AhnLab EPS

More security,
More freedom

다양한 특수목적시스템에 최적화된 보안 통제

표준제안서

AhnLab

CONTENTS

AhnLab

01
제안 배경

1. 공격 대상의 다변화
2. 산업 시설·사회 기반 시설 공격 증가
3. 특수목적시스템 겨냥한 공격 증가
4. 특수목적시스템 운영 환경의 특수성
5. 특수목적시스템의 보안 요구 사항

공격 대상의 다변화

일반 IT 시스템뿐만 아니라 산업 제어 시스템, 사회 기반 시설 운영을 위한 OT(Operational Technology) 시스템도 악성코드 등 사이버 공격의 타깃이 되고 있습니다.

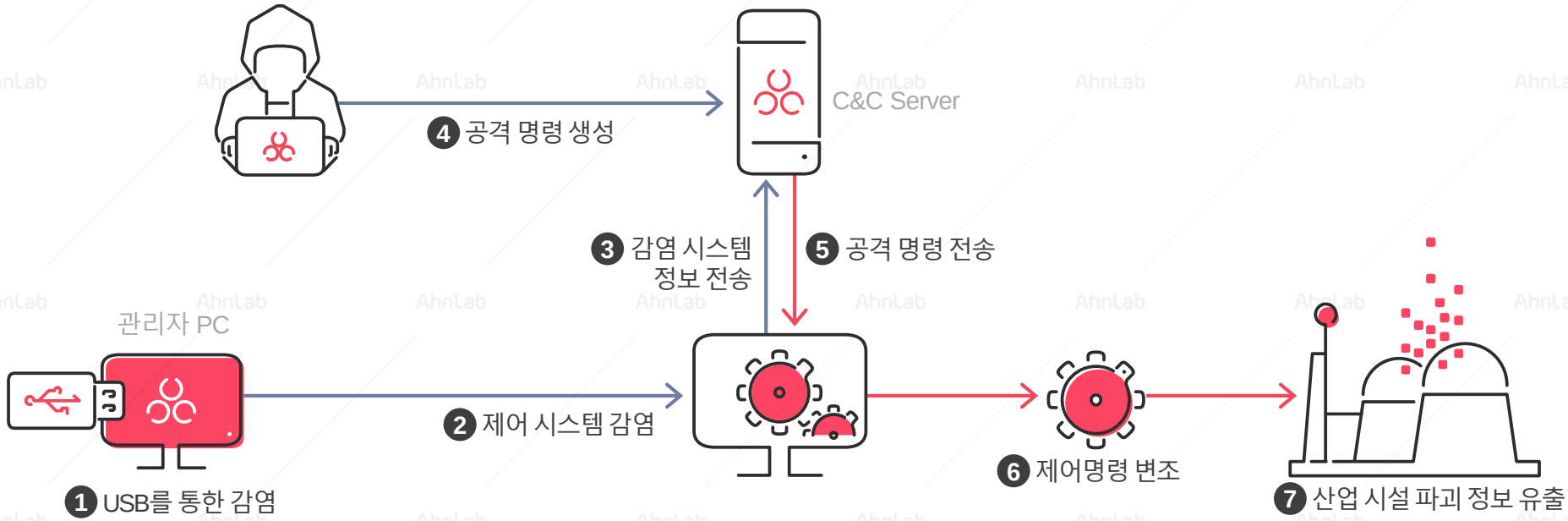
산업 제어 시스템 타깃형 악성코드

- 스턱스넷(Stuxnet) - 이란, 중국
- 미니플레임(miniFlame) - 서아시아

사회 기반 시설 해킹

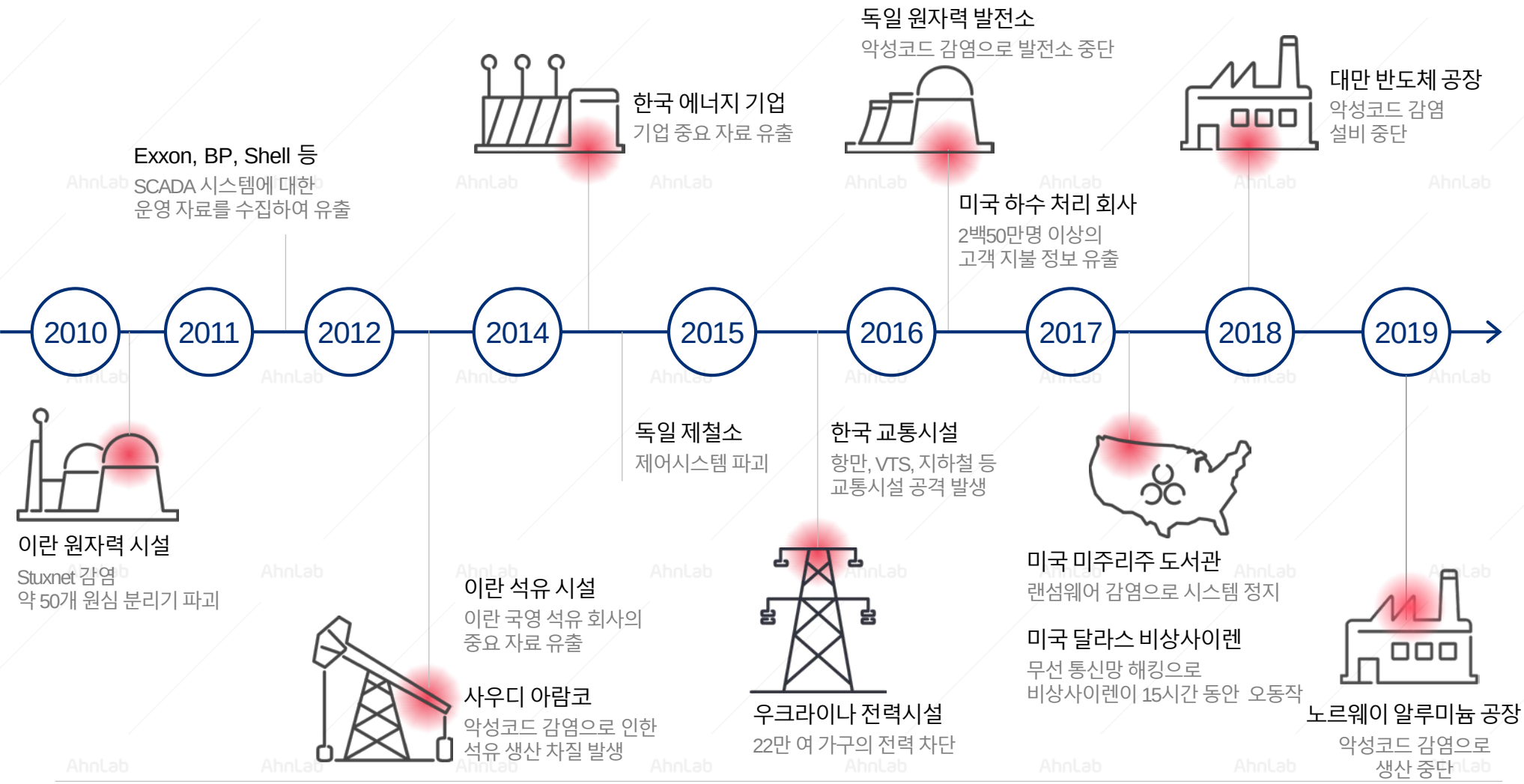
- 미국 뉴욕 댐 보안 침해 (2010)
- 우크라이나 발전소 해킹 및 정전 (2015)

스턱스넷 공격 개요



산업 시설·사회 기반 시설 공격 증가

산업 시설, 사회 기반 시설의 보안 침해 사고는 운영 중단에 따른 금전적인 손실뿐만 아니라 사회적 혼란을 야기할 수 있습니다.



특수목적시스템 겨냥한 공격 증가

POS(Point-of-Sale) 시스템 등 특수목적시스템을 노린 악성코드가 지속적으로 증가하면서 보안 침해에 따른 막대한 피해가 발생하고 있습니다.

