PC com Mayorista

5599 - 0670 | https://pccommayorista.com
contacto@pccommayorista.com

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

SANDBOX MULTI-ENGINE MULTI-LAYERED 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.

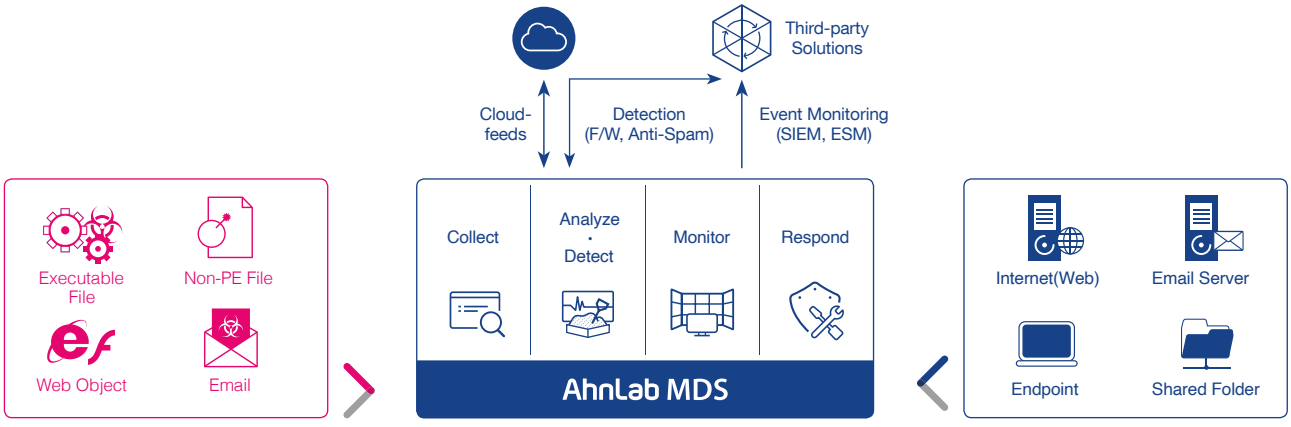
AhnLab MDS (Malware Defense System) is a sandbox-based solution that uses a proprietary multi-engine developed by AhnLab to precisely detect the threats that infiltrate the system via a diverse range of vectors. It provides comprehensive network- and endpoint-level responses based on threat visibility 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

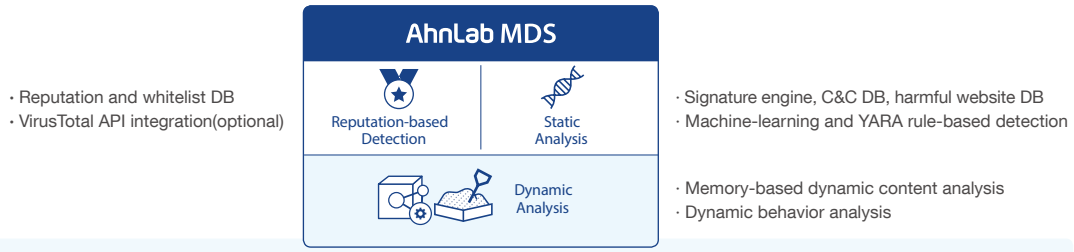
Provides optimized measures for each attack phase based on threat visibility
- Attack flowchart displays threat type, infection vector, correlation, and detection status
- Optimized response to specific and relevant attack phase



