AhnLab MDS

The Ultimate Sandbox Solution to Address Unknown Threats

- Sandbox-based file analysis
- Ransomware, malware, malicious URL, C2, and APT detections
- New and unknown threat response along with execution holding

Product Overview

In the past and still till this day, responding to ransomware and other malware remains the most critical component of cybersecurity strategies. Therefore, a solution that can detect and analyze malware entering through network, email, or endpoint domains is an essential requirement. While known malware can be mitigated with existing anti-malware software installed on endpoints, combating unknown threats requires a solution like **AhnLab MDS**.

AhnLab MDS, a sandbox-based file analysis solution, incorporates every aspect of our extensive expertise and experience in file analysis. It executes files in virtual environments (Windows and Linux) and analyzes their behaviors to identify potential cyber threats. The sandbox solution is equipped with multiple analysis engines for both behavioral and static file analysis, enabling precise detection of sophisticated techniques associated with files.

Unknown Threat Response - Sandbox

- Sandbox-based dynamic analysis (OS: Windows 7/10/11, Ubuntu)
- Anti-VM technique for advanced malware detection/analysis and correlation analysis

Cross-Domain Threat Data Collection & Analysis

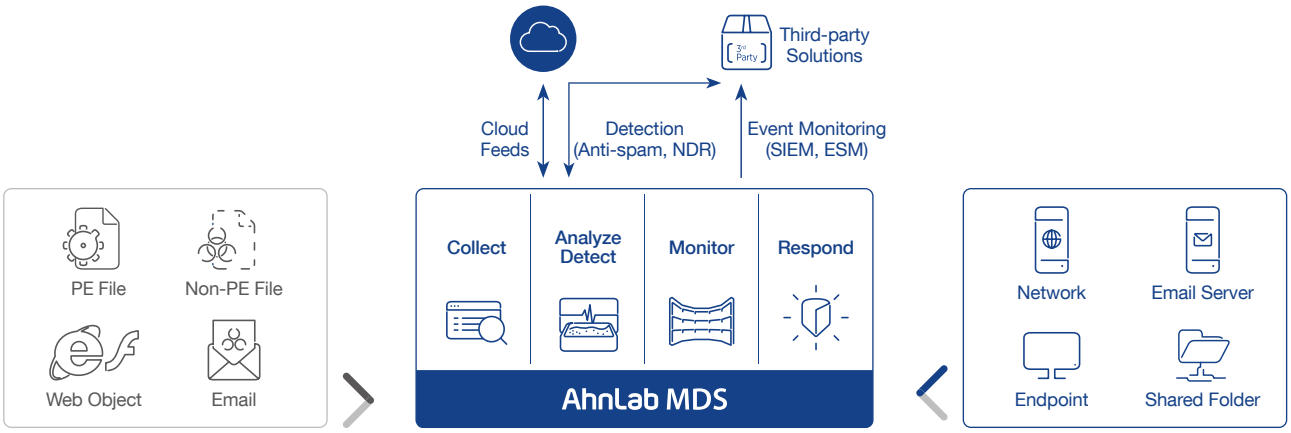
- Real-time collection and analysis of 10G network traffic (HTTP, HTTP/2, FTP, SMTP, SMB etc.)
- File collection and analysis through email license (MTA) and endpoint agents (MDS Agent)

Flexible Integration

- Seamless API integration for in-depth analysis of executable files, documents, emails, etc.
- Integration with various solutions - network bridge, anti-spam, SSL decryption, NDR, etc.

