Proofpoint Insider Threat Management

현대 기업을 위한 사용자 중심 Insider Threat Management

주요 이점

- 위험한 내부자 활동 감지 및 엔드포인트의 데이터 손실 방지
- 내부자 위협 및 데이터 손실 사고에 대한 대응 간소화
- 최신 클라우드 네이티브 백엔드를 기반으로 확장성이 뛰어난 SaaS를 구현하여 가치 창출 시간 단축
- 경량 엔드포인트 에이전트로 사용자의 생산성 유지

주요 ITM 사용 사례

- 사용자 위험 식별
- 엔드포인트의 데이터 손실 방지
- 사용자 원인 사고에 대한 신속한 대응
- 내부자 위협 프로그램 확대

Proofpoint ITM(Insider Threat Management)은 데이터 손실, 악의적인 행위, 내부자가 관련된 브랜드 이미지 손상으로부터 조직을 보호하는 사용자 중심의 접근 방식을 활용합니다. 권한 있는 사용자가 악의적의거나 부주의하게, 혹은 자신도 모르게 해를 끼치지 않도록 방어해 드립니다. 또한, 사용자 활동과 데이터 이동의 상관관계를 분석하여 내부자 주도 데이터 침해로부터 보호합니다. 여기에 실시간으로 위험한 행동을 감지하여 범죄의 증거를 알기 쉽게 설명합니다.

실시간 위험 동작 감지 및 방지

ITM을 사용하면 애플리케이션, 파일, 데스크톱, 서버 및 가상화 환경 전반에 걸쳐 위험한 동작을 상호 연관시킬 수 있습니다. 이는 사건이 발생한 후만이 아니라 사용자가 뒤에 있을 때 발생합니다. 실시간으로 상황을 파악할 수 있으므로 내부자 위협 사건의 연관성을 찾고 탐지하며 해결할 수 있는 강력한 방법을 새롭게 제공합니다.

크라우드 소싱된 실제 위협 시나리오

위험한 동작을 실시간으로 탐지할 수 있습니다. 여기에 해당되는 동작은 아래와 같습니다.

- 데이터 유출
- 위험한 데이터 수평 이동
- 특권 남용
- 애플리케이션 오용
- 무단 액세스
- 위험한 우발적 행동

부울 논리 기반 규칙 작성기를 사용하면 고객의 환경에 맞는 규칙 및 트리거를 쉽게 작성할 수 있습니다. 즉시 사용 가능한 위협 시나리오로 시작하여 기존 시나리오를 변경할 수 있습니다. 또는 처음부터 시나리오를 작성할 수도 있습니다. 당사의 광범위한 내부자 위협 규칙은 Carnegie Mellon의 CERT, NITTF, NIST 및 고객의 집단 지식에 기반합니다.

포인트 앤 클릭 위협 사냥

위협 사냥은 외부 위협에만 해당하지 않습니다. ITM을 사용하면 불필요하거나 악의적인 위험을 감수하는 내부자를 식별할 수 있습니다. 당사의 포인트 앤 클릭 인터페이스로 이상 동작을 선제적으로 탐색하고 검색할 수 있습니다.

간편한 포인트 앤 클릭 사냥으로 아래 행동을 수행할 수 있습니다.

- 환경에 맞춰 위험한 동작 및 활동 검토
- 지능형 그룹화로 관련 없는 수천 개의 활동을 필터링하고 관련 있는 활동에 집중
- 타임라인 및 스크린샷 기반 증거로 비정상적인 동작을 상황별로 파악

데이터 분류 지원

MIP(Microsoft Information Protection)와 통합합니다. ITM 에이전트는 사용자가 파일과 상호 작용할 때 민감도 레이블을 실시간으로 읽습니다. 파일 MIP 민감도 레이블, 파일 원본, 파일 유형 및 파일 대상을 기반으로 탐지 및 방지 규칙을 설정할 수 있습니다.

