가장 안전한 랜섬웨어 대응 솔루션

랜섬쉴드 엔터프라이즈

ESTsecurity

급증하는 신·변종 랜섬웨어, 끊임없는 피해

랜섬웨어 공격 타깃

1대만 감염되어도 조직 전체가 랜섬웨어 공격에 노출

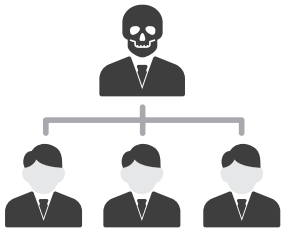
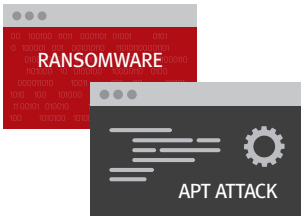
기업 또는 기관의 회계, 재무정보, 영업전략, CAD 설계도면, 사업계획서, 연구자료, 개발소스, 고객 개인정보 등은
훼손 또는 유실 시 치명적일 수 있는 기업의 핵심 정보이자 경쟁력이며 중요한 디지털 자산입니다.

최근 랜섬웨어 공격자들은 기업, 정부기관 등 업종, 규모와 상관없이 가치있다고 판단되는 모든 자료들을 노리고 있습니다.

특히, 보안에 대한 투자가 어려운 중소기업이 전체 피해의 약 60% 이상으로, 랜섬웨어로부터 기업 자산을
어떻게 더 효율적으로 보호하느냐에 따라 기업의 가치가 결정되기도 하는 실정입니다.

랜섬웨어 현주소

신종, 변종 등 다양한 랜섬웨어가 확산되어 전 세계적으로 피해 급증
랜섬웨어 피해 시 디지털 정보 자산 훼손, 업무 중단 등 기업/기관 업무에 심각한 상황 초래

랜섬웨어 서비스화 (RaaS)	글로벌 동시 다발적 공격 형태	특정 표적에 대한 APT 공격
		
랜섬웨어 제작부터 유포까지 수익분배형 랜섬웨어 등장	전 세계 120여개 국가에서 짧은 시간에 급격하게 증가 ※ 워너크라이(WannaCry)	특정 기업을 목표로 한 지능형 지속 위협(APT) 증가

사용자 PC에 대한 지능적이고 다양한 공격방법으로 지속적인 공격 시도

“ 랜섬웨어 위협 비상사태 ”

진화하는 랜섬웨어,
기존의 방어 체계만으로는 한계 존재

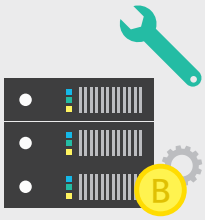
랜섬웨어 대응 한계

예방 수칙 준수, 일반 백업 등의 대응에도 지능화되는 랜섬웨어 공격에 피해 지속 증가

OS 및 SW 최신 업데이트
·
백신 소프트웨어 설치
·
중요 자료 정기 백업
·
출처 불명확한 URL링크 클릭 금지
·
파일공유 사이트 다운로드 주의

기본 예방 활동
기본적인 수준의
사전 예방 활동 수행

백업 솔루션 도입
정기 백업의 어려움으로
백업 누락에 의한 손실 발생



복구 서비스
디스크 HW복구 및 비트코인
지급 대행 서비스 수준

여전히…
랜섬웨어 피해 급증

랜섬웨어 행위 분석과 각 피해 단계별 대응 필요

급증하는 신종, 변종 랜섬웨어에 대비하여 탐지부터 백업까지 보다 효과적이고 체계적인 접근 방식 필요

탐지
- 악성 행위 모니터링
- 패턴 분석

차단
- 랜섬웨어 행위 차단
- 랜섬웨어 DB 등록
- 랜섬웨어 차단 알림

복구
- 훼손 파일 즉시 복구
- 실시간 자동 복구

로컬 백업
- 실시간 사용자PC 백업
- 폴더 보호
- 파일 암호화

클라우드 백업
- 실시간 클라우드 백업
- 관리자 중앙 백업 정책

기존과 차별화된 대응 방안 필요
랜섬웨어 피해 사전 방어 + 신속한 복구

랜섬쉴드

랜섬쉴드로 랜섬웨어 사전 방어와 공격 대상인 데이터 보호를 한번에!

