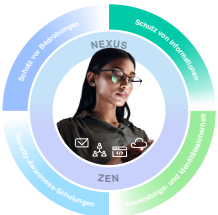
Ergänzen von Microsoft Purview mit Proofpoint Adaptive Email DLP

Stärkerer und intelligenterer Schutz vor Datenverlust per E-Mail dank Kombination von Microsoft Purview mit Proofpoint Adaptive Email DLP

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.



Microsoft Purview und Proofpoint Adaptive Email DLP gehen zwar beide gegen Datenverlust per E-Mail vor, nutzen dabei jedoch unterschiedliche Ansätze und beseitigen unterschiedliche Risiken. Den umfassendsten und zuverlässigsten Schutz vor Datenverlust per E-Mail erhalten Sie, wenn Sie Ihre Microsoft Purview-Implementierung mit den Bedrohungsdaten von Proofpoint Adaptive Email DLP ergänzen.

Microsoft Purview und Proofpoint Adaptive Email DLP im Vergleich

Microsoft Purview nutzt einen richtlinienbasierten Ansatz, der die meisten Funktionen von sicheren E-Mail-Gateways wie Verschlüsselung der Kommunikation sowie Datenkontrolle und Datenaufbewahrung liefern kann. Dabei setzt Microsoft Purview allerdings auf von Administratoren verwaltete Regeln. Deren Implementierung ist langsam und fehleranfällig, und anschließend müssen die Regeln mit großem Aufwand gepflegt werden. Dennoch sind sie nicht in der Lage, alle Risiken zu stoppen. Zudem bietet Microsoft Purview keine Verhaltensanalyse, um die Absichten Ihrer Anwender zu erkennen. Diese Informationen sind jedoch wichtig, um echte Risiken von False Positives zu unterscheiden.

Proofpoint Adaptive Email DLP nutzt verhaltensbasierte künstliche Intelligenz (KI) und verhindert versehentlichen und absichtlichen Datenverlust per E-Mail. Wenn fehlgeleitete E-Mails, falsche Anhänge und Datenexfiltrationsversuche gestoppt werden, reduzieren sich auch Ihre Risiken und Ihre Kosten für Behebungsmaßnahmen. Außerdem muss Ihr Sicherheitsteam weniger Zeit für die Untersuchung von False Positives aufwenden und kann sich stattdessen auf die Optimierung Ihrer Schutzmaßnahmen konzentrieren.

Microsoft Purview stoppt keine fehlgeleiteten E-Mails

Die E-Mail-Regeln in Microsoft Purview können zuverlässig verhindern, dass die vordefinierten Inhaltstypen Ihr Unternehmen verlassen. Sie können jedoch nicht verhindern, dass Anwender E-Mails an falsche Empfänger senden. Um fehlgeleitete E-Mails stoppen zu können, müssen Sie die typischen Verhaltensweisen der Mitarbeiter genau kennen. Dazu benötigen Sie historische E-Mail-Daten und Kontext.

Proofpoint Adaptive Email DLP analysiert die E-Mail-Daten der letzten 12 Monate und erlernt auf diese Weise typische Kommunikationsmuster zwischen Absendern und Empfängern. Mithilfe dieser Analysedaten identifiziert und stoppt die Lösung fehlgeleitete E-Mails, bevor sie abgeschickt werden.

Microsoft Purview kann Datenexfiltration per E-Mail kaum verhindern

Bei den meisten Datenexfiltrationen per E-Mail senden Mitarbeiter vertrauliche Daten an sich selbst, z. B. bevor sie zu einem Mitbewerber wechseln.

In Microsoft Purview können zwar kostenlose E-Mail-Services wie Gmail und Yahoo generell blockiert werden, das würde jedoch auch legitime geschäftliche E-Mail-Adressen mit einschließen. Außerdem kann mit diesem Schritt nicht verhindert werden, dass Anwender Daten an eine private E-Mail-Domain senden. Und wenn jede Interaktion mit einem kostenlosen E-Mail-Service eine Warnmeldung generiert, verursacht das zu viele False Positives, die Ihr Sicherheitsteam analysieren müsste.

Proofpoint Adaptive Email DLP nutzt hochentwickelte KI, die mit den größten Datensätzen der Branche trainiert wird. Durch die Analyse des E-Mail-Sendeverhaltens Ihrer Mitarbeiter lernt die Lösung, zwischen normaler und verdächtiger Kommunikation zu unterscheiden. Sie erhalten genauere und aussagekräftigere Warnungen, mit denen Sie Ihre Untersuchungen beschleunigen und so Zeit sowie Ressourcen sparen können.

Proofpoint Adaptive Email DLP schult Anwender in Echtzeit

In Microsoft Purview können Sie Richtlinientipps hinzufügen, damit bei einem Verstoß gegen E-Mail-Richtlinien eine Warnmeldung angezeigt wird. Diese Tipps müssen jedoch aufwändig konfiguriert und angepasst werden und werden bei zu häufigen Meldungen zudem häufig ignoriert. Dieses Phänomen wird auch als Überlastung durch zu viele Warnmeldungen bezeichnet.

Proofpoint Adaptive Email DLP liefert Anwendern ohne weitere Einrichtungsschritte und in Echtzeit kontextbezogene Warnmeldungen, die sie auf riskantes Verhalten hinweisen. Dadurch können Anwender fehlgeleitete E-Mails oder falsche Dateianhänge korrigieren, bevor sie gesendet werden. Wenn Mitarbeiter versuchen, vertrauliche Daten an sich selbst oder andere Personen zu senden, kann Proofpoint Adaptive Email DLP ihre Aktivitäten je nach Konfiguration blockieren oder nachverfolgen.

Gemeinsam stärker

Datenverlust per E-Mail kann für Ihr Unternehmen 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.

Um Ihre vertraulichen Daten zu schützen und solche schwerwiegenden Folgen zu vermeiden, benötigen Sie eine flexible und intelligente DLP-Lösung für E-Mails, die über einen statischen, regelbasierten Ansatz hinausgeht.

Durch die Kombination von Microsoft Purview mit den KI-gestützten Möglichkeiten von Proofpoint Adaptive Email DLP kann Ihr Unternehmen umfassende und robuste Schutzmaßnahmen gegen Datenverlust per E-Mail aufbauen.

Mehr unter Proofpoint.com/de

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.