

Proofpoint Cloud DLP

Transparenz und Kontrolle für vertrauliche Daten in Cloud-Anwendungen

Wichtige Vorteile

- Transparenz zu Cloud-Bedrohungen, riskanten Datenbewegungen, Cloud-Datenkompromittierungen und riskanter Nutzung von Cloud-Anwendungen
- Schutz vertraulicher Daten mit Datenverlustprävention (DLP), die Inhalts-, Verhaltens- und Bedrohungstelemetrie kombiniert
- Vereinfachte DLP-Vorgänge über Cloud, E-Mail, Web und Endpunkte hinweg mit einer einheitlichen Verwaltungsübersicht
- Schutz vor Kontoübernahmen, Missbrauch von OAuth-Anwendungen, dauerhaften Zugriffen und dateibasierten Angriffen
- Erkennung von Cloud-Insider-Risiken mit Machine-Learning-Modellen, die auf die Identifizierung ungewöhnlicher Downloads, Freigaben und Datenexfiltration ausgerichtet sind
- Schnellere Behebung mit automatisierten Aktionen, die Freigaben entfernen, Berechtigungen reduzieren, Konten sperren, OAuth-Zugriffe widerrufen und Risiken eindämmen

Proofpoint Cloud DLP nutzt einen personenzentrierten Ansatz, um Ihre Anwender und Ihre vertraulichen Daten vor Cloud-Bedrohungen zu schützen. Dazu hilft die Lösung Unternehmen, Datenkompromittierungen nachzuverfolgen, die SaaS-Nutzung zu verwalten und den Zugriff auf OAuth-Anwendungen von Drittanbietern zu kontrollieren.

Cloud-Sicherheit beginnt mit dem Schutz von IT-genehmigten Anwendungen (wie Microsoft 365, Google Workspace, Salesforce und Box), die Ihre wertvollsten Daten enthalten. Proofpoint Cloud DLP bietet Ihnen personenzentrierte Transparenz zu Cloud-Bedrohungen, Datenkompromittierungen, Anwenderverhalten und Datenbewegungen, damit Sie starke Cloud-Sicherheit aufbauen und aufrechterhalten können.

Als Teil der Proofpoint-Plattform für Datensicherheit korreliert Proofpoint Cloud DLP Bedrohungen und Anwenderverhalten und wendet konsistente DLP-Richtlinien auf Cloud-Anwendungen, E-Mail, Web und Endpunkte an.

Mit Proofpoint Cloud DLP können Sie verhindern, dass vertrauliche Daten übermäßig weitergegeben werden oder verloren gehen, sowie das Insider-Risiko und riskantes Anwenderverhalten reduzieren. Die Lösung bietet Schutz vor Angriffen mit Kontoübernahmen, schädlichen Dateien und OAuth-Missbrauch.

VProofpoint Cloud DLP bietet personenzentrierte Transparenz zu Cloud- und E-Mail-Bedrohungen und hilft Ihnen beim Identifizieren Ihrer besonders häufig angegriffene Personen (Very Attacked People™, VAPs) und beim Schutz Ihrer Cloud-Konten und Daten. Sie sehen die Dateien, die gegen DLP-Regeln verstoßen, und wer deren Eigentümer ist sowie wer sie herunterlädt, weitergibt und bearbeitet. Mit unseren leistungsstarken Analysen und adaptiven Kontrollen können Sie Ihren Endnutzern und Drittanbieter-OAuth-Anwendungen die Zugangsberechtigungen zuweisen, die den für Sie relevanten Risikofaktoren entsprechen.

Schutz für Anwender, Anwendungen und Daten vor Cloud-Bedrohungen

Proofpoint Cloud DLP kombiniert Anwenderkontext mit kanalübergreifenden Bedrohungsdaten aus dem Proofpoint Behavior Graph. Machine Learning und Bedrohungskorrelation helfen Ihnen bei der Erkennung von Cloud-Konten, die kompromittiert wurden und für verdächtige Aktivitäten (wie Versand oder Weiterleitung von E-Mails oder Datenexfiltrationen) genutzt werden.

