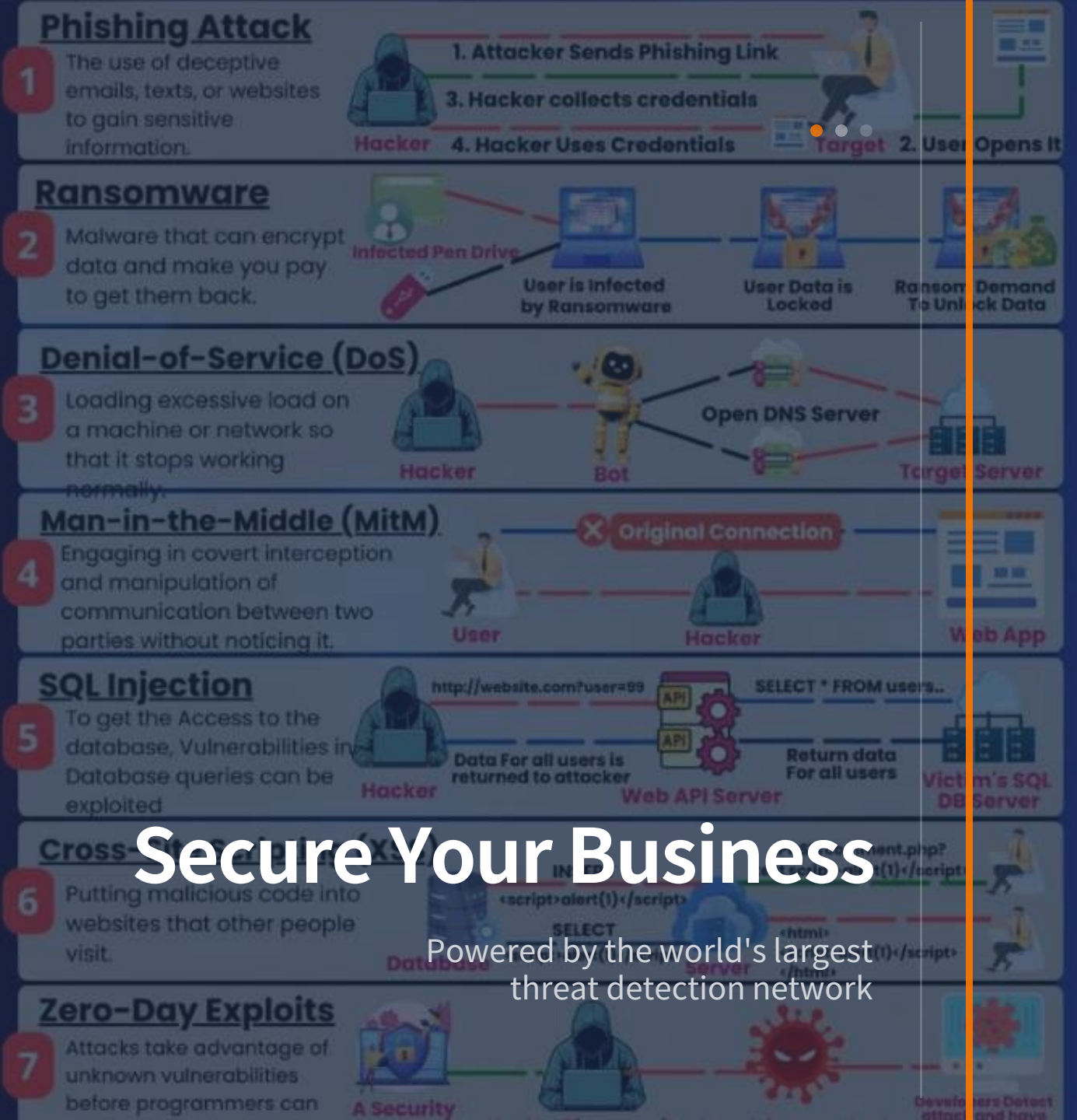




Avast Business 제안서

SMB 엔드포인트 보안 및
데이터 보호 통합 제안

- ☰ 판매사: (주)소프트메일
- ☎ 연락처: 02-3486-9220
- 👤 이메일: sales@avastkorea.com



Secure Your Business

Powered by the world's largest
threat detection network

Table of Contents

- 01 Gen Digital 회사 개요
- 02 시장 현황 및 보안 위협 트렌드
- 03 Avast Business 솔루션 개요
- 04 Business Hub 중앙관리 콘솔
- 05 위협 탐지 알림 화면
- 06 제품 라인업 비교
- 07 핵심 기능 및 차별점
- 08 경쟁사 비교 분석
- 09 구현 및 배포 프로세스
- 10 도입 사례 성공 스토리
- 11 가격 정책 및 ROI
- 12 Avast Business Linux 제품 (개요 및 적용사례)
- 13 결론 및 제안

About Us

🎯 Mission & Competency

엔드포인트 및 클라우드 보안 전문 기업으로서, SMB 및 중견 기업에 최적화된 보안 솔루션과 컨설팅을 제공합니다.

⚙️ Major Services

보안 컨설팅 · 솔루션 구축 · 운영 관리(MSP) · 임직원 보안 교육

📁 Key References

금융, 제조, 유통 등 다양한 산업군의 다수 고객사 레퍼런스 보유

🌟 Partnership & Certification

Avast Gold Partner · ISO 27001 인증 · 전문 보안 엔지니어 보유



