시큐어존 SecureZone v11

영역 암호화 기반 단말기 데이터 유출 방지 솔루션

시큐어존 v11 Brochure

산업기술 유출의 70%는 내부자 소행 — 영역 암호화와 반출 통제로 단말기 데이터 유출을 원천 차단함.

[도입 목적] 기업·기관이 시큐어존을 도입해야 하는 이유

23조원	70%	127건	100+
최근 5년 산업기술 유출 경제 피해 규모	산업기술 유출 중 내부자 비중	2023년 산업기술 유출사범 검거	시큐어존 보안 기능 수

- **내부자 데이터 무단 반출 차단 :** 퇴직 예정자·임직원이 USB·개인 메일·클라우드로 기밀 설계도면·소스코드를 무단 반출하는 행위를 영역 암호화(Virtual Secure Drive)로 원천 봉쇄함.
- **기존 DRM 한계 극복 :** API 후킹 방식 DRM의 App 버전 충돌·유지보수 비용 문제 해소. 디스크 영역 암·복호화로 어떤 Application 버전에서도 동작하며 설치 30분 내 완료함.
- **AI 플랫폼·외부 채널 유출 차단 :** ChatGPT·Copilot 등 외부 AI 플랫폼 접속 URL 기준 통제, 파일 업로드 용량·확장자 제한으로 기밀 데이터의 AI 학습 유입을 방지함.

[특장점] 시큐어존 v11이 경쟁 솔루션과 다른 핵심 우위

01
ENCRYPTION

차세대 영역 암호화

- 디스크 영역(Virtual Secure Drive) 기반 암·복호화
- App 버전·종류에 무관하게 동작, 소스코드 수정 불필요
- 국정원 KCMVP 암호모듈 탑재 인증 제품
- 설치 30분 내 완료, 유지보수 비용 최소화
- Web.xml·JDBC 드라이버 변경 없이 즉시 적용 가능

02
ONE-PLATFORM

통합 단일 플랫폼

- One Agent · One DB · One Manager 구조
- 솔루션별 관리 충돌·비용 과다 문제 완전 해소
- 최소 1명 인력으로 전사 보안 통합 관리 가능
- 재택·원격근무 환경에서도 완벽한 보안 지원
- 업데이트 시 충돌 발생 완화, 플러그인 경량화

03
AI CONTROL

AI 플랫폼 실시간 통제

- ChatGPT·Copilot URL 기준 접속 차단·허용 관리
- 업로드 파일 용량(MB)·확장자 세분화 제한
- 화이트/블랙리스트 기반 AI 서비스 접근 제어
- 기업 기밀의 AI 모델 학습 유입 원천 봉쇄
- 경로별 폴더 접근 제어로 비인가 데이터 차단

04
EXPORT CTRL

반출 결재·사후 통제

- 에이전트 트레이를 통한 반출 결재 상신
- 관리자 기안 내용·첨부파일 확인 후 승인/반려
- 엔파우치 연계 열람 횟수·기간·열기 암호 설정
- 원본반출 및 암호화반출 형태 선택 가능
- 반출 파일 사후 열람 권한 제어 및 추적 가능

05
COMPLIANCE

규제 준수·감사 체계

- 보안/개인정보 자동 검출 및 상세 리포트 제공
- 감사 로그(Audit) 전과정 기록·증빙 내재화
- 산업기술보호법·개인정보보호법 요건 대응
- 국정원 KCMVP 인증, GS 인증 취득 제품
- AI 로드 파일 내용 감사, 사용자 행위 로그 기록

06
ZERO-TRUST

제로트러스트 기반 정책

- 허가 프로세스만 보안 드라이브 파일 접근 허용
- 전자서명·SHA2 해시 검증으로 위변조 차단
- 에이전트 안전모드 우회 삭제 시도 완벽 방어
- 역할 기반 권한 관리 및 계정 상태별 접근 제어
- 퇴사자 계정 스케줄 기반 자동 데이터 삭제

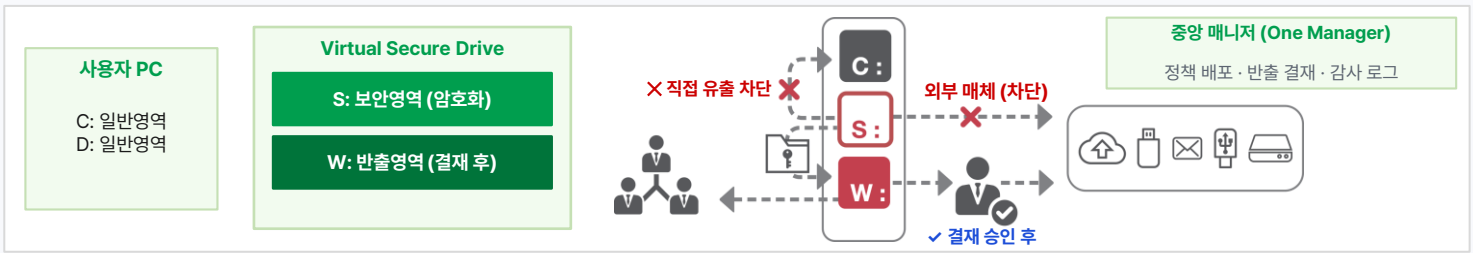
시큐어존 SecureZone v11

영역 암호화 기반 단말기 데이터 유출 방지 솔루션

시큐어존 v11 Brochure

영역 암호화·반출 통제·AI 차단을 One Platform으로 — 설치 30분, 관리 1인, 비용 최소화 실현함.

[제품 구성도] 보안 드라이브 구조 및 반출 통제 흐름



보안영역(S:) 데이터는 허가 프로세스만 접근 가능 · 반출은 반드시 결재 승인 경유 · 외부 매체/클라우드/메일로 직접 유출 원천 차단됨.

[주요기능] 보안 드라이브 및 다층 통제 — 100개 이상의 보안 기능

01 매체 제어 경로별 첨부 통제

- 휴대용 디바이스 접근 거부/읽기/쓰기 할당
- 경로별 파일 첨부 허가 폴더 지정 운영
- 확장자 기반 업로드 파일 차단
- 드라이브 은닉 및 비인가 접근 금지

02 메신저·SW 실행 차단

- 블랙리스트 SW 즉시 실행 차단·경고창
- 에이전트 종료 시 허용 프로세스 강제 종료
- Chrome·Edge 웹브라우저 프로세스 제어
- 전자서명·SHA2 해시값 위변조 검증

03 AI 플랫폼 접속 제한

- ChatGPT·Copilot URL 기준 접속 통제
- AI 사이트 업로드 용량·확장자 제한
- 허용/차단 URL 화이트·블랙리스트 관리
- 기본 폴더 경로 외 접근 원천 금지

04 반출 결재 사후 통제

- 에이전트 트레이로 반출 결재 상신
- 관리자 승인/반려 후 반출 실행
- 엔파우치 연계 열람횟수·기간·암호 설정
- 원본·암호화 반출 형태 선택 가능

05 키워드·개인정보 자동 보호

- 일반 영역 파일 실시간 감시·자동 이동
- 개인정보·보안정보 자동 검출 리포팅
- 보안드라이브 파일 자동 암호화 저장
- 파일 헤더 체크로 확장자 위변조 차단

[조달등록 가격정보] 이노 스마트 플랫폼 v11 — 조달청 등록 제품 단가 현황

(VAT 포함 : 단위 : 원)

모델명	물품식별번호	조달가격
Inno Smart Platform v11, 데이터보안솔루션, 중앙관리매니저	24082290	15,400,000원
nPouch SecureZone v11, 데이터보안솔루션, 1User	24082288	165,000원

※ 상기 가격은 조달청 등록 기준이며, 실제 공급 단가는 사업 규모 및 구성에 따라 별도 협의됨. | 문의: www.innotium.com

[구축 사례] 방산·금융·공공 50여 개 기업·기관 도입 완료

방산 · 대기업	두산에너빌리티, 현대모비스, 현대로템, KAI, HD한국조선해양, LIG넥스원, 한화 에어로스페이스 외
금융기관	현대카드, 현대캐피탈, 현대커머셜, 신한카드, KB증권, KDB산업은행, NH농협생명, 아이엠뱅크 외
공공기관	한국수력원자력, KSD 예탁결제원, 한국전력공사, 국방기술진흥원, 환경부 미세먼지센터, 인천공항공사 외

[보유 인증 및 특허] 국정원 암호모듈(KCMVP) · GS 인증 · 특허 9건

- ✓ 국정원 KCMVP 암호모듈 적용 인증 제품
- ✓ GS 인증 (이노 스마트 플랫폼 v11 · 2020.08.03)
- ✓ 랜섬웨어 대응제품 보안기능확인서 (V3.0 규격)
- ✓ 제로트러스트 보안 지능형 데이터 보안 플랫폼 특허
- ✓ 영역 암호화·백업·워터마크·블록체인 등 특허 9건
- ✓ 조달청 나라장터 등록 · 한국랜섬웨어침해대응센터 운영