Proofpoint-Bundle-Angebote

Menschen schützen. Daten sichern.

Proofpoint bietet einen einzigartigen personenzentrierten Cybersicherheitsansatz, der bei Ihren besonders häufig angegriffenen Personen – Very Attacked People™ (VAPs) – ansetzt und die Risiken für Ihr Unternehmen bewertet. Mit unseren Bundle-Angeboten Threat Protection und Information Protection erhalten Sie umfassende Lösungen, die eine Abwehr aktueller Bedrohungen ermöglichen, Ihre Ressourcennutzung optimieren und Ihre Sicherheitsstrategie untermauern. Dieses Dokument bietet einen Überblick über diese Bundle-Angebote und erklärt, wie Sie mit diesen Lösungen Ihre Mitarbeiter und Ihre Daten schützen können.

KI/ML-Innovation mit Unterstützung von Nexus Threat Graph

Proofpoint verwendet künstliche Intelligenz (KI) und Machine Learning (ML), um Mitarbeiter und Daten zu schützen. Diese Technologien sind tief in die Produkt-Suite integriert, um Kunden vollständigen und ständig weiterentwickelten Schutz vor einem breiten Spektrum an Bedrohungen zu bereitzustellen. Unsere Erfahrungen aus fast zwei Jahrzenten in den Bereichen KI, ML und Datenwissenschaften fließen in die KI-Plattform ein, die unsere Proofpoint-Produkte unterstützt, damit die Produkte die gesamte Bandbreite an Cybersicherheits- und Compliance-Risiken abwehren können.

Unsere Technologien für Bedrohungsdaten und Erkennung erobern den Markt mit ML-Modellen, die vom Proofpoint Nexus Threat Graph basierend auf Daten von mehr als einer Billion Knoten trainiert werden. Proofpoint Nexus Threat Graph hat Zugriff auf umfangreiche Cybersicherheitsdaten zu E-Mail, Cloud, Netzwerken und Domains. Unser integriertes Team aus Datenwissenschaftlern umfasst Inhaber von Doktortiteln und Masterabschlüssen im Bereich Cybersicherheit sowie aus Experten aus dem öffentlichen und Hochschulsektor. Dieses Team arbeitet bei unseren Produkten für Bedrohungsschutz, Informationsschutz sowie Archivierung und Compliance mit Bedrohungsforschern zusammen. Zudem arbeiten wir mit führenden Universitäten zusammen, um bei Datenwissenschaften ganz vorn dabei zu sein. Dadurch wird die Effektivität unsere Machine-Learning-Technologie maximiert.

Proofpoint Threat Protection-Bundle-Angebote: Schutz für Ihre Mitarbeiter

Schützen Sie Ihre Mitarbeiter vor Bedrohungen, die sie ins Visier nehmen. Durch die Integration mehrerer Kontrollen für E-Mail, Cloud, Anwender und Lieferanten bietet die Proofpoint Threat Protection-Plattform umfassenden Schutz vor Phishing, BEC-E-Mail-Betrug, Malware und Ransomware. Mit der integrierten, KI-gestützten Plattform erhalten Sie einen einzigartigen Überblick über Ihre Angriffsfläche. Daher können Sie effektiveren Schutz vor aktuellen Bedrohungen sowie positive operative Ergebnisse erzielen. Alle Bundle-Angebote sind als einfach implementierbare Inline+API- oder als MX-basierte Variante verfügbar. Beide Varianten bieten den gleichen zuverlässigen Schutz.

Überblick über Proofpoint Threat Protection

FUNKTIONEN	KOMPONENTE	PX	P0	P1	P1+
Bereitstellung und Verwaltung	• Lokal, hybrid oder Cloud • Inline+API oder MX-basiert	• Nur Microsoft 365-Konten • Nur Inline+API	✓	✓	✓
Business Email Compromise (BEC)	KI- und ML-gestützte Verhaltens- und Reputationsanalyse	✓	✓	✓	Dashboard zu Lieferantenrisiken
Phishing, Ransomware und Malware	KI- und ML-gestützte Verhaltens- und Reputationsanalyse	✓	✓	✓	✓
	URL-Veränderung und Sandbox-Analyse zum Klickzeitpunkt		✓	✓	✓
	Sandbox-Analyse von Anhängen		✓	✓	✓
Kontoübernahmen	Überblick über Konto-übernahmen	✓	✓	✓	✓
	Nachträgliche Untersuchungen mit Zeitleistenansicht	+	+	+	+
	Behebungsmaßnahmen für E-Mail- und Cloud-Umgebungen	+	+	+	+
Meldung und Behebung von E-Mails	Automatisches mSOAR	✓	✓	✓	✓
	Automatisiertes Abuse-Postfach	✓*	✓	✓	✓
	Berichte zu Anwender-E-Mails	✓		Warnhinweise in E-Mails	
Dashboards zu Bedrohungen und Anwendern	Erkenntnisse zu Bedrohungen, inkl. VAPs	✓	✓	✓	✓
	Dashboards zu Anwenderrisiken		✓	✓	✓
Hygiene für eingehende E-Mails und Konfiguration	Schutz vor Spam, Viren, Graymail		✓	✓	✓
	Funktionen für Führungskräfte/ VIP		✓	✓	✓
	Angepasste Richtlinien		✓	✓	✓
Mehrschichtiger Anwenderschutz	Isolierung veränderter E-Mail-Klicks	+		VAPs	Alle
	Schulungen zur Sensibilisierung für Sicherheit	+	+	✓	✓
E-Mail-Authentifizierung und interner Schutz	DMARC-Implementierung, Erkenntnisse	+	+	+	✓
	Bedrohungsschutz für interne E-Mails	+	+	+	<5.000 Nutzer

LEGENDE	
✓	Im Bundle-Angebot enthalten
+	Mit Zusatzkosten erhältlich

* Demnächst, nur Cloud-basiert

Beschreibung der Proofpoint Threat Protection-Bundle-Angebote

PAKET-ANGEBOT	ÜBERBLICK	BESCHREIBUNG	ENTHÄLT
PX	Schneller und einfacher KI-gestützter E-Mail-Schutz für Microsoft 365. Optimal für kleine Unternehmen, die die nativen Microsoft 365-Sicherheits-funktionen ergänzen und die E-Mail-Sicherheitsverwaltung mit vorkonfigurierten Einstellungen vereinfachen möchten. Wird innerhalb von Minuten per Inline+API bereitgestellt.	Proofpoint PX ist nur für Cloud-basierte Microsoft 365-Instanzen verfügbar. Dies ist die schnellste und einfachste Möglichkeit, branchenführende E-Mail- und Cloud Sicherheit zu implementieren. Mithilfe von Machine Learning, Verhaltensanalysen und Bedrohungsdaten erkennt und blockiert Proofpoint PX zuverlässig Phishing, Business Email Compromise (BEC) sowie Lieferketten- und Ransomware-Angriffe, die die Microsoft-Sicherheitsmaßnahmen umgehen.	KI-gestützte Erkennung sowie automatisierte Behebung, um die nativen Microsoft-Schutzfunktionen zu ergänzen.
P0	Erweiterte E-Mail- und Cloud-Sicherheit. Optimal für Unternehmen, die mit gezielteren Angriffen konfrontiert werden und weitere Anpassungs- und Konfigurationsmöglichkeiten benötigen.	Wehren Sie E-Mail-Bedrohungen in der gesamten Angriffskette ab – von der Erkennung bis zur Reaktion. Dies umfasst die automatisierte Verwaltung von Abuse-Postfächern, sodass von Anwendern gemeldete schädliche Phishing-E-Mails entfernt werden. Auf diese Weise werden Bedrohungen wie Phishing und Business Email Compromise (BEC), Lieferantenbetrug, Ransomware sowie andere Malware abgewehrt. Mit dieser Lösung erhalten Sie einen Überblick darüber, wer wie angegriffen wird, ob diese Personen auf Phishing-Köder klicken, solche E-Mails melden oder kompromittiert wurden.	Alle Funktionen von PX plus: • Flexiblere Bereitstellungsoptionen (hybrid oder lokal) • Verwaltung des E-Mail-Flusses durch Anpassung in einer vollständigen Verwaltungskonsole • Erweiterter Schutz zum Klickzeitpunkt für Anhang- und URL-basierte Angriffe, einschließlich TAP URL Isolation for VAP • HTML-basierte E-Mail-Warnhinweise mit Meldungsoption • Hygiene für Anwender-E-Mails, einschließlich Schutz vor Spam, Viren und Graymail sowie andere Kontrollen • Integriertes Dashboard zu Anwenderrisiken mit empfohlenen Kontrollen (Nexus People Risk Explorer)
P1	Erweiterter Bedrohungsschutz. Optimal für Unternehmen, die weitere integrierte, mehrschichtige Sicherheitsfunktionen benötigen und ihre Mitarbeiter schulen müssen.	Schulen Sie Endnutzer, damit sie nicht auf eingehende Bedrohungen hereinfallen. Ergänzen Sie Ihren Bedrohungsschutz mit einem robusten Schulungsprogramm zur Cybersicherheit, das Ihre E-Mail-Sicherheitskontrollen integriert und simulierte Phishing-Angriffe, Tests Ihrer Sicherheitskultur und des Wissens Ihrer Mitarbeiter sowie umfangreiche Schulungen und Security-Awareness-Materialien umfasst. Sie können den Lehrplan basierend auf den tatsächlichen Bedrohungen für Ihre Anwender anpassen und dabei den vollständigen Katalog interaktiver Schulungen und Tools für Verhaltensänderungen nutzen. Die Funktionen umfassen Bedrohungssimulationen, mit denen die Reaktionen der Anwender auf Phishing-Angriffe getestet werden. Für diese Simulationen, mit denen Sie den Sicherheitskenntnisstand und den Erfolg Ihrer Schulungsmaßnahmen feststellen können, stehen tausende Vorlagen in mehr als 40 Sprachen und 13 Kategorien zur Verfügung. Den Fortschritt Ihres Programms können Sie in einem speziellen CISO-Dashboard grafisch darstellen, das sich auf die Kennzahlen konzentriert, für die sich leitende Sicherheitsverantwortliche ganz besonders interessieren.	Alle Funktionen von P0 plus Security Awareness Training Enterprise

