AhnLab MDS

샌드박스 기반의 지능형 위협 대응 솔루션

네트워크, 이메일, 엔드포인트 위협 탐지 및 대응
위협 가시성을 통한 공격 단계별 최적의 대응

제품 개요

산업 분야나 조직 규모를 막론하고 현재 대부분의 기업과 기관은 랜섬웨어를 비롯해 각종 은닉 기법을 결합한 신·변종 악성코드, 정교한 사회공학기법을 이용한 스피어피싱, 타깃 공격 등 지능형 위협(Advanced Persistent Threat, APT)에 노출되어 있습니다.

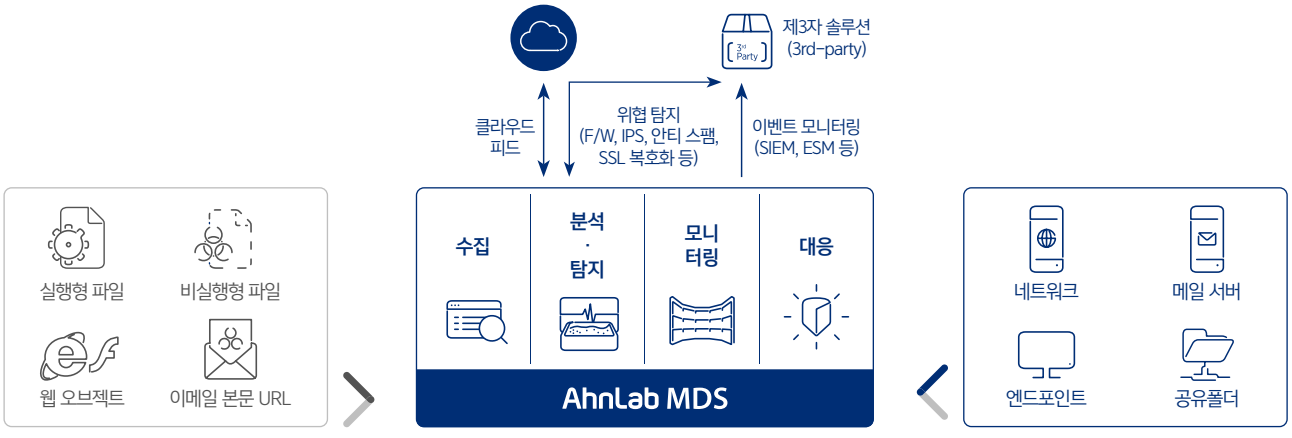
샌드박스 기반의 지능형 위협 대응 솔루션 **AhnLab MDS**(Malware Defense System)는 독자적인 기술의 멀티엔진을 이용해 고도화된 지능형 위협을 정밀하게 탐지합니다. 직관적인 위협 가시성과 '수집-분석·탐지-모니터링-대응' 프로세스를 기반으로 네트워크와 엔드포인트 레벨의 유기적인 대응을 제공해 다양한 경로를 통해 유입되는 지능형 위협을 효과적으로 차단합니다.

멀티엔진 기반의 하이브리드 분석을 통한 신·변종 위협 탐지
- 시그니처 및 머신러닝 기반의 정적 탐지, 평판 기반 탐지
- 샌드박스 기반의 동적 분석

다양한 경로를 통해 유입되는 위협 수집 및 분석
- 네트워크 트래픽 실시간 수집 및 분석, 이메일 본문 및 첨부파일 분석
- 엔드포인트의 의심스러운 파일 수집 및 의심스러운 프로세스 분석

네트워크-엔드포인트 연계, 솔루션 연동을 통한 멀티레이어드 대응
- 네트워크와 엔드포인트 레벨의 유기적인 대응
- 기 구축된 보안 솔루션 및 제3자(3rd-party) 솔루션 연동

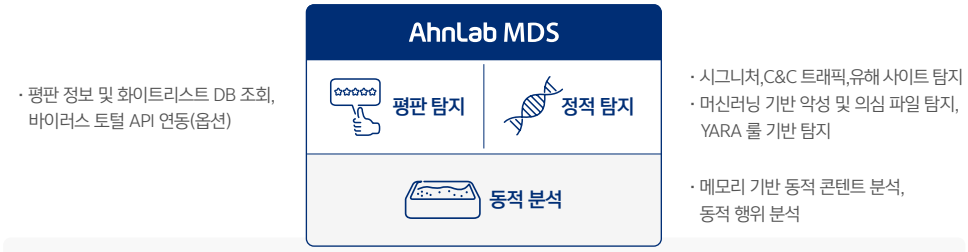
위협 가시성을 기반으로 공격 단계별 최적화된 대응 가능
- 위협 유형, 유입 경로, 연관 관계, 공격 프로세스 등에 대한 직관적인 가시성
- 공격의 진행 단계별 최적화된 대응 조치 제공

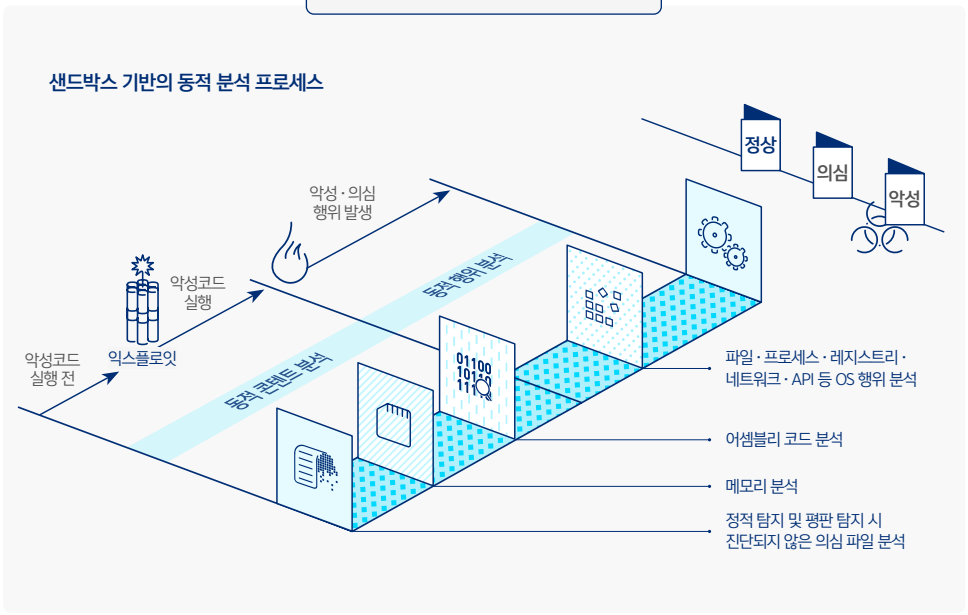


멀티엔진 기반의 정교한 위협 탐지

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.

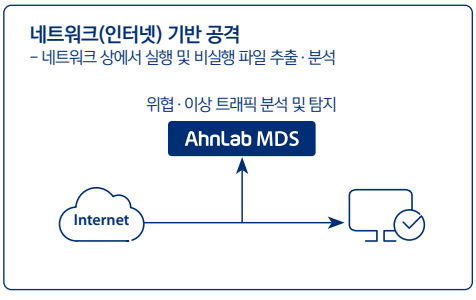
*익스플로잇(Exploit): 시스템이나 응용 프로그램의 버그 또는 보안 취약점 등을 이용해 악의적인 행위를 실행하는 공격 방식