Gen Digital Company Overview

Gen Digital

(NASDAQ: GEN)

2022년 NortonLifeLock과 Avast의 합병으로 탄생한 글로벌 최대 사이버 보안 기업입니다. 전 세계 5억 명 이상의 사용자를 보호하며 디지털 자유를 선도하고 있습니다.

5억+

Global Users

38억\$

Annual Revenue (2024)

145억

Attacks Blocked / Year

Brand Portfolio

Norton

Avast

AVG

Avira

CCleaner

Global Leadership

#1

Norton

US Consumer Security Market

Top Tier

Avast Business

SMB Endpoint Security

시장 현황 및 보안 위협 트렌드 (2024)

2024년, 국내 랜섬웨어 공격 급증

2024년 4분기 기준, 국내 랜섬웨어 피해 신고 건수는 전 분기 대비 44% 급증했습니다. 특히 보안 리소스가 부족한 중소기업과 제조업이 주요 타겟이 되고 있습니다.

1,899건

2024년 4분기 피해 건수
▲ 44% (전 분기 대비)

421건

제조업 피해 건수 (최다)
생산 라인 중단 위험

19.6%

중소기업 피해 비중
(2024년 3분기 기준)



RaaS(서비스형 랜섬웨어) 확산

RansomHub, Akira 등 랜섬웨어 그룹이 국내 제조업체 및 의료기관을 집중 공격



제조업 타겟 집중

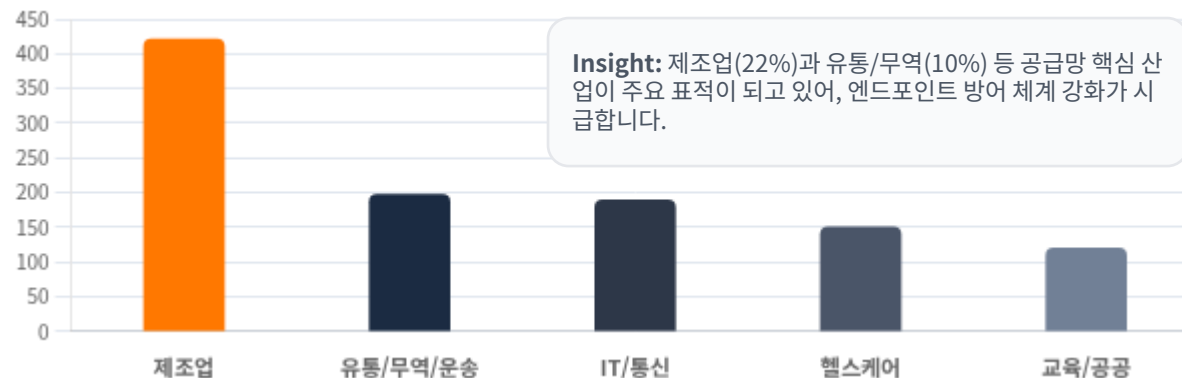
전체 피해의 약 22%가 제조업에 집중, 공장 가동 중단을 필미로 금전 요구



백업/취약점 악용 고도화

미패치된 VPN/서버 취약점을 통한 침투 및 백업 파일까지 암호화 시도

2024년 4분기 산업별 랜섬웨어 피해 현황 (단위: 건)



Avast Business 솔루션 개요

Avast Business Hub를 중심으로, 엔드포인트 보호부터 패치 관리, 데이터 백업까지 단일 플랫폼에서 통합 관리하는 SMB 최적화 보안 솔루션입니다.



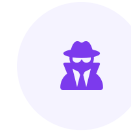
Business Hub (중앙 관리)

클라우드 기반의 통합 콘솔로 언제 어디서나 디바이스 상태 모니터링, 정책 배포, 리포팅 수행



강력한 엔드포인트 보호

수상 경력에 빛나는 차세대 AV 엔진으로 랜섬웨어, 멀웨어, 피싱 등 지능형 위협 실시간 차단



프라이버시 & 네트워크 보호

VPN으로 공공 Wi-Fi에서도 안전한 접속 보장, 웹캠 보호 및 브라우저 정리로 개인정보 유출 방지



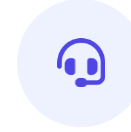
웹 및 디바이스 제어

유해 사이트 접속 차단(Web Control) 및 USB 등 외부 저장 장치 접근 제어로 내부 데이터 보호



자동화된 패치 관리

OS 및 타사 애플리케이션의 취약점을 자동으로 스캔하고 패치하여 보안 홀(Hole) 제거 (Add-on)



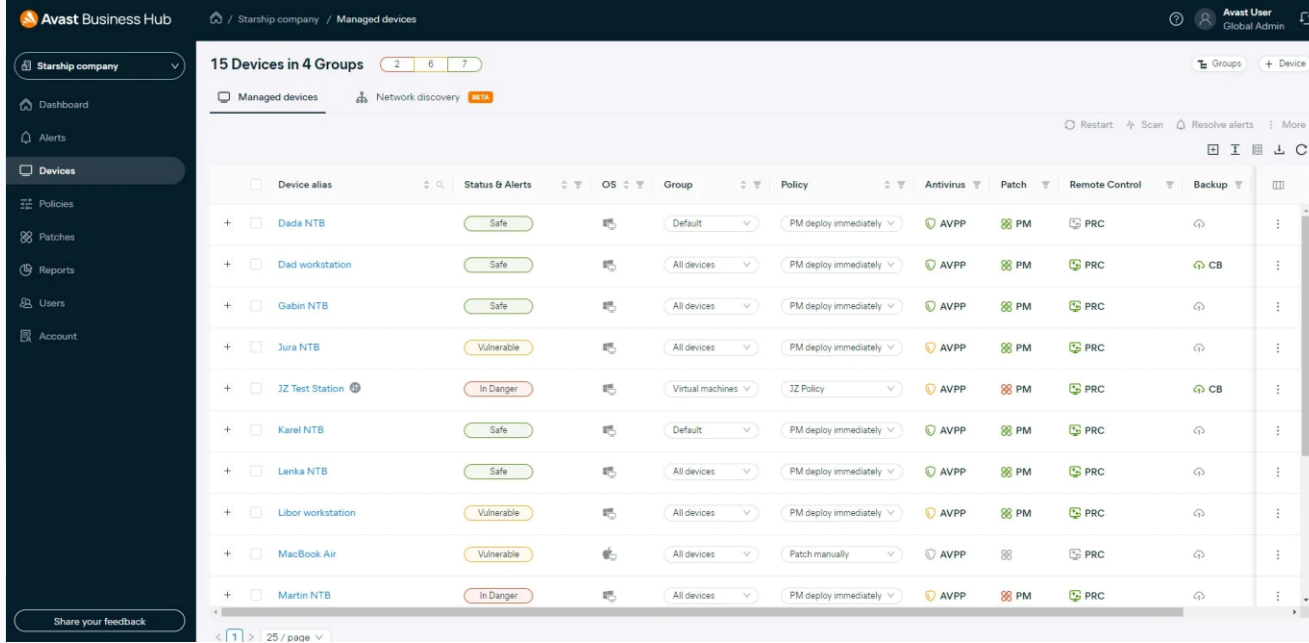
운영 효율성 강화

IT 관리자를 위한 원격 제어 지원 및 랜섬웨어 대비 클라우드 백업 기능 제공 (Add-on)

Avast Business Hub (중앙관리 콘솔)

단일 창에서 모든 보안 운영 통합

클라우드 기반의 Business Hub를 통해 언제 어디서나 디바이스 상태를 모니터링하고, 위협에 즉각 대응하며, IT 운영 효율성을 극대화할 수 있습니다.



1. 다중 지점 관리

본사 + 지점
통합 모니터링

2. 위협 대응 자동화

탐지 → 격리 → 알림
즉시 대응 & 리포트

3. 정기 점검 자동화

주말 → 스캔 → 보고
예약 스캔 및 리포트

주요 관리 기능



직관적 대시보드 & 알림

위협, 디바이스 상태, 라이선스 현황을 한눈에 파악하고 이메일/SMS로 즉시 알림 수신



유연한 정책 & 디바이스 관리

그룹별 보안 정책 설정, 예약 스캔, 재부팅 관리 및 실시간 명령어 실행



상세 리포팅 & 감사 로그

경영진 보고용 요약 리포트 자동 생성 및 운영자 활동 로그 추적



네트워크 디스커버리 & 원격 배포

네트워크 내 연결된 장치를 스캔하여 미보호 장치 식별 및 에이전트 원격 설치



원격 지원 & API 연동

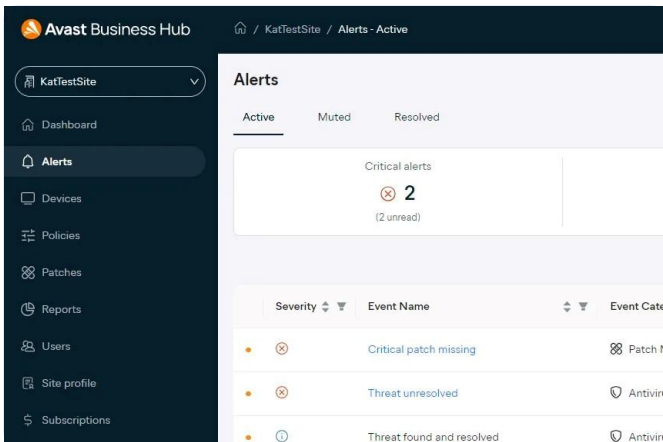
문제 발생 시 즉시 원격 접속(Premium Remote Control) 및 타 시스템과 API 연동



보안 위협 탐지 및 알림 프로세스

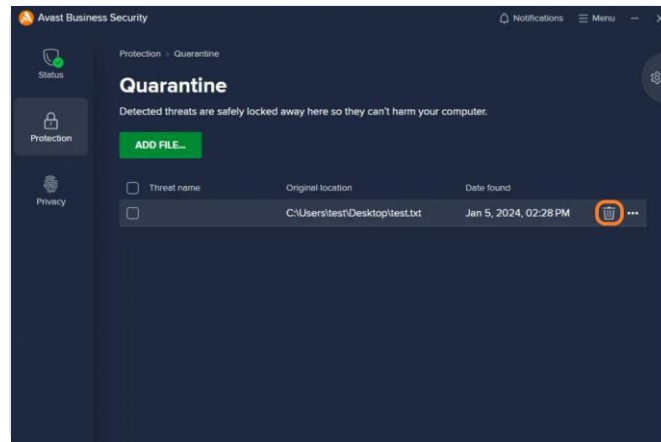
Avast Business Hub는 위협 발생 시 즉각적인 알림을 제공하고, 상세한 위협 정보를 통해 신속한 의사결정과 대응을 가능하게 합니다. 탐지부터 해결까지의 전체 과정을 투명하게 관리하세요.

1 알림 정책 설정



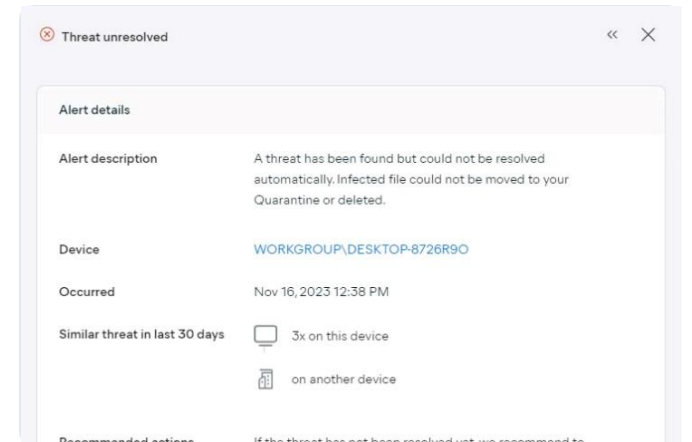
- ✓ 위협 유형별(바이러스, 멀웨어 등) 알림 맞춤 설정
- ✓ 이메일 및 SMS 즉시 발송으로 골든타임 확보
- ✓ 담당자별 수신 대상 지정 및 에스컬레이션

2 위협 탐지 및 분석



- ✓ 탐지된 위협의 상세 정보(파일명, 경로, 유형) 확인
- ✓ 감염된 디바이스 및 사용자 정보 실시간 파악
- ✓ 위협 심각도에 따른 자동 분류 및 필터링

3 대응 및 해결 관리



- ✓ 원클릭 격리, 삭제, 복원 등 즉각적인 조치 수행
- ✓ 조치 이력 자동 기록 및 감사 로그 생성
- ✓ 해결된 위협에 대한 상태 업데이트 및 리포팅

제품 라인업 비교

Features & Pricing	Essential	Premium	Ultimate
	기본적인 엔드포인트 보호	프라이버시 및 고급 보호	패치 관리 포함 통합 보안
	₩60,000 / device / year	₩78,000 / device / year	₩94,000 / device / year
Business Hub (중앙 관리)	✓	✓	✓
엔드포인트 보호 (AV)	✓	✓	✓
랜섬웨어 보호	✓	✓	✓
VPN (프라이버시 보호)	—	✓	✓
USB 보호	—	✓	✓
패치 관리 (Patch Management)	Add-on	Add-on	✓
Specialized Add-ons	Cloud Backup 데이터 보호 및 복구 ₩ 180,000	Linux Antivirus 서버 보안 강화 ₩ 600,000	Patch Mgmt (단독) 취약점 관리 자동화 ₩ 26,000

핵심 기능 및 차별점



클라우드 중앙관리 (Hub)

단일 패널에서 모든 엔드포인트에 대한 가시성을 확보합니다.

- ✓ 다중 사이트 및 역할 기반 접근 제어
- ✓ 원격 배포, 정책 설정, 실시간 경보
- ✓ 직관적인 대시보드 및 상세 리포팅



강력한 예방 보안

알려진 위협과 제로데이 공격을 사전에 차단합니다.

- ✓ 머신러닝 기반 차세대 AV 엔진
- ✓ 랜섬웨어 감지 및 암호화 시도 차단
- ✓ 피싱 사이트 및 가짜 웹페이지 방어



제어 및 거버넌스

사용자 행위와 디바이스 접근을 세밀하게 제어합니다.

- ✓ Web Control: 유해/비업무 사이트 차단
- ✓ USB/매체 제어: 데이터 유출 방지
- ✓ Wi-Fi 취약점 검사 및 보호



운영 자동화 (Patch)

반복적인 보안 작업을 자동화하여 운영 부담을 줄입니다.

- ✓ 수천 개 앱 취약점 자동 스캔 및 패치
- ✓ 우선순위 기반 패치 배포 정책
- ✓ 유지보수 윈도우(시간) 설정 및 재부팅 관리



원격 지원 및 가용성

비즈니스 연속성을 위한 부가 기능을 통합 제공합니다.

- ✓ Premium Remote Control: 실시간 IT 지원
- ✓ Cloud Backup: 데이터 자동 백업/복구
- ✓ 에이전트 하나로 기능 확장 (Add-on)



경쟁력 있는 TCO

SMB 환경에 최적화된 비용 효율성과 성능을 보장합니다.

- ✓ 복잡한 인프라 없이 즉시 도입 가능
- ✓ 시스템 리소스를 적게 차지하는 경량 에이전트
- ✓ 유연한 라이선스 (연간/월간, 기기 단위)

경쟁사 비교 분석

기능별 비교 평가

Avast Business vs 주요 경쟁사 6개 핵심 지표 비교



● Avast Business ● CrowdStrike ● Microsoft Defender ● Sophos

i Avast Business Advantage: 관리 편의성(9.5)과 비용 효율성(9.0)에서 가장 높은 평가를 받았으며, 통합성(8.5) 측면에서도 패치 관리 등 부가 기능 내재화로 우위를 점하고 있습니다.

A Avast Business



Best for SMB

비용 효율성: 숨겨진 비용 없는 투명한 라이선스와 낮은 TCO

✓ All-in-One 통합: EPP + Patch + VPN + USB 제어를 단일 에이전트로 제공, 복잡성 최소화

C CrowdStrike

Enterprise Leader

- + 강력한 위협 탐지 및 대응(EDR) 능력
- 모듈별 과금으로 인한 높은 비용 부담

M Microsoft Defender

OS Integrated

- + Windows 및 M365 환경과의 완벽한 통합
- Mac/Linux 등 이기종 환경 관리의 어려움

S Sophos

Network Focus

- + 방화벽 등 네트워크 보안 제품과의 연동성
- 무거운 에이전트로 인한 시스템 리소스 점유

Avast Business Hub 지원 OS

윈도우 PC 10/11, Mac, 윈도우서버 2016,2019,2022,2025 (윈도우 7/8. 윈도우서버 2008R2 EOL 예정)



Fast Track: 클라우드 중앙 관리 콘솔(Business Hub)을 통해 **평균 1주 이내**에 전체 배포 완료가 가능합니다.

도입 사례 성공 스토리



A사 (자동차 부품 제조기업)

ManufacturingEmployees: 150+Devices: 200+

"Avast Business 도입 후 보안 관리 시간이 획기적으로 줄었고, 랜섬웨어 걱정 없이 본업인 생산 활동에만 집중할 수 있게 되었습니다."

- A사 IT 운영팀장

⚠ 도입 배경 (Challenges)

- × 랜섬웨어 감염 사고 발생
생산 라인 PC 감염으로 2일간 공장 가동 중단 위기 경험
- × 패치 관리의 부재
SW 업데이트 수동 관리로 인한 보안 홀 방치 및 인력 부족
- × 통합 관리 도구 부재
본사 및 2개 공장의 PC 상태를 한눈에 파악 불가

✓ 도입 솔루션 (Solution)

Product Avast Ultimate Business Security

엔드포인트 보호 + 패치 관리(Patch Management) 통합 도입으로 보안성과 운영 효율성 동시 확보

Cloud Console

Patch Auto

Ransomware Shield

📈 정량적 성과 (Key Results)

-95%

보안 사고 감소

악성코드/피싱 유입 차단

70%

관리 시간 절감

패치 자동화로 수동 작업 제거

40%

운영 비용 절감

TCO 개선 및 중복 투자 방지

Before vs After Comparison

● 도입 전 (Before)

- 👤 패치 관리
개별 PC 수동 업데이트 (월 20시간 소요)
- 👁 가시성
각 공장별 보안 상태 확인 불가 (블라인드 스팟)
- 🛡 대응 속도
사고 발생 후 사후 대응 (평균 48시간)

● 도입 후 (After)

- ✍ 패치 관리
중앙 콘솔 자동화 (월 1시간 미만)
- 🔍 가시성
단일 대시보드에서 전사 현황 실시간 모니터링
- ⚡ 대응 속도
실시간 위협 알림 및 즉시 차단 (자동 대응)

가격 정책 및 ROI

구독 라이선스 (Subscription)

* 디바이스/연수 기준, VAT 별도 (첫해 할인가 적용 가능)

Essential

기본 엔드포인트 보호

₩ 60,000

/ device / year

- ✓ Business Hub (중앙 관리)
- ✓ Antivirus & Ransomware
- ✓ Data Protection

예상 견적 (100대/1년)

≈ ₩ 6,000,000 이하

Premium

프라이버시 & 고급 보호

₩ 78,000

/ device / year

- ✓ Essential 기능 전체 포함
- ✓ VPN (무제한)
- ✓ USB Protection

예상 견적 (100대/1년)

≈ ₩ 7,800,000 이하

Ultimate

패치 관리 포함 통합 보안

RECOMMENDED

₩ 94,000

/ device / year

- ✓ Premium 기능 전체 포함
- ★ Patch Management (포함)
- ✓ 취약점 자동 스캔 및 패치

예상 견적 (100대/1년)

≈ ₩ 9,400,000 이하

Available Add-ons:

Patch Mgmt

Cloud Backup

Premium Remote Control

순효과 (Net Benefit) = (A + B) - 비용

A) 사고 감소 효과:

(연간 예상 사고건수 × 평균 피해비용) × 감소율

B) 운영 효율:

(월간 보안/패치 소요시간 절감 × 인건비) × 12

사고 위험 저감



랜섬웨어 및 피싱 선제적 차단

운영 시간 단축



패치 및 배포 자동화 효과

가용성 확보



다운타임 최소화 및 비즈니스 연속성



Avast Business Antivirus for Linux

⚠ 왜 Linux에 백신이 필요한가?

"리눅스는 안전하다"는 더 이상 사실이 아닙니다. 클라우드 및 서버 환경의 확산으로 리눅스를 타겟으로 한 공격이 급증하고 있습니다.

Vulnerability Surge

1,117% ▲

2024년 Linux 커널 취약점(CVE) 급증 (전년 대비)



Ransomware Attacks

62% ▲

Linux 서버 대상 랜섬웨어 공격 시도 증가율



Cross-Platform Risk

Gateway Threat

리눅스 서버가 윈도우 클라이언트로 악성코드를 전파하는 '숙주' 역할 수행 가능성



“ Linux 악성코드는 더 이상 실험적인 것이 아니라, 실제 비즈니스에 치명적인 위협이 되고 있습니다.

Avast Business Antivirus for Linux

엔터프라이즈급 리눅스 서버 보안 솔루션

Starting at
₩ 600,000
/ device / year



Core Scanner

실시간 멀티스레드 스캔 데몬으로 시스템 성능 저하 없이 악성코드 탐지



CommunityIQ

4억 명 이상의 사용자로부터 수집된 실시간 위협 인텔리전스 활용



Command-line Scan

유연한 CLI 지원으로 스크립트 및 자동화 작업에 쉽게 통합 가능



File Server Shield

Samba 및 NFS 공유 폴더 실시간 감시로 윈도우 클라이언트 보호

Supported Distributions (x64)

Red Hat (RHEL) 7+

CentOS 7+

Ubuntu LTS 16.04+

Debian 9+

Linux 적용 사례 및 배포 시나리오

Avast Business Antivirus for Linux는 다양한 서버 환경에 유연하게 적용 가능하며, 특히 혼합 OS 환경(Windows 클라이언트 + Linux 서버)에서의 악성코드 확산을 효과적으로 차단합니다.



1. 웹/애플리케이션 서버

Apache, Nginx, Tomcat 등

웹 취약점을 통해 업로드되는 웹셸(Webshell) 및 악성 스크립트를 실시간으로 탐지하여 서버 장악을 방지합니다.

핵심 보호 대상

웹 루트 디렉토리 (/var/www), 업로드 폴더, 임시 디렉토리 (/tmp)

권장 정책: 실시간 감시(On-Access) + 업로드 폴더 집중 스캔



2. 파일/Samba 서버

NAS, File Server, FTP

Windows 클라이언트가 접속하는 공유 폴더를 감시하여, 리눅스 서버가 윈도우 악성코드의 숙주가 되는 것을 차단합니다.

핵심 보호 대상

Samba 공유 디렉토리, FTP 업로드 경로, 사용자 홈 디렉토리

권장 정책: 실시간 감시 + 주말 전체 검사(Full Scan)



3. 데이터베이스 서버

MySQL, PostgreSQL, Oracle

DB 서버의 OS 영역을 보호하고, 랜섬웨어가 데이터 파일을 암호화하려는 시도를 사전에 차단하여 가용성을 확보합니다.

핵심 보호 대상

OS 시스템 영역 (/bin, /sbin), DB 엔진 실행 파일 (데이터 파일 제외)

권장 정책: OS 영역 실시간 감시 + 데이터 폴더 예외 처리



4. 개발/CI/CD 환경

Jenkins, Git, Container Host

오픈소스 라이브러리나 외부 저장소에서 유입되는 악성코드를 빌드 단계에서 검사하여 공급망 공격(Supply Chain Attack)을 예방합니다.

핵심 보호 대상

소스코드 저장소, 빌드 아티팩트 저장소, 컨테이너 이미지

권장 정책: Command-line Scan을 CI/CD 파이프라인에 통합

국내 파트너 네트워크



어베스트코리아 / (주)소프트메일

Gen Digital의 한국 유일 공식 총판사

Customer Center
02-3486-9220

- 라이선스 공급
- 기술 지원 (Technical Support)
- 리셀러 및 파트너 관리

주요 전략 파트너

KT Telecommunication

통신 인프라 연동 및 결합 상품 제공

S1 Physical Security

물리 보안과 결합된 융합 보안 서비스

ICTIS IT Solution

IT 인프라 구축 및 보안 솔루션 통합

클라우드/호스팅 파트너

Cafe24 E-Commerce

호스팅 이용 고객 대상 보안 서비스 제공

NAVER Cloud Cloud Platform

클라우드 마켓플레이스 입점 및 협력

Avira SDK 파트너 및 더 많은
유통 파트너...

협력 분야

조달 및 공공 시장

나라장터 등록 및 공공기관 대상 보안 솔루션 공급
파트너십

MSP (Managed Service)

고객사 보안 관제 및 운영 대행 서비스 제공 파트너

교육 및 컨설팅

임직원 보안 인식 교육 및 ISMS 인증 컨설팅 협력

파트너십 문의: sales@avastkorea.com

결론 및 제안

Secure Your Business with Simplicity.

Avast Business는 복잡한 엔터프라이즈 솔루션의 대안으로, SMB 및 중견 기업에게 가장 현실적이고 강력한 보안을 제공합니다.



검증된 보안 성능

글로벌 위협 인텔리전스와 AV-Comparatives 인증을 받은 차세대 보호 기술



자동화된 운영 관리

패치 관리 및 중앙 제어를 통한 IT 리소스 절감 및 효율성 극대화



최적의 비용 효율 (TCO)

합리적인 라이선스 정책과 낮은 도입 장벽으로 최대의 투자 가치 실현

Recommended Next Steps

▶ 30일 무료 체험 (PoC) 01

최대 100대 디바이스까지 전체 기능을 실제 환경에서 검증해보세요.

👤 보안 워크숍 & 설계 02

전문 컨설턴트와 함께 현재 위협을 진단하고 최적의 정책을 수립합니다.

📄 \$ 맞춤형 견적 산출 03

필요한 기능(패치, 백업 등)만 선택하여 최적의 도입 비용을 제안합니다.

🚀 도입 및 기술 지원 04

신속한 에이전트 배포 지원 및 운영자 교육을 통해 안정화를 돕습니다.