CrowdStrike 제품

CROWDSTRIKE

FALCON CLOUD WORKLOAD PROTECTION

클라우드 워크로드 및 컨테이너 침해 방지

모든 환경에서의 클라우드 워크로드 보호

CrowdStrike Falcon® Cloud Workload Protection 은 프라이빗, 퍼블릭, 하이브리드, 멀티 클라우드 환경 전반에 걸쳐 종합적인 침해 보호 기능을 제공합니다. 모든 기능은 경량 Falcon 에이전트를 통해 제공되며 CrowdStrike® 클라우드 네이티브 플랫폼에서 관리합니다. Falcon 플랫폼을 사용하면 워크로드 전체에서 기술을 신속하게 도입하고 안전하게 보호할 수 있습니다.

주요 기능

우수한 가시성

클라우드 워크로드 이벤트 및 인스턴스 메타데이터에 대한 종합적 확인을 통해 탐지, 대응, 선제적 위협 사냥 및 조사가 가능하며 잠재적 악성 활동을 모두 밝혀낼 수 있습니다.

- 인스턴스 수준에서 메타데이터를 수집하여 경고와 관련된 자산의 소유자를 손쉽게 파악
- 호스트를 계정 ID 별로 분류하여 사용자별 자산을 빠르고 간편하게 시각적으로 확인하여 파악
- 의심스러운 악성 활동의 자동 탐지 및 스마트한 우선순위 선정
- 이벤트를 지속적으로 모니터링하여 컨테이너 내부 실행 활동을 포함한 워크로드 활동에 대한 가시성을 제공하며, 다양하고 풍부한 데이터와 이벤트 세부 정보를 통해 임시 워크로드와 제거된 워크로드 조사 가능
- 동일 콘솔의 모든 워크로드와 엔드포인트에 대한 선제적 위협 사냥 기능 제공
- 여러 환경과 다양한 유형의 워크로드에 걸쳐 모든 공격을

주요 이점

단일 콘솔에서 워크로드에 대한 종합적 가시성 제공

클라우드 워크로드 흔적을 자동으로 검색

주요 클라우드 통합 기능으로 마찰 제거

성능 저하 없이 개발운영 속도에 따라 워크로드 보호

사용량 기준 과금제로 사용한 만큼만 비용 지불

일관된 수준의 가시성 및 보호 기능으로 온프레미스에서 클라우드로 원활하게 마이그레이션

더욱 빠른 속도의 클라우드 내 위협 사냥 및 조사 지원

FALCON CLOUD WORKLOAD PROTECTION

탐지 및 조사하고 엔드포인트에서 인스턴스, 컨테이너로 전환

- 감염된 워크로드의 활동 범위 제한 및 조사를 수행하고 조치를 취할 수 있는 대응 기능 제공
- CrowdScore™ Incident Workbench 가 포함되어 있어 인시던트에 대한 보안 경고를 선별하고 상관 관계를 분석하며 긴급한 주의가 필요한 사안을 자동으로 심사, 우선순위 지정, 강조 표시하여 공격을 해결하고 대응 시간을 단축

멀티 클라우드 워크로드 검색

Falcon 은 퍼블릭 및 하이브리드 클라우드 흔적의 범위와 특성을 가시적으로 확인할 수 있습니다.

- 기존 Amazon Web Services(AWS) Elastic Compute Cloud(EC2) 인스턴스, Google Cloud Platform(GCP) Compute Engine 인스턴스, Microsoft Azure 가상 시스템을 열거(enumerating)하여 에이전트 설치 없이 기존 클라우드 워크로드 구축을 자동으로 검색
- AWS, GCP, Azure 시스템 규모 및 구성, 네트워킹, 보안 그룹 정보에 대한 배경 정보가 풍부한 메타데이터를 포함하는 워크로드 관련 정보를 실시간으로 제공
- Falcon 플랫폼을 통해 보호되지 않는 워크로드 파악
- 모든 워크로드를 보호하고 위험을 탐지 및 완화하며 공격 노출면을 줄일 수 있도록 클라우드 흔적에 대한 분석 정보 제공

컨테이너 보안

Falcon 을 통해 컨테이너 성능 저하 없이 보호 및 확인 기능을 이용할 수 있습니다.

- 호스트에서 실행되는 단일 Falcon 에이전트를 통해 호스트와 컨테이너를 보호
- 탐지가 특정 컨테이너와 관련되어 있으며 호스트 이벤트가 포함되지 않는 상황에서 컨테이너 인시던트를 간편하게 조사
- 컨테이너 시작, 종료, 이미지 및 런타임 정보를 비롯하여 컨테이너 내부에서 생성된 모든 이벤트를 단 몇 초만 실행되어도 수집
- 온프레미스 및 클라우드 구축 등의 컨테이너 흔적을 가시적으로 확인 가능하며 트렌드, 가동 시간, 사용된 이미지, 구성을 포함한 컨테이너 사용 정보를 표시하여 위험성이 있으며 잘못 구성된 컨테이너를 파악
- 호스트 및 컨테이너 보안에 대해 단일 관리 콘솔을 제공

런타임 보호

Falcon 플랫폼은 최고의 최신 기술을 결합하여 워크로드가 가장 취약한 상황, 즉 런타임 시 능동적 공격과 위협으로부터 보호합니다.

- 머신러닝(ML)과 인공지능(AI)으로 알려진 악성 코드와 알려지지 않은 악성 코드를 탐지
- 파일리스 공격, 맬웨어 프리 공격과 같은 정교한 공격을 탐지하는 동작 기반 공격 지표(IOA)를 포함
- 익스플로잇 방지 기능 제공
- 탐지 및 보호 기능을 맞춤 구성할 수 있는 맞춤형 IOA, 화이트리스트 및 블랙리스트 작성 기능 포함
- 통합 위협 인텔리전스를 제공하여 알려진 악성 활동을 차단하고 특성을 포함한 전체적 공격 배경 정보를 제공
- 24 시간 관리형 위협 사냥 기능을 제공하여 은밀한 공격이 탐지되지 않을 가능성을 없앰

멀티 클라우드와 광범위한 OS 지원

CrowdStrike Falcon 플랫폼은 Windows 및 Linux(Amazon, Red Hat, CentOS, Oracle, SUSE, Ubuntu, Debian) 전반에 걸쳐 구축할 수 있는 종합적 보호 범위를 제공합니다. AWS, Microsoft Azure, GCP 에서 사용할 수 있으며 vSphere 와 Hyper-V 를 포함하는 모든 하이퍼바이저와 함께 사용할 수 있습니다.

지원되는 컨테이너

Falcon 은 Docker 와 같은 OCI(Open Container Initiative) 준수 컨테이너, 자체 관리형 Kubernetes 와 같은 오케스트레이션 플랫폼을 비롯하여 GKE(Google Kubernetes Engine), EKS(Amazon Elastic Kubernetes Service), ECS(Amazon Elastic Container Service), AKS(Azure Kubernetes Service), OpenShift 와 같은 호스팅된 오케스트레이션 플랫폼을 지원합니다.

API 중심의 클라우드 통합

Falcon 은 마찰을 제거하여 클라우드 보안 효율성을 강화합니다.

- 강력한 API 를 통해 탐지, 관리, 대응, 인텔리전스 등, CrowdStrike Falcon 기능을 자동화
- Chef, Puppet, AWS Terraform 통합으로 지속적 통합/지속적 제공(CI/CD) 구축 워크플로 지원
- Google Cloud OS(Operating System) 구성 관리 통합 기능으로 맞춤 스크립트 없이도 GCP 에서 바로 Falcon 에이전트 구축을 자동화
- AWS PrivateLink 통합으로 센서-클라우드 트래픽을 지원하여 PrivateLink 를 통한 트래픽 흐름을 형성하므로 인터넷 노출이 감소하고 네트워크 아키텍처 간소화

간편함과 성능

클라우드용으로 개발되어 클라우드에 구축되는 Falcon 은 클라우드 워크로드 보호와 관련된 관리 비용, 마찰, 복잡성을 줄여줍니다.

- 프라이빗, 퍼블릭, 하이브리드와 같은 클라우드 종류와 관계없이 어디서나 모든 워크로드와 작업을 단일 플랫폼에서 처리
- 단일 콘솔을 통해 위치와 관계없이 클라우드 워크로드를 중앙에서 확인 가능
- Falcon 을 통해 전체 정책에 대한 유연성이 확보되어 개별 워크로드나 그룹, 또는 더 높은 수준에서 적용 가능
- 별도 인프라 없이 클라우드 워크로드 확장에 따라 규모 확장 가능
- 운영 시 호스트에 미치는 부담이 매우 적으며 분석, 검색, 조사 시에도 런타임 성능에 미치는 영향이 거의 없음
- 유연한 사용량 기준, 연 단위 구독 모델로 민첩한 비즈니스 계획 지원

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**