CrowdStrike 제품

CROWDSTRIKE

FALCON PREVENT
NEXT-GENERATION ANTIVIRUS

기존 AV 를 대체할 우수한 제품으로 가장 효과적인 예방 기술에 전체 공격 파악 기능과 간편함을 결합

기존 AV 솔루션의 세대 교체

기존 안티 바이러스 솔루션의 비효율성과 복잡성으로 인해 어려움을 겪는 조직이라면 CrowdStrike® Falcon Prevent™가 도움이 될 것입니다. Falcon Prevent 는 지속적인 시그니처 업데이트나 온프레미스 관리 인프라, 복잡한 통합 과정 없이 운영되는 단일 경량 에이전트를 통해 우수한 보호 기능을 제공합니다. Falcon Prevent 는 규모가 큰 조직에서도 몇 분 만에 가동됩니다.

기존 안티 바이러스 제품을 대체하기에 충분한 성능을 입증 — AV-Comparatives 및 SE Labs 의 독립 테스트를 통해 Falcon Prevent 의 안티 바이러스 기능에 대한 인증을 받았습니다. 또한 Falcon Prevent 는 PCI, HIPAA, NIST, FFIEC 규제 요건에 대한 검증도 거쳤습니다.

2019 Gartner 매직 쿼드런트 엔드포인트 보호 플랫폼(EPP) 부문에서 리더 그룹으로 선정 — CrowdStrike 는 리더 쿼드런트에 선정되었을 뿐 아니라 혁신, 마케팅, 제품 전략, 수직 산업, 지리적 전략을 비롯하여 비즈니스 모델 전체 검증과 같은 기준을 고려하는 "비전 완성도" 측면에서도 가장 높은 점수를 얻었습니다.

주요 이점

- 모든 유형의 공격을 방지
- 시그니처가 필요 없는 보호 기능 및 서비스형 소프트웨어(SaaS)를 제공하여 운영 간소화
- 몇 분 내로 구축되고 즉시 엔드포인트 보호 시작
- 기존 안티 바이러스 제품을 빠르고 안정적으로 대체
- 전환 간소화를 위한 마이그레이션 시 AV 와 함께 원활하게 운영됨
- 전체 공격에 대한 가시성 제공

FALCON PREVENT NEXT-GENERATION ANTIVIRUS

주요 기능

첨단 보호 기능

Falcon Prevent 는 오프라인 상태에서도 코모디티 악성 코드부터 정교한 공격에 이르는 모든 유형의 공격으로부터 엔드포인트를 보호합니다.

- 머신러닝과 인공지능을 통해 알려진 악성 코드와 알려지지 않은 악성 코드, 애드웨어, 잠재적 위해 프로그램(PUP)을 방지
- 동작 기반 공격 지표(IOA)를 통해 랜섬웨어, 파일리스 공격, 맬웨어 프리 공격 등의 정교한 공격을 방지
- 익스플로잇 차단으로 패치되지 않은 취약점을 통한 위협 실행과 유포 방지
- 위협 인텔리전스 보호 기능을 통해 악성으로 파악된 활동을 차단
- 맞춤형 IOA 로 차단할 특정 동작 정의
- 격리 기능으로 차단된 파일을 수집하고 조사를 위한 접근 가능
- 스크립트 기반 실행 모니터링으로 악성 Microsoft Office 매크로를 조사 및 차단

통합 위협 인텔리전스

- 고객의 환경에서 발견된 위협의 범위와 영향력을 자동으로 밝혀냄
- 공격 대상이 되고 있는지 여부, 공격 주체, 대비 및 선제 방어 방법을 파악
- Falcon Prevent 를 CrowdStrike Falcon X™와 통합 사용하여 다음을 도모
  - 고객 환경에 존재하는 위협과 대응 방법을 충분히 파악
  - 악성 코드 연구 및 분석 정보를 간편하게 이용
  - 위협 심각도 평가로 간편하게 대응 우선순위 지정
  - 심층 위협 분석으로 즉시 복구 조치를 진행하고 인시던트를 해결

전체 공격을 한눈에 파악

Falcon Prevent 의 독보적인 경고 배경 정보와 가시적 확인 기능으로 다음이 가능합니다.

- 모든 경고에 대해 세부 정보, 배경 정보, 활동 기록 제공
- 배경 정보 및 위협 인텔리전스 데이터로 보강된 이해하기 쉬운 단일 프로세스 트리에서 전체 공격을 해결
- 아무리 복잡한 탐지 내용도 빠르게 파악할 수 있도록 MITRE ATT&CK®(Adversarial Tactics, Techniques and Common Knowledge) 프레임워크로 경고를 매핑
- 탐지 세부 정보를 90 일 동안 유지

간단하고 신속한 경량 솔루션

클라우드 네이티브 CrowdStrike Falcon® 플랫폼과 경량 Falcon 에이전트로 복잡성이 사라지고 엔드포인트 보안 운영이 간소화됩니다.

- Falcon 은 지속적인 시그니처 업데이트나 복잡한 통합 과정, 온프레미스 장비 없이 운영됨
- 경량 에이전트로 최초 설치부터 일상적 사용에 이르기까지 엔드포인트에 미치는 영향이 거의 없으며 설치 후에도 재부팅할 필요가 없음
- 최소한의 CPU 관리 비용으로 시스템 성능과 최종 사용자 생산성 복구
- 사용 첫날부터 효과를 발휘하며 몇 분 이내에 구축되어 즉시 가동 가능
- 클라우드 네이티브 아키텍처와 SaaS 제공을 통해 자동 업데이트 관리
- Windows, Windows Server, macOS, Linux 를 포함한 광범위한 플랫폼 지원

FALCON PREVENT: 가장 간편한 AV 대체 솔루션

더욱 효과적인 보호

빠르고 간편한 구축

최적의 성능

복잡성 감소

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.

차세대 AV

무료 체험 시작하기

자세히 알아보기: **www.crowdstrike.com**