proofpoint.

EINKAUFSLEITFADEN

So wählen Sie die für Ihr Unternehmen beste E-Mail-Sicherheitslösung

Wichtige Funktionen

Achten Sie bei der Evaluierung moderner E-Mail-Sicherheitslösungen auf folgende wichtige Funktionen:

1. Schutz vor einem breiten Spektrum von Bedrohungen
2. Automatisierte Erkennung und Reaktion
3. Flexible Bereitstellungsoptionen
4. Hervorragende Anwenderfreundlichkeit
5. Bedrohungsschutz auch jenseits von E-Mails

Überblick

E-Mails sind weiterhin ein primärer Vektor für Cyberbedrohungen. Die Menschen nutzen heute allerdings mehrere digitale Kanäle zum Kommunizieren und Zusammenarbeiten, sodass sich die Angriffsfläche in den letzten Jahren vergrößert hat. Wenig überraschend springen Cyberkriminelle auf den Zug auf, um von dieser Entwicklung zu profitieren. Bei der Verteilung personenzentrierter Bedrohungen aller Art über digitale Kanäle sind sie sogar erfolgreicher denn je.

Als Reaktion darauf schustern sich Unternehmen einen Flickenteppich aus hochmodernen Einzellösungen zusammen, die den Bedrohungen Einhalt gebieten sollen.

Dabei verbleiben jedoch Lücken in den Schutzmaßnahmen und zahlreiche Risiken bleiben unbehandelt. Hinzu kommt: Die Verwaltung und Integration all dieser Sicherheitstools ist kompliziert und teuer. Unternehmen benötigen deshalb eine umfassende E-Mail-Sicherheitslösung, die über eine zentrale Plattform alle aktuellen und neuen personenzentrierten Bedrohungen stoppt.

In diesem Leitfaden stellen wir Ihnen die wichtigsten Funktionen vor, auf die Sie bei der Wahl einer umfassenden E-Mail-Sicherheitslösung achten sollten. Sie erfahren außerdem, warum diese Funktionen wichtig sind.

Abb. 1: Formen von E-Mail-basierte Bedrohungen.

© Proofpoint, Inc. 2025

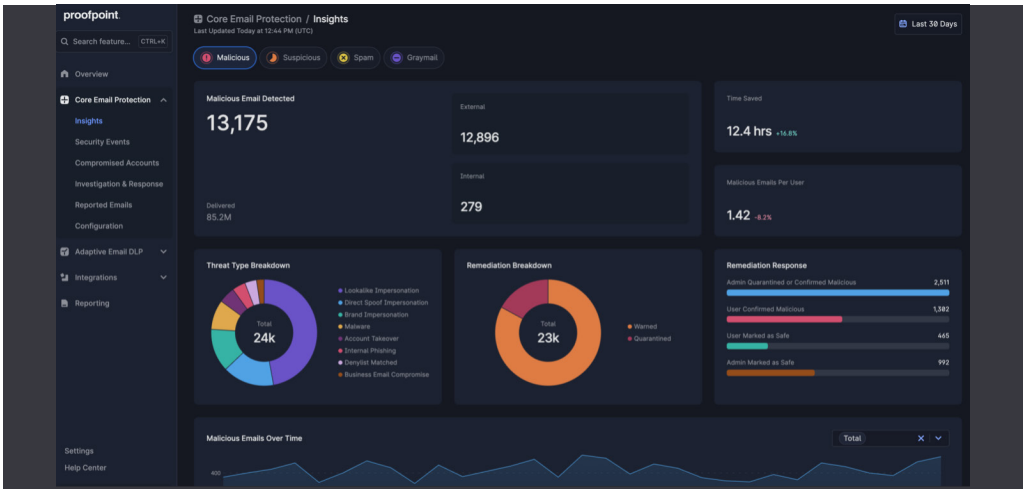

Abb. 2: Umfassender Überblick über E-Mail-basierte Bedrohungen, die von Proofpoint Core Email Protection verhindert wurden.

55 Mrd. USD

Weltweite Verluste durch BEC-Betrug von 2013 bis 2023[2]

60 Sekunden

Durchschnittliche Zeit, bis ein Benutzer auf eine Phishing-E-Mail hereinfällt[3]

1. Schutz vor einem breiten Spektrum von Bedrohungen

Im Durchschnitt belaufen sich die Kosten für eine durch Phishing oder Business Email Compromise (BEC) verursachte Datenschutzverletzung auf 4,88 Millionen US-Dollar.[1] Dies sind die zweithöchsten Kosten, direkt nach denjenigen, die durch böswillige Insider verursacht werden. Doch jede übersehene Bedrohung kann durch finanzielle Verluste und Markenschädigung hohe Kosten verursachen.

Die Sicherheitsteams versuchen, potenzielle Risiken auf ein Minimum zu reduzieren, doch dazu müssen sie eine Vielfalt an Bedrohungen stoppen.

Eine E-Mail-Sicherheitslösung sollte diese Vorteile bieten:

- **Verwendung von Echtzeit-Bedrohungsdaten:** Aktuelle Bedrohungsdaten tragen dazu bei, neue Bedrohungen zu identifizieren. Doch dabei geht es nicht nur um die eigentlichen Daten, sondern auch um die Einbeziehung hochqualifizierter Bedrohungsforscherteams. Wenn eine Lösung über beides verfügt, lassen sich globale Trends schneller und effizienter analysieren und zum Beispiel Cyberkriminelle sowie staatliche Akteure erkennen und nachverfolgen und Veränderungen innerhalb der Bedrohungslandschaft identifizieren.
- **Einsatz von KI zur Bedrohungserkennung:** Zum Stoppen von E-Mail-Angriffen, die auf Manipulation mit Schaddaten beruhen, ist ein mehrschichtiges, KI-gestütztes Paket aus Erkennungstechnologien gefragt. Achten Sie darauf, dass Large Language Models (große Sprachmodelle, LLMs), Beziehungs- und Verhaltensanalysen, Machine Learning und Bildanalysen zum Einsatz kommen. Diese tragen maßgeblich zum Stoppen von Bedrohungen im großen Maßstab bei.
- **Kontinuierliche Bedrohungsüberwachung:** Die Sandbox-Analyse von URLs und Anhängen ist eine wichtige Funktion. Doch nicht weniger wichtig ist der *Zeitpunkt*, zu dem diese Analyse stattfindet. Damit auch übersehene oder zeitlich verzögerte Angriffe erfasst werden, sollten Sie Lösungen bevorzugen, die Bedrohungen während ihres gesamten Lebenszyklus erkennen und stoppen – vor der Zustellung, nach der Zustellung und zum Klickzeitpunkt.
- **Übersicht über angegriffene Anwender:** Sie müssen wissen, wer wie angegriffen wird und ob die angegriffenen Personen reagiert haben. Außerdem müssen Sie wissen, auf welche Daten diese Personen zugreifen können und wie leicht sie sich täuschen lassen. Mit diesen Einblicken können Sie zum richtigen Zeitpunkt die richtigen Schutzmaßnahmen ergreifen.

Je früher Bedrohungen abgefangen werden, desto sicherer ist Ihr Unternehmen. Zudem müssen Ihre IT- und Sicherheitsteams keine wertvolle Zeit für die Reaktion auf Zwischenfälle und deren Behebung aufwenden.

1. IBM: *Cost of a Data Breach Report* (Kosten eines Datenschutzverstoßes), 2024.
2. FBI: *Business Email Compromise: the 55 $ Billion Scam* (Business Email Compromise: Der 55-Milliarden-Dollar-Betrug), September 2024.
3. Verizon: *Data Breach Investigations Report* (Untersuchungsbericht zu Datenkompromittierungen), 2024.

© Proofpoint, Inc. 2025

2. Automatisierte Erkennung und Reaktion

Schädliche Nachrichten, die in Postfächern landen oder von Anwendern gemeldet werden, können die Produktivität von Sicherheitsteams beeinträchtigen. Die manuelle Analyse und Entfernung all dieser Bedrohungen kostet viel Zeit. Es kommt darauf an, Bedrohungen frühzeitig zu erkennen und schnell auf sie zu reagieren, denn das kann darüber entscheiden, ob es sich um einen kleinen Zwischenfall oder eine ausgewachsene Kompromittierung handeln wird.

Eine E-Mail-Sicherheitslösung sollte diese Vorteile bieten:

- **Bereitstellung eines KI-gestützten Abuse-Postfachs:** Von Anwendern gemeldete verdächtige Nachrichten sollten so schnell wie möglich verarbeitet werden. Wenn diese Nachrichten automatisch an ein maschinell überwachtes Postfach weitergeleitet werden, können sie mithilfe von KI analysiert und als schädlich oder sicher eingestuft werden, ohne dass sie von Ihrem IT- oder Sicherheitsteam überprüft werden müssen. Im Idealfall informiert eine automatische Antwort-E-Mail die Anwender darüber, dass ihre Meldung eingegangen ist. Damit wird die Feedback-Schleife geschlossen, wodurch positive Verhaltensweisen gefördert werden.
- **Automatisierte Orchestrierung und Behebung:** Schädliche E-Mails sollten nicht im Posteingang der Anwender verbleiben, sondern im gesamten Unternehmen automatisch aus den Postfächern entfernt werden. Vergewissern Sie sich außerdem, dass sich die Lösung nahtlos in Ihre vorhandenen SIEM/SOAR-Tools integrieren lässt, sodass Sie eine einheitlichere Ansicht Ihres Sicherheitssystems erhalten.
- **Vereinfachte Workflows:** Sicherheitstools sollten Analysten die Arbeit erleichtern. Intuitive Workflows und klare, KI-generierte Bedrohungszusammenfassungen sind eine Möglichkeit der Entlastung. Features wie integrierte Suchfunktionen und prioritätsbezogene Warnmeldungen tragen dazu bei, dass Analysten Bedrohungen schneller aufspüren und verfolgen können. Auch Tools zur Beschleunigung der im Anschluss an die automatisierten Vorgänge noch verbleibenden Behebungsmaßnahmen sind ein Plus.

Wenn Ihr Sicherheitsteam effizienter arbeiten kann, stärkt dies den Schutz Ihres Unternehmens. Zudem können Sie vorhandene Sicherheitsressourcen und Investitionen optimal nutzen.

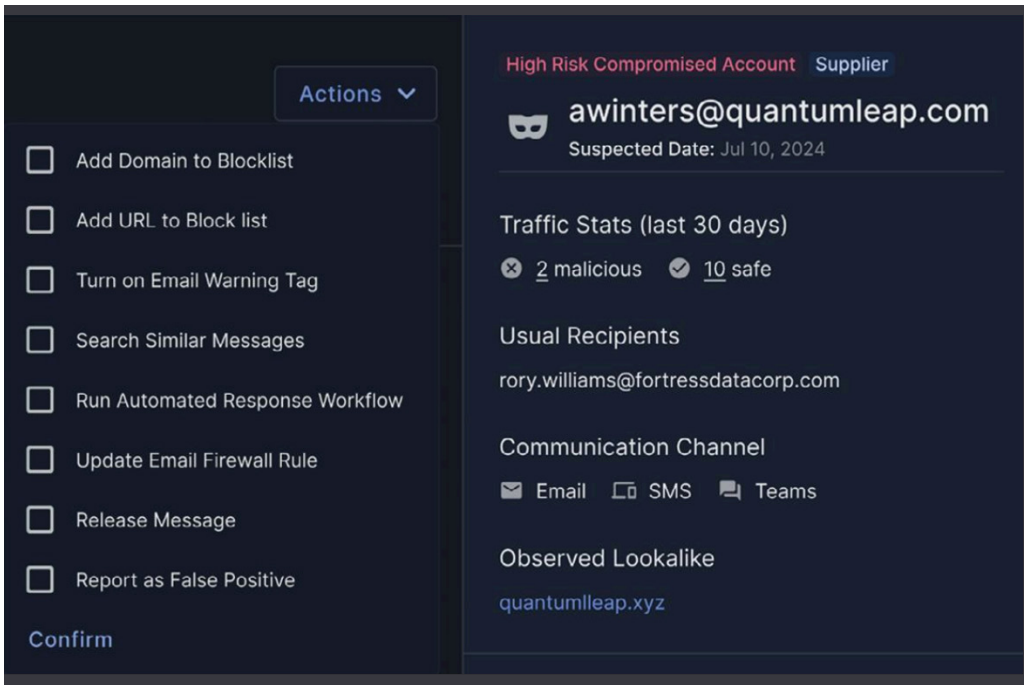

Abb. 3: Beispiel für automatisierte Workflows für Erkennung und Reaktion in Proofpoint Core Email Protection.

© Proofpoint, Inc. 2025

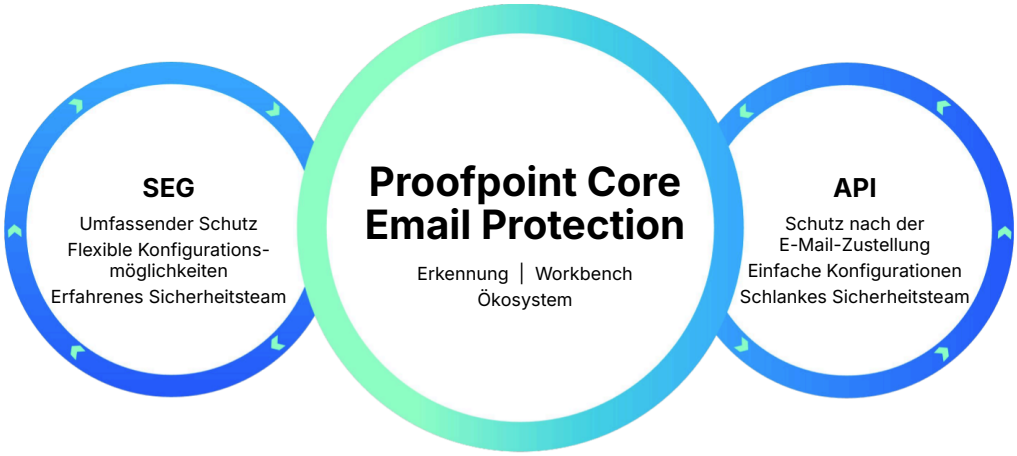

Abb. 4: Vorteile der SEG- und API-Bereitstellung mit Proofpoint Core Email Protection.

3. Flexible Bereitstellungs-optionen

Ihre Architektur, Sicherheitsrichtlinien und Compliance-Anforderungen unterliegen einem permanenten Wandel. Ihre E-Mail-Sicherheitslösung sollte deshalb in der Lage sein, mit Ihrem Unternehmen zu wachsen und Veränderungen zu unterstützen. Selbst wenn eine API-basierte Bereitstellung heute für Sie der beste Ansatz ist, trifft dies für künftige Geschäftsanforderungen möglicherweise nicht mehr zu (oder umgekehrt). Wenn Sie nicht an einen einzigen Bereitstellungsansatz gebunden sind, können Sie Ihr Sicherheitskonzept je nach Risiko optimieren.

Durch die Wahlmöglichkeit können Ihre IT- und Sicherheitsteams den Schutz skalieren, auf langfristigen Erfolg ausrichten und gewährleisten, dass Ihr Unternehmen auch bei Wachstum und Veränderungen von zuverlässigem Schutz profitiert.

Achten Sie auf folgende Funktionen:

- **SEG-Bereitstellung (sicheres E-Mail-Gateway):** SEGs bieten umfassenden Schutz für verschiedene Umgebungen. Diese Option bietet sich an, wenn Sie auf eine hochgradig anpassbare E-Mail-Sicherheitslösung Wert legen. SEGs bieten maximalen durchgängigen Schutz vor und nach der Zustellung sowie zum Klickzeitpunkt, flexible Konfigurationsoptionen sowie Einblick in die personenbezogenen Risiken.
- **API-basierte Bereitstellung:** Diese Option bietet einfaches Onboarding mit einem Bereitstellungsaufwand von wenigen Minuten – sowie vorkonfigurierte Kontrollen innerhalb von Cloud-Plattformen wie Microsoft 365. Die Bereitstellung per API ist dann die richtige Wahl für Sie, wenn Sie auf eine leistungsstarke, aber wartungsarme E-Mail-Sicherheitslösung Wert legen, die nur einmal eingerichtet werden muss, und dabei nicht auf verständliche Erkenntnisse zu Bedrohungen und automatisierte Behebungsfunktionen verzichten möchten.

