proofpoint.

KURZVORSTELLUNG

Proofpoint Threat Protection für kommerzielle Kunden

Schutz für Unternehmen mit bis zu 2.500 Postfächern vor aktuellen personenzentrierten Bedrohungen

Wichtige Vorteile

- Schnellere Erkennung und Blockierung verschiedenster E-Mail-Bedrohungen
- Zuverlässigeres Stoppen neuer Bedrohungen dank kontinuierlicher KI-gestützter Analysen und Bedrohungsdaten
- Erkenntnisse zu Risiken durch personenbezogene und bedrohungsbezogene Risiken
- Schulungen für Ihre Mitarbeiter und Förderung von Verhaltensänderungen
- Erkennung und Korrektur kompromittierter E-Mail- und Cloud-Konten
- Schutz Ihrer Marke mit E-Mail-Authentifizierung

E-Mail ist der wichtigste Risikovektor bei Cybersicherheitsbedrohungen. Derzeit nehmen unzählige Malware-, Phishing- und Social-Engineering-Angriffe Ihre Mitarbeiter ins Visier. Laut dem *Verizon Data Breach Investigations Report 2024* gehen 68 % aller Datenschutzverletzungen mit einer menschlichen Komponente einher.[1] Der personenzentrierte Sicherheitsansatz von Proofpoint Threat Protection schützt Ihre Mitarbeiter vor aktuellen Bedrohungen.

Cyberkriminalität ist ein Wachstumsmarkt

Laut einer Statista-Prognose werden die weltweiten Cybercrime-Aktivitäten bis zum Jahr 2029 jährliche Kosten in Höhe von 15,63 Billionen US-Dollar verursachen.[2] Bedrohungsakteure versuchen, wertvolle persönliche Informationen und Unternehmensdaten zu stehlen, Identitätsdiebstahl zu begehen und E-Mail-Angriffe zu starten, die auf Finanzbetrug abzielen. Und da E-Mails für den Geschäftsbetrieb moderner Unternehmen unverzichtbar sind, werden sie als wichtigster Angriffsvektor gegen Ihre Mitarbeiter genutzt.

Angriffe mit Phishing, Business Email Compromise (BEC), Lieferantenbetrug und Malware (z. B. Ransomware) beginnen alle mit einer E-Mail. Daher fällt es selbst gut ausgestatteten IT-Abteilungen äußerst schwer, die Belegschaft vor diesen aktuellen Bedrohungen zu schützen. Doch Proofpoint kann Ihnen helfen.

Stoppen von mehr Bedrohungen mit personenzentrierter Sicherheit

Proofpoint erkennt ein breites Spektrum aktueller Cyberbedrohungen mit einer Erkennungsgenauigkeit von 99,99 %. Dazu analysiert Proofpoint Nexus kontinuierlich E-Mail-Bedrohungen mit einer Kombination aus Bedrohungsdaten, Machine Learning, verhaltensbasierter KI und semantischen LLM-Analysen (Large Language Models). Auf diese Weise kann die Lösung Angriffe effektiv identifizieren und abwehren.

1. Verizon: *Data Breach Investigations Report* (Untersuchungsbericht zu Datenkompromittierungen), 2024.
2. Statista: *Estimated Cost of Cybercrime Worldwide, 2018-2029* (Schätzungen zu weltweiten Cybercrime-Kosten, 2018–2029), Juli 2024.

© Proofpoint, Inc. 2025

85 %

der Fortune 100 vertrauen beim Schutz ihrer Mitarbeiter vor Bedrohungen auf Proofpoint.

Quelle: Proofpoint, 2024

Da Sie dank Proofpoint weniger Bedrohungen untersuchen müssen, sinkt der Aufwand für Behebungsmaßnahmen und die Reaktionszeit auf Zwischenfälle wird verkürzt. Zudem entlasten wir Ihre IT- und Sicherheitsteams durch die automatisierte Entfernung schädlicher E-Mails nach der Zustellung. Dies gilt auch für E-Mails, die von Ihren Mitarbeitern über unsere anwenderfreundlichen, integrierten Reporting-Tools gemeldet werden. Darüber hinaus fördert Proofpoint durch automatisch zugewiesene personalisierte Sicherheitsschulungen positive Änderungen im Verhalten der Anwender. Administratoren können den Wissensstand der Mitarbeiter und den Erfolg des Programms anhand realistischer Phishing-Simulationen testen und einschätzen, die vom internationalen Proofpoint-Bedrohungsforscherteam sorgfältig ausgewählt wurden.

Angriffe auf Mitarbeiter setzen häufig auf Nachahmung und Kontoübernahmen. Bei kompromittierten E-Mail- und Cloud-Konten beschleunigt Proofpoint die Reaktion durch KI-basierte Erkennungen und automatische Behebungsmaßnahmen. Wir schützen die Marke Ihres Unternehmens vor Missbrauch durch Nachahmung und unterstützen Sie bei der Einrichtung einer E-Mail-Authentifizierung. Proofpoint arbeitet mit Experten für die DMARC-Implementierung und Hosting-Diensten zusammen, um dynamisch Doppelgänger-Domains zu identifizieren, von denen E-Mails versendet werden, die Ihr Unternehmen imitieren.

Unsere Tools bieten neben einem nahtlosen Anwendererlebnis auch umfassenden Schutz für Ihre Mitarbeiter. Doch E-Mails sind nicht der einzige Angriffsvektor, der geschützt werden muss.

Deshalb deckt der erweiterte Phishing-Schutz von Proofpoint nicht nur E-Mails ab, sondern auch schädliche URLs, die über Messaging-, Collaboration- oder Social-Media-Plattformen verbreitet werden. Unsere Lösung überprüft und analysiert die URL-Reputation in Echtzeit und blockiert zudem schädliche URLs zum Klickzeitpunkt. Auf diese Weise werden Ihre Anwender jederzeit und überall vor komplexen Phishing-Angriffen geschützt.

Proofpoint Threat Protection ist eine ganzheitliche Lösung, die die Sicherheit Ihrer Mitarbeiter und des ganzen Unternehmens verbessert. Sie reduziert das Bedrohungsrisiko und hilft Ihren IT- und Sicherheitsteams, positive operative Ergebnisse zu erzielen. Sie können flexibel zwischen einem sicheren E-Mail-Gateway (SEG) und einer API-basierten Microsoft 365-Bereitstellung entscheiden und damit die Methode wählen, die am besten zu Ihren Unternehmensanforderungen passt. Ganz gleich, ob Sie eine schnelle Lösung suchen, die nur einmal eingerichtet werden muss, oder umfassenderen Schutz benötigen: Proofpoint Threat Protection erfüllt Ihre Anforderungen. Zudem passt sich die Lösung dem Wachstum Ihres Unternehmens an und unterstützt Sie so bei der Abwehr der zunehmenden Cyberbedrohungen.

© Proofpoint, Inc. 2025

Proofpoint Threat Protection-Pakete für kommerzielle Kunden, Use Cases und Beschreibungen

Verfügbar für Kunden mit bis zu 2.500 Postfächern.

PAKET	USE CASES	ÜBERBLICK
Proofpoint Core Email Protection	Optimal für Unternehmen mit diesen Zielen: • Stoppen von E-Mail-Bedrohungen wie Phishing, BEC, Malware, Ransomware, schädliche QR-Codes und URLs usw. • Reduzieren von Spam-, Graymail- und anderen unerwünschten Nachrichten • Steigern der Effizienz durch automatisierte Abuse-Postfach-Verwaltung • Besseres Verständnis darüber, wie Mitarbeiter angegriffen werden	Proofpoint Core Email Protection ist eine umfassende, KI-gestützte Lösung, die 99,99 % aller Bedrohungen stoppt. Sie reduziert Risiken und entlastet Ihr Sicherheitsteam durch zuverlässige Erkennungen und automatisierte Behebungs-Workflows. Proofpoint Core Email Protection wird entweder als sicheres E-Mail-Gateway (SEG) oder API-basierte Lösung für Microsoft 365 angeboten und kann dadurch die individuellen Sicherheitsanforderungen jedes Unternehmens erfüllen.
Proofpoint Advanced Threat Protection	Optimal für Unternehmen mit diesen Zielen: • Verbessern des Bedrohungsschutzes • Ändern unsicherer Verhaltensweisen und Aufbau einer Kultur des Sicherheitsbewusstseins • Absichern von Identitäten durch Abwehr und Behebung von Kontoübernahmen • Schutz von Mitarbeitern vor Phishing-Bedrohungen in Messaging- und Collaboration-Anwendungen	Erweitern Sie den grundlegenden Schutz von Proofpoint Core Email Protection, indem Sie unsicheres Anwenderverhalten ändern und zusätzliche Kommunikationskanäle sowie digitale Identitäten schützen. Schulen Sie Ihre Anwender in der Erkennung und Abwehr von Bedrohungen. Nutzen Sie dazu integrierte Phishing-Simulationen, Wissenstests sowie tausende Security-Awareness-Schulungsmodule in über 40 Sprachen. Erweitern Sie den Phishing-Schutz vor schädlichen URLs, die über Nachrichten-, Collaboration- oder Social-Media-Anwendungen verteilt werden. Erkennen Sie kompromittierte Konten und korrigieren Sie sie, indem Sie den Zugriff der Angreifer blockieren. * Umfasst Proofpoint Core Email Protection
Proofpoint Prime Threat Protection für kommerzielle Kunden	Optimal für Unternehmen mit diesen Zielen: • Einsatz des derzeit umfassendsten Schutzes • Schutz vor Markenmissbrauch und Nachahmung durch E-Mail-Bedrohungen • Zuverlässige Nachrichtenzustellung durch E-Mail-Authentifizierung (DMARC) • Vereinfachte Umsetzung komplexer DMARC-Protokolle mit Unterstützung durch Experten	Schützen Sie die Marke Ihres Unternehmens vor Nachahmerbedrohungen und Domain-Spoofing durch Implementierung von E-Mail-Authentifizierungsprotokollen wie SPF, DKIM und DMARC. Lassen Sie sich bei der DMARC-Implementierung von Proofpoint-Experten unterstützen, die Sie bei jedem Schritt begleiten. Erhalten Sie einen besseren Überblick über Doppelgänger-Domains und E-Mail-Nachrichten, die unter Verwendung Ihrer E-Mail-Domain versendet werden, einschließlich externer Versender. Schützen Sie Ihre Mitarbeiter mit mehrschichtigem Schutz. Mit diesem umfassenden Paket erhalten Sie alle nötigen Kontrollen, um Ihre Mitarbeiter vor gezielten Bedrohungen zu schützen. Bei Lösungen von Mitbewerbern müssen häufig mehrere Add-ons (z. B. für Mailbox-Automatisierung, Security-Awareness-Schulungen und Produktivitätstools) erworben werden, um den gleichen Funktionsumfang wie bei Proofpoint Prime Threat Protection für kommerzielle Kunden zu erhalten. * Umfasst Proofpoint Core Email Protection und Proofpoint Advanced Threat Protection

© Proofpoint, Inc. 2025

Vergleich der Threat Protection-Pakete für kommerzielle Kunden

	FUNKTIONEN	PROOFPOINT CORE EMAIL PROTECTION	PROOFPOINT ADVANCED THREAT PROTECTION	PROOFPOINT PRIME THREAT PROTECTION FÜR KOMMER-ZIELLE KUNDEN
Weitere Details	Lokal, hybrid oder Cloud-basiert	✓	✓	✓
	Flexible Bereitstellungsoptionen	Sicheres E-Mail-Gateway oder per API	Sicheres E-Mail-Gateway oder per API	Sicheres E-Mail-Gateway oder per API
Business Email Compromise (BEC)	Proofpoint Nexus LM für verhaltensbasierte KI	✓	✓	✓
	Proofpoint Nexus RG für Beziehungsdiagramm	✓	✓	✓
Phishing, Ransomware und Malware	Proofpoint Nexus TI für Bedrohungsdaten und Reputationsanalyse	✓	✓	✓
	Proofpoint Nexus LM für verhaltensbasierte KI	✓	✓	✓
	Veränderung und Sandbox-Analyse von URLs	✓	✓	✓
	Sandbox-Analyse von Anhängen	✓	✓	✓
	Isolierung veränderter E-Mail-Klicks	für Very Attacked People (VAPs)	für Very Attacked People (VAPs)	für Very Attacked People (VAPs)
	Banner mit Warnhinweisen in E-Mails	✓	✓	✓
Meldung und Behebung von E-Mails	Automatisches mSOAR	✓	✓	✓
	Automatisiertes Abuse-Postfach	✓	✓	✓
	Berichte zu Anwender-E-Mails	✓	✓	✓
Dashboards zu Bedrohungen und Anwendern	Erkenntnisse zu Bedrohungen, inkl. VAPs	✓	✓	✓
	Dashboard zu personenbezogenen Risiken	✓	✓	✓
Hygiene für E-Mails und Konfiguration	Schutz vor Spam, Viren, Graymail	✓	✓	✓
	Funktionen für Führungskräfte/VIP	✓	✓	✓
	Angepasste Richtlinien	✓	✓	✓
Phishing-Schutz für Messaging- und Collaboration-Anwendungen	Blockierung schädlicher URLs in Echtzeit		✓	✓
	Kanalübergreifende Transparenz bei Phishing-Bedrohungen		✓	✓
Sensibilisierung für Sicherheit	Automatisierte risikobezogene Schulungen		✓	✓
	Bedrohungsbezogene Inhalte		✓	✓
	Realistische Phishing-Simulationen		✓	✓

© Proofpoint, Inc. 2025

Vergleich der Threat Protection-Pakete für kommerzielle Kunden (Forts.)

	FUNKTIONEN	PROOFPOINT CORE EMAIL PROTECTION	PROOFPOINT ADVANCED THREAT PROTECTION	PROOFPOINT PRIME THREAT PROTECTION FÜR KOMMER-ZIELLE KUNDEN
Schutz vor Konto-übernahmen	Zuverlässige Erkennung kompromittierter Konten		✓	✓
	Zeitleiste für Untersuchungen vor und nach dem Zugriff		✓	✓
	Automatische Entfernung von Angreifern und Zurücksetzung von Kontoänderungen		✓	✓
E-Mail-Authentifizierung	E-Mail-Authentifizierung zur Verhinderung von Domain-Spoofing und Gewährleistung der Zustellbarkeit			✓
	Geführte DMARC-Implementierung und zusätzliche Hosting-Services			✓
	Erkennung von Doppelgänger-Domains Ihres Unternehmens und vertrauenswürdiger Partner			✓
	Risikobewertung für automatisch identifizierte Anbieter oder Lieferanten			✓

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.

Verbinden Sie sich mit Proofpoint: LinkedIn

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

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →