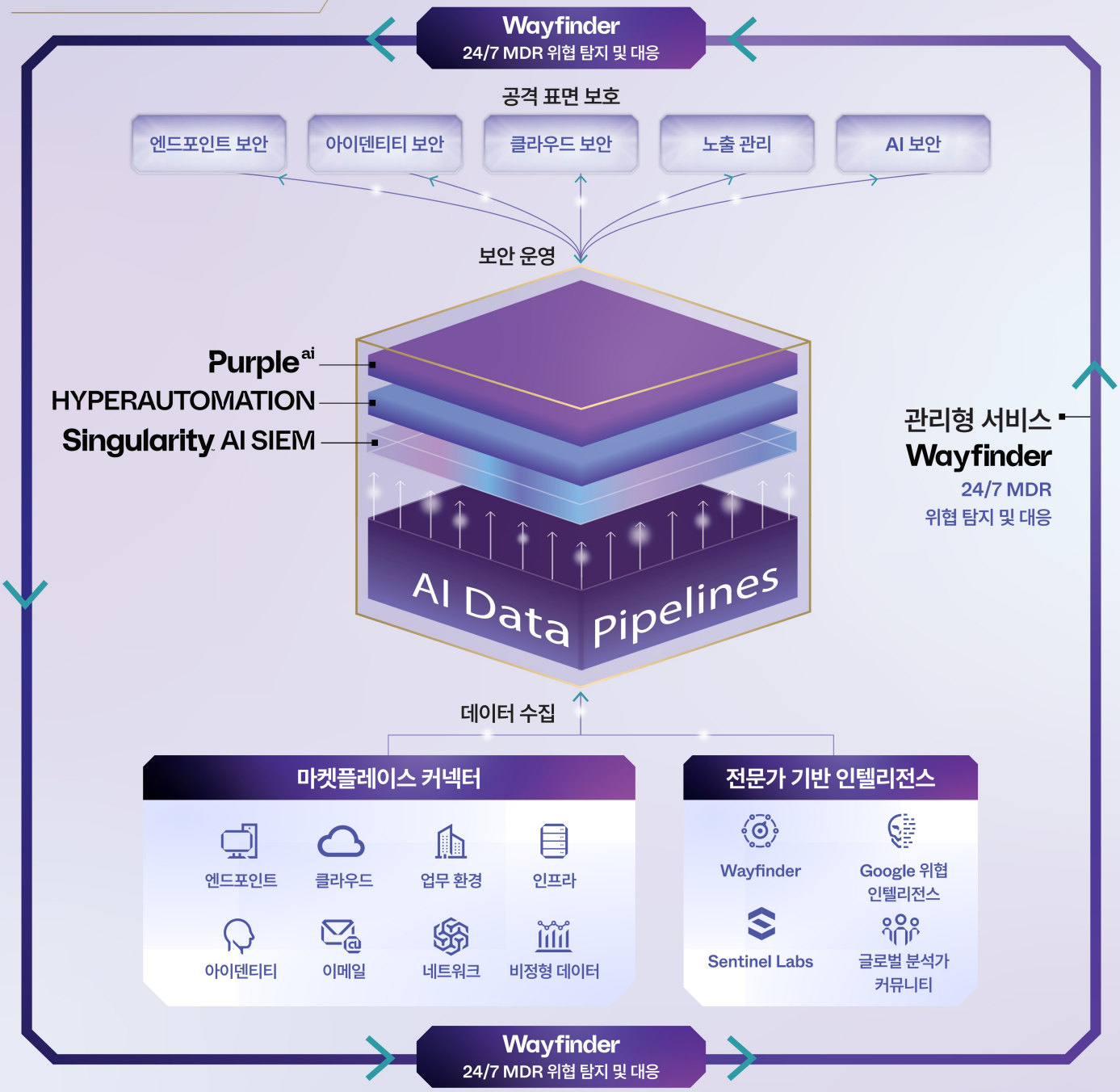
SentinelOne

기업 전체를 안전하게 보호하는 AI 기반 사이버 보안 플랫폼

전 세계에서 가장 발전된 AI 기반
사이버 보안 플랫폼으로 조직을 보호하세요.

