CrowdStrike 솔루션

CROWDSTRIKE

FALCON 플랫폼으로 LINUX 보호

모든 환경에서의 워크로드 보호에 필요한 여러 기술을 통합한 Falcon 솔루션

단일 플랫폼으로 모든 LINUX 워크로드 실행

대다수 비즈니스 핵심 애플리케이션을 실행하는 주요 운영 체제 중 하나인 Linux 서버는 공격 대상이 되는 경우가 많습니다. Linux 서버는 온프레미스나 프라이빗/퍼블릭 클라우드 모두에서 사용되므로 이를 보호하려면 위치와 관계없이 모든 Linux 호스트에 대해 런타임 보호 및 확인 기능을 제공하는 솔루션이 필요합니다.

CrowdStrike Falcon® 플랫폼은 퍼블릭/프라이빗 클라우드부터 온프레미스 및 하이브리드 데이터 센터에 이르기까지, 모든 환경에서 실행되는 Linux 워크로드를(컨테이너 포함) 간편하면서도 효과적으로 보호합니다.

주요 이점

- 통합 컨테이너 보호 기능 제공
- Linux 호스트와 컨테이너를 활성 공격으로부터 방어
- Linux 및 컨테이너용 EDR(엔드포인트 탐지 및 대응) 기능으로 시스템 환경 전반에서 가시성 실현
- 실제 및 가상, 클라우드, 컨테이너 등 지원되는 모든 Linux 배포 및 구축 환경 전반에 걸쳐 일관된 보호 기능을 제공하므로 복잡성 감소
- 잠재적으로 위험한 구성으로 실행되는 경우를 포함하여 사용자의 환경에서 실행되는 Linux 컨테이너를 파악
- 더욱 빠른 속도의 위협 사냥 및 조사 지원

CrowdStrike 솔루션

FALCON 플랫폼으로 LINUX 보호

주요 기능

예방

- CrowdStrike® Falcon 플랫폼은 머신러닝(ML), 인공지능(AI), 동작 기반 공격 지표(IOA), 맞춤형 해시 차단을 결합하여 악성 코드와 정교한 위협으로부터 Linux 워크로드 보호
  - **ML 및 AI** - 검사 또는 시그니처가 없이도 알려진 악성 코드와 알려지지 않은 악성 코드(컨테이너 내부에서 실행되는 경우 포함)를 모두 차단
  - **동작 기반 IOA** - 의심스러운 프로세스를 차단하고 정교한 파일리스 공격 및 맬웨어 프리 공격을 방지
  - **맞춤형 IOA** - 탐지 및 차단할 특정 동작을 정의할 수 있음
  - **해시 방지** - 자체 블랙리스트 정의 가능
- 통합 위협 인텔리전스를 통해 특성을 포함한 전체적인 공격 배경 정보를 제공
- 24 시간 관리형 위협 사냥 기능으로 은밀한 공격이 탐지되지 않을 가능성을 없애고 침해를 차단

지능형 EDR

CrowdStrike Falcon 플랫폼에 탑재된 지능형 EDR 의 기능:

- 이벤트를 지속적으로 모니터링하여 컨테이너 내부 실행 활동을 포함한 Linux 워크로드 활동에 대한 가시성을 제공하며, 다양하고 풍부한 데이터와 이벤트 세부 정보를 통해 임시 워크로드와 제거된 워크로드도 조사 가능
- Linux 관련 고유한 네트워크 이벤트를 수집하여 네트워크 연결 형성 프로세스, 사용된 프로토콜, 로컬 및 원격 서버 세부 정보를 파악하고 지난 한 시간 동안 이루어진 연결 횟수를 계산하여 표시(최대 90 일 동안 이벤트 기록 재현)
- 모든 워크로드에 대한 통합 가시성을 제공하므로 다양한 워크로드 유형 및 클라우드 환경에 걸친 공격을 탐지 및 조사
- 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
- 감염된 워크로드를 억제 및 조사할 수 있는 대응 기능 제공
- 경고를 MITRE ATT&CK® 프레임워크에 매핑하여 조사 속도 단축

멀티 클라우드 워크로드 검색

Falcon 은 다음과 같은 기능을 통해 퍼블릭 및 하이브리드 클라우드 흔적의 범위와 특성을 가시적으로 확인합니다.

- 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 Linux 워크로드 정보를 실시간으로 제공
- Falcon 플랫폼을 통해 보호되지 않는 Linux 워크로드 파악
- 모든 워크로드를 보호하고 위험을 탐지 및 완화하며 공격 노출면을 줄일 수 있도록 클라우드 흔적에 대한 분석 정보 제공

FALCOON 컨테이너 보안

Linux 호스트에서 실행되는 단일 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 구축을 포함하는 컨테이너 흔적을 가시적으로 확인 가능하며 트렌드, 가동 시간, 사용된 이미지, 구성을 비롯한 컨테이너 사용 정보를 표시하여 위험성이 있으며 잘못 구성된 컨테이너를 파악

호스트 및 컨테이너 보안에 대해 단일 관리 콘솔을 제공

간편함과 성능

- CrowdStrike 의 클라우드 네이티브 플랫폼으로 복잡성이 사라지고 보안 운영이 간소화되어 운영 비용을 절감할 수 있음
- 지속적인 시그니처 업데이트나 온프레미스 관리 인프라, 복잡한 통합 과정 없이 운영되는 솔루션
- 분석, 검색, 조사 중에도 설치 및 일상적 운영으로 인해 호스트에 미치는 영향 없음
- Falcon 을 통해 동일 콘솔의 모든 워크로드와 시스템에 대한 선제적 위협 사냥 기능 제공
- 몇 분 내로 구축 및 가동

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.

광범위한 지원

CrowdStrike Falcon 은 Linux 배포 환경(Amazon Linux, Red Hat, CentOS, Oracle, SUSE, Debian, Ubuntu) 전반에 걸쳐 구축할 수 있는 종합적 보호 범위를 제공합니다. AWS, GCP, Microsoft Azure 등, 모든 퍼블릭 클라우드와 함께 사용할 수 있습니다.

광범위한 컨테이너 지원의 예로는 Docker, Kubernetes 와 같은 OCI(Open Container Initiative) 기반 컨테이너를 비롯하여 GKE(Google Kubernetes Engine), EKS(Amazon Elastic Kubernetes Service), ECS(Amazon Elastic Container Service), AKS(Azure Kubernetes Service), OpenShift 와 같은 자체 관리형 및 호스트된 오케스트레이션 플랫폼 등이 있습니다.

차세대 AV

무료 체험 시작하기

자세히 알아보기: www.crowdstrike.com