Wenn Sie einen Anbieter mit flexiblen Bereitstellungsoptionen wählen, verfügen Sie jederzeit über die gerade benötigten Erkennungsfunktionen und zukunftsfähige Sicherheit.

© Proofpoint, Inc. 2025

74 %

Anteil der CISOs, die der Meinung sind, dass der Faktor Mensch die größte Cyberschwachstelle in ihrem Unternehmen ist[4]

40 %

Mit Security-Awareness-Schulungen lässt sich die Zahl der Mitarbeiterklicks auf echte Bedrohungen in weniger als 6 Monaten um 40 % reduzieren[5]

4. Hervorragende Anwenderfreundlichkeit

Das größte Risiko und die beste Verteidigungslinie liegen oft dicht beieinander: Es sind Ihre Mitarbeiter. Wenn Sie schädliche Nachrichten stoppen möchten, sollten Sie Ihren Mitarbeitern die richtigen Werkzeuge an die Hand geben.

Überforderte Mitarbeiter neigen eher dazu, Bedrohungen zu ignorieren oder Fehler zu machen. Spam, Graymail oder ständige Fehlalarme erhöhen dieses Risiko zusätzlich. Mitarbeiter benötigen klare Warnmeldungen mit relevanten Details, intuitive Meldungstools und sorgfältig konzipierte Phishing-Simulationen, damit positive, sichere Verhaltensweisen gestärkt werden können.

Eine E-Mail-Sicherheitslösung sollte diese Vorteile bieten:

- **Erkennung von Spam/Graymail:** Spam und Massennachrichten verstopfen die Postfächer und lenken Anwender ab. Graymail wie unerwünschte Marketing-E-Mails schaden der Produktivität. E-Mail-Sicherheitslösungen, die diese Nachrichten von Postfächern fern halten, verbessern das Anwendererlebnis und sorgen dafür, dass sich Mitarbeiter auf ihre Arbeit konzentrieren können.
- **Hinweise an Anwender bei verdächtigen Nachrichten:** Verdächtige E-Mails können schädlich sein oder auch nur so aussehen. Oft weiß das nur der Empfänger selbst. Kontextbezogene Benachrichtigungen (mit einer Vorschau) informieren die Anwender über die in einer Nachricht gefundenen Hinweise auf Bedrohungen. Gleichzeitig werden die mit der verdächtigen Nachricht verbundenen schädlichen URL-Links oder Anhänge unschädlich gemacht, und der Anwender muss zuerst auf die Benachrichtigung reagieren, bevor er Zugriff auf die eigentliche E-Mail erhält.
- **Schutz zum Klickzeitpunkt:** Auch Mitarbeiter mit besten Absichten können in der Hektik des Alltags Fehler machen und versehentlich auf einen schädlichen Link oder Anhang klicken. Schutz zum Klickzeitpunkt (z. B. in Form eines Banners mit einer Warnmeldung) kann Anwender dazu bringen, innezuhalten und nachzudenken, bevor sie mit einer E-Mail interagieren. Zusätzlichen Schutz bieten virtuelle Browserfenster, die Anmeldedaten-Diebstahl verhindern und das Herunterladen von Malware blockieren.
- **Personalisierte Security-Awareness-Schulungen:** Oft sind Phishing-Simulationen und Schulungen zur Sensibilisierung die primären Methoden, über die Mitarbeiter mit E-Mail-Sicherheitstools in Berührung kommen. Hocheffektive Tools bieten Anwendern Echtzeit-Lernerlebnisse, wenn sie auf ein Phishing-Element klicken. Interaktive, fokussierte Lernmodule sind auf den Wissensstand jedes einzelnen Anwenders zugeschnitten. Dieser personalisierte Ansatz schärft das Bewusstsein der Anwender und fördert langfristige Verhaltensänderungen.

Harmonische Anwendererlebnisse sorgen dafür, dass Ihre Mitarbeiter wachsam bleiben und konzentriert arbeiten können.

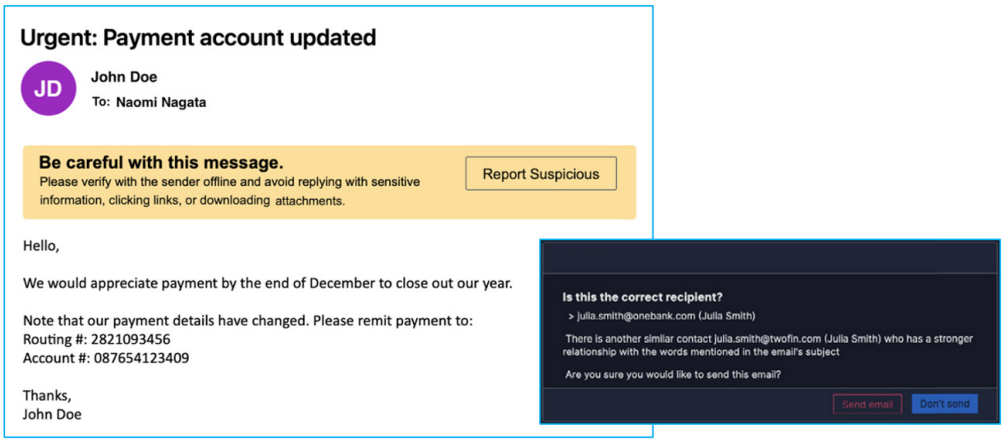

Abb. 5: Beispiel für einen E-Mail-Banner mit Warnhinweisen bei einer potenziell falsch adressierten Nachricht.

4. Proofpoint: *Voice of the CISO*, 2024.
5. Ergebnisse der Proofpoint ZenGuide-Forschung.

© Proofpoint, Inc. 2025

2.524 %

Zunahme der über SMS-basiertes Phishing zugestellten URL-Bedrohungen in den letzten drei Jahren[6]

5. Bedrohungsschutz auch jenseits von E-Mails

Angesichts der immer weiter wachsenden digitalen Arbeitsbereiche ist es wichtig, dass eine Plattform anpassungsfähig ist. Sie sollte in der Lage sein, nicht nur E-Mail, sondern auch neuere digitale Kommunikationskanäle zu schützen. Cyberkriminelle beschränken sich bei ihren Angriffen nicht mehr nur auf E-Mail, sondern sind den Anwendern auf Plattformen wie Microsoft Teams, Slack, Zoom, LinkedIn und WhatsApp gefolgt.

Eine zukunftssichere Lösung sollte zusätzliche moderne Schutzfunktionen beinhalten wie DMARC-basierte E-Mail-Authentifizierung, hochzuverlässige Erkennung kompromittierter Cloud-Konten und Einblick in lieferantenbezogene E-Mail-Bedrohungen.

Eine E-Mail-Sicherheitslösung sollte daher auch diese Vorteile bieten:

- **Optimierte E-Mail-Authentifizierung:** Eine der wirksamsten Methoden zum Stoppen von Spoofing-Nachrichten ist die E-Mail-Authentifizierung für ein- und ausgehende Nachrichten. Achten Sie zum Schutz Ihrer Marke darauf, dass der Anbieter vereinfachte Authentifizierungen per Hosting oder Managed Services bereitstellt. Die Unterstützung durch Experten kann sich im Zusammenhang mit DMARC als besonders nützlich erweisen.
- **Erkennung kompromittierter Konten:** Die Kombination aus Transparenz zu E-Mail-Bedrohungen (wie reale Klicks auf Phishing-Nachrichten) und Cloud Access Broker-Warnmeldungen sorgt dafür, dass kompromittierte Konten zuverlässiger erkannt werden und die Anzahl der False Positives reduziert wird. Gleichzeitig können automatisierte Reaktionen umgesetzt werden, z. B. das Erzwingen einer Kennwortzurücksetzung oder das Aufheben der Freigabe vertraulicher Dokumente.
- **Phishing-Schutz jenseits von E-Mails:** URLs zu schädlichen Webseiten sind mittlerweile die häufigste Zustellungsmethode für Bedrohungen. Das liegt unter anderem daran, dass Angreifer auf diesem Weg Anwender überall erreichen können, sei es über Messaging-, Collaboration- oder Social-Media-Anwendungen. Wählen Sie eine Lösung, die URLs in Echtzeit untersucht, damit schädliche Links unabhängig davon blockiert werden, wo und wann Anwender darauf zuzugreifen versuchen.
- **Reduziertes Risiko durch Lieferanten:** Ohne die erforderliche Transparenz ist es schwierig, Bedrohungen in der Lieferkette aufzuspüren. E-Mail-Sicherheitslösungen mit integrierten Funktionen zur Reduzierung von Lieferantenrisiken bewerten das Risiko von Lieferantenkonten und erkennen, wenn diese kompromittiert wurden. Dieser proaktive Ansatz trägt dazu bei, E-Mail-Betrug zu verhindern, und kann in Kombination mit Authentifizierung den Schutz vor einem der schwierigsten Angriffsvektoren enorm verbessern.

Mit Funktionen wie diesen sind Ihre IT- und Sicherheitsteams neuen Bedrohungen aus allen Bereichen stets einen Schritt voraus.

6. Ergebnisse des Proofpoint-Bedrohungsforschungsteams.

© Proofpoint, Inc. 2025

Fazit

Mehr als 94 % der Bedrohungen, die sich gegen Ihre Mitarbeiter richten, beginnen mit einer E-Mail.[7] Deshalb ist es besonders wichtig, diesen primären Vektor effizient zu schützen.

Für maximalen Bedrohungsschutz sollten Sie eine umfassende E-Mail-Sicherheitslösung wählen, die sowohl grundlegende als auch erweiterte Schutzfunktionen bietet und in der Lage ist, Bedrohungen automatisch zu erkennen und abzuwehren. Die Lösung sollte sich durch hervorragende Anwenderfreundlichkeit auszeichnen und idealerweise über flexible Bereitstellungsoptionen verfügen, sodass auch zukünftige Änderungen abgedeckt werden. Die Lösung Ihrer Wahl sollte auch digitale Kanäle jenseits von E-Mail absichern, darunter Collaboration-Tools, Messaging-Plattformen und Cloud-Anwendungen.

Wenn Sie momentan fragmentierte moderne Einzellösungen nutzen, besteht enormes Potenzial für verbesserten E-Mail-Schutz. Bewerten Sie jetzt, wie gut Ihre Sicherheitsmaßnahmen Sie vor allen personenzentrierten Bedrohungen schützen – in E-Mails und darüber hinaus.

Proofpoint bietet personenzentrierte Sicherheit

Mit Proofpoint Core Email Protection kann Ihr Unternehmen bestehende Risiken überall dort reduzieren, wo Ihre Anwender interagieren – heute ebenso wie morgen.

Proofpoint Core Email Protection stoppt 99,99 % aller E-Mail-Bedrohungen, bevor sie Schaden anrichten können. Unterstützt durch unsere branchenführende KI-Erkennungstechnologie Proofpoint Nexus identifiziert und behebt die Lösung moderne E-Mail-Bedrohungen wie Phishing, BEC, Malware, Ransomware, Kontoübernahmen, Nachahmung und Social Engineering. Eine moderne und intuitive Konsole ermöglicht Sicherheitsanalysten effizientes Arbeiten und bietet ihnen umfassenden Einblick in Bedrohungen sowie automatisierte Behebungs-Workflows. Mit ihren flexiblen SEG- und API-basierten Bereitstellungsoptionen deckt die zukunftsfähige Architektur unserer Lösung auch die Bedrohungen von morgen ab.

Deshalb vertrauen 2 Millionen Kunden, darunter 85 % der Fortune 100-Unternehmen beim Schutz der Mitarbeiter und des Unternehmens mit personenzentrierter Sicherheit auf Proofpoint.

Weitere Informationen erhalten Sie von unserem Vertriebsteam unter sales@proofpoint.com.

7. Ergebnisse des Proofpoint-Bedrohungsforschungsteams.

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. ©Proofpoint, Inc. 2025

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →

0203-010-04-02