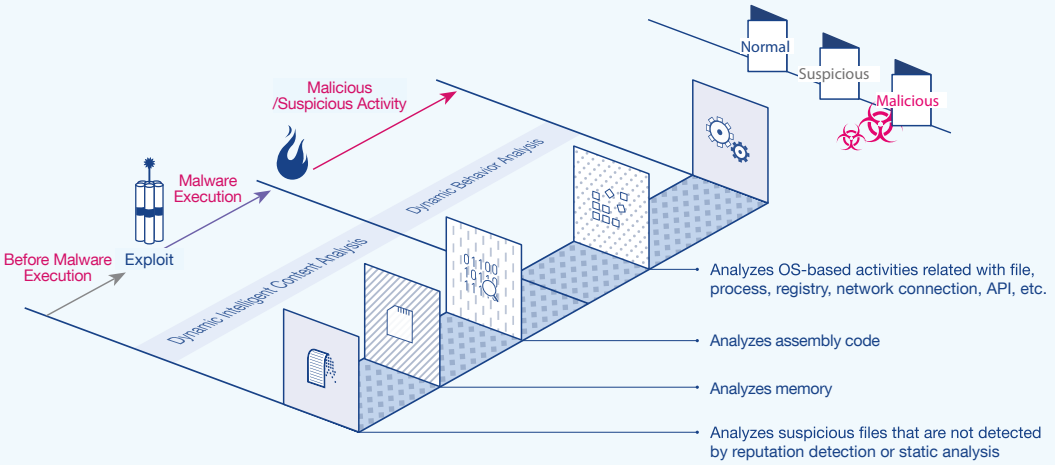
Multi-engine based Detection · Analysis

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



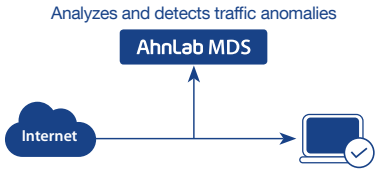
Sandbox-based Dynamic Analysis Process



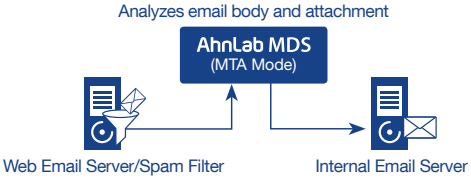
Optimized Responses for Diverse Attacks

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.

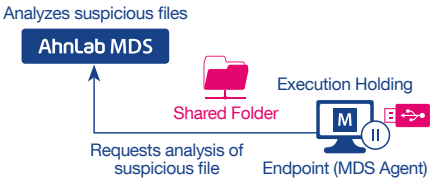
Response to Web-based Attack
- Extracts and analyzes executable and non-executable files



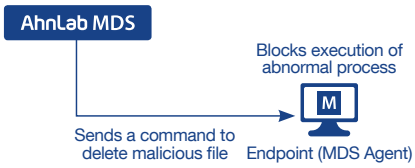
Response to Email-based Attack
- Detects and blocks malicious email content



Response to Endpoint-based Attack
- Detects and blocks malware introduced via USB and shared folder

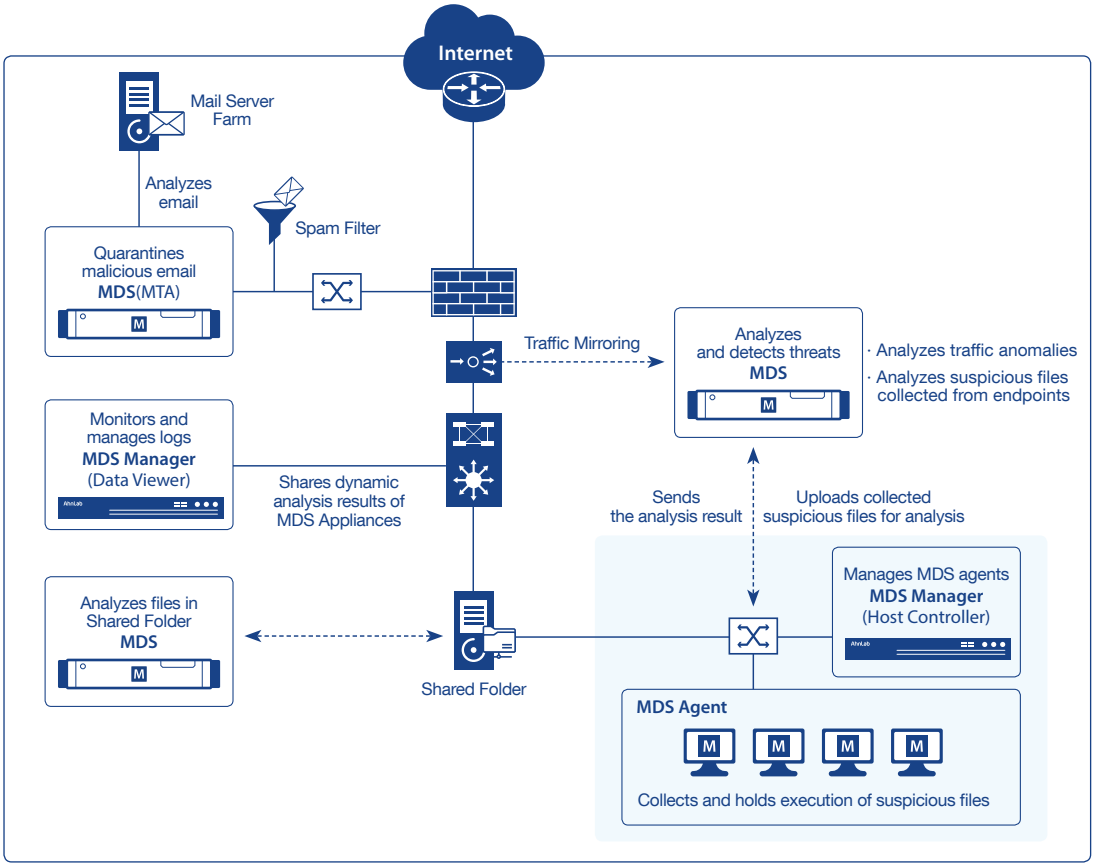


Response to Process and File based Attack
- Blocks execution of abnormal process and deletes a malicious file via MDS agent



Components and Deployment

AhnLab MDS is a complete advanced protection solution that is composed of the MDS appliance for detecting and analyzing threats; the MDS Manager for providing integrated monitoring and management; and the MDS Agent, a dedicated agent for endpoint threat responses.
AhnLab MDS can be deployed in basic or expanded architecture depending on the organization's environment and security requirements, and responds to threats attempting infiltration through various vectors, including the network (web), e-mail, shared file folders, and endpoints.



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 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 4000A	MDS 8000A	MDS 10000A	
Analysis Capacity	35,000 samples per day	90,000 samples per day	200,000 samples per day	
Agent Count	700	2,000	5,000	
Traffic Throughput	800Mbps	1.5Gbps	4Gbps	
HDD	1TB x 2ea.	1TB x 4ea.	1TB x 8ea.	
RAID Configuration	RAID 1	RAID 10	RAID 10	
Network Interface	1GbE 4 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)	1GbE 4 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)	**Default**	1GbE 2 Ports (Copper) 1/10G Base-T 2 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)
			Optional	1GbE 2 Ports (Copper) 1/10G Base-T 4 Ports (Copper) 1/10G SFP+ 6 Ports (Optical)
Power Supply	750W Redundant			
Form Factor	1U (19”)	1U (19”)	2U (19”)	
Chassis Dimensions (W x D x H)	482 x 721.91 x 42.8mm	482 x 721.91 x 42.8mm	482.4 x 715.5 x 86.8mm	

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 5000AR		MDS Manager 10000AR	
Agent Count	HC+DV Combined	HC Dedicated	HC+DV Combined	HC Dedicated
	2,000	5,000	5,000	10,000
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	500W Redundant		740W Redundant	
Form Factor	1U (19”)		2U (19”)	
Chassis Dimensions (W x D x H)	437 x 650 x 43mm		440 x 650 x 89mm	

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

System Requirement for AhnLab MDS Agent

	OS Support
Client PC	Windows XP SP3 or higher / 7 / 8(8.1) / 10
Server	Windows Server 2003 SP2 or higher / 2008 / 2012 / 2016

Both 32 and 64 bit are supported for the above OS

More security,
More freedom

PC com Mayorista

¡Contáctanos, juntos queremos hacer negocio contigo!

Av. Prol. División del Norte # 4318
Col. Nueva Oriental Coapa, Tlalpan C.P. 14300

(55) 5599-0670
https://pccommayorista.com
contacto@pccommayorista.com

AhnLab