PAKET-ANGEBOT	ÜBERBLICK	BESCHREIBUNG	ENTHÄLT
P1+	Vollständiger Schutz vor E-Mail- und Cloud-Bedrohungen. Optimal für Großunternehmen, die erweiterten E-Mail- und Cloud-Schutz sowie mehrschichtige Sicherheitsfunktionen und Einblicke benötigen.	Verbessern Sie den Schutz vor E-Mail- und Domain-Betrug (einschließlich BEC), um im Namen Ihres Unternehmens versendete Spoofing-Angriffe über ein- und ausgehende E-Mails zu stoppen. Bei BEC-Attacken kommen verschiedene Methoden zur Identitätstäuschung zum Einsatz. Daher benötigen Sie einen mehrschichtigen Ansatz zum Schutz Ihrer Mitarbeiter, Kunden und Geschäftspartner. Die integrierte Proofpoint-Lösung mit BEC-Schutz deckt alle Bedrohungstaktiken ab, liefert einen vollständigen Überblick über Ihr E-Mail-Ökosystem und gibt Ihnen Kontrollen in die Hand, mit denen Sie diese Angriffe noch vor der Zustellung in das Postfach abwehren können. Die Proofpoint-Lösung schützt nicht nur per DMARC, sondern bietet auch einen einzigartigen Überblick über Risiken durch Lieferanten, damit Sie die Herausforderungen komplexer Lieferkettenangriffe bewältigen können. Identifizieren Sie automatisch Ihre Lieferanten und bewerten Sie das Risiko der von ihnen verwendeten Domains zum Versenden von E-Mails an Ihre Anwender. Durch die Integration der Daten aus der Threat Protection-Plattform deckt die Lösung zudem das Nachrichtenaufkommen, die erkannten Bedrohungen von Lieferanten-Domains sowie die blockierten Nachrichten von schädlichen Doppelgänger-Domains Ihrer Lieferanten auf. Unternehmen mit weniger als 5.000 Anwendern profitieren außerdem von einem Echtzeit-Überblick sowie von automatischen Reaktionen auf interne E-Mail-Bedrohungen, die von kompromittierten Konten gesendet wurden. Sie können schnell feststellen, welche Konten kompromittiert wurden und wer betroffen ist.	Alle Funktionen von P1 plus: • Email Fraud Defense (EFD) • Supplier Risk Explorer • TAP URL Isolation für alle Anwender • Internal Mail Defense für Unternehmen mit weniger als 5.000 Anwendern

Proofpoint Information Protection-Bundle-Angebote: Schutz für Ihre Daten

Modernisieren Sie Ihre DLP-Lösung (Data Loss Prevention, Datenverlustprävention) mit unserem Proofpoint Enterprise DLP-Bundle-Angebot. Dieses Bundle-Angebot nutzt einen personenzentrierten Ansatz und setzt Inhalte, Verhalten und Bedrohungen in einen Kontext, um verwertbare Erkenntnisse zu gewinnen und Datenverlust zu verhindern. Stellen Sie Ihren Sicherheits- und Compliance-Teams Telemetriedaten zu E-Mail, Cloud und Endpunkten zur Verfügungen, damit sie mit einer einzigen Lösung die gesamte Bandbreite an personenzentrierten Datenrisiken bewältigen können.

Umfang von Proofpoint Enterprise DLP:

- **Email DLP:** Schützt mit integrierten Richtlinien, File Fingerprinting und „Smart Send“-Funktionen vor Datenverlust.
- **Cloud App Security Broker (CASB):** Bietet Schutz vor Cloud-Bedrohungen sowie Cloud-DLP, einschließlich Schutz vor zu freizügiger Weitergabe vertraulicher Daten, Kontrolle von Drittanbieter-Anwendungen und Funktionen zur Kontrolle von Schatten-IT.
- **Endpoint DLP und Insider Threat Management (ITM):** Für 3 % der Anwender. Beheben Sie Insider-Risiken mit einem ressourcenschonenden Endpunkt-Agenten und unterbinden Sie böswilliges sowie fahrlässiges Anwenderverhalten von Mitarbeitern, privilegierten Anwendern und externen Personen.

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.