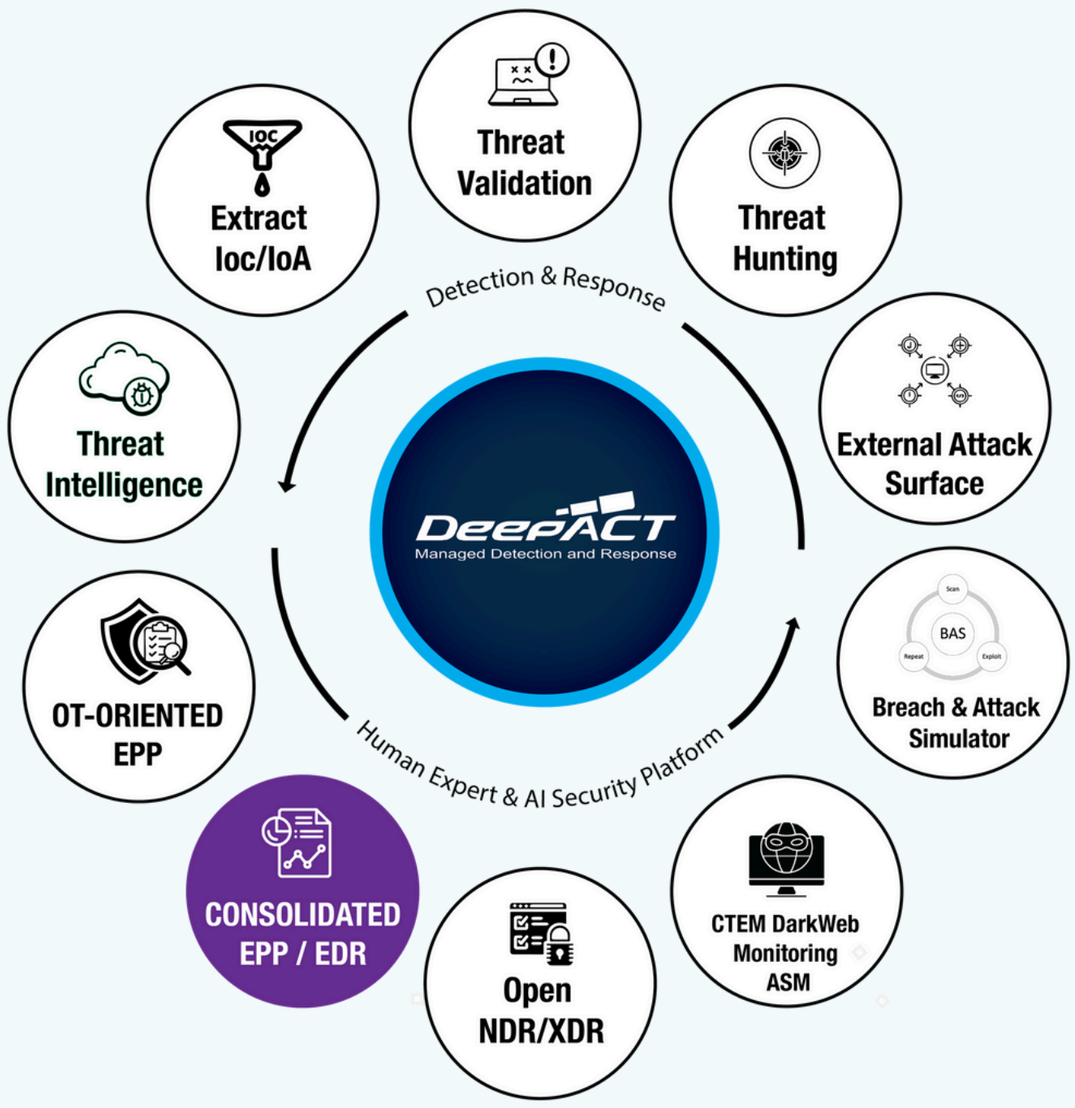
통합 EPP·EDR

IT, Cloud, Data Center, PC, Server, End Point Protection

SentinelOne은 전통적인 안티바이러스(Anti-Virus) 및 EDR 솔루션에 비해 가시성, 탐지, 대응 측면에서 모든 면에서 진화한 통합 엔드포인트 보호/탐지/조사 대응 솔루션입니다. PAGO의 MDR(Managed Detection and Response) 플랫폼인 DeepAct와 결합함으로써, 실시간 위협 탐지와 자율적 대응을 통해 고객의 사이버 리스크를 선제적으로 관리할 수 있습니다. 또한, 원클릭 복구 및 롤백 기능과 다양한 OS 및 플랫폼에 대한 지원을 통해 보다 강력하고 유연한 보안 환경을 제공합니다.



오늘날 보안 시장은 위협 탐지와 대응의 자동화, 그리고 전체 엔드포인트에 대한 가시성을 중시하는 방향으로 빠르게 변화하고 있습니다.