Leveraging Our Latest Threat Response Techniques

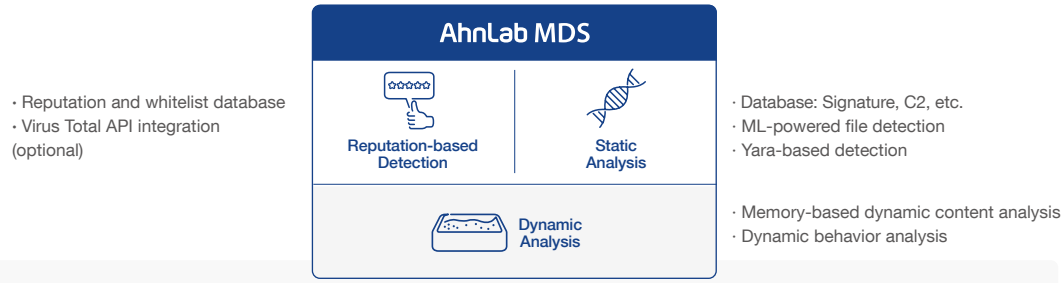
- ML-powered detection of fraudulent phishing emails that evade rule-based detection
- Various analysis-supporting tools, such as AhnLab TIP integration and expert analysis service



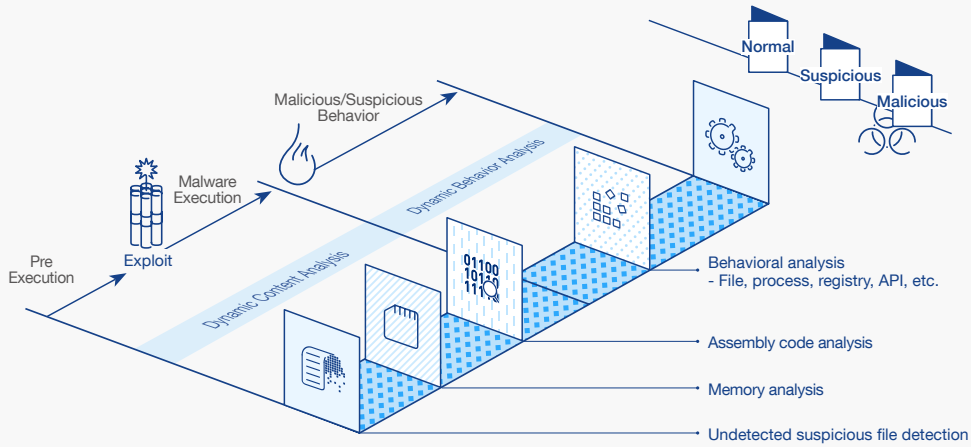
Multi-Engine Granular Detection

AhnLab MDS systematically detects both known and unknown threats, powered by its multi-engine delivering signature-based static detection, reputation analysis, and signature-less dynamic sandbox analysis. The exploit detection technology leveraging memory analysis further stretches its precise detection and response to advanced cyber-attacks that evade sandbox analysis using concealment techniques.

* Exploit: A technique that leverages system or application vulnerabilities to execute malicious actions



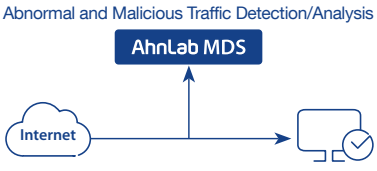
Sandbox-based Dynamic Analysis Process



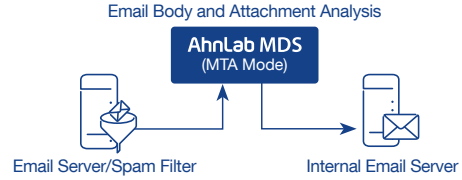
Optimal Response to Diverse Attacks

AhnLab MDS collects, analyzes, and detects cyber threats infiltrating through various domains across network, email, endpoint. Then, it delivers powerful response at the network and endpoint levels. The sandbox solutions also proactively prevents potential cyber threats by utilizing a dedicated endpoint agent to perform execution holding and suspicious file collection.

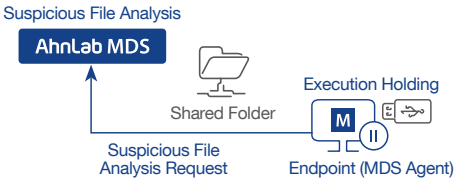
Network (Web) Attack Response
- Extracting and analyzing PE and non-PE files



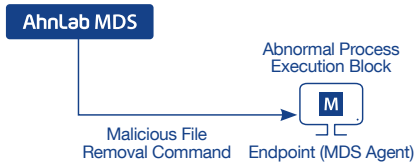
Email Attack Response
- Detecting and preventing malicious email content



Endpoint Attack Response
- Detecting and preventing malware (USB & shared folder)

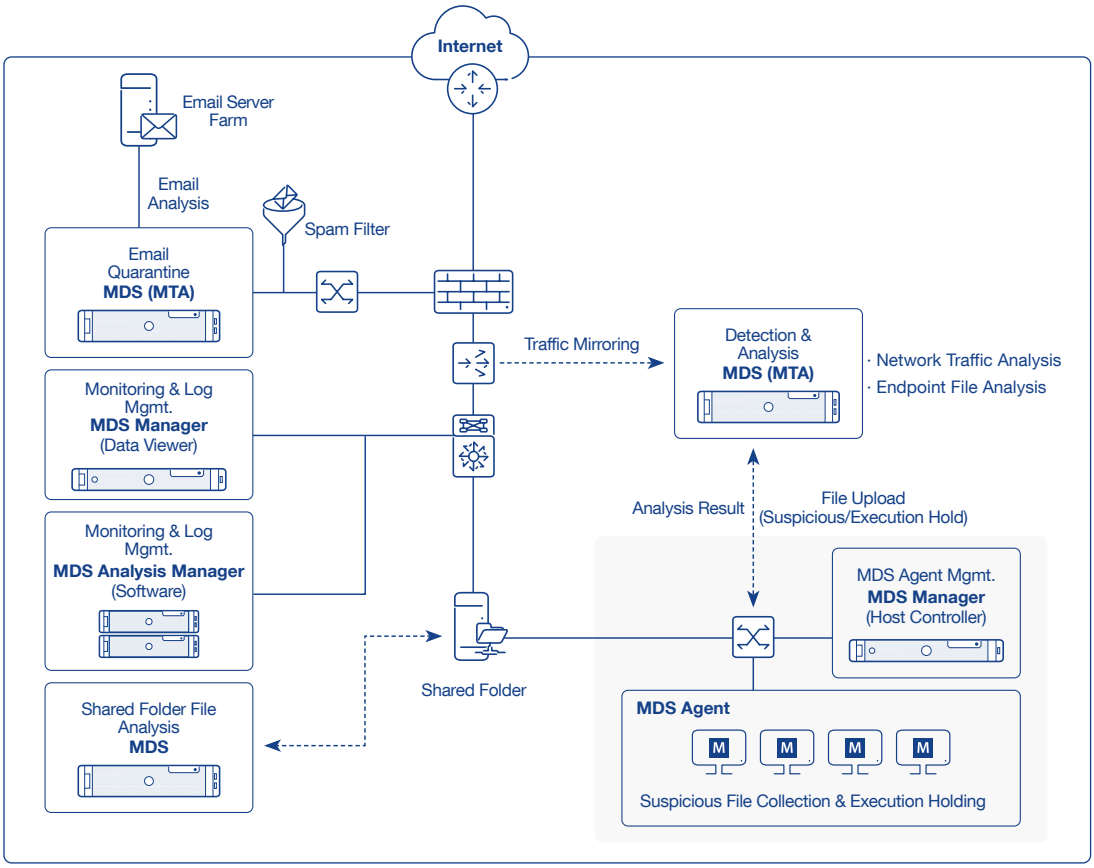


Process & File Attack Response
- Blocking abnormal process execution via MDS agent
- Removing malicious file



Architecture & Deployment

AhnLab MDS consists of **MDS** (file and threat analysis), **MTA** (email-dedicated license) and **MDS Agent** (dedicated agent for endpoint threat response). We recommend **MDS Manager** to effectively manage multiple appliances and agents.



