proofpoint.

KURZVORSTELLUNG

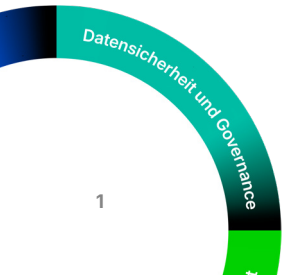
Proofpoint Data Loss Prevention

Transformieren Sie Ihr Datensicherheits-programm und Ihre Architektur

Wichtige Vorteile

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

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.



Mitarbeiter gefährden Daten heute auf ganz unterschiedliche Weise: Sie nutzen zunehmend nicht genehmigte Produktivitätstools wie generative KI (GenAI) und greifen über private Geräte auf die Cloud-Anwendungen ihres Arbeitgebers zu. Datensicherheitsteams können mit der Entwicklung kaum mehr Schritt halten, da sie ihre Arbeit mit immer weniger Ressourcen erledigen sollen. Gleichzeitig erweisen sich die Konsequenzen von Datenschutzverletzungen für die Unternehmen als immer kostspieliger. Finanzielle Einbußen, Rufschädigung und die Nichteinhaltung von Compliance-Vorschriften sind nur einige davon. Unternehmen benötigen daher mehr Einblicke in ihre E-Mail-, Cloud- und Endpunktdaten sowie in das Verhalten ihrer Anwender. Herkömmliche Lösungen für Datenverlustprävention (Data Loss Prevention, DLP) werden diesen Anforderungen allerdings nicht gerecht. Oft sind sie obendrein isoliert, teuer und lassen sich nur mit viel Aufwand warten und skalieren.

Die Proofpoint Data Loss Prevention (DLP)-Lösungen vereinfachen die Transformation Ihres Datensicherheitsprogramms und Ihrer Architektur. Sie folgen einem adaptiven Ansatz, der es Ihnen ermöglicht, Datenverlust durch menschliches Verhalten in Ihren E-Mail-, Cloud- und Endpunktkanälen effektiv und effizient zu begegnen.

Proofpoint kann vertrauliche Inhalte zuverlässig identifizieren und bietet umfassende Einblicke in das Anwenderverhalten. Über eine einheitliche Konsole lassen sich Warnmeldungen zentral verwalten und Zwischenfälle in sämtlichen Kanälen untersuchen. Leistungsstarke Analysefunktionen ermöglichen die schnelle und zuverlässige Bewertung von Datenrisiken, sodass Sie gezielte Maßnahmen ergreifen können. Unsere Lösungen basieren auf einer Cloud-nativen Architektur mit modernen Datenschutzkontrollen und einem äußerst stabilen Agenten. Sie werden automatisch skaliert und lassen sich einfach bereitstellen und warten.

Reduzierung von Risiken durch E-Mails, die Cloud und Endpunkte

Umfassende Einblicke in das Anwenderverhalten

Proofpoint überwacht, wie Ihre Mitarbeiter mit Daten interagieren – sei es per E-Mail, über verwaltete und nicht verwaltete Endpunkte oder in Cloud-Anwendungen wie Microsoft 365, Google Workspace und Salesforce. Wir liefern Ihnen Erkenntnisse zu den Absichten Ihrer Anwender, sodass Sie angemessen auf Datenrisiken reagieren können. Proofpoint erkennt und verhindert darüber hinaus die Exfiltration vertraulicher Daten, etwa durch Kopieren von Dateien auf ein nicht autorisiertes USB-Laufwerk oder das Hochladen von Daten in einen privaten Cloud-Ordner.

