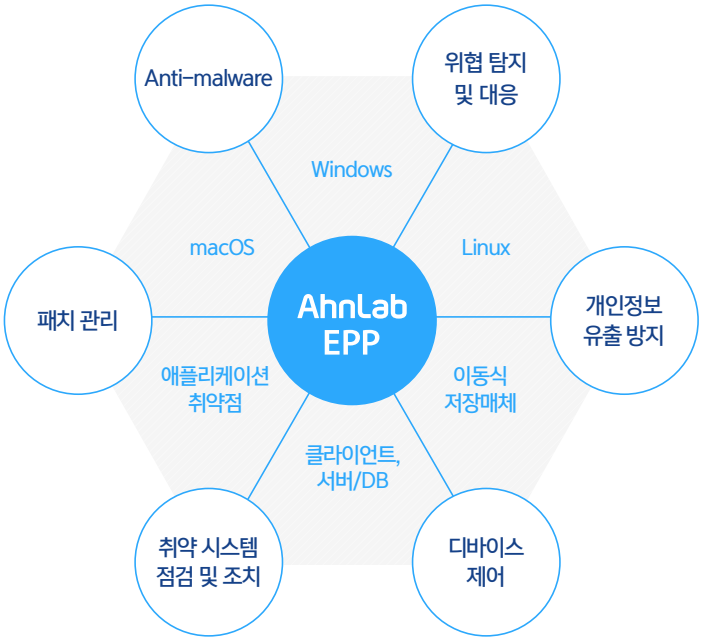
AhnLab EPP

차세대 엔드포인트 통합 보안 플랫폼

단일 에이전트, 단일 관리 콘솔의 편리한 통합 관리
연계 정책 및 대응을 통한 강력한 위협 대응

제품 개요

AhnLab EPP는 위협 관리 및 대응 관점의 **차세대 엔드포인트 보안 플랫폼(Endpoint Protection Platform)**입니다. 단일 에이전트, 단일 관리 콘솔을 기반으로 복잡다단한 엔드포인트 환경을 효율적으로 관리하고 고도화되는 보안 위협에 더욱 효과적으로 대응할 수 있습니다.

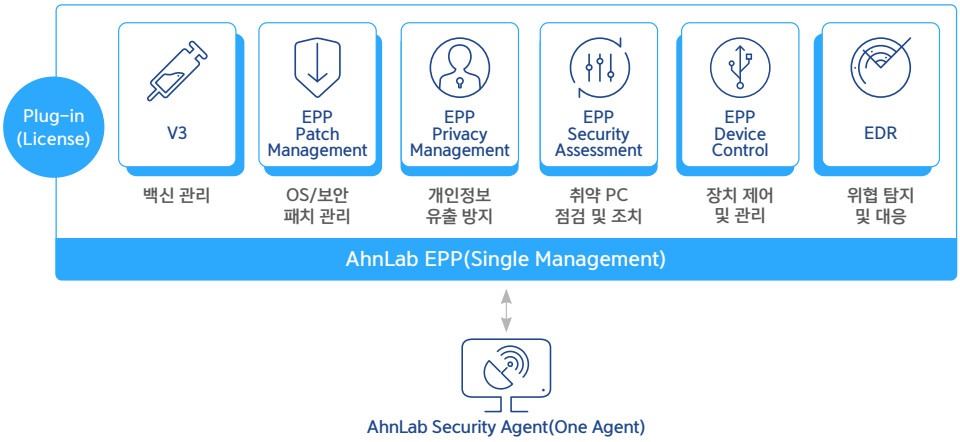


특장점

편리한 운영	· 단일 관리 콘솔(Single Management Console)을 통한 보안 운영 일원화/효율화 · 웹(Web) 기반의 관리 콘솔 및 다양한 관리 기능을 통한 운영 편의성
최적화된 위협 대응 · 관리	· 백신(V3)부터 EDR까지, 다양한 보안 솔루션 연계를 통한 위협 모니터링 및 대응 · 제3자 솔루션과의 Syslog 연동으로 보안 관제 효과 극대화
유연한 확장성 및 운영 안정성	· 소프트웨어 방식의 유연한 구축 및 확장 · 병렬 구조(Scale-out) 방식의 간편한 서버 추가 · 확장

차별적인 보안 체계

AhnLab EPP의 **단일 에이전트(One Agent), 단일 관리 콘솔(Single Management Console)**을 기반으로 백신과 패치 관리, 개인정보 유출 방지, 보안 취약 시스템(PC) 점검 및 조치, 장치 제어 · 관리를 비롯해 엔드포인트 위협 탐지 · 대응(Endpoint Detection & Response) 솔루션까지 쉽고 간편하게 통합 관리 및 운영할 수 있습니다.



다수의 보안 솔루션 운영을 단일 에이전트, 단일 관리 콘솔로 더욱 간편하게!

