proofpoint.

KURZVORSTELLUNG

Proofpoint Prime Threat Protection für Enterprise-Kunden

Wichtige Vorteile

- Blockierung verschiedenster Bedrohungen mit einer Genauigkeit von 99,99 %
- Ausweitung des Schutzes auf alle Plattformen – E-Mail und darüber hinaus
- Stärkung der Resilienz Ihrer Mitarbeiter mit risikobasierten Empfehlungen und Erkenntnissen
- Schnellere Reaktion bei kompromittierten Konten Ihrer Mitarbeiter und Lieferanten
- Vereinfachte Abläufe mit branchenführender Erkennungsgenauigkeit und automatisierten Workflows
- Maximale Kosteneffizienz durch Konsolidierung und vorkonfigurierte Integrationen

Überblick

E-Mails sind weiterhin ein primärer Vektor für Cyberbedrohungen. In den letzten Jahren hat sich die Angriffsfläche allerdings erweitert und Angreifer attackieren die Mitarbeiter per E-Mail und auf digitalen Kanälen wie Messaging-Plattformen, Collaboration-Tools, Cloud-Anwendungen und File-Sharing-Diensten.

Viele Unternehmen reagieren mit einem fragmentierten Sicherheitsansatz mit mehreren Einzelprodukten, bei dem zahlreiche Lücken in den Schutzmaßnahmen verbleiben und viele Risiken nicht berücksichtigt werden. Hinzu kommt: Die Verwaltung und Integration all dieser Tools ist kompliziert.

Zur Abwehr personenzentrierter Angriffe benötigen Sie einen umfassenden Ansatz. Hier kann Proofpoint Prime Threat Protection (Prime) helfen.

Mit Proofpoint Prime können Sie Ihr Unternehmen vor mehrstufigen Angriffen auf mehreren Kanälen schützen, die Sicherheit Ihrer geschäftlichen Kommunikation gewährleisten und die Sicherheitsabläufe auf allen Ebenen vereinfachen. Außerdem erhalten Sie risikobasierte Empfehlungen für Ihre Mitarbeiter.

Stoppen von Bedrohungen per E-Mail und auf anderen digitalen Kanälen

Für die effiziente Kommunikation und Zusammenarbeit nutzen Angestellte heute Microsoft Teams, Slack, Cloud-Anwendungen, File-Sharing-Dienste und andere Tools. Diese steigern die Produktivität Ihrer Mitarbeiter, vergrößern aber auch die Angriffsfläche. Personenzentrierte Cyberangriffe beschränken sich nicht mehr nur auf E-Mails. Ihre Schutzmaßnahmen sollten Schritt halten.

Proofpoint Prime schützt Ihren gesamten digitalen Arbeitsbereich in Echtzeit vor BEC, Ransomware, Spearphishing und zahlreichen anderen Bedrohungen, die über E-Mail, Sofortnachrichten, soziale Netzwerke oder Collaboration-Anwendungen erfolgen.

Proofpoint Prime nutzt die KI-Technologien von Proofpoint Nexus® und bietet hervorragenden Bedrohungsschutz mit einer Effizienz von 99,99 %. 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.

Dank der umfangreichen Abdeckung und der leistungsstarken KI-Funktionen wird Ihre Belegschaft umfassend geschützt – ganz gleich, wo Ihre Angestellten arbeiten.

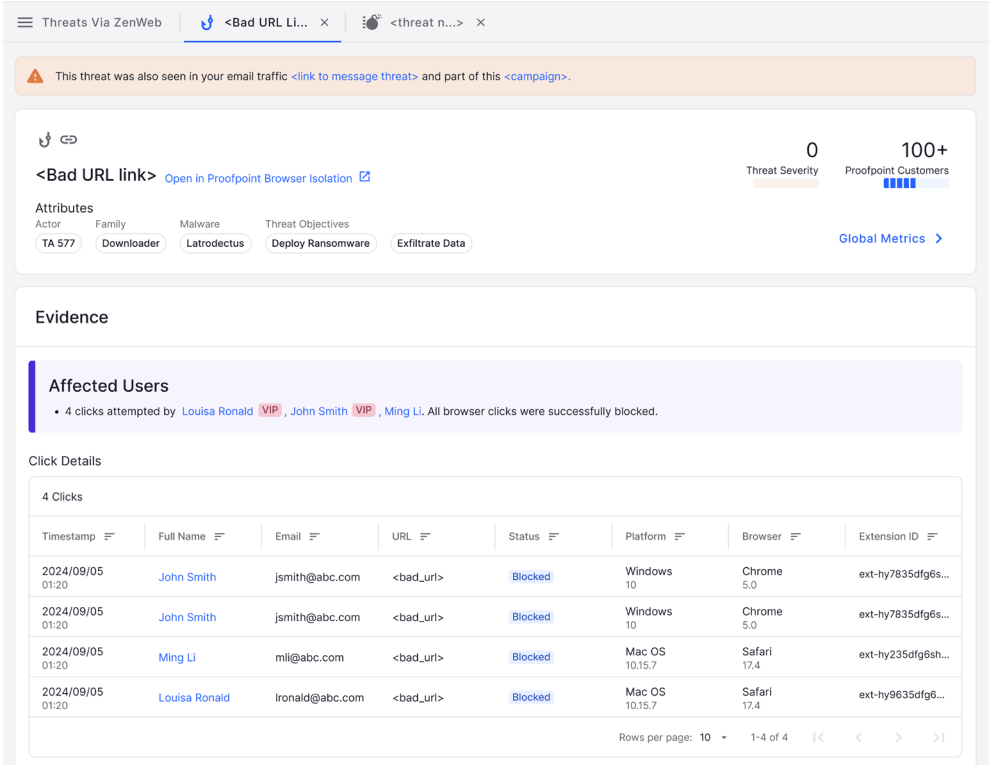


Abb. 1: Proofpoint erweitert den Phishing-Schutz auf Bereiche jenseits von E-Mails und blockiert auch schädliche URLs, die auf Collaboration- und Messaging-Plattformen geteilt werden.

Schutz vor mehrstufigen Angriffen

Angreifer setzen auf eine große Bandbreite an Taktiken wie Phishing, Brute-Force-Angriffe, Sitzungs-Hijacking und Social Engineering, um legitime Anwenderkonten zu übernehmen. Sobald ein Konto kompromittiert wurde, eskalieren Angreifer häufig Berechtigungen, greifen auf Ihre Daten zu und erlangen langfristige Persistenz. Dabei bietet auch Multifaktor-Authentifizierung (MFA) keinen zuverlässigen Schutz vor Kontoübernahmen.

Proofpoint Prime schützt vor Kontoübernahmen, die MFA umgehen, und bietet Sicherheitsteams die Möglichkeit, kompromittierte Konten auf gängigen Plattformen wie Microsoft 365, Google Workspace und Okta schnell zu erkennen, zu untersuchen und zu beheben.

Sie erhalten einen zentralen Überblick über die Aktivitäten von Angreifern nach einer Kompromittierung. Proofpoint Prime unterstützt zudem eine Vielzahl von automatisierten Reaktionen. Dabei können Teams wählen, ob kompromittierte Konten automatisch zurückgesetzt, Kennwortrücksetzungen durchgesetzt, nicht autorisierte Änderungen rückgängig gemacht oder verdächtige Drittanbieter-Anwendungen entfernt werden sollen.

Außerdem erhalten Sie Schutz vor mehrstufigen Angriffen von Cyberkriminellen, die kompromittierte Lieferantenkonten verwenden. Proofpoint Prime erkennt potenziell kompromittierte Drittanbieterkonten im gesamten Proofpoint-Ökosystem und warnt Ihr Sicherheitsteam entsprechend. Die Lösung unterstützt Ihr Team bei der Implementierung adaptiver Sicherheitskontrollen wie URL-Isolierung und Warnhinweisen in E-Mails, wobei legitime Nachrichten nicht beeinträchtigt werden.

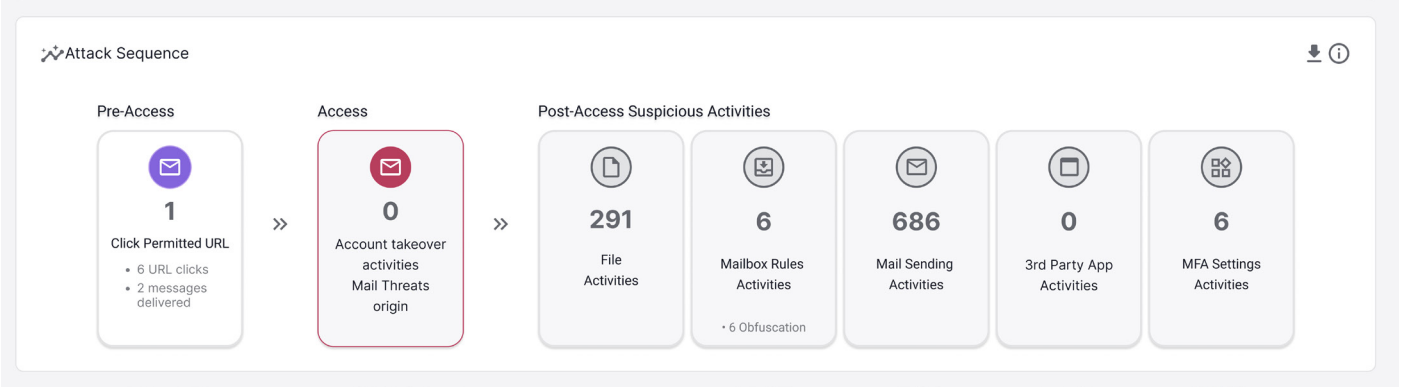


Abb. 2: Proofpoint Prime gibt Aufschluss über schädliche Aktionen an betroffenen Konten vor und nach dem Zugriff.

Schutz für Ihre vertrauenswürdige Geschäftskommunikation

Angreifer nutzen häufig Nachahmungstechniken, um sich in laufende geschäftliche Unterhaltungen zu hacken. 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 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. Dazu sucht die Lösung im Internet dynamisch nach Domains, die Ihrer eigenen Domain stark ähneln. Außerdem erhalten Sie detaillierte Erkenntnisse zu den Registrierungsdaten sowie zu potenziellem Missbrauch. 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.

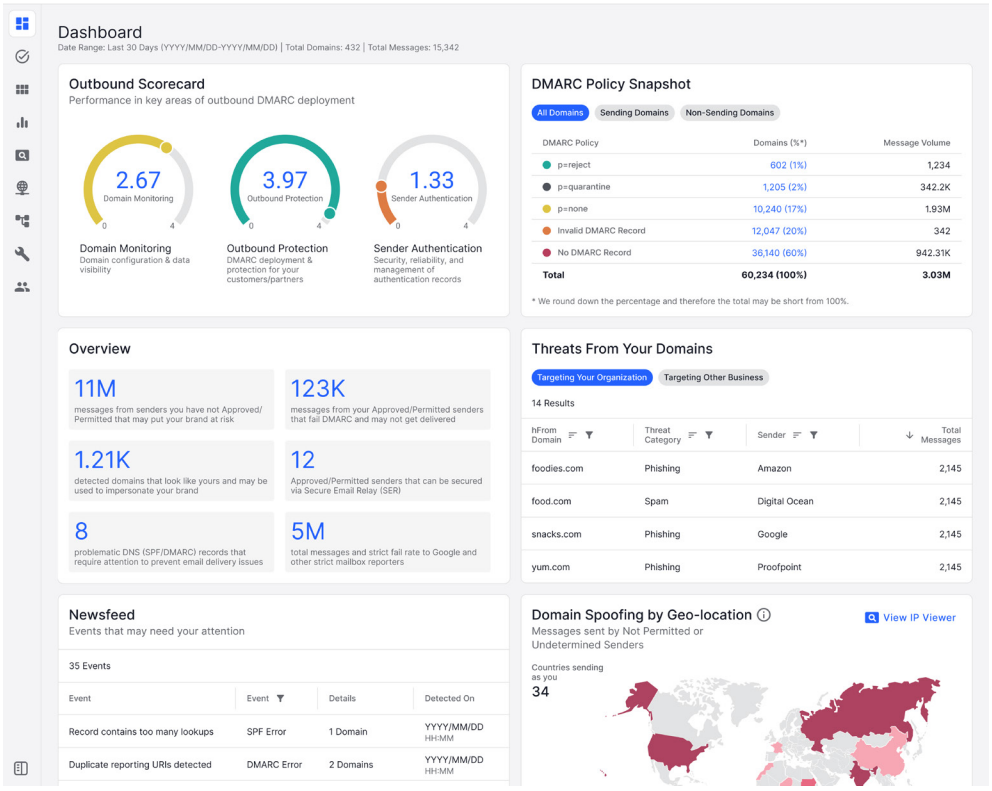


Abb. 3: Proofpoint Prime bietet Ihnen einen Überblick über Domain-Spoofing-Bedrohungen, über schädliche Doppelgänger Ihrer Domains und über E-Mails, die von Ihren vertrauenswürdigen Domains versendet werden.

Mehr Resilienz durch risikobezogene Empfehlungen und Erkenntnisse

Cyberangriffe richten sich gegen Menschen, und jährliche Sicherheitsschulungen sind absolut nicht ausreichend, um Ihre Gesamtsicherheit zu verbessern.

Mit Proofpoint Prime erhalten Sie Einblicke zu personenbezogenen Risiken sowie Empfehlungen, die relevante Verhaltensänderungen fördern und die Resilienz Ihrer Mitarbeiter langfristig stärken. Die dabei verwendeten adaptiven, risikobasierten Schulungsinhalte sind deutlich effektiver als die klassischen Universalansätze.

Durch die Aggregation von Erkenntnissen aus dem gesamten Proofpoint-Ökosystem hilft Proofpoint Prime Unternehmen bei der Bewertung personenbezogener Risiken sowie bei der Identifizierung besonders gefährdeter Personen. Mit der Pfade-Funktion (Pathways) für adaptives Lernen können Sicherheitsteams riskanten Anwendern automatisch maßgeschneiderte Lernerfahrungen zuweisen. Die Zuweisung kann dabei basierend auf Verhaltensweisen, Bedrohungsgefährdung, Rollen, Sicherheitskenntnissen und Berechtigungen erfolgen. Einer besonders häufig angegriffenen Person (Very Attacked Person, VAP) können zum Beispiel automatisch gezielte Aktionen wie Schulungseinheiten, Benachrichtigungen oder Phishing-Simulationen zugewiesen werden – je nachdem, durch welche Art von Bedrohung sie gefährdet ist. Dadurch können Sicherheitsteams relevantere bedrohungsbezogene Inhalte bereitstellen, effektivere Interaktionen priorisieren und Maßnahmen zur Förderung von Verhaltensänderungen effizienter für das gesamte Unternehmen skalieren.

Durch die Steigerung der Resilienz Ihrer Mitarbeiter reduzieren Sie das allgemeine Risiko und Ihre Belegschaft wird eine wichtige Verteidigungslinie zum Schutz vor dynamischen Bedrohungen. Mit Proofpoint Prime können Sie die Auswirkungen Ihres Programms zur Stärkung der Mitarbeiter-resilienz messen und genau feststellen, wie stark das personenbezogene Risiko reduziert wurde. Mit diesen Daten können Sie die Effektivität Ihres Programms nachweisen, sodass Sie leichter kontinuierliche Unterstützung durch Ihre Unternehmens-führung und Stakeholder erhalten.

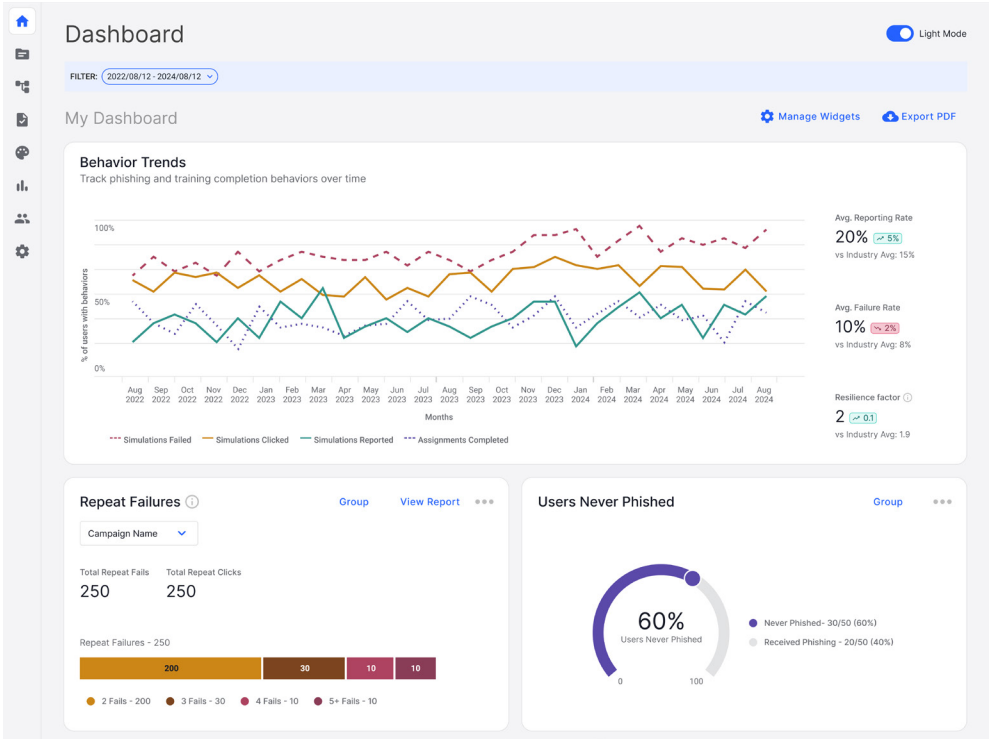
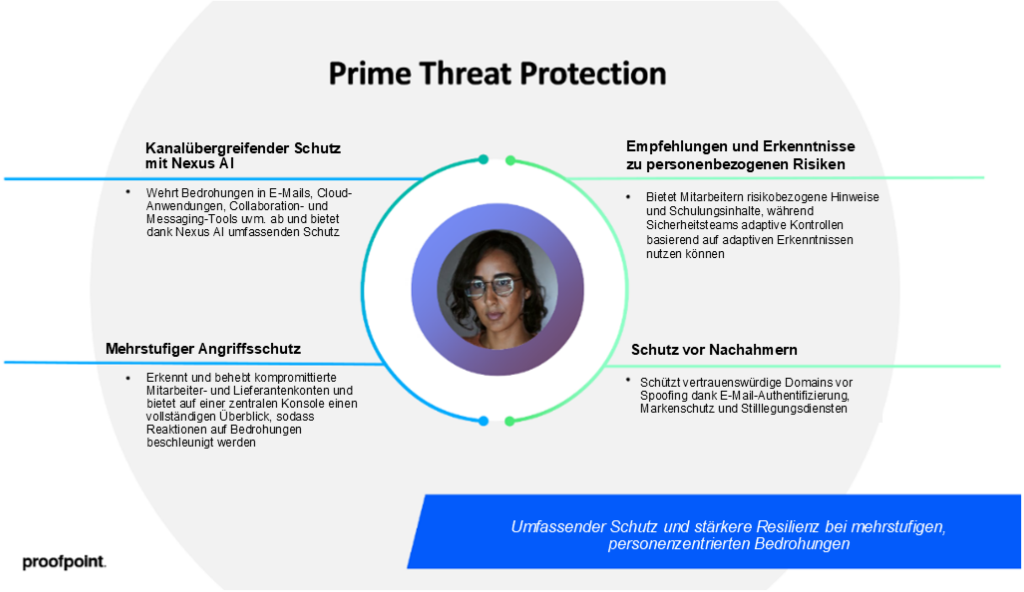


Abb. 4: Proofpoint Prime nutzt die weltweiten Bedrohungsdaten von Proofpoint, sodass Sie Einblicke in die hochdynamische Bedrohungslandschaft erhalten. Sie können Ihre Anwender zu neuen Bedrohungen schulen und parallel Verhaltenstrends im Zeitverlauf erfassen.

Die Vorteile integrierter Schutzmaßnahmen

Die Absicherung digitaler Arbeitsbereiche vor Cyberbedrohungen wird immer schwieriger. Bei einem Flickenteppich aus Einzellösungen bleiben Lücken in den Schutzmaßnahmen, sodass zahlreiche Risiken unbehandelt bleiben. Zudem gibt es Probleme bei der Integration, die Verwaltung ist äußerst komplex und die Lizenz- und Betriebskosten sind hoch.

Proofpoint Prime löst diese Probleme mit einem umfassenden Schutzansatz, der Sicherheitslücken schließt und die Komplexität reduziert, die durch fragmentierte, isolierte Lösungen entstehen. Mit unserer integrierten Bedrohungsschutzlösung können Ihre Sicherheitsteams schneller und effektiver agieren, da ihnen automatisierte Workflows, umfassende Bedrohungsdaten und vorkonfigurierte Integrationen zur Verfügung stehen. Außerdem bietet Proofpoint Prime Lizenzierungsvorteile, die die Betriebskosten senken und die Rendite steigern. Das Beste dabei: Gleichzeitig erhalten Sie einen branchenführenden, vertrauenswürdigen Partner, auf den Sie sich verlassen können.



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: X | LinkedIn | Facebook | YouTube

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →