

Proofpoint Adaptive Email DLP

Verhindern von Datenverlust dank KI-gestützter regelbasierter DLP

Wichtige Vorteile

- Vermeidung versehentlicher und vorsätzlicher Datenverluste über E-Mails
- Minimierung von Risiken für Marktreputation und Kundenabwanderung
- Reduzierung von Strafen für Verstöße gegen DSGVO und CCPA
- Verbesserte Sensibilisierung für Sicherheit im gesamten Unternehmen

Trotz bestehender E-Mail-DLP-Kontrollmechanismen beziehen sich die meisten gemeldeten DSGVO-Verstöße auf Daten, die per E-Mail in die falschen Hände gelangt sind. Regelbasierte Datenverlustprävention (DLP) spielt beim Schutz bekannter vertraulicher Daten wie personenbezogener Informationen, Sozialversicherungsnummern und Zahlkartendaten durchaus eine wichtige Rolle, einige Risiken werden von diesen Kontrollen jedoch nicht erkannt. Dazu gehören beispielsweise vertrauliche Daten, die an falsche Empfänger gesendet werden, und Mitarbeiter, die Daten für sich selbst und andere unbefugte Empfänger exfiltrieren.

Proofpoint Adaptive Email DLP nutzt verhaltensbasierte KI, um das normale E-Mail-Sendeverhalten Ihrer Mitarbeiter, ihre vertrauenswürdigen Beziehungen und ihr Verhalten bei der Kommunikation vertraulicher Daten zu verstehen und bei der Analyse aller E-Mails basierend auf den gewonnenen Erkenntnissen anormale Verhaltensweisen feststellen zu können. Wenn potenzielle Datenverlust-Ereignisse erkannt werden, werden Administratoren benachrichtigt, die Anwender in Echtzeit gewarnt und der Verlust vertraulicher Daten durch E-Mails verhindert.

Blockierung fehlgeleiteter E-Mails

Eine E-Mail gilt als fehlgeleitet, wenn ein Anwender sie versehentlich an den falschen Empfänger sendet. Diese häufige Ursache für Datenschutzverletzungen in Unternehmen lässt sich mit regelbasierten Ansätzen nur schwer ausschließen.

Proofpoint Adaptive Email DLP kann diesen Vorfällen ein Ende setzen, indem die Lösung Beziehungsdiagramme auswertet, E-Mail-Inhalte detailliert untersucht und Verhaltensweisen analysiert, um typische Verhaltensmuster zu verstehen und Datenverlust-Ereignisse zu erkennen. Dadurch bleiben die vertraulichen Daten Ihres Unternehmens auch dann geschützt, wenn E-Mails an falsche Empfänger gesendet werden oder Mitarbeiter falsche Anhänge weiterleiten.

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



Abb. 1: Proofpoint Adaptive Email DLP warnt Anwender in Echtzeit vor potenziell fehlgeleiteten Nachrichten, damit keine vertraulichen Daten durch E-Mails verloren gehen.

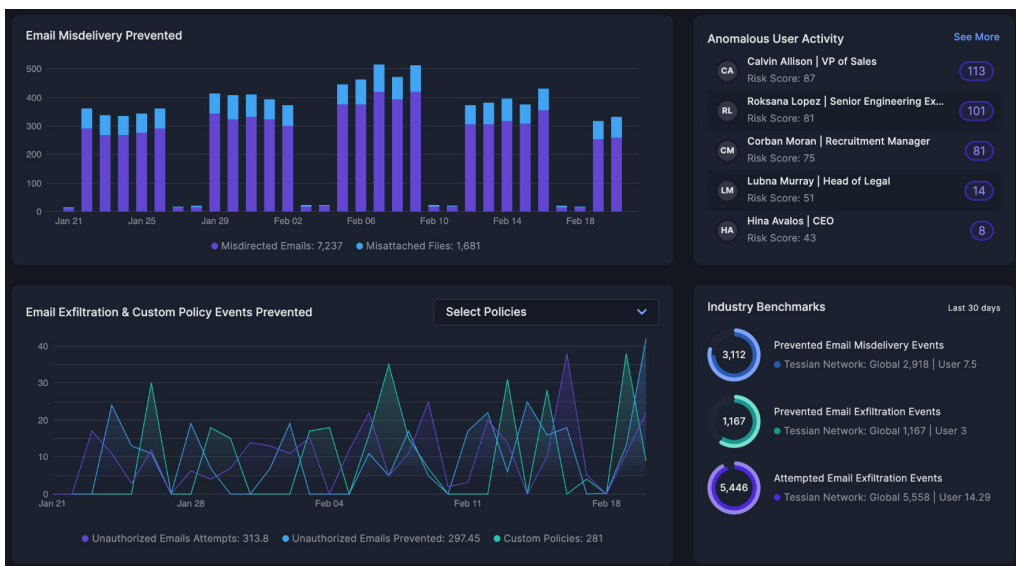


Abb. 2: Sicherheitsteams erhalten einen zuverlässigeren Überblick über Datenverlust-Ereignisse durch E-Mails.

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 für einen Empfänger als untypisch eingestuft wird, warnt Proofpoint Adaptive Email DLP den Anwender automatisch und in Echtzeit, bevor vertrauliche Informationen versehentlich an die falsche Person gesendet werden.

Stoppen von Exfiltration per E-Mail

Regelbasierte DLP spielt bei der Vermeidung von Datenverlust eine wichtige Rolle. Sie greift jedoch nur bei vordefinierten Risiken wie personenbezogenen Informationen, Zahlungskartendaten und Sozialversicherungsnummern. Datenschutzverletzungen erfolgen aber auch durch Insider, die vertrauliche Daten über private E-Mails und andere nicht vom DLP-System kontrollierte unbefugte Konten weiterleiten.

Proofpoint Adaptive Email DLP blockiert die Exfiltration vertraulicher Daten, indem es diese Daten automatisch klassifiziert, und erkennt die privaten E-Mail-Konten der Anwender anhand ihres E-Mail-Verhaltens. Wenn ein Mitarbeiter also versucht, Daten für sich oder andere zu exfiltrieren, werden die Versuche automatisch unterbunden und je nach Konfiguration protokolliert.

Schulung der Anwender im entscheidenden Moment

Echtzeit-Schulungen für Anwender können dazu beitragen, Fehler und Richtlinienverstöße rechtzeitig zu vermeiden. Proofpoint Adaptive Email DLP ergänzt Security-Awareness-Schulungen, indem es Ihre Anwender in Echtzeit über bestehende Risiken in ihren E-Mails informiert. Dadurch können sie ihre Fehler noch rechtzeitig korrigieren und verhindern, dass vertrauliche Daten verloren gehen.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter proofpoint.com/de.

INFORMATIONEN ZU 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.

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