between events to understand the entire flow of an attack. It reconstructs fragmented IoCs into a single context so that security managers can easily understand the status and impact of cyber threats.

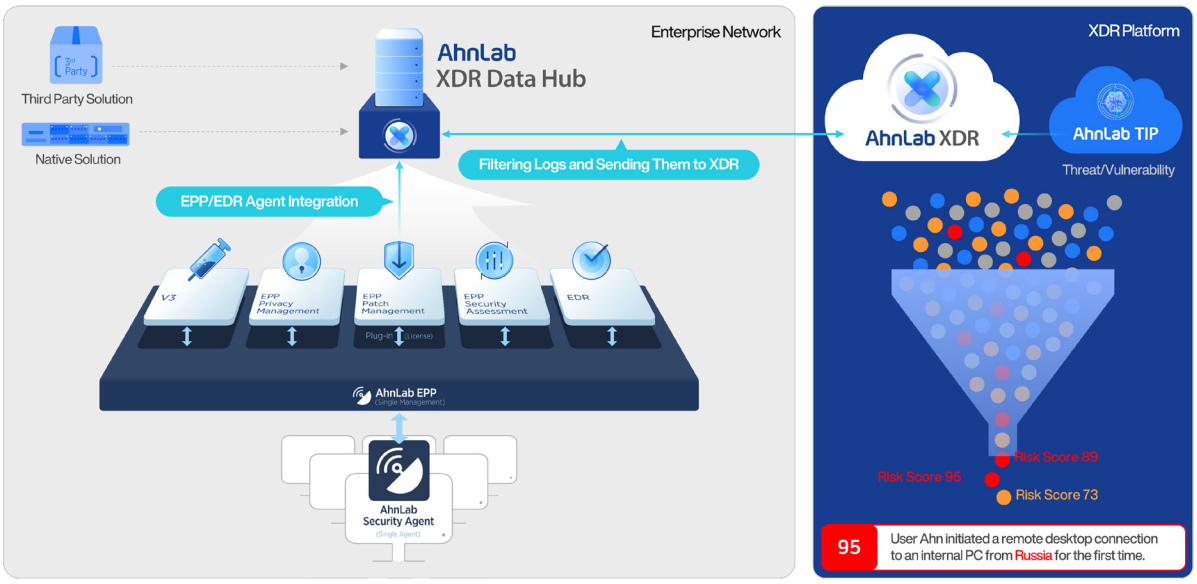

Figure 10. AhnLab XDR – centralized data processing and correlation analysis

Our XDR quantifies threat severities using a risk index, allowing customers to clearly determine response priorities. The generative AI "AhnLab Annie," integrated into AhnLab XDR, supports the user's entire security decision-making process. Additionally, its open XDR architecture allows seamless integration with third-party solutions, enabling customers to make their security systems more dynamic and scalable.

② MXDR – Centralized Security Operations Perfected by Experts

As for our MXDR service, experts directly manage and respond to cyber threats based on analysis into cross-domain data. The MXDR service remotely operates the customer's AhnLab XDR platform, performing 24-hour monitoring, threat hunting, risk management, and more. An expert analyzes anomalies, assesses the business impact, and provides optimal response guides.

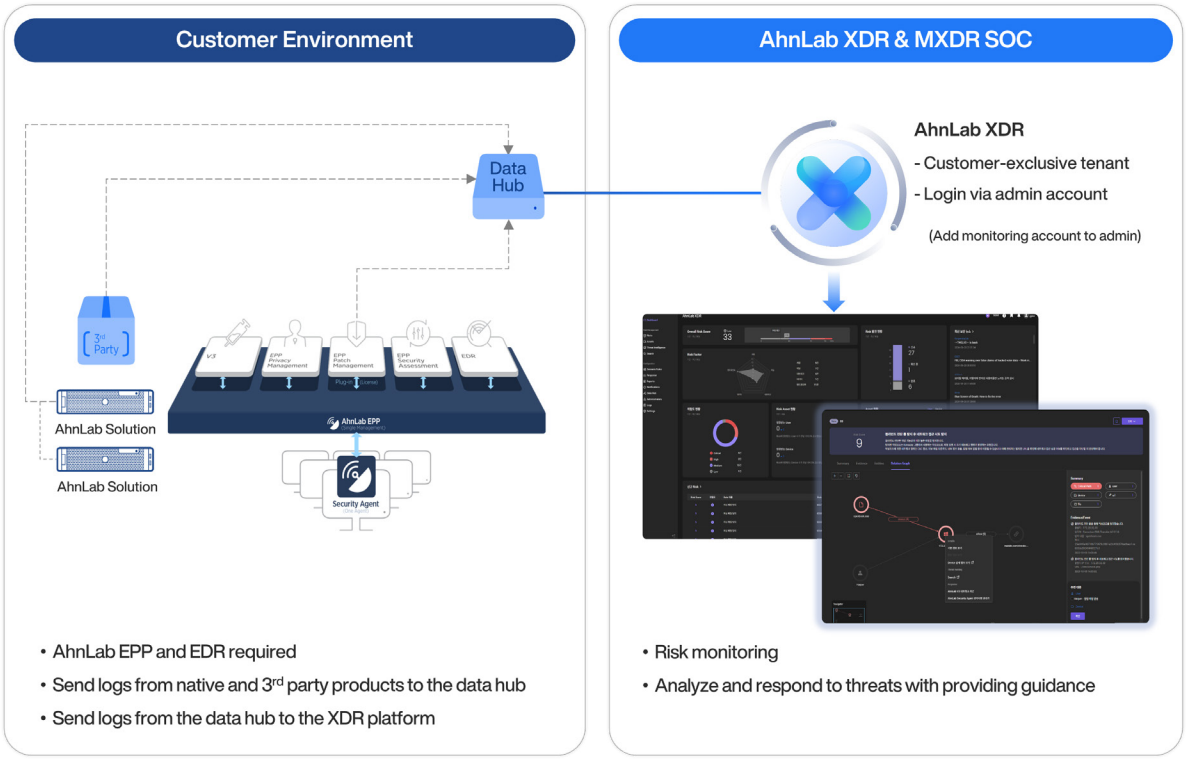

Figure 11. AhnLab MXDR's threat response architecture

MXDR is not a traditional managed security service (MSS); it is a hybrid operational model where experts continuously collaborate with customers as part of their security team. By combining XDR's data-driven risk management capabilities with human analytics, the service truly completes the process of threat detection, analysis, and response.

③ AhnLab TIP – Fueling Threat Intelligence to Security Solutions

AhnLab TIP is an industry-leading threat intelligence platform that delivers the latest IoCs, threat actor analysis, and cyber attack tactics (TTPs) information. It standardizes the threat information collected across the world to implement "predictable cybersecurity" by identifying the behavior patterns of adversaries.

AhnLab TIP flexibly integrates with our major solutions, including AhnLab EPP, AhnLab XTG, AhnLab EDR, and AhnLab XDR. It automatically feeds newly detected IoCs and related information to each product. AhnLab TIP fuels threat intelligence to our security products, and it is part of a unified security framework that encompasses comprehensive visibility, correlation analysis, and automated response.

Thanks to this flexible security architecture, our solutions are armed with a robust defense capabilities that incorporate data collection, threat detection, prevention, and response in real-time. AhnLab TIP is the central hub of this process, helping organizations stay response-ready against seemingly unpredictable cyber threats.

Rigorously Assessed Technology

The core solutions that make up our ransomware security offering have been demonstrating their excellent technical capabilities by achieving outstanding results in global cybersecurity evaluations.

First, AhnLab V3 has been continuously validated in AV-TEST since 2013 and has received certifications more than 60 times. In 2025, it earned perfect scores in the "Advanced Threat Protection Test (ATP Test)," demonstrating its ability to prevent sophisticated attacks. The ATP Test evaluated the product's detection and prevention capabilities using ten cyberattack scenarios designed based on the MITRE ATT&CK Framework.

Additionally, AhnLab EDR and AhnLab XDR achieved exceptional results in the MITRE ATT&CK Evaluation, one of the most trusted global security product tests. In Round 6 conducted in 2024, AhnLab EDR and XDR detected 95% of emulated behaviors carried out by major ransomware groups CL0P and LockBit across both Windows and Linux. The result is at the highest level among cybersecurity vendors worldwide.

In particular, out of 56 substeps detected, 49 received Technique which is the highest rating. It indicates that our customers can thoroughly understand the underlying context (how and why) of malicious behaviors and make informed decisions by referring to the evidence of our solutions.

As such, our industry-leading security solutions are constantly verified and strengthening customer trust.

Conclusion: People and Technology Complete Security

Ransomware is no longer a single-method attack. Even after infiltration, there is a complex attack chain involving lateral movement, internal spread, and data exfiltration. What is needed now is not a list of security solutions, but a dynamic architecture that can predict potential cyber threats.

Our unified anti-ransomware strategy is a model that realizes a proactive cybersecurity process. Through incorporating user and device verification (XTG) – threat detection and prevention (EPP & MDS) – endpoint behavior analysis and hunting (EDR) – expert-led endpoint detection & response (MDR) – centralized risk management (XDR) – expert-led cross-domain threat response (MXDR) – threat intelligence (TIP), our anti-ransomware offering quickly identifies cyber threats, and experts interpret the context and address cyber attacks. With the addition of AI technology, an optimal ransomware protection eventually materializes.

We are now in an era where "quick and accurate" response to cyber threats is crucial. AhnLab will continue to seamlessly integrate our solutions and services, combining human insight and AI-driven automation into a predictive security system to protect customers' business from ever-evolving threat campaigns.

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, Korea
Learn More: www.ahnlab.com
Contact Us: https://www.ahnlab.com/contact-us
Follow Us: Blog / LinkedIn / YouTube / X