- **POS 타깃형 악성코드의 급격한 증가** - Tracker, Dexter(BlackPOS), Mmon, Yorasa, Jackpos, Ompos, Brutepos, Backoff 등
- **POS 단말기 감염·해킹으로 대규모 고객 정보 유출 사고 발생** - 유출된 신용카드 정보의 암시장 판매 또는 복제 카드 등 2차 피해 발생

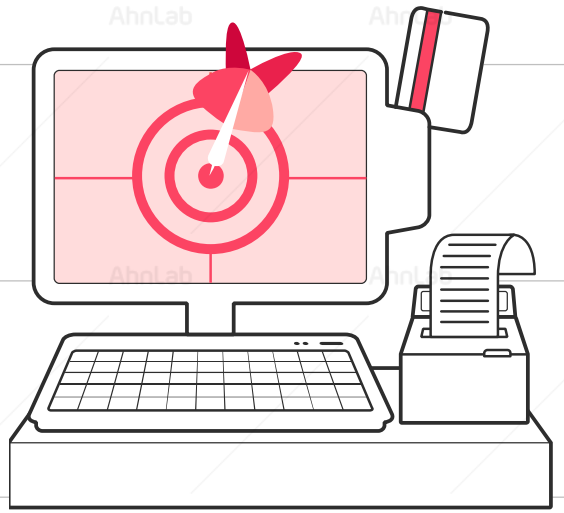
POS 시스템 보안 침해 사례 및 피해 규모

국내

커피전문점 및 음식점 2013
- 전국 85개 업체 POS 단말기 해킹
- 신용카드 정보 20만 5,000건 유출
- 복제 카드로 1억 2,000여 만원 인출

세탁 프렌차이즈 업체 2017
- POS 단말기 900여 대 악성코드 감염
- 신용카드 정보 탈취 시도

10만대 시스템 중단 2018
- 서비스거부(DOS) 공격으로 시스템 마비
- 원격 제어 악성코드, 채굴 악성코드
- 윈도우XP 취약점을 통한 감염



해외

Target 2013
- 미국 대형 소매업체 POS 단말기 감염
- 신용카드 정보 7천만 건 유출
- 약 2천만 달러의 피해 보상금 지불

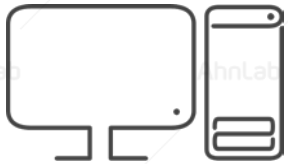
Home Depot 2014
- 생활용품 업체 홈디포 POS 단말기 감염
- 신용카드 정보 5천 6백만 건 유출
- 약 6천2백만 달러의 피해 보상금 지불

Saks Fifth Avenue 2018
- 미국 유명 백화점 POS 단말기 감염
- 신용카드 정보 500만 건 유출
- 피싱 메일을 통한 악성코드 감염

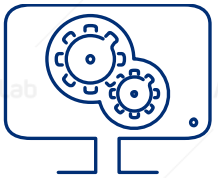
특수목적시스템 운영 환경의 특수성

생산 설비 시설, POS 시스템 등 특수목적시스템은 일반적인 IT 환경과 달리 운영 연속성, 시스템 가용성에 대한 민감도가 높기 때문에 일반적인 보안 체계를 적용할 수 없습니다.

일반 PC vs 특수목적시스템



VS



일반 PC		특수목적시스템
높은 시스템 자원	Environments 운영 환경	**제한된 시스템 자원**(저사양 장비)
불특정 다수의 애플리케이션 사용		**제한된 애플리케이션 사용**
인터넷 접근 용이		**인터넷 접근 제한**
사용 편의성 우선	Requirements 요구 사항	**가용성 우선**(다운타임 최소화)
주기적인 보안제품/엔진 업데이트		**엔진 업데이트 최소화**
1:1 관리		**1: N 관리**

특수목적시스템의 보안 요구 사항

특수목적시스템은 운영 환경의 특징을 고려한 보안 요구사항에 효과적으로 대응할 수 있는 전용 보안 솔루션이 필요합니다.

강력한 악성코드 대응

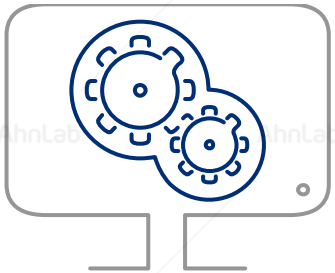
보안 사고 및 장애로 인한 가동 중단이 없어야 한다

- 시스템 및 네트워크 다운타임 최소화
- 악성코드로 인한 시스템 및 네트워크 장애 최소화

응용 프로그램 제어 네트워크 차단

정해진 프로그램만 사용할 수 있도록 하고 싶다

- 불필요한 프로그램의 실행 제어를 통한 시스템 안정성 유지
- 특정한 포트 이외에는 모두 차단하여 효율성 및 보안성 향상



초경량 보안 솔루션

보안 솔루션의 시스템 리소스 영향이 적어야 한다

- CPU, 메모리, 하드디스크 등 시스템 사양이 낮은 장비에서도 동작하는 보안 솔루션 필요
- 구 버전 OS, 보안 지원이 중단된 OS에서도 동작하는 보안 솔루션 필요

통합 관리

전체 시스템의 현재 상황을 한눈에 파악하고 싶다

- 이상 현상을 보이는 시스템에 대한 신속한 확인 필요
- 문제가 있는 시스템에 대한 빠른 조치
- 모든 제어용 시스템의 보안 로그 통합 관리

02
AhnLab EPS

AhnLab EPS 개요

AhnLab EPS는 산업 제어 시스템, POS/KIOSK 등의 안정적 운용에 대한 요구가 높고 정해진 프로그램만 사용하는 특수목적시스템에 최적화된 전용 보안 솔루션입니다. 악성코드 탐지 및 분석을 EPS 중앙 관리 서버에서 수행하여 특수목적시스템의 운영 안정성을 보장합니다.

