CROWDSTRIKE

CrowdStrike 제품

FALCON ENDPOINT DETECTION AND RESPONSE (EDR)

빠른 속도, 자동 처리, 독보적인 가시성으로 위협 탐지 및 대응 수명주기를 스트리밍

FALCON INSIGHT 로 더욱 간편해지는 EDR

기존 엔드포인트 보안 도구에는 사각지대가 존재해서 지능형 위협을 발견 및 차단할 수 없었습니다. CrowdStrike® Falcon Insight™는 조직 전반에 걸쳐 전체적인 엔드포인트 확인이 가능하므로 이러한 문제가 해결됩니다.

Falcon Insight 는 모든 엔드포인트 활동을 지속적으로 모니터링하고 데이터를 실시간으로 분석하여 위협 활동을 자동으로 파악하므로 지능형 위협이 발생할 경우 탐지와 차단이 모두 가능합니다. 또한 모든 엔드포인트 활동은 CrowdStrike Falcon® 플랫폼으로도 스트리밍되므로 보안 팀의 신속한 인시던트 조사, 경고 대응, 신종 위협의 선제적 사냥이 가능합니다.

최고의 엔드포인트 보호 솔루션으로 꾸준히 인정받는 CROWDSTRIKE

CrowdStrike 는 2019 년 Gartner 매직 쿼드런트에서 엔드포인트 보호 플랫폼 부문 리더로 선정되었습니다.

CrowdStrike 는 2018 년 MITRE 국가 에뮬레이션 테스트에서 지능형 공격을 추적 및 탐지하는 MITRE ATT&CK™ 프레임워크 검증을 거쳤습니다.

CrowdStrike 는 Forrester Wave™ 엔드포인트 탐지 및 대응(2018 년 3 분기) 부문과 Forrester Wave 엔드포인트 보안 제품군(2019 년 3 분기) 부문에서 모두 리더로 선정된 유일한 공급업체입니다.

CrowdStrike 는 2019 년 10 월 Gartner 가 발표한 "A 타입" 조직의 엔드포인트 보호 플랫폼 주요 기능 측면에서 최고점을 기록했습니다.

주요 이점

지능형 위협의 자동 탐지 및 스마트한 우선순위 지정

실시간 심층 포렌식 및 정교한 시각화를 통해 조사 속도 향상

안심할 수 있는 대응 및 해결 능력

엔터프라이즈 위협 점수인 CrowdScore™를 통해 전체적인 상황 파악

경고 피로도 90% 이상 감소

MITRE 기반 탐지 프레임워크와 CrowdScore Incident Workbench 로 복잡한 공격을 한눈에 파악

CrowdStrike 제품

FALCON EDR(Endpoint Detection and Response)

제품의 주요 기능

탐지 및 해결 간소화

- **공격 활동 자동 탐지:** Falcon Insight 는 IOA(공격 지표)를 사용하여 공격 동작을 자동으로 파악하고 우선순위에 따른 경고를 Falcon 사용자 인터페이스(UI)로 전송하므로 시간이 많이 필요한 연구와 수동 검색을 할 필요가 없습니다. CrowdStrike Threat Graph® 데이터베이스는 수십억 건의 이벤트 전체에 대해서도 5 초 이내에 이벤트 데이터를 저장하고 쿼리를 해결합니다.
- **간편한 단일 인터페이스:** CrowdScore Incident Workbench 는 심층 배경 정보를 통해 공격의 전모를 종합적으로 확인할 수 있어 더욱 빠르고 간편한 조사가 가능합니다.
- **MITRE ATT&CK™으로 조사 속도 향상:** MITRE ATT&CK™(Adversarial Tactics, Techniques, and Common Knowledge) 프레임워크로 경고를 매핑하여 아무리 복잡한 탐지 내용도 한눈에 파악할 수 있으므로 경고 심사 소요 시간이 단축되고 우선순위 지정 및 치료 속도가 빨라집니다. 또한 직관적 UI 를 통해 빠른 전환이 가능하며 조직 전체 검색도 몇 초 만에 이루어집니다.
- **배경 정보 및 인텔리전스 확보:** 통합 위협 인텔리전스를 통해 특성을 포함한 전체적인 공격 배경 정보를 제공합니다.
- **강력한 대응:** 악성 활동에 대한 실시간 대응으로 침해가 이루어지기 전에 공격을 막습니다. 강력한 대응 조치로 감염된 시스템을 억제 및 조사할 수 있으며 Falcon Insight 실시간 대응 기능을 통해 조사 중인 엔드포인트에 바로 접근할 수 있습니다. 따라서 보안 대응 시 해당 시스템에서 작업을 실행할 수 있고 위협을 매우 정밀하게 처리할 수 있습니다.

전체 영역의 실시간 확인 가능

- **실시간으로 전체적인 상황 파악:** CrowdScore 는 조직이 위협 수준을 실시간으로 파악할 수 있도록 간편한 지표를 제공합니다. 따라서 공격을 받을 경우 보안 팀 리더가 이를 빠르고 쉽게 파악할 수 있으며 위협의 심각도를 평가하여 적절한 대응을 구성할 수 있습니다.
- **중요한 세부 정보를 수집하여 위협 사냥과 포렌식 조사에 활용:** Falcon Insight 의 커널 모드 드라이버가 인시던트 추적에 필요한 400 건 이상의 원시 이벤트와 관련 정보를 수집합니다.
- **빠른 속도:** CrowdStrike Threat Graph 데이터베이스는 수십억 건의 이벤트 전체에 대해서도 5 초 이내에 이벤트 데이터를 저장하고 쿼리를 해결합니다.
- **최대 90 일 동안 기록 재현:** Falcon Insight 는 엔드포인트가 100 개 미만이든 50 만 개 이상이든, 사용자의 환경과 관계없이 시간에 따른 엔드포인트 활동에 대해 전체 기록을 제공합니다.

즉각적인 가치 실현

- **시간, 노력, 비용의 절감:** 클라우드 방식의 Falcon Insight 는 CrowdStrike Falcon 플랫폼을 통해 제공되며 온프레미스 관리 인프라가 필요하지 않습니다.
- **몇 분 이내에 구축:** CrowdStrike 를 이용하면 최대 7 만 개의 엔드포인트에 클라우드 제공 Falcon 에이전트를 구축하는 데 하루도 채 걸리지 않습니다.
- **즉각적인 가동:** 이용 첫날부터 독보적인 탐지 기능과 가시적 확인을 경험할 수 있는 Falcon Insight 는 재부팅이나 미세 조정, 기본 설정, 복잡한 구성 없이도 설치하면 바로 실행되어 모니터링과 기록을 원활하게 수행합니다.
- **엔드포인트에 영향을 주지 않음:** 엔드포인트에서는 경량 에이전트만 실행되므로 엔드포인트나 네트워크 성능 저하 없이 Threat Graph 데이터베이스 내에서 검색이 이루어집니다.

CROWDSTRIKE 소개

세계적으로 손꼽히는 사이버 보안 업체 CrowdStrike® Inc.(Nasdaq: CRWD)는 처음부터 철저히 보안 침해를 차단하기 위해 설계된 엔드포인트 보안 플랫폼을 기반으로 클라우드 시대에 걸맞도록 보안의 개념을 새롭게 정립합니다. CrowdStrike Falcon® 플랫폼의 단일 경량 에이전트 아키텍처는 클라우드 스케일 AI(인공지능)을 활용하며 엔터프라이즈 환경 전반에서 실시간 보호 및 가시성을 제공하여 네트워크 연결 여부와 관계없이 모든 엔드포인트에서 공격을 방지합니다. 독자적인 CrowdStrike Threat Graph®를 기반으로 CrowdStrike Falcon 은 전 세계적으로 매주 3 조 건 이상 발생하는 엔드포인트 관련 이벤트에 대해 실시간으로 상관관계를 파악하여 세계 최고 수준의 보안 관련 데이터 플랫폼에 공급하고 있습니다.

면책 조항:

Gartner 는 자사의 조사 발행물에 등장하는 어떠한 업체나 제품, 서비스도 지지하지 않으며 사용자에게 최고 등급을 받은 업체만을 선택하도록 조언하지 않습니다. Gartner 의 연구 조사 발행물은 Gartner 조사 기관의 의견을 바탕으로 작성되며 사실을 기술한 것으로 간주되어서는 안 됩니다. Gartner 는 본 연구 조사와 관련하여 특정 목적에 대한 판매 적격성 또는 적합성에 대한 모든 보증을 비롯하여 모든 종류의 명시적 또는 묵시적 보증을 부인합니다.

차세대 AV

무료 체험 시작하기

자세히 알아보기: **www.crowdstrike.com**