# 내부자 위협으로부터 방어

## 엔드포인트에서 인간 중심 데이터 손실 및 내부자 위협 방지

### 주요 이점

- 위험한 행동에 대한 가시성을 제공하여 재정적 손실과 브랜드 손상으로부터 보호
- 반박할 수 없는 증거로 조사 가속화
- 손쉬운 배포와 경량 엔드포인트 에이전트로 가치 창출 시간 단축

현대의 분산된 인력은 언제 어디서나 작업합니다. 직원, 타사 및 계약업체는 노트북, 이메일, 클라우드 등 데이터의 위치에 상관없이 그 어느 때보다 많은 데이터에 액세스할 수 있습니다. 따라서 데이터 손실 및 내부자 위협 위험이 사상 최고치에 도달했습니다.

내부자 위협은 부주의하거나 악의적이거나 손상된 사용자의 세 가지 유형으로 분류될 수 있습니다. 내부자 위협을 사전에 방어하려면 사용자 행동의 이면에 있는 맥락을 이해해야 합니다. 그러면 내부자 주도 사고가 발생한 경우에 가장 적합한 대응을 결정하는 데에도 도움이 됩니다.

Proofpoint는 사용자 활동 및 행동에 대한 심층적인 가시성을 제공하여 일반 사용자에 의한 데이터 손실로부터 보호하고 위험한 사용자의 위협을 방어합니다. Proofpoint는 채널 전반에서 가시성과 인사이트를 제공하는 포괄적이고 상황에 맞는 클라우드 네이티브 솔루션을 제공합니다. 중앙 집중식 콘솔에서 정책을 설정하고, 알림을 분류하고, 위협을 사냥하고, 사고에 대응할 수 있습니다. 데이터 손실을 방지하고 내부자 위반을 빠르고 효율적으로 조사할 수 있도록 도와드리겠습니다. 사고를 빠르게 해결할수록 비즈니스, 브랜드 및 수익 피해를 줄일 수 있습니다.

## 일반 사용자와 위험한 사용자를 모두 모니터링

### 단일 엔드포인트 에이전트를 통한 유연성

오늘날의 경쟁적인 환경에서는 내부자 위협과 엔드포인트 기반 데이터 손실을 관리할 수 있어야 합니다. 하지만 대부분의 조직은 모든 사용자의 모든 활동에 대한 엔드포인트 원격 측정을 항상 수집할 필요는 없으며 그렇게 해서도 안 됩니다. 대신 더 적응적인 위험 기반 접근 방식을 사용하는 것이 좋습니다. 그러면 모든 사용자의 일부 활동과 가장 위험한 사용자의 모든 활동에 대한 인사이트를 얻을 수 있습니다.

이 솔루션 세트는 Proofpoint의 통합 인간 중심 보안 플랫폼의 일부이며 사람에게서 비롯되는 위험 중 네 가지 주요 영역을 완화합니다.

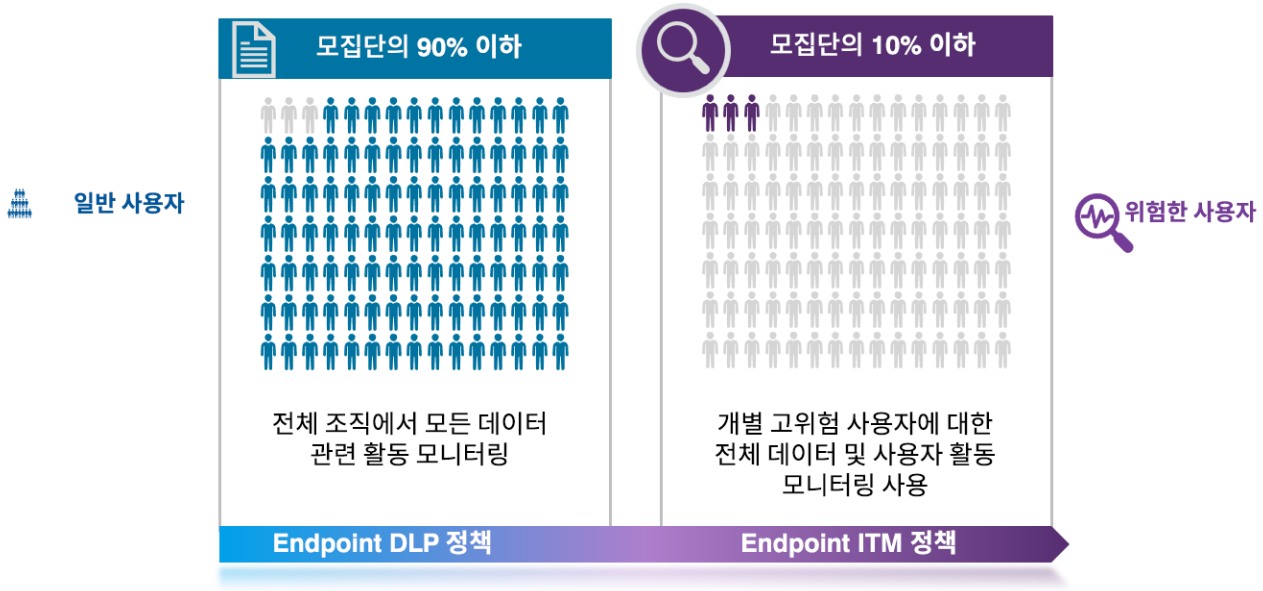


그림 1: 단일 경량 엔드포인트 에이전트에서 일반 사용자와 위험한 사용자 모두를 유연하게 모니터링할 수 있습니다.

이 요구 사항을 충족하기 위해 Proofpoint는 데이터 손실로부터 보호하고 사용자 활동에 대한 심층적인 가시성을 제공하는 경량 엔드포인트 에이전트를 개발했습니다. 정책 구성을 간단히 변경하여 각 사용자 또는 사용자 그룹에 대해 수집하는 데이터의 양과 유형을 조정할 수 있습니다. 이 적응형 접근 방식을 사용하면 보다 효과적으로 알림을 조사하고 대응할 수 있습니다. 또한 극단적으로 많은 데이터를 수집할 필요가 없습니다.

일반 사용자는 일반적으로 정상적인 비즈니스 사용자입니다. 일반 사용자는 위험도가 낮기 때문에 모니터링하여 데이터 활동과 사용자 컨텍스트에 대한 인사이트를 얻을 수 있습니다.

위험한 사용자는 더 많은 주의가 필요합니다. 위험한 사용자에는 퇴사하거나 입사하는 직원, 타사 계약업체, 권한 있는 계정 소유자 및 대상 사용자(예: 고위 임원)가 포함될 수 있습니다. 이들의 동기와 의도를 파악하려면 심층적인 인사이트가 필요합니다.

# 사용자 및 데이터 활동에 대한 가시성 및 컨텍스트 제공

## 일반 사용자와 위험한 사용자에 대한 가시성

Proofpoint는 엔드포인트에서 사용자의 데이터 상호 작용에 대한 원격 측정을 수집합니다. 여기에는 사용자가 파일 형식을 조작하는 경우(예: 파일 확장자 변경) 또는 민감한 데이터가 들어 있는 파일의 이름을 바꾸는 경우를 기록하는 것이 포함됩니다. 또한 승인되지 않은 웹사이트로 업로드하거나 클라우드 동기화 폴더에 복사하는 등 민감한 데이터를 이동하려고 시도하는 경우를 기록하는 것도 포함됩니다.

Proofpoint는 위험한 사용자를 모니터링할 수 있도록 엔드포인트 기반 활동을 전체적으로 보여줍니다. 데이터 상호 작용을 캡처하고, 응용 프로그램 사용, 엔드포인트 활동에 대한 화면 캡처 및 기타 위험한 행동에 대한 가시성을 제공합니다. 이러한 행동에는 승인되지 않은 도구 설치 및 실행, 보안 관리자 활동 수행 등이 포함될 수 있습니다. Proofpoint는 위험한 활동에 대한 질문(누가, 무엇을, 어디서, 언제)에 대답할 수 있도록 심층적인 인사이트를 제공합니다. 데이터 손실 또는 정책을 준수하지 않는 행동이 발생한 경우 컨텍스트와 인사이트를 통해 사용자의 의도를 더 잘 파악할 수 있습니다.

## 콘텐츠 스캔 및 데이터 분류

가장 위험한 이동 중인 민감한 데이터를 식별할 수 있습니다. 이를 위해 Microsoft Information Protection 등에서 이동 중인 콘텐츠를 스캔하고 데이터 분류 레이블을 읽을 수 있습니다.

보안 팀과 최종 사용자에 대해 별도의 워크플로를 만들지 않고 데이터 분류에 대한 기존 투자를 활용하여 민감한 비즈니스 정보(예: 지적 재산)를 식별할 수 있습니다. 데이터 분류를 활용하여 규제된 고객 데이터를 식별할 수 없는 경우도 있습니다. 하지만 Proofpoint Cloud DLP 및 Proofpoint Email DLP의 동급 최고의 검증된 콘텐츠 감지기를 활용할 수 있습니다.

# 위험한 사용자 행동 및 데이터 상호 작용을 실시간으로 감지

## 유연한 규칙 엔진

처음부터 환경에 맞춰서 규칙 및 트리거를 만들 수 있습니다. 또는 사전 구축된 위협 시나리오를 조정할 수 있습니다. 사용자 그룹, 앱, 날짜/시간, 데이터 민감도, 분류 레이블, 소스 및 목적지, 이동 채널 및 유형별로 시나리오를 수정할 수 있습니다.

## 알림 라이브러리

Proofpoint에는 즉시 사용 가능한 알림 라이브러리가 포함되어 있습니다. 알림 라이브러리를 사용하면 설정을 간소화하고 가치 창출 시간을 단축할 수 있습니다. 엔드포인트에서 위험한 데이터 이동 및 상호 작용을 경고할 수 있습니다. 또한 광범위한 위험한 내부자 위협을 경고할 수 있습니다.

## 엔드포인트의 승인되지 않은 데이터 유출 방지

위험한 사용자 및 데이터 활동을 감지하는 것으로는 충분하지 않은 경우도 있습니다. 또한 데이터 유출을 실시간에 적극적으로 차단해야 합니다. Proofpoint 플랫폼을 사용하면 USB 장치에서 데이터를 송/수신하거나 파일을 클라우드 폴더에 동기화하는 등 사용자의 정책을 준수하지 않는 민감한 데이터 상호 작용을 차단할 수 있습니다.

사용자, 사용자 그룹, 엔드포인트 그룹, 프로세스 이름, USB 장치, USB 일련 번호, USB 공급업체, 데이터 분류 레이블, 소스 URL, 콘텐츠 스캔 일치 등을 기준으로 보호를 맞춤 설정할 수 있습니다.

# 사고 조사 및 대응 가속화

## 통합 콘솔

Proofpoint를 이용하면 내부자 주도 조사 및 대응을 간소화할 수 있습니다. 엔드포인트, 이메일 및 클라우드에서 원격 측정을 수집하여 한 곳에서 다중 채널 가시성을 확보할 수 있습니다. 통합 콘솔에서는 활동을 모니터링하고, 알림의 상관관계를 파악하고, 조사를 관리하고, 위협을 사냥하고, 사고 대응을 조율할 수 있도록 직관적인 시각화를 제공합니다.

## 알림 분류

내부자로 인해 발생하는 보안 알림을 조사하고 해결하는 것이 쉽기만 한 것은 아닙니다. 처리하는 데 많은 시간과 비용이 들 수도 있습니다. 인사, 규정 준수, 법률 및 LOB(사업부) 관리자와 같은 비기술 부서가 포함되는 경우도 있습니다.

Proofpoint를 사용하여 각 알림을 심층적으로 분석할 수 있습니다. 타임라인 기반 보기를 통해 메타데이터를 확인하고 상황별 인사이트를 확보할 수 있습니다. 보안 팀은 추가 조사가 필요한 이벤트와 즉시 종결할 수 있는 이벤트를 신속하게 파악할 수 있습니다.

## 알림 라이브러리

| 데이터 활동 | 사용자 활동(ITM에만 해당) | |
|---|---|---|
| 데이터 상호 작용 및 유출 관련 알림(40개 이상의 알림): | 전체 엔드포인트 사용자 활동 관련 알림(100개 이상의 알림): | |
| • 웹에 파일 업로드<br>• USB에 파일 복사<br>• 로컬 클라우드 동기화에 파일 복사<br>• 파일 인쇄<br>• 파일 활동(이름 바꾸기, 이동, 삭제)<br>• 파일 추적(웹에서 USB, 웹 간 등)<br>• 웹에서 파일 다운로드<br>• 이메일 첨부 파일로 전송된 파일<br>• 이메일/엔드포인트에서 다운로드된 파일 | • 정보 숨기기<br>• 무단 액세스<br>• 보안 제어 우회<br>• 부주의한 행동<br>• 백도어 만들기<br>• 저작권 침해<br>• 승인되지 않은 일반 도구<br>• 승인되지 않은 관리 작업 | • 승인되지 않은 데이터베이스 관리자(DBA) 활동<br>• 공격 준비<br>• IT 방해 행위<br>• 권한 상승<br>• ID 도용<br>• 의심스러운 GIT 활동<br>• 허용되지 않은 사용 |

