# Proofpoint Email Protection

## Erkennung und Abwehr schädlicher E-Mails, die Anwender mit und ohne Malware angreifen

### WICHTIGE VORTEILE

- Blockiert BEC-Betrug, Phishing-Angriffe und hochentwickelte Malware bereits beim Eingang
- Steigert das Sicherheitsbewusstsein bei Endnutzern mit einem Warnhinweis in der E-Mail
- 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 E-Mail-Authentifizierung, 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

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.

Mehr als 96 % aller verdächtigen sozialen Aktionen beginnen heute mit einer E-Mail. Das macht die E-Mail zum wichtigsten Bedrohungsvektor.[1] 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. Email Protection entdeckt bekannte ebenso wie unbekannte 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 von Proofpoint können Unternehmen den allergrößten Teil der Bedrohungen abwehren, noch bevor sie in die Postfächer Ihrer Anwender zugestellt werden.

### Findet neue Bedrohungen, die anderen Systemen entgehen

#### Erkennt Phishing, betrügerische Nachrichten sowie E-Mails, bei denen die Identität des Absenders gefälscht wurde

Email Protection erkennt auch neuartige Bedrohungen, noch bevor sie in die Postfächer Ihrer Anwender zugestellt werden. Proofpoint Advanced BEC Defense, unterstützt von NexusAI, stoppt eine Vielzahl von E-Mail-Betrugsmaschen, einschließlich Umleitungen von Gehaltszahlungen und Bankverbindungen für Lieferanten über kompromittierte Konten. Da häufig keine Schaddaten eingesetzt werden, sind zur Erkennung solcher Bedrohungen hochentwickelte Erkennungstechniken erforderlich.

1 „Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen), Verizon 2020.

Advanced BEC Defense stützt sich auf Machine Learning und künstliche Intelligenz und ist speziell darauf ausgelegt, BEC-Angriffe zu erkennen und zu stoppen. Dazu werden dynamisch mehrere Nachrichtenattribute analysiert, zum Beispiel:

- E-Mail-Header
- IP-Adresse des Absenders (x-originating IP, Reputation)
- Nachrichtentext (insbesondere Wörter und Phrasen, die Dringlichkeit betonen)

Das Modul erkennt, ob es sich bei einer Nachricht um eine BEC-Bedrohung handelt, und identifiziert dabei verschiedene Taktiken der BEC-Akteure, zum Beispiel:

- Änderungen der Reply-to-Adresse
- Verwendung schädlicher IP-Adressen
- Verwendung nachgeahmter Lieferantendomänen

Advanced BEC Defense bietet zudem einen detaillierteren Überblick über BEC-Bedrohungen, einschließlich BEC-Varianten wie Gutscheinkarten-Betrug, Umleitung von Gehaltszahlungen und Betrug mit Lieferantenrechnungen. Außerdem liefert die Lösung Informationen dazu, warum die Nachricht als verdächtig eingestuft wurde, sowie Nachrichtenbeispiele, damit Ihr Sicherheitsteam den Angriff besser verstehen und kommunizieren kann. Die NexusAI-Daten werden an Proofpoint Nexus Threat Graph übergeben, dort analysiert und mit Bedrohungsinformationen aus den Kanälen unserer Kunden (einschließlich E-Mail, Cloud, Netzwerke und soziale Netzwerke) korreliert. Damit bieten wir den erforderlichen Schutz, um den Bedrohungen immer einen Schritt voraus zu bleiben.

## Blockiert schädliche und unerwünschte E-Mails

Email Protection von Proofpoint 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. Eingehende E-Mails werden nach Typ unter Quarantäne gestellt. Gemeinsam schützen diese Funktionen schon beim ersten Anzeichen schädlicher Aktivitäten.

## Findet jede E-Mail innerhalb von Sekunden

Email Protection besitzt die intelligente und äußerst umfangreiche Suchfunktionen, mit denen Sie schwer zu findende Protokolldaten basierend auf dutzenden Suchkriterien problemlos finden können. Sie können auch schnell nachverfolgen, woher E-Mails kommen und wohin sie übertragen wurden. Die Lösung 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

Proofpoint Email Protection unterstützt 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 Anwendern

Dank einer integrierten Warnfunktion können Anwender überlegte Entscheidungen bei E-Mails treffen, die in den Graubereich zwischen legitim und schädlich 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 Anwender leicht verständlich. Sie können eine E-Mail – auch von einem Mobilgerät – direkt über diese Kennzeichnung als verdächtig melden. 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 Anwendern die Möglichkeit geben, verschlüsselte E-Mails mit geringer Priorität (z. B. Massen-E-Mails) zu verwalten, Nachrichten, die unter Quarantäne gestellt wurden, zu überprüfen und direkt im Outlook-Aufgabenbereich 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 Email DLP

Sie können Ihren Schutz ganz einfach mit Proofpoint Targeted Attack Protection, Email Fraud Defense, 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**.