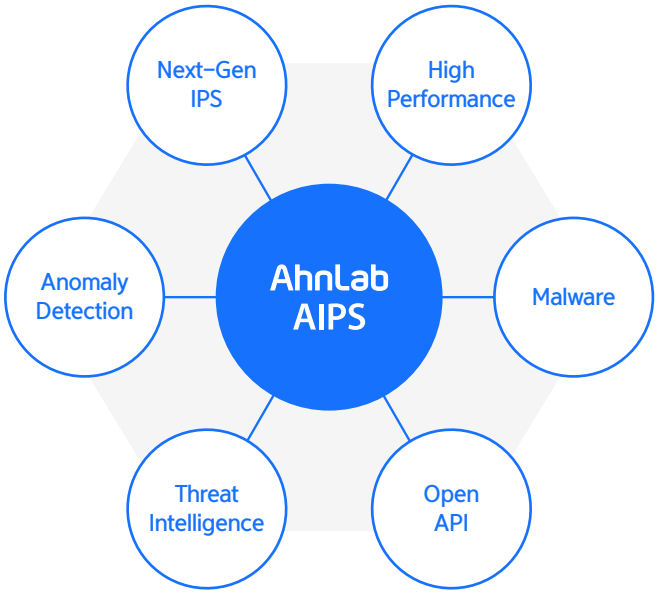
AhnLab AIPS

진화한 차세대 네트워크 침입방지 솔루션

AhnLab AIPS는 변화하는 네트워크 보안 위협에 대응하는
더욱 강력해진 차세대 침입방지 솔루션(IPS)입니다.

제품 개요

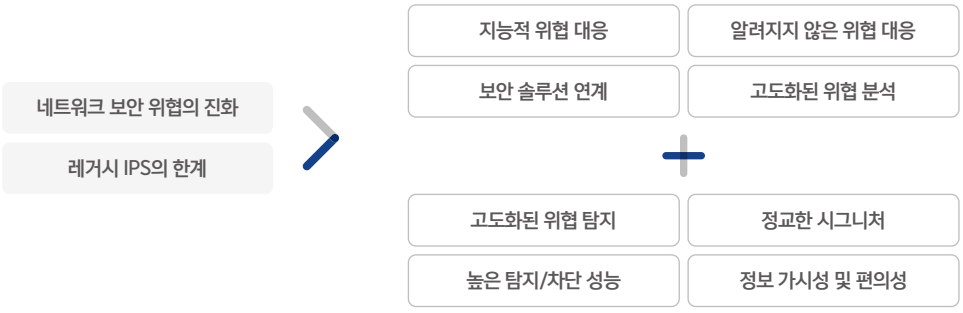
AhnLab AIPS(Advanced IPS)는 사이버 보안의 변화와 함께 고도화되는 네트워크 공격에 대응할 수 있는 **차세대 네트워크 침입방지 솔루션**입니다. 네트워크, OS, 웹 및 애플리케이션 취약점 기반의 공격은 물론 다양한 유형의 네트워크 기반 공격 및 악성코드를 통한 공격을 탐지하고 차단합니다.
AhnLab AIPS는 진화하는 네트워크 위협에 대응해 기업의 비즈니스 환경을 안전하게 보호합니다.



향상된 탐지엔진과 정교한 시그니처 기반의 **차세대 침입방지 솔루션**	다양한 탐지 필터와 가속 기술로 **뛰어난 위협 탐지 및 대응 능력**
HW 플랫폼과 SW 기술이 융합된 **고성능 패킷 처리 시스템**	다양한 보안 솔루션과의 협업을 위한 **Open API 방식 채택**
쉽고 빠르게 위협 정보 파악이 가능한 **편리한 사용자 인터페이스**	다양한 데이터, 높은 자유도를 통해 구현되는 **향상된 위협 분석**

차세대 IPS의 필요성

네트워크 보안 위협의 진화로 인해 IPS에도 변화가 생겨나고 있습니다. 기존의 IPS로는 한계에 달했고, 진화된 IPS가 필요해지고 있습니다. 알려지지 않은 공격, 수많은 멀웨어의 탐지는 물론, 공격에 활용되는 다양한 요소에 대해서도 방어가 가능해야 합니다. 또한 다양한 보안 솔루션과의 연동을 통해 네트워크 보안 위협에 대해 복합적이고 유기적으로 대응할 수 있는 차세대 IPS의 필요성이 증가하고 있습니다.



특장점

안랩이 보유한 아시아 최고, 최대 규모의 보안 위협 분석 조직 및 인프라를 기반으로, AhnLab AIPS는 국내 네트워크 환경에 최적화된 10,000여 개의 최신성과 정확성을 겸비한 네트워크 공격 대응 시그니처를 제공합니다. 이와 더불어 다양한 탐지 엔진, 뛰어난 가시성과 편의성을 통해 최신 보안 위협 환경에 최적화된 대응이 가능합니다.

지능화된 네트워크 위협 탐지

- 고도화된 탐지 엔진과 차세대 IPS 기능으로 다양한 경로의 보안 위협 대응
- 멀웨어 탐지, TMS 연계를 통해 복합적 위협에도 선제 대응

쉽고 편리한 운영 관리

- 뛰어난 가시성으로 쉽고 직관적으로 정보 확인
- 다양한 통계, 유연한 Drill Down으로 위협 정보 상세 분석

향상된 성능

- 고성능 HW와 가속 기술의 융합으로 향상된 탐지 성능
- 빅데이터 처리 기반 고성능 엔진을 통해 다양한 위협에 대한 유연하고 빠른 분석 성능 제공

보안 위협 대응

네트워크 환경 변화에 따라 기존 트래픽 기반의 공격과 더불어 멀웨어 기반의 공격이 증가하고 있습니다. AhnLab AIPS는 고도화된 탐지 엔진과 차세대 IPS 기능, 다른 보안 솔루션과의 연계를 통해 진화된 네트워크 보안 위협에 대응합니다.

트래픽 기반 탐지

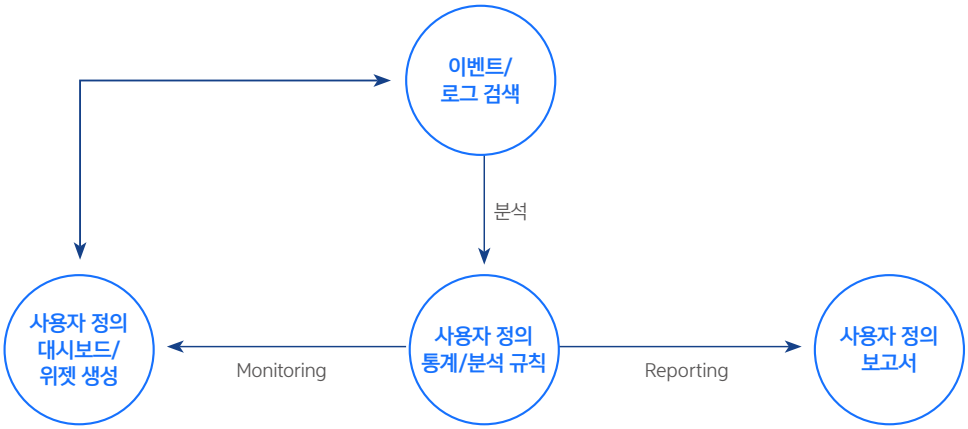
- 고속 패턴 매칭 / 애플리케이션 제어
- 행위기반 탐지(임계치 기반, SCAN 공격)
- 비정상 프로토콜 차단(HTTP, DNS, SIP)
- IP/MAC 기반 제어(비정상 MAC, IP 기반 Blacklist)
- 암호화 트래픽 분석
- C&C 서버 접속 탐지 및 차단
- IP/TCP 재조합 및 XFF 기능을 통한 우회 공격 방지

멀웨어 기반 탐지

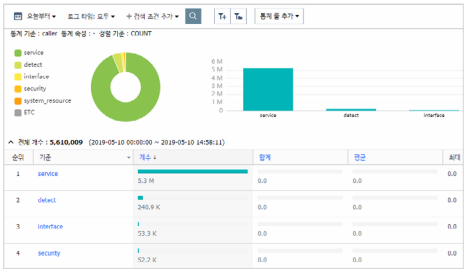
- YARA 엔진 및 시그니처(정적 분석)
- 악성파일 추출
- TMS 연계를 통한 정밀 분석

뛰어난 정보 가시성

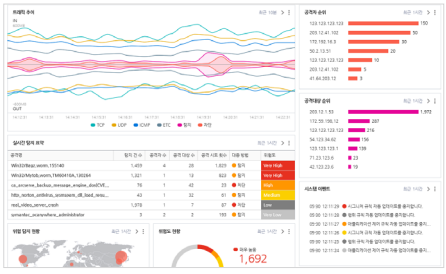
AhnLab AIPS는 사용자가 쉽고 빠르게 네트워크 상황을 인지하고, 위협에 대해 분석할 수 있도록 뛰어난 정보 가시성 기능들을 지원합니다. 사용자 정의 대시보드, 위젯을 통해 관리자가 원하는 정보만으로 대시보드를 구성할 수 있습니다. 위협 이벤트를 검색하고, 지속적인 통계와 분석이 필요한 경우, 사용자 정의 통계/분석 규칙을 생성합니다.



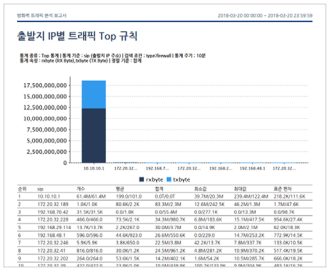
사용자 정의 통계/분석 규칙



사용자 정의 대시보드

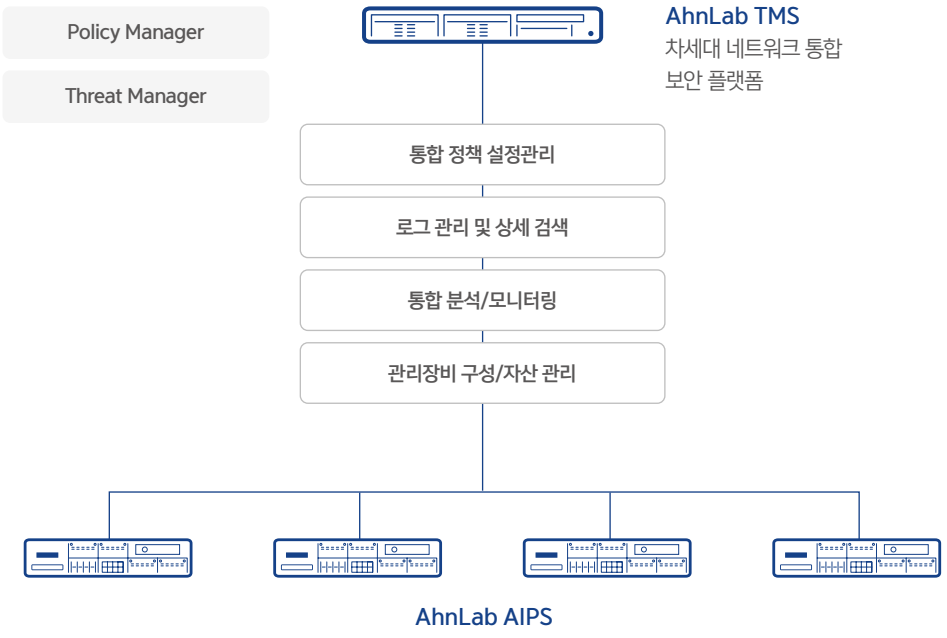


사용자 정의 보고서



더 강력한 통합 관리

다수의 보안 장비에 대한 간편한 정책 설정 및 통합 모니터링 환경을 제공하는 **차세대 네트워크 통합 보안 플랫폼인 AhnLab TMS**와의 연동을 통해 **효율적이고 직관적인 모니터링 및 극대화된 관리 편의성**을 경험할 수 있으며, TMS 연동된 안랩NW 제품들에 대해 머신러닝 기반으로 종합적인 위협 분석을 수행합니다. 또한, 공공 사이버 안전센터 연동을 통해 기관에서 배포하는 PCRE/YARA 정책의 배포가 가능합니다.



주요 기능

IPS
10,000개 이상의 시그니처 DB 제공
사용자 정의 시그니처
Security Zone 별 IPS 정책, 통계, 로그 및 모니터링
Snort 옵션 최대 지원
PCRE 정규표현식
PCRE 탐지 가속 기능
YARA(멀웨어 탐지)
과부하 시그니처 추출
정적 MAC 방어 기능
5tuple 기반 IP 제어
지역 국가별 IP 제어
비정상 프로토콜 차단(HTTP/DNS/SIP 등)
행위기반 탐지
5tuple 기반 세션 관리
트래픽 기반 자동 패턴 추출
카테고리 기반 URL 필터
악성 URL 기반 필터
DNS Query 기반 URL 필터
IP Fragmentation 공격 방지
TCP Segmentation 공격 방지
X-Forwarded-for 헤더 내 실제 IP 추출
SSL Inspection
클라우드 기반 C&C 서버 접속 탐지 및 차단
기능별 정책 예외 기능 지원
Application Control
1,600개 이상의 애플리케이션 제어
애플리케이션별 세부 제어
애플리케이션별 도움말 제공

공격 대응
패킷 탐지 및 차단
5tuple 기반 격리 기능
웹 차단 페이지 전송 기능
취약점 기반 공격 차단
네트워크 기반 공격 차단
악성코드 행위 제어
악성코드 유포지/경유지 차단
[TrusGuard 연동] 탐지 IP 블랙리스트 등록
Visibility
통합 대시보드
사용자 정의 대시보드 및 위젯
실시간 탐지/차단 모니터링
실시간 트래픽/세션 모니터링
다양한 로그/통계 정보
위협 상세 분석을 위한 유연한 Drill-Down
사용자 정의 통계 규칙
사용자 정의 보고서 생성
Network
방화벽 ACL
QoS
IPS 모드(Inline)
IDS 모드(Mirror/Span)
이중화 구성 및 HA Divert 기능
Infrastructure
클라우드 기반 보안 위협 수집/분석 시스템
MAPP Partnership
CDN 기반 안정적인 시그니처 업데이트
검증된 비상 대응체제/조직 보유

제품 사양 (Specification)

구분		AhnLab AIPS 2000B	AhnLab AIPS 5000B	AhnLab AIPS 10000B	AhnLab AIPS 20000
Max IPS Throughput (UDP)		20G	80G	120G	200G
CPU		8 Core, 3.5 Ghz	10 Core x 2, 2.4 Ghz	16 Core x 2, 2.9 Ghz	24 Core x 2, 3.0 Ghz
Memory		64GB	128GB	128GB	384GB
System Storage		SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB
Log Storage		HDD 2TB	HDD 2TB	HDD 2TB	SSD 1.92TB
NIC	1GC	10 (최대 34)	10 (최대 50)	10 (최대 50)	2 (최대 50)
	1GF	2 (최대 32)	4 (최대 24)	0 (최대 24)	0 (최대 24)
	10GF	0 (최대 2)	0 (최대 24)	4 (최대 24)	0 (최대 24)
	40GF	-	-	0 (최대 6)	0 (최대 6)
	100GF	-	-	-	2 (최대 4)
Power		Redundant	Redundant	Redundant	Redundant

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

인증 (Certification)

CC 인증(EAL4) GS 인증 IPv6 Ready Logo KC 인증

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901
© 2024 AhnLab, Inc. All rights reserved.

AhnLab