AhnLab EPS

POS Terminals | Plants | ATMs | KIOSKs | SCADA/ICS | Medical Devices

악성코드 관리/통제

강력한 악성코드 탐지 및 확산 방지 기능

애플리케이션 콘트롤

비허가 프로그램 실행 차단

비허가 행위 차단

비허가 행위 및 불필요한 네트워크/매체 차단

경량 / 리소스 점유 최소화

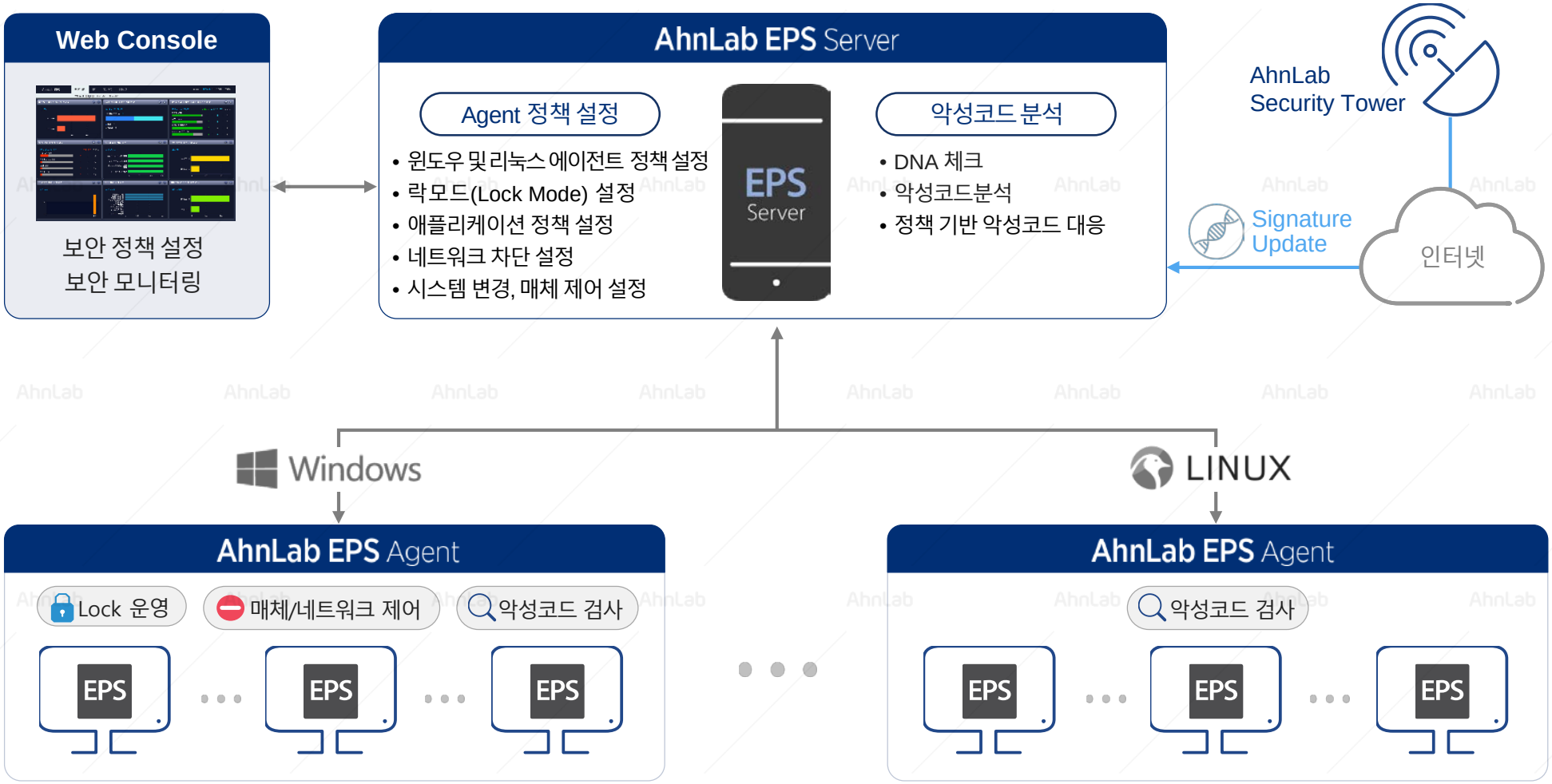
경량 보안 및 통제 솔루션

중앙 집중 통합 관리

중앙 집중식 관리 시스템

도입 방식

AhnLab EPS는 단말 시스템에 설치되는 초경량 에이전트(EPS Agent)와 중앙 모니터링 및 정책 관리 서버(EPS Server)로 구성됩니다.



주요 기능(1) – 3단계 운영 모드

AhnLab EPS는 편리한 정책 설정 및 관리를 위한 3단계 운영 모드(Lock Mode)를 제공합니다. 이를 통해 시스템 중단 없이 안정적으로 보안 관리 및 운영을 할 수 있습니다.

3단계 운영 모드

Unlock Mode

초기 운영 시스템 변경 또는 정책 업데이트

- 최초로 EPS Agent를 시스템에 설치한 상태
- 시스템의 변경 및 유지 보수 작업을 위한 상태
- 모든 시스템 상의 변경 작업이 가능한 상태

Lock Test Mode

보안 정책 설정 및 변경 시 시스템 동작에 문제를 야기하지 않는지 테스트 가능

- 이미 정의한 보안 설정에 대한 검증을 위한 상태
- 현재 구성된 보안 정책에 위배되는 상황이 발생하더라도 제어하지 않음
- 모든 보안 정책 위반 사항은 EPS Agent에서 EPS Server 로 전송되어 관리자 확인 가능

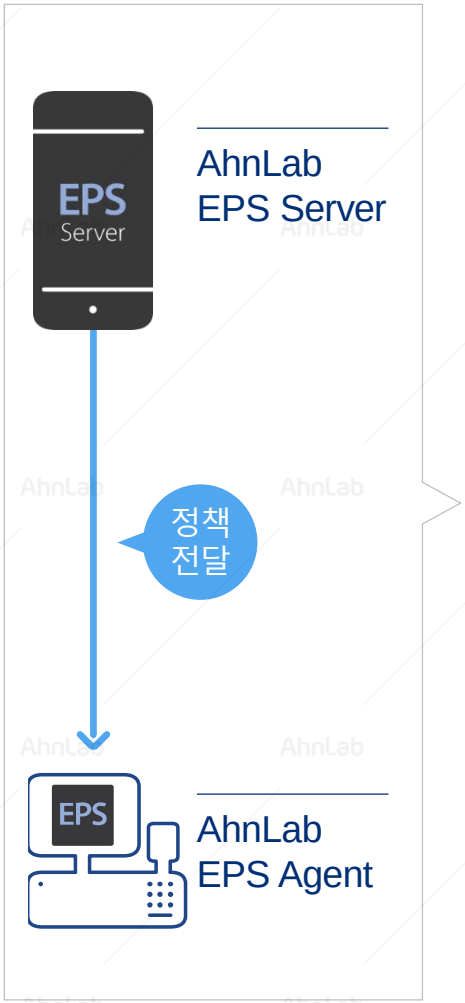
Lock Mode

테스트 모드를 통한 정책 검증 후 보안 운영 모드로 전환 가능

- 정의된 보안 정책을 기반으로 시스템 상의 모든 변경이나 허가되지 않은 프로그램의 실행을 허용하지 않는 상태
- 예외로 정의된 항목을 제외한 모든 변경 허용하지 않음

주요 기능(2) – 애플리케이션 제어 및 네트워크/저장 매체 차단

AhnLab EPS는 화이트리스트 기반의 '애플리케이션 제어'와 네트워크/저장 매체 차단 기능을 제공합니다. 특수목적시스템 운영에 필요한 프로그램만 실행을 허용하고 지정된 업무 외의 행위를 제어함으로써 악성코드 유입, 실행 및 확산을 차단합니다.



애플리케이션 실행 제어 및 시스템 락다운

- 허가된 프로그램만 실행 가능
- 관리자가 지정한 프로그램에 대한 실행 차단
- 독자적인 화이트 리스트 기반 방식으로 관리 편의성 제공
- 시스템 락다운 지원으로, 안전한 시스템 운영 환경 유지 지원

USB 등 다양한 이동형 매체 차단 및 자동 실행 방지

- USB 저장 장치 및 CD 자동 실행 차단
- 다양한 저장 매체에 대한 접근 제어를 지원, 불필요한 매체를 통한 악성코드 유입 방지
- 특정 매체에 대한 예외적으로 접근 허용 지원(인스턴스 경로 기반)

IP/포트 네트워크 연결 차단

- 허가되지 않은 IP / 포트로의 네트워크 통신 차단을 통한 악성코드 유입 및 내부 확산 방지

주요 기능(3) – 최적화된 악성코드 대응

특수목적시스템 운영 환경의 특수성을 고려한 AhnLab EPS는 EPS Server에 탑재된 악성코드 분석 엔진을 통해 EPS Agent가 설치된 단말 시스템의 네트워크 및 시스템 자원에 영향 없이 악성코드를 탐지 및 차단합니다.