MDS: Sandbox-based File Analysis

- VM supporting various OS (Windows 7/10/11 and Ubuntu)
- Quick signature-based static analysis and dynamic sandbox analysis
- Collection and analysis of major protocols (HTTP, HTTP/2, FTP, SMTP, POP3, IMAP, SMB, etc.)
- Managing blacklist and whitelist of hash (MD5, SHA-256), IP, URL, email, and digital signatures
- Applying multiple analysis engines optimized for different file characteristics
- Analysis into various versions of MS Office software
- Dedicated email license (MTA) for analyzing email header, body, and attachment
- Endpoint agent (MDS Agent) for execution holding, quarantining or removal of unanalyzed files
- AhnLab TIP integration and expert analysis services available as separate options

MDS (MTA): MDS for Email Domain

- Analysis into email header, subject, body and attachment
- Optical character recognition (OCR) and QR code phishing (Qshing) analysis
- Integration with anti-spam solutions

MDS Agent: Endpoint Agent

- Holding execution of unanalyzed files and deciding whether to execute after analysis
- Network quarantine of host suspected of malware infection – malware removal
- Suspicious file collection using proprietary ML technology
- Verifying certificates of executables and simultaneously collecting relevant files
- Supporting unified AV agent (AhnLab V3)

MDS Manager: Unified Management and Monitoring

- Central management and monitoring of multiple MDS appliances (Data Viewer)
- Central management of multiple MDS Agents (Host Controller)
- Data Viewer and Host Controller can be used individually or in package
- MDS Analysis Manager: A software-based, multi-tenant MDS Manager (multi-site management per IPs)

System Requirements

AhnLab MDS

	MDS 5000B	MDS 10000B	MDS 20000B
MAX Throughput	2G	5G	5G
Agent Count	1,000	3,000	3,000
Log Storage	SSD 1.92TB (1 each)	SSD 1.92TB (2 each)	SSD 1.92TB (4 each)
RAID	Not Supported	Optional (Default: Not Supported, RAID 1)	Optional (Default: Not Supported, RAID 10)
NIC	2 NICs can be installed ·1GC 8ports ·1GF 4ports ·1GF 8ports ·10GF 4ports		
Power	550W Redundant		
Rack Mount	1U		

※Performance varies depending on the system configuration and network environment.
※An additional MDS Manager appliance is required if the number of agents is exceeded.

AhnLab MDS Manager

※DV (Data Viewer): Integrated monitoring and log management
※HC (Host Controller): Integrated management of MDS Agent and MDS Manager required when adding the agent

	MDS Manager 5000BR		MDS Manager 10000BR	
Agent Count	HC+DV Combined	HC Dedicated	HC+DV Combined	HC Dedicated
	2,000	5,000	5,000	10,000
CPU	6 Core/3.30GHz*1		8 Core/3.40GHz*1	
RAM	32GB		64GB	
HDD	1TB (2 each) & 2TB (2 each)		2TB (2 each) & 4TB (2 each)	
RAID	RAID 1		RAID 1	
Network Interface	1GbE 2 Ports (Copper)		1GbE 2 Ports (Copper)	
Power Supply	400W Redundant		800W Redundant	
Rack Mount	1U (19”)		2U (19”)	
Size (WxDxH)	437x503x43mm		437x647x89mm	

※Performance varies depending on the system configuration and network environment.

AhnLab MDS Analysis Manager

	MDS Analysis Manager
CPU	Software
RAM	CPU: 8 Core/3.0GHz & MEM: 24GB & HDD: 2TB & SSD: 1TB
HDD	CPU: 16 Core/2.4GHz & MEM: 64GB & HDD: 4TB & SSD: 2TB
RAID	Supporting multitenancy & Not supporting the management of MDS Agent and MTA - To be supported
Network Interface	Supporting management of 100 sites (max)

System Requirement for AhnLab MDS Agent

	OS Support
Client PC	Windows 7 / 10 / 11
Server	Windows Server 2012 / 2016 / 2019 / 2022

※Both 32 and 64 bit are supported for the above OS

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

AhnLab