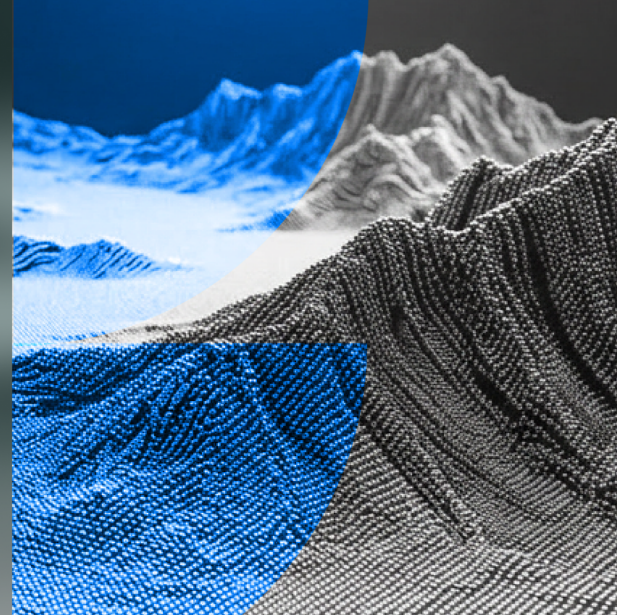


Proofpoint Collaboration Security Prime

Vollständig und kontinuierlich sichere Zusammenarbeit im KI-Zeitalter



Wichtige Highlights

- Blockiert verschiedenste Bedrohungen mit einer Genauigkeit von 99,999 %
- Kann eine Kontenkompromittierung innerhalb von Minuten eindämmen – unabhängig davon, ob die Bedrohung per E-Mail, über andere Vektoren oder durch einen kompromittierten Lieferanten initiiert wird
- Reduziert die Klicks auf schädliche Links im realen Einsatz innerhalb von sechs Monaten nach der Bereitstellung um 40 %
- Verhindert Nachahmung und legt Doppelgänger-Domains still, bevor Ihre Kunden angegriffen werden können
- Senkt die Gesamtbetriebskosten durch Plattformkonsolidierung um 40 %

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die Menschen und Daten an agentenbasierten Arbeitsplätzen schützt.

Überblick

Künstliche Intelligenz hat die Welt grundlegend verändert. Angreifer nutzen sie für neuartige und personalisierte Angriffe, die raffinierter und mit größerem Umfang erfolgen als je zuvor. Kampagnen wie Business Email Compromise (BEC) haben um 27 % zugenommen, und KI-generiertes Phishing erzielt mittlerweile eine 4,5-mal höhere Klickrate als herkömmliches Phishing. Die Anwender sind anfälliger für KI-generierte Inhalte geworden, während die Verteidiger mit der Priorisierung von Warnmeldungen sowie durch fragmentierte Tools überfordert sind.

Für diese neue agentenbasierte Welt, in der KI-gestützte Tools und Assistenten die erweiterte Belegschaft bei E-Mail-, Messaging- und Cloud-Anwendungen ergänzen und so die bereits ausgenutzte Angriffsfläche noch weiter vergrößern, benötigen Unternehmen einen grundlegend anderen Ansatz.

Leider nutzen viele Unternehmen immer noch einen fragmentierten Sicherheitsansatz mit mehreren Einzelprodukten, der zu zusätzlichen Lücken in den Abwehrmaßnahmen führt, Teams isoliert und die Komplexität der betrieblichen Prozesse erhöht.

Sicherheitsteams müssen kanalübergreifende und mehrstufige Angriffe abwehren, die per KI skaliert wurden, und vertrauenswürdige Interaktionen schützen – sei es von Mensch zu Mensch, von Mensch zu KI-Assistent oder von Mensch zu Cloud-Anwendung. Dies ist nur mit einem umfassenden Ansatz möglich. Hier setzt Proofpoint Collaboration Security Prime an. Die Lösung vereint Bedrohungserkennung und -abwehr am agentenbasierten Arbeitsplatz.

Vorteile der Lösung:

- Frühzeitige Erkennung neuartiger KI-generierter Bedrohungen dank besserem Überblick über die Angriffsfläche
- Zuverlässige Blockierung dank branchenführender Genauigkeit und geringer False-Positive-Rate
- Kontinuierlicher Schutz vor und nach der Zustellung sowie für Browser und KI-Agenten
- Schutz der Geschäftskommunikation überall dort, wo sie stattfindet – in Chats, Anwendungen und mit Agenten
- Eindämmung von Kontenkompromittierung innerhalb von Minuten statt Tagen

Frühere Erkennung neuer Bedrohungen dank besserer Übersicht

Neuartige, KI-generierte Angriffe laufen schneller ab, als herkömmliche Verteidigungssysteme sie erfassen können. Dadurch umgehen sie veraltete Filter und erreichen Ihre Mitarbeiter über E-Mails, Collaboration-Plattformen und Cloud-Anwendungen gleichermaßen.

Proofpoint Collaboration Security Prime schließt diese Lücke mit kontinuierlichem, kanalübergreifendem Schutz, der den gesamten Bedrohungslebenszyklus abdeckt – für die E-Mail-Architektur vor und nach der Zustellung sowie vom Klick bis zum Login.

Proofpoint Prime bietet Schutz vor einem breiten Spektrum an Bedrohungen, darunter:

- Hochentwickeltes Phishing, einschließlich Anmeldedaten-Phishing und Callback Phishing
- BEC- und CEO-Nachahmung
- Malware-Übertragung
- QR-Code-Angriffe
- Angriffe per Telefon
- E-Mail-Bombing
- Ransomware
- Kontoübernahmen
- Missbrauch legitimer Dienste
- KI-generierte Angriffe und Techniken zur KI-Ausnutzung wie Prompt-Injection

Kernstück dieses Schutzes ist Proofpoint Nexus® AI, das branchenweit fortschrittlichste Erkennungsmodul. Nexus AI wurde mit einem der größten und vielfältigsten Datensätze der Branche trainiert und wertet pro Nachricht über 1.000 Attribute aus. Das Modul kombiniert fünf Modelltypen – Sprachmodelle, Beziehungsdigramme, Machine Learning, Bedrohungsdaten und Bildanalyse (Computer Vision) –, die zusammenarbeiten und kontinuierlich aus jedem Urteil lernen.

Das Ergebnis ist eine Erkennungseffizienz von 99,999 % und die branchenweit niedrigste False-Positive-Rate, sodass echte Bedrohungen gestoppt werden, ohne die Teams mit irrelevanten Meldungen zu überfordern.

Schutz vor Kontenkompromittierung

Kontenkompromittierung beschränkt sich nicht auf Phishing-E-Mails. Bedrohungsakteure können ihre Anmeldedaten-Angriffe mithilfe von künstlicher Intelligenz weit über den Posteingang hinaus ausweiten – von der Generierung überzeugender, pixelgenauer Nachbildungen von Anmeldeseiten bis hin zur Überwindung der Multifaktor-Authentifizierung durch automatisiertes Prompt-Bombing.

In einem Arbeitsumfeld mit intensiver Zusammenarbeit, die von Agenten unterstützt wird, müssen diese Bedrohungen in jeder Phase gestoppt werden – vor, während und nach einer Kompromittierung.

Proofpoint Collaboration Security Prime kann Kompromittierungen verhindern, noch bevor sie entstehen. Die SSO Password Guard-Funktion von Proofpoint

Prime erkennt, wenn Mitarbeiter ihr Unternehmenskennwort auf externen Websites wiederverwenden, und schließt damit eines der häufigsten Einfallstore für Anmeldedaten-Angriffe. Dabei wird der Schutz über E-Mails hinaus auf den Browser selbst ausgeweitet.

Wenn Prävention nicht ausreicht, erkennt Proofpoint Prime die Kompromittierung in Echtzeit. Die Lösung korreliert Identitäts- und Zugriffsindikatoren in Microsoft 365, Google Workspace und Okta, um Konten zu identifizieren, die Anzeichen einer Kompromittierung aufweisen.

Sobald eine Kompromittierung identifiziert ist, hilft Proofpoint Prime Ihnen, diese innerhalb weniger Minuten statt Tagen zu untersuchen und einzudämmen. Dadurch wird ihr Wirkungsradius begrenzt, noch bevor ein Angreifer weiter in die Umgebung vordringen kann.

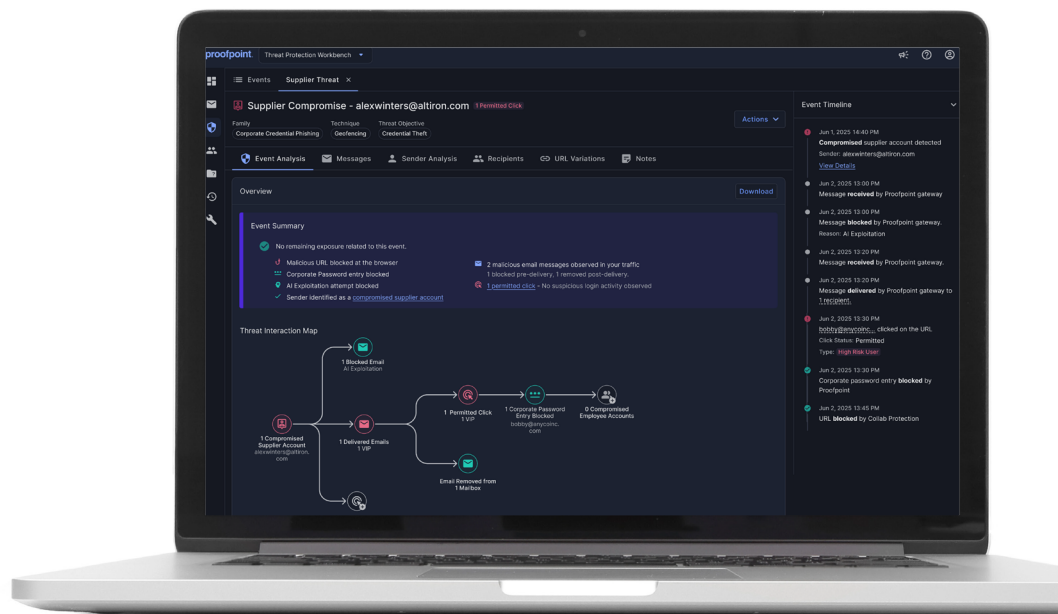


Abb. 1: Proofpoint Collaboration Security Prime stoppt und korreliert Bedrohungen über E-Mail-, Messaging- und Collaboration-, Cloud- und Lieferantentools hinweg.

Die KI-Modelle von Proofpoint Nexus® AI werden mit einem der größten und vielfältigsten Datensätze der gesamten Cybersicherheitsbranche trainiert.

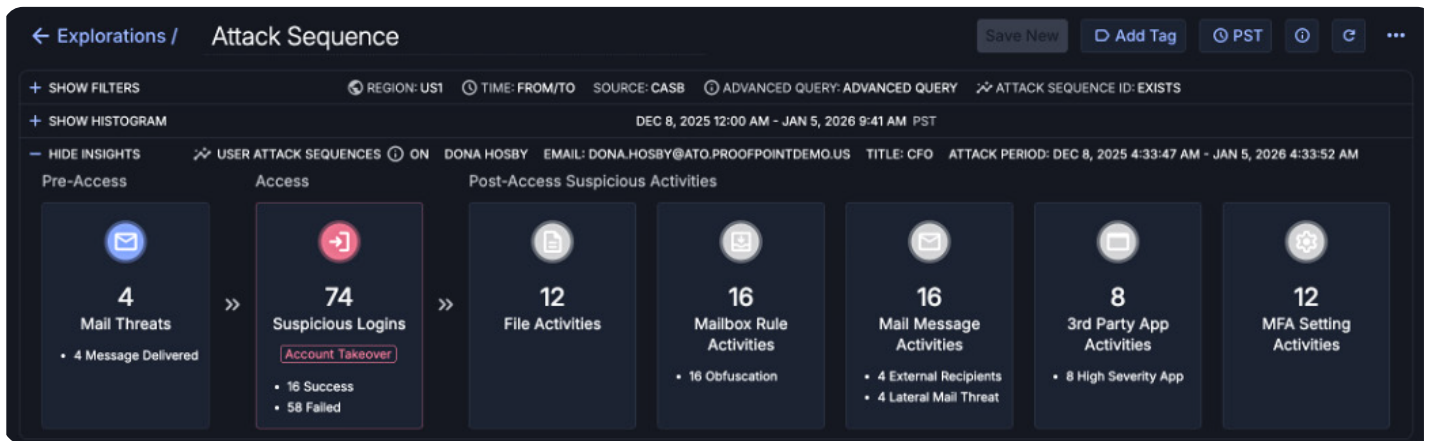


Abb. 2: Proofpoint Collaboration Security Prime bietet Einblicke in Angriffsabläufe und automatisiert die Eindämmung.

Schutz für Ihre vertrauenswürdige Geschäftskommunikation

Angreifer nutzen häufig Nachahmungstechniken, um sich in laufende geschäftliche Unterhaltungen einzuklinken, sei es durch direktes Domain-Spoofing, Doppelgänger-Domains oder kompromittierte Lieferantenkonten. Wenn Ihr Unternehmen oder Ihre Partner nachgeahmt oder kompromittiert werden, werden Ihre Mitarbeiter, Kunden und Partner gefährdet. Außerdem kann dies zu schwerwiegenden Schäden für Ihre Marke führen.

Mit Proofpoint Collaboration Security Prime können Sie diese Nachahmerrisiken proaktiv reduzieren. Sie erhalten einen vollständigen Überblick über alle E-Mails, die Ihre vertrauenswürdigen Domains verwenden. Dazu zählen auch Nachrichten von externen Versendern. Außerdem erhalten Sie Zugriff auf leistungsstarke Tools und Unterstützung durch Experten, die Sie bei der Implementierung der E-Mail-Authentifizierung zu jedem Schritt beraten. Dadurch können Sie vollständige DMARC-Compliance erreichen und verhindern, dass Angreifer Ihre Domains missbrauchen.

Wir schützen nicht nur von Anwendern generierte E-Mails, sondern auch App-E-Mails sowie Nachrichten und E-Mails, die in Ihrem Namen von externen SaaS-Partnern versendet werden.

In Bezug auf Lieferantenbedrohungen schützt Proofpoint Prime Ihre Mitarbeiter davor, von Angreifern ausgenutzt zu werden, die Konten von Drittanbietern verwenden. Proofpoint Prime identifiziert verdächtige Aktivitäten, die von Lieferantenkonten kommen, und wendet adaptive Schutzmaßnahmen wie Warnindikatoren und URL-Isolierung zur Risikoreduzierung an, ohne legitime Geschäftskommunikationen zu stören.

Proofpoint Prime bietet zudem Funktionen zur Erkennung von Doppelgänger-Domains. Die Lösung sucht im Internet dynamisch nach Domains, die Ihrer eigenen Domain sehr ähnlich sind, und bietet detaillierte Einblicke in deren Registrierungsdetails sowie potenzielle Missbrauchsversuche.

Dabei bieten wir nicht nur Erkennung, sondern können dank unserer engen Zusammenarbeit mit Registraren, Hosting-Unternehmen und Anbietern von Top-Level Domains (TLD) auch in Ihrem Namen schädliche Domains und URLs stilllegen. Unsere Experten verwalten den gesamten Prozess, sodass sich Ihre Teams auf Ihre zentralen geschäftlichen Abläufe konzentrieren können.

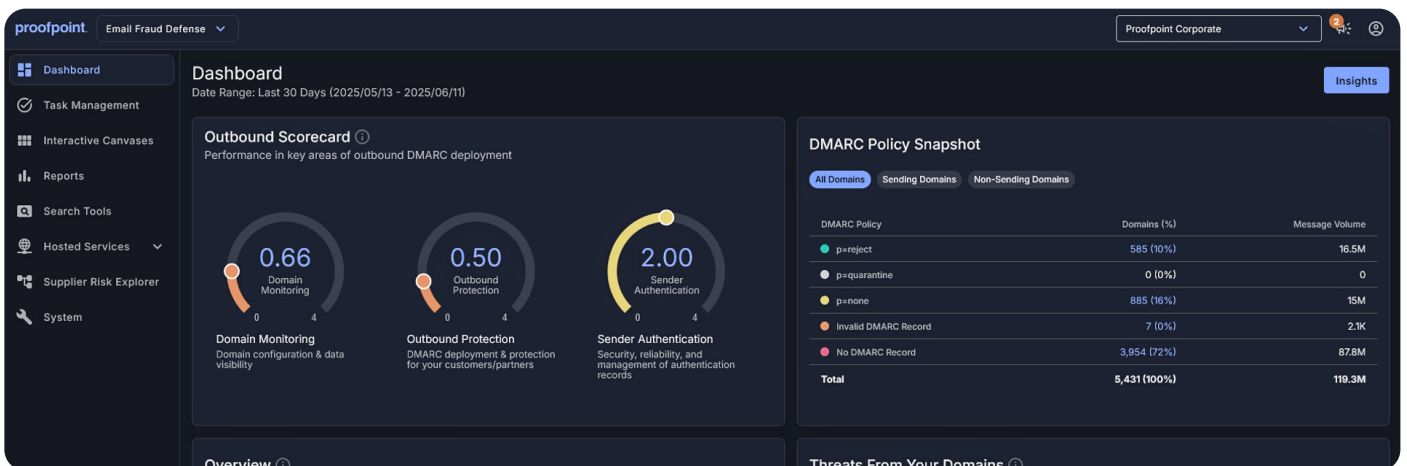


Abb. 3: Proofpoint Collaboration Security Prime bietet Einblicke in Nachahmungsbedrohungen wie Domain-Spoofing und schädliche Doppelgänger-Domains.

Stärkung der Mitarbeiter-Resilienz durch risikobasierte Hinweise

Da die Arbeit zunehmend kollaborativ und dynamisch wird, müssen die Mitarbeiter widerstandsfähiger gegen Cyberangriffe werden, was sich mit Compliance-orientierten Schulungen jedoch nicht erreichen lässt. Notwendig ist die Eindämmung personenbezogener Risiken durch Schulungen zum richtigen Zeitpunkt, die der Arbeitsweise von Anwendern entgegenkommen und zeigen, welche realen Risiken sie eingehen.

Proofpoint Collaboration Security Prime stärkt die menschliche Resilienz systematisch – nicht durch einmalige Schulungen, sondern durch einen kontinuierlichen Zyklus, der an reale Risiken gekoppelt ist.

Es beginnt mit der Zielgruppenbestimmung. Die Human Resilience Workbench erfasst Verhaltens- und Risikoindikatoren aus der gesamten Plattform und identifiziert automatisch besonders riskante Anwender, neue Mitarbeiter und Top Clicker, sodass sich die Sicherheitsteams auf die wichtigsten Punkte konzentrieren können.

Anschließend bestärkt Proofpoint Prime sichereres Verhalten in dem Moment, in dem das Risiko am höchsten ist. Mithilfe der KI-gestützten ThreatFlip-Funktion werden reale, aktive Bedrohungen mit einem Klick sofort in ausführbare Simulationen umgewandelt. Dadurch wird den Mitarbeitern unmittelbar nach dem Auftreten eines Angriffs gezeigt, wie dieser aussieht – und nicht erst Wochen später in einem allgemeinen Schulungsmodul.

Proofpoint Prime kann die Ergebnisse nachweisen. Dank Risikobewertungen und Benchmark-Analysen erhalten Administratoren einen klaren Überblick darüber, wo sich das Verhalten verbessert und wo noch Lücken bestehen. Unternehmen verzeichnen dank diesem Ansatz innerhalb von sechs Monaten 40 % weniger Klicks auf schädliche Links in der realen Welt. Dies zeigt, dass Resilienz – und nicht nur Sicherheitsbewusstsein – der Schlüssel zu nachhaltigem Wandel ist.

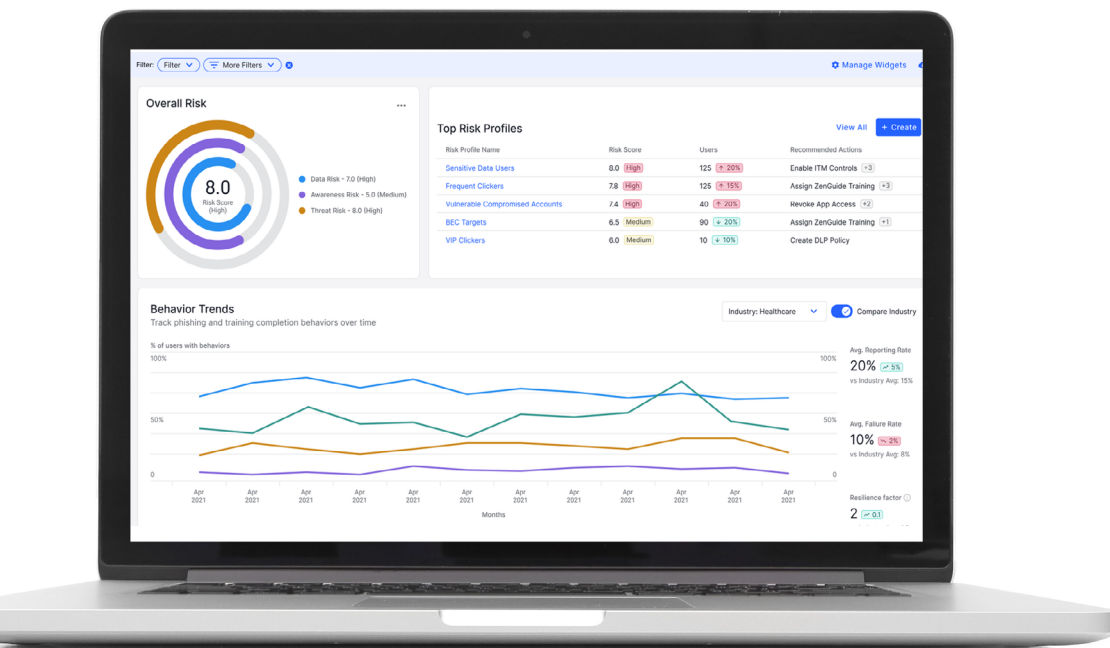


Abb. 4: Proofpoint Collaboration Security Prime bietet Einblick in das tatsächliche Anwenderverhalten, was gezielte, risikobasierte Schulungen ermöglicht.

Vereinfachung der Sicherheitsabläufe

Während sich Bedrohungen über E-Mail hinaus auf Collaboration-Tools, Cloud-Plattformen und Lieferantenökosysteme ausweiten, stehen Sicherheitsteams unter Druck, mit weniger Mitteln mehr zu erreichen. Die Situation wird durch isolierte Einzellösungen verschärft, da diese nicht nur die Komplexität erhöhen, sondern auch die Reaktionszeiten verlängern und die Betriebskosten in die Höhe treiben. Dies erschwert die Reduzierung von Risiken im großen Maßstab.

Proofpoint Collaboration Security Prime vereinfacht Ihre Sicherheitsabläufe, da hier die Bedrohungserkennung und -untersuchung vereint und Workflows sowie Reaktionsmaßnahmen automatisiert werden. Die Threat Protection Workbench nutzt native Integrationen, um Erkennungsdaten und Angriffsforensik aus E-Mails, Messaging- und Collaboration-Plattformen, Cloud-Konten sowie Lieferantenökosystemen zusammenzuführen. Dadurch können Teams in einem einzigen, einheitlichen Arbeitsbereich äußerst effizient mögliche Vorfälle untersuchen und konsequente Maßnahmen ergreifen.

Proofpoint Prime hilft Teams bei der effektiven Priorisierung ihrer Maßnahmen. Dazu korreliert die Threat Interaction Map Bedrohungen und Sicherheitsereignisse aus verschiedenen Kontrollpunkten und bietet eine Übersicht über die Angriffswege, sodass Analysten die schwerwiegendsten Vorfälle schnell identifizieren können. Parallel dazu untersucht die Lösung automatisch von Anwendern gemeldete Nachrichten, entfernt schädliche Inhalte und liefert Rückmeldungen an die Anwender. Dies reduziert den manuellen Aufwand und fördert sicheres Anwenderverhalten.

Das Ergebnis sind schnellere Reaktionen und weniger komplexe Betriebsprozesse. Gleichzeitig erhält Ihr Sicherheitsteam mit weniger Aufwand mehr Möglichkeiten, ohne dass der Schutz vernachlässigt wird.

Das richtige Schutzniveau

Proofpoint Collaboration Security Prime ist in mehreren Stufen verfügbar, sodass Sie den Schutz mit dem Risikoprofil und den betrieblichen Bedürfnissen Ihres Unternehmens in Einklang bringen können. Dabei baut jede Stufe auf der vorherigen auf.

Der Schutz erweitert sich von grundlegenden E-Mail-Bedrohungen und deckt Collaboration-Kanäle, Kontenkompromittierung, personenbezogene Risiken und fortschrittlichen Markenschutz ab.

Auf der nächsten Seite finden Sie eine Übersicht der verfügbaren Funktionen.



Weitere Informationen finden Sie unter **proofpoint.com/de**.

Über 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 10.000 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.

Alle Proofpoint Collaboration Security-Lösungsstufen sind sowohl für SEG- als auch für API-Bereitstellungen verfügbar. Je nach Bereitstellungsmodell sind möglicherweise unterschiedliche Funktionen verfügbar.

	Verfügbare Funktionen	Proofpoint Core Email Protection	Proofpoint Collaboration Security Tier 2	Proofpoint Collaboration Security Tier 3	Proofpoint Collaboration Security Prime
E-Mail-Sicherheit	BEC-, Phishing-, Callback-Phishing- und Malware-Schutz	✓	✓	✓	✓
	Mehrschichtige Erkennungslösungen, unterstützt von Nexus AI	✓	✓	✓	✓
	Hervorragende Bedrohungsdaten von über 2,8 Millionen Kunden	✓	✓	✓	✓
	Sandbox-Analyse von Anhängen und URLs	✓	✓	✓	✓
	URL-Veränderung und Sandbox-Analyse zum Klickzeitpunkt	SEG	SEG	SEG	SEG
	Isolierung verdächtiger Klicks bei veränderten URLs	VAPs*	Alle Anwender*	Alle Anwender*	Alle Anwender*
	Spam- und Graymail-Erkennung	✓	✓	✓	✓
	Kontextbezogene Warnhinweise in E-Mails	✓	✓	✓	✓
	Adaptive E-Mail-Hygiene, die basierend auf dem Anwenderverhalten selbstständig lernt	✓	✓	✓	✓
	Konfigurierbare Richtlinien zur E-Mail-Weiterleitung	SEG	SEG	SEG	SEG
	Automatische Behebung von Nachrichten	✓	✓	✓	✓
	Automatisiertes Abuse-Postfach	✓	✓	✓	✓
	Daten zu Very Attacked People (VAP)™, Bedrohungsakteuren und weltweiten Bedrohungen	✓	✓	✓	✓
Kanalübergreifender, mehrstufiger Bedrohungsschutz	Erkennung und Behebung kompromittierter Cloud-Konten		✓	✓	✓
	Blockierung schädlicher URLs, die über Messaging- und Collaboration-Anwendungen gesendet werden		✓	✓	✓
	Erkennung des Missbrauchs von Unternehmenskennwörtern auf riskanten oder nicht genehmigten Websites		✓	✓	✓
	Schutz vor kompromittierten Lieferantenkonten		✓	✓	✓
Mitarbeiter-Resilienz und Security-Awareness-Schulungen	Automatisierte, risikobasierte Schulungen für Anwender			✓	✓
	Stärkung des Mitarbeiterbewusstseins durch realistische, bedrohungs-basierte Simulationen			✓	✓
	Umwandlung von aktiven Bedrohungen in sichere Simulationen			✓	✓
	Erkennung und Priorisierung gefährdeter Anwender anhand von Verhalten, Bedrohungstelemetrie und Rollen			✓	✓
Schutz vor Nachahmern	E-Mail-Authentifizierung zur Verhinderung von Markenmissbrauch				✓
	Erkennung und Behebung von gefährlichen Doppelgänger-Domains				✓
	Sichere Weiterleitung von App-E-Mails (250 GB)				✓

SEG = Ausschließliche Bereitstellung eines sicheren E-Mail-Gateways

* = Nur für SEG-Bereitstellungen verfügbar.