

Proofpoint DLP 혁신

데이터 손실 방지 프로그램 및 아키텍처 혁신

주요 이점

- 클라우드 및 엔드포인트에서 영향을 끼치는 데이터 손실 위험을 신속하게 탐지하여 적절히 조치
- 사고 해결 가속화(DLP 알림 분류, 조사 및 대응 포함)
- 신속한 배포, 자동 확장, 손쉬운 관리, 시간 절약
- DLP 프로그램의 성공 보장

오늘날의 인력은 어디서나 작업합니다. 직원들은 더 편한 삶을 위해 생성형 AI와 같은 승인되지 않은 도구를 사용합니다. 또한 개인 장치를 사용하여 클라우드 응용 프로그램에서 조직의 데이터에 액세스합니다. 정보 보안 전문가는 데이터 개인정보 보호 요구 사항을 준수하면서 이러한 최신 IT 도구 및 관행을 안전하게 채택할 수 있도록 지원해야 합니다. 이렇게 하려면 클라우드 데이터와 사용자 행동에 대한 더 나은 가시성이 필요합니다. 기존 데이터 손실 방지(DLP) 도구는 이러한 요구 사항을 적절히 해결하지 못합니다. 심지어 사일로화되었고 가격이 비싸며 유지 및 확장하기 어려운 경우도 있습니다.

Proofpoint DLP 혁신을 통해 DLP 프로그램 및 아키텍처를 현대화할 수 있습니다. 이 솔루션에서는 데이터 손실 방지에 대한 인간 중심 접근 방식을 채택합니다. 또한 민감한 콘텐츠를 식별하고 사용자 행동에 대한 깊이 있는 가시성을 제공합니다. 분석가는 클라우드 및 엔드포인트에서 데이터 위험을 신속하게 평가하고, 정확도 높은 판단을 내리고, 적절한 조치를 취할 수 있습니다. 통합 콘솔과 강력한 분석을 통해 사고 해결을 가속화합니다. 이 솔루션은 최신 개인정보 보호 제어와 고도로 안정적인 에이전트를 갖춘 클라우드 네이티브 아키텍처를 기반으로 합니다. 또한 빠르게 배포되고, 자동으로 확장하며, 손쉽게 유지 관리됩니다.

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



클라우드 및 엔드포인트에서 영향을 끼치는 데이터 손실 위험 감지 사용자 행동에 대한 깊이 있는 가시성

인간 중심 접근 방식에 따라 Microsoft 365, Google Workspace, Salesforce 등과 같은 엔드포인트 및 클라우드 응용 프로그램에서 영향을 끼치는 데이터 손실 위험을 빠르게 감지할 수 있습니다. 사용자 의도에 대한 인사이트를 통해 데이터 위험에 적절한 방식으로 대응할 수 있습니다. 이를 위해 DLP 혁신에서는 관리형 및 비관리형 엔드포인트와 클라우드 전반에서 사용자의 데이터 상호작용을 모니터링합니다. 민감한 데이터 유출(예: 파일을 승인되지 않은 USB에 복사하거나 개인 클라우드 폴더에 업로드하는 행위)을 감지하고 방지합니다. 클라우드 응용 프로그램에서 민감한 파일의 광범위한 공유를 감지하고 파일 공유 권한을 자동으로 축소할 수 있습니다. 또한 다음에 관한 원격 측정 데이터를 수집합니다.

- 파일 조작(예: 민감한 데이터가 포함된 파일의 이름 바꾸기, 파일 확장자 변경)(그림 1 참조)
- 웹사이트 및 응용 프로그램 사용(예: 웹에서 데이터 백업 도구 또는 해킹 도구를 다운로드하여 설치)
- 가장 위험한 사용자의 위험한 행동(예: 제어를 제거하기 위한 Windows 레지스트리 조작)

정확한 콘텐츠 식별

DLP 혁신에서는 고급 콘텐츠 식별 방법을 사용하여 데이터를 보호합니다. 예를 들어 클라우드에서 정확한 데이터 일치(EDM)와 OCR(광학 문자 인식)을 사용하여 이미지에서 의료 기록 번호를 감지할 수 있습니다. 그러면 의료 서비스 공급업체에서 위양성과 위음성을 크게 줄일 수 있습니다.

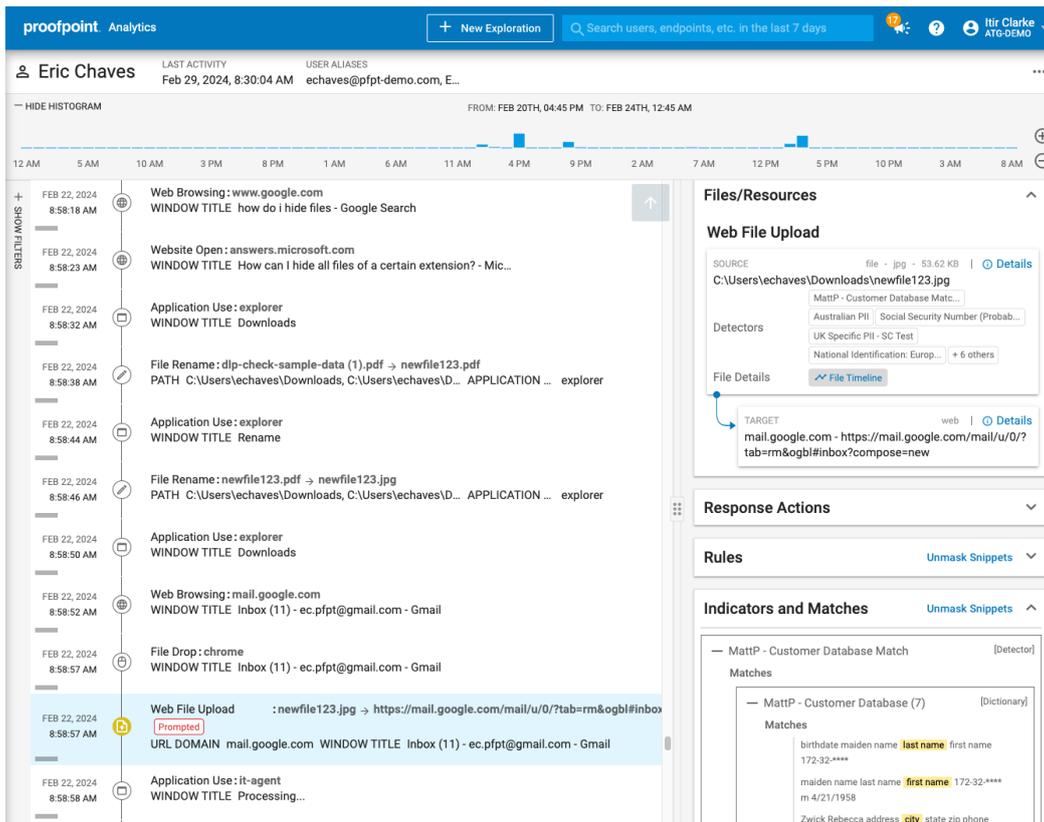


그림 1: 한 사용자가 “dlp-check-sample-date.pdf” 파일의 이름을 “newfile123.pdf”로 바꾸고, 파일 확장자를 jpg로 변경하고, 민감한 데이터를 개인 웹 메일에 업로드합니다. 이 사용자 행동 및 민감한 콘텐츠 식별 타임라인에서는 이 사용자가 회사 정책을 우회하려고 시도 중이며 추가 조사가 필요하다는 것을 시사합니다.

통합 콘솔로 사고 해결 가속화

효율적인 교차 채널 DLP 운영

기존 DLP 도구나 사일로화된 DLP 도구를 사용하는 보안 팀은 종종 조사 기간이 길어지고 위반 사항을 놓치게 되면서 부담을 느끼고 있습니다. DLP 혁신에서는 클라우드와 엔드포인트뿐만 아니라 이메일에서도 원격 측정 데이터를 수집하여 한곳에서 데이터 위험에 대한 교차 채널 가시성을 제공합니다. 따라서 Proofpoint Email DLP, 조사 및 대응을 포함하여 채널 전반에서 알림 분류가 간소화됩니다. 콘솔은 직관적인 시각화를 비롯한 강력한 분석과 워크플로를 제공하여 다음 사항을 지원합니다.

- 알림 분류 및 상관관계 파악(그림 2 참조)
- 타임라인 보기에서 사용자의 데이터 상호작용을 조사하여 위험의 의도성과 심각도 결정(그림 1 참조)
- 생성, 수정, 공유 중인 파일의 계보 추적
- 사고 대응 조율
- 즉시 사용 가능한 경영 보고서를 사용하여 효율 및 적용 범위를 입증하고 감사를 위한 유연한 보고서 생성
- 데이터 액세스 및 개인정보 보호를 위한 DLP 정책 및 관리자 제어 관리

사전 예방적 데이터 보안

콘솔의 정교한 검색 및 필터 기능을 통해 맞춤형 탐색 환경을 구축하여 데이터 위험을 사전에 관리할 수 있습니다. 조직에서 발생할 수 있거나 생성형 AI와 같은 새로운 도구의 도입에 따르는 위험한 활동과 데이터 유출을 검색할 수 있습니다. 사용자 활동 타임라인 보기를 사용하여 각 보안 사고에 대한 주체, 대상, 위치, 시기, 이유를 파악할 수 있습니다.