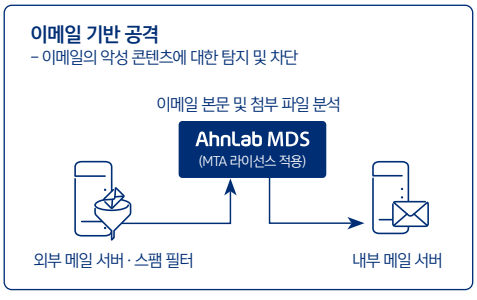


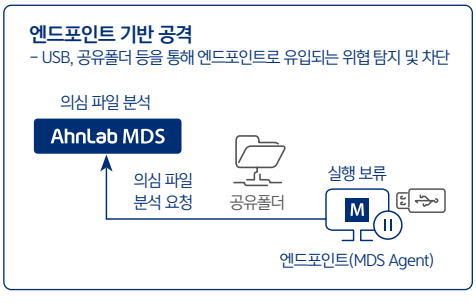


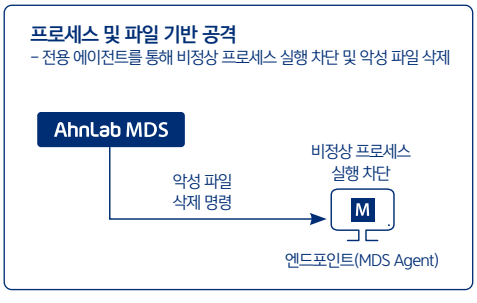
공격 유형별 최적화된 대응

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.



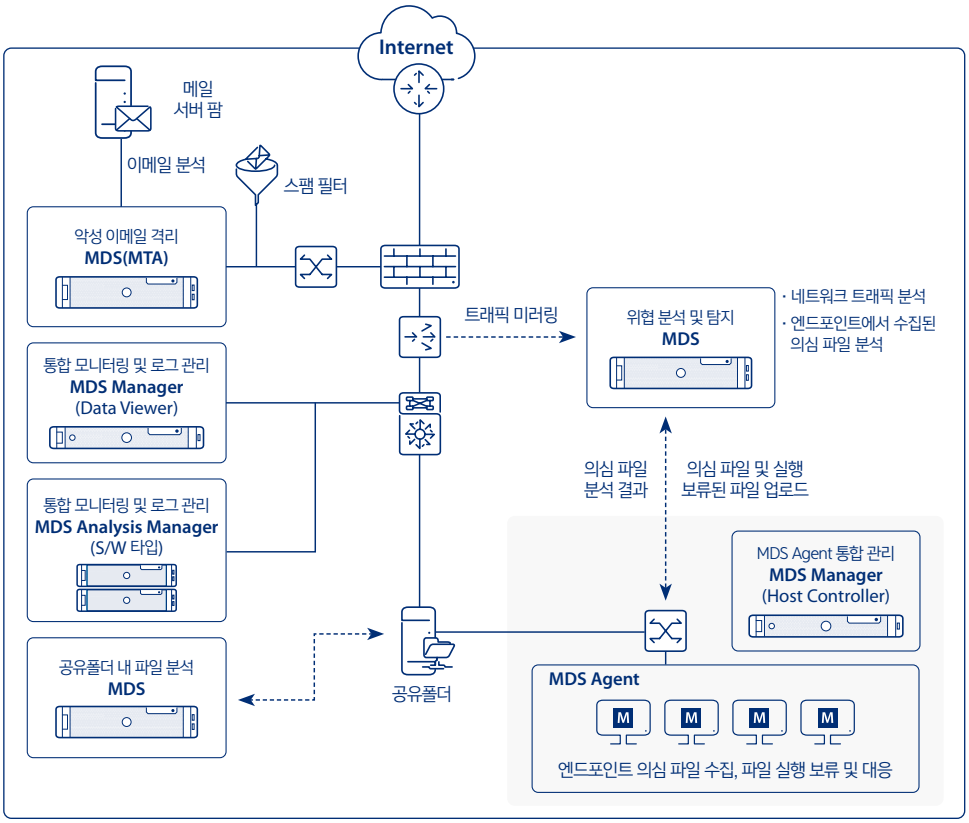






솔루션 구성 및 구축 방식

AhnLab MDS는 위협 탐지 및 분석을 위한 MDS와 통합 모니터링 및 관리를 위한 MDS Manager, MDS Analysis Manager(S/W 타입), 엔드포인트에서의 위협 대응을 위한 전용 에이전트(MDS Agent)로 구성되어 있습니다.



MDS : 멀티엔진 기반의 위협 탐지 및 분석

- 주요 인터넷 서비스 프로토콜 수집 및 분석(HTTP, SMTP, SMB/CIFS, FTP 등)
- 이메일 본문 및 첨부파일에 대한 위협 탐지 · 격리(MTA 라이선스 적용)
- 시그니처, 머신러닝 기반의 정적 진단 및 샌드박스 기반의 동적 분석을 통한 신종 위협 탐지
- MS오피스, 아래아한글 등 비실행형(non-PE) 파일의 악성코드 탐지를 위한 전용 엔진 탑재
- VM 분석 또는 C&C 탐지 내역에 대한 PCAP 기반 패킷 캡쳐 및 PCAP 파일 다운로드
- MDS Manager를 통한 행위 분석 결과 및 클라우드 기반 행위 분석 정보 공유

MDS Manager : 통합 모니터링 및 관리

Data Viewer : MDS 장비 통합 모니터링 및 로그 관리

- 직관적인 대시보드를 통해 주요 탐지 현황 및 이벤트 정보 제공
- 이벤트 종류, IP 주소, 행위 내역(파일/프로세스/레지스트리/네트워크) 등에 대한 상세 로그
- 네트워크 구간, 이메일 구간, 공유폴더 등 다중 경로에 설치된 MDS 탐지 이벤트 및 로그 통합 관리
- MDS 장비의 행위 분석 결과 공유(다수의 MDS 장비 구성 시 중복 분석 및 탐지 최소화)
- YARA 탐지 룰(Rule) 관리 및 배포 시스템 연동, Syslog 전송 기능(CEF, LEEF 포맷)

Host Controller: MDS Agent 통합 관리 및 대응

- MDS Agent의 설치, 패치 관리, 그룹 및 정책 관리
- MDS Agent 대응 명령 및 공지사항 전송

MDS Analysis Manager : MDS 장비 통합 모니터링 및 로그 관리 (S/W 타입)

- MDS Manager의 데이터 뷰어(Data Viewer)와 동일한 기능 제공
- 멀티테넌시 지원 (IP단위, 다수 사이트 관리자 접근 · 운영 가능)

MDS Agent : 엔드포인트 의심 파일 수집 및 대응 조치

- 독자적인 머신러닝 기술을 적용한 엔드포인트 의심 파일 수집 기능
- 악성코드 감염이 의심되는 호스트에 대한 네트워크 격리 등 대응 조치
- 비정상적인 프로세스 실행 탐지 및 의심스러운 파일에 대한 실행 보류 기능
- V3 통합 에이전트를 통한 엔드포인트 영역의 악성코드 치료 및 방어 체계 강화

제품 사양

AhnLab MDS

구분	MDS 4000A	MDS 8000A	MDS 10000A	
관리 에이전트 수(권장)	700개	2,000개	5,000개	
트래픽 처리	1Gbps	2Gbps	5Gbps	
HDD	1.2TB x 2ea.	1.2TB x 4ea.	1.2TB x 8ea.	
RAID	RAID 1	RAID 10	RAID 10	
네트워크 인터페이스	1GbE 4 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)	1GbE 4 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)	기본 (Default)	1GbE 2 Ports (Copper) 1/10G Base-T 2 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)
			옵션 (Optional)	1GbE 2 Ports (Copper) 1/10G Base-T 4 Ports (Copper) 1/10G SFP+ 6 Ports (Optical)
전원	750W Redundant			
랙 마운트	1U, 19 inch	1U, 19 inch	2U, 19 inch	
사이즈(WxDxH)	482 x 721.91 x 42.8mm	482 x 721.91 x 42.8mm	482.4 x 715.5 x 86.8mm	

※ 장비의 성능 수치는 고객사 환경 및 설정에 따라 다소의 차이가 있을 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	

※ 장비의 성능 수치는 고객사 환경 및 설정에 따라 다소의 차이가 있을 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