proofpoint.

KURZVORSTELLUNG

Proofpoint Enterprise DLP

Transformieren Sie Ihr Datensicherheitsprogramm und Ihre Architektur

Wichtige Vorteile

- Verhinderung von Datenverlust durch E-Mails, Cloud, Endpunkte und GenAI-Apps
- Schnellere Behebung von Zwischenfällen sowie schnellere Triage, Untersuchung und Reaktion bei DLP-Warnmeldungen
- Schnelle Bereitstellung, automatische Skalierung und einfache Wartung
- Erfüllung der Datenschutzanforderungen in den USA und anderen Regionen

Mitarbeiter gefährden Daten heute auf vielfältige Weise. Sie verwenden private Geräte, um auf Cloud-Anwendungen zuzugreifen und Daten über E-Mail, Endpunkte und Collaboration-Tools auszutauschen. Zudem sind nicht genehmigte GenAI-Tools (generative KI) oft nur einen Browserklick entfernt. Sicherheitsteams konzentrieren sich stärker darauf, die Privatsphäre zu schützen, die Einhaltung von Vorschriften zu gewährleisten und die verantwortungsvolle Nutzung von GenAI zu unterstützen. Sicherheitsverstöße haben heute immer größere Auswirkungen auf die Finanzen, die Reputation und Audits.

Unternehmen benötigen einen besseren Überblick über vertrauliche Daten und müssen sehen, wie Anwender diese Daten in E-Mails, Clouds, Endpunkten und in GenAI-Apps nutzen. Ältere DLP-Tools (Datenverlustprävention) sind jedoch oft isoliert, lassen sich kaum skalieren und decken nicht alle Kanäle konsistent ab. Außerdem sind sie nicht in der Lage, die neuen KI-bezogenen Risiken zu reduzieren.

Proofpoint Enterprise DLP unterstützt einen einheitlichen, adaptiven Ansatz zur Datenverlustprävention (DLP). Dazu verhindert die Lösung Datenverluste in E-Mails, Clouds, Endpunkten und KI-Apps, die von Menschen verursacht werden. Zudem hilft sie Sicherheitsteams, effizienter zu arbeiten.

Proofpoint identifiziert vertrauliche Inhalte und zeigt, wie Mitarbeiter sie verwenden. Über die einheitliche Konsole lassen sich Warnmeldungen zentral verwalten und Zwischenfälle in sämtlichen Kanälen untersuchen. Analysen und KI-gestützte Klassifizierungen helfen Teams, Datenrisiken einzuschätzen, fundiertere Entscheidungen zu treffen und schnell zu handeln. Die Lösung wird in der Cloud ausgeführt, skaliert von selbst und lässt sich einfach bereitstellen und warten. Zusätzlich verfügt sie über moderne Datenschutzkontrollen und einen hochstabilen Agenten.

Kanalübergreifende Reduzierung von Datensicherheitsrisiken

Ein klarer Überblick über das Anwenderverhalten

Proofpoint überwacht, wie Mitarbeiter Daten in E-Mails, auf verwalteten und nicht verwalteten Endpunkten, in GenAI-Tools und in Cloud-Apps (wie Microsoft 365, Google Workspace und Salesforce) verwenden, zeigt die Absicht der Anwender an und erkennt sowie verhindert Datenexfiltration. Beispiele hierfür sind das Kopieren von Dateien auf ein nicht autorisiertes USB-Laufwerk, das Hochladen vertraulicher Dateien in einen privaten Cloud-Ordner oder das Weitergeben vertraulicher Informationen über KI-Prompts.

Proofpoint hilft Unternehmen bei der sicheren Nutzung von GenAI, indem vertrauliche Daten erkannt, blockiert und redigiert werden, bevor sie für genehmigte oder nicht genehmigte KI-Apps freigegeben werden. Teams können Richtlinien in Browser- und Desktop-KI-Apps durchsetzen, und intelligente Problembehebungen und geführte Anwendererlebnisse helfen Anwendern, produktiv zu bleiben.

Proofpoint überwacht und steuert Folgendes:

- Datei-Uploads in KI-Apps
- Copy-and-Paste-Vorgänge, die vertrauliche Daten umfassen
- KI-Prompts, die regulierte oder proprietäre Informationen enthalten
- Vertrauliche Anhänge, die über E-Mail- und Cloud-Collaboration-Tools weitergegeben werden
- Riskantes Anwenderverhalten auf Endpunkten und in Cloud-Diensten

Proofpoint lässt sich in LDAP und Active Directory integrieren. Sie können Gruppen aus diesen Verzeichnissen verwenden, um detaillierte E-Mail-Verschlüsselungsrichtlinien zu definieren und dynamisch anzuwenden. Unsere Lösung überwacht zum Beispiel auf diese Verhaltensweisen:

- **Dateiänderungen**, z. B. Umbenennen von Dateien mit vertraulichen Daten oder Ändern ihrer Dateierweiterungen
- **Ungewöhnliche Nutzung von Websites und Anwendungen**, z. B. Herunterladen von Datensicherungen oder Hacking-Tools
- **Gefährliche Verhaltensweisen hochriskanter Anwender**, z. B. Manipulieren der Windows-Registrierung zur Deaktivierung von Sicherheitskontrollen

Präzise Erkennung von Inhalten und KI-gestützte Klassifizierung

Proofpoint verbessert die Erkennungsgenauigkeit mit mehr als 110 sofort einsetzbaren KI-gestützten Klassifikatoren, die Dokumentkategorien identifizieren und DLP-Warnmeldungen einen Geschäftskontext hinzufügen. Die Klassifikatoren arbeiten mit Musterabgleich, exaktem Datenabgleich (EDM), Abgleich indexierter Dokumente (IDM), Texterkennung mit OCR (Optical Character Recognition) und Fingerabdrucktechnologien. Diese Kombination reduziert Fehlalarme und verbessert den Schutz auf allen Kanälen.

Proofpoint Autonomous Custom Classification (ACC) verwendet große Sprachmodelle (LLMs), um die vertraulichen Inhalte des jeweiligen Unternehmens zu erfassen, ohne dass dazu manuelles Tuning erforderlich ist. Teams können proprietäre Daten wie Quellcode, Finanzmodelle, technische Dokumente und Kundendaten schnell finden und schützen. Dies vereinfacht die Erstellung von Richtlinien und ermöglicht schnellere Rendite.

Gemeinsam genutzte KI-gestützte Erkennungsmechanismen bieten konsistenten Schutz für alle DLP-Kanäle des Unternehmens. Unternehmen können personenbezogene Daten, geschützte Gesundheitsdaten, Zahlungskartendaten, Anmeldedaten, geistiges Eigentum und vertrauliche Geschäftsinformationen erkennen und klassifizieren. LLM-angereicherte Benachrichtigungen fügen Kontext hinzu, sodass Teams schneller Untersuchungen durchführen und reagieren können.

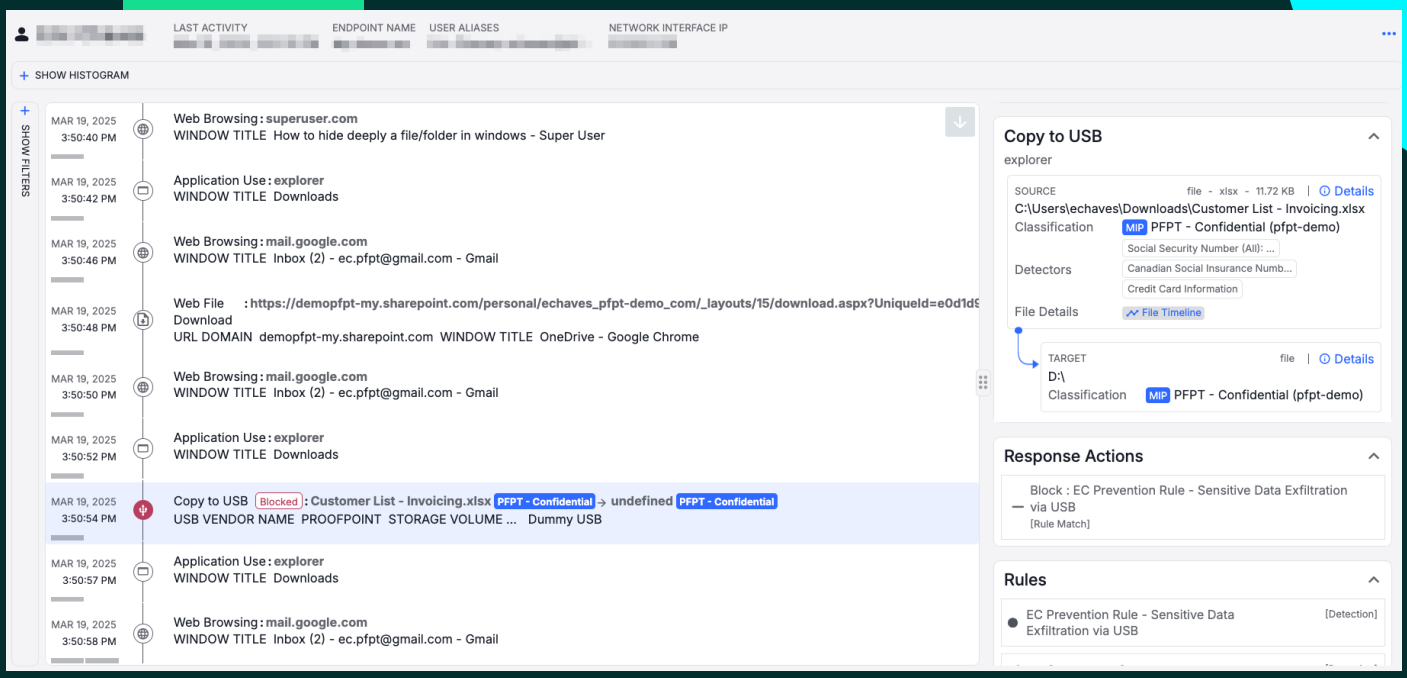

Abb. 1: Dieses Data Security Workbench-Beispiel zeigt eine riskante Abfolge von Anwenderaktionen. Der Anwender sucht nach Möglichkeiten, eine Datei zu verbergen, lädt eine vertrauliche Datei von SharePoint herunter und versucht, sie auf ein USB-Laufwerk zu kopieren. Die Aktionen und der Zeitplan deuten auf eine mögliche Umgehung von Richtlinien hin, die einer weiteren Überprüfung bedürfen.

Adaptive Richtliniendurchsetzung und geführte Behebung

Proofpoint ermöglicht die gemeinsame Durchsetzung von Richtlinien auf allen DLP-Kanälen. Teams können Richtlinien einmalig definieren und anschließend konsistent anwenden.

Adaptive Richtlinien helfen Teams, Anwender mit hohem Risiko zu überwachen, deren Absichten zu verstehen und Reaktionen zu automatisieren. Wenn eine Warnmeldung angezeigt wird, erfassen diese Richtlinien mehr Metadaten und visuelle Beweise. Durch klarere Einblicke können Analysten Untersuchungen beschleunigen, sodass die Gesamtbetriebskosten sinken.

Proofpoint verhindert auch den Verlust vertraulicher Daten durch GenAI-Prompts. Unsere Lösung unterstützt Anwender bei der sicheren KI-Nutzung. Dazu behebt sie automatisch das weit verbreitete File-Sharing in Cloud-Apps. Außerdem werden Anwender aufgefordert, das Kopieren vertraulicher Daten in einen Cloud-Ordner oder auf ein Netzlaufwerk zu begründen.

Geringere Betriebskosten und schnellere Behebung von Zwischenfällen

Effiziente, kanalübergreifende DLP-Aktionen

Teams, die isolierte, veraltete DLP-Tools verwenden, sehen sich häufig mit langsamen Untersuchungen, fragmentierter Transparenz und übersehenen Richtlinienverstößen konfrontiert. Proofpoint führt Erkennungs-, Richtlinien- und Governance-Kontrollen zu allen DLP-Kanälen zusammen. Die Data Security Workbench zentralisiert auch Telemetrie und Warnmeldungen. Dies unterstützt Teams beim Priorisieren von Warnmeldungen und hilft ihnen, schneller Untersuchungen durchzuführen und zügiger zu reagieren.

Die Data Security Workbench-Konsole bietet folgende Vorteile:

- Zeitleistenansichten der Anwenderinteraktionen mit vertraulichen Daten (siehe Abb. 1)
- Einheitliche Konfiguration von Warnmeldungen und DLP (siehe Abb. 2)
- Verknüpfte Untersuchungen über E-Mail, Cloud, Endpunkte und KI-Apps hinweg
- Nachverfolgung der Dateiherkunft, wenn Dateien erstellt, geändert und weitergegeben werden
- Bedrohungssuche zur frühen Erkennung und Untersuchung von Risiken
- Dashboards für Führungskräfte und Audit-Berichte

Proaktive Datensicherheit

Mit der Data Security Workbench können Sie Datenrisiken durchsuchen und filtern und benutzerdefinierte Ansichten erstellen, um diese Risiken zu verwalten, bevor sie wachsen. Sie können zum Beispiel nach Datenexfiltrationen und anderen riskanten Aktivitäten (z. B. nach der Verwendung nicht genehmigter GenAI-Tools) suchen. Die Anwenderzeitleiste zeigt, wer was, wo, wann und warum getan hat.

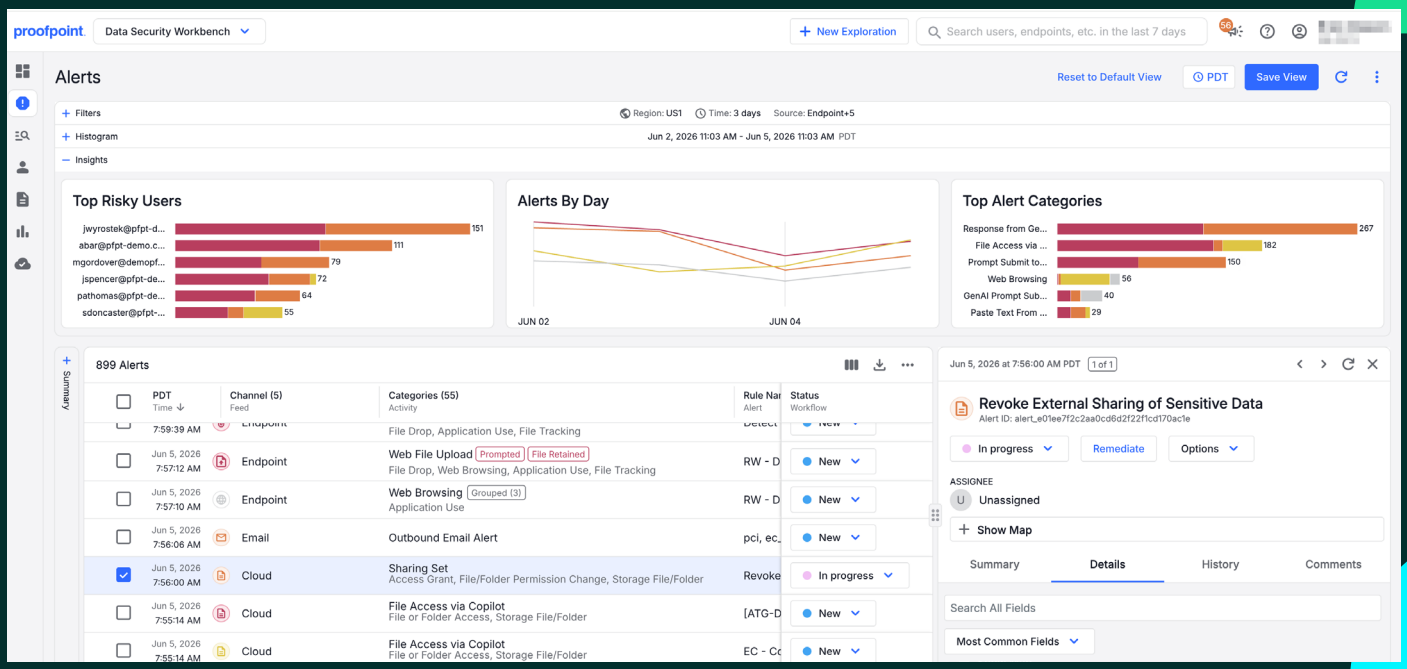

Abb. 2: In der Data Security Workbench können Sie benutzerdefinierte Untersuchungen von Datenrisiken erstellen.

Geschäftliche Flexibilität durch eine moderne Architektur

Proofpoint-Lösungen werden als Services bereitgestellt, sodass Sie wertvolle Zeit sparen. Die Services lassen sich schnell bereitstellen, skalieren automatisch und erleichtern die Wartung. Zudem sind sie modular aufgebaut und nutzen gemeinsam genutzte Cloud-Dienste. Unsere Cloud-nativen Lösungen unterstützen mehrere Mandanten und APIs. Sie sind auf Skalierbarkeit ausgelegt und können pro Mandant hunderttausende Anwender unterstützen. Die Proofpoint-Plattform lässt sich mit Partnern wie Microsoft, Okta, Splunk und ServiceNow integrieren.

Granulare Datenschutzkontrollen

Proofpoint bietet eine globale, Cloud-native Konsole und kann die Daten in mehreren Regionen speichern. Attributbasierte Zugriffskontrollen schränken nach Rolle, Funktion oder Region ein, wer Warnmeldungen und Untersuchungen einsehen kann. Datenmaskierung und Anonymisierung (siehe Abb. 3) tragen dazu bei, die regionalen Datenschutz- und Datenresidenzvorschriften einzuhalten.

Äußerst stabiler Endpunkt-Agent

Unser ressourcenschonender User Mode-Agent ist stabil, lässt sich schnell bereitstellen und nutzt bei der Erkennung von Datenverlust und möglichen Insider-Bedrohungen einen einzigartigen Ansatz. Sie können das Verhalten des Agenten ändern, indem Sie die Richtlinien auf der Plattform aktualisieren. Im Gegensatz zu Kernel Mode-Agenten gewährleistet der Agent von Proofpoint die reibungslose Nutzung und trägt so dazu bei, die Zahl der Helpdesk-Tickets zu reduzieren und Administratorzeit einzusparen.

Schnellere Rendite dank unseres Fachwissens

Für die Verhinderung von Datenverlust sind technische und produktbezogene Fachkenntnisse sowie ausgeprägte Kompetenzen im Bereich Datenkontrolle erforderlich. Proofpoint Applied-Services helfen Ihnen, Ihre Investition maximal zu nutzen, einen kontinuierlichen Betrieb zu unterstützen und Ihr Datenschutzprogramm weiterzuentwickeln.

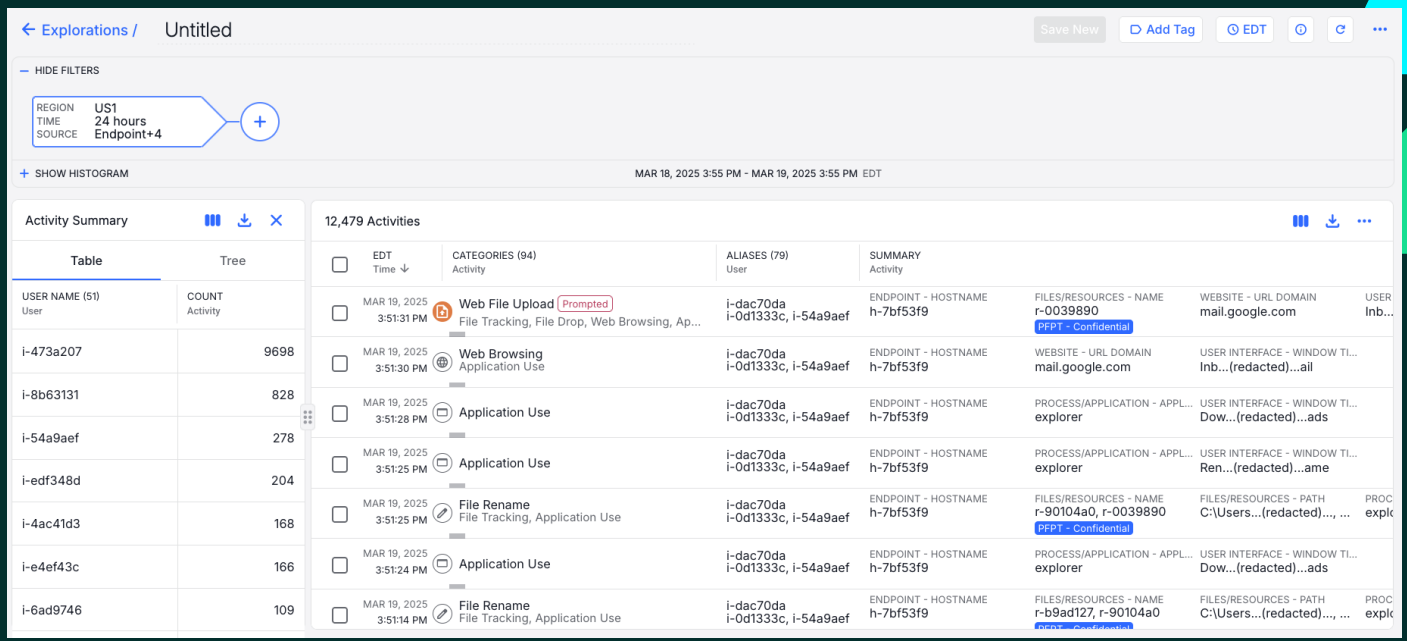

Abb. 3: Die Konsole kann Anwenderdaten während einer Untersuchung anonymisieren. Dies schützt die Privatsphäre und trägt dazu bei, Vorurteile von Analysten zu reduzieren.

Wichtige Funktionen	Proofpoint DLP Transform – Stufe 1	Proofpoint DLP Transform – Stufe 2	Add-ons
Detaillierter Anwender- und Dateikontext	✓	✓	
Bedrohungssuche zur frühzeitigen Erkennung und Untersuchung	✓	✓	
Ein User Mode-Agent für ITM und DLP	✓	✓	
Detaillierte DLP-Erkennungen (reguläre Ausdrücke, OCR, Abgleich indexierter Dokumente, exakter Datenabgleich) und Microsoft Information Protection (MIP)-Klassifizierung	✓	✓	
Sofort einsatzbereite KI- und autonome KI-Klassifizierer	✓	✓	
Datenherkunft zur Überwachung und Erkennung von Dateibewegungen	✓	✓	
API, Unterstützung von Forward/Reverse-Proxy	✓	✓	
Detektoren für verschiedenste Cloud-Bedrohungen	✓	✓	
Einheitliche Konfiguration von Warnmeldungen und DLP	✓	✓	
Granulare Kontrollen für Datenschutz und Zugriffsrechte	✓	✓	
Integration in das Sicherheitsökosystem (SIEM/SOAR/Teams)	✓	✓	
Erkennung und Analyse vertraulicher Daten in E-Mail-Nachrichten und -Anhängen		✓	
Dynamische Verschlüsselung von internen und an externe Empfänger gesendeten E-Mails		✓	
Fingerprinting für vertrauliche Dokumente in E-Mails		✓	
KI-gestützte Verhinderung von versehentlichem und vorsätzlichem Datenverlust per E-Mail			✓
Erkennung und Klassifizierung von Datenspeichern			✓
Erkennung und Behebung von Risiken in Datenspeichern			✓
Visuelle Erfassung von Insider-Bedrohungen			✓

Weitere Informationen

Weitere Informationen finden Sie unter **proofpoint.com/de**.

proofpoint.