AhnLab MDS

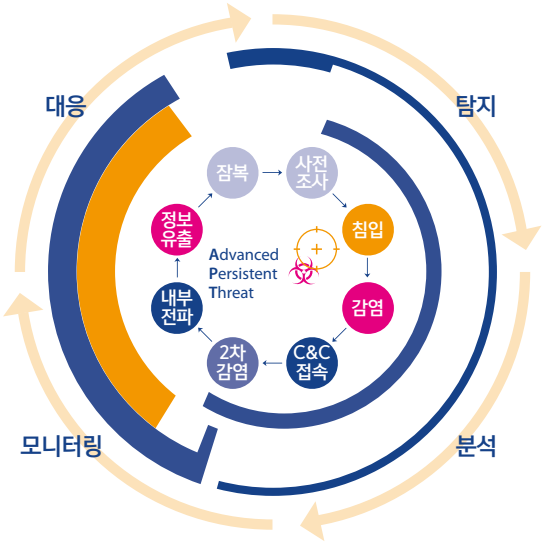
지능형 위협 대응 솔루션

차별적인 위협 가시성 제공
네트워크와 엔드포인트 레벨의 유기적 대응

탐지 분석 모니터링 대응

제품 개요

AhnLab MDS(Malware Defense System)는 차별적인 위협 가시성 기반의 지능형 위협(APT, Advanced Persistent Threat) 대응 솔루션입니다. 신종 악성코드 및 익스플로잇(exploit)에 대한 '탐지-분석-모니터링-대응' 프로세스를 통해 타깃 공격을 비롯한 APT 공격, 랜섬웨어 공격에 효과적으로 대응합니다.

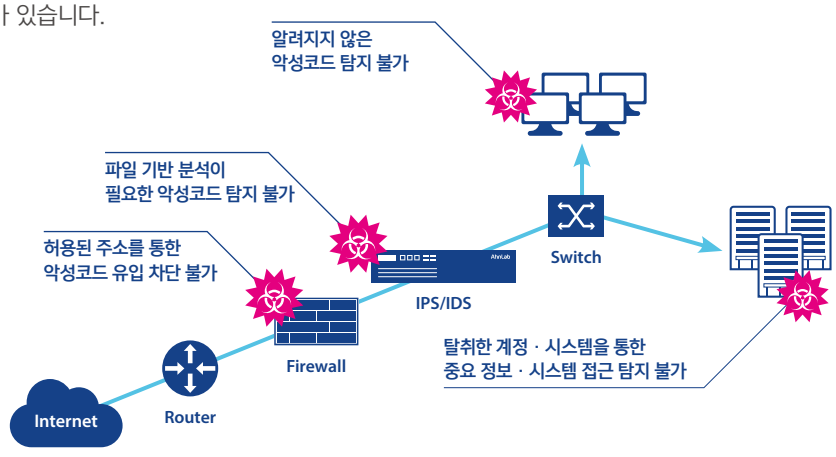


차세대 위협 대응의 모든 것, AhnLab MDS!

- 직관적인 대시보드, 차별적인 위협 가시성
- 신속한 신·변종 및 숨겨진 공격 탐지
- 머신러닝 등 독보적인 위협 분석 기술 다수 적용
- 네트워크 트래픽 실시간 분석 및 대응
- 엔드포인트 기반의 즉각적인 조치 및 대응

왜 '지능형 위협'인가?

최근 발생하는 타깃 공격과 지능형 위협은 각종 은닉 기법과 사회공학적 공격 등을 이용해 기존 보안 솔루션을 우회하고 있습니다. 따라서 기존 보안 솔루션만으로 나날이 고도화되는 최신 공격에 대응하기에는 한계가 있습니다.



[기존 보안 솔루션의 지능형 위협 대응 한계]

특장점

안랩의 독자적인 지능형 위협 분석 노하우가 집약된 AhnLab MDS는 탐지부터 분석, 모니터링, 네트워크-엔드포인트 대응의 워크플로우를 기반으로 효과적인 지능형 위협 대응에 기여합니다. AhnLab MDS의 독보적인 위협 대응 프로세스를 통해 알려지지 않은(unknown) 위협, APT 및 다양한 경로를 이용한 고도화된 공격을 조기에 탐지 및 대응할 수 있습니다.

