proofpoint.

KURZVORSTELLUNG

Proofpoint Collaboration Security Prime

Schutz vor KI-gestützten Angriffen per E-Mail und in anderen Kanälen

Wichtige Highlights

- Blockierung verschiedenster Bedrohungen mit einer Genauigkeit von 99,999 %
- Ausweitung des personenzentrierten Schutzes auf E-Mail und darüber hinaus
- Stärkung der Resilienz Ihrer Mitarbeiter mit risikobasierten Empfehlungen und Erkenntnissen
- Minimierung der Auswirkungen von Kompromittierungen interner Konten und Lieferantenkonten
- Vereinfachung der Prozesse durch eine einheitliche Plattform, die Workflows automatisiert
- Vermeidung der Kosten und Komplexität fragmentierter Lösungen durch Konsolidierung

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

Überblick

In der heutigen Zeit, die vom Einsatz von KI-Agenten in Unternehmen geprägt ist, sollen KI-gestützte Tools und Assistenten den Mitarbeitern helfen, effektiver zu arbeiten. Diese KI-Agenten werden Teil der erweiterten Belegschaft und interagieren mit Mitarbeitern, Anwendungen und anderen Agenten per E-Mail, Messaging-Plattformen, Cloud-Anwendungen und mehr. Mit der Erweiterung des Arbeitsplatzes wächst auch die Angriffsfläche, und Angreifer nutzen diese vertrauenswürdigen Kommunikationskanäle bereits aus.

Viele Unternehmen arbeiten mit einem 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:

- Schutz vor kanalübergreifenden, mehrstufigen Angriffen mit unübertroffener Genauigkeit
- Minimierung der Auswirkungen von Kompromittierungen von Mitarbeiter- und Lieferantenkonten
- Absicherung vertrauenswürdiger Geschäftskommunikation mit Lieferanten, Partnern und Kunden
- Stärkung der Resilienz Ihrer Mitarbeiter mit gezielten Schulungen, die auf personenbezogenen Risiken basieren
- Optimierung der Sicherheitsabläufe durch Automatisierung

Schützen Sie Anwender bei der Zusammenarbeit – per E-Mail und darüber hinaus

Da die Arbeit sich weiter in Richtung eines vernetzten und KI-unterstützten Arbeitsplatzes entwickelt, schützt Proofpoint Collaboration Security Prime die Anwender überall da, wo sie arbeiten. Die Lösung stoppt kanalübergreifende Angriffe per E-Mail sowie über Collaboration- und Messaging-Tools wie Microsoft Teams, Slack, soziale Netzwerke und Cloud-basierte Anwendungen. Darüber hinaus beeinträchtigt sie dabei nicht die Arbeitsabläufe.

Proofpoint Prime schützt die Anwender vor einem breiten Spektrum an Bedrohungen:

- Komplexe Phishing-Angriffe
- Business Email Compromise (BEC)
- Angriffe per Telefon (TOAD)
- E-Mail-Bombing
- Ransomware
- Kontoübernahmen
- KI-generierte Angriffe und Techniken zur KI-Ausnutzung wie Prompt-Injection

Darüber hinaus werden Angriffe in allen Phasen des Bedrohungszyklus gestoppt – vor und nach der Zustellung, zum Klickzeitpunkt und bei der Anmeldung.

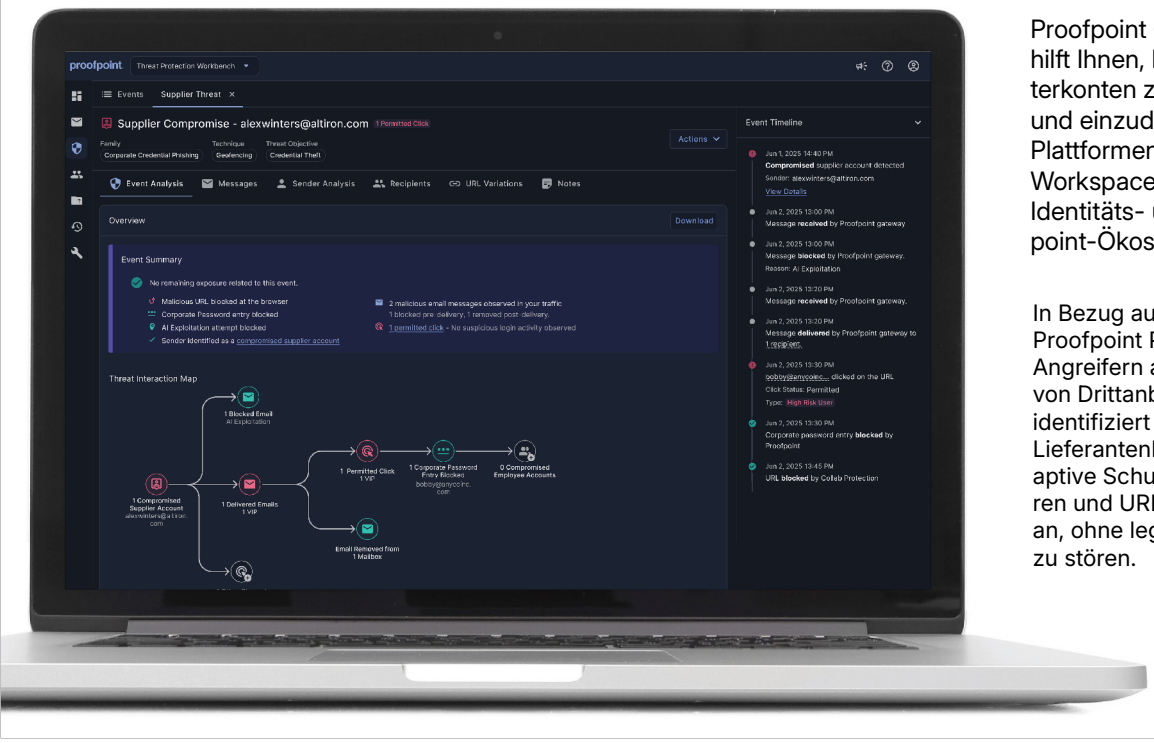

Abb. 1: Proofpoint Collaboration Security Prime stoppt und korreliert Bedrohungen über E-Mail, Messaging- und Collaboration-, Cloud- und Lieferantentools.

Proofpoint Prime nutzt die KI-Technologien von Proofpoint Nexus® und bietet hervorragenden Bedrohungsschutz mit einer Effizienz von 99,999 %. Dazu greift Proofpoint Prime auf unsere umfangreichen Bedrohungsdaten, hochentwickelte Sprachmodelle, Beziehungsdiagramme, Machine Learning, Verhaltensanalysen und Bilderkennung zurück. Diese Technologien arbeiten zusammen, um Angriffe zu erkennen und zu stoppen, noch bevor Schaden entsteht.

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

Schutz vor Kontenkompromittierung

Angreifer nutzen kompromittierte Identitäten, um auf legitime Konten Ihrer Mitarbeiter sowie Ihrer vertrauenswürdigen Lieferanten zuzugreifen und mehrstufige Angriffe zu starten. An einem Arbeitsplatz, der von Zusammenarbeit geprägt und von Agenten unterstützt wird, müssen die Auswirkungen dieser Bedrohungen so weit wie möglich minimiert werden.

Proofpoint Collaboration Security Prime hilft Ihnen, kompromittierte Mitarbeiterkonten zu erkennen, zu untersuchen und einzudämmen, und deckt dabei Plattformen wie Microsoft 365, Google Workspace und Okta ab. Dazu werden Identitäts- und Aktivitätssignale im Proofpoint-Ökosystem korreliert.

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

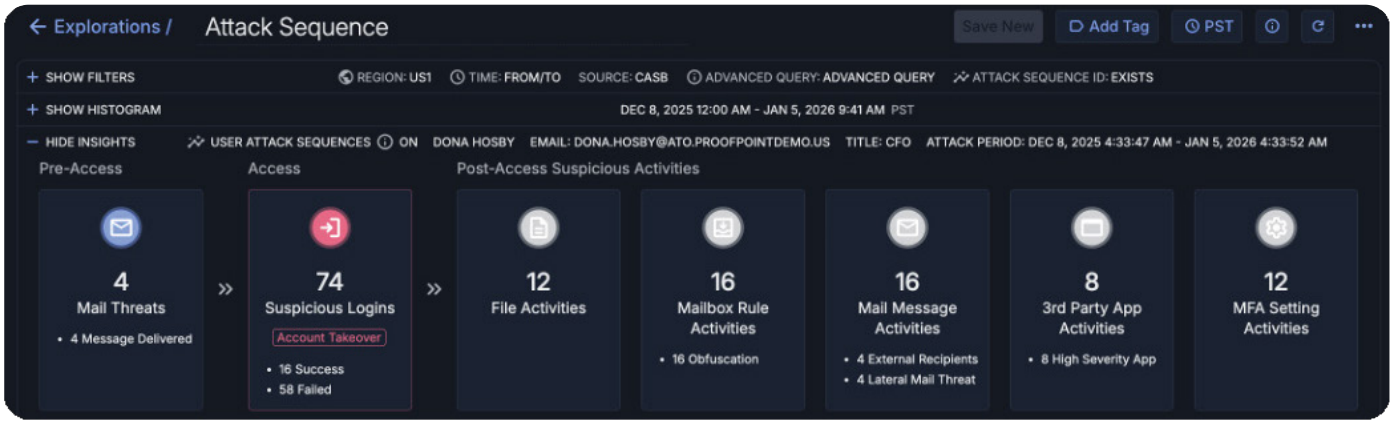

Abb. 2: Proofpoint Collaboration Security Prime bietet Einblicke in Angriffsabläufe und automatisiert die Eindämmung.

Schutz für Ihre vertrauenswürdige Geschäftskommunikation

Angreifer nutzen häufig Nachahmungstechniken, um sich in laufende geschäftliche Unterhaltungen einzuklinken. Wenn Ihr Unternehmen nachgeahmt wird (z. B. durch Domain-Spoofing oder Doppelgänger-Domains), 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.

Proofpoint Prime bietet zudem Funktionen zur Erkennung von Doppelgänger-Domains. Die Lösung sucht dynamisch im Internet 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.

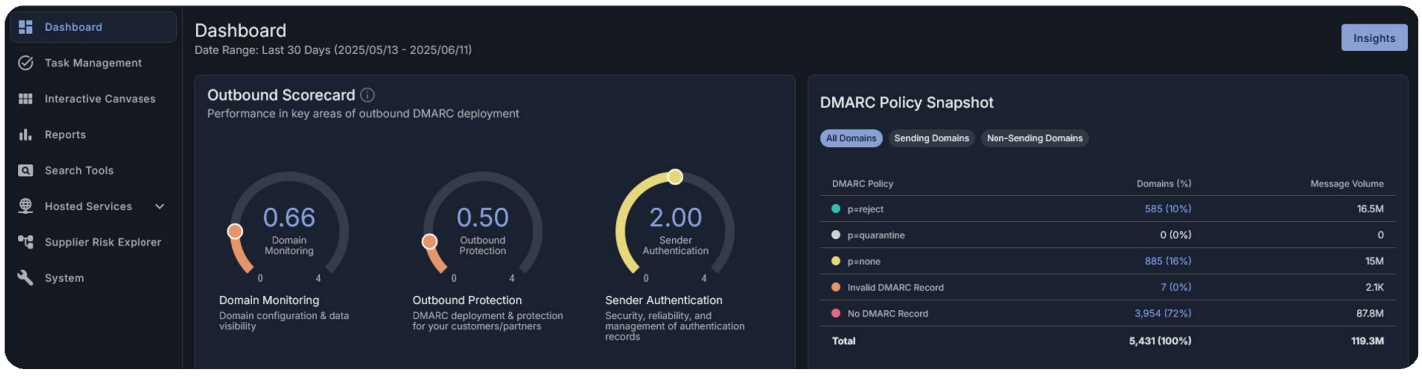

Abb. 3: Proofpoint Collaboration Security Prime bietet Einblicke in Nachahmungsbedrohungen wie Domain-Spoofing und böswillige Doppelgänger-Domains.

Stärkung der Mitarbeiter-Resilienz durch risikobasierte Hinweise

Da die Arbeit zunehmend kollaborativ und dynamisch wird, müssen die Mitarbeiter widerstandsfähiger gegen Cyberangriffe werden, was sich jedoch mit Compliance-orientierten Schulungen 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 hilft Ihrem Unternehmen, indem Ihre Mitarbeiter zu sichereren Entscheidungen angeleitet werden. Die Lösung bietet automatisierte, zielgerichtete Schulungen, die auf das Verhalten, die Rolle, die Angriffsanfälligkeit und das individuelle Risikoprofil – kurz: auf das personenbezogene Risiko – des jeweiligen Anwenders zugeschnitten sind. Mithilfe von KI verwandelt Proofpoint Prime reale Bedrohungen mit einem einzigen Klick in sofort verfügbare Simulationen. Dies stellt sicher, dass die Schulung aktive Risikoindikatoren nutzt und messbare sowie nachhaltige Verhaltensänderungen fördert.

Die Schulungsmodule passen sich nicht nur an individuelle Risikoindikatoren an, sondern werden auch durch ansprechende, Gamification-Erlebnisse vermittelt. Dadurch sind die Anwender zur Teilnahme motiviert, und ihr sicheres Verhalten wird im Laufe der Zeit verstärkt. In intuitiven Dashboards erhalten die Anwender einen klaren Überblick über ihren Fortschritt, damit sie informiert sind und sich verantwortlich verhalten.

Gleichzeitig können Administratoren ihre Programme leicht an die Risikoprioritäten des Unternehmens anpassen. Das steigert die Motivation, fördert messbare Verhaltensänderungen und verbessert die Sicherheitskultur in Ihrem Unternehmen.

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 leisten. 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 Kontrollpunkte 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 mehr Möglichkeiten mit weniger Aufwand, ohne den Schutz zu vernachlässigen.

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.

proofpoint.

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 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.

	Verfügbare Funktionen	Proofpoint Core Email Protection	Proofpoint Collaboration Security – Stufe 2	Proofpoint Collaboration Security – Stufe 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		●	●	●
	Schutz vor kompromittierten Lieferantenkonten		●	●	●
Mitarbeiter-Resilienz und Security-Awareness-Schulungen	Automatisierte, risikobasierte Schulungen für Anwender			●	●
	Stärkung des Mitarbeiterbewusstseins durch realistische, bedrohungsbasierte Simulationen			●	●
	Umwandlung von aktiven Bedrohungen in sichere Simulationen			●	●

SEG = nur bei Bereitstellung als sicheres E-Mail-Gateway

***** Nur für SEG-Bereitstellungen verfügbar.