Proofpoint-Produkte

Proofpoint bietet Schutz und Transparenz für Ihre wichtigste Ressource und Ihr größtes Sicherheitsrisiko: Ihre Mitarbeiter. Wir bieten effektive Tools zum Schutz vor Bedrohungen, die auf Ihre Anwender abzielen, zur Absicherung von Informationen, die diese erstellen und abrufen, sowie zum Schutz der Anwender selbst.

Unsere Lösungen für Cybersicherheit und Compliance umfassen den Schutz für E-Mails, soziale Medien, das Web, Netzwerke und Cloud-Plattformen (einschließlich Microsoft Office 365). Zudem bieten wir strategische Technologie-Integrationen mit den branchenweit besten Sicherheitsanbietern. Dadurch können Sie Ihre Mitarbeiter, Daten und Ihre Reputation besser schützen.

SCHUTZ VOR E-MAIL-BEDROHUNGEN

Schutz vor E-Mail-Bedrohungen, Gewährleistung kontinuierlicher E-Mail-Verfügbarkeit und Implementierung von Richtlinien für ein- und ausgehende E-Mails

Email Protection

Proofpoint Email Protection schützt Anwender vor unerwünschten und schädlichen E-Mails, unabhängig davon, ob sie Malware enthalten oder Malware-lose Bedrohungen darstellen. Zu letzterer Kategorie zählen Betrugsmails, die von Accounts, deren Anmeldedaten gestohlen wurden, verschickt werden, sowie Business Email Compromise (BEC). Wir bieten einen detaillierten Überblick und gewährleisten den störungsfreien Geschäftsbetrieb für Unternehmen aller Größen. Durch die Kontrolle über alle Aspekte ein- und ausgehender E-Mails sowie die Einrichtung von Richtlinien unterstützen wir Ihr IT- und Sicherheitsteam beim Schutz Ihrer Anwender vor E-Mail-Bedrohungen und gewährleisten die E-Mail-Kommunikation auch bei einem Systemausfall.

Email Fraud Defense (EFD)

Proofpoint Email Fraud Defense (EFD) schützt Ihre Mitarbeiter, Kunden und Geschäftspartner vor allen Formen von E-Mail-Betrug, indem E-Mails mit gefälschter Identität gestoppt werden, bevor sie den Posteingang erreichen. In einem zentralen Portal können Sie legitime E-Mails autorisieren, betrügerische Nachrichten blockieren und alle E-Mail-Betrugsversuche sehen – ganz gleich, welche Taktik angewendet und welcher Mitarbeiter angegriffen wird. Durch E-Mail-Authentifizierung, Machine Learning und Richtlinien sowie DMARC-Authentifizierung erlaubt EFD das Blockieren aller Betrugstaktiken, die Kriminelle für ihre raffinierten Angriffe einsetzen.

Threat Response Auto-Pull (TRAP)

Proofpoint Threat Response Auto-Pull (TRAP) nutzt Funktionen zur Koordinierung und Automatisierung, um schädliche E-Mails zurückzuziehen, die bereits an Postfächer der Anwender gesendet wurden. Diese grundlegende Threat Response-Lösung identifiziert und entfernt schädliche E-Mails basierend auf TAP-Warnmeldungen und wendet anschließend Geschäftslogik an, um den Weg der E-Mails zu größeren Empfängergruppen aufzudecken und auch diese Nachrichten zu entfernen. TRAP generiert außerdem Berichte zu Quarantäneversuchen, Erfolgen/Fehlern sowie zu den Anwendern, die am häufigsten angegriffen werden. Dadurch wird Ihr Sicherheitsteam deutlich entlastet.

Internal Mail Defense

Proofpoint Internal Mail Defense bietet zuverlässigen, mehrstufigen Schutz, der die unternehmensinternen E-Mails absichert und die Erkennung kompromittierter Konten vereinfacht. Die Lösung überprüft alle internen E-Mails auf Spam, schädliche Anhänge und gefährliche URLs. Wenn eine intern gesendete E-Mail gekennzeichnet wird, kann sie automatisch entfernt und isoliert werden. Außerdem erhält Ihr Sicherheitsteam einen Überblick über die Konten, von denen die schädlichen E-Mails gesendet wurden, um potenziell kompromittierte Konten schnell zu identifizieren und Maßnahmen zu ergreifen.

