ThinkShield

최전선에서. 실시간으로.
완벽한 사이버 공격 차단

엔드 유저 디바이스들은 데이터 생태계에서 위협에 가장 취약한 부분이 될 수 있습니다. 종래의 안티 바이러스 솔루션에만 의존하는 방식은 진화하는 위협 환경에 대처하는 데 역부족일 수 밖에 없으며, 불필요한 장치 리소스를 소모하게 됩니다. ThinkShield 보안 설계 접근 방식은 사용자를 위한 엔드 투 엔드 보호에서 차별화를 실현합니다.
레노버는 모든 엔드포인트 전반의 다양한 위협 벡터들을 차단하는 솔루션을 제공합니다. 레노버 고객들은 이제 특허받은 행동 AI(Behavioral AI, BAI) 기술로 실시간 차단, Active EDR, IoT 보안, 클라우드 워크로드 보호 기능을 실행하는 SentinelOne이 설치된 디바이스를 사용할 수 있습니다. 업계 최고의 레노버 디바이스에 업계 최강의 엔드포인트 보안 기술을 결합함으로써 단일 에이전트 통합을 통해 사이버 공격에 맞서는 최일선 방어 체계를 강화하여 강력한 보안과 탁월한 사용자 경험을 제공합니다.

공격들은 평균적으로
95일 이상
감지되지 않은
상태로 있습니다.

자율 엔드포인트 보호

SentinelOne은 기존 안티 바이러스를 AI 기반 보호로 대체합니다.

- 장치가 자체적으로 치유되며 자율적으로 클린(clean) 상태로 롤백됨
- 단일 에이전트 모델
- 인터넷 연결 또는 사람의 개입에 전혀 의존하지 않음

자가 치유 ActiveEDR

SentinelOne의 특허받은 행동 AI는 모든 장치 프로세스를 모니터링하고 매핑합니다.

- 시스템 속도로 모든 공격을 중단시키고 교정하는 사전 예방적 조치
- IT 팀에서 이용 가능한 위협 헌팅(threat hunting), 스토리라인 포렌식, 상세한 교정(remediation) 데이터

탁월한 사용 용이성

다수의 장치 에이전트를 하나로 통합한 뒤, 사용자 친화적인 콘솔에서 쉽게 관리할 수 있습니다.

- 제품군의 주요 기능들: 장치 제어, 엔드포인트 방화벽 제어, 애플리케이션 인벤토리, 취약성 매핑
- 관리 대상 여부에 관계없이 모든 네트워크 자산에 대한 가시성

완벽한 통합

ThinkShield의 핵심 부분인 라이센스는 레노버 디바이스와 함께 구매할 수 있습니다.
또한, SentinelOne은 300개 이상의 설정 가능한 API를 제공하며 60개 이상의 네이티브 API를 사이버 보안 및 IT 운영 기술들에 통합했습니다.

SentinelOne™

솔루션에 대한 자세한 내용은 아래 사이트에서 확인하실 수 있습니다.
https://techtoday.lenovo.com/kr/ko/solutions/large-enterprise/thinkshield
https://kr.sentinelone.com/

Smarter technology for all

Lenovo