# 랜섬크런처 RansomCruncher v11

행위 기반 안티랜섬웨어 · 자동 복구 통합 솔루션

랜섬크런처 v11 Brochure

**랜섬웨어 피해 74조원 시대 — 행위 기반 탐지·자동 롤백으로 비즈니스 연속성을 사수함.**

## [도입 목적] 기업·기관이 랜섬크런처를 도입해야 하는 이유

| 740억$ | 29분 | 2,383건 | 82% |
|---|---|---|---|
| 2026년 글로벌 연간 피해액 | 평균 브레이크아웃 타임 | 2025년 국내 침해사고 신고 | 멀웨어프리(Malware-free) 위협 |

- **선제적 방어 강화 :** 행위·상황 기반 탐지로 시그니처 없는 신종·변종 랜섬웨어를 사전 차단함.
- **데이터 소실 원천 차단 :** 감염 즉시 원본 자동 롤백으로 업무 데이터 손실 0건 보장함.
- **시그니처 백신 한계 극복 :** EDR 킬러·BYOVD 공격에도 자체 보호(Self-Protect) 구조로 보안 무력화 차단함.

## [특장점] 랜섬크런처 v11이 경쟁 솔루션과 다른 핵심 우위

### 01

LAYER 1

#### 지능형 SW 인증

화이트리스트(White-List) 기반 인증으로 비인가 프로세스의 중요 파일 접근을 원천 차단함.

- 신뢰 SW 자동 분류·인증 목록 등재
- 랜섬웨어 의심 SW 감시 목록 자동 등재
- 문서·DB·도면 등 핵심 자산 비인가 접근 차단
- 조직별 업무용 SW 화이트리스트 일괄 적용 가능

### 02

LAYER 2

#### 행위·상황 기반 실시간 탐지

CARB 엔진 기반 0.3초/7회 변조 룰 적용, 커널 레벨 I/O 실시간 모니터링으로 파일리스(Fileless)·신종 공격을 시그니처 없이 사전 차단함.

- 제로데이(Zero-day) 공격 사전 차단
- AI 폴리모픽 변종에도 행위 기반 대응
- 오탐 발생 시 마지막 작업 상태부터 재개

### 03

LAYER 3

#### 순간 백업 · 자동 롤백

데이터 변조 시도 즉시 원본을 안전 영역(대피소)으로 백업하고, 감염 즉시 자동 원상 복구하여 복구 시간을 수주→수분으로 단축함.

- 원본 즉시 백업 → 감염 파일 자동 삭제
- 자동 원상 복구 (별도 운영자 개입 불필요)
- BitLocker 악용 드라이브 암호화 공격 무력화

### 04

LAYER 4

#### 중앙관제 · 자체 보호

One Agent·One DB·One Manager 구조로 전사 정책 통합 운영. 관리자 권한으로도 종료 불가한 자체 보호(Self-Protect)로 EDR 킬러·BYOVD 무력화 차단함.

- 전사 에이전트·정책·예외처리 단일 콘솔 운영
- MBR 부팅 영역 감염 차단 · RDP 시간 기반 통제
- SIEM/SOAR 연계 통합운영 지원

### 05

ONE-PLATFORM

#### 통합 단일 플랫폼

Inno Smart Platform v11 기반 DRM·DLP 연동 충돌 최소화. Windows·Linux, 한·영·중·일 지원으로 멀티환경 완벽 커버하며 운영 부담 최소화함.

- 최소 1명 인력으로 전사 통합 관리 가능
- 재택·원격근무 환경 완벽 지원
- 업데이트 충돌 완화, 플러그인 경량화

### 06

COMPLIANCE

#### 국가 인증 · RanCERT 데이터

국정원 보안기능확인서(V3.0)·GS 인증·NEP 신제품 획득. RanCERT 10년 누적 25,000건 침해 분석 데이터 기반 최적화 행위 탐지·자동 복구 엔진 탑재함.

- 국가용 보안요구사항 V3.0 충족
- 조달청 나라장터 등록 공식 제품
- 방산·금융·공공 90여 개 기관 도입 완료

# 랜섬크런처 RansomCruncher v11

행위 기반 안티랜섬웨어 · 자동 복구 통합 솔루션

랜섬크런처 v11 Brochure

**행위 탐지·순간 롤백·One Platform으로 — 설치 즉시, 운영 최소, 비즈니스 무중단 실현함.**

## [제품 구성도] 4계층 방어 아키텍처 및 자동 복구 흐름

| L1 | L2 | L3 | L4 |
|---|---|---|---|
| **지능형 SW 인증** | **행위·상황 기반 탐지** | **순간 백업·자동 롤백** | **중앙관제 시스템** |
| White-List 기반<br>비인가 프로세스 차단 | CARB 엔진<br>0.3초/7회 변조 룰 | 대피소 백업<br>감염 즉시 원상 복구 | One Manager<br>Self-Protect 구조 |

보안영역 데이터는 허가 프로세스만 접근 가능 · 감염 즉시 자동 롤백 · 외부 침투 경로(RDP·MBR·BitLocker 악용) 원천 차단됨.

## [주요기능] 탐지·차단·복구·통제·관제의 5축 통합 — 단일 에이전트 100+ 보안 기능

### 01 행위·상황 기반 탐지

CARB 엔진 기반 커널 I/O 실시간 감시 · 0.3초/7회 변조 룰 · 파일리스 공격 대응 · 오탐 시 업무 무중단 재개함.

### 02 순간 백업·자동 롤백

데이터 변조 시점 즉시 원본 대피소 백업 · 감염 파일 자동 삭제 · 자동 원상 복구로 데이터 무손실 보장함.

### 03 BitLocker·MBR·RDP 통제

BitLocker 악용 드라이브 암호화 공격 무력화 · MBR 부팅 영역 감염 차단 · RDP 시간 기반 접속 통제함.

### 04 White-List SW 인증

신뢰 SW 자동 분류·등재 · 비인가 프로세스 핵심 자산 접근 차단 · 정책 기반 예외 처리 일괄 적용 가능함.

### 05 중앙 통계·리포팅

에이전트 현황·탐지/차단 이력·접속자·프로세스 로그 통합 대시보드 · SIEM/SOAR 연계 통합운영 지원함.

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

(VAT 포함 : 단위 : 원)

| 모델명 | 물품식별번호 | 조달가격 |
|---|---|---|
| Inno Smart Platform v11, 데이터보안솔루션, 중앙관리매니저 | 24082290 | 15,400,000원 |
| Inno Smart Platform v11, 단말기랜섬웨어탐지/차단보안솔루션, 1User | 24082286 | 55,000 |
| Inno Smart Platform v11, 서버랜섬웨어탐지/차단보안솔루션, 1Server | 24082287 | 800,000 |

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

## [구축 사례] 공공·금융·기업 90여 개 기관 구축 완료

| | |
|---|---|
| 공공· 지자체 | 전라남도청 본청 및 12개 산하기관, 경상남도청·양산시청 통합, 한국철도공사 코레일 전사, 제주특별자치도청 16개 기관, 한국고용정보원 본원·지원 |
| 금융·대기업·제조 | 현대카드, 현대캐피탈, 현대커머셜, 신한카드, KB증권, KDB산업은행, NH농협생명, 아이엠뱅크 외 |

## [보유 인증 및 특허] 국정원 암호모듈(KCMVP) · GS 인증 · 보안기능확인서 · 특허 보유

- ✓ 국정원 보안기능확인서 (랜섬웨어 대응제품 V3.0 규격)
- ✓ GS 인증 1등급 (Inno Smart Platform v11)
- ✓ NEP 신제품 인증
- ✓ 국가용 보안요구사항 V3.0 충족
- ✓ 제로트러스트 기반 지능형 데이터 보안 플랫폼 특허
- ✓ 행위 기반 탐지·백업·롤백 관련 특허 보유
- ✓ 조달청 나라장터 등록 공식 제품
- ✓ 한국랜섬웨어침해대응센터(RanCERT) 자체 운영