AhnLab EPS Server

단말 시스템 부담 최소화

단말 시스템의 자원을 거의 사용하지 않고
모든 실행 파일에 대한 실시간 검사 수행

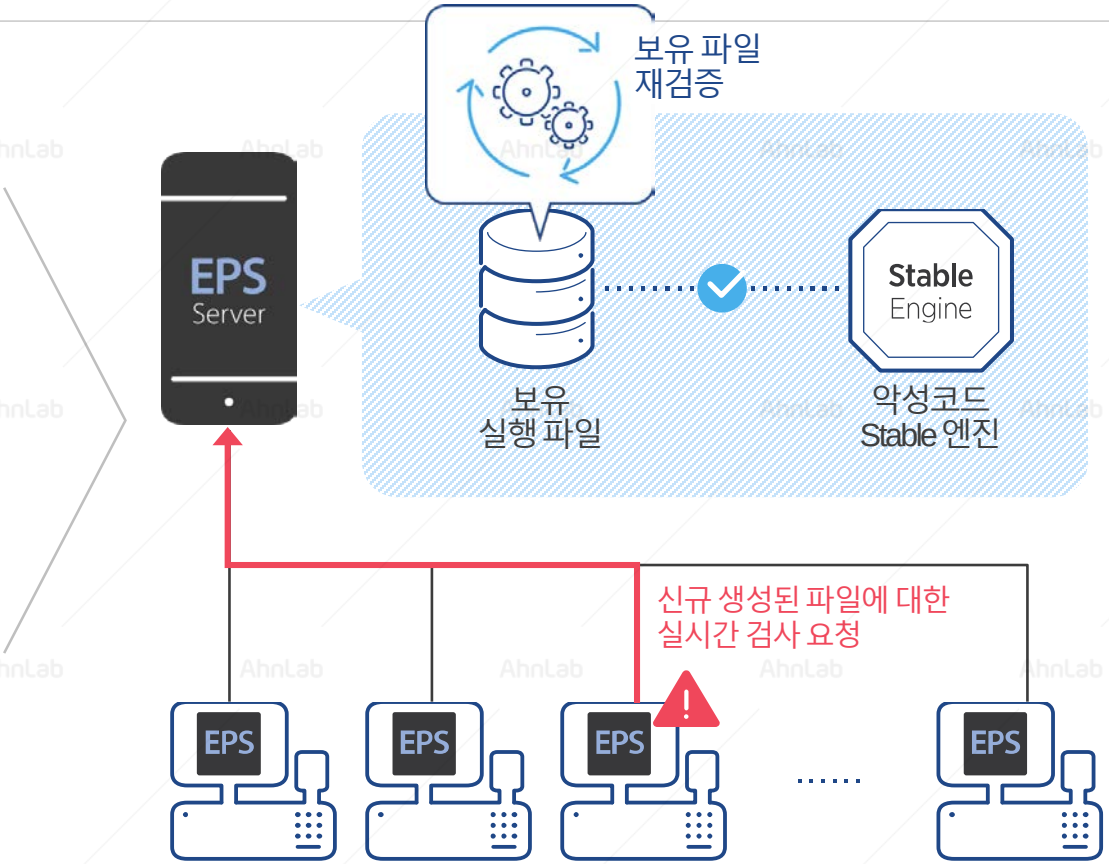
보유 파일 재검증

분석 엔진 업데이트 시 서버 내 보유된
파일에 대한 재검증 작업 수행

검사 시점 이후 발생한 보안 위협까지 대응

Stable 엔진 탑재

안정성이 검증된 Stable 엔진으로
오진 사고 발생 가능성 최소화



주요 기능(4) – 윈도우 및 리눅스 단말 악성코드 검사

EPS Server에 탑재된 악성코드 분석 엔진은 EPS Agent가 설치된 윈도우 및 리눅스 OS 기반의 단말 시스템에 대해 네트워크 및 시스템 자원 영향 없는 주기적인 악성코드 검사 및 탐지를 제공합니다.

AhnLab EPS Server
- 악성코드 검사

- 악성코드 탐지 정보 확인
- 탐지된 악성 파일 삭제 요청

특수목적시스템 운영 부담 최소화
- 단말 리소스 점유 최소화

파일 전송 ---------- 파일 전송

윈도우 및 리눅스 단말 악성코드 검사 정책
- 악성코드 수동 검사 명령
- 악성코드 예약 검사 설정
- 정책 설정에 따라 탐지된 악성코드에 대해 OS별 대응 지원
  - Windows: 실행 차단 및 삭제 기능 제공
  - Linux: 삭제 기능 제공

AhnLab EPS 2.0
Client for Windows

윈도우 기반 특수목적시스템에 대한
실시간 및 예약 검사 수행

AhnLab EPS 2.0
Client for Linux

리눅스 기반의 특수목적시스템에 대한
기본적인 보안 체계 마련

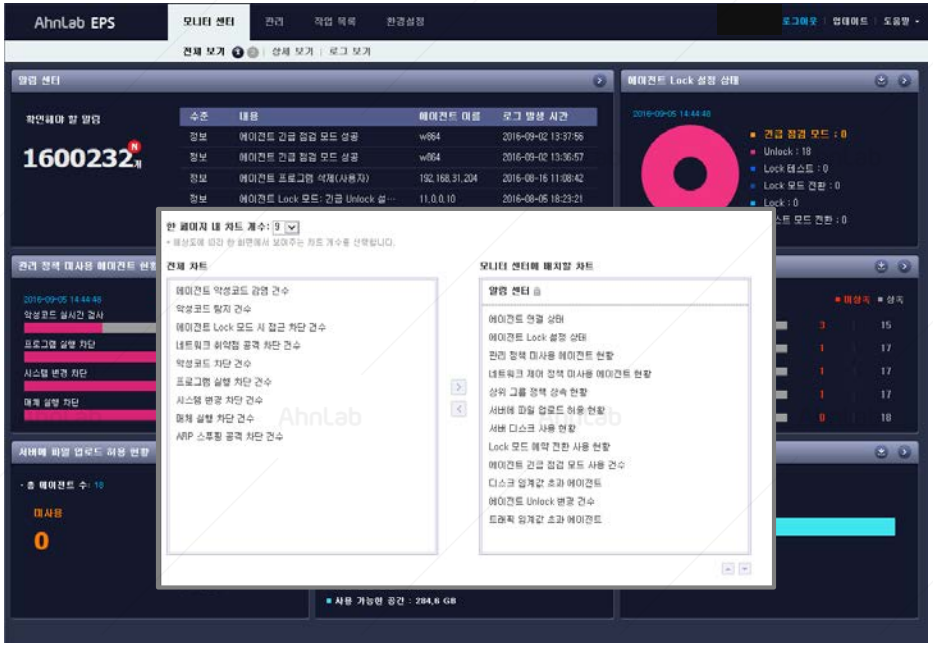
주요 기능(5) – 관리자 기능

AhnLab EPS의 웹 기반 관리 시스템을 통해 각각의 설비 시설에 산재되어 있는 시스템을 효율적으로 통합 관리할 수 있습니다.
또한 관리 대상 시스템을 그룹으로 설정해 공통 또는 개별 보안 정책을 일관성 있게 설정 및 적용할 수 있으며, 모든 시스템에서 발생하는 로그를 한 곳에서 확인할 수 있어 편리하게 관리할 수 있습니다.

웹 기반 통합 관리 시스템

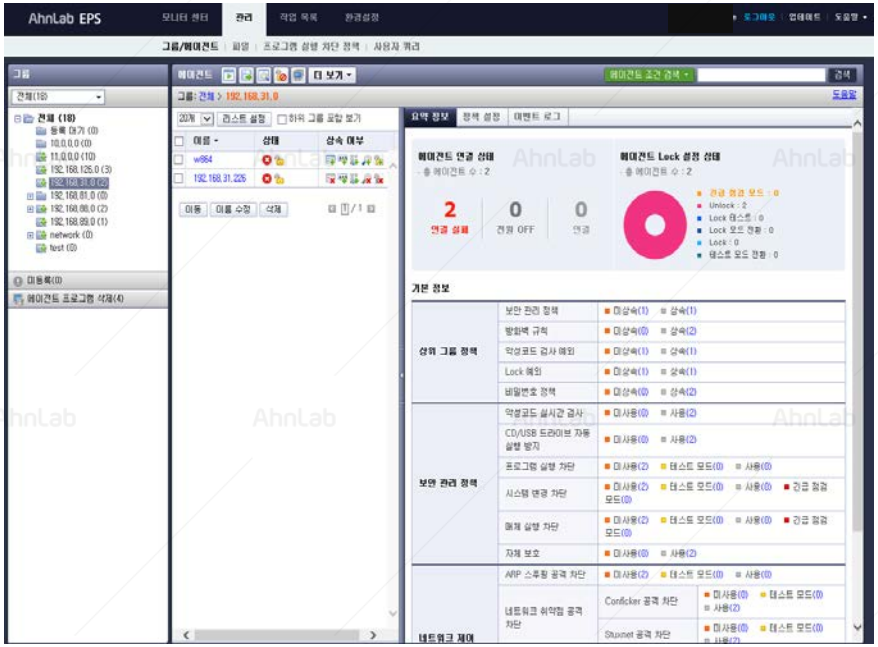
다양한 차트 제공

Agent 의 연결 상태, Lock 모드 사용 등의 설정 상태와 함께
Agent 의 악성코드 탐지/차단, 보안 정책 위배 행위에 대한 모니터링 제공



편리하고 일관된 정책 설정

Agent 그룹 또는 개별 Agent 별 정책 설정과 함께
Agent 별 이벤트 로그 조회



특장점(1) – 차별적인 화이트리스팅

블랙리스트 기반의 일반적인 안티바이러스 제품과 달리, AhnLab EPS는 독자적인 화이트리스트 기술을 기반으로 생산 설비 시스템과 같이 특정한 애플리케이션만을 사용해야 하는 특수목적시스템 환경에 최적화된 보안을 제공합니다.