Singularity™ 플랫폼

자율 보안 인텔리전스 기반 플랫폼



단일 콘솔 & 통합 AI 플랫폼

단순하게 설계되어,
툴과 벤더를 통합하고
대응 속도를 가속화

실질적으로 작동하는 보호

업계 평가에서
수년 연속 검증된
리더십 입증

AI는 우리의 DNA

AI로 AI에 맞대응!
탐지부터 권장 조치, 대응까지

업계 최고의 CWPP

코드에서 클라우드까지,
완전한 가시성과
탁월한 런타임 보호 제공

최고 수준의 오픈 에코시스템

기존 투자 극대화, 엔터프라이즈
전반의 데이터를 기반으로
조사 수행 가능

빠른 보안 가치 실현

수일 내 구축과 보호가 가능하며,
최소한의 운영 부담으로
하나의 플랫폼만 교육 가능,
책임 있는 아키텍처 제공

총 소유비용 (TCO) 절감

툴과 교육 통합,
데이터 수집 및 보존 비용 절감

신속한 대응

원클릭 롤백 및
차별화된 자동화를 통해
완전한 Remediation을 보장

AI 보안

혁신의 속도를 유지하며 엔터프라이즈 전반의 모든 AI 상호작용을 안전하게 보호하는 솔루션

임직원 (임직원의 AI 활용 보안)

임직원이 Shadow AI, 개인정보, 규제 리스크에 대한 우려 없이 AI를 안전하게 도입·활용할 수 있도록 지원합니다.

- AI 사용 가시성 확보
- 리스크 및 컴플라이언스 관리
- 데이터 프라이버시 보호
- 사용자 인식 강화

자체 개발 AI 애플리케이션 보안

프롬프트 인젝션, 데이터 유출, 유해한 응답에 대한 걱정 없이 사내 자체 개발 AI 애플리케이션의 가치를 안전하게 확장할 수 있도록 지원합니다.

- AI 리스크 대응
- 데이터 보호
- 콘텐츠 안전성 관리
- 가시성과 컴플라이언스

AI 레드팀

배포 전 프롬프트 인젝션, 탈옥, 데이터 포이즈닝 등 다양한 취약점을 사전에 찾아내고, 리스크 스코어 기반 결과와 Remediation 가이드를 제공하여 취약점 진단부터 런타임 보호까지 자연스럽게 연결되는 보안 체계를 지원합니다.

AI 코드 어시스턴트

AI 기반 코드 어시스턴트를 도입하면서도 시크릿 보호, 취약점 점검, 개발 생산성 유지를 동시에 실현 가능합니다.

- 기밀 정보 및 개인정보 보호
- 전체 가시성 및 거버넌스
- 폭넓은 호환성

에이전틱 AI

조직 내에서 동작하는 AI 에이전트 전반에 대해 실시간 가시성, 리스크 평가, 정책 적용을 제공합니다.

- 에이전트 및 MCP 탐지
- 지속적인 리스크 평가
- 정책 기반 제어
- 감사 로그 및 추적

Wayfinder MDR Elite 위협 탐지 및 대응

신뢰할 수 있는 단일 파트너의 세계적 수준 위협 탐지 및 대응을 통해, 공격에 앞서 대응하고 핵심 비즈니스에 집중 가능한 환경을 제공

MDR Essentials

엔드포인트, 아이덴티티, 클라우드, AI 자산 전반에 걸쳐 상시형 MDR과 통합된 선제적 위협 헌팅을 지원

MDR Elite

Essentials의 모든 기능에 전담 위협 전문가, DFIR 지원, 번들형 IR Retainer(사전 계약)까지 제공하는 프리미엄 지원 패키지

위협 헌팅

24시간 자동화된 인텔리전스 기반 탐지를 통해, 보안 사각지대와 계속 진화하는 공격자 인프라를 식별

긴급 대응

사전 계약 없이도 유연하게 활용 가능한 40시간 단위의 인시던트 대응·포렌식·멀웨어 분석 등의 신속 대응 서비스 제공

사고 대비 및 대응

필요 시 전문가 주도의 DFIR, 침해 대응 준비 워크숍, 선제적 침해 여부 점검을 제공

observo.ai
A SentinelOne Company

보안 및 DevOps를 위한 AI 데이터 파이프라인

실시간으로 텔레메트리를 필터링·보강·라우팅하여, 필요한 데이터를 필요한 곳에 즉시 전달합니다.

데이터 최적화 및 절감
가치가 낮은 텔레메트리를 제거해
데이터 적재량을 최대 80% 줄이고
SIEM 비용을 50% 이상 절감 가능합니다.

스마트 라우팅
텔레메트리를 적절한 툴로 라우팅해
벤더 종속성을 줄이고 활용도를 향상합니다.

이상 징후 탐지
데이터 패턴을 학습해 이상 징후를
실시간으로 탐지,
MTTR을 40% 이상 단축합니다.

데이터 보강
로그에 Geo-IP와
위협 인텔리전스 컨텍스트를 추가,
트리아지와 대응 속도를 높입니다.

검색가능한 저비용 Data Lake
전체 원본 데이터를 압축·인덱싱된
형태로 보관, 빠르고 저렴한 검색을 지원합니다.

민감 데이터 탐지
데이터 흐름 전반에서 민감 정보를 찾아
마스킹하고 데이터 보호 및 컴플라이언스
요구사항을 충족할 수 있습니다.

Singularity™ 위협 인텔리전스

업계 최고 수준의 위협 인텔리전스로 위협 탐지, 조사, 인시던트 대응 역량을 강화

위협 환경에 대한 심층적 이해
인시던트를 특정 위협 행위자, 멀웨어 계열,
조직을 겨냥한 활성 캠페인과 연결해
더 정밀하게 해석이 가능합니다.

신종 위협에 대한 선제적 모니터링
인텔리전스 기반 위협 헌팅 역량을 통해
사이버 위협보다 한발 앞서 대응 가능합니다.

조직 내 공격자 신속 식별
이미 알려진 위협을 실시간으로 탐지,
우선 순위화하고 대응하여 영향이 큰 인시던트에
집중하고 잠재 피해를 최소화할 수 있습니다.

Singularity™ AI SIEM

업계에서 가장 빠른 AI 기반 오픈 SIEM -
모든 데이터와 워크플로우를 하나로

현대적인 아키텍처. 운영 자율성. 지능형 툴.

사이버 복원력 강화
성능 저하나 리스크 증가 없이
모든 데이터에 접근이 가능합니다.

보안 태세 개선
모든 데이터 소스를
손쉽게 연동해 보안 사각지대
최소화가 가능합니다.

SOC 효율성 향상
오탐(False Positive)과
반복적인 조치 업무를 축소합니다.

컴플라이언스 유지
데이터 사일로를 해소해
전체 환경에 대한
완전한 가시성을 확보합니다.

관리 탐지 조사 대응

100배
레거시 SIEM 대비
100배 더 빠른 속도

50%
운영 비용
50% 절감

246%
투자 대비 수익률
(ROI)

99%
리스크 노출
99% 감소

Singularity™ 하이퍼오토메이션

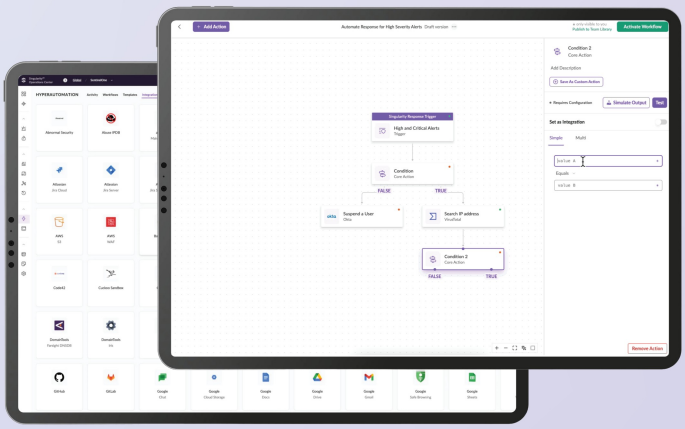
빠르고 확장 가능한 자동화로
보안 운영을 최적화하는 솔루션

모든 것을 연결하세요
어떤 SaaS 애플리케이션과도 손쉽게 연결해
보안 환경 전반을 통합·자동화 가능하며,
직관적인 노코드 캔버스에서 유연한
커스텀 워크플로우 구성이 가능합니다.

대응을 가속화하세요
자동화된 워크플로우에서 제공되는
실시간 인사이트와 가시성을 바탕으로
단일 플랫폼 내에서 더 빠르게 인시던트에
대응하고 업무 중단을 예방 가능합니다.

효율성을 향상하세요
비효율적이고 수동적인 워크플로우를
자동화해 시간을 절감하고, 주요 보안
솔루션용 사전 구축 커넥터와 템플릿을
활용해 자동화를 빠르게 확장합니다.

- 쉬운 자동화
- 통합 워크플로우
- 사전 구축된 연동 기능



- 맞춤형 연동 지원
- 지속적인 개선을 위한 인사이트
- 기본 제공 워크플로우

온프렘 EDG
(Endpoint Data Gateway)

온프레미스 및 에어갭 환경에서 포괄적인 위협 탐지, 분석,
컴플라이언스 보고가 필요한 조직을 위한 기술 솔루션

기술 구성

- **데이터 수집**

  Windows, macOS, Linux 시스템 전반에 배포된 엔드포인트 에이전트로부터 EDR 텔레메트리를 수집합니다.

- **데이터 변환**

  수집된 텔레메트리는 초기에 protobuf 형식으로 생성되며, EDG 컴포넌트를 통해 JSON 형식으로 변환합니다.

- **데이터 스트리밍**

  변환된 JSON 데이터는 인증된 채널을 통해 Kafka 토픽으로 스트리밍됩니다.

- **데이터 인입 및 적재**

  고객의 데이터 레이크 및 SIEM 시스템은 Kafka 토픽에서 해당 데이터를 수집해, 추가 분석과 다른 보안 데이터와의 상관 분석에 활용 가능합니다.

온프레미스 및 에어갭 환경을 위한 포괄적 위협 탐지, 분석, 컴플라이언스 지원

향상된 위협 탐지

EDR 텔레메트리를 데이터 레이크와 SIEM으로 연동하여 엔드포인트 데이터를 다양한 보안 이벤트와 연계해 통합적 상관분석이 가능하며, 이를 통해 조직의 보안 태세를 보다 입체적으로 파악하고, 고도화된 분석 기반의 위협 탐지 체계 마련이 가능합니다.

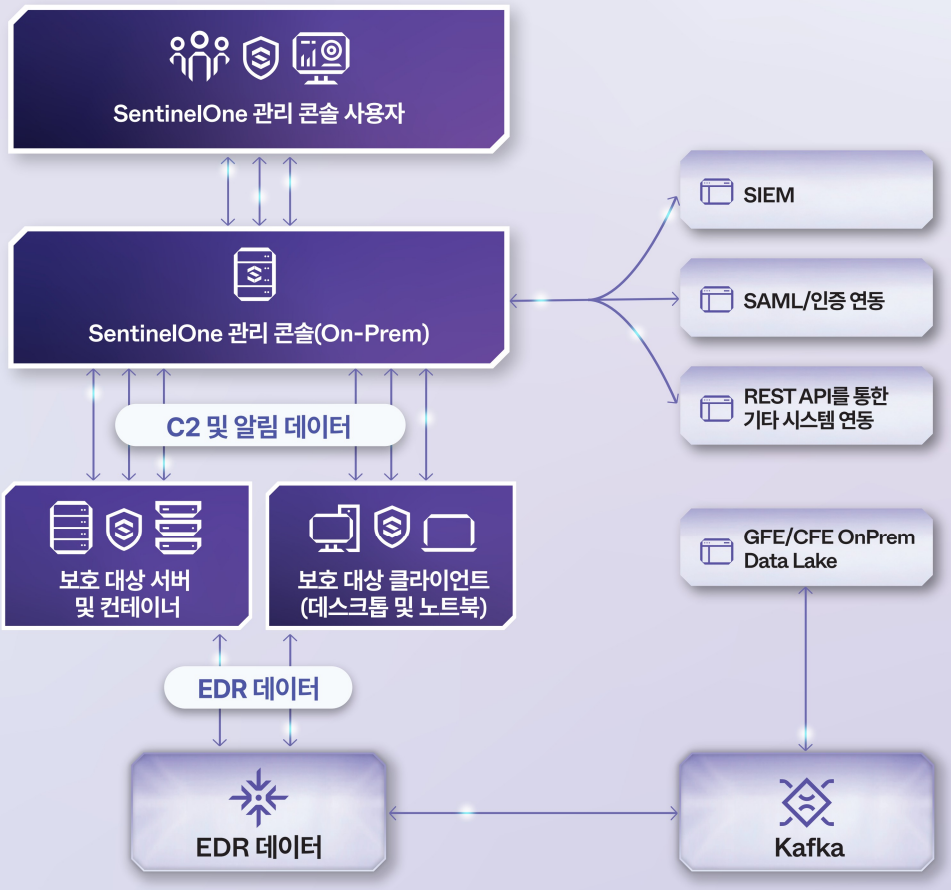
규제 준수 지원

EDR 텔레메트리를 데이터 레이크와 SIEM으로 내보내 장기 데이터 보관 및 리포팅 관련 규제 요구사항 충족이 가능하며 특히 금융, 헬스케어, 공공 부문처럼 컴플라이언스 요구가 엄격한 산업에 중요하게 적용됩니다.

운영 효율성 향상

EDR 텔레메트리를 데이터 레이크와 SIEM에 중앙집중화해 보안 팀의 워크플로우를 효율적으로 운영할 수 있고, 고급 분석 및 자동화 기능을 활용해 위협 조사와 대응에 드는 시간과 노력을 줄일 수 있습니다.

SentinelOne 온프레미스 아키텍처



Purple ai

공격을 더 일찍 탐지하고, 더 빠르게 대응하며, 한발 앞서 나갈 수 있도록 지원하는 에이전틱 AI 보안 분석가

복잡성을 단순하게

방대하고 분산된 데이터를
실행 가능한 인사이트로 전환하고
네이티브 및 서드파티 데이터를
아우르는 가장 폭넓은
가시성을 확보,
AI 에이전트가 중요한 항목을
분석·우선순위화하여
보안팀이 정말 중요한 이슈에
집중할 수 있도록 지원합니다.

모든 애널리스트의 역량 강화

반복적인 업무를 AI 에이전트와
에이전틱 시스템에 맡겨
애널리스트의 생산성을 향상하고
AI가 보강한 요약,
위협 헌팅 쿼스타트,
가이드형 조사, 상황 맥락 기반
지원을 통해 보안 팀이 더 빠르고
정확하게 대응할 수 있도록 돕습니다.

