AhnLab MDS

Ultimate Threat Response with Powerful Visibility

Comprehensive threat detection for network, email, and endpoints
Multi-layered and optimized response empowered by threat visibility

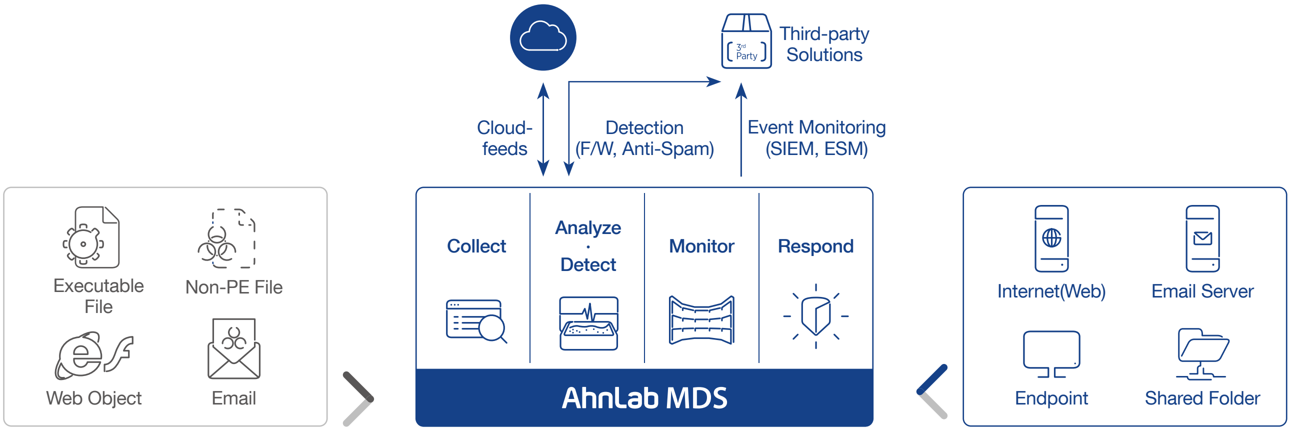
Regardless of industry type or scale, most organizations are constantly exposed to advanced persistent threats (ATPs) in the form of new and unknown malware, ransomware, spear phishing, and other targeted attacks. **AhnLab MDS** (Malware Defense System) is a sandbox-based solution that uses a proprietary multi-engine developed by AhnLab to precisely detect the threats that infiltrate the system via a diverse range of vectors. It provides comprehensive network- and endpoint-level responses based on threat visibility and a "collect-detect/analyze-monitor-respond" process that effectively prevents threats.

Detects unknown threats or variants with multi-engine based hybrid analysis
· Static detection based on signature, reputation, and machine learning
· Sandbox-based dynamic behavior analysis

Collects and analyzes threats that infiltrate through multiple sources
· Collection and analysis of network traffic, email content and attachment
· Collection of suspicious files and analysis of abnormal processes in endpoints

Multi-layered responses to threats through integration as well as interoperation
· Integrated responses at the network and endpoint levels
· Interoperation with existing or third-party security solutions

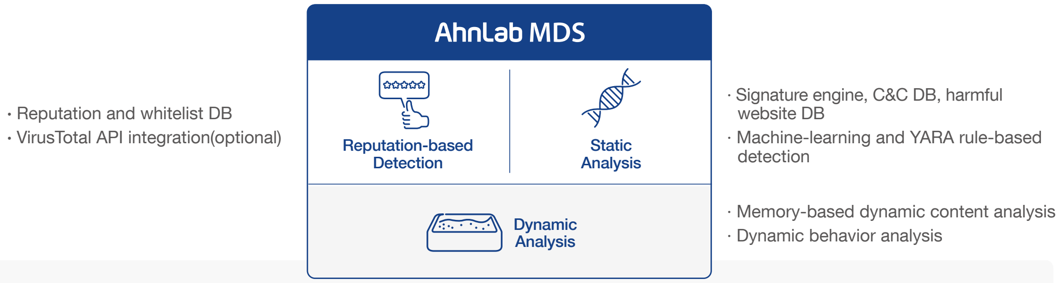
Provides optimized measures for each attack phase based on threat visibility
· Attack flowchart displays threat type, infection vector, correlation, and detection status
· Optimized response to specific and relevant attack phase



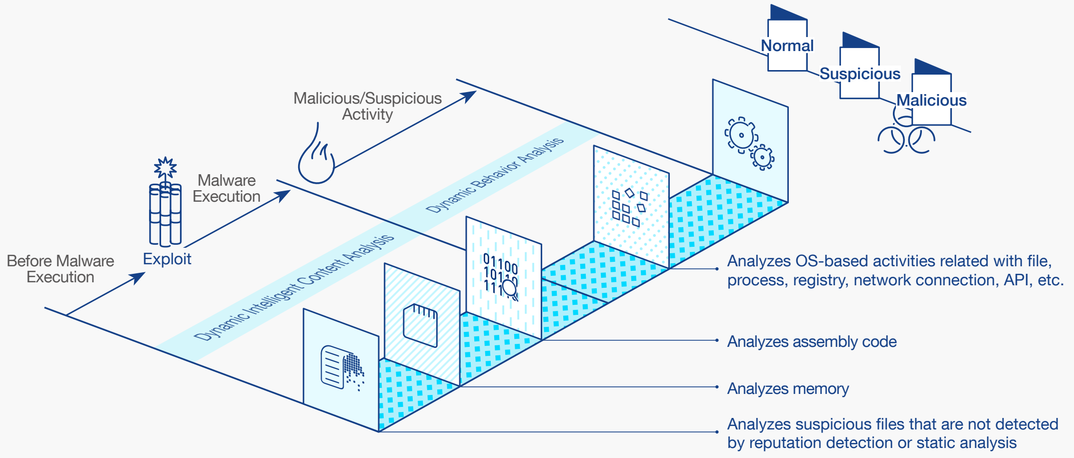
Multi-engine based Detection · Analysis

AhnLab MDS leverages its multi-engine capabilities to perform both signature-based static and reputation detection, as well as sandbox based dynamic analysis to detect both known as well as new and variant threats. It also effectively detects and prevents exploitation using its proprietary memory analysis, thereby containing elusive threats that attempt to bypass sandbox analysis.

*Exploit: a sequence of commands that takes advantage of an application bug or vulnerability to activate malicious activity


AhnLab MDS
Reputation-based Detection
Static Analysis
Dynamic Analysis
· Reputation and whitelist DB
· VirusTotal API integration(optional)
· Signature engine, C&C DB, harmful website DB
· Machine-learning and YARA rule-based detection
· Memory-based dynamic content analysis
· Dynamic behavior analysis

Sandbox-based Dynamic Analysis Process

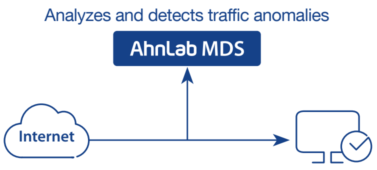

Normal
Suspicious
Malicious
Malicious/Suspicious Activity
Malware Execution
Before Malware Execution
Exploit
Dynamic Behavior Analysis
Dynamic Intelligent Content Analysis
01100 101 111
Analyzes OS-based activities related with file, process, registry, network connection, API, etc.
Analyzes assembly code
Analyzes memory
Analyzes suspicious files that are not detected by reputation detection or static analysis

Optimized Responses for Diverse Attacks

AhnLab MDS collects, detects, and analyzes threats that infiltrate along a wide range of vectors including the network, e-mail, and endpoints. It also provides an effective response at the network and endpoint levels based on the threat type. With its lightweight agent, AhnLab MDS suspends the execution or collects suspicious files at the endpoint, proactively shutting down potential threats.

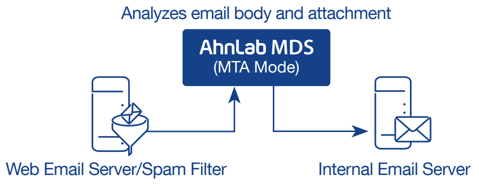
Response to Web-based Attack

- Extracts and analyzes executable and non-executable files



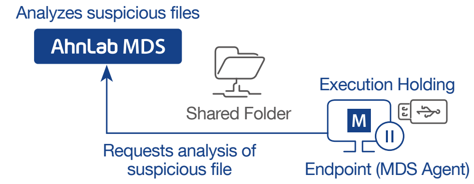
Response to Email-based Attack

- Detects and blocks malicious email content


Analyzes email body and attachment
AhnLab MDS
(MTA Mode)
Web Email Server/Spam Filter
Internal Email Server

