EdgeSecure Server

Linux 서버를 위한 AI 기반 안티바이러스 솔루션

탐지에서 보고까지, Linux 서버 보안 운영을 자동화합니다

Linux 서버는 클라우드·온프레미스·프라이빗 클라우드 등 다양한 환경에서 핵심 인프라로 운영되며, 금융·공공·제조·통신 분야에서도 보안 요구가 높아지고 있습니다. 랜섬웨어, 크립토마이너, 백도어 등 주요 위협에 대응하기 위해 예방, 탐지, 자동 조치, 감사까지 이어지는 보안 운영 체계가 필요합니다.

> “AI 기반 탐지 고도화에서 운영 자동화까지,
> Linux 서버 보안 운영을 하나의 흐름으로 연결합니다”

신·변종 위협 대응

시그니처 프리 AI 탐지

파일 특징값·구조적 패턴을 분석으로
변형·신종 위협 대응력을 높입니다.

정책 기반 조치

자동 격리·대응

위협 탐지 시 기본 정책에 따라
자동 격리·삭제 등 후속 조치를 수행합니다.

운영 안정성

승인형 복원

관리자 승인 절차를 거쳐
격리 파일을 안전하게 복원합니다.

자동 보고서 지원

자연어 AI 리포트

탐지 결과와 대응 방향을
자연어 리포트로 요약합니다.

Linux 서버 보안 운영을 체계적으로 통합 관리합니다

EdgeSecure Server는 Manager와 Agent 기반 구조를 통해 다수의 Linux 서버를 중앙에서 관리하는 안티바이러스 솔루션입니다. 관리자는 단일 콘솔에서 정책 설정, 탐지 결과, 자동 조치, 복원 승인, 감사 이력을 통합 관리할 수 있습니다.

주요 보안 운영 과제

- **예방·탐지 기준 관리**
  서버별 감시 경로, 예외 정책, 탐지 민감도, 조치 기준이 개별 관리되면 보안 정책의 일관성을 유지하기 어렵습니다.
- **탐지 결과 해석 부담**
  탐지 로그만으로는 위협의 원인, 위험도, 조치 우선순위를 빠르게 판단하기 어렵습니다.
- **조치 판단 지연**
  격리, 삭제, 복원 여부를 결정할 때 보안 대응과 서비스 안정성을 함께 고려해야 합니다.
- **감사 증적 관리**
  탐지 이력, 조치 내역, 복원 결과를 체계적으로 기록하고 증명해야 합니다.
- **망분리 환경 대응**
  폐쇄망 및 네트워크 단절 상황에서도 정책 기반 보호와 이력 관리가 유지되어야 합니다.

EdgeSecure Server 핵심 운영 기능

자율 동작 파이프라인

위협 탐지 후 사전 정의된 정책에 따라 자동 격리·삭제 등 후속 조치로 이어지는 대응 흐름을 지원합니다.

2단계 판정 구조

오프라인 경량 분석으로 1차 판정 후, 필요 시 분석 서버 기반 심층 분석을 통해 판정 신뢰도를 보강합니다.

승인형 복원

관리자 승인 절차를 거쳐 격리 파일을 안전하게 복원할 수 있도록 지원합니다.

감사 이력 자동 기록

탐지·조치·복원 이력을 자동으로 기록하여 보안 운영 및 감사 대응 자료로 활용합니다.

오프라인 보호 및 TLS 암호화

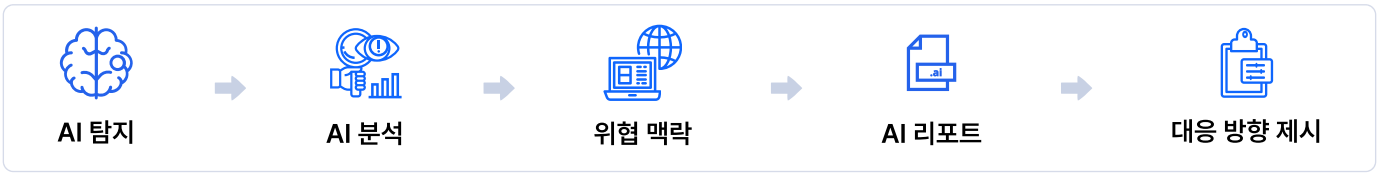
네트워크 단절 환경에서도 정책 기반 보호를 유지하고, 관리 통신 전반에 TLS 100% 암호화를 적용합니다.

중앙 관리 구조

Manager Console	Central Management Server	Linux Agent	Linux Server
정책 설정·모니터링	정책 배포·로그 수집	탐지·조치 수행	보호 대상 서버

AI가 탐지하고,
자연어 리포트로 설명합니다

EdgeSecure Server는 파일 특징값과 구조적 패턴을 AI 모델로 분석해 악성 가능성을 판정합니다.
탐지 결과는 자연어 AI 리포트로 요약되어 위협 원인, 기술 분석, 대응 방향을 빠르게 이해할 수 있도록 지원합니다.



탐지 방식 비교

기존 시그니처 방식
Signature-based Detection

- 등록된 해시·패턴 기반 탐지
- 시그니처 업데이트 의존
- 알려진 위협 식별 중심
- 미등록·변형 위협 탐지 제한 기능

vs

EdgeSecure AI Model
Signatureless

- 파일 특징값·구조적 패턴 분석
- 학습된 AI 모델 기반 판정
- 변형·신종 위협 탐지 대응력 확대
- 판정 근거를 자연어 AI 리포트로 연결

실제 비교 지표

항목	AI Model (Signatureless)	기존 시그니처 방식
ELF 탐지율 Linux 실행 파일 · 1,056개	**99.24%** ↑23.7%p 1,048 / 1,056	75.57% 798 / 1,056
처리 시간 전체 데이터셋 기준	**37.2s** 22.8배 빠름	847.5s 14분 7초
처리 속도 (Throughput)	**99.5 MB/s**	4.5 MB/s
메모리 사용량 (최대/평균)	**558 MB / 386 MB**	1,782 MB / 1,496 MB

※ 테스트 조건: MalwareBazaar daily bulk 데이터셋 기준, 2025.10.29~2025.11.05, 총 1,757개 샘플(PE 701개 / ELF 1,056개) 대상. 기존 시그니처 기반 탐지는 ClamAV 기준.
정상 샘플 오탐 테스트는 프로덕션 시스템 파일 10,000개(Windows PE 5,000 / Linux ELF 5,000) 기준.

AI 리포트 생성 흐름

탐지 정보
악성 여부 · 신뢰도 · 위협명

→

분석 근거
파일 특징값 · 구조적 유사성 · 유사 샘플

→

자연어 AI 리포트
위협 요약 · 기술 분석 · 대응 방향

Server Endpoint Security

EdgeSecure Server

시스템 사양 (최소/권장)

Manager

CPU	4 Core / 8 Core 이상
RAM	12 GB / 16 GB 이상
SSD	100 GB / 500 GB 이상 (로그 보관 기간에 따라 조정)
네트워크	1 Gbps 이상

Agent

CPU	2 Core / 4 Core 이상
RAM	2 GB / 4 GB 이상
SSD	5 GB / 10 GB 이상
아키텍처	x86_64 / ARM64 (aarch64)

필수 환경 및 지원 OS

Manager 필수 환경

- Linux 64비트
- Docker Engine 20.10 이상
- Docker Compose v2 이상

Agent 지원 OS

- RHEL 8 / 9+
- CentOS 8 / 9+
- Rocky Linux 8+
- Oracle Linux 8+
- Debian 10+
- AlmaLinux 8+
- Ubuntu 18.04 LTS+

문의처

EMAIL
bmckorea@comtec.ai.kr

PHONE
010-3756-2530

WEB
www.comtec.ai.kr