SentinelOne™

SentinelOne™

데이터시트

Singularity™ EPP+EDR

통합 보호 / 탐지 / 조사 / 대응

전통적인 Anti-Virus 및 EDR 솔루션과 비교하여 가시성, 탐지, 대응,
모든 면에서 진화한 최신 위협 대응 EPP + EDR 솔루션

REAL TIME
엔드포인트 보호

- AI 기반 기술로 위협 탐지/제거
- 클라우드 파일 평판 기술
- 최신위협대응(스크립트, 파일리스 공격)

ACTIVE
분석 & 대응

- 악성파일 활동 상세 분석
- 위협 행위기반 스토리라인(상관분석)
- 위협 제거(네트워크 단절, 원상 복구)

DISCOVERY
엔드포인트 가시성

- 프로세스 / 파일 / 네트워크 모니터링
- 관리되지 않는 Endpoint 탐색, 알림
- 상관 분석을 통한 위협 시각화

보호 단계별 제공 기능

1단계	Prevention	위협 방어	• Static AI 기술을 사용하여 실시간으로 공격을 방어 • 레거시 안티바이러스 제품을 대체함
2단계	Detection	위협 탐지	• Behavioral(행위기반) AI 특허 기술로 악의적인 위협 행동 탐지
3단계	Threat Hunting	위협 분석	• Mitre 프레임워크와 연계한 위협 단계 및 기술정보 제공 • 최신 위협 탐지를 위한 분석 쿼리 제공
4단계	Active Response	위협 대응	• 네트워크 격리, 랜섬웨어를 포함한 모든 위협 제거, 악성코드로 인한 시스템 변경 사항 및 암호화된 파일 복구

One-Click 복구

랜섬웨어 등으로 인해 손상 및 암호화된 파일 복구

KILL
Stop all processes related to the threat

QUARANTINE
Encrypts and moves the threat and its executables

REMEDIATE
Deletes all filles and system changes created by the threat

ROLLBACK
Restores files and configurations that the threat changed

ActiveEDR™ 기반

ActiveEDR은 악성 프로세스가 발생하면 행동 AI로 이를 식별하고, 상관 관계가 있는 이벤트에 태그를 지정하고, 조사를 시각화 및 가속화할 수 있도록 공격 스토리라인을 자동으로 생성합니다. 보호 모드에서 SentinelOne은 공격을 식별할 뿐만 아니라 감염을 자동으로 차단합니다. 그런 다음 관리자는 손쉽게 클릭 한번으로 허가 없이 발생한 모든 변경 사항을 되돌릴 수 있습니다.

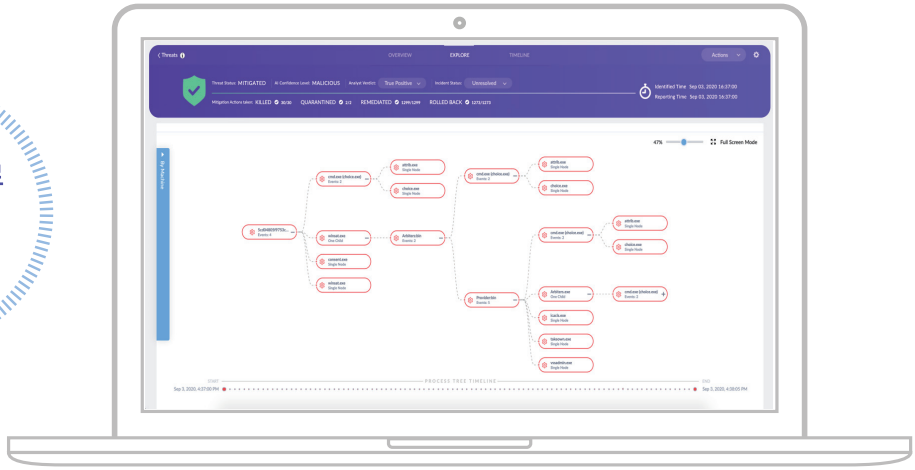
강력한 포렌식, 분석 가속화, 신속한 대응

EDR은 더 이상 소수의 독점 분야가 아닙니다. 위협 체류 시간과 MTTR(평균 복구 시간)을 줄이고 생산성을 극대화하려면 탐지 및 대응 프로세스를 간소화해야 합니다. 데이터 센터, 클라우드 서비스 공급업체, 사무실 또는 원격 근무지 등 모든 환경과 OS에서 전체 이벤트를 AI로 쉬지 않고 모니터링합니다. Deep Visibility는 위협 헌팅 팀이 필요로 하는 모든 포렌식 데이터를 제공합니다.

| 주요 이점 |

* 통합형 자율 EPP/EDR
* Linux, macOS, Windows, 쿠버네티스 및 Docker 플랫폼 지원
* 온라인/오프라인 보호, 탐지 및 대응
* 이벤트 상관 관계를 자동으로 스토리라인으로 구성
* 특허받은 원클릭 교정 및 롤백
* MITRE ATT&CK 프레임워크와 결합된 정보 제공
* 유연한 EDR 데이터 보존 :14일에서 365일까지 연장 가능
* 모든 OS 에 대한 원격 포렌식
* EPP 단일 또는 EDR 결합 라이선스 제공

Storyline™ 으로 분류 및 조사 가속화



외부 평가 결과

ATT&CK®

2021 MITRE ATT&CK

- 누락 건수 최소
- 상관관계 파악 최다
- 데이터 보강 범위 최고

Gartner

2021 MQ EPP 부문

- 매직 쿼드런트 리더로 선정
- 가트너가 정의한 세 가지 고객 유형 모두에서 최고 점수 획득

FORRESTER®

2020 FORRESTER WAVE™ EDR

- 우수 성과 기업

kuppingercole ANALYSTS

2020 KUPPINGERCOLE MARKET COMPASS

- 주요 EPDR 혁신 기업

랜섬웨어 보상 정책

랜섬웨어는 빠르게 진화하고 있으며 새로운 변종은 더 은밀하고 훨씬 더 공격적입니다. 전 세계의 조직은 보호 솔루션을 배포하고 공격의 금융 피해를 최소화하기 위해 분주하게 움직이고 있습니다.

업계를 선도하는 센티넬원은 랜섬웨어 공격이 감지되지 않고 회복할 수 없는 피해를 입히지 않도록 고객에게 보증을 제공합니다.

고객이 파일 복구 비용을 지불해야 하는 경우 센티넬원 랜섬웨어 보증이 적용되는 고객은 Endpoint 당 최대 $1,000 USD, 회사당 최대 $1,000,000 USD 를 보상받게 됩니다.

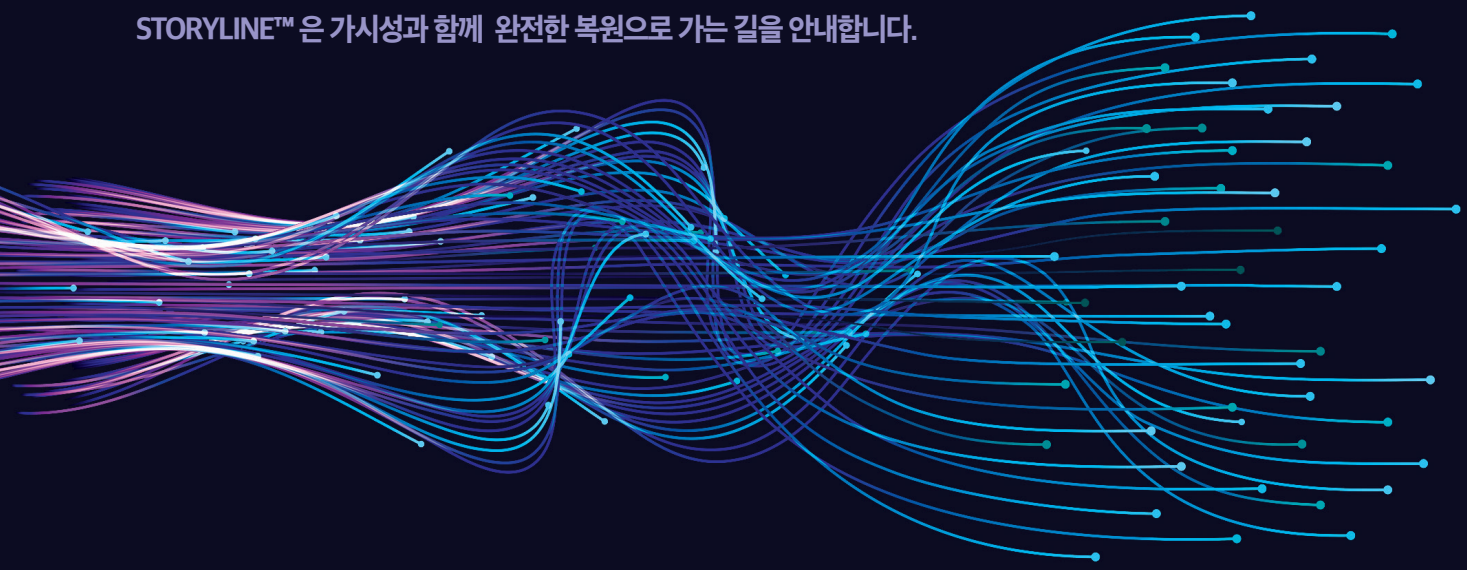
(본사가 요청하는 구성 요구사항 만족 필요)

센티넬원에 대하여

센티넬원은 2013년 사이버 보안 전문가 그룹에 의해 설립되었습니다. 엔드포인트 보호에 대한 근본적으로 새롭고 획기적인 접근 방식을 개발했습니다.

정교한 기계 학습 및 지능형 자동화를 기반으로 하는 단일 플랫폼에서 예방, 탐지 및 대응을 통합합니다. 센티넬원을 사용하여 조직은 모든 공격 벡터에서 악의적인 행동을 탐지하고, 완전 자동화된 통합 대응 기능으로 위협을 신속하게 제거 및 교정하고, 가장 진보된 사이버 공격에 대해 보호할 수 있습니다.

대부분의 스토리는 정상입니다. 하지만 몇몇은 그렇지 않습니다.
STORYLINE™ 은 가시성과 함께 완전한 복원으로 가는 길을 안내합니다.



SentinelOne의 엔드포인트 보호 기능에 대해 더 자세한 정보가 필요하시면 kr.sentinelone.com 에 방문하세요

SENTINELONE LABS KOREA
서울시 영등포구 의사당대로 83 오투타워 20층, WeWork 07325
arthurw@sentinelone.com / jungsup@sentinelone.com

ESCARE
서울시 영등포구 국제금융로6길 33 맨하탄빌딩 12F26호 07331
s1@escare.co.kr / www.escare.co.kr