AhnLab MDS

알려지지 않은 위협 대응을 위한 선택

샌드박스 기반 파일 분석 및 APT 대응 솔루션
최고 수준의 악성코드, 랜섬웨어, URL, C&C 탐지
악성 파일 실행 보류 및 대응 기능 제공

제품 개요

2024년 이전, 이후에도 랜섬웨어를 비롯한 악성코드 대응은 사이버보안 전략의 가장 중요한 부분입니다. 따라서 네트워크, 이메일, 엔드포인트 구간에 유입되는 악성코드를 탐지하고 분석하는 솔루션이 필요합니다. 알려진 악성코드는 엔드포인트에 설치된 기존 바이러스 백신으로 대응할 수 있습니다. 하지만 알려지지 않은 악성코드에 대응하려면 **AhnLab MDS**(Malware Defense System)가 필요합니다.

샌드박스 기반 파일 분석 솔루션인 Ahnlab MDS에는 파일 분석에 관한 안랩의 모든 노하우가 적용되어 있습니다. AhnLab MDS는 Windows 및 Linux OS 기반 가상 환경에서 파일을 실행한 후, 발생한 행위를 분석합니다. 신종 파일도 알려진 악성 행위를 포함하기 때문에 AhnLab MDS로 탐지할 수 있습니다. AhnLab MDS는 파일의 행위 또는 파일 자체 분석을 위해 다수의 분석 엔진을 탑재했으며, 이를 통해 고도화된 위협을 정밀하게 탐지합니다.

알려지지 않은(Unknown) 위협 대응 – 샌드박스

- 샌드박스 기술 기반 동적 분석 지원 (지원 OS: Windows 7/10/11, Ubuntu)
- Anti-VM(가상환경 회피) 악성코드 탐지/분석 기법 및 연관 파일 분석 기능

다양한 경로를 통해 유입되는 위협 수집 및 분석

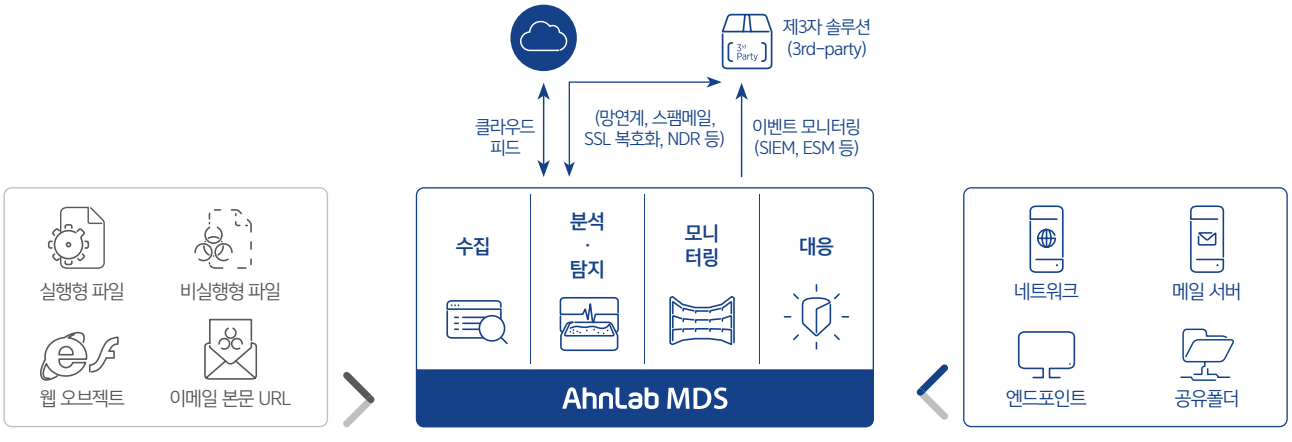
- 10G 네트워크 트래픽 실시간 수집 및 분석 (HTTP, HTTP/2, FTP, SMTP, POP3, IMAP, SMB 등)
- 이메일 구간 라이선스(MTA) 및 엔드포인트 에이전트(MDS Agent)를 통한 파일 수집 및 분석

다양한 솔루션 연동 지원

- 실행 파일, 문서 파일, 이메일 등 정밀 분석을 위한 MDS 연동 지원 (API)
- 망연계 솔루션, 스팸 메일 솔루션, SSL 복호화 솔루션, NDR 솔루션 등과의 연동 지원

최신 안랩 위협 대응 기법 적용

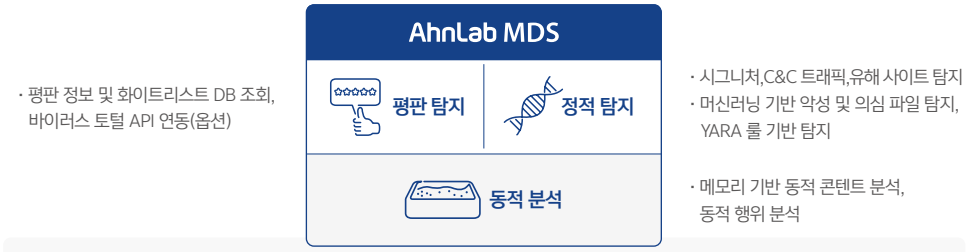
- 정적 규칙으로 탐지할 수 없는 사기성 피싱 메일(EML파일)에 대한 머신러닝(ML) 기반 탐지
- AhnLab TIP 연동, 전문가 분석 서비스 등 다양한 분석 보조 도구 제공



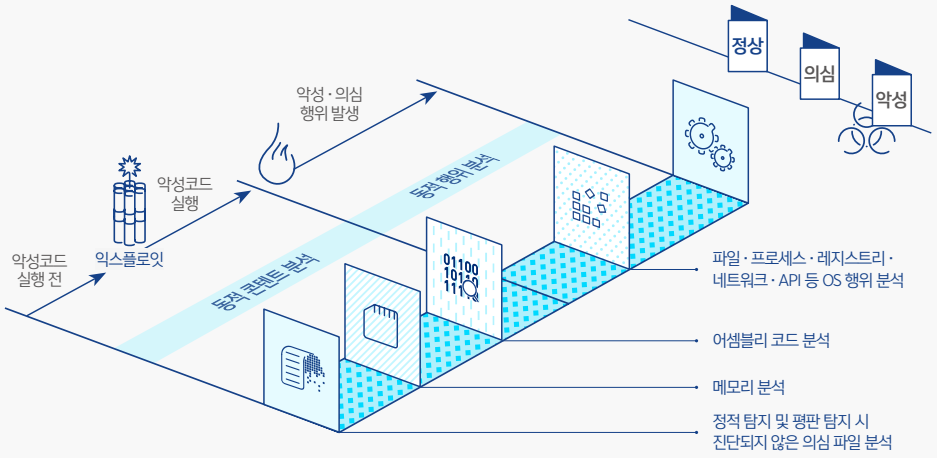
멀티엔진 기반의 정교한 위협 탐지

멀티엔진이 탑재된 AhnLab MDS는 시그니처 기반의 정적(Static) 탐지와 평판 탐지, 비시그니처(Signature less) 방식인 샌드박스 기반의 동적(Dynamic) 분석을 통해 알려진 위협은 물론, 신·변종 위협을 효과적으로 탐지합니다. 또한 '메모리 분석 기반의 익스플로잇 탐지 기술'로 은닉 기법을 이용해 샌드박스 분석을 우회하는 고도화된 공격까지 정밀하게 탐지하고 대응합니다.

*익스플로잇(Exploit): 시스템이나 응용 프로그램의 버그 또는 보안 취약점 등을 이용해 악의적인 행위를 실행하는 공격 방식

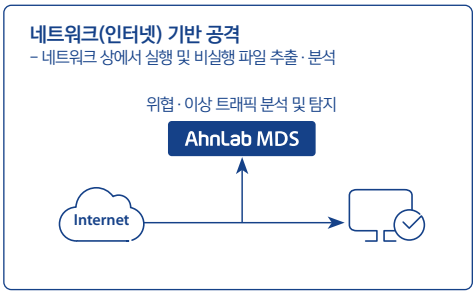


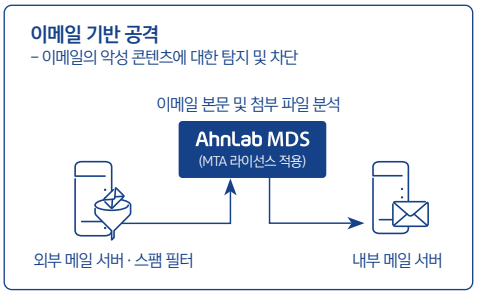
샌드박스 기반의 동적 분석 프로세스

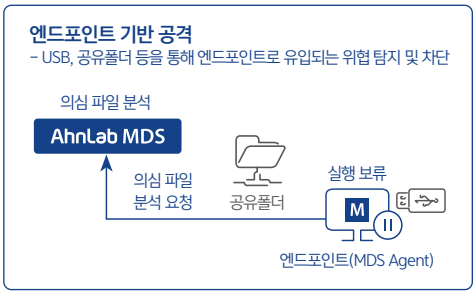


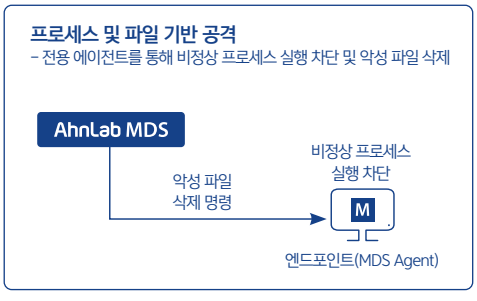
공격 유형별 최적화된 대응

AhnLab MDS는 네트워크, 이메일, 엔드포인트 등 다양한 경로를 통해 침입하는 위협을 수집·분석·탐지하여 위협 유형에 따라 네트워크 레벨과 엔드포인트 레벨에서 효과적으로 대응합니다. 또한, 전용 에이전트를 이용해 엔드포인트의 의심 파일에 대한 '실행 보류', '의심 파일 수집'을 수행함으로써 잠재적인 위협까지 능동적으로 예방합니다.



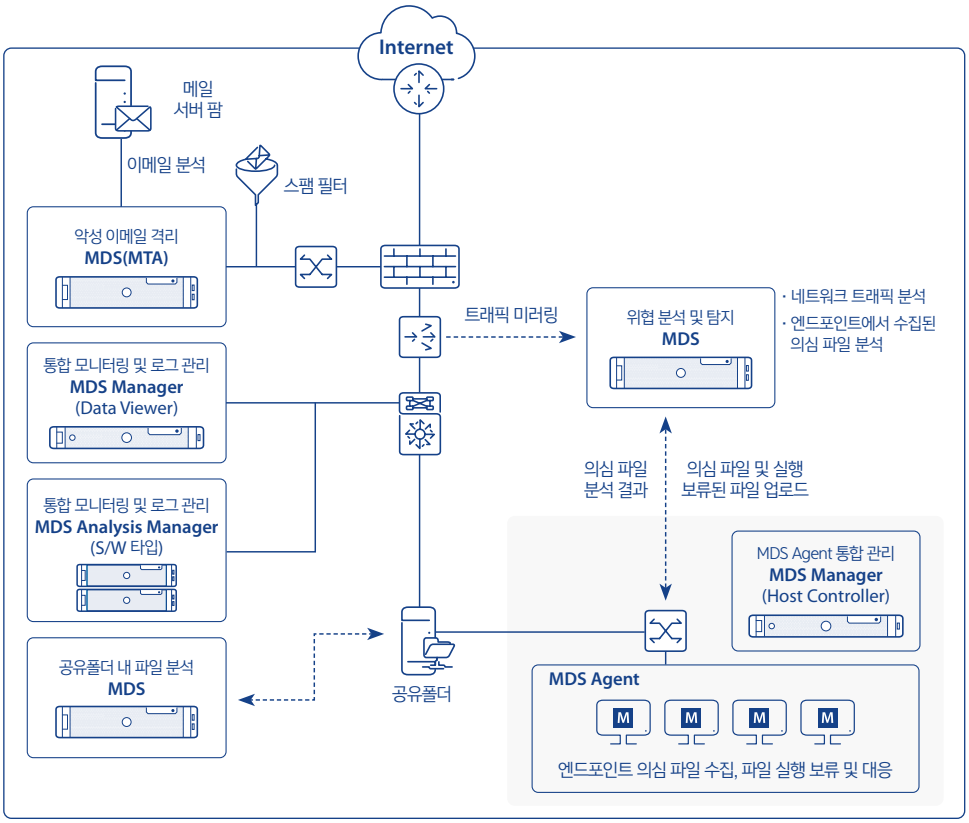






솔루션 구성 및 구축 방식

AhnLab MDS는 파일 및 위협 분석을 위한 MDS, 메일 구간 전용 라이선스 MTA, 엔드포인트 위협 대응을 위한 전용 Agent로 구성되어 있습니다. 다수의 장비 및 에이전트를 관리하기 위해서는 별도의 MDS Manager가 필요합니다.



MDS: 샌드박스 기반 파일 분석 솔루션

- 다양한 OS 환경 VM 지원 (Windows 7/10/11 및 Ubuntu)
- 시그니처 기반 빠른 정적 분석 및 샌드박스 기반 정밀한 동적 분석 지원
- 주요 프로토콜 수집 및 분석 (HTTP, HTTP/2, FTP, SMTP, POP3, IMAP, SMB 등)
- 파일 특성에 맞는 다양한 분석 엔진 적용
- 정식 라이선스를 기반으로 하는 다양한 버전의 MS오피스, 한글오피스 분석 환경 제공
- 메일 헤더, 본문 및 첨부 파일 분석을 위한 메일 구간 전용 라이선스 제공 (MTA)
- 엔드포인트 구간에서 미분석 파일의 실행 보류 및 삭제/격리 등을 위한 에이전트 제공 (MDS Agent)
- AhnLab TIP 연동 및 전문가 분석 서비스 별도 옵션으로 사용 가능

MDS(MTA): 메일 구간에 사용하는 MDS

- 메일 헤더, 제목, 본문, 첨부 파일 분석 지원
- 피싱 메일 탐지를 위한 ML 기반 분석 기능 제공
- 스팸 메일 솔루션 연동 지원

MDS Agent: 엔드포인트에 설치하는 MDS Agent

- 미분석 파일 실행 보류 및 분석 후 파일 실행 여부 결정
- 악성코드 감염이 의심되는 호스트 네트워크 격리 및 악성코드 삭제/대응
- 독자적인 ML 기술을 적용한 의심 파일 수집
- 실행 파일 인증서 검증 및 연관 파일 동시 수집 기능 제공
- V3 통합 에이전트 지원

MDS Manager: 통합 관리 및 모니터링

- MDS 다수 장비 통합 관리 및 모니터링 지원 (Data Viewer)
- 다수의 MDS Agent 필요 시 Agent 관리 (Host Controller)
- Data Viewer, Host Controller 통합, 별도 사용 가능
- MDS Analysis Manager: MDS Manager S/W 타입으로 멀티테넌시 제공 (IP 단위 다수 사이트 관리)

제품 사양

AhnLab MDS

구분	MDS 5000B	MDS 10000B	MDS 20000B
MAX Throughput	2G	5G	10G
관리 Agent 수	1,000개	3,000개	6,000개
Log Storage	SSD 1.92TB * 1ea.	SSD 1.92TB * 2ea.	SSD 1.92TB * 4ea.
RAID	미지원	Optional (기본: 미지원, RAID 1)	Optional (기본: 미지원, RAID 10)
NIC	2개 NIC 장착 가능 (관리 Port 별도 존재) ·1GC 8ports ·1GF 4ports ·1GF 8ports ·10GF 4ports		
Power	550W, Redundant		
랙 마운트	1U		
CC인증	EAL 3 (기타)		

※ 성능 수치는 세부 환경 및 시스템 구성에 따라 달라질 수 있습니다.
※ 에이전트 추가 시 MDS Manager 추가 필요

AhnLab MDS Manager

※ **DV(Data Viewer)**: 통합 모니터링 및 로그 관리
※ **HC(Host Controller)**: MDS Agent 통합 관리 · 에이전트 추가 시 MDS Manager 추가 필요

구분	MDS Manager 5000BR		MDS Manager 10000BR	
관리 에이전트 수	HC+DV 통합형	HC 단독형	HC+DV 통합형	HC 단독형
	2,000개	5,000개	5,000개	10,000개
CPU	1 * 3.30GHZ, 6Core		1 * 3.40GHz, 8Core	
RAM	32GB		64GB	
HDD	1TB x 2ea., 2TB x 2ea.		2TB x 2ea., 4TB x 2ea.	
RAID	RAID 1		RAID 1	
네트워크 인터페이스	1GbE 2 Ports (Copper)		1GbE 2 Ports (Copper)	
전원	400W Redundant		800W Redundant	
랙 마운트	1U, 19 inch		2U, 19 inch	
사이즈(WxDxH)	437 x 503 x 43mm		437 x 647 x 89mm	

※ 성능 수치는 세부 환경 및 시스템 구성에 따라 달라질 수 있습니다.

AhnLab MDS Analysis Manager

구분	MDS Analysis Manager
타입	소프트웨어
운영체제(OS)	CentOS 7.9
최소 사양	CPU: 8Core, 3.0GHz, MEM: 24GB, HDD: 2TB, SSD: 1TB
권장 사양	CPU: 16Core, 2.4GHz, MEM: 64GB, HDD: 4TB, SSD: 2TB
특징	멀티테넌시 기능 지원, Agent & MTA 관리 미지원 (향후 업데이트 예정)
멀티테넌시 사양	최대 관리 사이트 100개 지원

AhnLab MDS Agent 사용 환경

구분	운영체제(OS)
클라이언트 PC	Windows 7 SP1 (KB4490628, KB4474419 패치 환경) / Windows 8(8.1) / 10 / 11
서버	Windows Server 2008 SP2 (KB4493730, KB4474419 패치 환경) Windows Server 2008 R2 SP1 (KB4490628, KB4474419 패치 환경) Windows Server 2012 / 2016 / 2022

※ 상기 OS의 32/64 bit를 지원합니다.

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901

AhnLab