산업용 단말 보안을 위한 효과적인 보호 대책

More security,
More freedom

The Security Next Conference 2016

안랩 제품기획팀 이지훈 차장

AhnLab

관련 위협 동향 및 산업용 단말

More security,
More freedom

AhnLab

2016년 국내 5대 보안위협

AhnLab

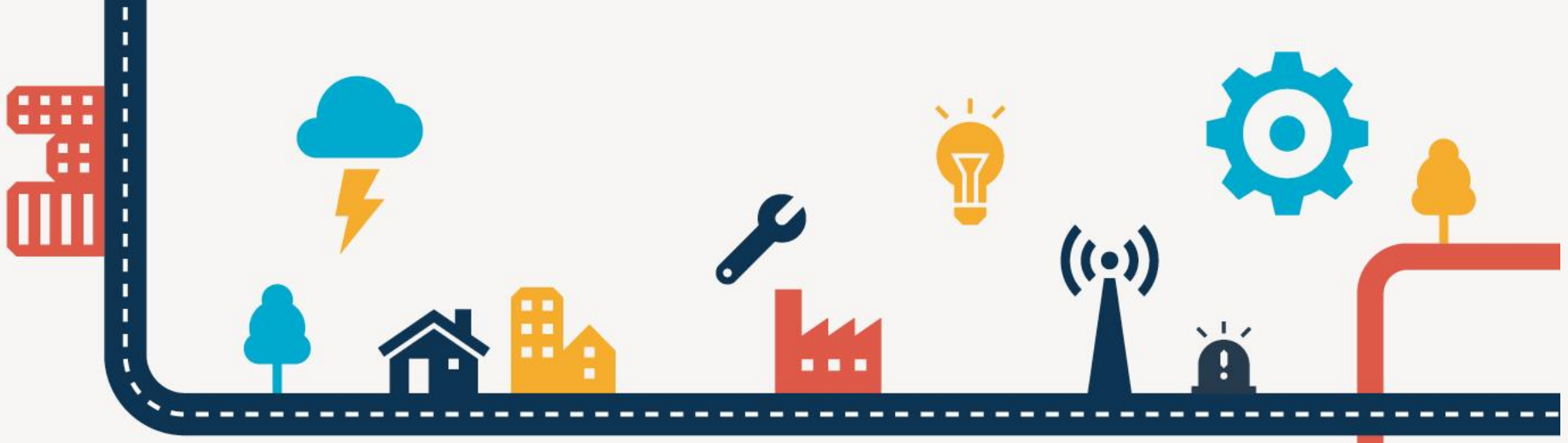
랜섬웨어 고도화 및
스마트폰으로 공격 확대

기반시설 사이버테러
발생 가능성 증가

사물인터넷 위협 증가 및
드론, 스마트카 위협 현실화

소프트웨어 취약점 노린
공격 기승 예상

인터넷 전문은행 출범에
따른 금융서비스 위협 심화



2016년 국내 5대 보안위협 #2

기반시설 사이버테러 발생 가능성 증가

이전의 테러가 물리적인 파괴에 국한되었던 것에 반해 최근 인터넷을 통한 테러리스트들의 이념 선전 및 정보수집, 적대국가 도·감청 및 정보 유출 등 테러는 이미 사이버 환경에 깊숙이 침투했다. 일반 대중들의 공포감을 조성하는 것이 테러의 목적이라는 점에서 국가기반시설을 노린 고도화된 지능형 위협 APT(Advanced Persistent Threat)의 가능성을 배제할 수 없다.

산업용 단말이란

AhnLab

계측 및 제어(I&C, Instrumentation and Control) 시스템에서 계측한 정보를 모니터링 하는 부분

관리
- ERP / MES / SCADA Svr.

운영 / 계측 및 제어
- HMI / MMIS / Industrial Workstation

Remote I/O Field
- PLC, RTU, Distributed I/O

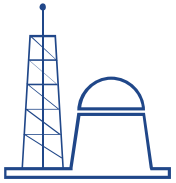
산업용 단말이란

AhnLab

제조설비/산업설비/기반시설의 모니터링 및 제어 목적의 단말, 또는 지불처리(POS 등)/의료정보처리/KIOSK 용도의 단말 등 한정 목적(Fixed-Function) 으로 운영하는 단말을 포괄적으로 이야기함

공공분야 기반 시설

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



Fixed-Function Device

의료 분야

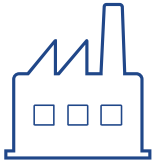
병원처방시스템 등

금융/유통 분야

결제시스템(POS), ATM
금융회사의 중요 단말기

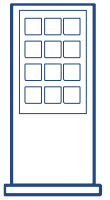
디지털 생산 설비 분야

반도체, 디스플레이, 가전,
자동차 생산 자동화 설비



기타

키오스크
교통흐름 전광판
콜센터, 통신사 대리점 등의
기타 비범용 PC

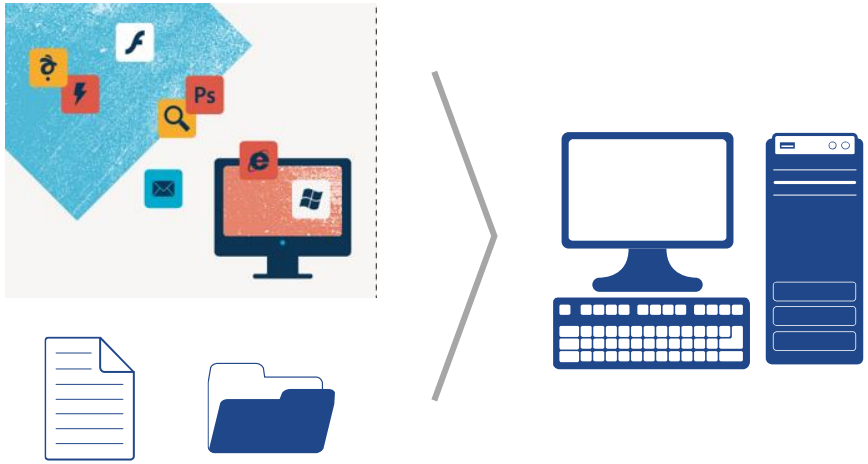


사용 목적에서의 차이

AhnLab

산업용 단말도 결국은 컴퓨터를 사용하여 정보를 처리한다는 점에서 업무용도의 범용 단말과 다르지 않음.
하지만, 사용 목적에서 차이가 있음

기밀성 / 무결성 / 가용성 보호



Information 처리

정보를 효율적/효과적으로 처리하기 위하여 물리적인 환경(컴퓨터 하드웨어)을 이용

안전성 / 신뢰성 / 가용성 보호

Physical 환경 처리

물리적인 환경을 효율적/효과적으로 처리하기 위하여 정보를 이용

우려

AhnLab

산업용 단말에 대한 보안우려가 현실이 되는 경우, 실 환경에 미치는 경제적 또는 환경적인 영향이 매우 광범위 할 수 있음

Stuxnet	Malicious access	Blaster virus
Zotob	Confiicker	PE_SALITY

안전성 / 신뢰성 / 가용성 보호 실패

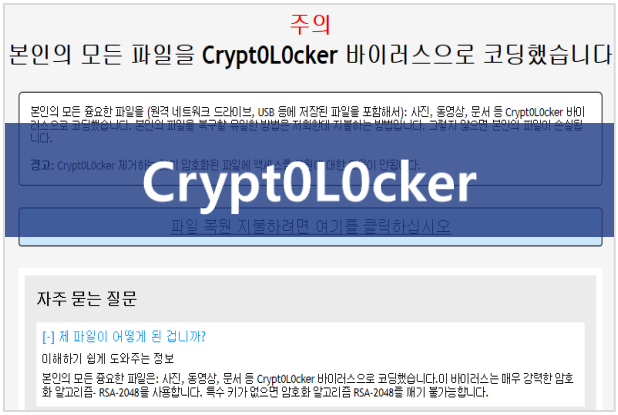
시스템 정지, 오동작, 정보 유출

실 생활에 경제적, 환경적 영향

가정을 한 번

AhnLab

산업용 단말을 인질로 잡는 악성코드에 감염 된다면?



고려해야 할 보안 특성

AhnLab

보안이슈	일반 단말	산업용 단말
백신	통상적이며 쉽게 설치, 운영	시스템 영향으로 인해 설치 및 운영 어려움
패치관리	통상적이고 광범위한 사용	효과적인 설치 및 적용이 불가능
변화관리	최소 사용 주기에 맞추어 정기적으로 수행	시스템 영향으로 인해 전략적으로 계획 및 수행
보안 우선 순위	정보가 적절히 관리되어 정보누출을 방지하는 것이 중요	시스템을 계속해서 안전하게 가동하는 것이 중요
보안 대상	정보	물건 (설비, 제품) 서비스 (연속가동)
기술 지원 기간	2~3년	10~20년
요구되는 가용성	재기동이 허용범위인 경우가 많음	24시간 365일 안정가동 (재기동이 허용되지 않는 경우가 많음)
운영관리 주체	정보시스템 부문	현장 기술 부문

자료출처: 안랩 CERT Report, 2015년 6월호

실제 환경

More security,
More freedom

AhnLab

다양한 위협 환경

AhnLab

악성코드 뿐만 아니라 다양한 위협 환경이 존재함

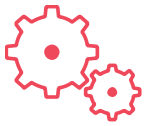
보안 위협

사람에 의한 실수 및 오남용

- 보안 사고의 60-80%가 사람에 의한 실수(Human Error) - 출처: IAEA NSS No.17
- 취약시간(24시간 교대근무 환경 등)에 단말 오남용
- 비허가 프로그램 설치

악성코드

- 하루 평균 약 20만개의 신종 악성코드 유포
- POS 악성코드 등 특정 시스템을 노리는 악성코드 증가 추세 - Stuxnet, Flame, Duqu 등



운영 환경적 위협 요인

- 네트워크 연결 및 폐쇄망 환경에서의 USB 등 매체를 통한 악성코드 감염 • 확산 가능성
- 시스템 복원 이미지나 악성코드에 감염되어 있던 백업파일의 사용
- 범용 OS, 애플리케이션 및 표준 프로토콜 사용에 따른 보안 위협 - 취약점 등
- OS 패치 미적용 단말에 대한 알려진 취약점 악용 공격
- 제한된 시스템 자원 환경에서 보안 솔루션이 리소스를 과다 사용하여 가용성 침해

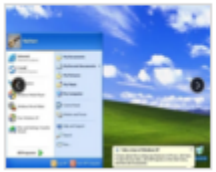
취약한 운영 환경(1/2)

AhnLab

운영되는 어플리케이션의 호환성, 기술지원 이슈 등으로 지원 종료 된 운영체제를 사용

호주 병원, 윈도XP 바이러스 감염돼 대혼란

[2016.01.26]



호주 멜버른의 가장 큰 병원에서 사용되고 있는 컴퓨터 네트워크가 바이러스에 감염돼 병원 컴퓨터가 마비되는 사태가 발생했다. 이 때문에 병원의 검사 기록 등 많은 작업이 수동으로 이뤄지는 등 병원과 환자들이 큰 혼란을 겪었다. 26일 기가진에 따르면 최근 로얄 멜버른 병

Tags 윈도XP, 바이러스

"윈도서버 2003 종료...기술지원 연장 없다"

[2015.04.13]

"오는 7월15일로 종료되는 윈도서버 2003의 기술 지원의 연장 계획은 없으며, 최신 버전인 '윈도서버 2012 R2'나 'MS Azure'로 업그레이드해야 한다." 마이크로소프트(MS)가 윈도서버 2003의 지원 종료를 약 100일을 앞두고 아·태평양 지역의 기업들에게 이 같은 대처를 권장하