Essentials für KMUs

Proofpoint Essentials macht die Funktionen von Proofpoint Email Protection für kleine Unternehmen verfügbar. Die Lösung bietet Spam-Filterung, erkennt Phishing, verfügt über mehrstufigen Virenschutz, dynamische Sandbox-Analysen von URLs, eine zuverlässige Filterregel-Engine, kontinuierliche E-Mail-Verfügbarkeit, per Richtlinie erzwungene Verschlüsselung, E-Mail-Archivierung sowie Schutz von Social-Media-Konten. Der größte Vorteil ist jedoch, dass Proofpoint Essentials über eine einfache und intuitive Benutzeroberfläche verwaltet wird. Dies erleichtert KMUs, die häufig über kleine Sicherheitsteams verfügen, die Verwaltung.

SCHUTZ VOR HOCHENTWICKELTEN BEDROHUNGEN

Schnellere, präzisere und zuverlässigere Erkennung, Untersuchung und Behebung von Bedrohungen

Targeted Attack Protection (TAP)

Proofpoint Targeted Attack Protection (TAP) unterstützt die Erkennung, Beseitigung und Blockierung hochentwickelter Bedrohungen mit schädlichen Anhängen und URLs, mit denen Mitarbeiter über E-Mail und Cloudanwendungen wie Microsoft Office 365 und Google G Suite angegriffen werden. Dank TAP erhalten Sie eine Übersicht der besonders häufig angegriffenen Personen (Very Attacked People, VAPs) in Ihrem Unternehmen. Ebenso bietet die Lösung die Möglichkeit, alle eingebetteten URLs zu ändern, um Ihre Anwender auf jedem Gerät zu schützen und Klicks auf schädliche Links zu erfassen.

Email Isolation

Mit Proofpoint Email Isolation können Ihre IT- und Sicherheitsteams den Zugriff von Anwendern auf ihre privaten Webmails über Unternehmensgeräte gestatten, ohne dass dem Sicherheitsbedenken entgegenstehen. Die Lösung kann mit TAP integriert werden und stellt dann eine zusätzliche Sicherheitsebene für Ihre VAPs bereit, sodass alle Anwender vor unbekannten oder riskanten Websites geschützt sind, da Malware oder schädliche Inhalte den Anwender oder das Gerät nicht beeinträchtigen können. Unser Cloud-Dienst trennt Webinhalte von Unternehmensdaten und -netzwerken. Er erleichtert die Risikominimierung sowie die Senkung der Betriebskosten und verbessert gleichzeitig Ihre Sicherheitslage.

Browser Isolation

Proofpoint Browser Isolation erweitert den Funktionsumfang von Proofpoint Email Isolation auf den Schutz der gesamten Webnutzung aller Endnutzer (einschließlich Ihrer VAPs). Die Lösung stellt einen Dienst zur sicheren und anonymen Webnutzung bereit, der einfach implementiert, verwaltet und unterstützt werden kann. Dadurch erhalten Ihre Anwender die gewünschte Privatsphäre, wenn sie auf Websites wie Webmail zugreifen – ohne zusätzliche Risiken für Ihr Unternehmen.

Threat Response

Proofpoint Threat Response wurde für Sicherheitsteams konzipiert, die ein hohes Sicherheitsniveau erreichen möchten. Mit dieser Lösung erhalten Sie eine aussagekräftige Übersicht der Netzwerkbedrohungen, auf deren Basis Sie direkt handeln können. Warnungen lassen sich erweitern und die Erfassung sowie der Vergleich von Forensikdaten können automatisiert werden. Dank dieser Lösung entfallen zudem der manuelle Aufwand und das Rätselraten rund um die Reaktion auf Zwischenfälle, sodass Ihr Sicherheitsteam Bedrohungen schneller und effizienter beseitigen kann. Im Gegensatz zu herkömmlichen Vorfallreaktionstools kann Threat Response automatisch Malware-Infektionen bestätigen, nach Hinweisen auf frühere Infektionen suchen und Sicherheitswarnungen durch automatisches Hinzufügen interner und externer Kontextinformationen optimieren.