V3 제품군

최고의 안티멀웨어(Anti-malware, 백신) 솔루션
- 다수의 글로벌 인증 기관을 통해 검증된 세계 최고 수준의 악성코드 대응 성능
- 다차원 분석 플랫폼 기반의 강력한 악성코드 탐지
- 다양한 운영체제(Multi OS) 기반의 PC 및 서버 보안
  - PC용: V3 Internet Security 9.0, V3 Endpoint Security 9.0(매체관리 기능 제공), V3 for Mac, V3 Desktop for Linux
  - 서버용: V3 Net for Windows Server, V3 Net for Unix/Linux Server

EPP Patch Management

독보적인 패치 관리 솔루션
- 자체 패치랩을 통해 검증한 안전한 패치 제공
- 자동화된 패치 관리로 보안 사고 방지
- 다양한 패치 관리 정책 설정 가능

EPP Privacy Management

개인정보 유출 의심 파일 탐지 · 차단 솔루션
- 엔드포인트의 다양한 경로를 통한 개인정보 유출 의심 파일 탐지 및 조치
- 뉴런 검색 기술로 탐지 정확성 및 사용자 편의 극대화
- 문서 변환 기술로 다양한 문서 파일 내의 개인정보 검출

EPP Security Assessment

취약 시스템(PC) 점검 및 조치 솔루션
- 동종 제품 중 최대 수준의 점검 항목 제공
- 관리자 정의 점검 기능을 통해 점검 항목 추가 가능
- 편리한 자동 조치 기능으로 사용자(End User) 편의 극대화

EPP Device Control

장치 제어 및 통합 관리 솔루션
- 외부 주요 장치 접근 차단 및 보조 저장 매체에 대한 파일 반출 제어
- 고객사 업무 환경에 따른 장치 제어 시간대 및 장치별 예외 기간 설정
- 장치 제어 현황 모니터링 및 제어 로깅을 통한 이력 관리

EDR

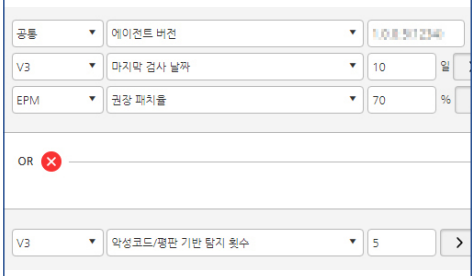
엔드포인트 위협 탐지 · 대응 솔루션
- 최고의 엔드포인트 보안 기업의 차세대 엔드포인트 위협 탐지 · 대응 솔루션
- 행위 분석 엔진을 기반으로 엔드포인트의 모든 행위 정보 수집 및 분석
- 지속적인 모니터링 및 엔드포인트 위협 가시성 제공

강력한 위협 대응

AhnLab EPP를 통해 다수의 엔드포인트 보안 솔루션간의 규칙 및 대응 조치를 유기적으로 연계 및 설정함으로써 보안 위협에 더욱 강력하게 대응합니다. 보안 담당자의 필요에 따라 다양한 보안 정책을 적용할 수 있어 고객 주도적이며 능동적인 보안 운영이 가능합니다.

- 연계 규칙 설정: 개별 제품의 조건을 and/or 규칙으로 연계하여 정책 설정 가능
- 연계 대응 설정: 연계 규칙을 위반한 시스템에 대해 개별 또는 공통 대응 정책 설정 가능

연계 규칙 설정 예시



▲특정한 버전의 모든 에이전트 중
▲일정 기간 동안 V3로 검사하지 않았고(and)
▲패치율이 70% 미만이거나(or)
▲V3의 악성코드 탐지 횟수가 일정 기간 동안 일정 횟수를 초과한 시스템 탐지

연계 대응 설정 예시

연계 규칙을 위반한 시스템에 대해
▲공지사항(alert)을 보내고
▲V3로 검사를 진행하며
▲패치 정책에 따라 소프트웨어를 설치하고
▲EDR을 통해 특정 해시 값을 갖는 파일이 존재하는지 확인

최적화된 보안 운영

AhnLab EPP의 다양하고 편리한 기능을 이용해 기업 및 기관의 비즈니스 환경 및 보안 요구에 따라 최적화된 보안 운영 체계를 구축할 수 있습니다.

자동화된 Syslog 연동

- 다양한 타 솔루션과 원활한 연동 가능 – SIEM, ESM, 통합 로그 등
- Syslog UDP 및 TCP, TCP over SSL 동시 지원 – 보안 관리자가 선택적으로 연동 정보 지정 가능
- AhnLab EDR 등 다수의 안랩 솔루션과 제3자 솔루션의 연계를 통해 풍부한 위협 인텔리전스 확보 가능

엔드포인트 위협 정보 자동 수집

- 엔드포인트의 의심 단말 분석
- 에이전트를 통한 위협 정보 자동 수집(AhnReport 자동 수집 및 뷰어)
- 안랩의 전문가 서비스(AhnLab Professional Service)를 통한 추가 분석 및 대응 연계 가능
  – 상세 분석 보고서, 대응 가이드 제공 가능

유연한 확장성 및 운영 안정성

- 고객사 규모 · 환경에 따른 다양한 시스템 구축 방식 지원
- 모듈별 구성 방식을 통한 다양한 구축 및 유연한 확장
- 로드밸런서(Load Balancer, Active-Active) 기반의 성능 과부하 방지 및 분산을 통한 운영 안정성

관리
편의성 강화

AhnLab EPP는 편리한 보안 솔루션 운영을 위해 웹 기반의 관리 콘솔과 다양한 관리 메뉴를 제공합니다. 동적 UX 기반의 직관적인 대시보드를 통해 한눈에 파악할 수 있는 엔드포인트 위협 가시성을 제공함으로써 보안 관리자의 효율적인 보안 관리 및 즉각적인 위협 대응에 기여합니다.

▲ AhnLab EPP 대시보드

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