데이터 손실 방지

ITM은 공통 엔드포인트 채널을 통해 중요 데이터의 유출을 방지할 수 있습니다. 여기에는 로컬 동기화 폴더, 네트워크 연결 스토리지, 플래시 드라이브, 멀티미디어 장치 및 전화와 같은 USB 연결 장치가 포함됩니다. 사용자가 오프라인 상태일 때도 작동합니다.

다음과 같이 사용자, 그룹 및 호스트별로 USB 기반 활동을 관리할 수 있습니다.

- USB로의 데이터 쓰기 차단
- 일부 USB 장치의 허용 목록
- 파일명 패턴과 일치하는 파일 차단
- 차단 파일 형식
- 차단 파일 소스
- 글로벌 방지 규칙 적용

Proofpoint Enterprise DLP 제품군은 메일 및 클라우드 앱으로 보호 기능을 확장할 수 있습니다.

사고 대응 가속화

많은 조직이 보안 관련 사고 발생 후 내부자 위협 이니셔티브에 착수합니다. 그리고 이런 조직 대다수는 기존 보안 툴의 일반 워크플로우가 내부자 위협과 함께 작동하지 않는다는 사실을 깨닫게 됩니다. 내부자 데이터는 민감하기 때문에 비사이버 보안팀과 매우 긴밀하게 협업해야 합니다.

직접 컨텍스트와 반박할 수 없는 증거

당사의 워크플로우는 사용자 주도 이벤트에 맞춰 조정됩니다. 수집된 모든 메타데이터 및 스크린샷에서 키워드와 필터를 사용하여 보안 이벤트를 검색할 수 있습니다. 다시 말하면, 완전히 새로운 쿼리 언어를 배울 필요가 없습니다. 선제적인 위협 사냥이나 향후 조사에 참조할 수 있도록 필터를 저장할 수 있습니다.

조사와 관련된 중요 이벤트 및 경고를 식별하면 이러한 이벤트에 태그를 지정하고 분류할 수 있습니다. 증거를 공유해야 하는 경우 태그로 관련 이벤트 및 경고를 찾을 수 있습니다. 또한, PDF와 같은 일반 파일 형식으로 내보낼 수 있습니다. 이러한 보고서에는 스크린샷 증거와 누가 무엇을 어디에서 언제 했는지에 대한 관련 컨텍스트가 포함됩니다. 이로써 사이버보안을 훨씬 더 쉽게 관리할 수 있으며 인사, 법률, 규정 준수팀 및 조사관이 이해하기 쉽습니다.

ITM 아키텍처의 장점

당사의 클라우드 기반 아키텍처는 조정, 사용 편의성, 보안 및 확장성을 고려하여 구축되었습니다. 업계 최고의 경량 엔드포인트 에이전트를 사용하여 작업 데이터를 수집합니다. 사용자를 방해하지 않으면서 사용자가 시스템에서 수행하는 작업에 대해 앱에 구애받지 않는 강력한 가시성을 얻을 수 있습니다.

순수 SaaS 구축

Proofpoint Endpoint DLP는 조정, 분석, 보안, 개인 정보 보호 및 확장성을 위해 구축된 최신 SaaS 플랫폼입니다. 이는 백엔드에서 설정 시간과 비용을 절감합니다. 또한, 조직 전반에 걸쳐 보안 관리자의 지속적인 관리를 간소화합니다. 이를 통해, 데이터 활동을 즉각적으로 파악할 수 있습니다.

두 가지 문제, 하나의 경량 솔루션

Endpoint DLP 및 Insider Threat Management는 경량 단일 에이전트와 최신 SaaS 아키텍처를 사용합니다. Endpoint DLP를 함께 사용하면 일반 사용자를 데이터 손실 위험으로부터 보호할 수 있습니다. ITM은 이러한 보호 기능을 악성 및 고위험 사용자의 모든 위험한 동작으로 확장합니다.

자세한 정보

자세한 내용은 **proofpoint.com**을 참조하십시오.