랜섬쉴드의 랜섬웨어 대응 3단계

- 랜섬웨어의 행위를 분석하여 탐지하고 차단하는 랜섬웨어 사전 방어
- PC로컬 백업(1차)과 클라우드 백업(2차)을 통해 유사 시 신속한 파일 복원으로 업무의 연속성 보장

STEP 01
랜섬웨어 방어

랜섬웨어로 **탐지** 시 랜섬웨어 **차단** 및 훼손 파일 바로 **복구**

STEP 02
PC 백업

파일 생성/수정 시 **PC에 실시간 백업**, 필요 시 사용자가 일괄 복원

STEP 03
클라우드 백업

관리자 정책에 따라 **클라우드에 한번 더** 실시간 백업

왜 랜섬쉴드인가?

'랜섬쉴드'는 **보안 전문 기업 이스트시큐리티**가 랜섬웨어 차단 및 문서 보안 기술 융합으로 만든 랜섬웨어 대응 솔루션입니다.

TECHNOLOGY

랜섬웨어를 **잘 차단합니다.**

- 국내 최초 랜섬웨어 차단 기술특허 보유 (특허10-1710918호)
- 랜섬웨어 차단 약 397만 건 이상 (2016년기준)

BIG DATA

랜섬웨어를 **잘 알고 있습니다.**

- 국내 1위 백신 "알약(ALYac)" 기술과 노하우
- 국내 최다 랜섬웨어 활동/수집 정보 보유

FILE PLATFORM

랜섬웨어로부터 **파일을 안전하게 보호합니다.**

- 문서보안 솔루션 등 파일관리시스템 기술
- 국내 최대 규모 구축형 파일서버(클라우드) 운영 기술

SECURITY EXPERT

랜섬웨어 **대응 전문가와 함께합니다.**

- 랜섬웨어 전문가로 구성된 "시큐리티대응센터" 운영
- 국가 정보기관과의 "랜섬웨어 대응 협의체" 구성 (미래부, 국정원 등)

랜섬웨어 차단부터 복구까지, 랜섬웨어 대응 A-Z

랜섬웨어 사전방어

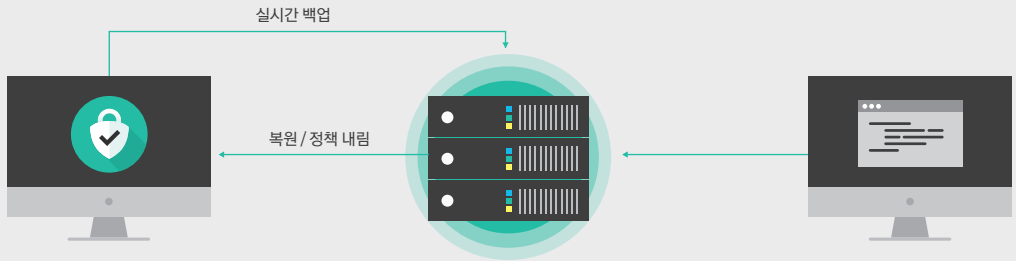
랜섬웨어 행위 차단	랜섬웨어 행위를 감시, 분석하여 차단
훼손 파일 자동 복구	랜섬웨어 공격으로부터 보호할 확장자 지정 가능 파일 훼손 시 원본 파일을 안전한 곳에 별도 보관하여 자동 복구
강력한 시스템 보호	MBR 공격 차단 기능으로 시스템 부트 영역인 '마스터 부트 레코드(MBR)'를 파괴하는 악성 공격 차단

실시간 백업

중요 파일의 실시간 백업	중요 파일의 확장자 지정으로 파일 생성, 수정 시 실시간으로 PC와 클라우드에 백업
쉽고 빠른 복원	백업 파일의 시점 별 버전 관리로, 특정 시점의 전체 파일 일괄 복원 또는 개별 파일의 백업 히스토리에서 원하는 버전 복원 가능
작업 이력 관리 용이	백업된 문서 파일의 문서 탐지, 백업 및 복원 이력 조회 가능 파일의 백업 유무 확인 및 형상 관리, 히스토리 추적에 용이
PC와 클라우드 이중 백업 (클라우드 구축)	사용자 PC 및 클라우드 이중 백업으로 중요 파일을 더욱 안전하게 보호