Tags MS, 마이크로소프트, 윈도서버 2003

1년전 단종된 윈도XP, 여전히 OS시장 2위

[2015.04.03]

1년 전 공식적으로 사망 선고를 받은 윈도XP가 여전히 녹록치 않은 인기를 누리고 있다. 윈도10 출시를 앞둔 마이크로소프트(MS) 입장에선 적잖은 고민거리다. 윈도XP가 운영체제(OS) 시장 점유율 16.9%를 기록하면서 윈도7에 이어 2위에 랭크됐다고 씨넷이 2일(현지 시

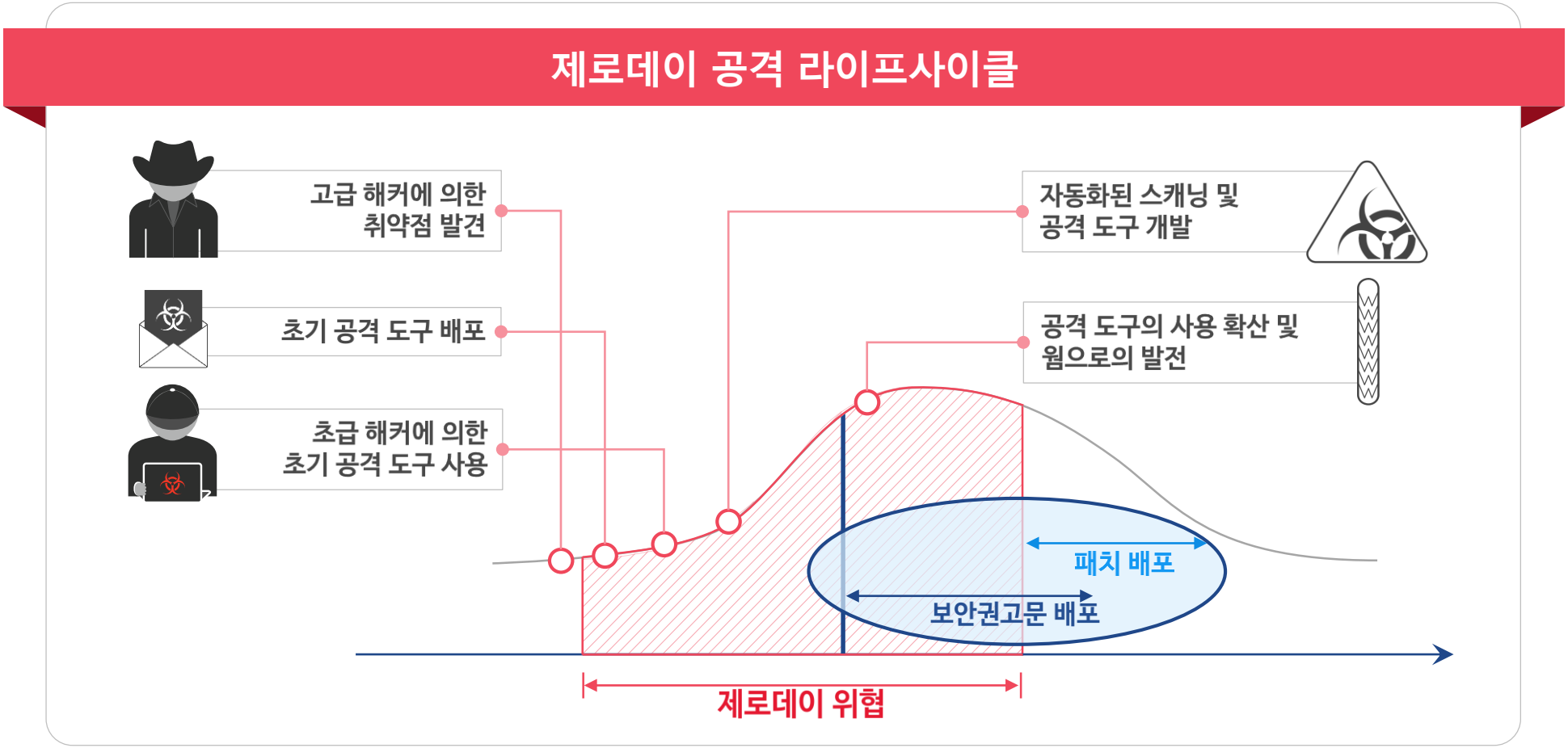
Tags 윈도XP, MS, 운영체제, 넷애플리케이션즈

자료출처: 지디넷(www.zdnet.co.kr)