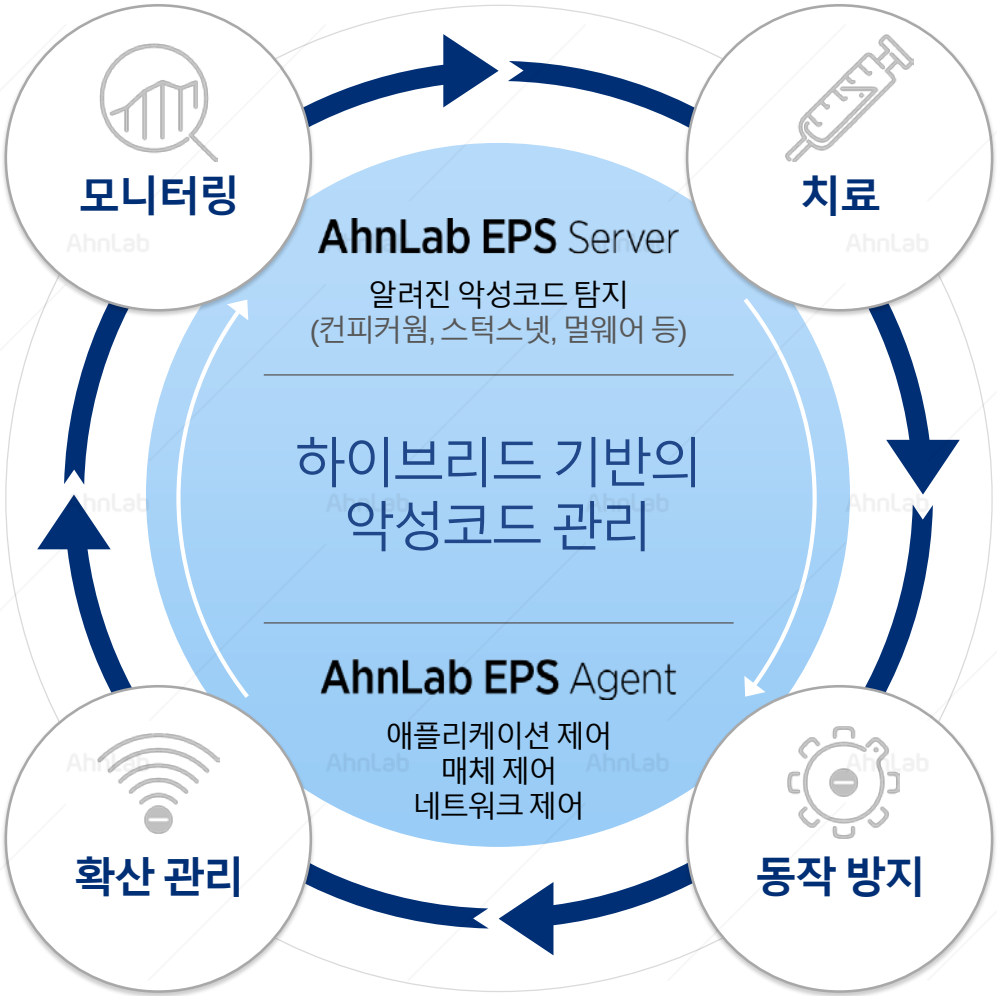
EPS Agent를 통해 단말 시스템에서 **안전한 파일만 실행되도록 제한 가능**
사전 방역 효과

관리자의 애플리케이션 **화이트리스팅 작업 불필요**
정책 설정 부담 없이 특화된 애플리케이션에 대해서도 유연한 관리 가능

EPS 화이트리스트 기반의 EPS Agent		VS. 블랙리스트 기반의 기존 백신 제품
사전 예방	처리 방식	사후 처리
허용된 애플리케이션만 사용	애플리케이션 실행 범위	모든 애플리케이션 사용 가능
변경 없음	엔진 크기	지속적인 변동 발생
낮음	자원 점유율	높음
매우 높음	보안 수준	보통
엔진 업데이트는 불필요 (EPS 서버에서 업데이트 필요)	엔진 업데이트	주기적인 엔진 업데이트 필요

특장점(2) – 하이브리드 대응

단말 내 파일의 악성 여부를 EPS 서버에서 검사함으로써 특수목적시스템의 운영 안정성 확보와 악성코드 방어가 가능합니다.



악성코드 분석/관리

- 악성코드 실시간 감시
- 로그 검색

악성코드 제거

- 정책적 삭제

감염 통제

- 네트워크 차단(IP/포트) 및 매체 차단을 통한 악성코드 유입 및 확산 방지

악성코드 동작 방지

- 애플리케이션 실행 제어 및 실행파일 생성/변경 차단 기능을 통한 사전 방역 기능 지원

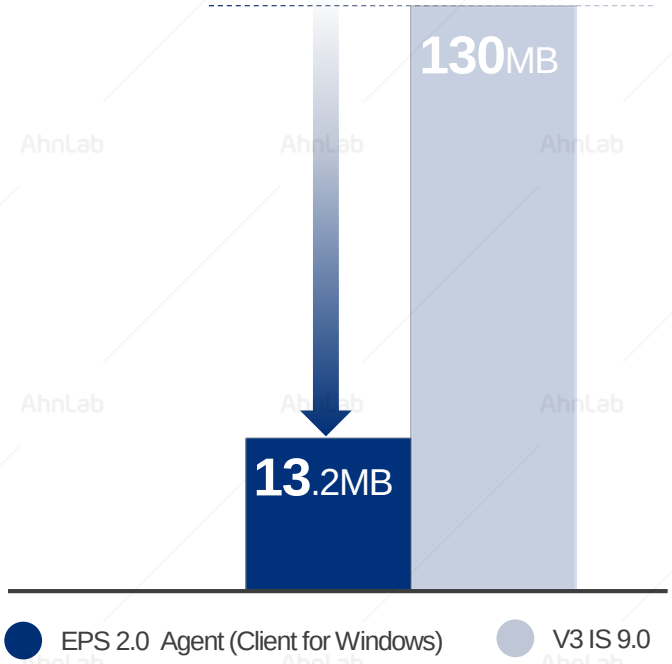
특장점(3) – 초경량 솔루션

특수목적시스템 운영에 최적화된 초경량 솔루션 AhnLab EPS의 에이전트(EPS Client)는 기존 보안 솔루션 대비 현저히 적은 시스템 자원만 사용하며, 최초 설치 이후 변동이 거의 없어 시스템 운영의 연속성에 영향을 주지 않습니다.

AhnLab EPS Server — 악성코드 검사, 엔진 업데이트 등 시스템 자원 사용이 요구되는 작업은 EPS Server에서 수행

AhnLab EPS Agent — 엔진 업데이트 불필요 → 하드디스크 자원 사용 정도의 변화 거의 없음

설치본 크기



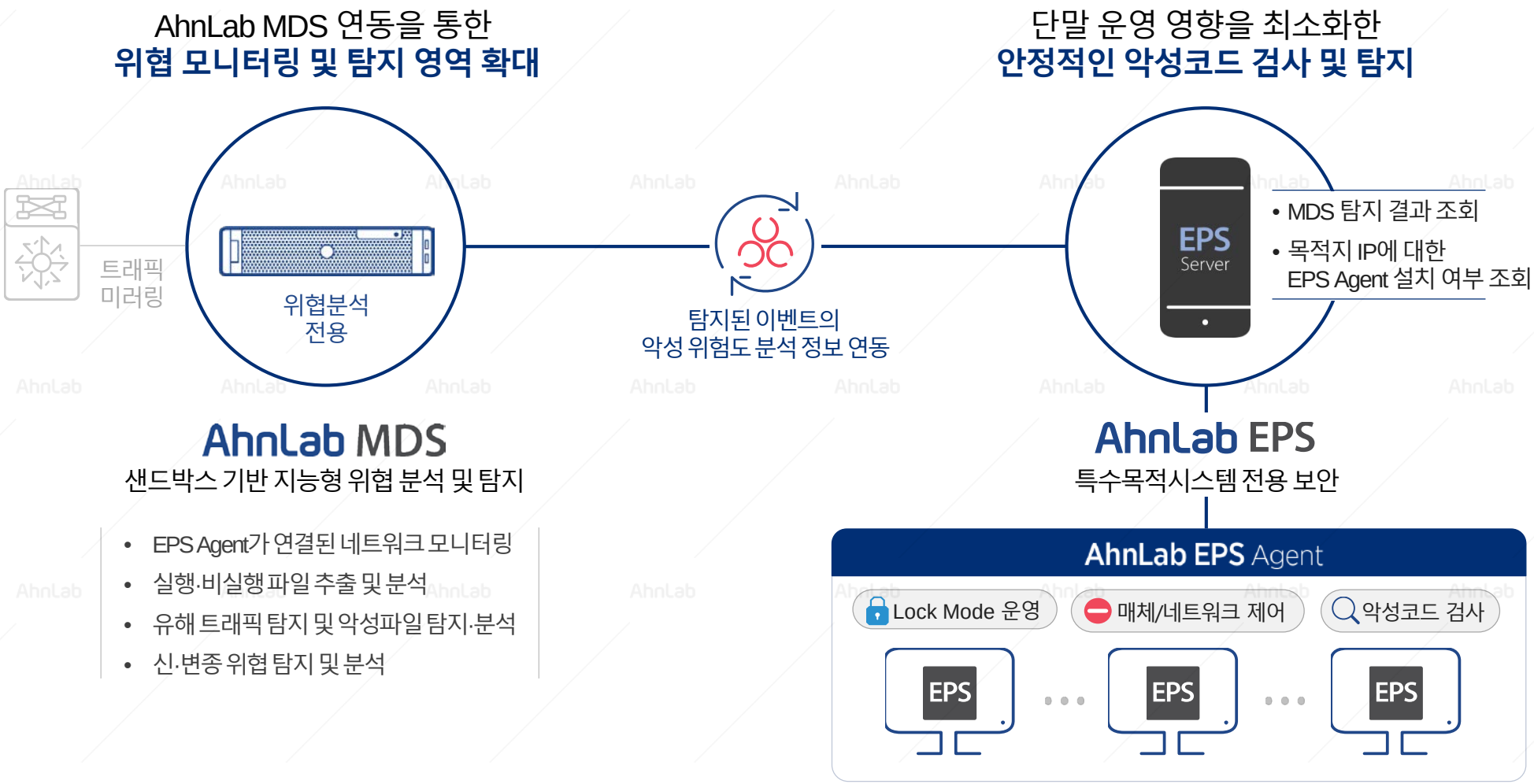
시스템 자원 사용량

테스트 제품: EPS 2.0 Agent - Client for Windows
* 수동/예약 검사 시 CPU 사용량은 제한 옵션 제공

	메모리 사용량(Idle)	검사 시 메모리 사용량	CPU 사용량(Idle)
OS: Windows 10 19H1 CPU 2 Core, MEM 2GB	5MB	6.14MB	0.24%
OS: Windows Server 2008 CPU 1 Core, MEM 1GB	5.1MB	6.9MB	0.12%

특장점(4) – 위협 모니터링 정보 확대

지능형 위협 분석 솔루션인 AhnLab MDS 연동을 통해 EPS Agent가 설치된 특수목적시스템 환경의 네트워크 모니터링을 강화함으로써 다양한 유형의 악성 파일과 유해 트래픽 탐지 및 차단이 가능합니다.



사용 환경

AhnLab EPS는 중앙 모니터링 및 정책 관리 서버(EPS Server)와 윈도우 또는 리눅스 단말에 설치되는 에이전트(AhnLab EPS Client)로 제공됩니다.

AhnLab EPS Server

구분		최소 권장 사양
하드웨어	CPU	Intel® Xeon® Processor E5 Family (4 core*2 또는 8 core 이상, 3GHz 이상, 8MB Cache 이상)
	Memory	16GB 이상
	HDD	• OS용: 300GB x 2 (RAID 1) 이상 • DATA용: 1TB 이상 (RAID 구성 권장) ※고객사의 파일 수집 양에 따라 증설이 필요할 수 있습니다.
운영체제		RHEL 6.5(64 bit) ~ RHEL 6.10(64 bit)
콘솔(브라우저)		Internet Explorer 8.0 이상

*최대 8,000 agent 권장

사용 환경

AhnLab EPS Client for Windows

구분		최소 권장 사양
하드웨어	CPU	Pentium 133MHz
	Memory	64MB(15MB 이상 여유 공간)
	HDD	2GB(100MB 이상 여유 공간)
운영체제	Embedded OS	• Windows XP Embedded • Windows Embedded Standard 2009 • Windows Embedded Standard 7 • Windows Embedded POSReady 2009 • Windows Embedded POSReady 7 • Windows Embedded 8.1 Industry (Pro, Enterprise)
	Client OS	• Windows 2000 Professional • Windows XP (Home, Professional) • Windows Vista (Enterprise, Ultimate) • Windows 7 (Enterprise, Professional, Ultimate) • Windows 8/8.1 (Enterprise, Pro) • Windows 10 (Enterprise, Pro, IoT Enterprise)
	Server OS	• Windows 2000 (Server, Advanced Server) • Windows Server 2003 (Standard, Enterprise)/ 2008 (Standard, Enterprise) • Windows Server 2012 (Essentials, Standard) /2016 (Essentials, Standard) • Windows Server 2019 (Essentials, Standard)

* 매체제어는 Windows XP SP2 이상, Windows Server 2003 SP2 이상부터 지원되며 XP Embedded는 매체제어 동작을 위한 추가 모듈 설치가 필요할 수 있습니다.

AhnLab EPS Client for Linux

구분		최소 권장 사양
하드웨어	CPU	Intel 계열 (32/64 bit)
	Memory	1GB 이상
	HDD	500MB 이상의 여유 공간
운영체제	CentOS	• 3.3 ~ 7.5
	Red Hat Enterprise	• 3.3 ~ 7.4

도입 효과

AhnLab EPS

안정적인 시스템 운영

- 최적화된 응용 프로그램 통제 및 시스템 락다운(Lockdown) 모드 제공
- 시뮬레이션 모드 지원을 시스템 운영에 최적화된 정책 설정 지원
- 예외처리 기능, 긴급 점검 모드 지원으로, 안정적인 시스템 운영 지원

다양한 운영 환경에 최적화된 보안

- 윈도우(Windows) 및 리눅스(Linux) 단말 시스템 내 파일에 대한 악성코드 검사 및 대응 기능
- 컨피커(Conficker), 스턱스넷(Stuxnet) 등 주요 네트워크 공격 차단 및 ARP Spoofing 공격 차단
- 중앙에서의 통합 관리를 통한 일원화된 보안 관리 지원
- 개별 정책 설정 지원 - 시스템 특성에 따른 정책 설정 지원(Windows, Linux Agent 정책 통합 관리)
- 에이전트 삭제 비밀번호 설정(Windows, Linux)

비즈니스 연속성 확보 및 생산성 향상

- 단말 시스템의 리소스 및 업무 프로세스에 영향을 주지 않고 악성코드 탐지/차단 가능
- 업무 외 프로그램 차단을 통해 비즈니스 생산성 향상
- 계획하지 않은 파일 변경 등으로 인해 단말 시스템 다운타임 사전 예방 가능
- 과다한 네트워크 트래픽 발생 차단 등 잠재적 위협 및 장애 요소 제거

비용 절감 효과

- 백신 등 별도의 보안 솔루션 추가 도입 불필요
- 추가 솔루션 도입에 따른 비용 발생 및 운영 리소스 부담 해소

적용 분야

초경량 보안 및 통제 솔루션 AhnLab EPS는 생산설비시스템, POS 시스템, 키오스크(KIOSK), 병원 시스템과 같이 시스템 안정성 및 운용에 대한 민감도가 높은 특수목적시스템의 안정적인 운용과 비즈니스 연속성 확보에 기여합니다.

금융 분야

결제시스템(POS)
ATM

디지털 생산 설비 분야

반도체
디스플레이
가전
자동차 생산 자동화 설비

의료 분야

병원처방시스템 등

공공분야 기반 시설

전력, 수도, 가스,
난방 등 설비 제어 시스템,
무인민원발급기,
신호제어 시스템

기타

키오스크
교통흐름 전광판 등

03
AhnLab EPS Standalone

1. AhnLab EPS Standalone 개요
2. 도입 방식
3. 사용 환경
4. 자사 제품 기능 비교

AhnLab EPS Standalone

AhnLab EPS Standalone은 가용성 및 운용 안정성에 대한 요구가 높은 특수목적시스템 보안에 최적화된 '독립형 에이전트' 솔루션으로, 오프라인 운영 환경에서 정해진 애플리케이션만을 사용해야 하는 시스템을 각종 보안 위협으로부터 안전하게 보호합니다.

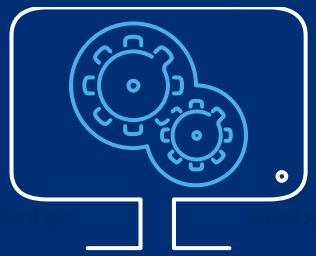
애플리케이션 콘트롤

허가된 프로그램만 실행 허용

초경량/ 리소스 점유 최소화

초경량 보안 에이전트로
시스템 가용성 유지

AhnLab
EPS Standalone



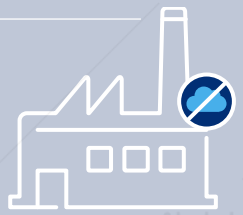
독립형 에이전트

오프라인 운영 환경 보호
EPS 서버 연결 불필요

Lockdown 기능

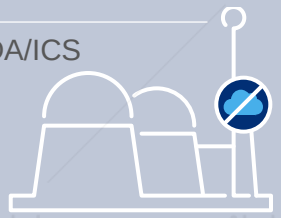
실행 파일 생성 및 변경 방지로
악성코드 감염 예방

Plants



KIOSKs

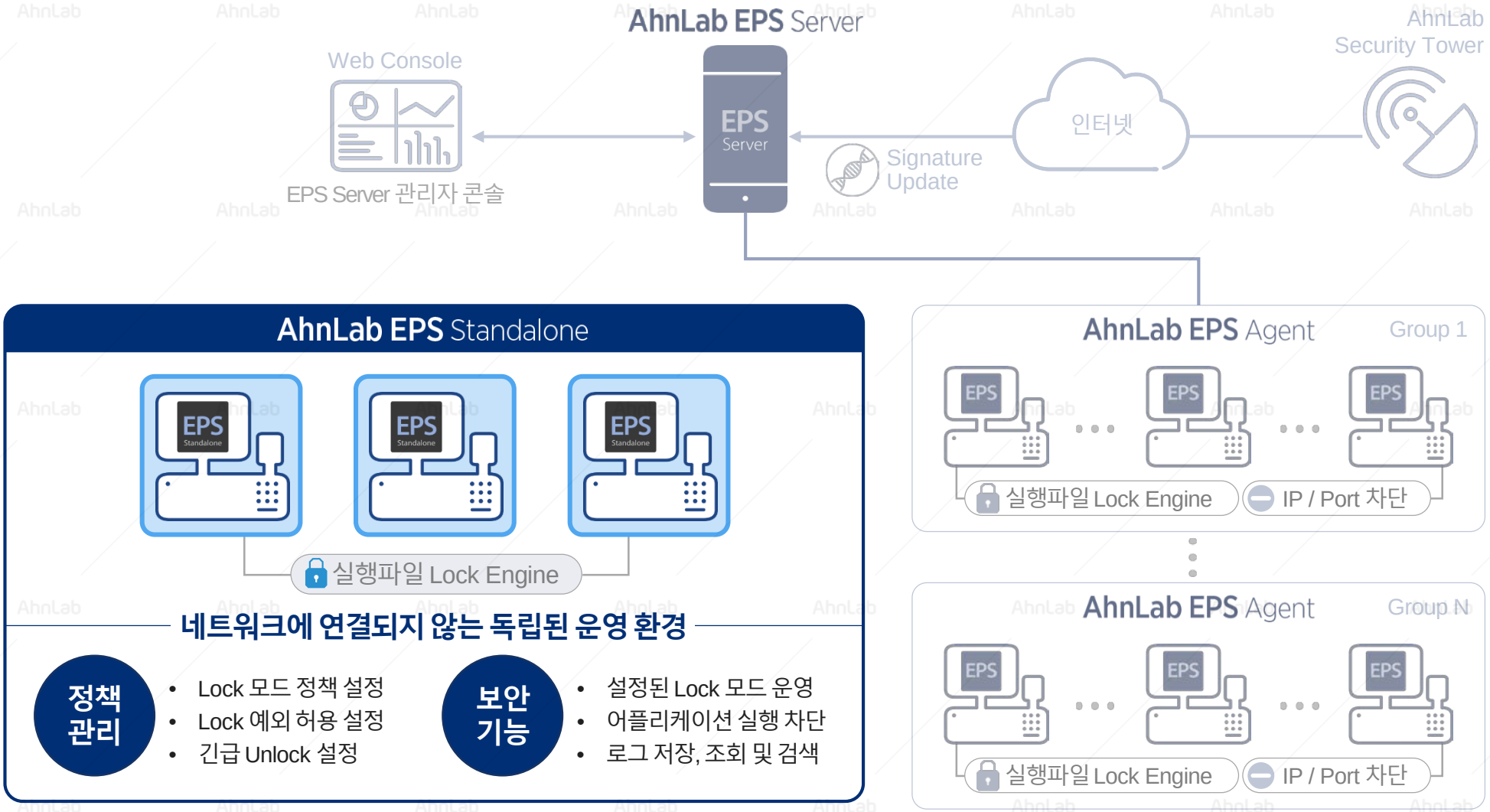
SCADA/ICS



Medical Devices

도입 방식

AhnLab EPS Standalone은 오프라인 환경의 특수목적시스템 단말기에 설치되는 독립형 초경량 에이전트입니다.



사용 환경

AhnLab EPS Standalone

구분		최소 권장 사항
하드웨어	CPU	Pentium 233MHz 이상
	Memory	64MB 이상 여유 공간
	HDD	1.5GB 이상 여유공간
운영체제	Embedded OS	• Windows Embedded Standard 2009 • Windows Embedded Standard 7 • Windows Embedded POSReady 2009 • Windows Embedded POSReady 7 • Windows Embedded 8.1 (Pro, Industry)
	Client OS	• Windows XP SP3 (Home, Professional) • Windows Vista (Enterprise, Ultimate) • Windows 7 (Professional, Enterprise, Ultimate) • Windows 8 (Professional, Enterprise) • Windows 8.1 (Professional, Enterprise) • Windows 10 (Pro, Enterprise)
	Server OS	• Windows Server 2008 (Standard, Enterprise) • Windows Server 2012 (Essentials, Standard) • Windows Server 2016 (Essentials, Standard)

* 상기 OS의 32/64 bit 지원

자사 제품 기능 비교

AhnLab EPS Standalone은 EPS 서버와 연결되지 않는 단독 운영 장비를 대상으로 락모드(Lock Mode) 기능만 제공합니다.

AhnLab EPS (Client for Windows) vs. **AhnLab EPS Standalone** 기능 비교

구분		AhnLab EPS (Client for Windows)	AhnLab EPS Standalone
Agent 관리 방식		EPS 서버 연결형	독립형 에이전트
보안 정책 설정(관리 콘솔)		EPS 서버 웹 콘솔	단말에 설치되는 에이전트 내 관리자 UI 제공
Lock Mode	락모드 지원	O	**O**
	락(Lock) 예외 경로 및 파일 지정	O	**O**
	테스트 모드 지원	O	**O**
	긴급 언락(Unlock) 지원	O	**O**
매체 제어		O	-
네트워크 공격 탐지		O	-
방화벽		O	-
악성코드 검사		O	-
로그		O	**O**

04
주요 레퍼런스

주요 레퍼런스

제조 분야

삼성전자 | 삼성디스플레이 | 삼성 SDI | 삼성전기 | SK하이닉스 | 현대기아자동차

LG 디스플레이 | LG 화학 | LG 이노텍 | 롯데케미칼 | CSOT

POS, KIOSK 등 특수목적시스템 분야

신세계 | 호텔 신라 | 세븐일레븐 | 롯데백화점 | 다이소아성산업 | 삼성물산 (에버랜드리조트)

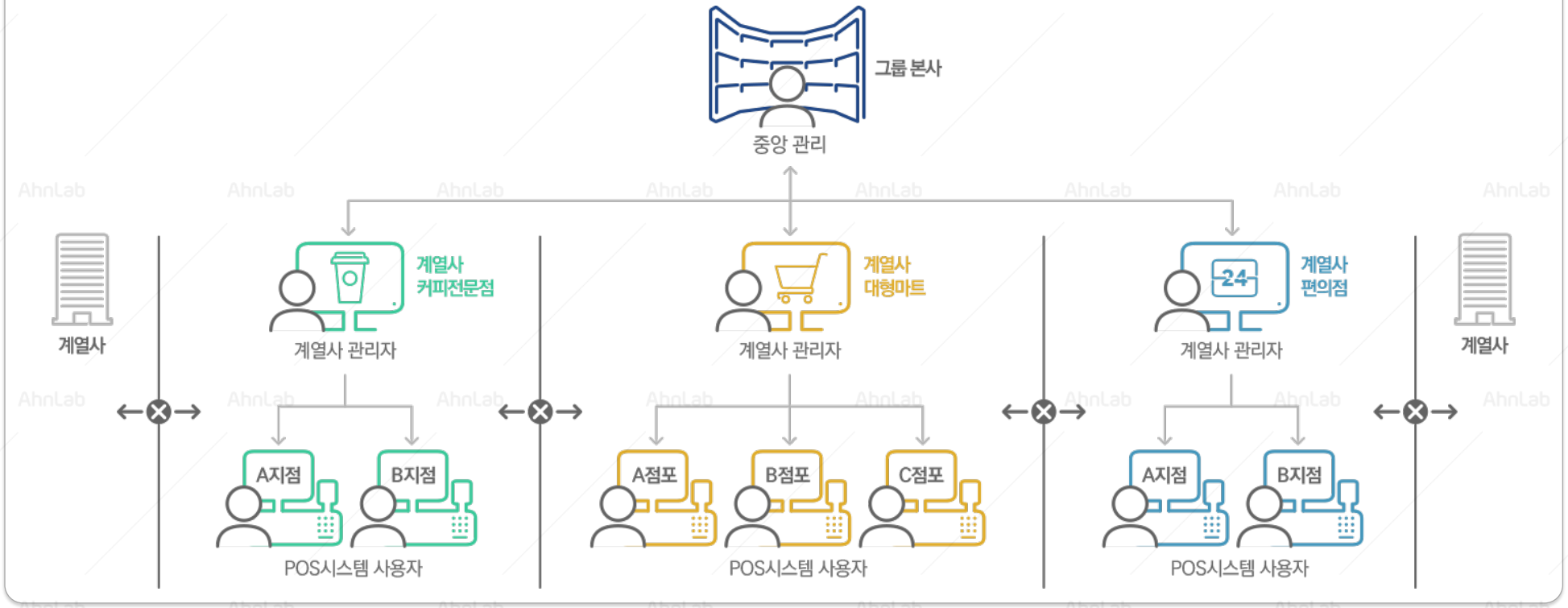
인천국제공항공사 | 여수시청 | LF

도입 사례 1 – S 유통 그룹

유명 유통기업인 S 그룹은 해킹, 악성코드, 비인가 소프트웨어 설치 및 POS 시스템 오남용 방지 등을 위해 대형마트, 백화점, 커피전문점 등 6개 계열사 9,000여 대의 POS 단말기에 AhnLab EPS를 적용했습니다.

- 낮은 네트워크 대역폭 환경
- 백신 패치 및 엔진 업데이트 시 트래픽 이슈
- Embedded OS 지원하는 보안 솔루션 필요
- 저사양 단말기에서 POS 프로그램 운용
- 수천 대의 POS에 대한 안전한 중앙 관리 필요

유통기업 S 그룹의 AhnLab EPS 도입 구성도



도입 사례 2 – I 공항

I 공항은 저사양 시스템에서 운용되는 1,800여 대의 FIDS의 안정적인 운영과 강력한 보안 체계를 구축하기 위해 AhnLab EPS를 도입하였습니다.
이를 통해 폐쇄망 환경에서도 일관된 보안 정책 적용 및 관리가 가능하게 되었습니다.

도입 배경

- Embedded XP를 사용하는 공항 FIDS에 대한 보안 대책 부재
- 일반 PC용 백신 프로그램 운영으로 인한 시스템 성능 저하
- 백신 엔진 업데이트 시, 네트워크 리소스 부담
- 폐쇄망 환경에 따른 백신 프로그램의 최신 엔진 반영 불가

I사 요구사항

- 성능 저하 방지 및 안정적인 FIDS 운영 보장
- CF메모리 상에서의 안정적인 보안 솔루션 운용
- 폐쇄망 환경에서도 실효성 있는 보안
- 효율적인 보안 관리 및 위협 대응

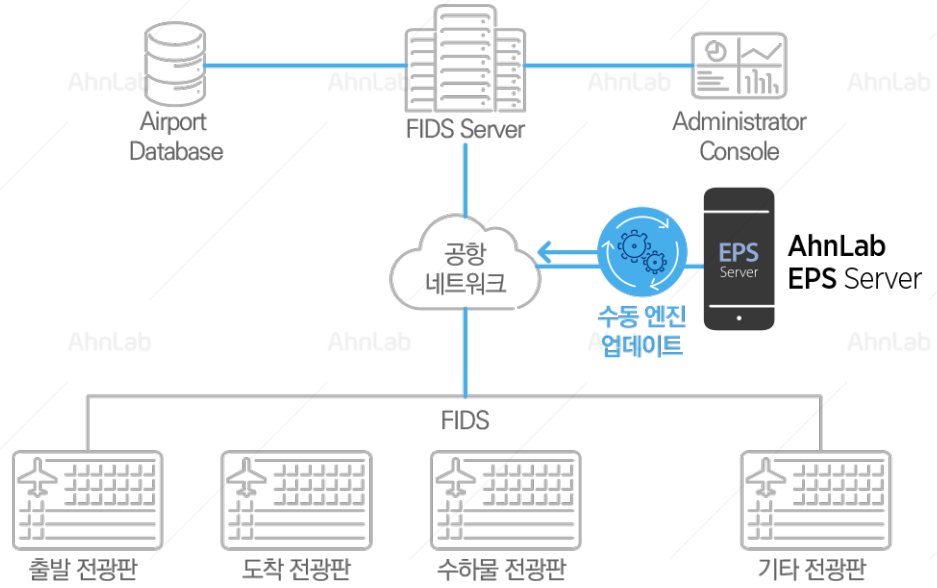
I 공항 AhnLab EPS 구성도 및 도입 효과

강력한 보안 체계 구축

- 애플리케이션 제어: FIDS 프로그램만 실행
- 비인가 시스템 변경 차단, 비인가 네트워크 연결 차단

안정적인 FIDS 운영 가능

- 서버형 분석 엔진 사용으로 개별 시스템에서의 업데이트 불필요
- 초경량 에이전트를 통한 시스템 부하 최소화
- 폐쇄망에서 안정적인 보안 솔루션 운영 가능



도입 사례 3 – S전자 반도체

S반도체는 컨피커웜 등 악성코드 감염으로 인한 생산 설비의 운영 중단 문제를 해결하기 위해 AhnLab EPS를 도입하였으며,
현재 전체 생산 설비로 AhnLab EPS의 확대 적용을 진행하고 있습니다.

도입 배경

- 지속적인 악성코드 감염
- 컨피커 웜 감염으로 생산 설비 운영 차질
- 저사양 PC에 일반 AV 솔루션 적용 어려움
- AV 솔루션의 오진 가능성 우려

S사 요구사항

- 강력한 악성코드 방역
- 제품 패치 최소화
- 저사양 PC에서의 안정적인 동작 보장
- 보안 솔루션의 오진 방지

도입 효과

화이트리스트 기반의 사전 방역

오진 사고 확률 제거

저사양 PC까지 보안 대응책 적용

전체 생산 라인의 중앙 집중 관리 가능

* 컨피커 웜(Conficker worm)

컨피커 웜은 윈도 OS의 보안 취약점을 이용해 네트워크와 USB로 전파되는 악성코드로 세계적으로 많은 감염 피해를 유발하고 있다.
컨피커웜은 취약점을 이용하는 방법 외에도 다양한 전파방법, 지속적인 진화, 자기보호 및 탐지우회방법 등의 종합적인 특징을 가지고 있어, 대처가 매우 까다롭다.

도입 사례 4 – L 전자부품 전문 업체

L전자부품 전문 업체는 민감한 생산 설비를 보호하고 정보 유출을 방지하기 위해 AhnLab TrusLine 을 도입, 그 과정에서 시스템 내부에서 수천 개의 악성코드를 확인 및 제거하는 등 상당한 효과를 거뒀습니다.
이를 계기로 L사는 국내에 이어 중국의 생산 라인에 AhnLab EPS 를 확대 도입하였습니다.

도입 배경

- 산업시설을 겨냥한 악성코드의 빠른 증가
- 기밀정보 유출 방지
- 생산 설비 보호

S사 요구사항

- 악성코드 방역
- USB 등 외부 저장장치 이용 차단을 통한 내부 정보 유출 방지
- 민감한 생산 시설의 안정적인 운영 보장

도입 효과

컨피커 웜 등 3,000 여 개의 악성코드 탐지 및 제거

강력한 보안 정책 적용 가능

전체 생산 라인에 대한 중앙 관리 가능

초경량 솔루션 도입으로 안정적인 설비 운영

국내 및 중국 생산 라인까지 솔루션 확대 도입

More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우)13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용 상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com

AhnLab EPS

AhnLab