proofpoint.

KURZVORSTELLUNG

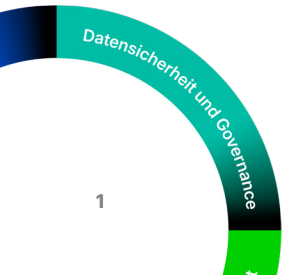
Proofpoint-Lösung für Datensicherheit

Einheitlicher Schutz vor Datenexfiltrationen, Datenkompromittierungen und Insider-Bedrohungen

Wichtige Vorteile

- Umfassender Schutz mit der branchenweit ersten einheitlichen Datensicherheitslösung
- Minimierung von Datensicherheitsrisiken durch Datenverlustprävention, Schutz vor Insider-Bedrohungen und Verwaltung der Datensicherheit auf allen Kanälen
- Optimierte Sicherheitsprozesse, schnellere Rendite der Sicherheitsmaßnahmen sowie niedrigere Gesamtbetriebskosten
- Geschäftliche Agilität dank sicherer KI-Nutzung und hoher Produktivität der Endanwender

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



Daten verlieren sich nicht von selbst

Menschliches Verhalten ist heute das größte Datensicherheitsrisiko. Dabei gefährden Mitarbeiter die Daten auf verschiedene Weise – durch Fehler, böswillige Absichten oder Kontenkompromittierungen. Proofpoint-Untersuchungen von 2024 zeigten, dass 71 % aller Datenverlustereignisse auf fahrlässige Anwender zurückgehen. Mitarbeiter, die das Unternehmen verlassen, waren für 87 % aller Cloud-basierten Dateiexfiltrationen verantwortlich.[1]

Die ständig zunehmende Verbreitung von Daten ist zu einer echten Herausforderung geworden. Heute speichern Wissensspezialisten ihre Daten in Public Clouds, File-Sharing-Diensten sowie in lokalen Datenbanken und steuern auch Daten zu Large Language Models (LLM) bei. Aufgrund dieser Fragmentierung fällt es IT- und Sicherheitsteams schwer, den Überblick zu behalten. Bei einem Drittel der Vorfälle werden „Schatten-Daten" kompromittiert, was im Durchschnitt zu 16 % höheren Kosten pro Datenschutzverletzung führt.[2]

Viele Datensicherheitstools berücksichtigen kein menschliches Verhalten und böswillige Absichten, können daher also auch nicht zwischen sicheren Aktivitäten und Datendiebstahlversuchen unterscheiden. Das führt zu falschen Alarmen, langwierigen Untersuchungen und einer ineffizienten Nutzung des Sicherheitsteams. Laut Gartner werden bis zum Jahr 2027 ganze 70 % aller Chief Information Security Officers (CISOs) in großen Unternehmen einen konsilidierten Ansatz zur Abwehr von Insider-Risiken und Datenexfiltrationen implementieren.[3]

Minimierung von Risiken, Senkung der Kosten und Steigerung der geschäftlichen Agilität

Proofpoint revolutioniert die Datensicherheit mit einem personenzentrierten und adaptiven Ansatz. Damit verringern bereits 53 % der Fortune 100 ihre Cybersicherheitsrisiken, senken die Betriebskosten und steigern die geschäftliche Agilität.

Unsere einheitliche Lösung schützt zuverlässig und präzise vor fahrlässigen, böswilligen und kompromittierten Anwendern. Dazu analysiert sie Inhalte und Verhalten in E-Mails, auf Endpunkten, in Software-as-a-Service-Anwendungen sowie in lokalen und Cloud-Datenspeichern. Die anpassbaren und automatisierten Kontrollen reagieren in Echtzeit auf neue Bedrohungen. Dadurch erhalten Sie umfassenden und tiefgehenden Schutz vor Datenexfiltrationen, Kompromittierungen und Insider-Bedrohungen.

70 %

aller CISOs werden bis 2027 einen konsolidierten Ansatz zur Abwehr von Insider-Risiken und Datenexfiltrationen implementieren.

Quelle: Gartner

1. Proofpoint: *Data Loss Landscape-Bericht*, 2024.
2. IBM und Ponemon Institute: *Cost of Data Breach Report* (Kosten von Datenkompromittierungen), 2025.
3. Gartner: *Market Guide for Data Loss Prevention* (Market Guide für Datenverlustprävention), 2025.

Produkte

- Proofpoint Enterprise DLP
- Proofpoint Data Security Posture Management
- Proofpoint Insider Threat Management
- Proofpoint Adaptive Email DLP

Reduzierung von Datensicherheitsrisiken

Die Proofpoint-Datensicherheitslösung vereint Datenverlustprävention (DLP), Data Security Posture Management (DSPM) und Abwehr von Insider-Bedrohungen (ITM). Dank dieser vereinten Komponenten können Sie datenbezogene Risiken effektiver identifizieren, überwachen und beheben. Unsere Lösung bietet folgende Vorteile:

- **Transformation Ihres DLP-Programms:** Die einheitliche Konsole mit einem einzigen Agenten für Proofpoint DLP und Proofpoint ITM identifiziert vertrauliche Informationen mithilfe von künstlicher Intelligenz. Dadurch versteht sie Inhalt sowie Kontext und kann so riskantes Verhalten aufdecken. Sie wendet adaptive Kontrollen an, die Datenexfiltrationen und Insider-Risiken auf Endpunkten, in E-Mails sowie der Cloud verhindern.
- **Kontrolle von Insider-Risiken:** Proofpoint ITM passt die Überwachung und Kontrolle abhängig vom Anwenderrisiko an. Sie erfasst eindeutige Nachweise für verdächtiges Anwenderverhalten und beschleunigt dadurch die Untersuchungen.
- **Reduzierung von Datenkompromittierungen:** Proofpoint DSPM nutzt In-Place-Scans zum Erkennen und Klassifizieren vertraulicher Daten in Cloud- und Hybrid-Umgebungen. Sie können übermäßige Berechtigungen mit einem einzigen Klick entfernen, erhalten einen Überblick über die Datenverbreitung und können auf diese Weise das Risiko für Datenkompromittierungen minimieren.
- **Schutz vor Datenverlust durch E-Mails:** Proofpoint Adaptive Email DLP erkennt und blockiert falsch adressierte E-Mails, falsche Dateianhänge und E-Mails an nicht autorisierte Konten.

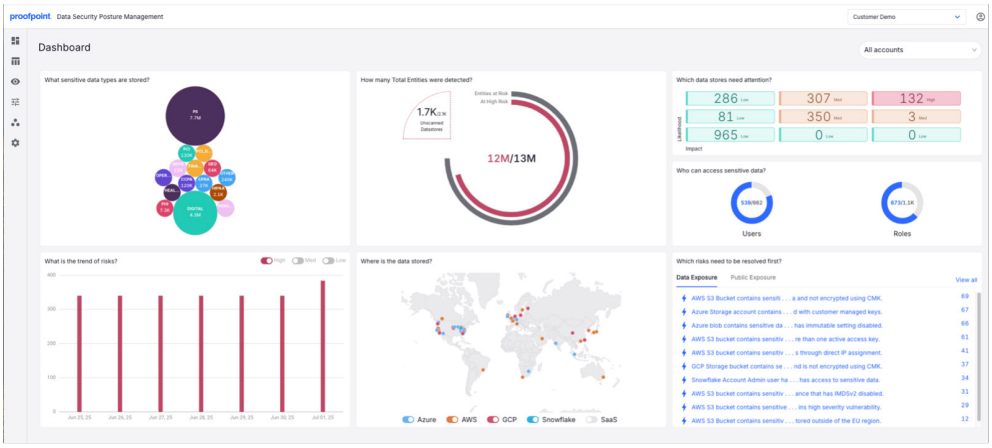
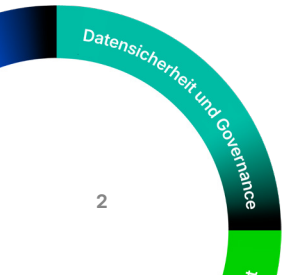


Abb. 1: Das DSPM-Dashboard zeigt die Arten der wertvollen oder vertraulichen Daten, ihren Geldwert und Risiken sowie die zugriffsberechtigten Personen.