Emerging Threats Intelligence

Proofpoint Emerging Threats Intelligence (ET) bietet 100-prozentig überprüfte Bedrohungsdaten von einer der weltweit größten Malware-Börsen. Außerdem integriert sich die Lösung nahtlos mit anderen Sicherheitstools, sodass Sie den historischen Kontext (Ursprung und Akteurs hinter einer Bedrohung) besser verstehen können. Im Gegensatz zu anderen Datenquellen, die nur Informationen zu Domänen oder IP-Adressen liefern, umfasst unsere Lösung neben einer Verlaufsübersicht über zehn Jahre und beweisfähigen Informationen auch mehr als 40 Bedrohungskategorien sowie damit in Zusammenhang stehende IP-Adressen, Domänen und Exemplare.

Emerging Threats Pro Ruleset

Proofpoint Emerging Threats (ET) Pro Ruleset bietet einen Regelsatz, mit dem Ihre vorhandenen Netzwerksicherheits-Appliances – einschließlich Firewalls der nächsten Generation sowie Netzwerk-IDS/IPS – Bedrohungen nicht nur schnell, sondern auch zuverlässig erkennen und blockieren können. ET Pro Ruleset wird täglich in den Formaten Suricata und SNORT aktualisiert und umfasst mehr als 40 unterschiedliche Kategorien, einschließlich Netzwerkverhalten, Befehls- und Steuerungskommunikation von Malware, DoS-Angriffe, Botnets, Exploits, Schwachstellen, SCADA-Netzwerkprotokolle, Exploit-Kit-Aktivitäten und vieles mehr. Dank der täglichen Aktualisierungen und der automatisierten Sandbox-Umgebung kann sich Ihr Sicherheitsteam darauf verlassen, dass alle Bedrohungen korrekt bewertet werden.

Premium Threat Information Service (PTIS)

Mit Proofpoint Premium Threat Information Service (PTIS) können Sie Sicherheitsentscheidungen basierend auf einem umfassenderen Verständnis der aktuellen Bedrohungslandschaft priorisieren. Die drei PTIS-Komponenten bieten direkten Zugang zu unserem branchenführenden Threat Research Team, monatliche individuelle Bedrohungsberichte sowie dank der Nutzung neuester Analystenerkenntnisse erweiterte Warnungen vor neuen Bedrohungen. Dieser Service unterstützt Ihre wertvollen Sicherheitsanalysten tagtäglich, da manuelle Prozesse vermieden werden und sie sich daher auf die schwerwiegendsten Probleme konzentrieren können.

SECURITY AWARENESS-TRAINING

Machen Sie Ihre Endnutzer zu einer starken letzten Verteidigungslinie gegen Phishing und andere Cyberangriffe, die Bedrohungen zuverlässig erkennt und meldet.

Anti-Phishing Suite

Mit der Proofpoint Anti-Phishing Suite können Sie die Anfälligkeit Ihrer Mitarbeiter für Phishing-Angriffe und Malware-Infektionen ermitteln und um bis zu 90 Prozent verringern. Wenn Anwender auf einen simulierten ThreatSim-Phishing-Angriff hereinfallen, erhalten sie einen Hinweis inklusive wertvoller Tipps dazu, wie sie sich in Zukunft verhalten sollten. Ihre Anwender können automatisch für eines von acht Anti-Phishing-Schulungsmodulen angemeldet werden.

Alternativ lassen sich die Module individuell zuweisen. Dieses Paket bietet Administratoren Zugriff auf unsere PhishAlarm®-Schaltfläche, damit Anwender vermutete potenzielle Phishing-E-Mails mit nur einem Klick melden können, sowie zum E-Mail-Analysetool PhishAlarm Analyzer. Diese Tools sind Bestandteil unserer Lösung Closed Loop Email Analysis and Response (CLEAR), die die Meldung schädlicher E-Mails vereinfacht und automatisierte Reaktionen auf aktive Phishing-Angriffe ermöglicht.

Security Awareness-Training: Enterprise

Das Enterprise-Paket des Proofpoint Security Awareness-Trainings umfasst zusätzlich zur Anti-Phishing Suite noch ThreatSim-USB-Simulationen, CyberStrength®-Wissenstests, unsere gesamte Bibliothek der verschiedensten Schulungsmodule sowie alle unsere Materialien zur Steigerung des Sicherheitsbewusstseins (einschließlich Videos). Dieses Paket ist speziell für Kunden gedacht, die das effektivste und umfassendste Schulungsprogramm zur Steigerung des Sicherheitsbewusstseins selbst verwalten möchten. Dank Zugriff auf weitere Tools zur Identifizierung von Risiken, Änderung des Anwenderverhaltens und Verringerung der Anfälligkeit ist Ihre personenorientierte Sicherheitsstrategie mit diesem Paket noch erfolgreicher.

CLOUD-APP-SICHERHEIT

Schutz Ihrer Mitarbeiter und Daten vor Bedrohungen, Datenverlust und Compliance-Risiken in Cloudanwendungen

Cloud Account Defense (CAD)

Proofpoint Cloud Account Defense (CAD) bietet automatisierten Schutz vor Kontenkompromittierung und schädlichen Dateien in Office 365 und G Suite. Eine Kontenkompromittierung beginnt üblicherweise mit Phishing, Malware für Anmeldedaten-Diebstahl oder Brute-Force-Angriffen, z. B. durch Wiederverwendung von Anmeldedaten. Kompromittierte Konten werden meist dazu genutzt, weitere Angriffe innerhalb oder außerhalb des Unternehmens zu starten. Dazu gehören BEC und Phishing. Mit CAD können Sie Cyberkriminelle, die es auf Ihre vertraulichen Daten und vertrauenswürdigen Konten abgesehen haben, entdecken, untersuchen und abwehren. Die Lösung bietet personenorientierte Bedrohungserkennung, Korrelation der Bedrohungsaktivitäten, detaillierte Forensik basierend auf umfassenden Bedrohungsdaten sowie flexible Richtlinien zur automatisierten Reaktion.

Cloud App Security Broker

Proofpoint Cloud App Security Broker (PCASB) schützt Unternehmen vor der Kompromittierung von Cloud-Konten, der versehentlichen Weitergabe vertraulicher Daten sowie Compliance-Risiken in der Cloud. Proofpoint CASB bietet für Zugriff auf Cloud Apps ebenso wie die Datenverarbeitung in der Cloud einen detaillierten personenorientierten Überblick. Unsere Lösung kombiniert die Erkennung kompromittierter Konten, Zugangskontrollen, Schutz vor Datenverlust (DLP), Kontrolle von Drittanbieter-Anwendungen sowie Analysen, um Office 365, G Suite, Box und andere Plattformen abzusichern. Dank unserer leistungsstarken Analyse können Sie Ihren Endnutzern und Drittanbieter-Anwendungen die Zugangsberechtigungen zuweisen, die den für Sie relevanten Risikofaktoren entsprechen.

SCHUTZ IHRER INFORMATIONEN

Suche, Überwachung und Absicherung von Daten in E-Mails, Cloudanwendungen, lokalen Dateifreigaben und SharePoint

Email Data Loss Prevention (DLP)

Proofpoint Email DLP verhindert fahrlässiges Mitarbeiterverhalten durch die Blockierung vertraulicher und privater Informationen in ausgehenden Nachrichten. Ihre Mitarbeiter müssen nicht mehr Richtlinienentscheidungen über Art und Schutz der versendeten Inhalte treffen (wodurch sich der Arbeits- und Zeitaufwand erhöhen würde), sondern können einfach ihre Arbeit erledigen, während unsere Lösung die Richtlinien für die E-Mail-Kommunikation zentral und automatisch durchsetzt. Dank mehr als 80 detailliert anpassbaren Richtlinien, die vertrauliche E-Mails automatisch finden, klassifizieren und blockieren, wird die Wahrscheinlichkeit einer Datenkompromittierung deutlich gesenkt.

Email Encryption

Proofpoint Email Encryption ermöglicht dank richtlinienbasierter Verschlüsselung von Nachrichten und Anhängen die nahtlose sowie automatische Absicherung der Anwender-Kommunikation. Im Gegensatz zu herkömmlichen E-Mail-Verschlüsselungsdiensten, die häufig schwierig zu bedienen sind, müssen Ihre Mitarbeiter ihre E-Mails nicht manuell verschlüsseln, um Nachrichten auf sichere Weise zu versenden und zu empfangen – die Verschlüsselung erfolgt automatisch im Hintergrund. Mit unserer Lösung sind Ihre vertraulichen E-Mails geschützt. Gleichzeitig können Ihre Tochterunternehmen, Geschäftspartner und Endnutzer problemlos auf abgesicherte Nachrichten auf Computern sowie Mobilgeräten zugreifen.

Data Discover

Proofpoint Data Discover findet, überwacht und schützt vertrauliche Daten in Dateifreigaben, Datenspeichern und SharePoint-Sites. Die Lösung führt automatisierte Inhaltsanalysen durch, sodass Informationen im lokalen Netzwerk Ihres Unternehmens nachverfolgt werden können. Anschließend identifiziert Data Discover automatisch gefährdete vertrauliche Daten (einschließlich personenbezogener Daten sowie Gesundheitsinformationen) und ermöglicht durch Isolierung, Blockierung oder Löschung Echtzeit-Behebungsmaßnahmen, die die nicht autorisierte Informationsweitergabe verhindern.

Meta

Proofpoint Meta ist die Lösung der nächsten Generation für sicheren Zugriff auf Unternehmensanwendungen. Als personenorientierte Lösung gewährleistet Meta, dass Mitarbeiter, Auftragnehmer und Partner über identitätsbasierten Zero-Trust-Zugriff auf Unternehmensressourcen im Rechenzentrum und jeder beliebigen Cloud verfügen.

ObservelT

Im November 2019 wurde ObservelT von Proofpoint übernommen. ObservelT ist eine schlanke Endgerätelösung, die Unternehmen bei der Erkennung und Behebung von Insider-Risiken unterstützt. Damit schützt die Lösung die Unternehmensdaten vor böswilligem sowie fahrlässigem Anwenderverhalten von Mitarbeitern, privilegierten Anwendern und Dritten. Dank ObservelT können Unternehmen das Risiko von Sicherheitszwischenfällen verringern, indem sie das Anwenderverhalten überwachen und in Echtzeit Schulungs- sowie Präventionsmaßnahmen bereitstellen.

ObservelT verkürzt den Zeitaufwand für Untersuchungen von Tagen auf Minuten und bietet ein vollständiges Playback der Sicherheitsereignisse, um die Reaktionszeiten zu verbessern und die Einhaltung von Compliance-Vorschriften zu vereinfachen.

SCHUTZ VOR DIGITALEN RISIKEN

Schutz für Ihre Marke und Ihre Kunden vor Bedrohungen in sozialen Netzwerken, Webdomänen und im Dark Web

Digital Risk Protection

Proofpoint Digital Risk Protection schützt Ihre Kunden und Ihre Marke vor digitalen Sicherheitsrisiken in Webdomänen, sozialen Netzwerken sowie im Deep Web. Die Lösung kann nicht nur Markenbetrug im Zusammenhang mit Unternehmensdomänen verhindern, sondern auch Social-Media-Konten absichern und auf Phishing, Kontoübernahmen sowie Spam überwachen. Außerdem analysiert sie Deep Web- und Dark Web-Aktivitäten auf Bedrohungen für Führungskräfte, kompromittierte Anmeldedaten, Orte physischer Angriffe sowie nahe Ereignisse, die hohe Schäden verursacht haben. Dank Machine Learning sind Sie Bedrohungen immer einen Schritt voraus – unabhängig davon, ob sie noch in der Planungsphase sind, unmittelbar bevorstehen oder bereits (in Echtzeit) aktiv eingesetzt werden.

ARCHIVIERUNG UND COMPLIANCE

Aufbewahrung, Erkennung und Kontrolle der Daten für alle Kommunikationsplattformen zur Gewährleistung von Compliance

Enterprise Archive

Proofpoint Enterprise Archive speichert und erkennt geschäftskritische Informationen mithilfe von Cloud-Funktionen und Machine Learning. Dabei deckt die Lösung mit den Punkten Beweiserhebungsverfahren, Einhaltung von Vorschriften sowie Reduzierung von Kosten und Komplexität drei wichtige Herausforderungen ab, ohne dass sich Ihr Team Gedanken über die interne Archivverwaltung machen muss. Unsere skalierbare Cloud-Architektur, garantierte Suchleistung, unübertroffene Kundenzufriedenheit sowie die branchenweit fortschrittlichste Verschlüsselung ermöglichen die vollständige Kontrolle über rechtliche und Compliance-Fragen.

Enterprise Collaboration Archive

Proofpoint Enterprise Collaboration Archive nutzt richtlinienbasierte Kontrollen zur Erfassung von Social-Media-Inhalten in Salesforce Chatter, Jive, Skype Enterprise, LinkedIn, Twitter sowie weiteren Plattformen. Diese Inhalte werden wie andere wichtige Datenressourcen in Ihrem Compliance-Archiv oder Ihrer Überwachungsplattform verwaltet und überprüft. So sorgen Sie dafür, dass Sie die für Sie geltenden Vorschriften einhalten. Die Lösung stellt zudem erweiterte Funktionen zur Automatisierung und Vereinfachung wichtiger Compliance-Aufgaben bereit.

Intelligent Supervision

Mit Proofpoint Intelligent Supervision können Finanzdienstleister die Einhaltung strenger und komplexer Compliance-Vorschriften wie FINRA, SEC und IIROC vereinfachen. Die Lösung ist vollständig mit Enterprise Archive verzahnt und nutzt Machine Learning zur einfachen Erfassung, effizienten Überprüfung sowie effektiven Berichterstellung, um regulatorische Maßnahmen zu unterstützen. Dadurch profitieren Sie von einer vollständigen Übersicht über alle E-Mails, Instant Messaging Nachrichten, Collaboration Tools, Sprach- und SMS-Nachrichten sowie Social-Media-Aktivitäten.

E-Discovery Analytics

Proofpoint E-Discovery Analytics bietet einen intuitiven E-Discovery-Workflow für Ihre Rechtsabteilung. Dank Machine Learning und Echtzeit-Suchergebnissen sowie integrierten frühzeitigen Fallanalysen werden die Erkenntnisse und der Überblick verbessert. Wir unterstützen Sie bei der proaktiven Vorbereitung auf Rechtsstreitigkeiten, was für Sie mehr Kontrolle und weniger Risiko bedeutet.

Social-Media-Compliance

Proofpoint hilft dabei, die Lücke zwischen Social-Media-Compliance und Marketing-Abläufen zu schließen, damit Anwender die geltenden Vorschriften für soziale Netzwerke einhalten. Digital Risk Protection integriert sich in führende Archivierungslösungen, um Social-Media-Inhalte für zukünftige Suchen und E-Discovery zu erfassen und zu klassifizieren. Dadurch sparen Sie bei einem Audit Zeit und Geld.

WEITERE INFORMATIONEN

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

proofpoint.

1201-002-01-01 02/20