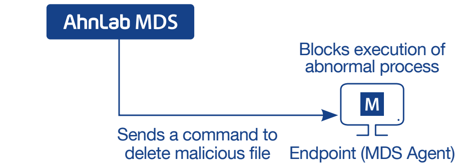
Response to Endpoint-based Attack

- Detects and blocks malware introduced via USB and shared folder


Analyzes suspicious files
AhnLab MDS
Shared Folder
Execution Holding
M
Requests analysis of suspicious file
Endpoint (MDS Agent)

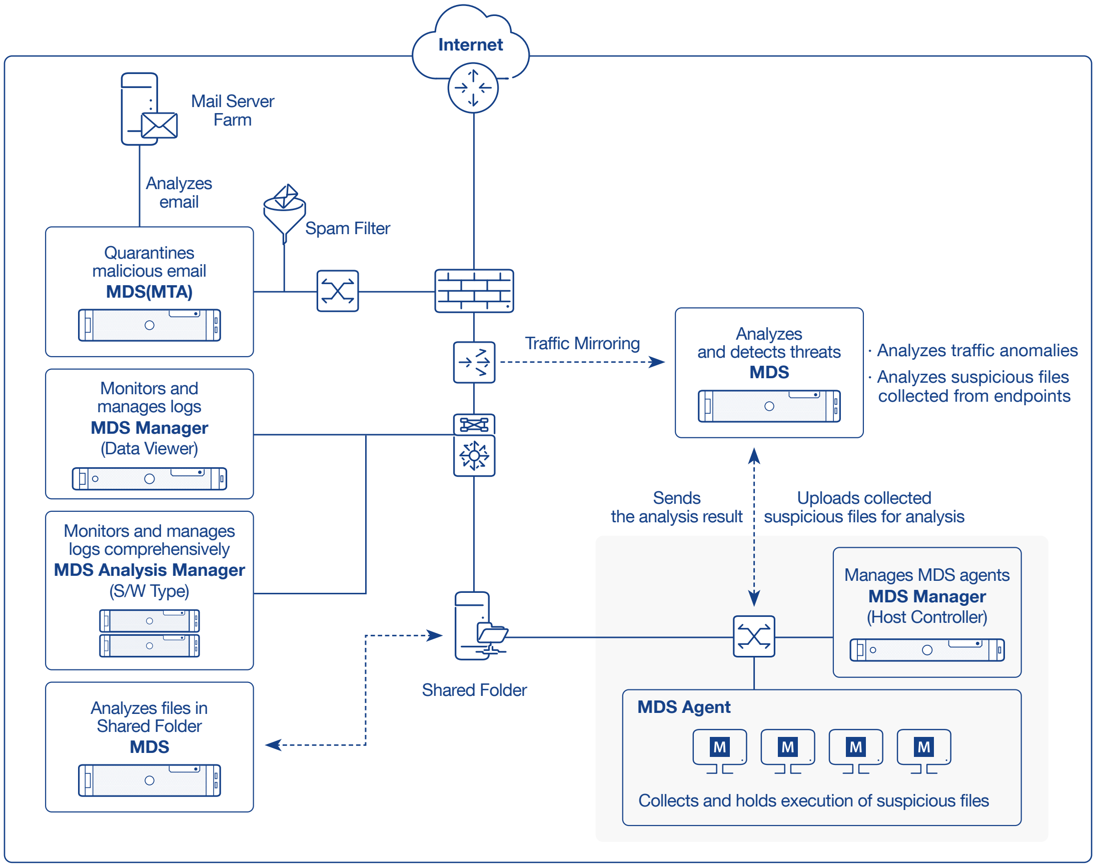
Response to Process and File based Attack

- Blocks execution of abnormal process and deletes a malicious file via MDS agent


AhnLab MDS
Blocks execution of abnormal process
M
Sends a command to delete malicious file
Endpoint (MDS Agent)

Components and Deployment

AhnLab MDS is a complete advanced protection solution that is composed of MDS for detecting and analyzing threats, MDS Manager and MDS Analysis Manager(S/W type) for providing integrated monitoring and management, and the MDS Agent, which is a dedicated agent for endpoint threat responses.


Internet
Mail Server Farm
Analyzes email
Spam Filter
Quarantines malicious email
MDS(MTA)
Traffic Mirroring
Analyzes and detects threats
MDS
· Analyzes traffic anomalies
· Analyzes suspicious files collected from endpoints
Monitors and manages logs
MDS Manager
(Data Viewer)
Sends the analysis result
Uploads collected suspicious files for analysis
Monitors and manages logs comprehensively
MDS Analysis Manager
(S/W Type)
Manages MDS agents
MDS Manager
(Host Controller)
Shared Folder
MDS Agent
M
M
M
M
Collects and holds execution of suspicious files
Analyzes files in Shared Folder
MDS

MDS : Multi-engine based Threat Detection and Analysis

- Inspects and analyzes various Internet service protocols (HTTP, SMTP, SMB/CIFS, and FTP)
- Detects and quarantines malicious emails and attached files (available when MTA license is applied)
- Identifies new and unknown malware through sandbox-based dynamic analysis and static detection based on signature and machine learning
- Adopts its exclusive engine for non-PE malware analysis (MS Office, Hancom Office, etc.)
- Provides PCAP-based packet capture and PCAP file download for VM analysis and C&C detection
- Shares behavior analysis results of MDS appliances through MDS Manager and cloud-feed

MDS Manager : Integrated Monitoring and Management

Data Viewer : Centralized monitoring and log management of MDS appliances

- Provides threat status and events information on a user-intuitive dashboard
- Provides detailed logs on event type, IP address and behaviors on file, process, registry, and network
- Integrates and manages events and logs detected by MDS appliances deployed on the network
- Distributes behavior analysis results of MDS appliances (preventing analysis duplication)
- Interoperates and manages YARA rules
- Forwards syslog in CEF and LEEF formats

Host Controller: Integrated MDS Agent management and response

- Installs, patches, and configures groups and policies for MDS Agent
- Sends response commands and notices via MDS Agent

MDS Analysis Manager: Unified Monitoring and Log Management of MDS appliances (S/W Type)

- Provides same functions as Data Viewer of MDS Manager
- Supports IP multi-tenancy that enables system administrators to access and operate multiple sites

MDS Agent : Response to Suspicious Files in Endpoints

- Extracts and collects suspicious files from host systems using machine-learning technology
- Responds to suspected infected host systems including malware removal, system isolation, etc.
- Detects abnormal process and conducts Execution Holding on suspicious files

System Requirements

AhnLab MDS

	MDS 5000B	MDS 10000B	MDS 20000B
MAX Throughput	2G	5G	10G
Agent Count	1,000	3,000	6,000
Log Storage	SSD 1.92TB * 1ea.	SSD 1.92TB * 2ea.	SSD 1.92TB * 4ea.
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 Supply	550W, Redundant		
Rack Mount	1U		

⁎ Note: Performance values vary depending on the system configuration and network environment
⁎ Note: If the number of agents is exceeded, an additional MDS Manager appliance is required

AhnLab MDS Manager

⁎ DV (Data Viewer) : Centralized monitoring and log management of MDS appliances
⁎ HC (Host Controller) : Integrated MDS Agent management and response

	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	1 * 3.30GHZ, 6Core		1 * 3.30GHZ, 6Core	
RAM	32GB		64GB	
HDD	1TB x 2ea., 2TB x 2ea.		2TB x 2ea., 4TB x 2ea.	
RAID Configuration	RAID 1		RAID 1	
Network Interface	1GbE 2 Ports (Copper)		1GbE 2 Ports (Copper)	
Power Supply	400W Redundant		800W Redundant	
Form Factor	1U (19”)		2U (19”)	
Chassis Dimensions(WxDxH)	437 x 503 x 43mm		437 x 647 x 89mm	

⁎ Note: Performance values vary depending on the system configuration and network environment

AhnLab MDS Analysis Manager

	MDS Analysis Manager
Type	Software
OS Support	CentOS 8 or more
System Requirement	CPU: 8Core, 3.0GHz, MEM: 24GB, HDD: 2TB, SSD: 1TB
Recommended Requirement	CPU: 16Core, 2.4GHz, MEM: 64GB, HDD: 4TB, SSD: 2TB
Multi-tenancy	Max. 100 sites supported

System Requirement for AhnLab MDS Agent

	OS Support
Client PC	Windows 7 SP1 (KB4490628, KB4474419) / Windows 8(8.1) / 10 / 11
Server	Windows Server 2008 SP2 (KB4493730, KB4474419), Windows Server 2008 R2 SP1 (KB4490628, KB4474419), Windows Server 2012 / 2016 / 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