AhnLab CLOUD PLUS

AhnLab AIPS VM

클라우드에 최적화된 차세대 네트워크 침입방지 솔루션

AhnLab AIPS VM은 클라우드 환경에서
고도화된 네트워크 보안 위협에 대응하는 차세대 침입방지 솔루션입니다.

제품 개요

비즈니스 자산들이 클라우드에 저장되면서, 이를 노리는 보안 위협들도 계속해서 고도화되고 있습니다. 해당 자산들을 보호하고 비즈니스 생산성을 제고하고 위해서는 네트워크 침입을 효과적으로 탐지해 차단 가능한 침입방지 솔루션이 필요합니다.

AhnLab AIPS VM은 클라우드에서 독보적인 네트워크 보안 위협 대응 역량을 제공하는 차세대 클라우드 네트워크 침입방지 솔루션입니다. 클라우드 상 비즈니스 자산을 노리는 네트워크, OS, 웹 및 애플리케이션 취약점 활용 공격과 네트워크 기반 공격 및 악성코드를 탐지해 차단합니다. 또한, 클라우드에 최적화된 통합 위협관리 솔루션 AhnLab TMS VM과 연동해 탁월한 통합 관리 역량을 제공합니다.

AhnLab AIPS VM

차세대 클라우드 네트워크 침입 방지 솔루션

Next-Gen IPS
향상된 탐지 엔진과 정교한 시그니처
기반 차세대 침입방지 솔루션

Anomaly Detection
다양한 탐지 필터와 기능으로
뛰어난 위협 탐지 및 대응 능력 보유

Threat Intelligence
안랩만의 위협 인텔리전스를 기반으로 지
능적인 위협 대응

Malware
멀웨어 및 알려지지 않은 공격을 탐지하여
고도화된 위협 대응

Optimization
하이브리드 클라우드 환경에
최적화된 침입방지 기능 및 성능

Open API
다양한 보안 솔루션 연동을 위한
Open API 방식 채택

특장점

AhnLab AIPS VM은 안랩의 아시아 최고, 최대 규모의 보안 위협 분석 조직 및 인프라를 기반으로 국내 네트워크 환경에 최적화된 10,000여 개의 최신 네트워크 공격 대응 시그니처를 제공합니다. 더불어, 정교한 탐지 엔진을 바탕으로 뛰어난 가시성을 제공하고 AhnLab TMS VM 연동을 통해 관리 편의성을 확보하여 보안 위협에 효과적으로 대응할 수 있도록 합니다.

지능화된 네트워크 위협 탐지
- 고도화된 탐지 엔진과 차세대 IPS 기능으로 다양한 경로의 보안 위협 대응
- 멀웨어 탐지, AhnLab TMS VM 연계를 통해 복합적인 위협에 선제 대응

쉽고 편리한 운영 및 관리
- 뛰어난 가시성을 제공해 쉽고 직관적인 정보 확인 가능
- 다양한 통계와 유연한 드릴 다운(Drill Down)으로 위협 정보 상세 분석

쉽고 안정적인 배포
- CSP 마켓플레이스에서 서비스 신청 시 간단한 절차로 이용 가능
- 이중화 구성을 지원하여 장애로부터 네트워크 안정성 확보

도입효과 1
탁월한 위협 대응

AhnLab AIPS VM이 제공하는 탁월한 위협 대응의 중심에는 고도화된 탐지 엔진이 있습니다. AhnLab AIPS VM의 탐지 엔진은 고속 패턴 매칭을 기반으로 L2-L7에 대한 탐지부터 트래픽 내 악성 파일 탐지를 지원합니다. 이와 함께, 차세대 IPS 기능과 다른 보안 솔루션과의 연동을 통해 네트워크 보안 위협에 대응하고, 고객의 비즈니스 환경을 안전하게 보호합니다.

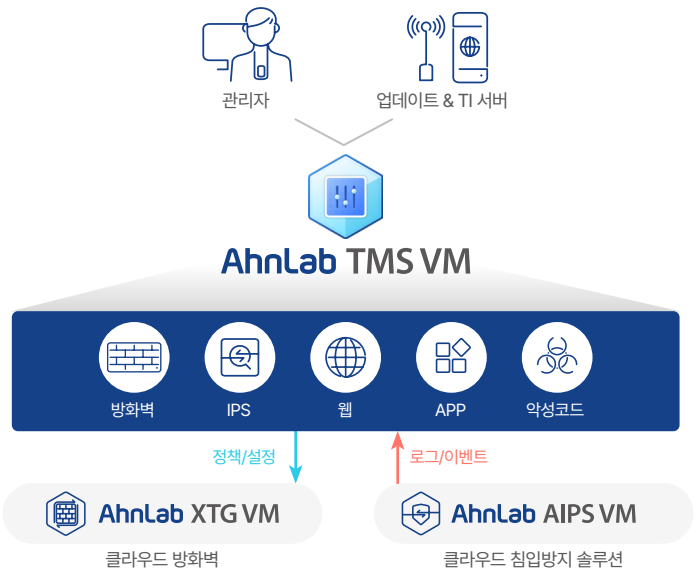
트래픽 기반 탐지
- 고속 패턴 매칭
- 애플리케이션 제어
- 행위기반 탐지(임계치 기반, SCAN 공격)
- 비정상 프로토콜 차단(HTTP, DNS, SIP)
- 암호화 트래픽 분석

멀웨어 기반 탐지
- YARA 엔진 및 시그니처(정적 분석)
- 악성파일 추출
- TMS VM 연계를 통한 정밀 분석

도입효과 2
편리한 통합 관리

AhnLab AIPS VM은 차세대 네트워크 통합 보안 플랫폼 AhnLab TMS VM 연동을 통해 더욱 효율적이고 직관적인 모니터링과 관리 편의성을 제공합니다. AhnLab TMS VM은 AhnLab AIPS VM 뿐만 아니라 안랩의 네트워크 가상화 제품들과도 유연하게 연동하여 종합적인 위협 분석을 수행합니다. 특히, 공공기관 위협 대응 체계 연동을 통해 기관에서 배포하는 탐지 규칙의 배포/관리가 가능합니다.

* AhnLab TMS VM는 별도 구매 필요



공공기관 위협 대응체계 연동

AhnLab AIPS VM과 TMS VM을 연계 구축하면, 클라우드 환경의 국가·공공기관 시스템을 노리는 사이버 공격을 즉시 탐지해 대응하는 위협 대응체계와 연동할 수 있습니다. 국가기관 또는 상위기관에서 배포하는 탐지 규칙을 하위 기관의 AhnLab AIPS VM에 자동 배포하고, 탐지 결과를 상위기관으로 전송하여 클라우드 환경의 공공기관 정보시스템 위협 탐지 및 모니터링 서비스를 지원합니다.

* 공공기관 위협 대응 체계 연동을 위해서는 AhnLab TMS VM 필수 구매 필요

AhnLab AIPS VM

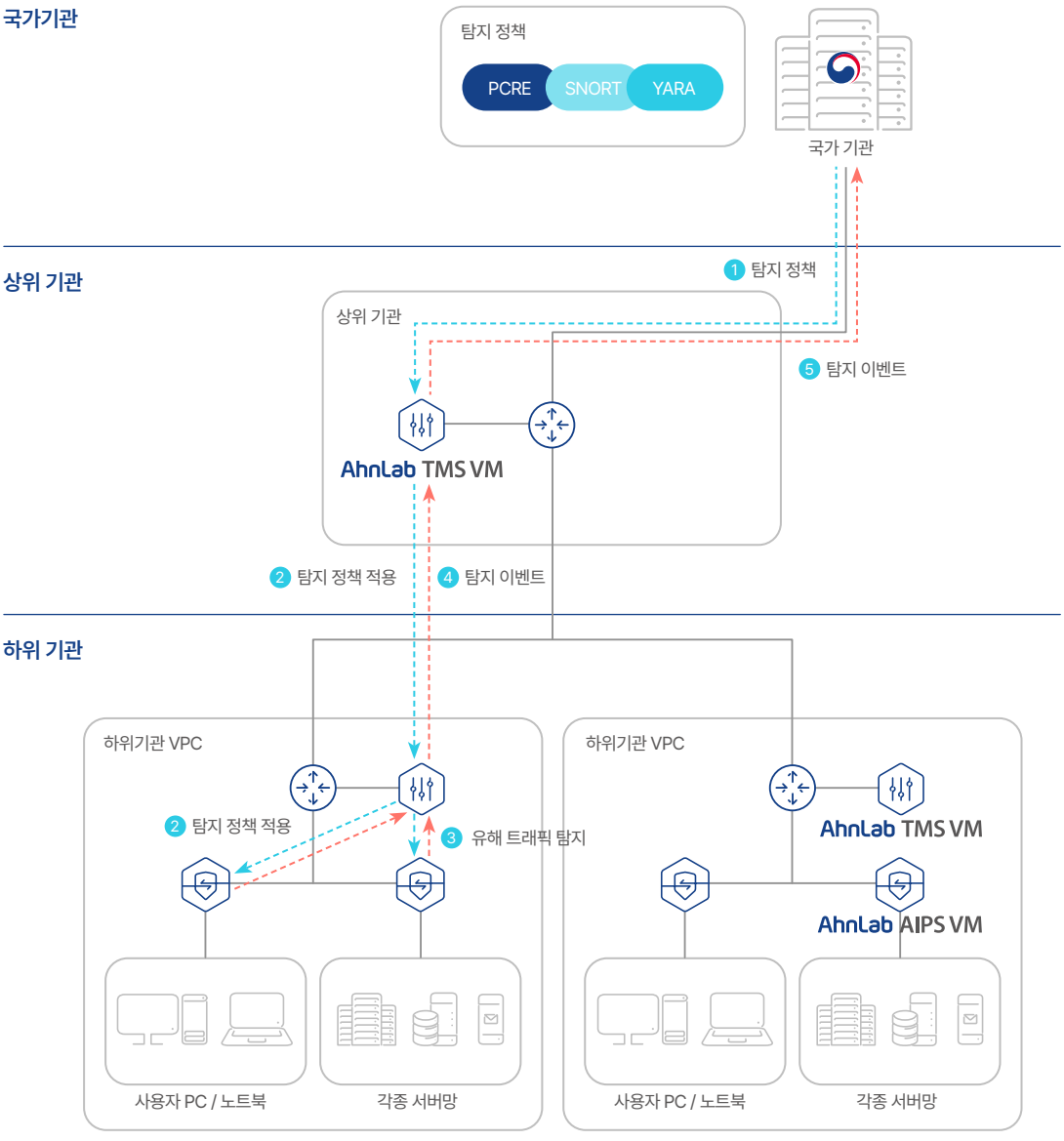
- 위협 탐지/차단
- PCRE/SNORT/YARA
- High Performance
- Threat Intelligence

AhnLab AIPS VM (Sensor) | AhnLab TMS VM (Manager)

AhnLab TMS VM

- 통합 정책/설정 관리
- 통합 위협 분석
- 향상된 모니터링/가시성
- 빅데이터 엔진

공공기관 위협 대응 체계



주요 기능

위협 탐지/차단

- Security Zone
- PCRE 정규표현식
- YARA
- Anti-virus
- 5tuple 기반 IP 제어
- 비정상 프로토콜 차단
- 행위기반 탐지 규칙
- 웹 방어
- 임계치 기반 차단
- X-Forwarded-For 헤더 내 실제 IP 추출
- SSL 트래픽 검사
- 애플리케이션 제어
- C&C 연결 차단

보안 솔루션 연계

- 통합위협관리 - AhnLab TMS VM 연동
- 공공기관 위협 대응 체계 연동
- 국가기관/상위기관 탐지 규칙 배포
- 배포 현황 관리
- 탐지 결과 전송

정보 가시성

- Pre-defined/사용자 정의 대시보드
- Pre-defined/사용자 정의 위젯
- 실시간 트래픽 모니터링
- 실시간 탐지/차단 모니터링
- 다양한 로그/통계 정보
- Drill-down을 이용한 유연한 분석
- 사용자 정의 통계 규칙
- 사용자 정의 보고서 생성

시스템 구성

- 이중화 구성
  (Active-Active/Active-Standby)

제품 사양

구분	AIPS VM	TMS VM
vCPU (Min / Recommend)	4 Core / 8 Core	4 Core / 8 Core
Memory (Min / Recommend)	8 GB / 16 GB	16 GB / 32 GB
Storage (Min / Recommend)	60 GB / 500 GB	500 GB / 500 GB

* 사이버안전센터 연동을 위해서는 TMS VM을 필수로 설치해야 합니다.
* 세부 환경 및 구성에 따라 성능 수치가 상이할 수 있습니다.
* 사용 환경에 맞는 라인업 및 CSP별 인스턴스 사양 등은 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