AhnLab
NETWORK PLUS

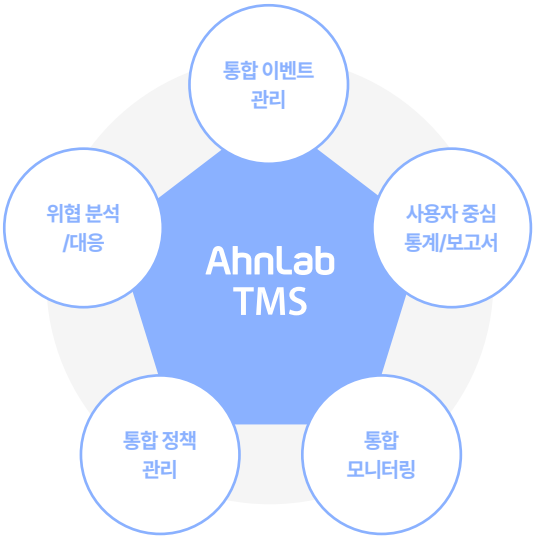
AhnLab TMS

차세대 네트워크 통합 위협 관리 플랫폼

AhnLab TMS는 다수의 네트워크 보안 장비를 관리하며,
대용량 이벤트에 대한 고도화된 위협 분석과 모니터링을 제공합니다.

제품 개요

AhnLab TMS(Threat Management System)는 다수의 장비를 관리하며 다양한 위협 정보를 종합적으로 모니터링하고 분석하며 연동된 장비들과 유기적으로 대응하는 **네트워크 통합 위협 관리 플랫폼**입니다. 연동 장비에 대한 효율적인 정책 관리와 대용량 이벤트에 대한 수집/관리, 차세대 분석 기술을 통한 심층적인 분석과 대응을 제공하는 차세대 통합 위협 관리 솔루션입니다.

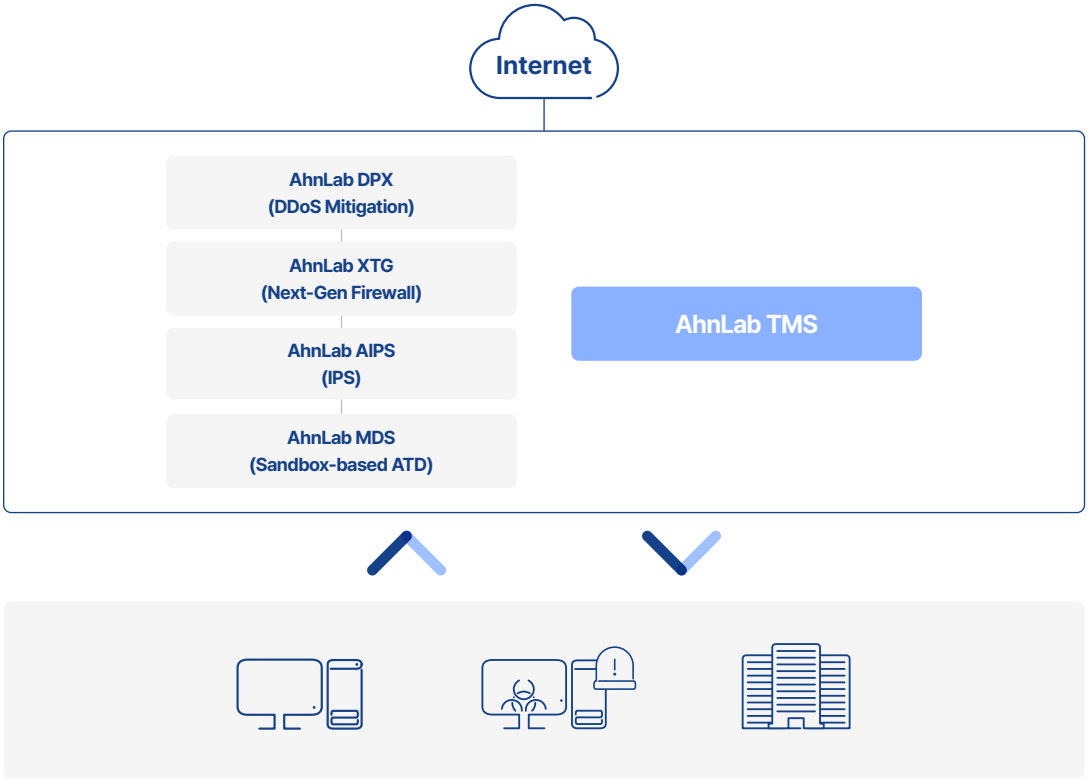


차세대 통합 위협 관리의 필요성

최근의 네트워크 환경은 모바일에서 IoT 기기까지 다양화 되고 있으며, 보안의 위협은 갈수록 진화되고 있습니다. 기존의 단일 솔루션으로 이러한 환경의 변화와 보안 위협을 대응하기 어렵기 때문에 종합적으로 관리하고 대응하는 통합 위협 관리 플랫폼의 필요성이 점점 더 요구되고 있습니다.

차세대 네트워크 통합 위협 관리 플랫폼

AhnLab TMS는 자사의 네트워크 보안 솔루션인 차세대 방화벽, IPS, DDoS 대응 솔루션과 APT 대응 솔루션에 대해 통합 매니지먼트를 제공합니다. 하나의 솔루션에서 대응할 수 없는 다양한 보안 위협에 대해서 통합적으로 분석 및 대응할 수 있도록 유기적인 연동을 제공합니다.

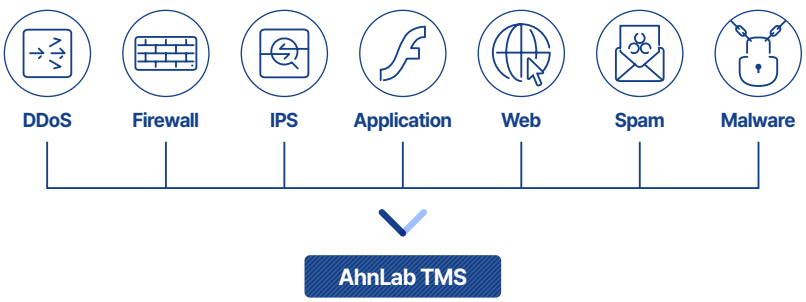


NW 보안 영역부터 Anti-APT 영역까지 폭넓은 위협 분석과 대응

효율적이고 유연한 장비 관리
- 연동 장비의 효율적 운영 및 모니터링
- 방화벽, DDoS, VPN, IPS에 대한 다수 장비 보안 정책 관리(MDS 정책 미지원)

고성능 빅데이터 엔진 기반 통합 이벤트 관리
- 다수의 장비에서 수집되는 대용량 로그의 빠른 수집 및 관리
- 빠른 검색과 유연한 통계 설정으로 위협에 대한 신속한 분석
- 소프트웨어 기술력이 집약된 고성능 빅데이터 처리 엔진

다양한 위협에 대한 심층 분석과 대응
- 다양한 장비에서 수집된 다양한 이벤트의 종합적 분석
- 고도화된 분석 기술을 적용한 심층적인 위협 분석
- 신속한 대응을 위한 자동대응 기능 제공



심층적인 위협 분석

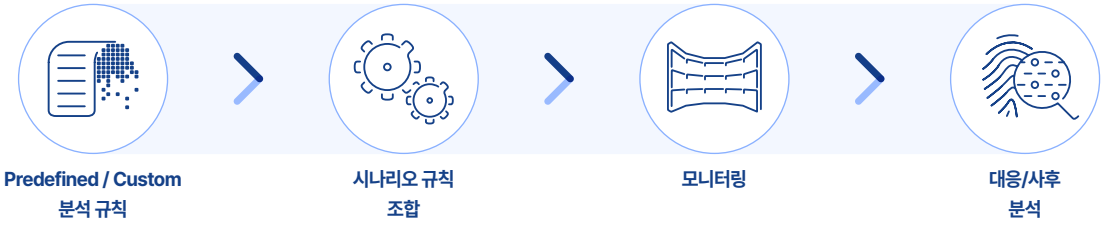
AhnLab TMS는 보안 위협 분석을 위해 머신러닝 기반 이상행위 분석을 제공합니다. 다양한 연동 장비로부터 수집된 대용량의 이벤트를 자동적이고, 심층적으로 분석함으로써 보안 관리자에게 보안 위협을 보다 신속하고, 편리하게 분석하고 대응할 수 있도록 지원합니다.

머신 러닝을 적용한 네트워크 이상행위 탐지

지속적인 모니터링과 분석이 필요한 대상에 대해 학습을 통해 축적된 패턴을 바탕으로 비정상 행위를 자동적으로 판단하고, 경보하는 자동화된 분석을 제공합니다.

시나리오 기반 상관 분석

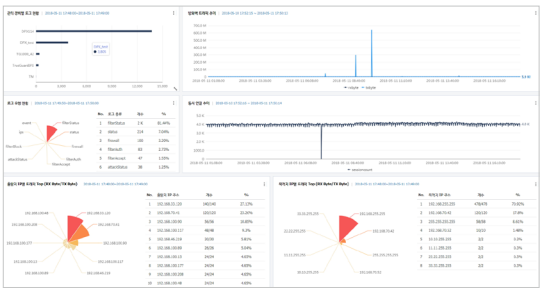
연동 제품으로부터 수집된 다양한 종류의 이벤트를 조합하여 시나리오 기반 상관 분석과 임계치 기반 분석을 제공합니다. 단일 제품에서 탐지할 수 없는 다양한 침투 시나리오에 대해 각종 이벤트를 조합한 다 계층의 탐지 분석 규칙으로 통합적으로 분석하며, 분석 상태에 대한 실시간 모니터링과 대응을 지원합니다.



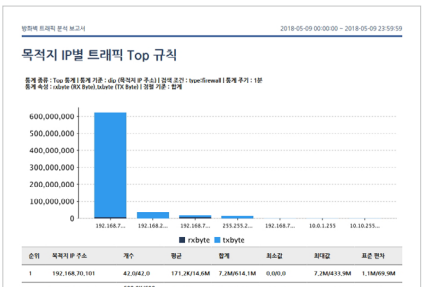
사용자 중심의 유연한 통계/분석

AhnLab TMS는 사용자 중심의 유연한 모니터링과 가시성을 지원하기 위해서 Custom 모니터링과 리포팅 기능을 제공합니다. 보안 관리자는 위협 이벤트를 검색하고, 지속적인 통계와 분석이 필요한 경우 사용자 정의 통계/분석 규칙으로 생성합니다. 또한, 생성된 통계/분석 규칙은 실시간 모니터링을 위해 Custom 대시보드에 추가하고, 리포팅을 위해 Custom 보고서로 유연하게 사용할 수 있습니다.

Custom 대시보드



Custom 보고서



모듈 구성

AhnLab TMS는 효과적인 위협관리와 통합 정책관리를 위해서 Threat Manager, Policy Manager의 2가지 모듈을 제공합니다.

Threat Manager

- 다수 장비 로그 수집 및 통합 로그 검색 (XTG, AIPS, DPX, MDS)
- 3rd Party 장비 로그 수집
- Custom 대시보드, Custom 보고서
- 고도화된 위협 분석 (상관 분석, 연관 분석, 이상행위 분석)
- 유연한 통계 모니터링
- 시스템, 네트워크, 보안 이벤트, 장애 상태, VPN 모니터링
- 지역기반 모니터링, 토폴로지 모니터링

Policy Manager

- 다수 장비 통합 / 개별 정책 설정 및 관리(MDS 정책 미지원)
- 정책 백업 / 복원
- 폐쇄망 엔진 업데이트
- 통합 스크립트

제품 사양

구분		TMS 5000C	TMS 15000C	TMS 25000C
CPU		8Core	16Core	32Core
RAM		32GB	64GB	128GB
SSD		480GB	480GB	480GB
Interface 기본	Mgmt	2 * 1G Copper (Default)	2 * 1G Copper (OCP/Default)	2 * 1G Copper (OCP/Default)
Interface 옵션	1GC	2	2	2
	1GF	-	2	2
	10GF	-	2	2
Log Storage	RAID	-	기본 RAID 5[1]	기본 RAID 5[1]
	HDD	기본 2TBx1 Slot 1 Type: 1TB/2TB/4TB/8TB	기본 2TBx3 Slot 4 Type: 1TB/2TB/4TB/8TB/12TB	기본 2TBx3 Slot 8 Type: 1TB/2TB/4TB/8TB/12TB
	SSD(옵션)	-	Type: 960GB/1.92TB	Type: 960GB/1.92TB
SIZE (mm) Rack Unit		437 × 429 × 43 1U	437 × 650 × 43 1U	437 × 648 × 89 2U
Power		500W Single	860W Redundant	1200W Redundant

1) RAID 타입 옵션 0, 1, 5, 6, 10, 50, 60

* AhnLab TMS의 로그 수용 성능, 정책 관리 대수 성능은 운영 모드와 환경에 따라서 차이가 있기 때문에 별도의 기술 상담을 통해서 가이드 받으실 수 있습니다.

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

AhnLab