Über Integrationen in LDAP und Active Directory hilft Ihnen Proofpoint dabei, detaillierte Richtlinien zur E-Mail-Verschlüsselung zu definieren und dynamisch anzuwenden. Unsere Lösungen erfassen außerdem Telemetriedaten zu folgenden Verhaltensweisen:

- **Dateimanipulation** wie das Umbenennen von Dateien mit vertraulichen Daten oder Ändern ihrer Dateierweiterungen
- **Nutzung von Websites und Anwendungen** wie das Herunterladen und Installieren von Daten-Backups oder Hacker-Tools
- **Gefährliche Verhaltensweisen hochriskanter Anwender** wie das Manipulieren der Windows-Registrierung zur Deaktivierung von Sicherheitskontrollen

© Proofpoint, Inc. 2025

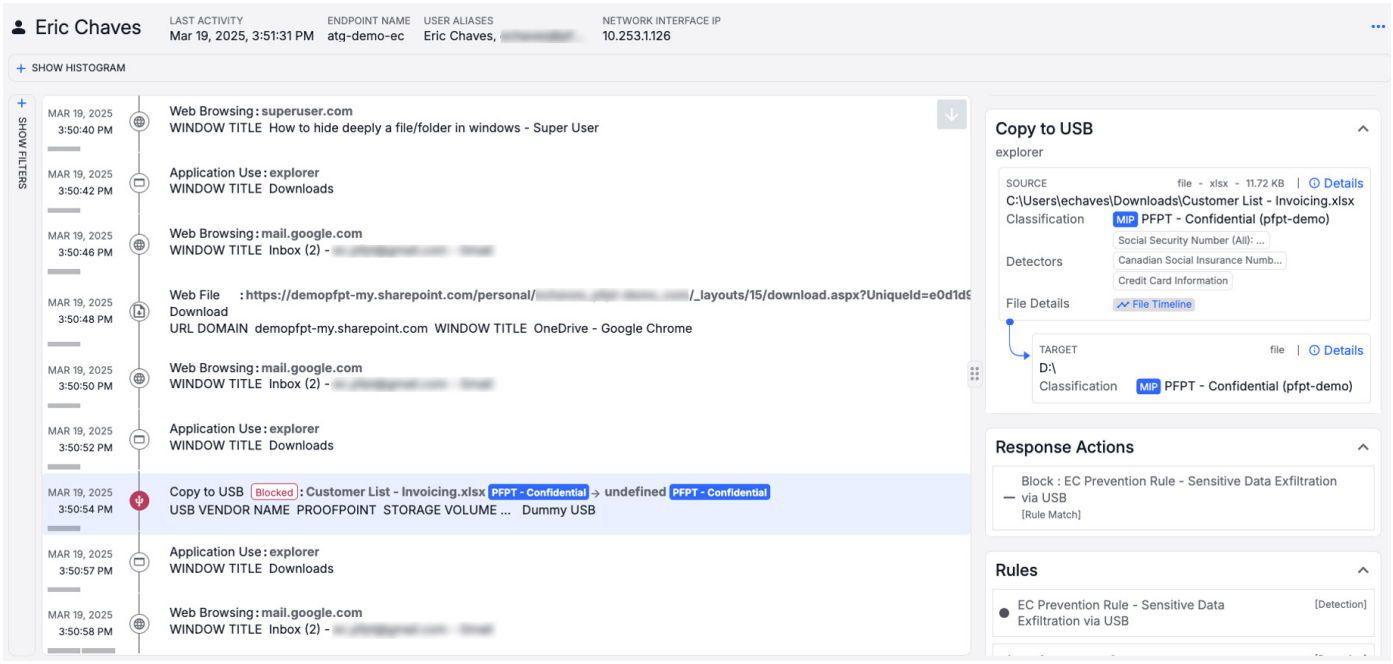


Abb. 1: In diesem Screenshot der Data Security Workbench-Konsole ruft ein Anwender eine Website mit einer Anleitung zum Verbergen von Dateien/Ordnern in Windows („How to hide deeply a file/folder in Windows“) auf. Anschließend lädt der Anwender eine Datei vom Sharepoint-Laufwerk des Unternehmens herunter. Danach kopiert er eine vertrauliche Datei mit Kundendaten (Customer List – invoicing.xlsx) auf ein USB-Laufwerk. Die Zeitleiste mit dem Anwenderverhalten und die Identifizierung von vertraulichem Inhalt ist für Analysten ein Zeichen dafür, dass der Anwender plant, die Unternehmensrichtlinie zu umgehen, und dass weitere Untersuchungen angebracht sind.

