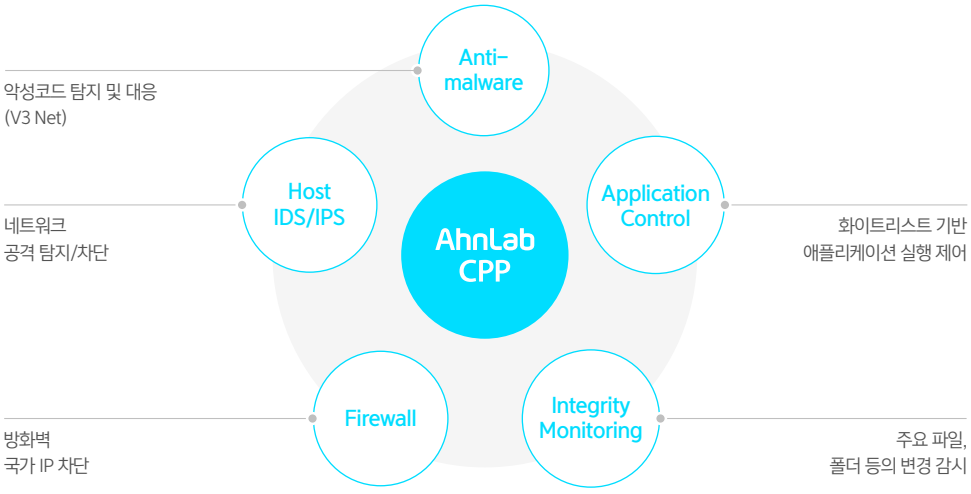
AhnLab CPP

하이브리드, 멀티 클라우드 환경을 위한 보안 플랫폼

클라우드 워크로드에 대한 가시성 제공
서버 워크로드 특성에 최적화된 보안 지원

제품 개요

AhnLab CPP(Cloud Protection Platform)는 클라우드 서버 워크로드 보호에 필요한 다양한 기능을 지원하는 보안 플랫폼입니다. 클라우드 계정 연동을 통해 오토스케일링되는 클라우드 서버 워크로드 자동 식별과 물리 및 가상 서버에 대한 통합 관리를 지원합니다. 안티멀웨어, IDS/IPS, 방화벽, 애플리케이션 제어, 무결성 검사 등 다양한 보안 기능을 제공하며, 이를 선별적으로 적용해 효율적인 서버 보안 체계 유지에 기여합니다. 서버 시스템과 함께 구동되는 컨테이너에서 악성코드와 네트워크 침입 공격을 탐지하며, 탐지된 이벤트 기반으로 다양한 대시보드와 함께 알림을 제공해 보안 위협에 대한 관리자의 신속한 대응을 지원합니다.



주요 기능

Anti-malware	· 다수 글로벌 인증 기관을 통해 검증된 V3를 통한 악성코드 대응 · 시그니처, 평판 기반의 강력한 악성코드 탐지 / 다양한 Windows, Linux 서버 지원
Application Control	· 애플리케이션 실행 제어를 통해 신뢰된 애플리케이션만 실행 허용 · 다양한 신뢰 조건 정의 지원 / 중요 파일 접근 제한 가능
Host IPS & Firewall	· 검증된 시그니처 기반의 공격을 탐지 및 차단함으로써 네트워크 침입공격 방어 · 시그니처 사용자 정의 지원 / 서버 취약점을 기반한 시그니처 추천(Recommendation) · 방화벽 및 국가(IP 기반) 차단 지원
Integrity Monitoring	· 중요 파일, 폴더, 레지스트리, 프로세스, 사용자, 그룹, 서비스 등에 대한 변경 모니터링 · 실시간 / 수동 / 예약 검사 지원

Application Control

AhnLab Application Control은 특정 애플리케이션만 구동되는 서버 워크로드를 보호하는데 최적화된 **서버 워크로드 애플리케이션 제어 솔루션**입니다. 신뢰된 애플리케이션에 대한 실행만 허용하고 그 외 애플리케이션은 실행을 차단해 워크로드 용도에 불필요한 프로그램 실행은 사전에 차단하고 보다 안정적인 서비스 운영을 지원합니다. 또한 유지보수 모드, 시뮬레이션 모드 등의 다양한 운영 모드 지원을 통해서도 서비스의 안정적인 운영에 기여합니다. 또한 일반적으로 변경이 없어야 하는 특정 파일/폴더, 레지스트리, 시작 프로그램, 서비스 등에서 변경이 있는지 감시하여, 서버로의 공격이나 위험을 사전에 탐지할 수 있도록 합니다.

클라우드 서버 환경에 최적화된 보안 솔루션

- 사전에 만들어진 이미지 기반으로 운영되는 클라우드 워크로드 환경에서의 최적화된 보안 지원
- 신뢰하는 애플리케이션만 실행 허용함으로써 안정적인 서비스 운영 지원

관리자 업무 부담 최소화

- 관리자가 지정한 신뢰 기준(서명자, 공급자, 클라우드 평판 분석 결과)에 따른 실행을 허용해 보다 유연한 관리 지원

서버 가용성 고려한 다양한 기능 제공

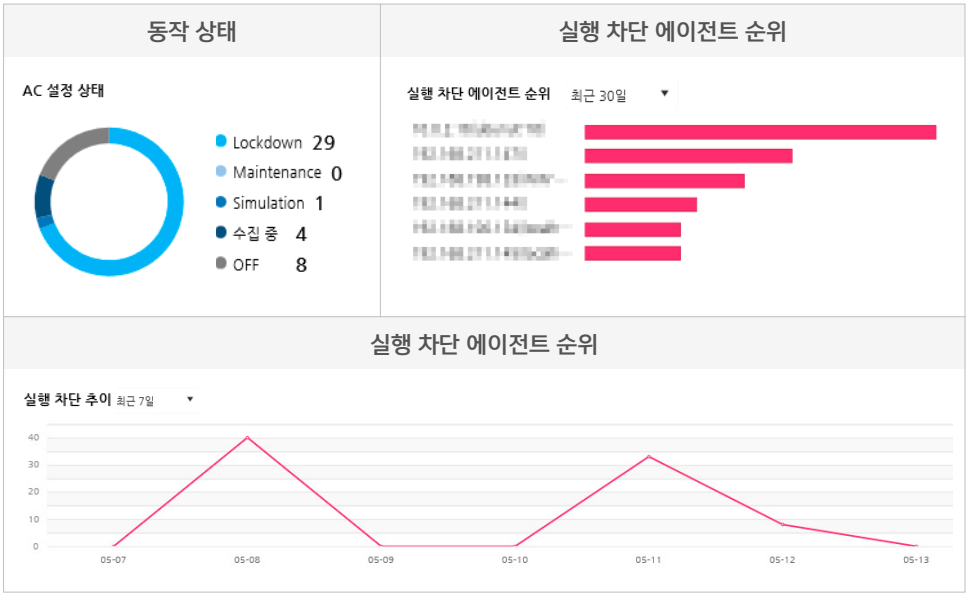
- 서비스 원활한 운영을 최우선시 하여 다양한 운영 모드 지원
  - 보안 운영 모드
  - 업데이트를 고려한 유지보수 모드
  - 차단 없이 탐지만 지원, 정책 적절성을 판단할 수 있는 시뮬레이션 모드
- 과도한 탐지 단말에 대한 알림 및 인벤토리 초기화 지원(연계규칙 활용)

다양한 대시보드를 통해 세분화된 가시성 제공

- 실행차단 추이, 실행 차단 에이전트 순위, 파일 순위 등 주요 이벤트에 대한 직관적인 가시성 제공

무결성 모니터링

- 중요 파일, 폴더, 레지스트리, 서비스, 프로세스, 포트, 사용자, 그룹, 시작프로그램 등에 대한 변경 감시
- 기본 룰과 함께 사용자 룰 정의 지원



AhnLab CPP 대시보드(Application Control)

Host IPS

AhnLab Host IPS는 시스템으로 들어오거나 나가는 트래픽을 분석해 의심스러운 패턴의 트래픽을 시그니처 기반으로 탐지 및 차단하는 **호스트 기반 침입 방지 솔루션**입니다. 운영체제, 웹, 애플리케이션 취약점에 기반한 공격은 물론 다양한 유형의 네트워크 기반 공격 위협으로부터 서버를 안전하게 보호합니다. 또한 서버 워크로드가 가진 알려진 취약점 정보를 기반으로 시그니처를 추천해 워크로드 특성에 최적화된 시그니처 적용을 지원합니다. 시스템으로의 네트워크 공격 뿐만 아니라, 구동중인 컨테이너로의 네트워크 공격을 탐지, 식별을 지원합니다.

검증된 시그니처 제공

- 안랩이 보유한 보안 위협 분석 조직 및 인프라를 기반으로 국내 환경에 최적화된 시그니처 제공

고객사 서버 환경에 최적화된 시그니처 적용

- 서버가 보유한 취약점에 매핑되는 시그니처 추천(Recommendation)
- 시그니처에 대한 사용자 정의 지원으로 고객이 필요한 시그니처 직접 설정 및 적용 지원
- 사용자 정의 시 Snort, PCRE 지원으로 설정 용이성 제공

방화벽

- IP, Port, 프로토콜 기반 차단/허용 지원(XFF지원)
- 특정 국가 IP 에 대한 인/아웃바운드 차단 지원

서버 가용성을 고려한 다양한 기능 제공

- Inline 모드 외에도 Tap 모드, Bypass 모드와 같은 다양한 네트워크 엔진 모드 제공
- IDS 모드 지원 및 긴급 OFF 지원
- 특정 조건의 탐지 단말에 대한 알림 지원(연계규칙 활용)
- 지정한 CPU 임계치 초과 시 기능 OFF 지원

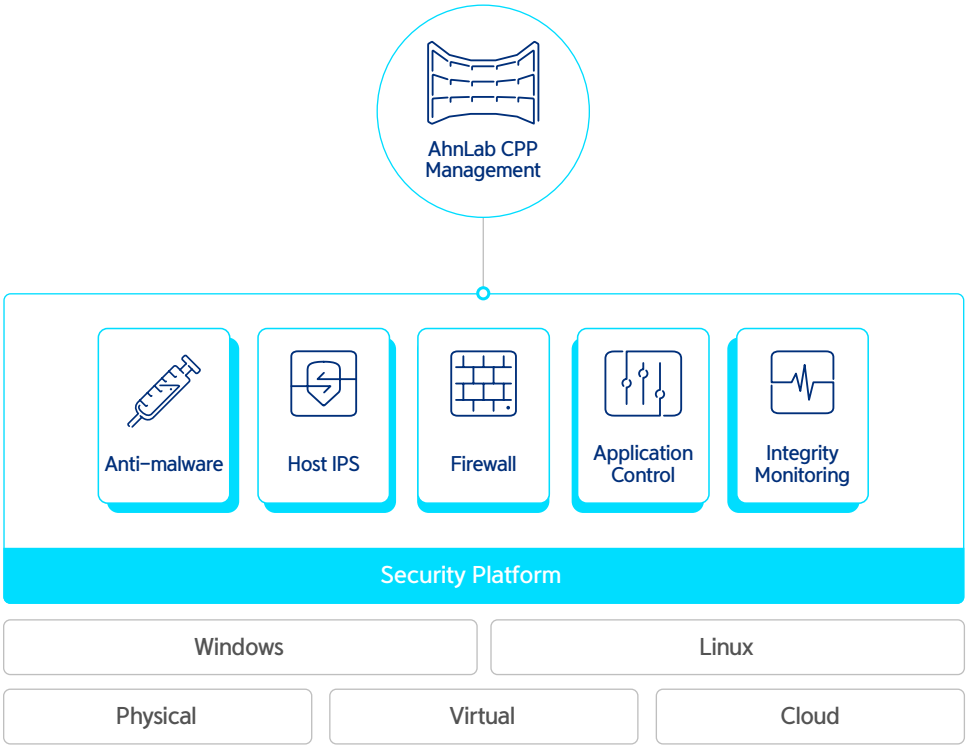
위협 가시성과 함께 대응 용이성 제공

- 탐지 에이전트, 공격자, 시그니처 Top, 공격 추이 등 다양한 대시보드 제공
- 탐지 트래픽에 대한 상세 정보 제공
- 탐지 이벤트에서 예외 IP 설정 지원
- 특정 시그니처에 대한 전체시스템 적용 지원

AhnLab CPP 대시보드(Host IPS)

최적화된 보안 운영 및 관리

AhnLab CPP는 다양한 보안 기능을 **단일 에이전트(One Agent)**를 기반으로 통합 운영 및 관리를 제공해 하이브리드 클라우드 서버 워크로드 보호에 최적화된 보안 플랫폼을 구축할 수 있도록 지원합니다.



AhnLab CPP 기반 솔루션 연계 범위

특장점

효율적인 서버 통합 보안 관리	· 클라우드(AWS, Azure, NHN, NCP 등)와 함께 물리/가상 환경에서 운영되는 서버에 대한 통합 관리 지원 · 단일 에이전트(One Agent)로 안랩 서버 보안 솔루션에 대한 통합 운영 및 관리 제공
서버 워크로드에 최적화된 위협 관리 및 대응	· 다양한 대시보드를 통해 보안 위협에 대한 모니터링 및 가시성 제공 · 안랩 서버 보안 솔루션 간 연계 규칙 제공을 통해 조직에 최적화된 위협 대응 체계 지원 · Syslog, 오픈 API 제공을 통해 서드 파티 솔루션(SIEM, 통합로그분석시스템 등)과의 쉽고 간편한 연동 지원
유연한 구성과 함께 비용 절감 효과	· 모듈화된 서버 구성 지원으로 고객사 환경에 맞춘 유연한 구성 및 확장 가능 · 업무 특성에 필요한 보안 솔루션 라이선스만 적용함으로써 보안 솔루션 도입 및 관리 비용 효율성 향상

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

AhnLab