Über das intuitive Proofpoint Cloud DLP-Dashboard können Sie Warnmeldungen zu verdächtigen Anmeldungen, Dateiaktivitäten und administrativen Aktivitäten untersuchen und forensische Daten zur weiteren Analyse in eine SIEM-Lösung (Sicherheitsinformations- und Ereignis-Management) exportieren. Dies ist manuell oder über REST-APIs möglich.

Mit den zuverlässigen Richtlinien, Echtzeit-Warnmeldungen und automatisierten Reaktionen von Proofpoint Cloud DLP können Sie Folgendes erreichen:

- Schutz vor Cloud-Kontoübernahmen und Sperrung kompromittierter Konten
- Anwendung risikobasierter Authentifizierung und adaptiver Zugriffskontrollen
- Verhinderung von Datendiebstahl und Missbrauch von OAuth-Anwendungen, indem riskante Zugriffe Dritter identifiziert und widerrufen werden

- Erkennung und Isolierung schädlicher Dateien
- Entfernung unangemessener Dateifreigaben und Berechtigungen
- Einschränkung des Zugriffs auf vertrauliche Inhalte
- Sperrung von Anwenderkonten und Automatisierung von Behebungsmaßnahmen
- Untersuchung von und Reaktion auf verdächtige administrative Cloud-Aktivitäten

Proofpoint Cloud DLP hilft Ihnen zudem bei der Identifizierung von Insider-Risiken. Speziell entwickelte Machine-Learning-Modelle erkennen Verhaltensweisen, die typischerweise mit Insider-Bedrohungen und scheidenden Mitarbeitern in Verbindung gebracht werden. Dazu gehören ungewöhnliche Downloads, übermäßige Freigaben, verdächtige Datenzugriffsmuster und potenzielle Datenexfiltrationen, die nicht den sonst üblichen Mustern für Anwender oder das Unternehmen entsprechen.

Das optionale Add-on Proofpoint SaaS Isolation bietet zusätzlich die Möglichkeit, Anwender zu schützen, DLP auf nicht verwalteten Geräten anzuwenden und Ihre Identitätsmanagement-Lösung per SAML-Authentifizierung (Security Assertion Markup Language) zu integrieren.

Einheitliche Datenverlustprävention für alle Kanäle

Proofpoint Cloud DLP teilt DLP-Klassifizierer mit anderen Proofpoint-Datensicherheitslösungen. Diese Klassifizierer umfassen integrierte intelligente Identifikatoren, Wörterbücher, Regeln, Vorlagen und Autonomous Custom Classifiers (ACC), die große Sprachmodelle (LLMs) nutzen, um unternehmensspezifische vertrauliche Inhalte automatisch zu erkennen und zu klassifizieren.

Dieser Ansatz vereinfacht die schnellere Identifizierung und Absicherung vertraulicher Daten. Da Proofpoint Cloud DLP Teil der Proofpoint-Datensicherheitsplattform ist, können Sie konsistente DLP-Richtlinien für SaaS-Anwendungen, E-Mail, Web und Endpunkte bereitstellen.

Wir kombinieren Telemetriedaten zu Inhalten, Verhalten und Bedrohungen aus diesen Kanälen, damit Sie schnell feststellen können, ob der Anwender, der die DLP-Warnung ausgelöst hat, kompromittiert wurde oder böswillig bzw. fahrlässig handelt. Sie können die

Verwaltung der DLP-Warnmeldungen zudem für mehrere Kanäle vereinheitlichen.

Die mehr als 240 integrierten Klassifizierer decken Daten ab, die Vorschriften zum Schutz von Zahlungskartendaten (PCI DSS), personenbezogenen Daten (z. B. DSGVO) sowie Gesundheitsdaten unterliegen. Erweiterte Erkennungstechnologien wie exakte Datenabgleiche helfen Ihnen bei der Erstellung maßgeschneiderter Kontrollen wie kontextbezogener Richtlinien. Sie können den Datenzugriff von nicht verwalteten Geräten einschränken, das Hochladen vertraulicher Dateien in nicht genehmigte Cloud-Anwendungen verhindern und übermäßige Freigabeberechtigungen entfernen. Außerdem können Sie stark gefährdete vertrauliche Dateien identifizieren und verdächtige Anmeldeaktivitäten mit DLP-Zwischenfällen korrelieren.

Kontrolle über Cloud- und Drittanbieter-Anwendungen

Proofpoint Cloud DLP macht Schatten-IT sichtbar und erkennt in Ihrem Unternehmen eingesetzte Cloud-Anwendungen. Unser Katalog umfasst 46.000 Anwendungen mit jeweils mehr als 50 Attributen. Sie können Cloud-Anwendungen nach Typ und Risiko kategorisieren, um Sicherheitsrisiken, potenzielle Schwachstellen für Datenverlust und nicht konforme Bereiche einfacher festzustellen. Zudem können Sie gefährliche Anwendungen blockieren oder Anwendern schreibgeschützten Zugriff auf diese Anwendungen gewähren.

Wir erkennen und bewerten OAuth-Berechtigungen für Drittanbieter-Anwendungen, die auf Ihre von der IT freigegebenen zentralen Cloud-Dienste zugreifen. Unsere Analyse hilft bei der Identifizierung riskanter Anwendungen sowie bei der Reduzierung Ihrer Angriffsfläche. Basierend auf dem ermittelten Risiko und Kontext können Sie geeignete Maßnahmen definieren oder automatisieren.

Schnelle Bereitstellung

Durch unsere Multimode-Architektur können Sie schneller einen Mehrwert erzielen und innerhalb von weniger als vier Wochen Cloud-Dienst-APIs, hybride Identitätsverwaltungstools und Produkte für die Koordinierung von Sicherheitsmaßnahmen (einschließlich Proofpoint Threat Response) integrieren.

Dies ermöglicht automatisierte Maßnahmen zum Erkennen sowie Eindämmen von Bedrohungen und Schützen Ihrer Daten. Durch risikobasierte SAML-Authentifizierung und die Isolierung von SaaS-Umgebungen lassen sich unbefugte Zugriffe auf Unternehmensanwendungen blockieren sowie BYOD-Strategien umsetzen.

Mit Proofpoint Cloud DLP mehr erreichen

Proofpoint Cloud DLP kombiniert Datenschutz, Cloud-Bedrohungsschutz, Erkennung von Insider-Risiken, Transparenz zu Cloud-Datenkompromittierungen sowie adaptive personenzentrierte Kontrollen in einer einzigen Lösung. Durch die Integration von Cloud-Aktivitäten, Anwenderverhalten, Bedrohungsdaten und DLP-Telemetrie können Unternehmen vertrauliche Informationen besser schützen und gleichzeitig die operative Komplexität reduzieren.

Weitere Informationen

Weitere Informationen finden Sie unter proofpoint.com/de.

Über Proofpoint, Inc. Proofpoint, Inc. ist ein weltweiter Marktführer bei personen- und agentenzentrierter Cybersicherheit und schützt Verbindungen zwischen Anwendern, Daten und KI-Agenten über E-Mail, Cloud und Collaboration-Tools. Proofpoint ist ein vertrauenswürdiger Partner für mehr als 80 Prozent der Fortune 100, über 10.000 große Unternehmen sowie für Millionen kleinerer Firmen und stoppt Bedrohungen, verhindert Datenverlust und sichert die Interaktionen zwischen Anwendern und KI-Workflows ab. Die Collaboration- und Datenschutzplattform von Proofpoint hilft Unternehmen jeder Größe, ihre Mitarbeiter zu schützen und zu unterstützen, damit sie KI sicher und bedenkenlos einsetzen können. Weitere Informationen unter www.proofpoint.de

Verbinden Sie sich mit Proofpoint: [LinkedIn](#)

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

proofpoint[®]