Zuverlässige Identifizierung von Inhalten

Proofpoint schützt Ihre Daten durch modernste Methoden zur Identifizierung von Inhalten. So lassen sich beispielsweise in der Cloud durch exakten Datenabgleich und optische Zeichenerkennung (OCR) in Bildern medizinische Datensätze erkennen, wodurch Anbieter aus dem Gesundheitswesen die Anzahl der False Positives und False Negatives reduzieren können.

Durch Erstellen von DLP-Richtlinien mit LLM-Klassifizierern (Large Language Model) können Sie neu entwickelte vertrauliche Inhalte ohne vorherige Klassifizierung schützen und dadurch Zeit sparen. Durch die Kombination von LLM-Klassifizierern und Musterabgleichen lässt sich zudem auch die Anzahl der False Positives reduzieren.

Warnmeldungen, die mit LLM angereichert wurden, machen das Kategorisieren von Dokumenten einfacher. Wird beispielsweise im Rahmen eines Musterabgleichs von Identifikationsnummern eine Warnmeldung ausgelöst, kann Proofpoint feststellen, ob es sich bei dem Dokument um eine Information zu einer Steuererstattung, ein Patientenformular oder um einen Kreditantrag handelt. Dies beschleunigt die Triage und Untersuchungen.

Adaptive Durchsetzung von Richtlinien

Dank der gewonnenen Einblicke in das Anwenderverhalten und in die Übertragung vertraulicher Daten können Sie gezielter auf Datenrisiken reagieren. Die Proofpoint-Lösungen verhindern den Verlust vertraulicher Daten über GenAI-Prompts und fördern den angemessenen Umgang mit KI, indem sie Anwender zu sicheren Verhaltensweisen schulen. Bei umfassender Freigabe von Dateien in Cloud-Anwendungen greifen sie automatisch ein und fordern Anwender zur Angabe eines Grundes auf, wenn sie versuchen, vertrauliche Daten in einen Cloud-Ordner oder auf ein Netzwerklaufwerk zu kopieren.

Adaptive Richtlinien ermöglichen eine engere Überwachung von Anwendern mit hohem Risiko und liefern Ihnen somit mehr Kontext und ein besseres Verständnis darüber, was Ihre Anwender vorhaben. Anstatt Richtlinien manuell anzupassen, können Sie Ihre Reaktion auf riskante Verhaltensweisen automatisieren. Dynamische Richtlinien erfassen bei der Auslösung einer Warnmeldung zusätzliche Metadaten und visuelle Nachweise über die Aktivitäten der Anwender, während Sie – dank der verbesserten Transparenz und verwertbaren Erkenntnisse – bei der Untersuchung wertvolle Zeit sparen und Ihre Gesamtbetriebskosten senken.

