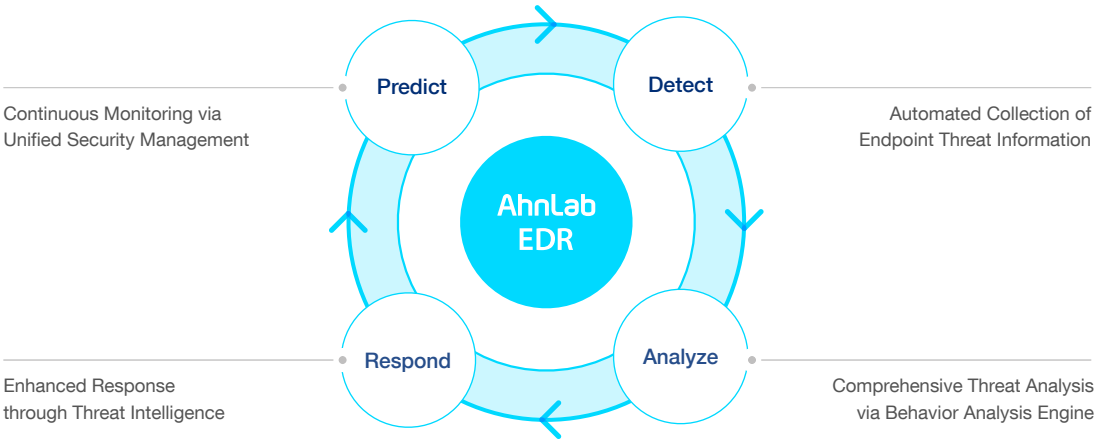
AhnLab EDR

Precise Detection, Advanced Analysis & Response, Proactive Hunting

Through detection, analysis, and response capabilities verified by MITRE ATT&CK evaluations, AhnLab EDR takes initiative in hunting threats to establish robust security for enterprises.

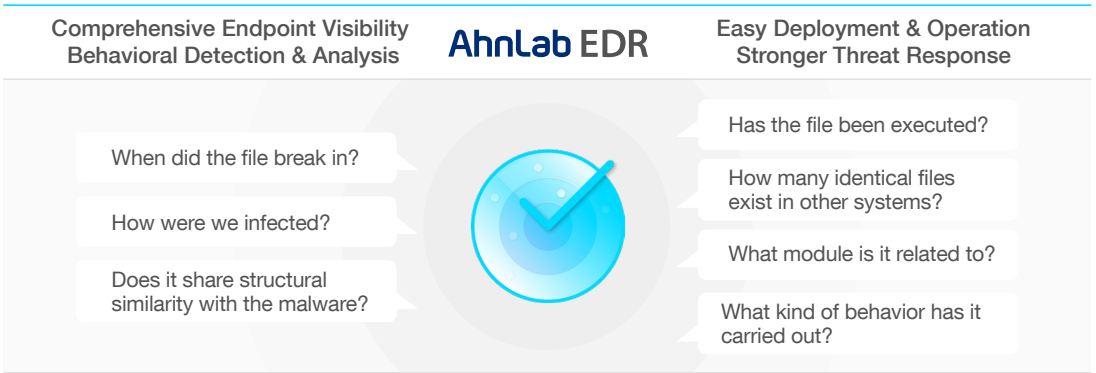
Product Overview

AhnLab EDR is the next-generation threat detection and response solution, providing powerful threat monitoring, analysis, and response capabilities based on our behavior analysis engine. Proven its greatness in MITRE ATT&CK evaluations, AhnLab EDR further reinforces its overall threat detection and response process by integrating with our MDR (Managed Detection & Response) service.



Why AhnLab EDR

Attacks against endpoints are becoming more sophisticated. New malware and variants appear every day, making it impossible to block all threats beforehand. Therefore, enterprises are required to establish a security system that minimizes impact via continuous monitoring and prompt identification of breach incidents. AhnLab EDR provides broader endpoint visibility via detection and analysis of behavior information and enables next-gen threat detection and response with convenient deployment and operation. The solution also actively tracks threats, allowing customers to construct a system that takes preventive measures and avoid recurrence.



Strengths

Convenient Operation

AhnLab EDR provides 'EDR Analyzer', an exclusive console that is the culmination of AhnLab's technological capabilities and expertise. The EDR Analyzer dashboard is designed in a way that allows users to precisely perceive threats from a detection, analysis, and response perspective and configure security conditions accordingly. AhnLab EDR continuously gathers information related to suspicious behaviors based on type, saving them to the EDR Analyzer's central server. Then it adjusts the information into different levels to optimize management and reduce the burden on the storage.

AhnLab EDR Analyzer Dashboard

Advanced Threat Detection and Classification

Powered by our behavior analysis engine, AhnLab EDR independently analyzes global and local threat actors by engineering detection patterns and rules to further elaborate threat detection. In addition, it classifies threats into 16 behavior categories based on the MITRE ATT&CK Framework, enabling the user to identify security risks intuitively. Other information such as threat severity and risk probability is also provided via machine-learning technology.

Professional Analysis and Response

To effectively deal with detected threats, AhnLab EDR offers detailed analysis including threat information from the MITRE ATT&CK Framework, inflow paths, major behaviors, correlations, severities, and links. The analyzed data is then displayed in form of ▲diagrams, ▲process trees, ▲and timelines, allowing the user to easily identify the overall attack flow. Users can also carry out on-demand scans for key behaviors and perform an additional analysis via interoperation with AhnLab TIP and AhnLab MDS.

Default Managed Service Adding Resilience

Among the events detected by AhnLab EDR, primary/secondary reports and statistics-based reports are provided for high severity events, allowing users to utilize the solution more efficiently. Furthermore, threat response can also be implemented under prior consultation with the customer.

*The service is provided by default in AhnLab EDR. However, it cannot be provided if external transmission of EDR detection logs is unavailable.

Proven in MITRE ATT&CK Evaluations

In the fourth round of MITRE ATT&CK Evaluations, AhnLab EDR presented 92% detection rate by detecting 83 out of 90 steps, emulating the most up-to-date techniques used by the 'Wizard Spider' and 'Sandworm'. The result clearly proves our outstanding detection capabilities against advanced threats.

Features

AhnLab EDR classifies threats according to detection type and supports a swift workflow from initial recognition to analysis and response. In addition, it allows endpoint security operations to become optimized to each customer's environment by interoperating with various other solutions and maximizing response capabilities. AhnLab EDR also offers a feature to configure correlated rules with other products in AhnLab EPP.

Detection, Classification, Analysis, and Response to Advanced Threats

- Gathers and saves all behavioral information – users can always verify overall event-related threat information
  - Collects behavioral information on processes, files, registries, networks, and systems
- Allows users to search and view information in detail per information units such as agents, files, and behaviors
- Supports automatic response configuration of user-defined rules (IoC, Yara, static and dynamic behavior rules)
- Immediate response upon threat detection (network block, process termination, rollback, file collection/search/ deletion/restoration, etc.)
- Automatic response through user settings (user-defined rules, advanced rules, preemptive process block based on blacklist hash)
- Creates user-defined report in various formats (CSV, XLS, PDF)
- Analyzes major behaviors and V3-diagnosed malware behaviors via on-demand scans
- Threats classified into 16 categories based on MITRE ATT&CK tactics
- Provides file monitoring information on major malicious behaviors, such as ransomware, injections, network access, C&C connections, system settings alteration, privilege escalation, fileless methods, and information theft
- Collects additional information (AhnReport, Artifacts, Windows event log) for breach response

Platform-based Security Operation and Management

- Establishes a powerful threat response system together with AhnLab EPP
  - Efficient security operation and management with single agent
- Actionable threat response available with flexible policy settings
- Minimizes threat detection and response time based on comprehensive endpoint visibility

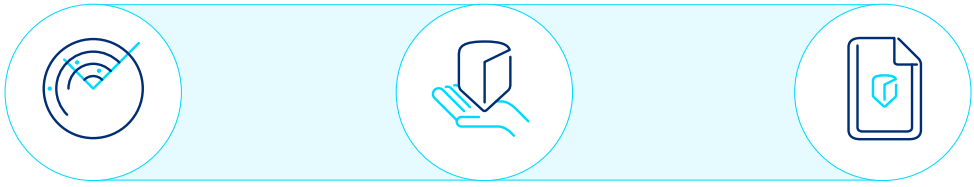
Securing Intelligence and Enhancing Response via Flexible Interoperation

- Ample threat intelligence secured by interoperation with third-party solutions
- Interaction with SIEM, SOAR, integrated logs, and API & Syslog
  - Simple interaction settings through the console and various protocols available (UDP, TCP, TCP over SSL, etc.)

EDR Premium

EDR Premium is the combination of AhnLab EDR and MDR service providing specialized threat detection and response capabilities. EDR Premium customers are assisted by our cybersecurity experts who monitor, analyze, and determine known threats or suspicious behaviors and respond proactively. At the heart of EDR Premium, there is AhnLab's unparalleled threat response expertise accumulated for decades. EDR Premium generates tickets on threats that occur in customer endpoint environments and utilizes reputation and malware behavior information for systematic task implementation based on AhnLab's threat response process. Furthermore, AhnLab offers a wide range of professional services linked to EDR Premium, such as forensics, professional malware analysis, providing various options to improve threat analysis and response capabilities.

*EDR Premium is a charged service; for service cost and other details, please make a separate inquiry.



Threat Detection
Continuous Detection for Wide Range Threat

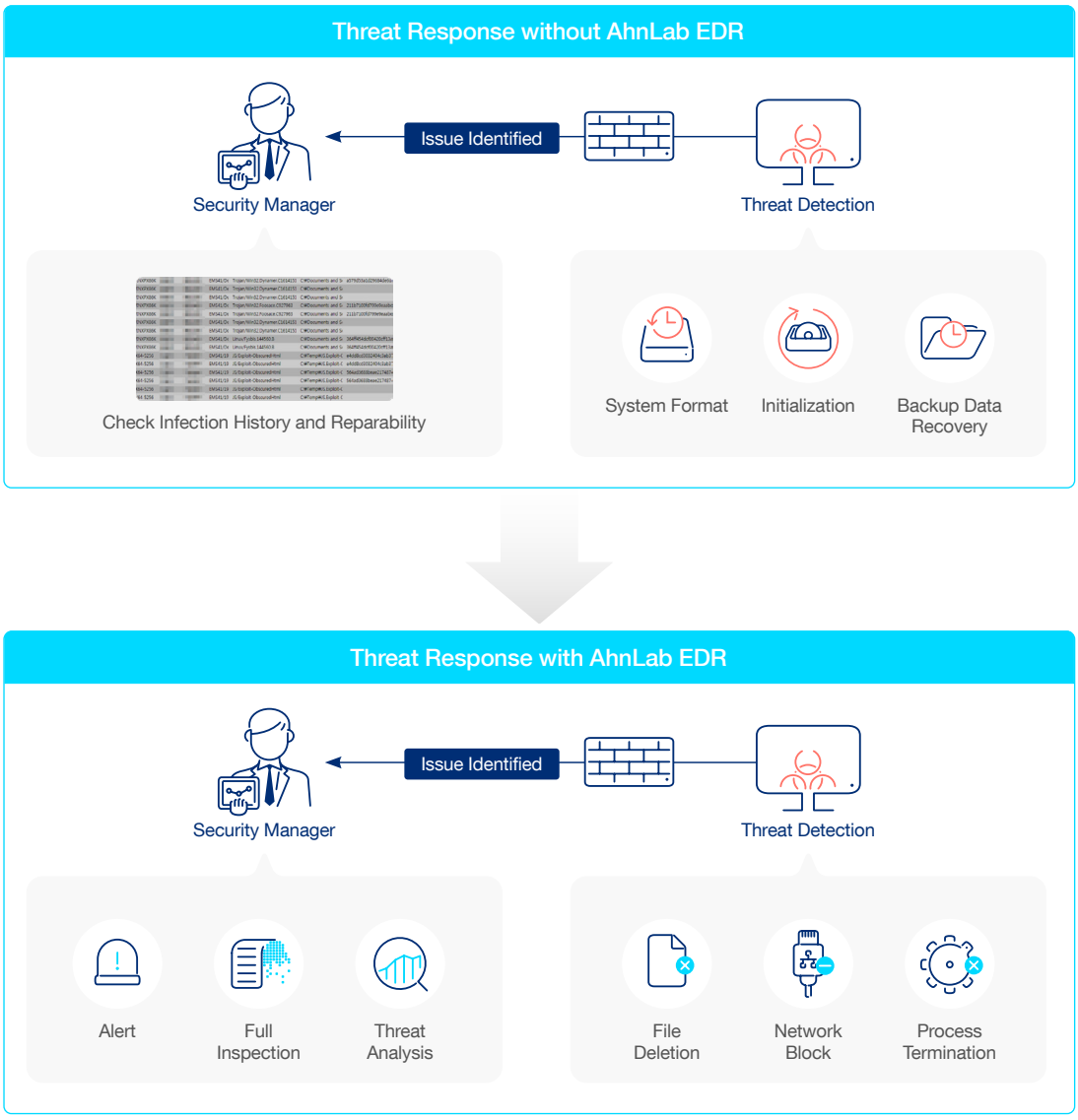
Professional Analysis & Response
Threat Mitigation and Recovery via Proactive Analysis & Response

Report
Enhancing Overall Threat Detection & Response Process

Benefits

When a malware infection is identified in a system without AhnLab EDR, the system is formatted or reset, and backup data is retrieved to resume tasks. The anti-malware management server records the PC malware infection history, but it is impossible to identify the exact path of infection. Therefore, threat response becomes a one-time event, and limitations exist in establishing recurrence prevention measures.

However, with the implementation of AhnLab EDR, users can identify causes, respond with appropriate measures, and establish processes to prevent threat recurrence. When a breach occurs, the administrator receives notification and runs full scan and threat analysis based on predefined rules. Through such measures, appropriate actions can be taken, such as suspicious file collection, process termination, and network isolation. Moreover, AhnLab EDR enables preemptive prevention response and post-detection management through vulnerability and infection record identification.



AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com / global.sales@ahnlab.com
© 2022 AhnLab, Inc. All rights reserved.

AhnLab