Zuverlässige KI-gestützte Erkennung und kürzere Time-to-Value

- Der **KI-gestützte, agentenlose Scanner** von Proofpoint DSPM ermöglicht die zuverlässigste Datenklassifizierung auf dem Markt. Durch die Kombination aus Prüfungen regulärer Ausdrücke, Verarbeitung natürlicher Sprache (NLP) und LLMs wird die Leistung optimiert und der Ressourcenbedarf minimiert.
- **Proofpoint Nexus AI-Klassifizierer** identifizieren zuverlässig Dokumentkategorien wie Quellcode sowie Rechts-, Buchhaltungs- und Personaldokumente. Dadurch lassen sich geschäftskritische Informationen zuverlässig schützen.
- Die **Anomalieerkennung** identifiziert ungewöhnliche Datei-Änderungen und Anwenderaktivitäten in der Cloud und auf Endpunkten. Dies verhindert Datenverlust, Insider-Bedrohungen und Kontenkompromittierungen.
- Die **verhaltensbasierte KI** von Proofpoint Adaptive Email DLP stoppt Datenexfiltrationen an unautorisierte Konten, fehlgeleitete E-Mails und falsche Dateianhänge, die regelbasierte E-Mail-DLP-Lösungen nicht sehen.
- Die **KI-unterstützte Suche** nutzt NLP zur Vereinfachung von Analysen und Beschleunigung von Untersuchungen.

Höhere Effizienz und geringere Betriebskosten

Mit Proofpoint können Sie die Effizienz und Agilität Ihrer Datensicherheitsmaßnahmen und Insider-Bedrohungsabwehr steigern. Dadurch erzielen Sie schneller Rendite aus Ihren Sicherheitsmaßnahmen und können die Gesamtbetriebskosten senken.

Effiziente, kanalübergreifende Aktionen

Die adaptive und umfassende Proofpoint-Lösung steigert die Effizienz Ihres Datensicherheitsprogramms mithilfe von KI und intelligenter Automatisierung. Dank des umfassenden Überblicks, umfangreicher Kontextinformationen und erweiterter Analysen werden False-Positive-Warnungen vermieden. Ihr Sicherheitsteam erhält mehr Zeit, um sich auf strategische Initiativen zu konzentrieren.

- Der personenzentrierte Proofpoint-Schutz kombiniert Datentelemetrie mit Bedrohungsdaten und Erkenntnissen über Anwenderverhalten und Absichten. So können Sie zwischen sicheren sowie böswilligen Datenaktivitäten unterscheiden und effektiv auf Risiken reagieren.
- Das einheitliche Richtlinienmodul von Proofpoint setzt Richtlinien für DLP, DSPM und ITM konsistent durch. Adaptive Richtlinien passen sich an Veränderungen der Anwenderrisiken an.
- Proofpoint DSPM analysiert den Wert von Daten, die Wahrscheinlichkeit und Einfallstore potenzieller Angriffe sowie übermäßige Zugriffsrechte, um Risikobehebungsmaßnahmen zu priorisieren. Die Behebung übermäßiger Zugriffsrechte mit einem Klick vermeidet Datenkompromittierungen.
- Proofpoint Data Security Workbench hilft bei der Suche nach Bedrohungen, noch bevor sie zu Kompromittierungen werden können.

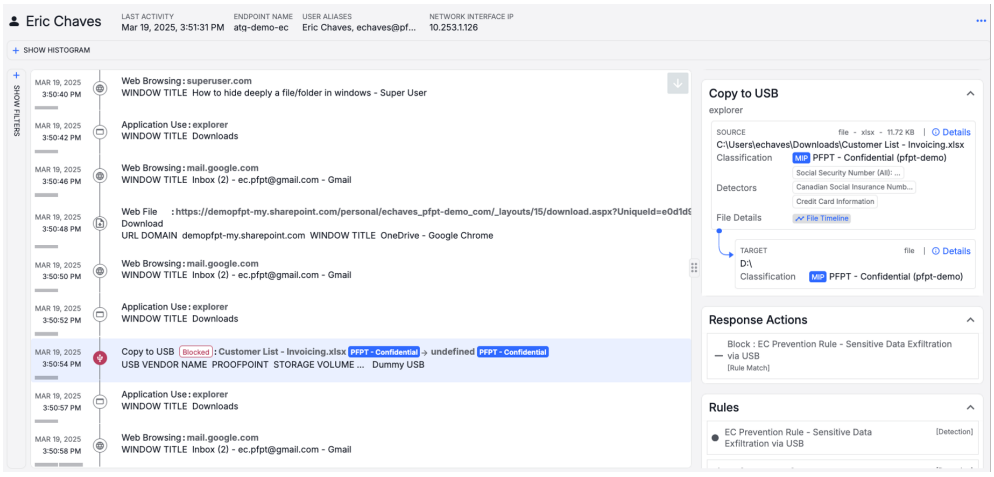
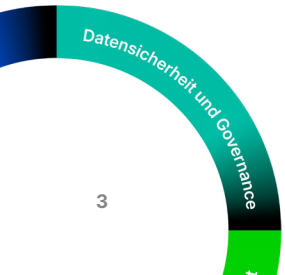


Abb. 2: In diesem Screenshot der Data Security Workbench-Konsole ruft ein Anwender eine Website mit einer Anleitung zum Verbergen von Dateien/Ordnern in Windows („How to hide deeply a file/folder in Windows“) auf und lädt eine Datei vom SharePoint-Laufwerk des Unternehmens herunter. Danach kopiert er 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.



58 %

Proofpoint senkt die DLP-Verwaltungskosten um 58 %.

Quelle: Enterprise Strategy Group

182 %

Proofpoint Enterprise DLP bietet über drei Jahre eine Rendite von 182 %.

Quelle: Enterprise Strategy Group

Schnelle Rendite und geringe Betriebskosten

Laut dem Bericht der Enterprise Strategy Group zur Analyse der wirtschaftlichen Vorteile von Proofpoint Enterprise DLP, der 2025 herausgegeben wurde, senkt Proofpoint die DLP-Verwaltungskosten um 58 % und bietet eine Rendite von 182 %.[4] Das ist dank folgender Funktionen möglich:

- Der Cloud-native Proofpoint-Service optimiert die Bereitstellung, Integration und Verwaltung.
- Durch die KI-gestützten Datensicherheitsfunktionen mit Erkenntnissen über das Anwenderverhalten lassen sich Rendite innerhalb von Wochen erzielen (statt Monaten bei klassischen Lösungen).
- Die einheitliche Proofpoint-Lösung ist kostengünstiger und effizienter als ein Flickwerk eigenständiger Tools.
- Proofpoint DSPM identifiziert und entfernt redundante Daten und verwaiste Backups sowie Snapshots. Das reduziert die Angriffsflächen und senkt die Cloud-Speicherkosten.

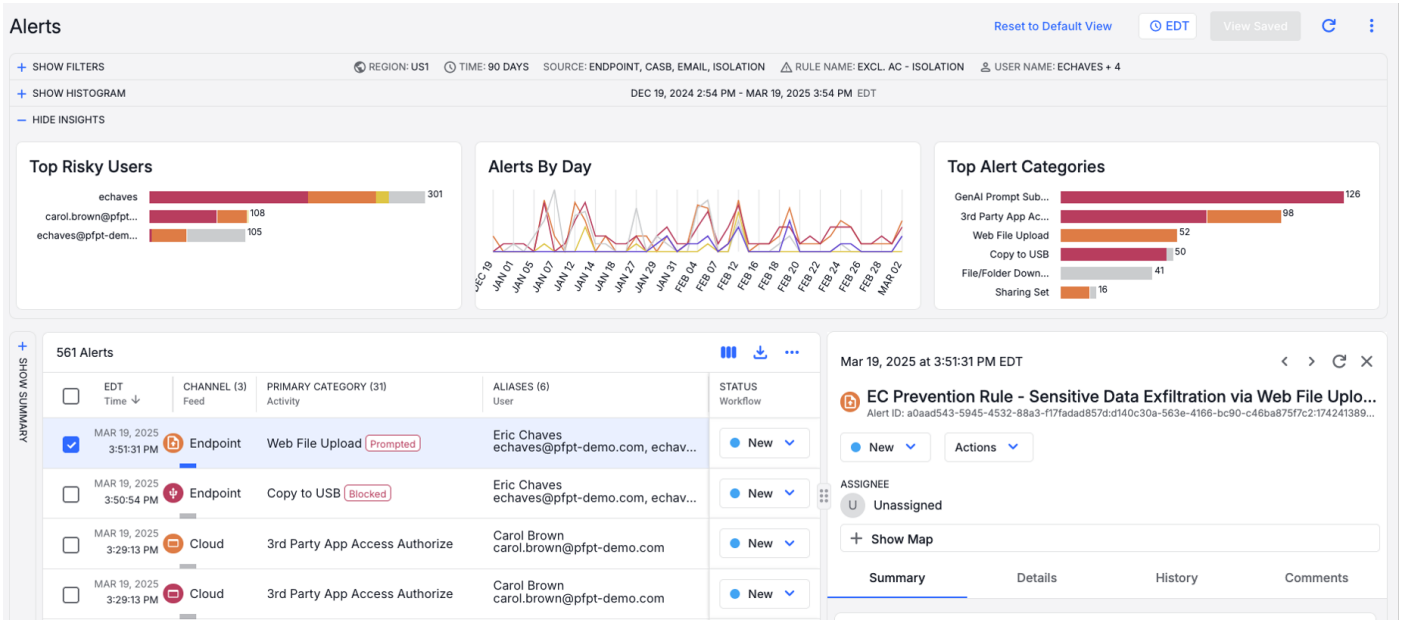


Abb. 3: Die Data Security Workbench führt die Verwaltung von Warnmeldungen zu E-Mails, Cloud und Endpunkten in einer zentralen Konsole zusammen. In diesem Beispiel hat ein Analyst die Warnmeldungen für einen bestimmten Anwender gefiltert. Das Dashboard zeigt, dass der Anwender vertrauliche Daten in sein geschäftliches E-Mail-Konto hochgeladen und anschließend versucht hat, eine Datei auf ein USB-Laufwerk zu kopieren, was jedoch blockiert wurde.

4. Enterprise Strategy Group: *Analyzing the Economic Value of Proofpoint Enterprise DLP* (Analyse der wirtschaftlichen Vorteile von Proofpoint Enterprise DLP), Juni 2025.

Agilität bei Veränderungen in Geschäftsumgebungen

Unabhängig davon, ob Ihr Unternehmen eine Umstrukturierung durchläuft, geografisch expandiert oder neue Technologien implementiert, schützt die Proofpoint-Datensicherheitslösung Ihre vertraulichen Informationen zuverlässig. Als Proofpoint-Kunde profitieren Sie von folgenden Vorteilen:

- **Unterstützung organisatorischer Veränderungen** durch die Reduzierung von Risiken für geistiges Eigentum, vertrauliche Informationen und weitere sensible Daten. Dies umfasst Informationen im Zusammenhang mit Fusionen und Übernahmen oder Umstrukturierungen. Dank des Überblicks über die Umgebungen übernommener Unternehmen können Sie vererbte Sicherheitslücken schließen. Unsere Automatisierung hilft, Sicherheitsrichtlinien und -standards anzuwenden und durchzusetzen. Adaptive Richtlinien passen sich in Echtzeit an wechselnde Risiken an.
- **Gewährleistung sicherer und vorschriftenkonformer KI-Nutzung**, indem verhindert wird, dass vertrauliche Daten für öffentliche GenAI-Tools, eigene Large Language Models (LLMs) und KI-Agenten freigegeben werden. Sie können die Nutzung geschützter Informationen in GenAI-Prompts in Browsern oder installierten Anwendungen einschränken und verhindern, dass Ihre vertraulichen Daten zum Training eigener LLMs verwendet werden.
- **Sicherstellung der Endanwender-produktivität** durch Gewährleistung der Endpunkt-Leistung und der Anwendungszugriffe. Durch den einzelnen, ressourcenschonenden User-Mode-Agenten für DLP und ITM werden Software-Inkompatibilitäten, Systemausfälle und Endpunkt-Leistungseinbußen vermieden, die für Kernel-Mode-Agenten typisch sind. Statt Anwendungen pauschal zu blockieren, können Sie Anwendern entsprechende Hinweise geben. Das kann beispielsweise eine Echtzeit-Erinnerung daran sein, dass vertrauliche Informationen nicht in ChatGPT-Prompts enthalten sein dürfen. Sie können auch Anwender auffordern, Rechtfertigungen für das Kopieren vertraulicher Daten anzugeben.

Maximale Wirksamkeit Ihrer Programme für Datensicherheit und zur Abwehr von Insider-Bedrohungen

Als strategischer Partner unterstützt Proofpoint Sie dabei, Ihr Programm für Personen, Prozesse und Technologien erfolgreich zu gestalten. Die Premium-Services von Proofpoint helfen Ihnen bei der Optimierung und Weiterentwicklung Ihrer Programme für Datensicherheit und zur Abwehr von Insider-Bedrohungen. Proofpoint bietet Beratung, Technik-Empfehlungen sowie operative Hinweise mit Branchenexpertise, die Ihnen jederzeit zur Verfügung stehen.

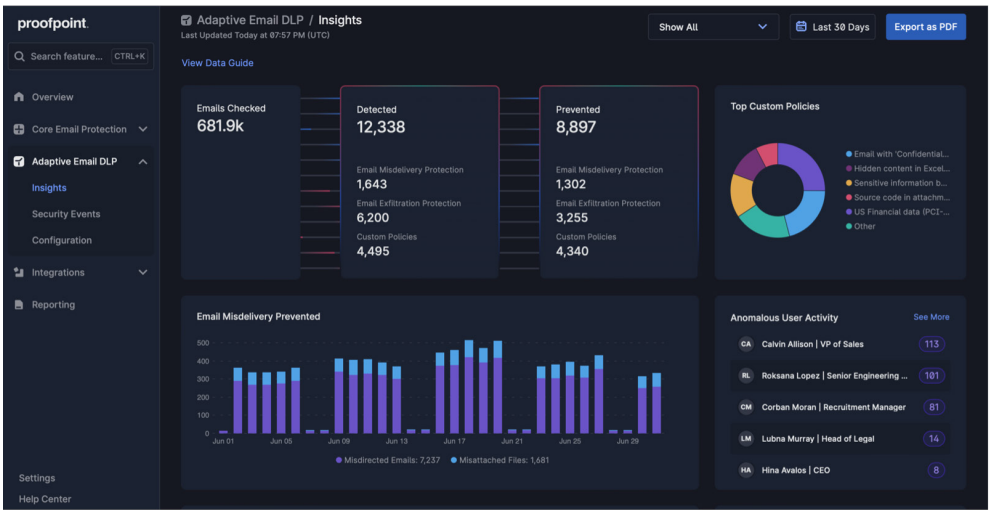
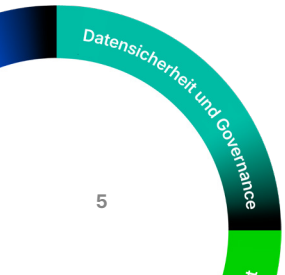


Abb. 4: Das Insights-Dashboard von Proofpoint Adaptive Email DLP zeigt Statistiken zur Erkennung und Verhinderung von E-Mail-Datenverlust. Dazu gehören Kennzahlen zu fehlgeleiteten E-Mails, angewandten benutzerdefinierten Richtlinien sowie Anwendern mit ungewöhnlichem Verhalten.



Stufen der Proofpoint-Lösung für Datensicherheit

Wir bieten die Proofpoint-Lösung für Datensicherheit in drei Stufen an: Data Security Core, Data Security Core Plus und Data Security Complete. Die Funktionen und Möglichkeiten dieser Lösungsstufen finden Sie in der folgenden Tabelle.

WICHTIGE FUNKTIONEN	PROOFPOINT DATA SECURITY CORE	PROOFPOINT DATA SECURITY CORE PLUS	PROOFPOINT DATA SECURITY COMPLETE
Detaillierter Anwender- und Dateikontext	✓	✓	✓
Bedrohungssuche für proaktive Erkennungen und Untersuchungen	✓	✓	✓
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	✓	✓	✓
Überwachung und Erkennung von Dateibewegungen, inkl. Datenherkunft	✓	✓	✓
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	✓	✓	✓
Erkennung und Klassifizierung von Datenspeichern		✓	✓
Erkennung und Behebung von Risiken in Datenspeichern		✓	✓
KI-gestützte Verhinderung von versehentlichem und vorsätzlichem Datenverlust durch E-Mails			✓

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: X | LinkedIn | Facebook | YouTube

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →