proofpoint.

KURZVORSTELLUNG

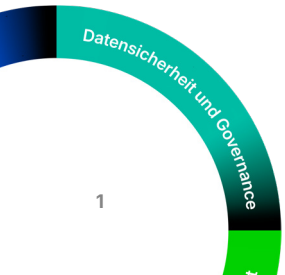
E-Mail-Datensicherheit mit einem adaptiven Ansatz modernisieren

Proofpoint Adaptive Email DLP für mehrschichtigen Schutz vor Datenverlust über E-Mails

Wichtige Vorteile

- Vermeidung versehentlicher und vorsätzlicher Datenverluste über E-Mails
- Minimierung von Risiken für Schädigung der Reputation und Kundenabwanderung
- Reduzierung von Strafen für Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) und den California Consumer Privacy Act (CCPA)
- Verbesserte Sensibilisierung für Sicherheit im gesamten Unternehmen

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



Der Verlust vertraulicher Daten kann Geschäftsabläufe stören und zu weiteren Schäden für Ihr Unternehmen führen. Laut dem *Proofpoint Data Loss Landscape-Bericht 2024* berichteten bei einer Umfrage 85 % der Unternehmen von einem Datenverlustereignis im letzten Jahr, wobei die Zwischenfälle bei 50 % dieser Unternehmen zu unterbrochenen Geschäftsabläufen führten. Die am häufigsten genannte Ursache für Datenverlust waren fahrlässige Anwender.

Deshalb ist Datenverlustprävention (DLP) für E-Mails, die unbeabsichtigte Exfiltrierung vertraulicher Informationen per E-Mail verhindert, eine entscheidende Komponente Ihrer allgemeinen Datensicherheitsstrategie. Ein effektives E-Mail-DLP-Programm kombiniert Inhaltsprüfungen, Echtzeit-Warnmeldungen, Richtlinienerzwingung und Anwenderschulungen, verhindert Datenverlust und gewährleistet, dass die rechtlichen Vorgaben eingehalten werden.

Herkömmliche E-Mail-DLP-Produkte bieten eine solide Grundlage, indem sie Regeln und Richtlinien für bekannte Risiken durchsetzen. Sie können Ihre Schutzstrategie für E-Mail-Daten jedoch erheblich verbessern, wenn Sie ein herkömmliches E-Mail-DLP-Produkt mit Proofpoint Adaptive Email DLP kombinieren. Auf diese Weise setzen Sie einen dynamischen, personenzentrierten Ansatz zur Verhinderung von Datenverlust über E-Mails durch.

Die Ergänzung von Proofpoint Adaptive Email DLP in Ihrer Unternehmensumgebung bietet folgende Vorteile:

Umfassenderer Schutz

- **Herkömmliche E-Mail-DLP-Produkte** konzentrieren sich auf den Inhalt und bieten regelbasierten Schutz vor bekannten Risiken wie vertraulichen Daten, die per E-Mail gesendet werden. Dabei können sie bekannte und gut definierte strukturierte Daten wie personenbezogene Informationen, Kreditkartennummern usw. sehr effektiv schützen.
- **Proofpoint Adaptive Email DLP** analysiert den Kontext und erweitert die Abdeckung klassischer E-Mail-DLP-Produkte auf unbekannte und neu aufkommende Bedrohungen. Die Lösung nutzt verhaltensbasierte künstliche Intelligenz (KI), um ungewöhnliches Anwenderverhalten zu erkennen, z. B. wenn ein Anwender vertrauliche Daten an falsche Empfänger sendet, Dateien auf ungewöhnliche Weise weitergibt oder eine E-Mail an ein nicht autorisiertes Konto verschickt.

Adaptive Erkennung

Proofpoint Adaptive Email DLP verwendet verhaltensbasierte KI, um ungewöhnliches E-Mail-Verhalten zu erkennen. Dabei sucht unsere KI nicht nur nach bestimmten Datenmustern, sondern analysiert den umfassenderen Kontext, z. B.:

- An welche Empfänger Anwender üblicherweise E-Mails senden

33 %
der Anwender

haben eine oder zwei E-Mails an den falschen Empfänger gesendet.

Quelle: *Proofpoint Data Loss Landscape-Bericht*, 2024

84 %

der im vergangenen Jahr fehlgeleiteten E-Mails enthielten Anhänge.

Quelle: *Proofpoint Data Loss Landscape-Bericht*, 2024

50 %

der unbeabsichtigten Datenschutzverletzungen im Jahr 2023 wurden durch eine fehlgeleitete E-Mail verursacht.

Quelle: Verizon: *2024 Data Breach Investigations Report* (Untersuchungsbericht zu Datenkompromittierungen 2024)

160.000

fehlgeleitete E-Mails wurden von Proofpoint Adaptive Email DLP im Jahr 2024 erkannt.

Quelle: Proofpoint

- Welche Arten von Anhängen Anwender üblicherweise weitersenden
- Wie Anwender üblicherweise vertrauliche Daten handhaben

Proofpoint Adaptive Email DLP passt sich an das Verhalten Ihrer Mitarbeiter und an die dynamischen E-Mail-Muster an. Die Lösung erkennt potenzielle Datenverlustereignisse sogar dann, wenn die Daten nicht umfassend definiert sind. Wenn zum Beispiel ein Mitarbeiter, der normalerweise keine Finanzdaten versendet, plötzlich Dateien mit Finanzdaten an einen nicht autorisierten externen Kontakt senden möchte, erkennt Proofpoint Adaptive Email DLP das nicht autorisierte E-Mail-Konto und den Anhang mit vertraulichen Daten und generiert eine Warnung.

Blockieren fehlgeleiteter E-Mails

Eine E-Mail gilt als fehlgeleitet, wenn ein Anwender sie versehentlich an den falschen Empfänger sendet. Fehlgeleitete E-Mails sind eine häufige Ursache für Datenschutzverletzungen. Laut Proofpoint-Daten senden 33 % der Angestellten pro Jahr ein oder zwei E-Mails an falsche Empfänger. Das ist auch das häufigste Datenverlustereignis, das beim britischen Information Commissioner's Office gemeldet wird.[1] Gleichzeitig hat Verizon festgestellt, dass 50 % aller unbeabsichtigten Datenschutzverletzungen durch fehlgeleitete E-Mails verursacht werden.[2]

Fehlgeleitete E-Mails lassen sich mit regelbasierten herkömmlichen E-Mail-DLP-Produkten nur schwer verhindern. Im Gegensatz dazu verwendet Proofpoint Adaptive Email DLP erweiterte Inhaltsanalysen und Verhaltensanalysen auf Basis von Proofpoint Nexus® Relationship Graph (RG), um fehlgeleitete E-Mails zu erkennen, bevor sie gesendet werden. Wenn ein Anwender versucht, eine E-Mail an den falschen Empfänger zu senden, erkennt Proofpoint Adaptive Email DLP diesen Fehler und interveniert mit einer Warnmeldung. Proofpoint-Daten zeigen, dass die Lösung im Jahr 2024 mehr als 160.000 fehlgeleitete E-Mails verhindert hat.

Vermeidung falscher Dateianhänge

Ein Dateianhang gilt als falsch, wenn ein Anwender eine E-Mail zwar an die richtige Person sendet, aber die falsche Datei anhängt. Wenn die verhaltensbasierte KI einen Anhang erkennt, der sie für einen Empfänger als untypisch einstuft, wird dem Anwender in Echtzeit eine Warnmeldung angezeigt. Dadurch kann der Anwender das Problem beheben, bevor ein Datenverlustereignis eintritt und Schaden entsteht.

1. Information Commissioner's Office: *Common data protection mistakes (and how to fix them)* (Häufige Fehler beim Datenschutz – und wie man sie behebt), Februar 2025.
2. Verizon: *2024 Data Breach Investigations Report* (Untersuchungsbericht zu Datenkompromittierungen 2024), 2024.

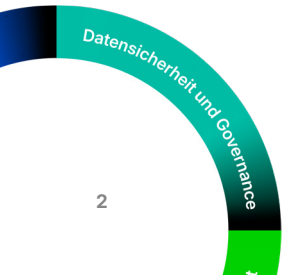


Abb. 1: Das Dashboard von Proofpoint Adaptive Email DLP bietet IT-Sicherheitsteams einen vollständigen und zuverlässigen Überblick über E-Mail-Bedrohungen, wodurch die Datenverlustprävention vereinfacht wird.

1.100.000

Proofpoint Adaptive Email DLP hat im Jahr 2024 mehr als 1.100.000 E-Mails mit Datenexfiltration erkannt.

Quelle: Proofpoint

Blockierung kostspieliger E-Mail-Exfiltration

Die Behebungsmaßnahmen, die nach der Exfiltration vertraulicher Daten durch E-Mails erforderlich sind, erweisen sich meist als sehr kostspielig. Das Ponemon Institute hat festgestellt, dass Sicherheitsteams für die Erkennung und Behebung eines erfolgreichen Datenexfiltrationsereignisses 48 bis 72 Stunden aufwenden müssen.[3] Mit Proofpoint Adaptive Email DLP entfällt dieser Aufwand. Die Lösung analysiert und klassifiziert automatisch Ihre vertraulichen Daten und erkennt private und nicht autorisierte E-Mail-Konten Ihrer Anwender. Wenn Anwender versuchen, vertrauliche Daten an sich selbst oder andere Personen zu senden, kann Proofpoint Adaptive Email DLP ihre Aktivitäten je nach Konfiguration blockieren oder nachverfolgen. Proofpoint-Daten zeigen, dass die Lösung im Jahr 2024 mehr als 1.100.000 E-Mails mit Datenexfiltration erkannt hat.

3. Ponemon Institute: *Email Data Loss Prevention: The Rising Need for Behavioral Intelligence* (Datenverlustprävention für E-Mails: Der wachsende Bedarf nach Verhaltensanalysen), Mai 2022.

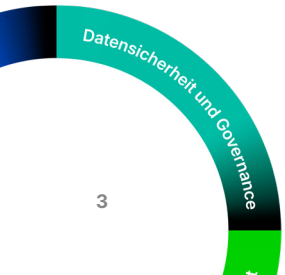


Abb. 2: Proofpoint Adaptive Email DLP warnt Anwender in Echtzeit über nicht autorisierte Konten sowie fehlgeleitete E-Mails.

Schulung der Anwender im entscheidenden Moment

Dank Echtzeitschulungen können Anwender Fehler und Richtlinienverstöße vermeiden. Proofpoint Adaptive Email DLP ergänzt Security-Awareness-Schulungen, indem die Lösung Anwender in Echtzeit über bestehende Risiken in ihren E-Mails informiert. Dadurch können sie ihre Fehler korrigieren, ohne dass ein Administrator eingreifen muss.

Gemeinsam stärker

Der Verlust vertraulicher Daten kann schwerwiegende Folgen wie Geldstrafen, Rufschädigung und entgangene Geschäfte nach sich ziehen.

Zusätzlich können solche Ereignisse für höhere Personalkosten für Untersuchungen sowie für die Dokumentation der Vorschriften und Compliance-Vorgaben sorgen.

Durch die Integration eines herkömmlichen E-Mail-DLP-Produkts und Proofpoint Adaptive Email DLP kann Ihr Unternehmen einen modernen, mehrschichtigen Ansatz für E-Mail-Datensicherheit umsetzen. Damit kombinieren Sie zuverlässigen Schutz vor bekannten Bedrohungen mit dynamischer und intelligenter Erkennung unbekannter personenzentrierter Datenverlust-Bedrohungen und erhalten robusten Datenschutz, bessere Anwender-Compliance, eine insgesamt stärkere E-Mail-Datensicherheit und können zudem die Betriebskosten senken.

proofpoint.

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →