

Proofpoint Impersonation Protection

Schutz für Ihre Kommunikation mit vertrauenswürdigen Partnern, Kunden und Lieferanten



Wichtige Highlights

- **Schutz Ihrer vertraulichen Unternehmenskommunikation vor Nachahmerbedrohungen**
- **Verhinderung des Missbrauchs Ihrer Identität und Marke durch Nachahmer**
- **Erkennung und Stilllegung schädlicher Doppelgänger-Domains**
- **Erkennung von und Schutz vor riskanten Lieferanten, einschließlich kompromittierten Lieferantenkonten**
- **Absicherung der E-Mails, die in Ihrem Namen von Anwendungen, Geräten, SaaS-Plattformen und KI-Agenten gesendet werden**
- **Unterstützt von Nexus[®] AI, Machine Learning, LLMs und Verhaltensanalysen**

Die Geschäftsabläufe der meisten Unternehmen sind auf E-Mails angewiesen. Angreifer haben jedoch herausgefunden, wie sie vertrauenswürdige Geschäftskommunikation kapern können. Und dank generativer KI sind diese Angriffe schneller, überzeugender und einfacher skalierbar geworden. Die Bedrohungsakteure können sich als Ihr Unternehmen, Ihre Marke oder Ihre Geschäftspartner ausgeben und innerhalb von Minuten statt Stunden glaubwürdige E-Mails und Websites erstellen.

Laut dem Internet Crime Complaint Center des FBI verursacht Business Email Compromise (BEC) jedes Jahr Verluste in Milliardenhöhe, wobei die Verluste kontinuierlich weiter steigen. Mittlerweile wird KI vom FBI als eigenständiger Bedrohungsfaktor eingestuft, der insbesondere durch Angriffe mit bestätigter KI-Komponente für BEC-Verluste in zweistelliger Millionenhöhe verantwortlich ist. Gleichzeitig warnt das FBI davor, dass diese Zahl das wahre Ausmaß wahrscheinlich nur unzureichend wiedergibt.

Bei diesen Angriffen werden häufig gleich mehrere Nachahmungstaktiken wie gefälschte Domains, Doppelgänger-Domains und kompromittierte Lieferantenkonten kombiniert. Dadurch gefährden sie die Kommunikation mit vertrauenswürdigen Partnern, Kunden und Lieferanten, sodass es für die Empfänger schwieriger ist, zwischen legitimen und betrügerischen Nachrichten zu unterscheiden.

Proofpoint nutzt einen umfassenden und mehrschichtigen Ansatz, um Ihr Unternehmen und Ihre Marke vor Missbrauch durch Nachahmer zu schützen. Wir bieten die Tools, Technologien und Ressourcen, um von Anwendern generierte E-Mails und App-E-Mails zu authentifizieren, in Ihrem Namen gesendete Nachrichten abzusichern, riskante oder potenziell kompromittierte Lieferantenkonten zu identifizieren und nach schädlichen Doppelgänger-Domains zu suchen, damit diese stillgelegt werden können.

Schutz Ihrer Marke vor Missbrauch durch Nachahmer

Eine der häufigsten Nachahmungstaktiken ist Domain-Spoofing. Durch generative KI ist es schneller möglich, gefälschte Nachrichten zu erstellen, die sich schwerer von echten unterscheiden lassen. Ohne geeignete Kontrollen können Angreifer dabei ganz einfach Ihre vertrauenswürdigen Domains übernehmen und mithilfe von KI im großen Maßstab absolut überzeugende Nachrichten erstellen. Auf diese Weise können sie Ihre Kunden, Partner und sogar Ihre Mitarbeiter so schnell und raffiniert ins Visier nehmen, wie es noch vor einem Jahr nicht möglich war. E-Mail-Authentifizierung bietet hier den besten Schutz.

Proofpoint Impersonation Protection vereinfacht die DMARC-Implementierung, indem Sie durch jeden Schritt der Einrichtung geführt werden, damit sowohl Ihre Anwender- als auch Ihre App-E-Mails authentifiziert werden. Unsere Experten helfen Ihnen, alle Ihre legitimen Versender zu erkennen und stellen zudem sicher, dass alle Ihre E-Mails – einschließlich E-Mails von autorisierten externen Dienstleistern – zuverlässig authentifiziert werden.

Durch die Integration mit Proofpoint Threat Protection können Sie die DMARC-Authentifizierung für eingehende Nachrichten zuverlässig durchsetzen. Die Lösung bietet eine zusätzliche Schutzebene gegen KI-generierte Nachahmungsversuche, die Ihre vertrauenswürdigen Domains fälschen. Außerdem können Sie DMARC-Richtlinien außer Kraft setzen, ohne legitime E-Mails zu blockieren oder durch Safelists die Sicherheit zu gefährden. Diese Integration bietet Ihnen einen vollständigen Überblick über ein- und ausgehende E-Mails sowie über alle Nachrichten, die Ihre vertrauenswürdige Domain verwenden. Dazu zählen auch Nachrichten von externen Versendern sowie E-Mails, die in Ihrem Namen von KI-Agenten gesendet werden.

Schutz vor kompromittierten Lieferantenkonten

Angreifer nutzen zunehmend die Supply Chain aus, um vertrauenswürdige Geschäftskommunikation zu gefährden, indem sie mit kompromittierten Lieferantenkonten die E-Mail-Threads zwischen Ihnen und Ihren Geschäftspartnern kapern. Mithilfe von generativer KI können sie frühere Gespräche analysieren und den Schreibstil eines Lieferanten nachahmen, sodass betrügerische Nachrichten schwerer zu erkennen sind. Und wenn diese E-Mails von legitimen Lieferantenkonten stammen und keine Schaddaten enthalten, können sie herkömmliche Authentifizierungs- und Erkennungskontrollen unterlaufen. Die möglichen Folgen: erhebliche finanzielle Verluste, Datendiebstahl, Erpressung oder Ransomware.

Proofpoint Impersonation Protection hilft Ihnen, riskante und potenziell kompromittierte Lieferanten zu erkennen und zu blockieren. Die Lösung nutzt verhaltensbasierte KI, Machine Learning und Bedrohungsdaten aus der großen Kundenbasis von Proofpoint, um Anzeichen für kompromittierte Lieferanten aufzudecken. Dazu gehören auch Angriffe, bei denen mithilfe generativer KI überzeugendere Köder erstellt werden. Adaptive Kontrollen wie die automatische URL-Isolierung tragen dazu bei, das Risiko durch kompromittierte Absender zu verringern. Die Integration mit Proofpoint Threat Protection in Verbindung mit dem Kontext zu Absender-/Empfänger-Beziehungen vereinfachen die Reaktion auf Zwischenfälle mit Lieferanten sowie entsprechende Untersuchungen.

Erkennung und Entfernung schädlicher Websites sowie Doppelgänger-Domains

Bedrohungsakteure erstellen speziell für Angriffe konzipierte Websites. Einige geben sich als andere Unternehmen, Marken oder Institutionen aus, um Ihre Mitarbeiter, Kunden oder Partner zu täuschen. Andere ahmen Ihr eigenes Unternehmen nach und verwenden Domains und Webseiten, die Ihrem Logo, Layout und Markenerlebnis täuschend ähnlich sind. Durch generative KI lassen sich beide Arten von Angriffen einfacher erstellen, erkennen und skalieren. Betrüger nutzen diese Websites für Anmeldedaten-Phishing, BEC, Angriffe per Telefon und andere Methoden, für die eine überzeugende digitale Präsenz notwendig ist.

Mit Proofpoint Impersonation Protection suchen wir kontinuierlich nach neu registrierten Domains, die sich

als Ihr Unternehmen ausgeben könnten, und stellen den Kontext zur Verfügung, der zur Bewertung potenzieller Risiken erforderlich ist.

Die Erkennung ist nur der erste Schritt. Wenn Sie eine verdächtige Website an unser Takedown-Team senden, untersuchen wir sie, sammeln verfügbare Beweise und bemühen uns, schädliche Aktivitäten einzudämmen und die Website zu entfernen. Wir unterhalten ein breites Netzwerk von Internet-Infrastrukturanbietern und vertrauenswürdigen Partnern, darunter Registraren, Hosting-Anbietern, E-Mail-Dienstanbietern, Blocklist-Partnern und mehr.

Unser Team verwaltet den Takedown-Prozess in Ihrem Namen, sodass Sie nicht selbst ermitteln müssen, wen Sie kontaktieren sollen oder welche Unterlagen erforderlich sind. Unsere Takedown-Services beschränken sich nicht auf Doppelgänger-Domains, sondern bieten Unterstützung bei der Abwehr von schädlichen Subdomains und URLs sowie von Nicht-Doppelgänger-Domains.

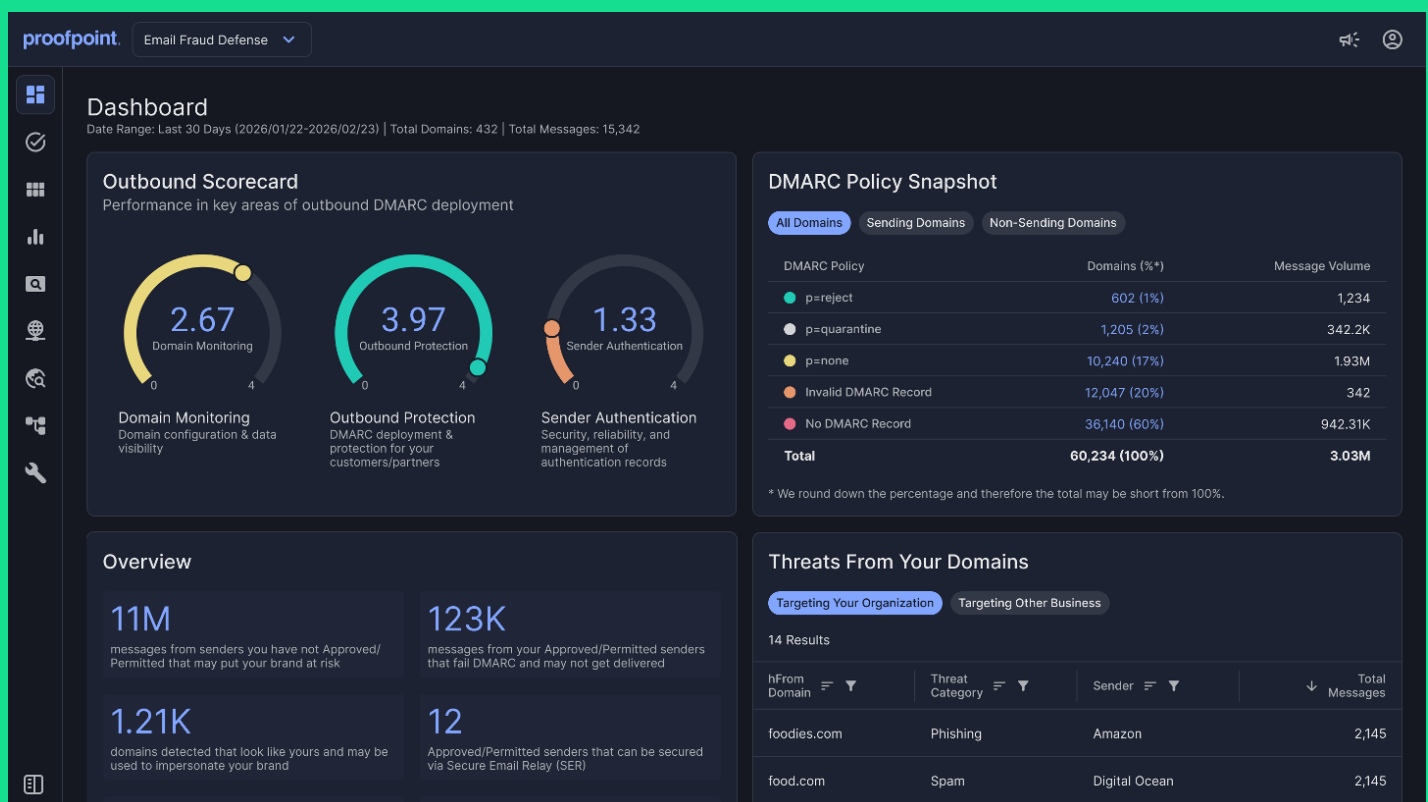


Abb. 1: Proofpoint bietet Ihnen einen Überblick über Domain-Spoofing-Bedrohungen, schädliche Doppelgänger Ihrer Domains sowie E-Mails, die von Ihren vertrauenswürdigen Domains versendet werden.

Sichere E-Mail, die in Ihrem Namen gesendet werden

Nicht alle E-Mails, die Ihre Domain verlassen, stammen von einer Person, die eine Nachricht verfasst. HR-Plattformen senden Gehaltsabrechnungen, CRM-Tools senden Kundenbelege, Bürogeräte senden Scan-to-E-Mail- sowie Fax-Benachrichtigungen, und neuerdings generieren auch KI-Agenten Nachrichten in Ihrem Namen. Jede Quelle kann als Einfallstor missbraucht werden. Wenn eine Anwendung, ein Gerät oder ein Versanddienst kompromittiert wird, können Angreifer über diesen vertrauenswürdigen Kanal schädliche E-Mails versenden, die anscheinend von Ihnen stammen, die Authentifizierungsprüfungen bestehen und (wenn sie mit generativer KI verbessert werden) absolut überzeugend aussehen.

Proofpoint Impersonation Protection schließt diese Lücke mit einem sicheren, dedizierten Relay für automatisierte Absender, die Ihre Domains verwenden – von internen Apps und Bürogeräten bis hin zu SaaS-Plattformen und KI-Agenten. Die Lösung akzeptiert nur E-Mails von verifizierten, authentifizierten Quellen, wendet auf jede Nachricht erweiterte Spam- und Virenschutz-Scans an und DKIM-signiert genehmigte E-Mails. Dadurch unterstützen Ihre ausgehenden Quellen den DMARC-Abgleich und die SPF-Konformität, ohne den legitimen Nachrichtenfluss zu stören. Proofpoint SER isoliert diesen Verkehr auch hinter dedizierten, seriösen IP-Adressen und trägt so dazu bei, Ihre Versandinfrastruktur und den Ruf Ihrer Marke vor Bedrohungsakteuren zu schützen,

die andernfalls die Vertrauenswürdigkeit Ihrer Domain missbrauchen könnten.

Schaffen Sie Sichtbarkeit, Kontrolle und Compliance

Proofpoint Impersonation Protection bietet Ihnen eine zentrale Übersicht und Kontrollen für große Versanddienste wie Amazon SES. Sie können sehen, welche Nachrichten Ihre Domain in großen Mengen verlassen, und Nachrichten bis zu der Anwendung, dem Gerät oder dem KI-Agenten zurückverfolgen, die sie gesendet haben. Die optionale Verschlüsselung und Datenverlustprävention tragen zum Schutz sensibler Daten wie personenbezogenen Daten und geschützten Gesundheitsdaten in Transaktionsnachrichten bei. Diese Kontrollen unterstützen die Einhaltung von Frameworks und Vorschriften wie HIPAA-, SEC- und FINRA-Anforderungen.

Proofpoint Impersonation Protection hilft Ihnen auch dabei, die wichtigsten Anforderungen von Postfach-Anbietern in Bezug auf Absenderidentität und Nachrichtenintegrität für Massenversender zu erfüllen. Durch die Unterstützung von Abmelde-Headern sowie die zentrale Listenverwaltung gewährleistet die Lösung, dass legitime E-Mails weiterhin den Posteingang erreichen.

Weitere Informationen

Weitere Informationen finden Sie unter proofpoint.com/de.



Information zu Proofpoint, Inc. Proofpoint, Inc. ist ein weltweiter Marktführer bei personen- und agentenzentrierter Cybersicherheit und schützt Verbindungen zwischen Anwendern, Daten und KI-Agenten über E-Mail, Cloud und Collaboration-Tools. Proofpoint ist ein vertrauenswürdiger Partner für mehr als 80 Prozent der Fortune 100, über 14.000 große Unternehmen sowie für Millionen kleinerer Firmen und stoppt Bedrohungen, verhindert Datenverlust und sichert die Interaktionen zwischen Anwendern und KI-Workflows ab. Die Collaboration- und Datenschutzplattform von Proofpoint hilft Unternehmen jeder Größe, ihre Mitarbeiter zu schützen und zu unterstützen, damit sie KI sicher und bedenkenlos einsetzen können. Weitere Informationen unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: [LinkedIn](#)

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

proofpoint®