기본 워크플로 및 정보 공유 기능은 부서 간 협업을 간소화합니다. 여러 이벤트에 걸친 위험한 활동 기록을 일반 파일 형식(예: PDF)으로 내보낼 수 있습니다. Proofpoint를 사용하면 PDF 내보내기에 스크린샷 증거와 관련 컨텍스트가 포함됩니다. 따라서 인사, 법률 등 비기술 팀에서 포렌식 조사를 위해 데이터를 쉽게 해석할 수 있습니다.

### 위험한 사용자를 위한 화면 캡처

사진 한 장이 천 마디 말보다 더 가치가 있을 수 있습니다. Proofpoint는 사용자 활동에 대한 스크린샷을 캡처할 수 있습니다. 악의적이거나 부주의한 행동에 대한 명확하고 반박할 수 없는 증거가 있으면 인사, 법률 및 관리자의 의사 결정을 알리는 데 도움이 될 수 있습니다.

복잡한 보안 환경에 쉽게 통합하기 위해 웹훅을 사용하여 SIEM 및 SOAR 도구에서 알림을 쉽게 수집할 수 있습니다. 그러면 사고를 신속하게 식별하여 분류할 수 있습니다.

복잡한 보안 인프라를 사용하는 경우 전체 시스템에서 단일 정보 소스를 유지해야 할 수 있습니다. Proofpoint에서는 Proofpoint 데이터를 사용자가 소유하고 운영하는 AWS S3 스토리지로 자동으로 내보내므로 간단합니다.

## 개인정보 보호 및 규정 준수 요구 사항 해결

### 데이터 상주 및 스토리지 관리

Proofpoint는 다중 지역 데이터 센터 지원을 제공합니다. 따라서 데이터 개인정보 보호 및 데이터 상주 요구 사항을 충족하는 데 도움이 됩니다. 현재 미국, 유럽, 오스트레일리아 및 일본에서 데이터 센터를 운영하고 있습니다.

엔드포인트를 그룹화하여 엔드포인트 데이터 스토리지를 제어할 수 있습니다. 저장을 위해 각 그룹 또는 영역을 데이터 센터로 매핑할 수 있습니다. 그러면 고객이 지역별로 데이터를 쉽게 분류할 수 있습니다.

### 속성 기반 액세스 제어를 통해 개인정보 보호 문제 해결

개인정보 보호 요구 사항을 해결하려면 데이터 액세스에 대한 통제권과 유연성이 필요합니다. Proofpoint를 사용하면 보안 분석가가 알아야 하는 데이터만 볼 수 있도록 액세스를 쉽게 관리할 수 있습니다. 분석가에게 특정 사용자의 데이터에 대한 액세스 권한만 부여하거나 해당 데이터에 액세스할 수 있는 기간을 유연하게 제한할 수 있습니다.

## 다중 채널 가시성 및 컨텍스트 확보

Proofpoint에서는 콘텐츠, 행동 및 위협에 대한 인간 중심 접근 방식에 따라 데이터 손실을 막고 내부자 위협을 차단합니다. 통합 콘솔을 통해 엔드포인트, 클라우드, 이메일, 웹 등 여러 채널에 대한 가시성 및 상황별 인사이트를 확보할 수 있습니다.

채널에 상관없이 하나의 콘솔에서 정책을 설정하고, 위협을 사냥하고, 알림을 조사하고 대응할 수 있습니다. 또한 알림 메타데이터를 심층적으로 분석할 수 있습니다. 그러면 이벤트 이전, 도중, 이후에 발생한 내용을 파악할 수 있습니다. Proofpoint는 신속하게 배포될 수 있는 클라우드 네이티브 솔루션이며, 가치 창출 시간을 단축할 수 있도록 도와줍니다.

## 자세히 알아보기

자세한 내용은 **proofpoint.com**을 참조하십시오.