

# Proofpoint Email Protection

## Erkennung und Abwehr bekannter sowie unbekannter E-Mail-Bedrohungen

### WICHTIGE VORTEILE

- Erkennt mehr Bedrohungen, findet sie schneller und schützt besser
- Verbessert die Produktivität dank schneller E-Mail-Verfolgung und E-Mail-Hygiene
- Auch für sehr große Unternehmen vollständig flexibel skalierbar
- Ermöglicht dank automatisierter Sicherheitsabläufe und Reaktion auf Bedrohungen effiziente operative Abläufe
- Erweitert den Schutz durch Integration mit Email Encryption, Email DLP, Targeted Attack Protection usw.
- Bietet bei Bereitstellung in der Cloud branchenweit führende SLAs:
  - 99,999 % Service-Verfügbarkeit
  - 100 % Virenschutz
  - E-Mail-Latenz unter einer Minute
  - Spam wird zu 99 % blockiert oder umgeleitet

Mehr als 90 % aller Cyberangriffe beginnen heute mit einer E-Mail. Das macht die E-Mail zum wichtigsten Bedrohungsvektor.<sup>1</sup> Neben verbreiteten E-Mail-Bedrohungen wie Phishing und Malware tritt mit Business Email Compromise (BEC), der so genannten Chefmasche, eine weitere gefährliche E-Mail-Angriffsform auf den Plan, die sich speziell gegen Mitarbeiter in Unternehmen richtet. Proofpoint Email Protection entdeckt bekannte ebenso wie unbekannt Bedrohungen, die anderen Tools entgehen. Dafür analysiert Proofpoint täglich Milliarden E-Mails und findet dadurch mehr Bedrohungen und ist besser in der Lage, gut getarnte Malware-lose Bedrohungen wie Impostor-E-Mails, die Adressaten durch die Nutzung einer gefälschten Identität zu überlisten versuchen, schnell und zuverlässig zu erkennen. Dank Email Protection können Unternehmen den allergrößten Teil der Bedrohungen abwehren, noch bevor sie in die Postfächer Ihrer Anwender zugestellt werden.

Proofpoint Email Protection schützt und kontrolliert alle ein- und ausgehenden E-Mails. Die Lösung nutzt Machine Learning und mehrschichtige Erkennungstechniken, um schädliche E-Mails zu erkennen und zu blockieren. Zudem werden aktuelle Bedrohungen aber auch Massenmailings (Bulk) dynamisch klassifiziert. Unternehmen erhalten dadurch detaillierte Kontrollmöglichkeiten für eine Vielzahl von E-Mail-Typen, einschließlich Impostor-E-Mails, Phishing, Malware, Spam und Massen-E-Mails. Die benutzerdefinierten Sicherheitsrichtlinien und E-Mail-Weiterleitungsregeln ermöglichen vollständige Flexibilität. Proofpoint Email Protection ist die am häufigsten eingesetzte E-Mail-Sicherheitslösung unter den Fortune 1000-Unternehmen. Sie lässt sich selbst für die größten Unternehmen skalieren und kann in der Cloud, als lokale Lösung oder als Hybrid-Installation bereitgestellt werden.

<sup>1</sup> „Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen), Verizon 2019.

## FINDET NEUE BEDROHUNGEN, DIE ANDEREN ENTGEHEN

### Erkennt Phishing ebenso wie E-Mails, bei denen die Identität des Absenders gefälscht wurde

Proofpoint Email Protection erkennt auch neuartige Bedrohungen, noch bevor sie in die Postfächer Ihrer Anwender zugestellt werden. Der Stateful Composite Scoring Service (SCSS) von Proofpoint, eine hochentwickelte Machine Learning-Technologie, klassifiziert zuverlässig verschiedene E-Mail-Typen und erkennt selbst Malware-lose Bedrohungen wie Anmeldedaten-Phishing und Impostor-E-Mails (auch als Business Email Compromise (BEC) oder Chefmasche bezeichnet). Diese Daten werden durch unternehmensspezifische Informationen ergänzt. So wird auch der typische Kommunikationsverkehr des jeweiligen Unternehmens in die Bewertung mit einbezogen. Mithilfe dieser Datenbasis können wir schnell alle E-Mails finden und blockieren, die außerhalb des jeweiligen Normbereichs liegen, was die allgemeine Effektivität erheblich steigert. SCSS ist nicht von Aktualisierungen abhängig, sondern lernt in Echtzeit, um zulässige (bzw. erwünschte) sowie schädliche ebenso wie unerwünschte E-Mails besser zu klassifizieren. Es reagiert dabei direkt auf Veränderungen bei Angriffstaktiken.

### Blockiert schädliche und unerwünschte E-Mails

Email Protection besitzt mehrschichtige Erkennungstechniken zur Abwehr der sich permanent weiterentwickelnden Bedrohungen. Dank signaturbasierter Erkennung werden bekannte Bedrohungen wie Viren, Trojaner und Ransomware blockiert. Zudem bewertet die Lösung mithilfe dynamischer Reputationsanalysen kontinuierlich lokale sowie globale IP-Adressen, bevor eingehende E-Mails akzeptiert werden. Unsere einzigartigen E-Mail-Klassifizierer können ein großes Spektrum an E-Mails dynamisch klassifizieren. Dazu gehören E-Mails, bei denen die Identität des Absenders gefälscht wurde (so genannte Impostor-E-Mails), aber auch Mails, deren Inhalte gegen Richtlinien des Unternehmens verstoßen (beispielsweise nicht jugendfrei sind), Phishing, Malware, Spam und Massen-E-Mails. Dabei werden Ihre eingehenden E-Mails je nach Typ in separate Quarantänen unterteilt. Gemeinsam schützen diese Funktionen schon beim ersten Anzeichen schädlicher Aktivitäten.

## FINDET JEDE E-MAIL INNERHALB VON SEKUNDEN

Email Protection besitzt die umfangreichsten Suchfunktionen. Mit der intelligenten Suchfunktion lassen sich problemlos schwer zu findende Protokolldaten basierend auf dutzenden Suchkriterien finden. Sie können auch schnell nachverfolgen, woher E-Mails kommen und wohin sie übertragen wurden. Email Protection bietet detaillierte Informationen zu Suchergebnissen, einschließlich Metadaten mit mehr als 100 Attributen. Für die Suche sind nicht Minuten, sondern lediglich wenige Sekunden erforderlich.

Die Suchergebnisse mit bis zu einer Million Einträgen können heruntergeladen und exportiert werden. Außerdem sind im Produkt mehrere Echtzeitberichte integriert, sodass Unternehmen immer einen detaillierten Überblick über die Aktivitäten im E-Mail-Kanal und damit verbundene Trends erhalten und Probleme sofort bei ihrem Auftauchen beseitigen können.

## SKALIERT FÜR GROSSE UNTERNEHMEN MIT VOLLSTÄNDIGER FLEXIBILITÄT

Im Gegensatz zu anderen Lösungen unterstützt Proofpoint Email Protection auch die Anforderungen der weltweit größten Unternehmen. Mit dieser Lösung lassen sich äußerst anpassbare E-Mail-Firewall-Regeln auf globaler, Gruppen- und Anwenderebene erstellen. Unternehmen können alle erforderlichen Sicherheitsrichtlinien und Regeln zur E-Mail-Weiterleitung mit der Lösung abbilden – und problemlos durchsetzen. Email Protection bietet verschiedene Bereitstellungsoptionen: lokale Hardware, virtuelle Maschinen sowie SaaS.

## STEIGERT DAS SICHERHEITSBEWUSSTSEIN BEI ENDNUTZERN

Dank einer integrierten Warnfunktion können Endnutzer überlegte Entscheidungen bei E-Mails treffen, die in den Graubereich zwischen legitim und verdächtig fallen. Dabei wird eine kurze Beschreibung des Risikos angezeigt, das eine bestimmte E-Mail darstellt. Die Risikostufe wird in unterschiedlichen Farben angezeigt und ist damit für Ihre Endnutzer leicht verständlich. Diese Funktion verringert damit das Risiko potenzieller Kompromittierungen, da Anwender bei nicht eindeutig legitimen E-Mails vorsichtiger agieren werden.

Dank Email Protection können E-Mail-Administratoren ihren Endnutzern die Möglichkeit geben, E-Mails mit geringer Priorität (z. B. Massen-E-Mails) zu verwalten, Nachrichten, die unter Quarantäne gestellt wurden, zu überprüfen und entsprechende Aktionen vorzunehmen. Die Rückmeldungen der Anwender werden anschließend an Proofpoint übertragen, sodass wir die Zuverlässigkeit der Klassifizierung allgemein steigern können.

## ZENTRALE VERWALTUNG FÜR EMAIL ENCRYPTION UND DLP

Sie können Ihren Schutz ganz einfach mit Proofpoint Targeted Attack Protection, Email Encryption oder Email Data Loss Prevention (DLP) erweitern. Email Protection bietet Ihnen grundlegende Funktionen für E-Mail-Verschlüsselung und DLP. Doch auch unsere vollständigen Lösungen in diesen Bereichen können über die gleiche Verwaltungskonsole gesteuert werden. Dank dieser engen Integration können Sie alle per E-Mail versendeten vertraulichen Daten sicher verwalten. Ebenso werden Datenlecks oder Datenverluste über E-Mails verhindert, wodurch verschiedene Compliance-Vorschriften erfüllt werden.

## WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://proofpoint.com/de).

### INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. 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 personenorientierten 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](https://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.