

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



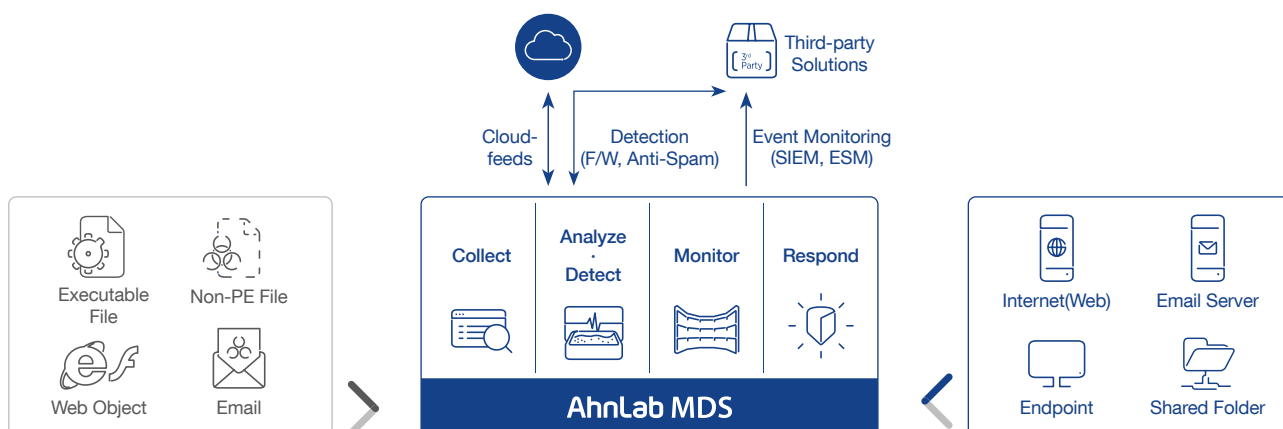
Multi-layered responses to threats through integration as well as interoperation

- 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

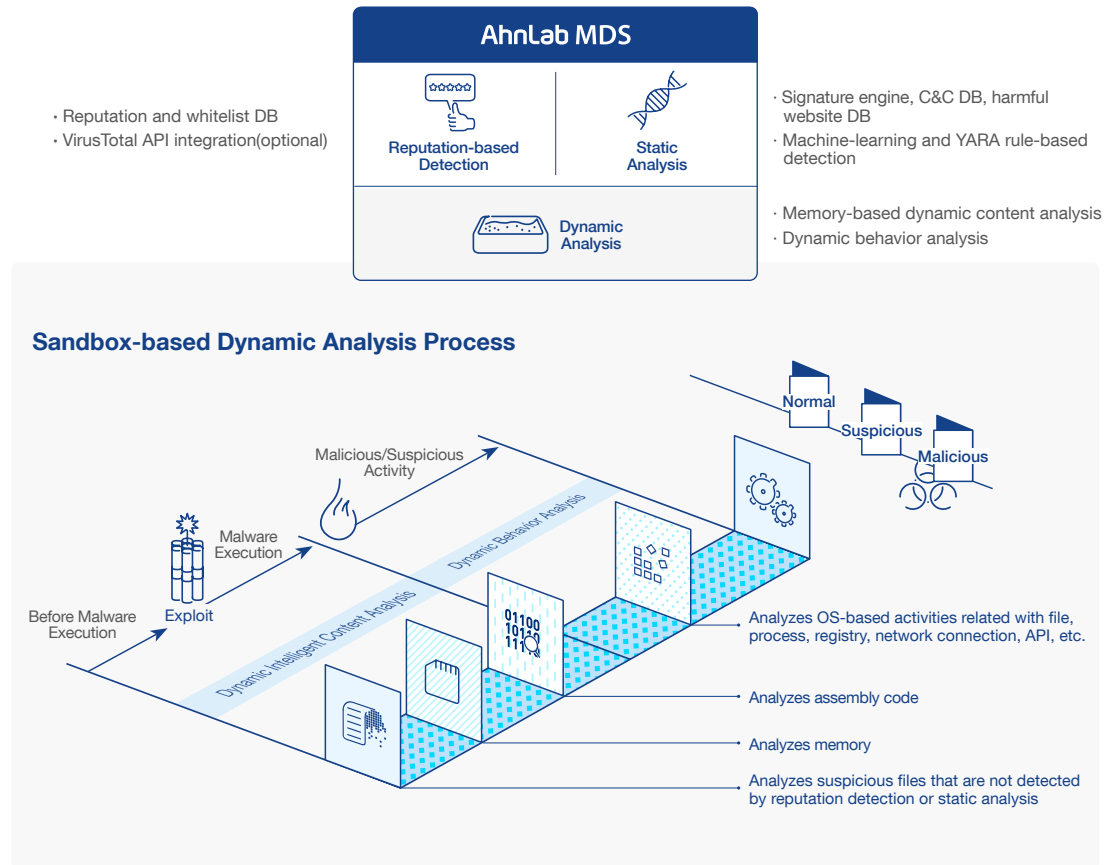
- Attack flowchart displays threat type, infection vector, correlation, and detection status
- Optimized response to specific and relevant attack phase



Multi-engine based Detection · Analysis

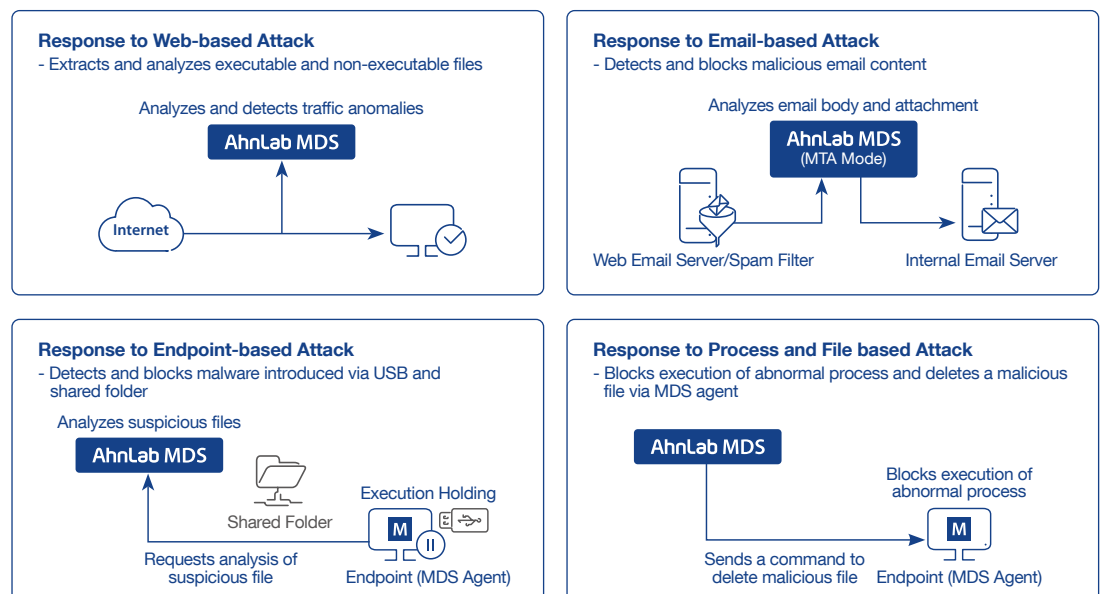
AhnLab MDS leverages its multi-engine capabilities to perform both signature-based static and reputation detection, as well as sandbox based dynamic analysis to detect both known as well as new and variant threats. It also effectively detects and prevents exploitation using its proprietary memory analysis,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



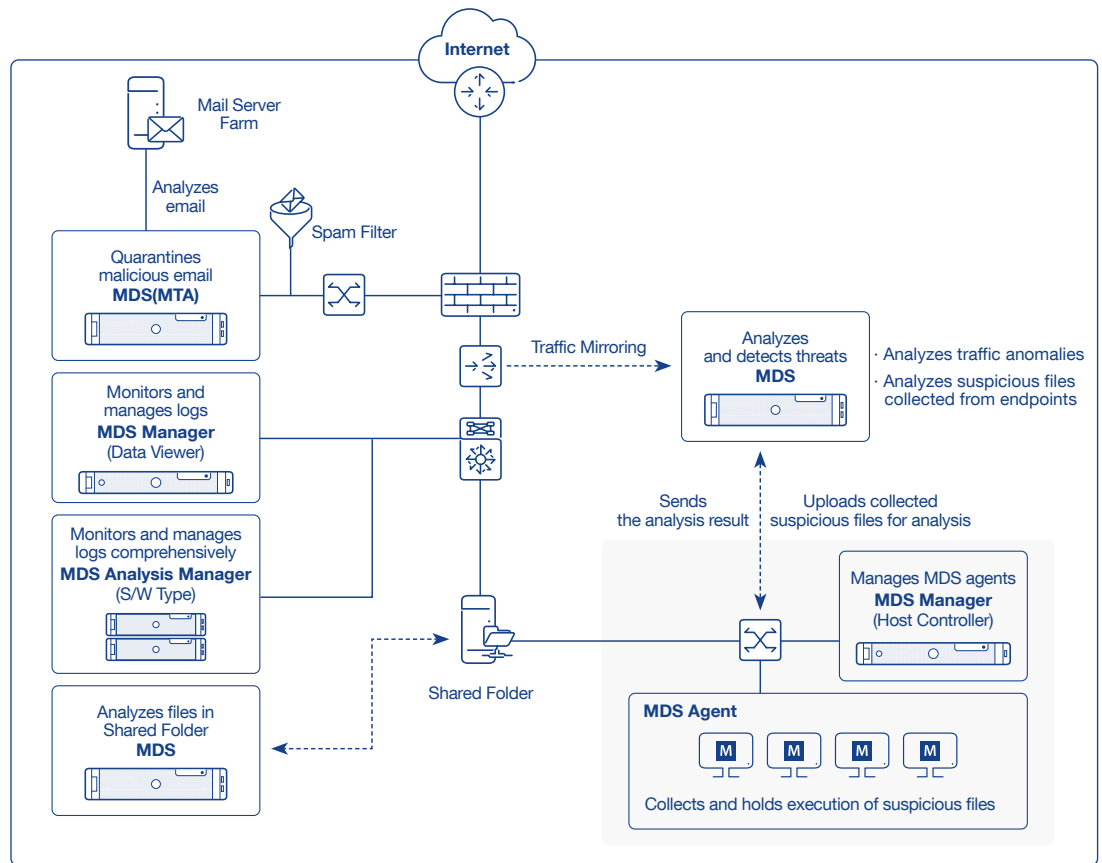
Optimized Responses for Diverse Attacks

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.



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.



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

Specifications

AhnLab MDS

	MDS 5000B	MDS 10000B	MDS 20000B
MAX Throughput	2G	5G	10G
Agent Count	1,000	3,000	3,000
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 (Separate management port available) ·1GC 8 Ports ·1GF 4 Ports ·1GF 8 Ports ·10GF 4 Ports		
Power Supply	550W, Redundant		
Rack Mount	1U		

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

* An additional MDS Manager is required when adding the agent.

AhnLab MDS Manager

* DV (Data Viewer): Integrated monitoring and log management

* HC (Host Controller): An additional MDS Manager is required when adding or centrally managing agents.

	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, 6 Core		1 * 3.40GHz, 8 Core	
RAM	32GB		64GB	
HDD	1TB x 2ea., 2TB x 2ea.		2TB x 2ea., 4TB x 2ea.	
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 inch		2U, 19 inch	
Size (WxDxH)	437 x 503 x 43mm		437 x 647 x 89mm	

* 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
AID	Supporting multitenancy & Not supporting the management of Agent and MTA (to be supported in future)
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

© 2025 AhnLab, Inc. All rights reserved.

AhnLab