© Proofpoint, Inc. 2025

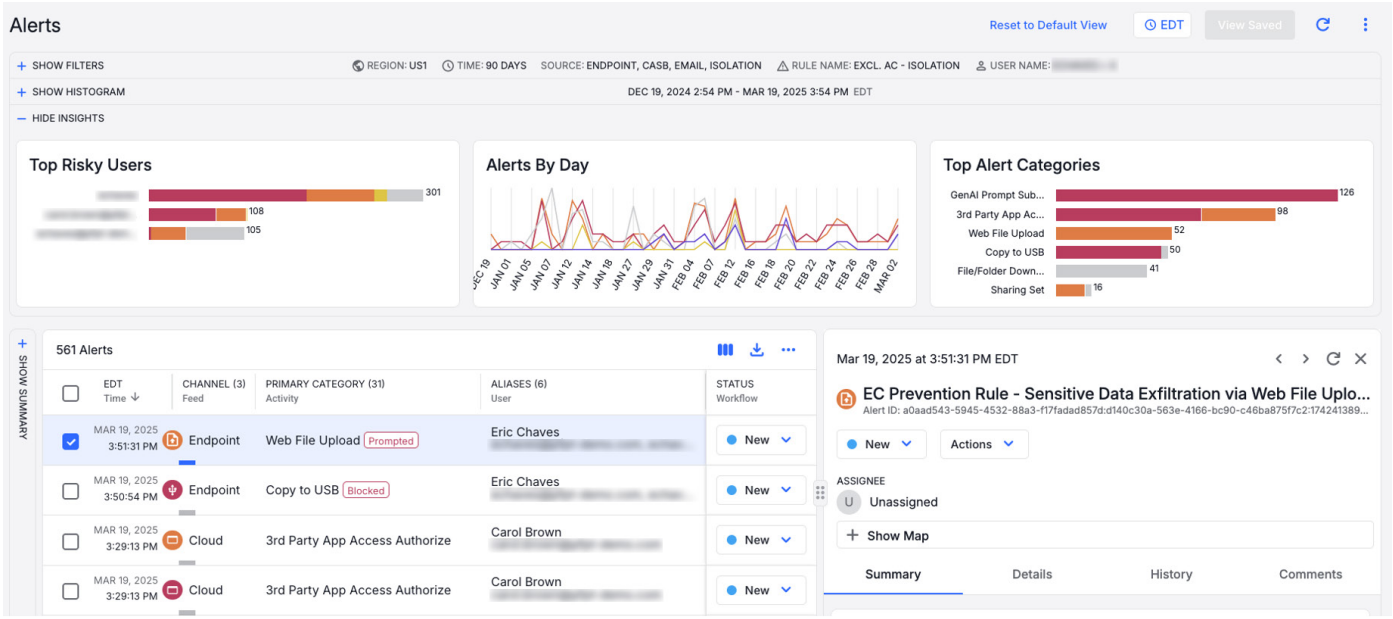


Abb. 2: Die Data Security Workbench führt die Verwaltung von Warnmeldungen zu E-Mails, Cloud und Endpunkten in einer zentralen Konsole zusammen. In diesem Beispiel hat ein Analyst die Warnmeldungen für einen bestimmten Anwender gefiltert. Die Workbench zeigt, dass der Anwender vertrauliche Daten in sein geschäftliches E-Mail-Konto hochgeladen und anschließend versucht hat, eine Datei auf ein USB-Laufwerk zu kopieren, was jedoch blockiert wurde.

Geringere Betriebskosten und schnellere Behebung von Zwischenfällen

Effiziente, kanalübergreifende DLP-Aktionen

Sicherheitsteams, die veraltete oder isolierte DLP-Tools verwenden, haben oft mit langwierigen Untersuchungen und unerkannten Richtlinienverletzungen zu kämpfen. Proofpoint bietet an einem zentralen Ort einen umfassenden und kanalübergreifenden Überblick über Ihre Datenrisiken, indem Telemetriedaten von Cloud-Anwendungen, Endpunkten und E-Mails erfasst werden. Dadurch wird die Triage von Warnmeldungem für alle Kanäle optimiert und Untersuchungen und Reaktionen werden beschleunigt. Mithilfe der in der Data Security Workbench-Konsole verfügbaren leistungsstarken Analysefunktionen, intuitiven Visualisierungen und effizienten Workflows lässt sich Folgendes erzielen:

- Untersuchung der Anwenderinteraktionen mit Daten in einer Zeitleistenansicht, um Absicht und Schweregrad des Risikos zu bestimmen (siehe Abb. 1)
- Triage und Korrelierung von Warnmeldungen (siehe Abb. 2)
- Verfolgung einer Datei mit Blick auf ihre Erstellung, Modifizierung und Freigabe
- Koordination der Reaktion auf Zwischenfälle
- Nutzung vorkonfigurierter Berichte für Führungskräfte, um Effizienz und Abdeckung zu demonstrieren, sowie Generierung benutzerdefinierter Berichte für Auditzwecke
- Implementierung und Verwaltung konsistenter DLP-Richtlinien und Administratorkontrollen für Datenzugriff und Datenschutz in allen Kanälen

Proaktive Datensicherheit

Die Data Security Workbench-Konsole enthält erweiterte Such- und Filterungsfunktionen, mit denen Sie individuelle Untersuchungen erstellen und Datenverlust-Risiken proaktiv reduzieren können. Sie können zum Beispiel nach Datenexfiltrationen und anderen riskanten Aktivitäten (z. B. nach der Verwendung nicht genehmigter GenAI-Tools) suchen. Dank einer Zeitleistenansicht der Anwenderaktivitäten finden Sie Antworten auf die Fragen nach dem Wer, Was, Wo, Wann und Warum hinter jedem Sicherheitszwischenfall.

© Proofpoint, Inc. 2025

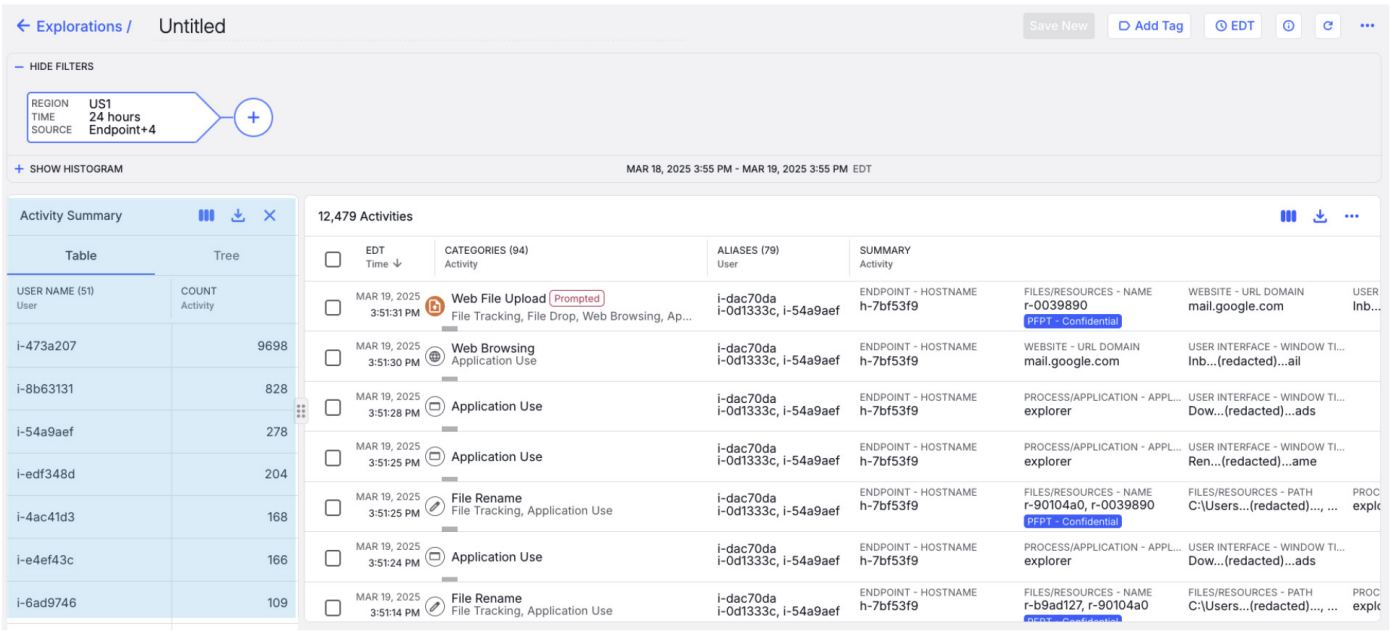


Abb. 3: Indem die Konsole die Namen der Anwender anonymisiert, wird deren Privatsphäre geschützt und Verzerrungen durch Analysten werden ausgeschlossen.

Geschäftliche Flexibilität durch eine moderne Architektur

Durch unsere modular aufgebauten und als Services bereitgestellten Lösungen, die sich schnell bereitstellen lassen, automatisch skalieren und einfache Wartung bieten, sparen Sie wertvolle Zeit. Unsere mandantenbasierten, Cloud-nativen Lösungen nutzen APIs, sind hochgradig skalierbar und können pro Mandant hunderttausende Anwender unterstützen. Die Proofpoint-Plattform bietet API-Integrationen in Produkte von Ökosystempartnern wie Microsoft, Okta, Splunk und ServiceNow.

Granulare Datenschutzkontrollen

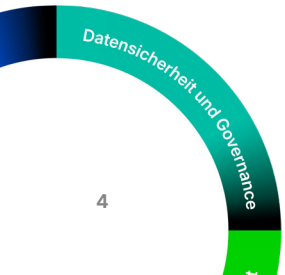
Proofpoint bietet zwar eine globale, Cloud-native Konsole, kann jedoch Daten in mehreren Regionen speichern. Sie können Warnmeldungen und Untersuchungen für alle Funktionen und regionalen Rollen mithilfe von attributbasierten Zugriffskontrollen verwalten sowie vertrauliche Daten maskieren oder anwenderbezogene Daten anonymisieren (siehe Abb. 3). Auf diese Weise wird die Einhaltung regionaler Anforderungen an Datenschutz und Speicherort sichergestellt.

Äußerst stabiler Endpunkt-Agent

Unser ressourcenschonender User Mode-Agent ist stabil, lässt sich schnell bereitstellen, bietet eine einzigartige Erkennung von Datenverlust und liefert einen Überblick über potenzielle Insider-Bedrohungen. Das Verhalten des Agenten lässt sich verändern, indem Sie die entsprechenden Richtlinien in der Plattform anpassen. Im Gegensatz zu Kernel Mode-Agenten gewährleistet der Agent von Proofpoint die reibungslose Nutzung, wodurch die Zahl der Helpdesk-Tickets und der Administrationsaufwand reduziert werden.

Schnellere Rendite dank unseres Fachwissens

Die Verhinderung von Datenverlust ist kein einfaches Unterfangen. Neben technischem Know-how und Produktkenntnissen ist dazu ein tiefes Verständnis von Datenkontrolle und Verwaltung notwendig. Proofpoint kann Sie als vertrauenswürdiger Partner auf Ihrem Weg begleiten, um Ihr DLP-Programm zum Erfolg zu führen. Mit unseren Services erhalten Sie die erforderliche Expertise, um Ihre Technologieinvestition zu optimieren, den kontinuierlichen Betrieb zu gewährleisten und Ihre Datenschutzstrategie zu optimieren.



© Proofpoint, Inc. 2025

Wichtige Funktionen von Proofpoint DLP-Lösungen

Vergleichen Sie unsere Lösungen, um die richtige Variante für Ihr Unternehmen zu finden

WICHTIGE FUNKTIONEN	PROOFPOINT DLP TRANSFORM	PROOFPOINT DLP TRANSFORM ADVANCED	ADD-ONS
Detaillierter Anwender- und Dateikontext	✓	✓	
Bedrohungssuche für proaktive Erkennungen und Untersuchungen	✓	✓	
Ein Benutzermodus-Agent für ITM und DLP	✓	✓	
Detaillierte DLP-Erkennungen (reguläre Ausdrücke, OCR, Abgleich indexierter Dokumente, exakter Datenabgleich) und Microsoft Information Protection (MIP)-Klassifizierung	✓	✓	
Überwachung und Erkennung von Dateibewegungen, inkl. Datenherkunft	✓	✓	
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			✓

proofpoint.

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune 100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: LinkedIn

Proofpoint ist eine eingetragene Marke von Proofpoint, Inc. in den USA und/oder anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer. © Proofpoint, Inc. 2025

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →