

Proofpoint Email DLP und Proofpoint Email Encryption

Schutz Ihrer Anwender vor Angriffen, die sie dazu verleiten, vertrauliche Daten per E-Mail zu verschicken

Wichtige Vorteile

- Zentrale Verwaltung und Erzwingung von E-Mail-DLP und Verschlüsselung über unser branchenführendes E-Mail-Gateway
- Integration mit der Proofpoint Information and Cloud Security-Plattform mit umfassender Einbeziehung der gesamten Bandbreite durch Menschen verursachter Datenverlust-Szenarien
- Analyse und Klassifizierung vertraulicher Informationen in strukturierten und unstrukturierten Daten
- Nahtloses Anwender- und Mobilerlebnis

Compliance

- Mehr als 240 integrierte Klassifizierer
- Insiderhandel-Begriffe für PCI DSS, SOX, GLBA, SEC und andere globale und länderspezifische Vorlagen
- DSGVO, DPA (GB), DPD (EU), PIPEDA (Kanada), nationale Versicherungsnummern (GB), japanische Kreditkartennummern
- Geschützte Gesundheitsdaten, HIPAA, ICD-9, ICD-10, nationale Arzneimittelnummern und andere im Gesundheitswesen verwendete Datensätze

Proofpoint Email Data Loss Prevention (DLP) und Proofpoint Email Encryption bieten einzigartige Transparenz und Durchsetzung, ohne die Komplexität und Kosten separat eingesetzter Einzellösungen. Mit diesen Lösungen lassen sich Daten automatisch klassifizieren und transparent verschlüsseln – mit zentraler Verwaltung im Gateway. Sie können Richtlinien für Ihre gesamte E-Mail-Umgebung definieren und implementieren, was die Verwaltung vereinfacht.

Proofpoint Email DLP und Proofpoint Email Encryption geben Ihnen mehr Kontrolle über Ihre vertraulichen Daten und unterstützen Sie bei der Einhaltung von Vorschriften. Die Lösungen schützen Ihre Anwender vor Angriffen, die sie dazu verleiten, vertrauliche Daten per E-Mail zu verschicken. E-Mail ist der wichtigste Risikovektor bei eingehenden Bedrohungen und stellt bei ausgehenden Nachrichten ein ebenso hohes Risiko für Datenverlust dar.

Email DLP: Verhinderung potentieller Datenschutzverletzungen

Proofpoint Email DLP klassifiziert zuverlässig vertrauliche Informationen, erkennt Datenexfiltrationen per E-Mail und verhindert, dass vertrauliche Daten aus Ihrem Unternehmen nach außen gelangen.

Exakter Datenabgleich

Proofpoint Email DLP verfügt über eine Funktion für den exakten Datenabgleich. Sie erkennt vertrauliche Daten, die geschützt bleiben müssen, und ermöglicht es Ihnen, benutzerdefinierte Wörterbücher sowie unternehmensspezifische Identifikatoren hochzuladen oder anzulegen. Dafür werden zum Beispiel Kontonummern von Finanzdienstleistern, Ausweisnummern und Krankenblattnummern herangezogen, damit die für Sie relevanten E-Mail-Daten analysiert werden. Vorhandene Wörterbücher lassen sich außerdem mit eigenen Begriffen und Codes erweitern. Zudem können Sie Richtlinien mit routenbasierten Definitionen für Ihre ein- und ausgehenden Nachrichtenströme erstellen.

Schutz vor E-Mail-Betrug

Proofpoint Email DLP bietet mehr als 240 detaillierte Klassifizierer, die im Rahmen von BEC-Angriffen (Business Email Compromise, auch als Chefmasche bezeichnet) üblicherweise verwendete E-Mails automatisch finden, klassifizieren und blockieren. Auf diese Weise minimieren sie deutlich das Risiko, dass Personalakten und Steuerunterlagen verschickt werden oder Geld an Betrüger überwiesen wird.

Tiefgehende Analyse und Fingerprinting

Proofpoint Email DLP erkennt zuverlässig vertrauliche Daten innerhalb unstrukturierter Inhalte. Mit Email DLP profitieren Sie von folgenden Vorteilen:

- Standardmäßige Prüfung von über 300 Dateitypen
- Gewährleistung der ordnungsgemäßen Verarbeitung vertraulicher Daten jenseits gängiger Microsoft Office- und PDF-Dokumente
- Verwendung des Dateityp-Profilers, sodass auch neue, benutzerdefinierte oder proprietäre Dateitypen erkannt werden können (Dateitypen können auch Patente und Memos umfassen)
- Dokumente mit Fingerabdrucksensor mit voller und teilweiser Übereinstimmungsfunktion (Daten können mit Fingerabdruck versehen werden, auch wenn die Daten in unterschiedlichen Dateiformaten vorliegen)

Automatisierte Vorschriften-Compliance

Proofpoint Email DLP findet mehr als beim Abgleich anhand einfacher regulärer Ausdrücke und erkennt mithilfe integrierter Wörterbücher in kürzester Zeit gefährdete vertrauliche Daten. Vorteile von Email DLP:

- Zuverlässige Erkennung von Kommunikation, die gegen Compliance-Vorschriften verstößt
- Detaillierte, in intelligenten Identifikatoren integrierte algorithmische Prüfungen
- Reduzierung von False Positives für Kreditkartennummern, Ausweisnummern und verschiedenste vertrauliche Informationen
- Erweiterte Näherungs- und Korrelationsanalyse zur besseren Erkennung mehrerer Elemente

Wörterbuch-Begriffe können ganz nach Bedarf gewichtet werden, um die Stärke der Übereinstimmung für einen Begriff anzupassen oder Ausnahmen zu erstellen.

Verbesserte operative Effizienz

Integration in die Information and Cloud Security-Plattform

Proofpoint Email DLP ist in die Proofpoint Information and Cloud Security-Plattform integriert und führt unsere marktführenden DLP-Lösungen für E-Mail, Cloud, Web, Endpunkte und lokale Datei-Repositorys zusammen. Dazu kombiniert unsere Plattform Telemetriedaten zu Inhalten, Verhalten und Bedrohungen aus diesen Kanälen im Warnungs-Manager, sodass Sie die gesamte Bandbreite an personenzentrierten Datenrisiken über eine zentrale Benutzeroberfläche verwalten. Mit einheitlichen Datenklassifizierern können Sie einheitliche DLP-Richtlinien für alle Kanäle festlegen. Auf diese Weise sparen Sie viel Zeit und Verwaltungsaufwand.

Smart Send

Die Smart Send-Funktion ermöglicht E-Mail-Versendern das Beheben eigener Richtlinienverstöße bei ausgehenden Nachrichten. Dieses leistungsfähige, einfach zu verwaltende Tool hilft bei der Schulung von Anwendern, damit Ihrem IT-Team mehr Zeit für strategische Aufgaben bleibt. Sie können Nachrichten mit vertraulichen Assets durch das richtlinienbasierte Routing blockieren. In diesem Fall werden

die E-Mails mit einem entsprechenden Hinweis an den Anwender, die Personalabteilung, die IT oder eine andere Person zurückgesendet.

Proofpoint-Echtzeitberichte

Proofpoint Email DLP bieten umfassende Transparenz und die nötigen Workflows, damit Sie schnell entscheiden und handeln können. Die Lösung liefert einen Überblick über Echtzeitstatistiken sowie Trends und ermöglicht die Verwaltung aktueller Zwischenfälle sowie die Ergreifung geeigneter Maßnahmen für Nachrichten, die gegen Compliance-Vorschriften verstoßen – alles von einem zentralen Dashboard aus. Zu jedem Zwischenfall können Sie weitere Details abrufen. Dabei erhalten Sie eine Vergleichsansicht, in der Bereiche einer E-Mail oder eines Anhangs hervorgehoben werden, um Übereinstimmungen mit dem ursprünglichen Schulungsdokument oder der Richtlinie zu zeigen. Im Incident Manager können Sie Verstöße kommentieren, verfolgen, suchen und Nachrichten mit Treffern exportieren.

Grafische Berichte zeigen Verstöße im Zeitverlauf und können nach Richtlinie, Anwender, häufigsten Akteuren pro Richtlinie und mehr geordnet werden. Lassen Sie sich Trends anzeigen, um herauszufinden, in welchen Bereichen sich Verbesserungen zeigen und wo noch Nacharbeit nötig ist. Um Zeit zu gewinnen, können Berichte Zeitplanbasiert per E-Mail verschickt oder auf einer Intranet-Seite veröffentlicht werden.

Email Encryption: Zuverlässige Verschlüsselung, Transparenz und Kontrolle

Proofpoint Email Encryption wird über das richtlinienbasierte DLP-Modul aktiviert. Die Lösung hat folgende Funktionen:

- Definieren von Verschlüsselungsrichtlinien
- Dynamisches Anwenden von Richtlinien auf globaler, Gruppen- und Anwenderebene mit Integration in LDAP oder Active Directory
- Festlegen der Verschlüsselung basierend auf Empfänger (z. B. Geschäftspartner, Lieferanten) oder Versender- und Nachrichtenattributen, z. B. Anhangstypen)

Proofpoint Email Encryption kann auch als TLS-Fallback dienen, um einen störungssicheren Verschlüsselungsmechanismus gewährleisten.

Die Vorteile von Email Encryption:

- Sichere und zuverlässige Geschäftskommunikation
- Sichere Kommunikation zwischen Gruppen oder Anwendern, da Internal-to-Internal-Verschlüsselung zum Einsatz kommt, E-Mails nicht an externe Anbieter geleitet werden müssen und auf andere, schwierig zu implementierende Lösungen verzichtet werden kann
- Präzise Rückrufregelungen für verschlüsselte E-Mails ermöglichen Nachrichtenrückruf, Ablauf und Wiederherstellung des Zugriffs auf verschlüsselte E-Mails, ohne dass andere Anwender oder andere Nachrichten an denselben Empfänger dadurch beeinträchtigt werden

No-Touch-Schlüsselverwaltung

Der Aufwand für die Schlüsselverwaltung fällt weg, damit Sie sich auf Ihre Bedürfnisse für die Verschlüsselung konzentrieren können. Generierte Schlüssel werden sicher gespeichert und verwaltet und sind zudem über unsere Cloud-basierte Infrastruktur hochverfügbar. Die Speicherung der Schlüssel erfolgt aus Datenschutz- und Sicherheitsgründen getrennt von E-Mail-Inhalten.

Verbessertes Erlebnis beim Empfänger

Ein nahtloses Anwendererlebnis ist ein absolutes Muss. Mit Proofpoint Email Encryption vermeiden Sie, dass Anwender die festgelegten Richtlinien umgehen. Wir bieten Anwendern mehrere Optionen für den Zugriff auf verschlüsselte Nachrichten. Die Standardmethode für sicheres Lesen (Secure Reader) führt Anwender über einen Klick auf den verschlüsselten Anhang der Nachricht auf ein Web-Portal, wo sie die verschlüsselte Nachricht

problemlos einsehen können. Die andere Methode ist das geführte Entschlüsseln (Decrypt Assist), das speziell für den Zugriff von mobilen Geräten aus konzipiert ist. Die Anwender erhalten eine Nachricht mit einem Link, über den sie auf ein für mobile Geräte optimiertes Web-Portal geleitet werden. Von dort können sie auf die verschlüsselte Nachricht zugreifen.

Der Zugriff auf verschlüsselte Nachrichten und die Verwaltung aller Nachrichten erfolgt über die Secure Reader Inbox. Dies gewährleistet ein nahtloses Anwendererlebnis beim Umgang mit verschlüsselten Nachrichten und ermöglicht dem Unternehmen die unkomplizierte Verwaltung vorhandener Nachrichten. Mit der integrierten Outlook-Add-in-Funktion können Anwender verschlüsselte Nachrichten mit einem Klick auf eine Schaltfläche bequem lesen und verschicken. Zusätzlich können Sie die Internal-to-Internal-Verschlüsselung für vertrauliche Kommunikation zwischen Mitarbeitern aktivieren.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.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 mehr als die Hälfte der Fortune-1000-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.