AhnLab CLOUD PLUS

AhnLab CPP

하이브리드 & 멀티 클라우드 환경을 위한 보안 플랫폼

다양한 형태의 클라우드 워크로드에 대한 최적화된 보안 적용
쿠버네티스 기반 컨테이너 식별 및 이미지 보안 검사
단일 에이전트 기반 통합 운영 및 관리 지원

제품 개요

AhnLab CPP(Cloud Protection Platform)는 물리 서버, 가상 서버, 클라우드 VM, 쿠버네티스(Kubernetes) 클러스터, 서버리스 컨테이너 등 다양한 형태의 클라우드 인프라에서 운영되는 워크로드를 통합적으로 보호하는 클라우드 워크로드 보안 플랫폼 (Cloud Workload Protection Platform, CWPP) 입니다. AhnLab CPP는 호스트 보호부터 실행 중인 컨테이너 식별 및 이미지 검사까지 하나의 매니지먼트에서 운영하여 클라우드 워크로드에 대한 단일 보안 관리 역량을 제공합니다.

주요 기능

Anti-malware	· 물리/가상 서버 및 클라우드 VM에 설치되어 윈도우와 리눅스 환경에서 실시간, 예약, 수동 검사 지원 · 독보적인 기술력을 갖춘 엔진으로 신속 정확한 악성코드 진단/치료 및 다중 압축 파일 검사 지원 · 쿠버네티스 환경에서는 DaemonSet 방식으로 배포되어 컨테이너 워크로드와 노드를 동시에 보호
Host IPS & Firewall	· 호스트(물리 서버/가상 서버/VM 인스턴스), 쿠버네티스 및 서버리스 환경에 최적화된 보안 · 시그니처 기반 네트워크 위협 탐지 및 차단과 사용자 정의 룰 지원 · Inline, Tap, Bypass 등 유연한 운영 모드 제공 · 방화벽: IP, 포트 및 프로토콜 제어와 Geo-IP 차단 · 포트 스캔 및 호스트 스윕을 통한 의심스러운 행위 탐지
Application Control & Integrity Monitoring	· 애플리케이션 실행 제어를 통해 신뢰된 애플리케이션만 실행 허용 · 다양한 신뢰 조건 정의 지원 / 중요 파일 접근 제한 가능 · 중요 파일, 폴더, 레지스트리, 프로세스, 사용자, 그룹, 서비스 등에 대한 변경 모니터링 · 실시간 / 수동 / 예약 검사 지원
Container Security	· Kubernetes 클러스터 연동, 토폴로지 가시화 · 동작 중인 컨테이너 식별하여 이미지 Pull 및 검사 · 검사된 이미지에 대한 클러스터, 네임스페이스, 파드 배포 현황 다이어그램

Host IPS

Host IPS는 시스템으로 들어오거나 나가는 트래픽을 분석해 의심스러운 패턴의 트래픽을 시그니처 기반으로 탐지 및 차단하는 호스트 기반 침입 방지 모듈입니다. 운영체제, 웹, 애플리케이션 취약점 기반 공격은 물론 다양한 유형의 네트워크 기반 공격으로부터 서버를 안전하게 보호합니다. 또한, 서버 워크로드의 알려진 취약점 정보를 바탕으로 시그니처를 추천해 워크로드 특성에 최적화된 시그니처를 적용할 수 있도록 합니다. 시스템으로의 네트워크 공격 뿐만 아니라, 구동 중인 컨테이너로의 네트워크 공격을 탐지 및 식별합니다.

검증된 시그니처 제공
· 안랩이 보유한 위협 분석 조직 및 인프라를 기반으로 국내 환경에 최적화된 시그니처 제공

서버 환경에 최적화된 시그니처 적용
· 서버의 취약점에 매핑되는 시그니처 추천
· 시그니처 사용자 정의 지원으로 고객이 필요한 시그니처 직접 설정 및 적용 지원
· 사용자 정의 시, Snort와 PCRE를 지원해 설정 용이성 제공

방화벽
· IP, Port, 프로토콜 기반 차단 및 허용 (XFF 지원)
· 특정 국가 IP 에 대한 인/아웃바운드 차단

서버 가용성을 고려한 다양한 기능 제공
· Inline 모드 외에도 Tap, Bypass 모드 등 다양한 네트워크 엔진 모드 제공
· IDS 모드 및 긴급 OFF 지원
· 특정 조건의 탐지 단말에 대한 알림 지원 (연계 규칙 활용)
· 지정한 CPU 임계치 초과 시 기능 OFF 지원

위협 가시성과 대응 용이성
· 대시보드를 통해 탐지 에이전트, 공격자, Top 시그니처, 공격 추이 등 폭 넓은 현황 확인
· 탐지 트래픽에 대한 상세 정보 제공
· 탐지 이벤트에서 예외 IP 설정
· 특정 시그니처에 대한 전체 시스템 적용

Application Control

Application Control은 특정 애플리케이션만 구동되는 서버 워크로드를 보호하는데 최적화된 서버 워크로드 애플리케이션 제어 모듈입니다. 신뢰된 애플리케이션 실행만 허용하고 워크로드 용도에 불필요한 프로그램 실행은 사전에 차단하여 보다 안정적인 서비스 운영을 지원합니다. 또한 유지보수 모드, 시뮬레이션 모드 등 다양한 운영 모드를 지원해 서비스 안정성을 더합니다. 일반적으로 변경이 없어야 하는 특정 파일, 폴더, 레지스트리, 시작 프로그램, 서비스 등에 변경이 있는지 감시하여, 서버로의 공격이나 위험을 사전에 탐지합니다.

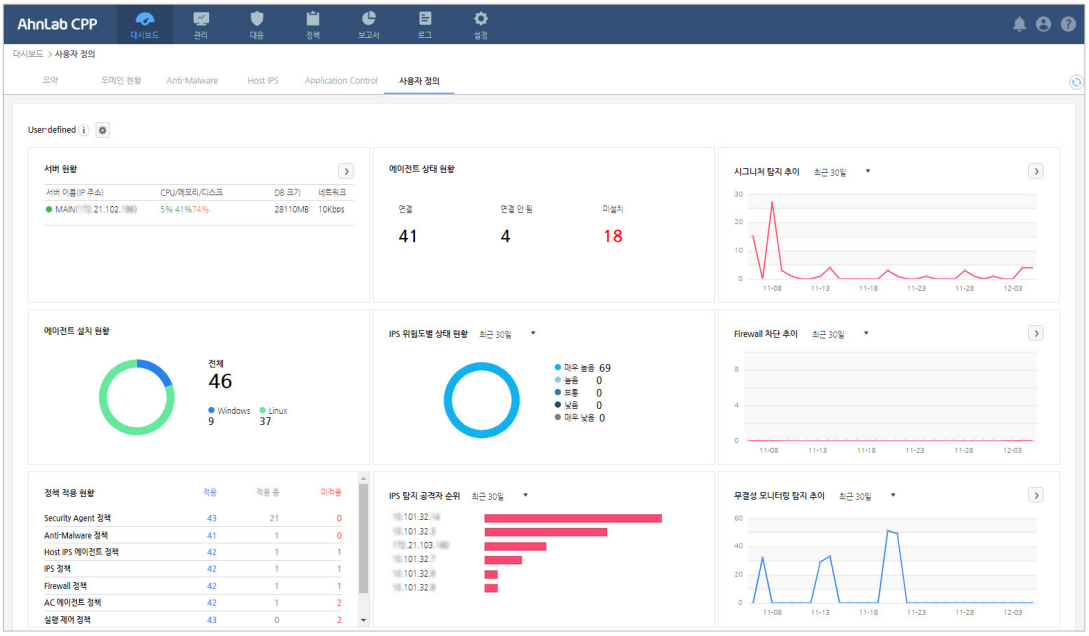
클라우드 서버 환경에 최적화
· 사전에 만들어진 이미지를 기반으로 운영되는 클라우드 워크로드에 대한 최적화된 보안 지원
· 신뢰하는 애플리케이션 실행만 허용하여, 안정적인 서비스 운영 지원 관리자 업무 부담 최소화

관리자 업무 부담 최소화
· 관리자 지정 신뢰 기준(서명자, 공급자, 클라우드 평판)을 기반으로 실행을 허용해 유연한 관리 지원
서버 가용성을 고려한 다양한 기능

서버 가용성을 고려한 다양한 기능
· 원활한 서비스 운영을 우선순위에 둔 다양한 운영 모드 지원
#1. 보안 운영 모드
#2. 유지보수 모두 (업데이트 고려)
#3. 시뮬레이션 모드 (차단 없이 탐지만 지원 - 정책 적절성 판단)
· 탐지량이 많은 단말 알림 및 인벤토리 초기화 지원 (연계 규칙 활용)

다양한 대시보드를 통해 세분화된 가시성 제공
· 실행 차단 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
· 쿠버네티스 환경에서는 daemonset으로 배포되어 컨테이너 워크로드와 노드 동시 보호



AhnLab CPP 대시보드

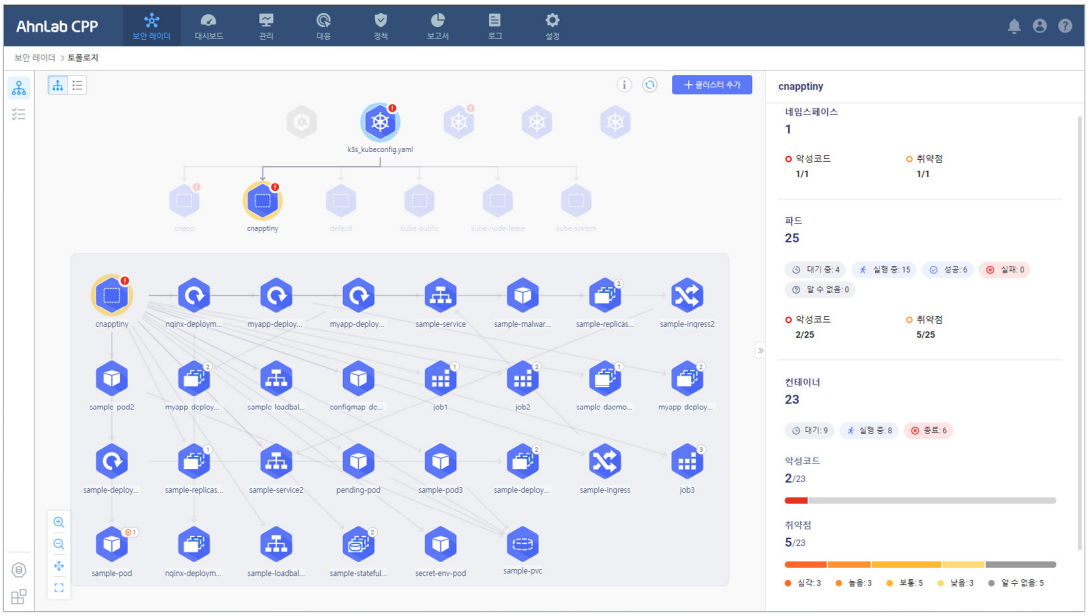
Container Security

Container Security는 Kubernetes 환경에서 실행 중인 컨테이너를 식별하여 토폴로지 가시화를 제공하고, 식별된 컨테이너 이미지의 악성코드 및 취약점 검사를 수행하는 컨테이너 보안 모듈입니다. 기업의 컨테이너 환경 보안을 강화하고, 잠재적인 위협을 신속하게 식별하여 대응할 수 있도록 합니다.

간편한 Kubernetes 클러스터 및 컨테이너 레지스트리 연동
· kubeconfig 및 계정 연동 방식으로 Kubernetes 클러스터 연동
· Harbor, Nexus, Docker Hub, Amazon ECR 등 다양한 컨테이너 레지스트리 연동

Kubernetes 토폴로지 가시화:
· 클러스터, 네임스페이스, 파드 정보를 토폴로지로 시각화해 리소스 구성 및 보안 상태를 한 눈에 확인

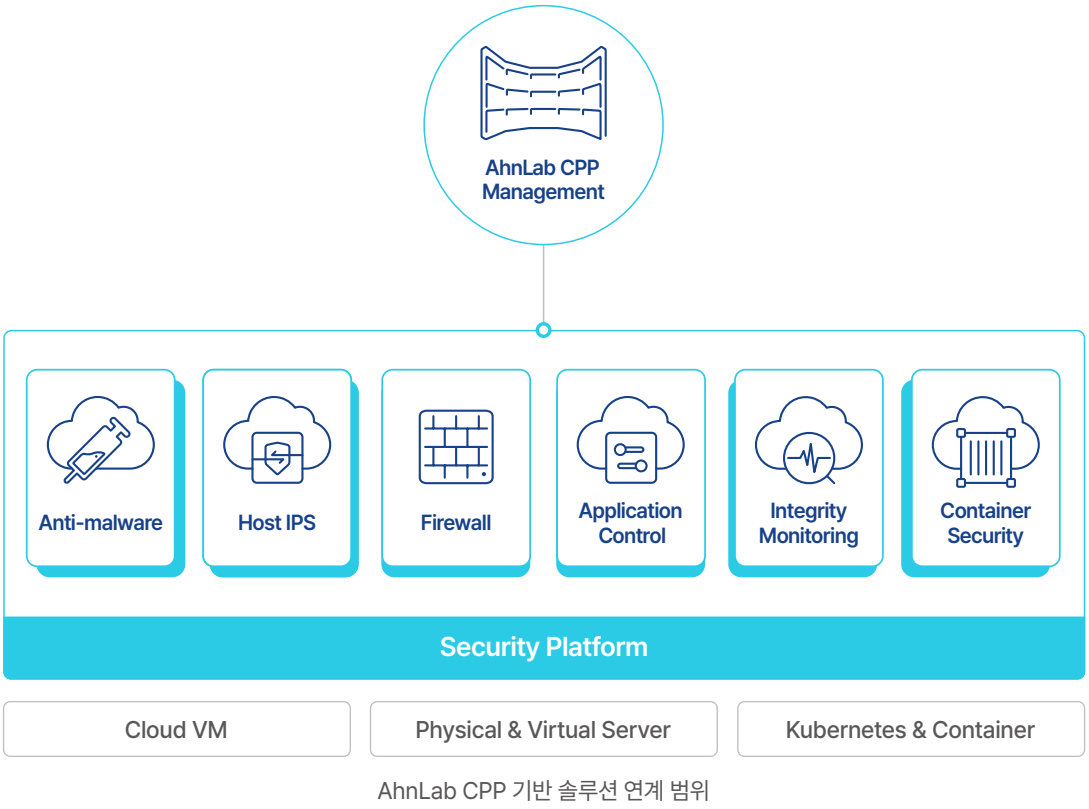
동작 중인 컨테이너 식별 및 검사:
· Kubernetes 환경에서 실행 중인 컨테이너를 식별하고, 해당 컨테이너 이미지 악성코드 및 취약점 검사
· 배포에 사용된 이미지가 연동된 컨테이너 레지스트리에 존재하지 않는 경우, 상태 정보 제공
· 검사된 이미지에 대한 배포 현황 다이어그램 및 목록 제공



AhnLab CPP 보안 레이어

최적화된 보안 운영 및 관리

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



AhnLab CPP 기반 솔루션 연계 범위

특장점

효율적인 서버 보안 통합 관리	· 퍼블릭 클라우드(AWS, Azure, NHN, NCP 등)와 물리/가상 환경 서버 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 위협에 대한 모니터링 및 가시성 제공 · 안랩 서버 보안 솔루션 간 연계 규칙을 제공해 조직에 최적화된 위협 대응 체계 확립 · Syslog, 오픈 API를 제공해 서드 파티 솔루션(SIEM, 통합로그분석시스템 등)과 편리한 연동
유연한 구성과 비용 절감	· Host IPS, Application Control, V3 Net, Container Security 등 다양한 기능을 단일 매니지먼트로 통합 운영하여 고객의 필요에 맞춰 효율적 관리 가능 · 업무 특성에 필요한 보안 솔루션 라이선스만 적용하여 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