중앙 관리 기능 (클라우드 구축)

차단, 백업 정책 관리 일원화	관리자가 랜섬쉴드를 설치한 임직원 PC의 랜섬웨어 차단 및 백업 정책 강제 적용 가능
세분화된 정책 수립 및 맞춤 적용	랜섬쉴드의 모든 기능으로 세분화된 정책 수립 사용자/부서별 특성에 따라 개별 정책 적용 가능
사용자 및 조직도 관리	랜섬쉴드 설치 사용자를 조직도 형태로 등록 및 관리 에이전트 설치 및 삭제 권한 관리가 가능
실시간 모니터링	사용자의 중요 문서 탐지 및 백업, 복원, 삭제 등의 내역을 실시간으로 확인 가능



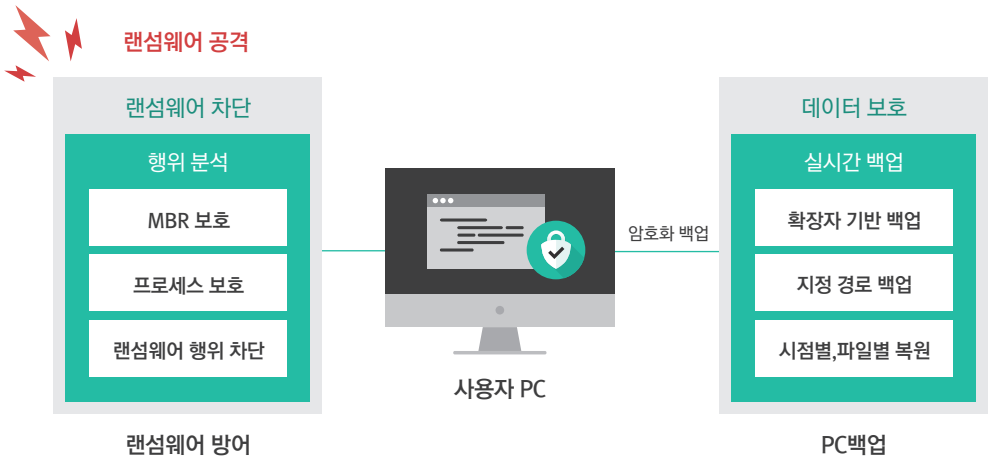
로컬 PC	랜섬쉴드 서버	관리자
랜섬웨어 탐지	확장자 기반 백업 설정	차단, 백업 정책 설정
랜섬웨어 차단	생성/수정 시 실시간 백업	사용자 – 에이전트 관리
훼손파일 자동복구	시점별/파일별 복원	작업내역 실시간 모니터링

랜섬쉴드 도입 시나리오

랜섬웨어 사전차단 + PC백업을 간편하게

랜섬쉴드 기본구성 (랜섬웨어 방어+1차 백업)

랜섬웨어 행위 분석을 통한 사전 차단과 데이터 보호를 위한 PC 백업이 가능한 기본 구성입니다.



추천 대상

랜섬웨어 피해를 예방하기 위해 대응 솔루션을 도입하고 싶지만 리소스에 한계가 있는 기업 및 기관

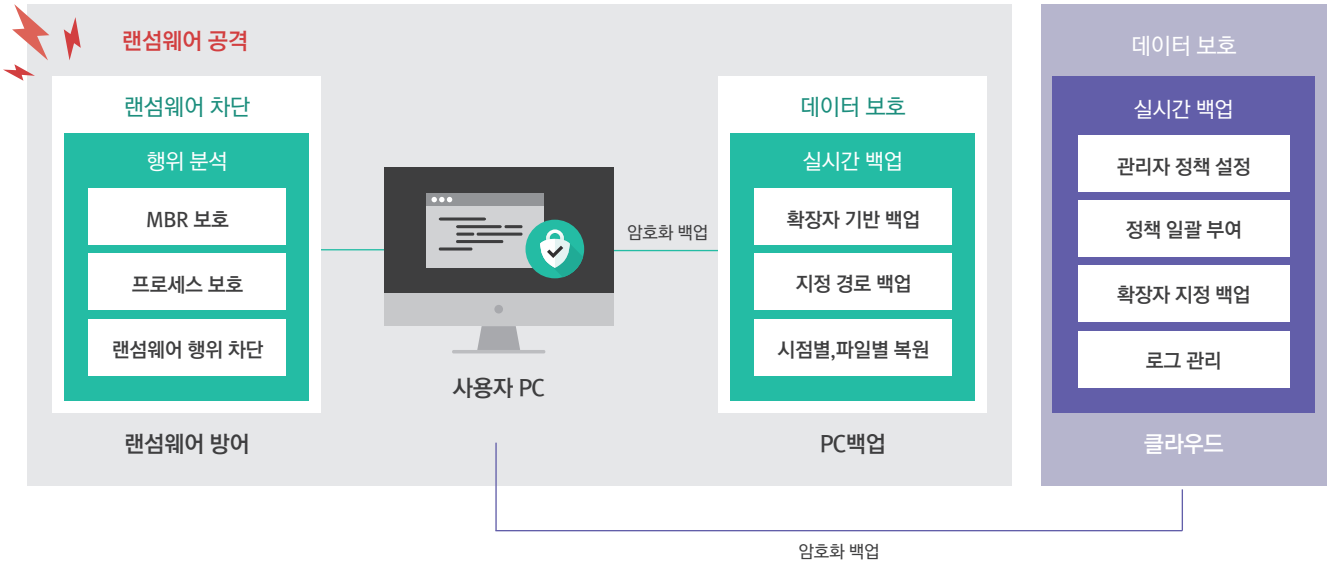
도입 효과

AS-IS	· 랜섬웨어 등 보안 취약 · PC 내 중요 자산 보호 필요	· 데이터 유실로 업무 손실 증가 · 데이터 관리 어려움	· 보안 솔루션 도입 비용의 부담 · 관리 리소스 부족
TO-BE	 **랜섬웨어 완벽대응** 고도화된 랜섬웨어 위협으로부터 중요 자산을 안전하게 보호하여 업무 연속성 보장	 **데이터 보호** 랜섬웨어, 악성코드 공격, 사용자 실수, 퇴사로 인한 데이터 훼손/유실 시 백업된 데이터로 일괄 복원	 **쉬운 도입** 기존 업무환경의 변경이나 관리 리소스, 서버 구축 없이 사용자 설치만으로 쉽게 도입 (기존 보안제품과 충돌 없음)

클라우드 백업으로 더욱 안전하게

랜섬쉴드 클라우드 구축형 (랜섬웨어 방어+PC백업+클라우드백업)

랜섬웨어 행위 분석을 통한 사전 차단과 데이터의 더욱 안전한 보호를 위한 PC/클라우드 이중 백업이 가능하며, 관리자가 중앙 통제 관리할 수 있는 솔루션 구성입니다.



추천 대상

랜섬웨어 및 다양한 유실 가능성에 대비하여 더욱 확실하고 안전하게 통합 보안 환경 구축을 원하는 기업 및 기관

도입 효과

AS-IS	· 랜섬웨어 등 보안 취약 · PC 내 중요 자산 보호 필요	· 데이터 유실로 업무 손실 증가 · 다양한 유실 위협 대응 필요	· 기업 내 데이터 보안 관리 부족 · 안전한 업무 환경 구축 필요
TO-BE	 **랜섬웨어 완벽대응** 고도화된 랜섬웨어 위협으로부터 중요 자산을 안전하게 보호하여 업무 연속성 보장	 **강력한 데이터 보호** 랜섬웨어, 사용자 실수, PC 물리적 훼손, 분실 등 예기치 못한 위협에도 더욱 안전한 클라우드 백업으로 데이터 강력 보호	 **효율적인 통합 관리** 중앙 관리콘솔을 통해 사용자별/부서별로 맞춤 정책을 적용하고, 작업 내역 모니터링 등 효율적인 통합 관리가 가능

회사위치 및 연락처

ESTsecurity · ESTsoft

(우) 06711
서울시 서초구 반포대로 3 이스트빌딩
02.583.4616
www.estsecurity.com