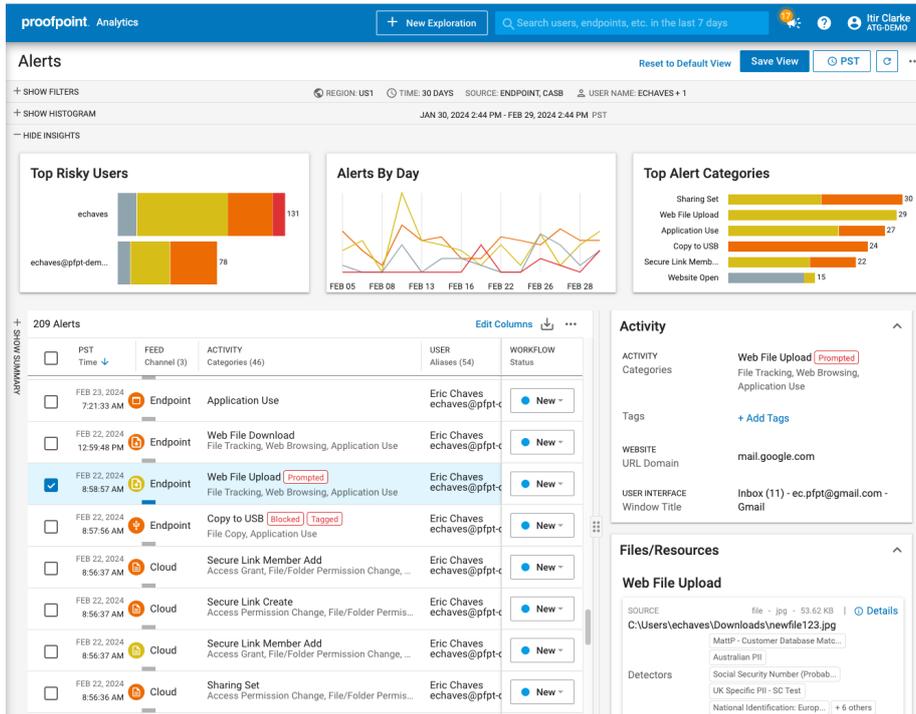


그림 2: 통합 콘솔은 여러 콘솔 간에 전환할 필요가 없어 클라우드 및 엔드포인트 전반에서 알림 관리를 간소화합니다. 이 예에서 분석가는 특정 사용자에 대한 알림을 필터링했습니다. 해당 사용자는 민감한 데이터를 개인 Gmail 계정(파란색 강조 표시)에 업로드하고, 파일을 USB에 복사하고, 회사 클라우드 파일을 공유하여 알림을 생성했습니다.

Table	Tree	EDIT	FEED	ACTIVITY	USER	ACTIVITY
User Name (1)	ALERT	Time	Channel (1)	Categories (13)	User Name (1)	Summary
u-59d0e7b	136	JUN 7, 2022 8:38:45 AM	Endpoint	Document Open File Open, Application Use	u-59d0e7b	ENDPOINT - HOSTNAME e-8d12173 FILES/RESOURCES - NAME codes.txt FILES/RESOURCES - PATH C:\Users*****\txt
u-008edd3	114	JUN 7, 2022 7:55:08 AM	Endpoint	Copy File to Clipboard File Copy, Application Use	u-59d0e7b	ENDPOINT - HOSTNAME e-b07cb90 FILES/RESOURCES - NAME oitcons PROCESS/APPLICATION - APP Finder
u-afdc052	84	JUN 6, 2022 10:52:41 AM	Endpoint	Web File Download File Tracking, Web Browsing, Applica...	u-afdc052	ENDPOINT - HOSTNAME e-10b6ebb FILES/RESOURCES - NAME sample (1).pdf WEBSITE - URL DOMAIN 10.2.2.48
u-d46e23c	48	JUN 6, 2022 10:52:33 AM	Endpoint	Web File Download File Tracking, Web Browsing, Applica...	u-afdc052	ENDPOINT - HOSTNAME e-c4654bf FILES/RESOURCES - NAME csharp_tutorial (1).pdf WEBSITE - URL DOMAIN 10.2.2.48
u-fbe199a	25	JUN 6, 2022 10:09:27 AM	Endpoint	Web File Download File Tracking, Web Browsing, Applica...	aeb8c30	ENDPOINT - HOSTNAME e-beee960 FILES/RESOURCES - NAME nws-tpc-5.doc WEBSITE - URL DOMAIN 10.2.2.48
u-fc43f27	22	JUN 6, 2022 8:51:16 AM	Endpoint	Web File Download File Tracking, Web Browsing, Applica...	u-afdc052	ENDPOINT - HOSTNAME e-f31730d FILES/RESOURCES - NAME sample.pdf WEBSITE - URL DOMAIN 10.2.2.48
aeb8c30	8					
114a883	7					

그림 3: 콘솔에서 사용자 식별 정보를 익명화하면 조사 대상 사용자의 개인정보를 보호하고 분석가의 편견을 없앨 수 있습니다.

최신 아키텍처를 통한 신속한 배포 및 자동 확장

서비스로 제공되는 DLP 혁신은 소중한 시간을 절약합니다. 또한 빠르게 배포되고, 자동으로 확장하며, 손쉽게 유지 관리됩니다. 이 솔루션은 클라우드에 공유 서비스가 구축된 모듈식 솔루션입니다. Proofpoint 멀티 테넌트 클라우드 네이티브 솔루션은 확장성이 뛰어나며 API를 기반으로 합니다. 이 솔루션은 테넌트당 수십만 명의 사용자로 확장될 수 있습니다. 이 솔루션은 Proofpoint Email DLP 및 에코시스템 파트너(Microsoft, Okta, Splunk, ServiceNow 등)와의 API 통합을 지원합니다.

세분화된 데이터 개인정보 보호 제어

DLP 혁신은 글로벌 클라우드 네이티브 콘솔을 제공하지만 여러 지역에서 데이터를 저장할 수 있습니다. 속성 기반 액세스 제어를 통해 지역별 역할에 따라 부서 간에 협력적으로 알림 및 조사를 관리할 수 있습니다. 콘솔에서 민감한 데이터를 가리고 사용자 식별 데이터를 익명화할 수 있습니다. 즉, 작업 위치에 상관없이 지역별 데이터 개인정보 보호 및 상주 요구 사항을 충족할 수 있습니다.

안정성이 뛰어난 엔드포인트 에이전트

Proofpoint의 사용자 모드 경량 에이전트는 안정성이 뛰어나며 빠르게 배포할 수 있습니다. 또한 데이터 손실 탐지 성능이 뛰어나며 잠재적 내부자 위협에 대한 가시성을 높입니다. 플랫폼에서 정책을 변경하기만 하면 보안 관리자가 에이전트의 행동을 즉시 변경할 수 있습니다. 커널 모드 에이전트와 달리 안정적인 사용자 경험을 보장하여 지원 센터 예약 티켓을 없애고 시간을 절약할 수 있습니다.

사전 예방적 전문 지식을 통해 DLP 프로그램의 성공 보장

DLP 프로그램을 시작하거나 혁신하기 위해 도움이 필요한 경우 Proofpoint 관리형 정보 보호 서비스를 선택할 수 있습니다. DLP 프로그램을 설계, 구현, 공동 관리할 수 있도록 고도로 숙련된 전문가를 지원합니다. 직원 연속성을 보장하고 임원급 지표 등에 액세스하여 DLP 프로그램의 성공을 보장할 수 있습니다.

자세히 알아보기

자세한 내용은 proofpoint.com을 참조하십시오.

Proofpoint 정보

Proofpoint, Inc.는 조직의 최대 자산과 최대 위험인 사람을 보호하는 업계 최고의 사이버 보안 회사입니다. 통합된 클라우드 기반 솔루션 제품군을 통해 Proofpoint는 전 세계 기업이 타겟 위협을 차단하고, 데이터를 보호하고, 사이버 공격에 대한 사용자의 회복력을 강화하도록 지원합니다. Fortune 100대 기업의 85%를 비롯한 모든 규모의 선도적인 조직들이 Proofpoint의 사람 중심 보안 및 규정 준수 솔루션을 활용하여 이메일, 클라우드, 소셜 미디어 및 웹을 통해 전파되는 가장 중요한 위협을 완화하고 있습니다. 자세한 내용은 www.proofpoint.com에서 확인할 수 있습니다.