네트워크 및 엔드포인트 레벨 위협 탐지

- 웹, 이메일, 파일 전송(FTP/SMB/CIFS/NFS)을 통해 유입/전파되는 위협 탐지
- 실행 및 비실행형 파일, 웹 오브젝트, 안드로이드 앱(app) 파일 추출
- 암호화 채널을 통해 유입/전파되는 의심스러운 파일의 실행 보류 후 수집
- 독자적인 머신러닝 기술을 활용한 의심 파일 추출

멀티엔진 기반의 위협 분석

- 시그니처, 평판, 비시그니처(signature-less) 등 멀티엔진 기반의 위협 분석
- 정적(static) 분석 및 동적(dynamic) 분석 기술이 융합된 하이브리드 분석 제공
- 취약점 공격(exploit)을 이용한 문서형 악성코드 탐지에 최적화된 독자적인 '동적 콘텐츠 분석' 기술 적용
- 신종 악성코드 분석에 최적화된 Windows 가상 OS 환경 제공

실시간 위협 모니터링

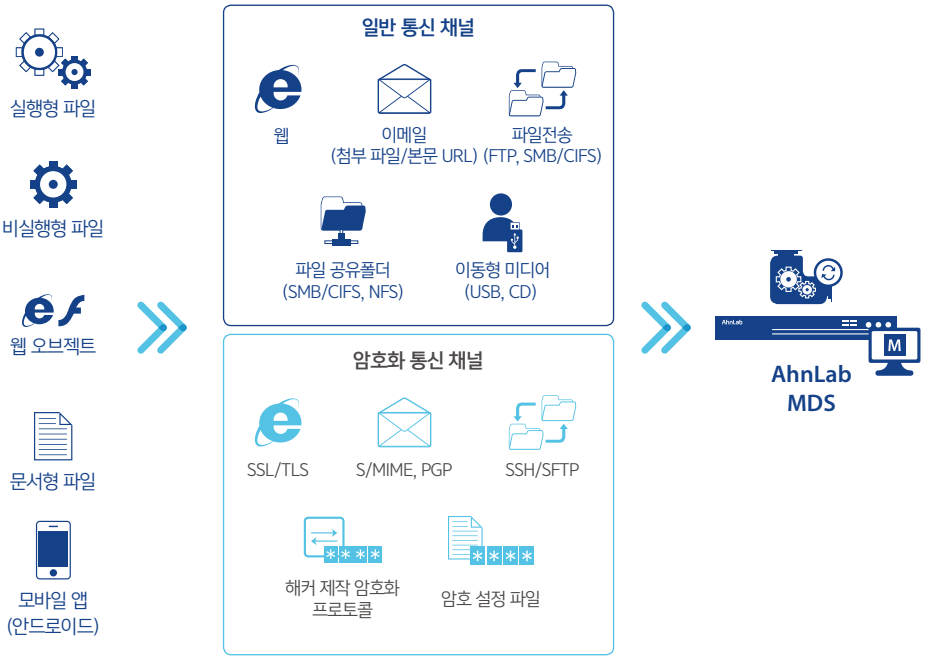
- 모든 탐지 및 분석 대상의 악성 여부에 대한 명확한 가시성 제공
- 신종 악성코드 및 의심 파일/이벤트에 대한 선별적 모니터링 가능
- 관심 이벤트(파일, IP, 도메인)에 대한 집중 모니터링 기능 제공

네트워크 및 에이전트 기반 위협 대응

- C&C 통신 차단 및 악성코드 유포 · 배포 사이트 접속 차단
- PC 내 악성 여부가 확인되지 않은 실행형 파일 및 문서 파일에 대한 '실행 보류' 기능 제공
- 탐지된 신종 악성코드에 대한 즉각적인 제거 및 해당 PC 격리 기능 제공
- V3 Internet Security/Endpoint Security 9.0과 통합 설치본 형태의 에이전트 제공 가능

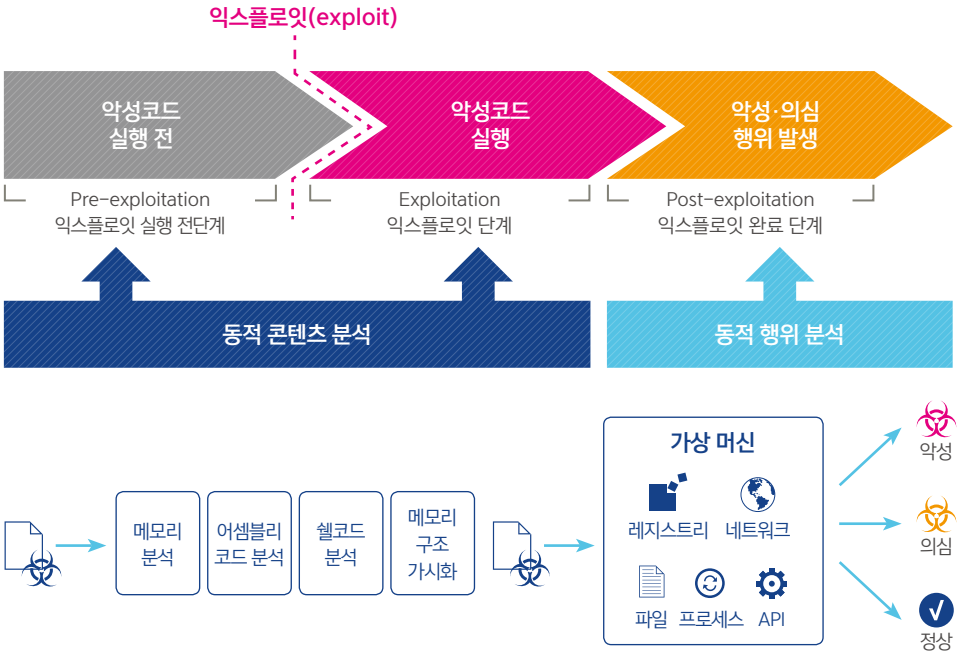
탐지-분석-모니터링-대응

AhnLab MDS는 네트워크 레벨에서 엔드포인트 레벨까지 지능형 위협이 유입될 수 있는 모든 경로를 능동적으로 **탐지**합니다. 특히 다양한 암호화 채널을 통해 유입되는 의심스러운 파일은 엔드포인트 레벨에서 에이전트를 통한 '실행 보류(Execution Holding)' 후 수집 · 분석을 진행함으로써 잠재적인 위협까지 탐지합니다.



탐지-**분석**-모니터링-대응

AhnLab MDS는 정적(static) 및 동적(dynamic) 악성코드 분석 기술과 노하우가 융합된 **하이브리드 분석 기술**을 통해 알려지지 않은 신종 위협까지 정확하게 탐지합니다. 독보적인 '메모리 분석 기반의 익스플로잇(exploit) 탐지 기술'이 적용된 AhnLab MDS는 악의적인 행위의 종류나 행위 발생 여부와 관계없이 악성코드를 정확하게 탐지해 제로데이 공격은 물론, 샌드박스 분석을 우회하는 악성코드에 대한 분석이 가능합니다.

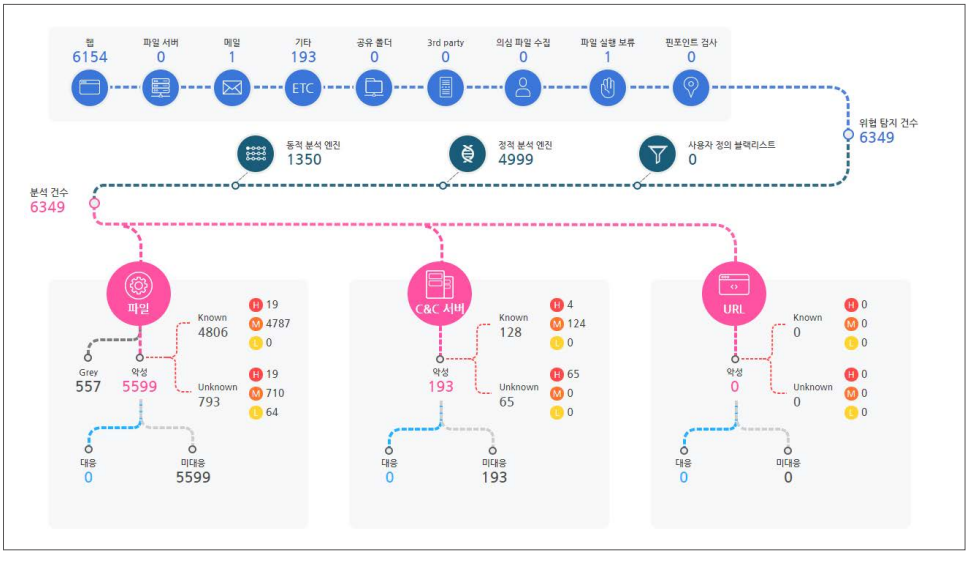


- 리버스 엔지니어링 기법의 메모리 분석
- 상세 메모리 덤프 및 어셈블리 코드 분석
- 쉘코드의 익스플로잇(exploit) 여부와 상관없이 악성 판정 가능
- 행위 발생 여부와 상관없이 탐지 가능

- 파일, 프로세스, 레지스트리, 네트워크, API 등 OS 행위 분석
- 개별 행위 객체에 대한 평판 지수 반영
- 행위간 상관 분석을 통해 숨겨진 의도까지 정확하게 파악 가능

탐지-분석-**모니터링**-대응

AhnLab MDS는 위협의 종류, 유입 경로, 확산 정도 및 분석 현황 등에 대해 직관적이고 차별적인 위협 가시성을 제공합니다. 위협의 종류, 행위 및 공격 단계에 따라 대응 및 조치 방안을 제시하며, 동적 콘텐트 분석(DICA)을 통해 어셈블리코드 및 메모리 분석에 관한 상세하고 직관적인 리포트를 제공해 효율적인 위협 대응 및 관리에 기여합니다.



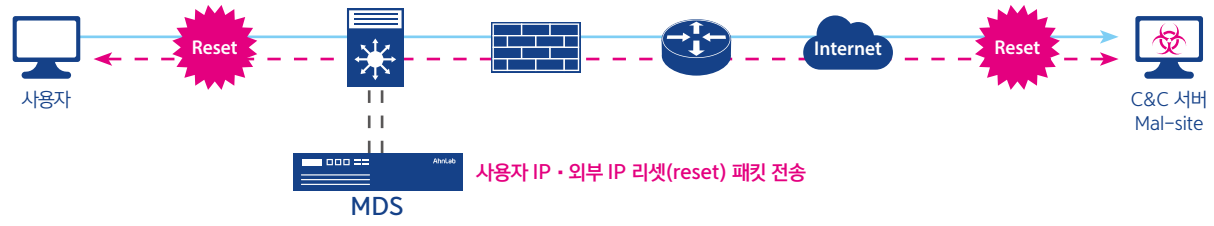
▲ AhnLab MDS 대시보드(위협 추이)

탐지-분석-모니터링-**대응**

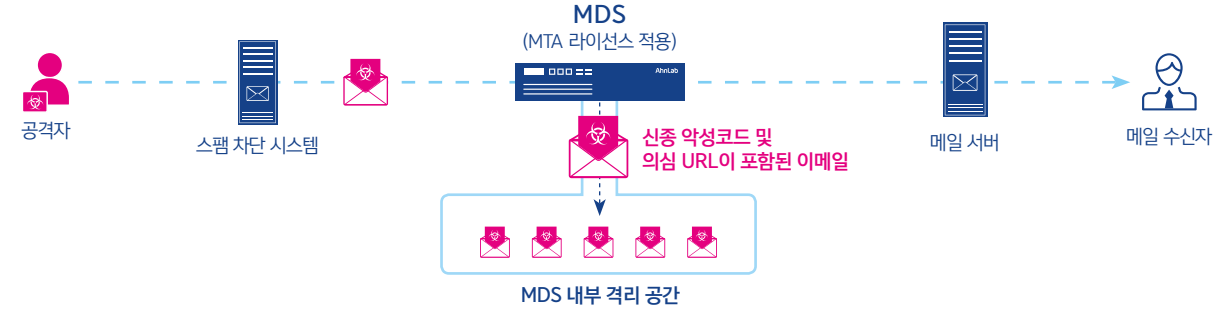
AhnLab MDS는 에이전트 설치 여부와 관계없이 네트워크 기반의 대응이 가능합니다. 또한 네트워크 레벨뿐만 아니라 엔드포인트 레벨에서의 능동적인 대응을 위해 제공되는 전용 에이전트를 통해 신종 악성코드 삭제 및 의심스러운 실행형 파일에 대한 '실행 보류(Execution Holding, EH)' 기능을 이용할 수 있습니다. AhnLab MDS 에이전트는 기존에 설치된 안티바이러스 솔루션(AV, 백신)과 충돌 없이 동시에 설치가 가능합니다.

네트워크 기반 대응

네트워크 이상 트래픽 차단

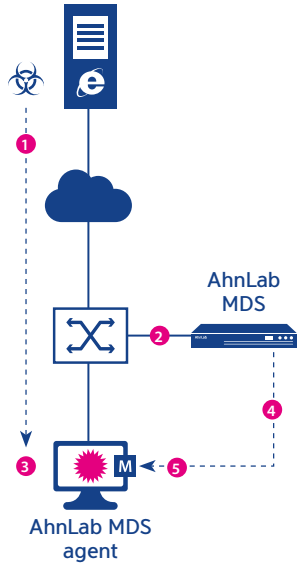


악성 메일 격리 (*MTA 라이선스 적용 방식)



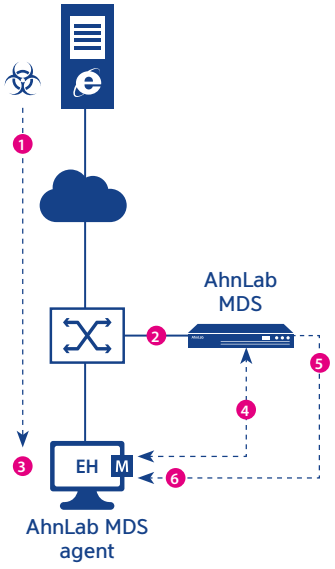
엔드포인트 기반 대응

호스트 격리/악성코드 삭제 기능



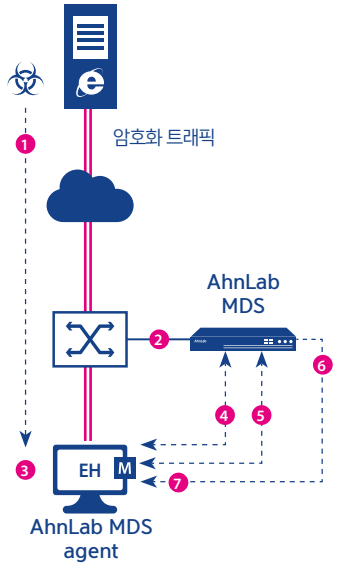
1. 악성코드 다운로드
2. 트래픽 미러링 및 분석 시작
3. 악성코드의 PC 유입/저장
4. 분석 완료 및 '신종' 악성코드 판정
5. 호스트 격리 및 악성코드 삭제

실행 보류 기능



1. 악성코드 다운로드
2. 트래픽 미러링 및 분석 시작
3. 악성코드의 PC 유입/저장
4. 실행 보류(EH) 동작 및 분석 여부 확인
5. 분석 완료 및 '신종' 악성코드 판정
6. 호스트 격리 및 악성코드 삭제

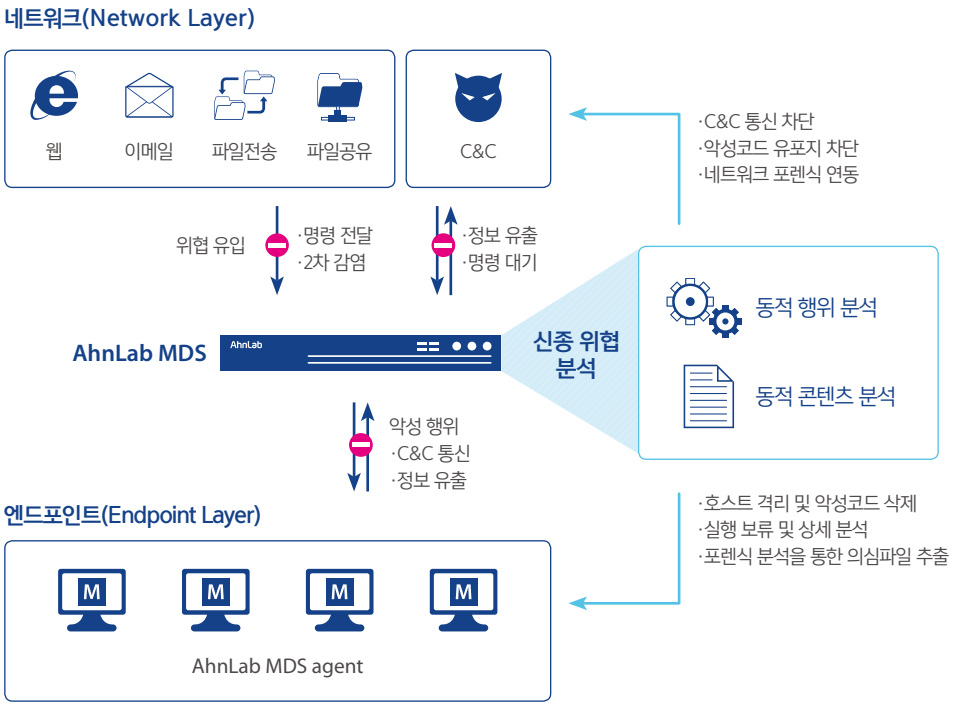
파일 업로드 분석 기능



1. 악성코드 다운로드(암호화 트래픽)
2. 트래픽 미러링 - 단, 분석 불가능
3. 악성코드의 PC 유입/저장
4. 실행 보류(EH) 동작 및 분석 여부 확인
5. 해당 파일을 AhnLab MDS로 전송 후 분석
6. 분석 완료 및 '신종' 악성코드 판정
7. 호스트 격리 및 악성코드 삭제

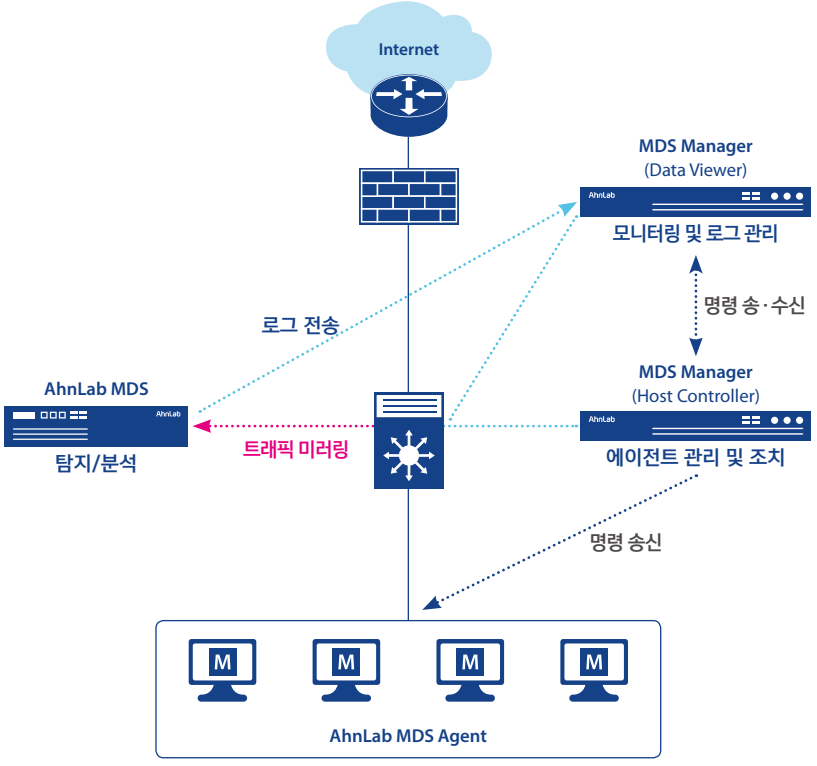
차별적인 대응 체계

AhnLab MDS는 네트워크로 유입되는 위협의 최초 감염 단계부터 감염 이후 C&C 서버와의 통신을 통한 2차 감염, 내부 전파(확산), 정보 유출 등 악의적인 행위, 잠복 단계까지 '지능형 위협의 라이프사이클'을 중심으로 위협에 대한 가시성과 실질적인 대응 체계를 제공합니다.



솔루션 구성 예시

지능형 위협에 대한 '탐지-분석-모니터링-대응' 체계를 제공하는 AhnLab MDS는 기업의 환경 및 도입 목적에 따라 기본형, 통합형, 또는 단독 조합형 등 다양하고 유연한 방식으로 구축할 수 있습니다.



제품 사양

▶ AhnLab MDS

구분		AhnLab MDS 4000	AhnLab MDS 8000	AhnLab MDS 10000
제안 성능	동적 분석 건수	35,000 건/1일	90,000 건/1일	200,000 건/1일
	관리 에이전트	700개	2,000개	5,000개
트래픽 처리		800Mbps	1.5Gbps	4Gbps
HDD		2 TB	4 TB	8 TB
인터페이스		1G Copper * 4 ea. 1G/10G Fiber * 4 ea.	1G Copper * 4 ea. 1G/10G Fiber * 4 ea.	1G Copper * 2 ea. 1G/10G Copper * 4 ea. 1G/10G Fiber * 6 ea.
전원		550W Redundant Power (dual)	550W Redundant Power (dual)	750W Redundant Power (dual)
랙 마운트		1U, 19 inch	1U, 19 inch	2U, 19 inch
사이즈(WxDxH, mm)		482.4 x 676.9 x 42.8	482.4 x 676.9 x 42.8	482.4 x 723.0 x 87.3

* 에이전트 추가 시 MDS Manager 추가 필요

▶ AhnLab MDS 에이전트 사용 환경

구분	운영체제(OS)
Client PC	Windows XP SP2 이상 / 7 / 8(8.1) / 10
Server	Windows Server 2003 / 2008 / 2012

* 상기 OS의 32/64 bit 지원

▶ AhnLab MDS Manager

구분		MDS Manager 5000AR	MDS Manager 10000AR
관리 에이전트	통합형(DV + HC)	2,000개	5,000개
	단독형 (Host Controller 전용)	5,000개	10,000개
HDD		6 TB	12 TB
RAID		Raid 1	Raid 1
인터페이스		2 x 1GbE Ports(Copper)	2 x 1GbE Ports(Copper)
전원		500W Redundant Power	740W Redundant Power
랙 마운트		1U, 19 inch	2U, 19 inch
사이즈(WxDxH, mm)		437 x 508 x 43	427 x 648 x 89
구축 가능 조합		Host Controller + Data Viewer Data Viewer Host Controller	

- DV(Data Viewer): 통합 모니터링 및 로그 관리 기능
- HC(Host Controller): 에이전트 관리 및 조치 기능

※ 각 장비의 성능 수치는 고객사 환경 및 설정에 따라 다소의 차이가 있을 수 있습니다.

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