SecOps 가속화

Purple AI는 트리아지부터
대응까지 전 구간의 속도를 높여
보안 팀이 위협을 55% 더 빠르게
해결할 수 있도록 지원하고
자동 트리아지된 알람,
자동으로 문서화되는 노트북,
자동 생성 보고서, 그리고 지능형
Next Step 제안을 통해
팀의 대응 효율을 극대화합니다.

데이터와 프라이버시 보호 강화

데이터와 프라이버시를
보호하도록 설계되었으며,
Purple AI는 책임 있는
보안 아키텍처를 기반으로 구축되어,
최고 수준의 보호 장치를
갖춘 안전한 기반 위에서 동작합니다.

Singularity™ 아이덴티티

실시간 아이덴티티 위협 탐지 및 대응

- AD 보안 모범 사례 적용
- 단일 디바이스 설치
- 의심스러운 AD 이벤트에 대한 가시성
- 도메인 수준 노출에 대한 가시성
- 디바이스 수준 노출에 대한 가시성
- 사용자 수준 노출에 대한 가시성

Singularity 아이덴티티
보안 태세 관리 (IPM)

온프레미스 Active Directory와 클라우드 기반 Entra ID(구 Azure AD) 환경 전반에서
아이덴티티 인프라의 오구성, 노출, 취약점을 식별하고 조치하여 아이덴티티 공격 표면을 축소합니다.

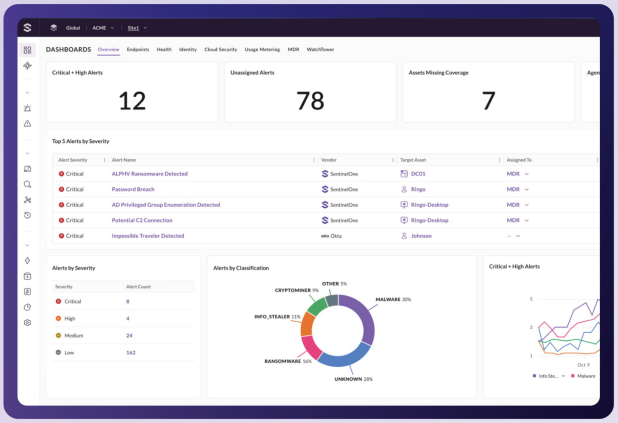
Singularity 아이덴티티
위협 탐지 및 대응 (IRR)

아이덴티티 보호에 대한 통합 접근 방식을 제공: 단순화된 에이전트와 콘솔을 통해 통합 아이덴티티 보호, 정책 기반 조건부 접근,
크리덴셜 침해 보호를 함께 제공하여 엔드포인트와 Active Directory 전반에서 더 빠른 탐지와 대응을 지원합니다.

- 통합 아이덴티티 보호
- 정책 기반 조건부 접근 (PBCA)
- 자격 증명 침해 보호
- 도메인 컨트롤러 및 서버용 에이전트
- 간소화된 아이덴티티 정책
- 운영 센터 내 아이덴티티 대시보드
- 엔드포인트의 아이덴티티 탐지 기능 고도화

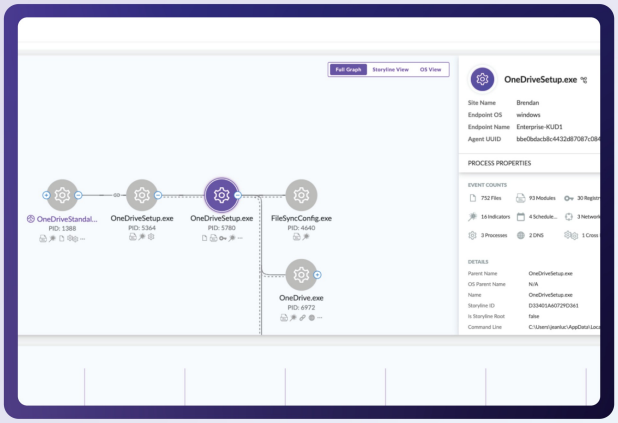
Singularity™ 엔드포인트

AI 기반 자율 보호, 탐지 및 대응



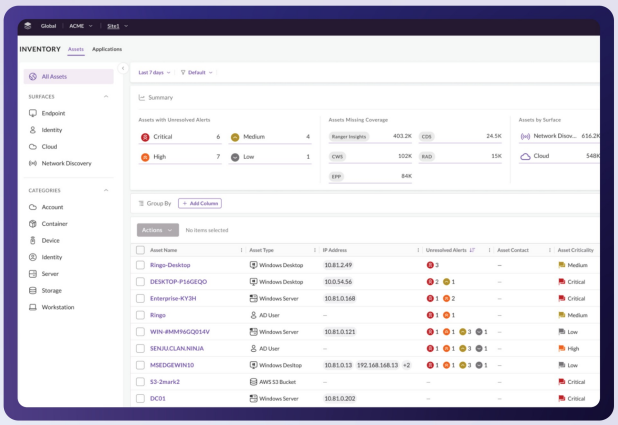
차별화된 보호 및 탐지 역량으로 공격 차단

- 온디바이스 AI 기반의 자율형 머신 스피드 예방으로 멀웨어를 차단합니다.
- 이상 행위와 악성 패턴을 실시간으로 분석하는 Behavioral AI 및 Static AI 모델을 통해, 사람의 개입 없이 랜섬웨어를 탐지합니다.
- 시스템 레벨 공격부터 아이덴티티 기반 공격까지, 실시간 가시성을 바탕으로 중요한 엔드포인트 및 아이덴티티 알림을 제공합니다.
- 모바일 디바이스를 제로데이 멀웨어, 피싱, 중간자 공격(MITM)으로부터 보호합니다.



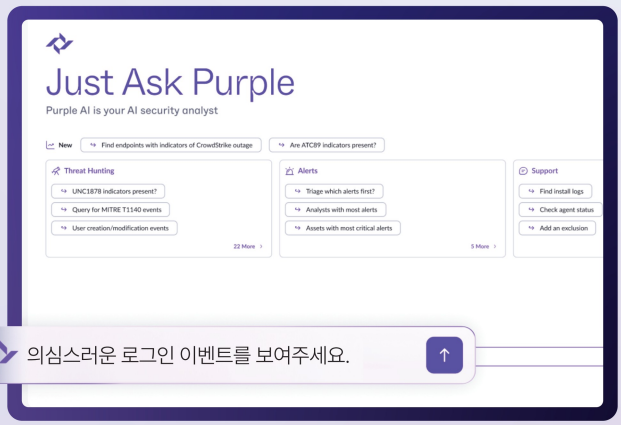
빠른 대응과 복구로 업무 중단 최소화

- 자동화 또는 1-Click 대응·Rollback 기능으로 위협을 신속하게 조치합니다.
- 관련 이벤트를 자동으로 연결해 주는 Storyline®을 통해 공격 전반을 한눈에 파악하고, 실시간 상관분석과 실행 가능한 컨텍스트를 기반으로 빠르게 대응할 수 있습니다.
- 워크스테이션, 아이덴티티, 익스포저 전반의 알림을 상관분석하고 우선순위를 정합니다.



경량 통합 에이전트로 통제력 유지

- EDR 기능과 아이덴티티 보호를 하나의 패키지로 제공하도록
- 처음부터 설계된 아키텍처를 기반으로, 포괄적인 보안을 제공합니다. Windows, macOS, Linux 전반에서 업계 최고 수준의 커버리지를 제공합니다.
- 사용자 영향은 최소화하고 커널 상호작용은 줄이도록 설계된 경량 자율 에이전트를 활용할 수 있습니다.



생성형 AI로 보안 팀 역량 강화

- 퍼스트파티 및 서드파티 데이터에 대한 자연어 질의를 통해 위협 헌팅과 조사를 단순화합니다.
- 헌팅 쿼스타트, 결과 및 이벤트에 대한 자연어 요약, 추천 후속 질문을 통해 SecOps를 가속화합니다.
- 오용과 환각(Hallucination)을 방지할 수 있도록 최고 수준의 보호 장치를 갖춘 AI 모델로 데이터를 보호합니다.

Innovative. Trusted. Recognised.

Gartner
Magic Quadrant

A Leader.
Five Years Running

A Leader in the 2024 Magic Quadrant™ for Endpoint Protection Programmes

MITRE ENGENUITY
A Foundation for Public Good

Record Breaking
ATT&CK Evaluation

AI-Powered Protection.
100% Detection, 100% Real Time

Singularity™ 클라우드 보안

AI 기반 CNAPP으로 실제 악용 가능한 리스크를 검증하고, 런타임 위협을 차단하는 솔루션

CNAPP

클라우드 네이티브 애플리케이션 보호 플랫폼

- 완전한 가시성과 통제를 위한 통합 플랫폼
- 실시간 탐지 및 대응
- Verified Exploit Paths™ 기반 우선순위 중심 조치
- 노코드 Hyperautomation
- AI 보안 분석가
- 업계 최고 수준의 위협 인텔리전스

CSPM

클라우드 보안 태세 관리

- 수분 내 가능한 에이전트리스 배포
- 오구성 제거
- 손쉬운 컴플라이언스 점검

CWPP

1위 클라우드 워크로드 보호 플랫폼

- 실시간 AI 기반 보호
- 모든 워크로드에 대한 모니터링, 탐지, 보호
- 컨테이너, Kubernetes, 가상 머신, 물리 서버, 서버리스 지원
- 퍼블릭, 프라이빗, 하이브리드, 온프레미스 환경 지원

CDR

클라우드 탐지 및 대응

- 전체 포렌식 텔레메트리 제공
- 대응, 격리, 조치 지원
- 사전 구축 및 커스터마이징 가능한 탐지
- 전문가 기반 인시던트 대응

AI-SPM

AI 보안 태세 관리

- AI 파이프라인 및 모델 탐지
- AI 서비스 보안 점검 항목 설정
- AI 서비스에 Verified Exploit Paths™ 적용

CIEM

클라우드 인프라 권한 관리

- 클라우드 권한 관리
- 시크릿 유출 방지
- 권한 최소화 및 정교화

EASM

외부 공격 표면 관리

- 알려지지 않은 클라우드 및 자산 탐지
- 자동화된 펜테스트 및 익스플로잇 경로 탐색
- CSPM을 넘어서는 보호 범위 제공

Graph Explorer

그래프 기반 자산 인벤토리

- 클라우드, 엔드포인트, 아이덴티티 자산을 시각적으로 매핑
- 다양한 소스의 알림을 추적·상관분석
- 위협의 영향 범위와 Blast Radius 파악

DevSecOps

Shift-Left 보안 테스트

- CI/CD 파이프라인 연동
- 리포지토리, 컨테이너 레지스트리, 이미지, IaC 템플릿 스캔
- 에이전트리스 취약점 스캐닝
- 1,000개 이상의 기본 제공 및 커스텀 룰 지원

KSPM

컨테이너 및 Kubernetes 보안 태세 관리

- 오구성 점검
- 컴플라이언스 기준 정렬 지원

Leader SUMMER 2024 | Best Est. ROI SUMMER 2024 | Best Support SUMMER 2024 | Easiest To Use SUMMER 2024 | Easiest Setup SUMMER 2024

업계에서 가장 많은 상을 받은 CNAPP

5점 만점에 4.9점을 받은 유일한 CNAPP제품으로
240개가 넘는 상을 받았고 지금도 계속 수상 중입니다.

SentinelOne®