취약한 운영 환경(2/2)

AhnLab

패치 미적용에 따른 실질적 제로데이 공격의 피해 가능



Solution

More security,
More freedom

AhnLab

보호대책 적용이 어려운 환경

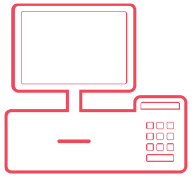
AhnLab

일반적인 보호대책 적용 시 어려움을 겪을 수 있고, 실 운영 환경에서 주요 정책 적용을 하지 못해 효과성을 보장할 수 없는 환경

- 사용하는 애플리케이션이 명확함
- 특정 애플리케이션을 이용해 제한적인 기능만 수행
- 수십~수백 대의 시스템 대비 관리자 부족, 효율적인 관리 불가
- 저사양 장비에서의 제어 시스템 운용에 따른 제한된 시스템 자원
- 폐쇄망 환경에서의 보안 솔루션 운용의 어려움

일반 PC vs 산업용 단말

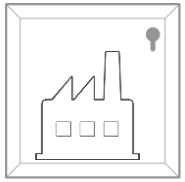
VS



일반 PC		산업용 단말
높은 시스템 자원 사용 편의성 우선 인터넷 접근 용이	Environments 운영 환경	제한된 시스템 자원 인터넷 접근 불가 가용성 우선
주기적인 SW 패치 주기적인 보안 제품 업데이트 불특정 다수의 애플리케이션 사용	Requirements 요구 사항	다운타임 최소화 제한된 애플리케이션 사용 요구

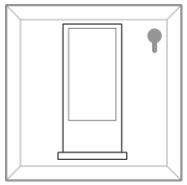
요구되는 보호대책의 주요 기능

AhnLab



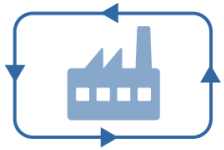
설비제어

POS



KIOSK

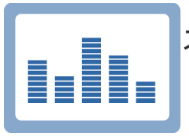
기타



중단 없는 가동

응용프로그램 사용 제한

저사양 시스템



전체제어 시스템의 통합관리

보안 사고 및 장애로 인한 가동중단이 없어야 한다

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

정해진 프로그램만 사용할 수 있도록 하고 싶다

- 불필요한 프로그램의 실행을 막아 시스템 안정성 유지
- 사용하는 포트 이외에는 모두 막아 효율성 및 보안성 향상

시스템 사양이 낮은 장비이므로 리소스 점유가 적어야 함

- 낮은 사양의 CPU, Memory 에서도 동작
- 적은 용량의 Hard Disk, 오래된 OS에서 도 동작

관리대상 단말의 상황을 한눈에 파악하고 싶다

- 이상 현상을 보이는 단말의 빠른 확인
- 문제가 있는 관리대상 단말에 대한 빠른 조치 및 통합 보안 로그 관리

적용 가능한 솔루션

AhnLab

화이트리스트 기반 기술(Positive Security Model)을 사용하여 위협을 효과적으로 차단

화이트리스트 기반의 제어단말 전용 보안	VS.	블랙리스트 기반의 기존 보안 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
업데이트가 필요한 경우 정기적인 제어 시스템 점검 시 스케줄링 가능	업데이트/패치	주기적인 업데이트/패치 적용으로 다운타임 발생

Case Study

More security,
More freedom

AhnLab

사례(1/3)

AhnLab

높은 신뢰도가 요구되는 제조사 생산라인의 산업용 단말 적용 사례

도입 배경

- 지속적인 악성코드 감염
- 컨피커 웜 감염으로 생산 설비 운영 차질
- 저사양 PC에 일반 AV 솔루션 적용 어려움
- AV 솔루션의 오진 가능성 우려
- 시스템 OS 업데이트 시 시스템 리소스 부담

제조사 요구사항

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

도입 효과

- 전체 생산 라인의 중앙 집중 관리 가능
- 화이트리스트 기반의 사전 방역
- OS 업데이트 최소화
- 오진 사고 확률 제거
- 저사양 PC까지 보안 대응책 적용

※ 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.

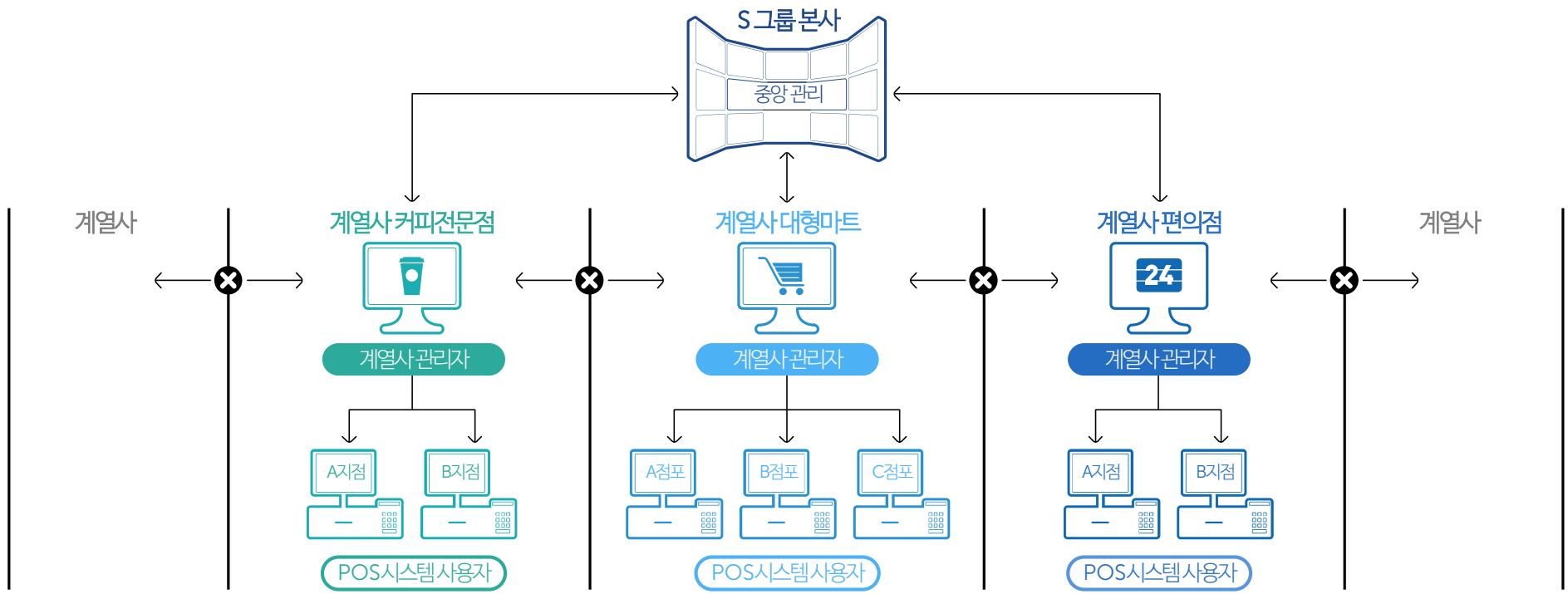
사례(2/3)

AhnLab

A 유통기업은 해킹, 악성코드, 비인가 소프트웨어 설치 및 POS 시스템 오남용 방지 등을 위해 대형마트, 백화점, 커피전문점 등 계열사 만여 대 이상의 POS 단말기에 적용

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

A 유통기업 의 도입 사례



사례(3/3)

AhnLab

항공편 정보를 제공하는 산업용 단말 적용 사례

도입 배경

- Embedded OS를 사용하는 공항 시스템에 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

요구사항

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

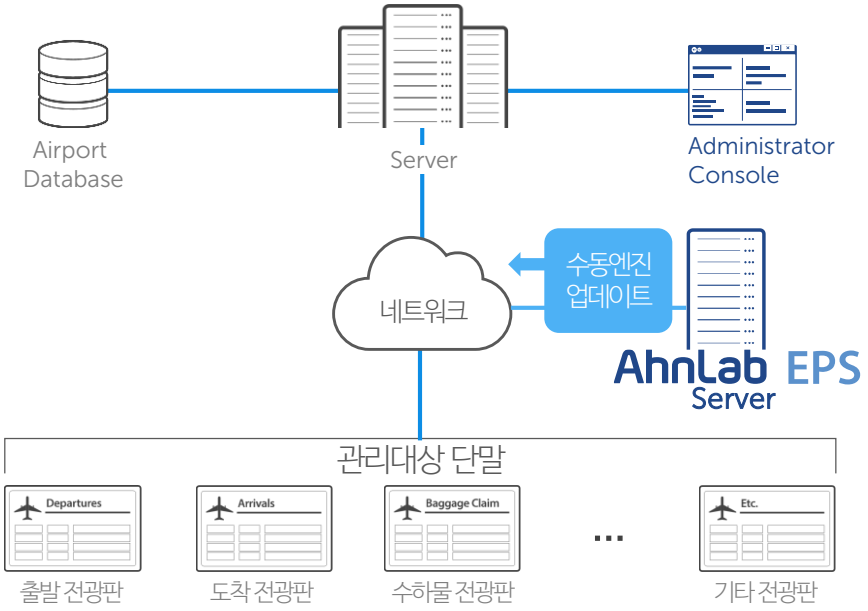
구성도 및 도입 효과

강력한 보안 체계 구축

- 애플리케이션 제어: 필수 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



Product

More security,
More freedom

AhnLab

AhnLab EPS(Endpoint Protection System)

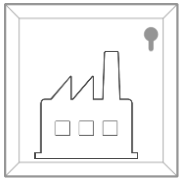
AhnLab

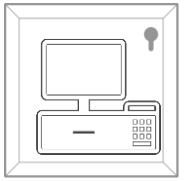
EPS는 **한정된 목적으로 사용하는, 산업용 단말**을 **화이트리스트 기반의 기술**을 사용하여 보호하는 단말보안솔루션

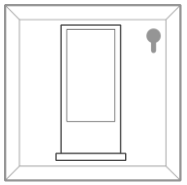
악성코드
형상관리 실패
비인가 소프트웨어의 사용
내부사용자의 오남용
사용자의 실수

AhnLab EPS

- ✓ 단말 환경을 고려한 보안기능
- ✓ 악성코드 예방 & 탐지
- ✓ 어플리케이션 화이트리스팅
- ✓ 운영 편의성, 신뢰성


설비제어


POS


KIOSK


기타

산업용 단말 보안을 위하여 최적화 된 검증 된 제품

AhnLab

✓ POS, 설비제어, KIOSK 등 산업용 단말을 안전하게 운영하기 위하여,
✓ 분야 별 TOP 기업들이 도입하고, 안정적으로 운영하고 있는 제품

검증 되고, 지속적으로 개선되는 제품	* 분야 별 TOP 기업들이 도입하여 검증 된 제품 (수십만 대 이상의 단말에 적용)
	* 2010년 출시 이후 지속적으로 개선되어 온 제품 및 지원 (구, TrusLine)
단말 운영 환경에 최적화된 기능 제공	* 낮은 네트워크 대역폭 환경 등 제한된 운영 환경을 고려
	* 관리대상 자산의 식별로부터, 안전한 운영을 위한 위협 대응 기능까지. 최적화된 기능 제공

More security, More freedom

AhnLab