SentinelOne은 이러한 트렌드에 맞춰, 단순한 탐지를 넘어서는 완벽한 엔드포인트 보호를 제공하므로서 기업은 위협 대응 속도와 정확성을 높이고, 보안 인프라 운영의 복잡성을 대폭 줄일 수 있습니다.

pago's choice

엔드포인트 위협 탐지 및 차단

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

위협 분석 및 대응

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

가시성 확보

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

pago's Added Value

- **24/7 전문가 모니터링 및 위협 대응**
  자동화로 누락될 수 있는 잠재적인 위협 관리

- **맞춤형 보안 인텔리전스 제공**
  업계 동향, 최신 위협 정보 등을 포함한 맞춤형 인텔리전스를 제공

- **고급 위협 분석 및 포렌식**
  보안 전문가의 심층 분석을 통해 위협의 원인과 경로를 신속히 파악, 정확한 조치를 제안하고, 유사 위협에 대한 예방 대책 제시

- **최적화된 보안 정책 및 설정 지원**
  고객의 인프라에 맞춘 커스터마이징을 통해 보안 효과 극대화

- **정기 리포팅 및 개선 제안**

- **자동화된 위협 대응 강화**

- **고객 맞춤형 위협 헌팅 서비스**

- **보안 교육 및 컨설팅 제공**

www.pagonetworks.com

- **통합형 자율 EPP/EDR**

EPP(Endpoint Protection Platform)와 EDR(Endpoint Detection and Response)이 결합된 솔루션으로, 엔드포인트 보안의 두 가지 중요한 요소를 하나의 통합된 시스템에서 제공합니다. 이는 침입을 예방하는 보안 기능(EPP)과 실시간으로 발생하는 위협을 탐지하고 대응하는 기능(EDR)을 한 곳에서 관리할 수 있도록 합니다. 즉, 기업은 한 번의 설치로 엔드포인트 보안을 전반적으로 관리하고 강화할 수 있습니다.

- **EPP 단일 또는 EDR 결합 라이선스 제공**

기업의 보안 요구에 따라 선택할 수 있도록 EPP와 EDR을 개별적으로, 또는 결합된 형태로 라이선스를 제공합니다. 이를 통해 기업은 필요에 따라 유연하게 구성하여 비용 효율적으로 보안 솔루션을 도입할 수 있습니다.

- **특허 받은 원클릭 교정 및 롤백**

탐지된 위협이 발생했을 때, 버튼 클릭 한 번으로 시스템을 복구하고 원상태로 되돌릴 수 있습니다. 특히 랜섬웨어로 파일이 암호화된 경우에도 롤백 기능을 통해 중요한 데이터와 시스템을 신속히 복원할 수 있습니다. 이는 보안 사고로 인한 비즈니스 중단을 최소화하는 데 매우 유용한 기능입니다.

- **모든 OS에 대한 원격 포렌식**

리눅스, mac OS, 윈도우 등 다양한 운영체제(OS)를 지원하며, 원격에서 모든 엔드포인트의 포렌식 데이터를 수집할 수 있습니다. 즉, 물리적으로 접근할 필요 없이도 위협의 증거를 빠르게 확보하여 보안 분석 및 조치를 취할 수 있습니다.

- **온라인/오프라인 보호, 탐지 및 대응**

네트워크가 연결되지 않은 오프라인 상태에서도 보호 기능을 제공합니다. 예를 들어, 출장을 다니며 네트워크가 불안정하거나 연결되지 않은 상태에서도 시스템은 여전히 보호를 받으며, 악성코드를 탐지하고 대응할 수 있습니다.

- **최신 위협 탐지를 위한 문석 쿼리 제공**

최신 보안 위협에 대한 분석 및 대응이 가능한 쿼리 기능을 제공합니다. 이를 통해 보안팀은 새롭게 나타나는 위협 유형을 신속히 탐지하고, 탐지된 위협에 대한 심도 있는 분석을 수행할 수 있습니다.

- **다양한 플랫폼 지원**

Linux, macOS, Windows뿐만 아니라 컨테이너화된 환경인 Kubernetes와 Docker까지 지원합니다. 이로써 다양한 IT 환경을 가진 기업에서도 일관된 보안을 유지할 수 있습니다.

- **이벤트 상관 관계를 자동으로 스토리라인으로 구성**

탐지된 위협 이벤트들을 자동으로 상관 관계 지어 하나의 스토리라인으로 연결합니다. 예를 들어, 악성코드가 실행된 시간, 이로 인해 발생한 네트워크 활동, 파일 수정 등을 시간 순으로 정리하여 직관적으로 확인할 수 있어 보안 분석이 더욱 용이합니다.

- **MITRE ATT&CK 프레임워크와 연계한 위협 단계 및 기술정보 제공**

MITRE ATT&CK 프레임워크에 맞춰 각 위협의 단계와 기술적 세부 정보를 제공합니다. 이는 보안팀이 공격의 진행 상태와 사용된 기법을 파악하고, 필요한 조치를 이해하는 데 큰 도움이 됩니다.