Proofpoint Advanced Email Security

Schutz vor raffinierten E-Mail-Bedrohungen, optimierte Sicherheitsabläufe und verwertbare Einblicke in personenbezogene Risiken und die Bedrohungslandschaft

Produkte

- Proofpoint Email Protection
- Proofpoint TAP
- Proofpoint TRAP
- Proofpoint Email Isolation
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Email Fraud Defense
- Proofpoint Internal Mail Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

Wichtige Vorteile

- Blockierung von Bedrohungen, die schädliche URLs, Anhänge und Ransomware enthalten oder E-Mail-Betrugsversuche sind
- Automatische Entfernung von Nachrichten, die von Anwendern gemeldet oder nach Auslieferung aktiviert wurden, mittels integrierter Workflows
- Einzigartiger Überblick über Ihre Mitarbeiter, Bedrohungen sowie andere Einblicke wie Lieferanten- und Cloud-Risiken
- Einfache Bereitstellung von DMARC-Richtlinien sowie schnelle und zuverlässige Authentifizierung, um betrügerische E-Mails zu blockieren, die vertrauenswürdige Domänen missbrauchen
- Schulung und Unterstützung Ihrer Anwender, damit sie zu einer starken Verteidigungslinie gegen Cybersicherheitsbedrohungen werden

E-Mails sind für moderne Unternehmen unverzichtbar, gleichzeitig jedoch auch der Bedrohungsvektor Nr. 1. Zudem entwickeln sich E-Mail-Angriffe – von Phishing-Angriffen über Business Email Compromise (BEC), Lieferkettenangriffen bis hin zu Ransomware- und Cloud-Kontenkompromittierungen – ständig weiter. Es fällt daher selbst großen und gut ausgestatteten IT-Abteilungen äußerst schwer, diesen Vektor effektiv vor Bedrohungen zu schützen. Proofpoint kann Ihnen helfen.

Bei der Abwehr dieser Bedrohungen vertrauen mehr Unternehmen in den Fortune 100, Fortune 1000 und Global 2000 auf Proofpoint als auf jeden anderen E-Mail-Sicherheitsanbieter. Unsere Lösung nutzt einen Inline- und API-Ansatz, um vollständigen Schutz für alle ein- und ausgehenden Nachrichten zu gewährleisten. Dabei konzentriert sich die Lösung nicht allein auf E-Mails, die von herkömmlichen Sicherheitslösungen übersehen werden. Der integrierte mehrstufige Ansatz minimiert das Risiko eines erfolgreichen Angriffs, indem Bedrohungen schnell und zuverlässig erkannt werden. Dank der führenden Erkennungsfunktionen und einer skalierbaren Plattform wird die operative Effektivität verbessert. Mit verwertbaren Erkenntnissen können Sie die bestehenden Risiken besser verstehen und schneller sowie effektiver reagieren.

Erkennung und Abwehr hochentwickelter Bedrohungen

Vertrauenswürdige Effektivität

Mit den Bedrohungsdaten und Erkennungsfunktionen von Proofpoint verfügen Sie über eine zuverlässige Abwehr gegen hochentwickelte Bedrohungen – bei einer äußerst geringen Anzahl an False Positives.

Um Schaddaten (z. B. solche, die sich in Anhängen oder URLs verstecken) zu erkennen, nutzen wir Reputation, URL-Veränderung sowie prädiktive Sandbox-URL-Analysen zum Klickzeitpunkt. Die Erkennung von Umgehungs- und Verschleierungstaktiken wie CAPTCHA, Kennwortschutz, ressourcenintensive Websites, Umleitungen sowie File-Sharing-Websites ist integriert.

Zudem nutzen wir Modelle für künstliche Intelligenz (KI) und Machine Learning (ML) aus dem Nexus Threat Graph, die Bedrohungen ohne Schaddaten (z. B. BEC) erkennen. Die KI/ML-Modelle bewerten Signale wie Lieferantenrisiken, Anwendersignale aus Collaboration-Tools, Inhalte aus verarbeiteter natürlicher Sprache, Empfängerbeziehungen und Absichten. Anhand von Ausgangswerten und Kontextinformationen können wir schnell schädliche E-Mails erkennen.

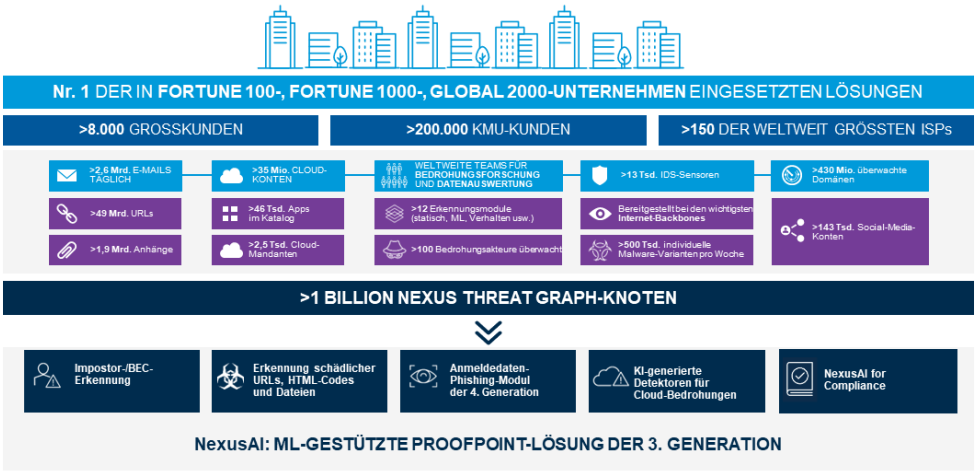

Abb. 1: Nexus Threat Graph.

In Anbetracht der aktuellen personenzentrierten Bedrohungslandschaft sind Ihre Anwender Ihr größtes Kapital, aber auch Ihr größtes Risiko.

Die Modelle arbeiten nahtlos mit unseren Bedrohungsdaten sowie anderen gezielten Erkennungsmodulen zusammen, um False Positives zu minimieren.

Wir untersuchen E-Mails mit mehrstufiger inhaltlicher Analyse sowie mit Reputations- und Sandbox-Analysen. Dadurch können wir hochentwickelte E-Mail-Bedrohungen (einschließlich polymorpher Malware und Ransomware) effektiv stoppen, bevor sie Ihre Anwender erreichen. Zudem nutzen wir die Sandbox für prädiktive URL-Analysen zum Klickzeitpunkt, um schädliche URLs zuverlässig zu erkennen und zu blockieren. Durch das Umschreiben von URLs werden Ihre Anwender in jedem Netzwerk und an jedem Gerät geschützt. Gleichzeitig schützt das vor Nachrichten, die nach der Zustellung manipuliert werden.

Sichere Klicks dank Email Isolation und Browser Isolation

Mit Proofpoint Browser Isolation und Proofpoint Email Isolation erhalten Sie eine sichere Umgebung, in der Ihre Anwender auf Websites sowie auf private und geschäftliche E-Mails zugreifen können. Angreifer versuchen über verschiedene Taktiken und Bedrohungsvektoren (z. B. durch Kompromittierung von Lieferantenkonten) Zugang zu Ihren Systemen zu erlangen. Sie können Ihre Anwender beispielsweise über private E-Mails oder über ungeschützte Kanäle ins Visier nehmen. Mithilfe der Isolierungsfunktionen können Sie Uploads und Downloads deaktivieren und die Dateneingabe so lange beschränken, bis die Website vollständig analysiert wurde (was meist nur wenige Minuten dauert). Diese Technologie bietet zusätzlichen Schutz vor Anmeldedaten-Diebstahl, Malware und Ransomware und schützt insbesondere vor solchen Phishing-E-Mails, deren URLs erst nach der Zustellung in den Posteingang des Adressaten „scharf geschaltet“ werden.

Verhinderung von E-Mail-Betrug dank E-Mail-Authentifizierung

E-Mail-Authentifizierung fügt eine zusätzliche Schutzebene hinzu, mit der sich Malware-lose Impostor-Bedrohungen wie BEC zuverlässig stoppen lassen. Allerdings zögern viele Unternehmen, DMARC-Standards einzuführen und durchzusetzen, da dadurch legitime E-Mails blockiert werden könnten.

Proofpoint unterstützt Sie bei der vollständigen Bereitstellung und Durchsetzung von DMARC und stellt sicher, dass der legitime E-Mail-Verkehr nicht unterbrochen wird. Unsere Lösung verhindert Domänen-Spoofing und den Versand betrügerischer E-Mails über Ihre vertrauenswürdigen Domänen. Betrügerische E-Mails werden am Proofpoint-Gateway gestoppt und die E-Mail-Identität Ihres Unternehmens geschützt. Zudem sehen Sie in einem zentralen Portal eine Übersicht aller Impostor-Bedrohungen, einschließlich schädlicher Doppelgänger Ihrer Domänen. Diese Übersicht steht Ihnen unabhängig davon zur Verfügung, welche Taktik angewendet und welcher Mitarbeiter angegriffen wird. Mit unserem Virtual Takedown-Service können Sie E-Mail-Angriffe über betrügerische Doppelgänger-Domänen proaktiv verhindern. Unsere Berater unterstützen Sie in jeder Phase der DMARC-Implementierung. Wir arbeiten mit Ihnen zusammen,

um alle vertrauenswürdigen E-Mail-Versender, die unter Verwendung Ihrer Domänen E-Mails versenden (dazu zählen auch externe Dienstleister), zu identifizieren, sodass diese alle ausgehenden E-Mails zuverlässig authentifizieren. Proofpoint hat bereits mehr als einem Drittel der Fortune 1000-Unternehmen durch diesen Prozess begleitet und ist in der Lage, mit äußerst komplexen Konfigurationen zu arbeiten.

Schutz für interne E-Mails und schnelle Eindämmung von Bedrohungen

Interne E-Mails müssen ebenso sorgfältig geschützt werden wie eingehende Nachrichten. Angreifer nutzen kompromittierte Konten zum Versenden von Phishing, BEC oder Malware. Wir analysieren interne E-Mails auf schädliche URLs und Anhänge. Wenn schädliche interne E-Mails gefunden werden, können Sie diese unerwünschten Nachrichten automatisch unter Quarantäne stellen oder löschen, selbst wenn sie von anderen Anwendern empfangen und weitergeleitet wurden. Sie erhalten außerdem Berichte mit genauen Angaben dazu, welche Konten möglicherweise kompromittiert wurden, sodass Sie schnell gezielte Maßnahmen ergreifen können.

Einzigartige Transparenz zu Angriffen und zur menschlichen Angriffsfläche

Damit Sie Risiken besser beheben und gegenüber Ihren Führungskräften kommunizieren können, benötigen Sie folgende Informationen:

- Welche Anwender besonders gefährdet sind und wie sie angegriffen werden
- Einblicke in die Bedrohungslandschaft, Zielsetzungen, Akteure und Trends
- Andere Signale wie Erkenntnisse zu Lieferanten- und Cloud-Risiken

Proofpoint bietet Ihnen diese Informationen und noch sehr viel mehr. Durch unsere Plattform erhalten Sie zudem einen umfassenden Überblick über personenzentrierte Risiken – ohne Daten-Silos. Wir ermöglichen Ihnen, proaktiv gegen hochentwickelte Bedrohungen vorzugehen.

Minimierung von Risiken durch personenzentrierte Einblicke

In Anbetracht der aktuellen personenzentrierten Bedrohungslandschaft sind Ihre Anwender Ihr größtes Kapital, aber auch Ihr größtes Risiko. Wir bieten Ihnen einen einzigartigen Überblick über gezielte Angriffe und die menschliche Angriffsfläche und zeigen Ihnen, wer das größte Risiko für Ihr Unternehmen darstellt und warum.

In unserem Bericht zu besonders häufig angegriffenen Personen (Very Attacked People™, VAP) sehen Sie, welche Anwender am häufigsten angegriffen werden. Der Top Clicker-Bericht zeigt Ihnen zudem, welche Anwender auf echte schädliche Nachrichten geklickt haben. VIPs lassen sich auf dem Dashboard eintragen und nachverfolgen. Mit diesen Erkenntnissen können Sie Risiken priorisieren und mithilfe adaptiver Kontrollen für die gefährdeten Anwender minimieren. Zu diesen Kontrollen gehören unter anderem gezielte Schulungen, Browser-Isolierung und Multifaktor-Authentifizierung.

Bedrohungsbezogene Erkenntnisse für mehr Kontext

Wir bieten in Echtzeit forensische Informationen zu einzelnen Bedrohungen sowie zu Kampagnen. Unsere tiefgehenden Bedrohungsanalysen zeigen auf, wer angegriffen wird, woher der Angriff stammt und wie der Angriff aussah. Wir stellen außerdem das Ziel des Angriffs fest. (Wir können beispielsweise sagen, ob er dazu dienen sollte, Daten zu exfiltrieren, Ransomware zu installieren oder Betrug zu begehen.) Wir stellen Verbindungen zwischen E-Mail-Angriffen und verdächtigen Anmeldungen her, sodass sich Kontenkompromittierungen effektiver aufdecken und stoppen lassen. Zudem erhalten Sie über die Plattform umfassende Benchmark-Analysen der für Ihr Unternehmen relevanten Arten von Bedrohungen und Zielen im Vergleich zu Ihren Branchenkollegen.

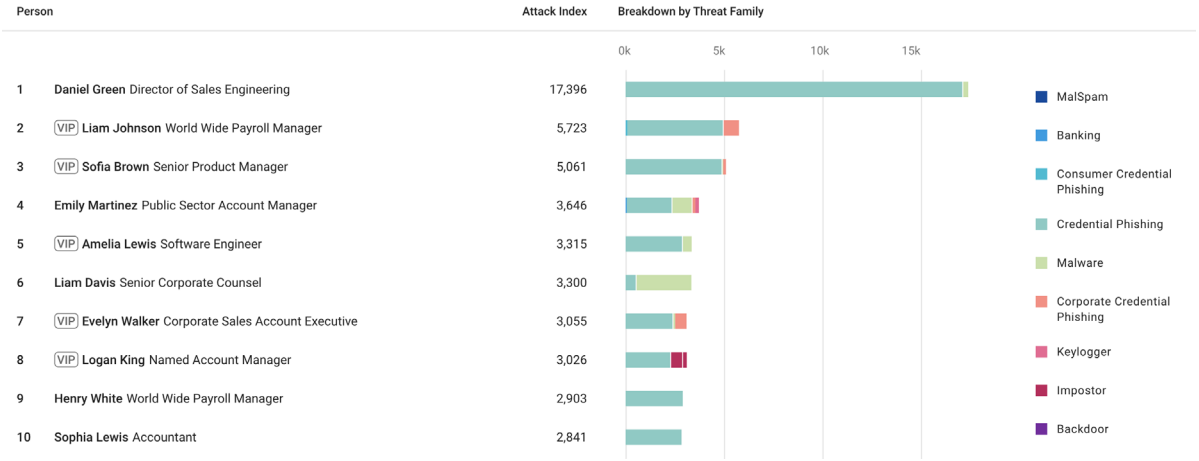

Abb. 2: Der Proofpoint-Bericht zu besonders häufig angegriffenen Personen (Very Attacked People, VAP) zeigt die am häufigsten angegriffenen Anwender sowie die jeweiligen Bedrohungsarten.

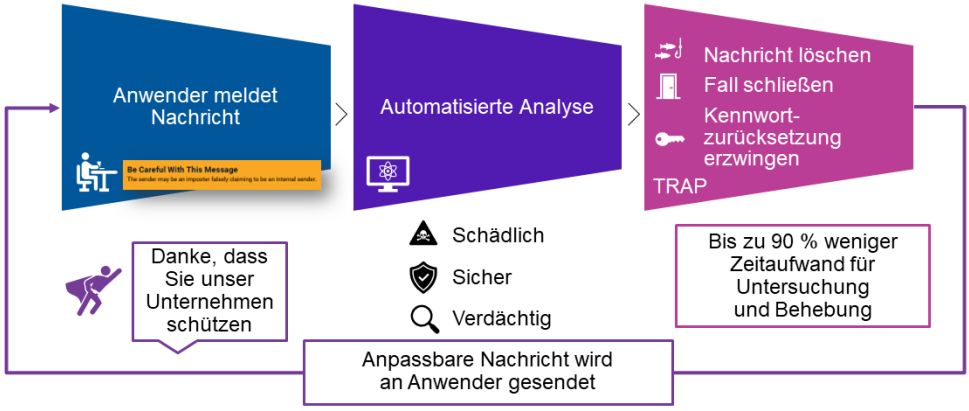

Abb. 3: Die automatisierte Proofpoint-Lösung für Abuse-Postfächer CLEAR (Closed-Loop Email Analysis and Response).

Integrierte Erkenntnisse zu Lieferanten- und Cloud-Risiken

Proofpoint bietet Ihnen einen Überblick über Kompromittierungs- und Lieferantenrisiken, sodass Sie komplexe Attacken über diese Angriffsvektoren zuverlässig eindämmen können. Mit Nexus Supplier Risk Explorer identifizieren wir automatisch potenziell kompromittierte Lieferanten und die Domänen, über die sie E-Mails an Ihre Anwender senden. Zudem steht Ihnen die Funktion SaaS Defense zur Verfügung, die Ihnen Einblicke zu potenziell kompromittierten Anwendern, schädlichen oder gefährdeten Dateien sowie riskanten Anwendungen von Drittanbietern bietet.

Verbesserte operative Effizienz

In vielen Unternehmen ist das Sicherheitsteam unterbesetzt oder überlastet. Häufig müssen die Teams mehrere, nicht miteinander kommunizierende Sicherheitsanbieter und -produkte verwalten. Wir bieten eine integrierte Lösung, die sich auf die relevanten Bedrohungen konzentriert und die Erkennung sowie Behebung von Bedrohungen automatisiert. Dadurch sparen Sie Zeit und Geld, denn Ihr Sicherheitsteam muss im Vergleich zur Nutzung parallel laufender Lösungen weniger interne Ressourcen zur Behebung aufwenden.

Automatisches Löschen schädlicher E-Mails

Mit unserer Lösung entfallen der manuelle Aufwand und das Rätselraten rund um die Reaktion auf Zwischenfälle, sodass Sie Bedrohungen schneller und effizienter beseitigen können. Wir entfernen Phishing-E-Mails mit URLs, die nach der Zustellung in den Posteingang „scharf geschaltet“ werden. Zudem können wir alle unerwünschten E-Mails mit einem Klick oder automatisch aus kompromittierten internen Konten entfernen, selbst wenn die Nachrichten weitergeleitet wurden oder andere Anwender sie bereits empfangen haben. Durch unseren Nexus Threat Graph werden Warnmeldungen um zusätzliche Informationen ergänzt und verschiedene forensische Daten automatisch korreliert und grafisch dargestellt, damit Sie eine aussagekräftige Bedrohungsübersicht erhalten. Auf diese Weise lässt sich die Behebungszeit für E-Mails um bis zu 90 % verringern.

Vereinfachte Abuse-Postfachprozesse

Wir helfen Ihnen, den Abuse-Postfachprozess zu vereinfachen und die Belastung für das IT-Team zu verringern. Anwender können verdächtige E-Mails ganz einfach mit einem Klick melden. Dies erfolgt entweder direkt über einen E-Mail-Warnhinweis oder über das PhishAlarm®-Add-in für E-Mail-Meldungen. Wird die Nachricht als schädlich erkannt, kann sie – einschließlich aller Kopien – automatisch unter Quarantäne gestellt werden. Ihre Endnutzer erhalten eine E-Mail mit der Information, dass die Nachricht als schädlich eingestuft wurde. Das fördert richtiges Verhalten und motiviert Ihre Mitarbeiter, ähnliche Nachrichten auch weiterhin zu melden. Administratoren erhalten detaillierte Berichte zum Anwenderverhalten und darüber, wie zuverlässig schädliche Nachrichten gemeldet werden (einschließlich Vergleich zu anderen Unternehmen).

Änderung des Anwenderverhaltens durch datengestützte Schulungen

Aktuelle Bedrohungen werden häufig erst durch einen Menschen aktiviert. Ihre Angestellten müssen nicht zwangsläufig eine Schwachstelle in Ihrem Sicherheitssystem sein. Tatsächlich können sicherheitsbewusste Mitarbeiter die letzte Verteidigungslinie gegen einen Cyberangriff bilden.

Mit Proofpoint können Sie Maßnahmen für Ihre VAPs oder Top Clicker ergreifen. Die über sie gesammelten Daten werden automatisch in unsere Security-Awareness-Plattform integriert, um ein gezielteres und wirkungsvolleres Schulungsprogramm zusammenzustellen. Sie können dabei auf reale Phishing-Simulationen basierend auf Proofpoint-Bedrohungsdaten zurückgreifen, die für ein praxisnahes und relevantes Schulungerlebnis sorgen. Anwender, die auf einen simulierten Angriff hereinfallen, erhalten sofort relevante Hinweise und können automatisch für bestimmte Schulungen angemeldet werden. Zudem erhalten Anwender E-Mail-Warnhinweise mit Meldungsoptionen. Diese enthalten kurze veränderbare Beschreibungen und Darstellungen der Risiken, die mit einer bestimmten E-Mail verbunden sind, und bieten die Möglichkeit, Nachrichten direkt über den Warnhinweis zu melden. Dadurch können Anwender informierte Entscheidungen treffen. Die Funktionen arbeiten nahtlos auf allen Geräten und Anwendungen.

Schutz vor Datenverlust per E-Mail

E-Mail ist der wichtigste Risikovektor für eingehende Bedrohungen und Datenverlust. Deshalb müssen vertrauliche Daten vor Exfiltration per E-Mail geschützt werden. Sie erhalten von Proofpoint Transparenz sowie Funktionen zur Durchsetzung von Richtlinien, damit absichtlicher und unbeabsichtigter Datenverlust bei der E-Mail-Kommunikation vermieden wird.

Die Funktionen für Datenverlustprävention (DLP) und E-Mail-Verschlüsselung sind eng integriert und lassen sich zentral in der Information and Cloud Security-Plattform verwalten. In der neuen einheitlichen Verwaltungsübersicht können Sie mitgelieferte Datenanalysen anpassen, um nach relevanten DLP-Verstößen zu suchen und diese zu melden. Dabei können Sie Ihre Abläufe mit optimierten Workflows und Behebungsfunktionen vereinfachen. Wir analysieren vertrauliche Informationen innerhalb von strukturierten und unstrukturierten Daten. Zudem stellen wir detailliert anpassbare Richtlinien sowie vorab konfigurierte Wörterbücher zur Verfügung, mit denen Sie automatisch Daten identifizieren können, die durch gesetzliche Compliance- und Datenschutzvorschriften geschützt sind. Dies vereinfacht die Einhaltung von Datenschutzgesetzen wie PCI DSS, SOX, HIPAA sowie DSGVO und verringert den manuellen Aufwand. Sie können individuelle Richtlinien festlegen, mit denen vertrauliche Daten in E-Mails automatisch verschlüsselt werden. Dadurch lässt sich der Austausch vertraulicher Daten einfacher verwalten und absichern.

Zusammenfassung

Mit Proofpoint Advanced Email Security erhalten Sie Schutz vor E-Mail-basierten Bedrohungen. Außerdem erhalten Sie einen verwertbaren Überblick über Angriffe und Ihre am häufigsten angegriffenen Mitarbeiter. Unsere Lösung bietet folgende Möglichkeiten:

- Blockierung raffinierter Bedrohungen, bevor diese den Posteingang erreichen
- Einzigartiger Überblick über personenbezogene Risiken, Bedrohungen und andere Einblicke
- Verbesserte operative Effizienz und automatisierte Reaktionen auf Bedrohungen
- Schulung und Unterstützung von Anwendern, damit sie eine effektive Verteidigungslinie bilden
- Schutz vor Datenverlust per E-Mail

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU 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 75 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**.

proofpoint.

0201-016-01-03 4/22