

Proofpoint-Bundle-Angebote

Die Antwort auf Ihre drängendsten Cybersicherheitsprobleme

Um aktuelle raffinierte Angriffe zu stoppen, müssen Sie sich auf den Schutz Ihrer Mitarbeiter konzentrieren. Proofpoint bietet einen einzigartigen personenorientierten Cybersicherheitsansatz, der bei Ihren besonders häufig angegriffenen Personen – Very Attacked People (VAPs) – ansetzt und die Risiken für Ihr Unternehmen bewertet. Mit unseren Bundle-Angeboten erhalten Sie umfassende Lösungen, die eine Abwehr aktueller Bedrohungen ermöglichen, Ihre Ressourcennutzung optimieren und Ihre Sicherheitsstrategie untermauern.

Bundle-Angebot P1: Erweiterte E-Mail-Sicherheit

Beginnen Sie beim Schutz Ihres Unternehmens beim Bedrohungsvektor Nr. 1: E-Mails. Wehren Sie E-Mail-Bedrohungen in der gesamten Angriffskette ab – von der Erkennung bis zur Reaktion. Erfahren Sie, wer wie angegriffen wird, ob diese Personen auf Phishing-Köder klicken, solche E-Mails melden oder kompromittiert wurden. Lassen Sie (Malware-basierten und Malware-losen) E-Mail-Angriffen keine Chance. Schulen Sie Ihre Anwender, damit sie stärker für eingehende Bedrohungen sensibilisiert sind. Automatisieren Sie Ihre Behebungsmaßnahmen und ergänzen Sie Ihren Bedrohungsschutz mit einem robusten Schulungsprogramm zur Cybersicherheit. Nutzen Sie die simulierten Phishing-Angriffe, umfassende Schulungen und automatisierte Abuse-Postfach-Verwaltung.

UMFANG VON P1:

- Email Protection
- Threat Response Auto-Pull (TRAP)
- Basic Email Encryption (TLS)
- Targeted Attack Protection (TAP)
- Security Awareness-Training: Enterprise
- Basic Email DLP (RegEx)

Bundle-Angebot P1+: Abwehr von BEC-Angriffen

Ergänzen Sie Ihren Bedrohungsschutz um die Abwehr von Angriffen mit gefälschter Identität. Dies beinhaltet sowohl eingehende Angriffe auf Ihre Mitarbeiter sowie ausgehende Angriffe, die „in Ihrem Namen“ an Kunden und Geschäftspartner versendet werden. Bei BEC-Attacken kommen verschiedene Methoden zur Identitätstäuschung zum Einsatz. Durch die Integration von DMARC-Authentifizierung in Ihr E-Mail-Gateway erhalten Sie einen mehrschichtigen Sicherheitsansatz, der E-Mail-Angriffe mit gefälschter Identität zuverlässig abwehrt. Unsere integrierte BEC-Lösung 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.

P1+ UMFASST P1 SOWIE:

- Email Fraud Defense (EFD)

Bundle-Angebot P2: Abwehr von BEC- und EAC-Angriffen

Analysieren Sie Hinweise auf Email Account Compromise (EAC) und wehren Sie diese Angriffe ab, bei denen schädliche E-Mails intern über kompromittierte Konten versendet werden. Zusätzlich erhalten Sie in Echtzeit einen Überblick über kompromittierte Konten, angegriffene Personen und in Ihrem Unternehmen versendete Bedrohungen. Dieses Bundle-Angebot automatisiert Ihre Reaktionsmaßnahmen, beispielsweise die Entfernung schädlicher E-Mails, Kennwortzurücksetzungen, Sperrung von E-Mail-Konten usw. Ebenso haben Angriffe über private Webmails und riskante Websites in unternehmensbezogenen E-Mails keine Chance.

P2 UMFASST P1+ SOWIE:

- Internal Mail Defense (IMD)
- Cloud Account Defense (CAD)
- Email Isolation
- Email Encryption
- Email DLP

Bundle-Angebot P2+: Schutz von Cloudanwendungen

Schützen Sie Ihre Mitarbeiter und sichern Sie Ihre Daten bei der Arbeit in Microsoft Office 365, Google G Suite und weiteren Cloudanwendungen. Durch die Integration unserer CASB-Lösung in Ihre personenorientierte Sicherheitsstrategie erhalten Sie einen zentralen Überblick über Ihre Cloud-Umgebung. Gleichzeitig bietet das Bundle-Angebot Schutz vor Cloud-Bedrohungen und kompromittierten Konten, liefert Einblicke in riskante Cloudanwendungen von Drittanbietern und sichert wertvolle Daten ab, die Ihre Mitarbeiter erstellen und nutzen.

P2+ UMFASST P2 SOWIE:

- Cloud App Security Broker (CASB)

Bundle-Angebot P3: Vollständige personenorientierte Sicherheit

Bauen Sie ein strategisches Sicherheitsprogramm auf, das Ihre gesamte menschliche Angriffsfläche – einschließlich des gesamten Ökosystems – vollständig abdeckt. Dazu gehören Ihre Domänen, Konten in sozialen Netzwerken, Ihre Führungskräfte und Speicherorte, aber auch weitere Technologieinfrastruktur in Ihrer Umgebung sowie jegliche Web-Zugriffe. Schützen Sie Ihre VAPs mit integrierten, adaptiven Kontrollen und Quarantänefunktionen. Ihnen zur Seite steht ein dedizierter Bedrohungsanalyst, der den Bedrohungsschutz konkret für Ihr Unternehmen optimiert.

P3 UMFASST P2+ SOWIE:

- Browser Isolation
- Threat Response
- Digital Risk Protection
- Premium Threat Information Service (PTIS)

Bundle-Angebote

proofpoint.

P1 P1+ P2 P2+ P3

Schutz vor Bedrohungen	<ul style="list-style-type: none"> • Schützen Sie den Posteingang der Anwender vor Phishing, E-Mail-Betrug und Malware <i>Email Protection, Targeted Attack Protection (TAP)</i> • Vollständige Transparenz über die VAPs (Very Attacked People, besonders häufig angegriffene Personen) und die gegen sie gerichteten Bedrohungen <i>TAP, CASB</i> • Automatische Entfernung schädlicher E-Mails aus den Posteingängen der Anwender anhand von Endnutzer-Meldungen sowie erst nachträglich aufgetretenen Bedrohungen <i>TRAP, CLEAR</i> • E-Mail-Authentifizierung, damit betrügerische Nachrichten, die von vertrauenswürdigen Domänen gesendet wurden, blockiert werden können <i>Email Fraud Defense (EFD)</i> • Schutz vor den Risiken durch den Abruf privater E-Mails auf unternehmenseigenen Endgeräten <i>Email Isolation</i> • Untersuchung und Reaktion auf die Risiken durch kompromittierte Cloud-Konten, einschließlich von diesen Konten ausgehender interner Bedrohungen <i>TRAP, CAD, IMD</i> • Erlaubt Anwendern das Surfen im Internet und verhindert gleichzeitig, dass Geräte des Unternehmens durch schädliche Inhalte beeinträchtigt werden <i>Browser Isolation</i> • Betrugserkennung im Hinblick auf verdächtige Webdomänen und Social-Media-Konten <i>Digital Risk Protection</i> • Dedizierter Bedrohungsanalyst stellt Bedrohungsdaten und Empfehlungen speziell für Ihr Unternehmen bereit <i>PTIS</i> 	•	•	•	•	•
Schutz Ihrer Anwender	<ul style="list-style-type: none"> • Bedrohungssimulationen zum Testen der Reaktionen von Anwendern auf Phishing-Angriffe; Tausende Vorlagen, mehr als 35 Sprachen und 13 Kategorien <i>ThreatSim</i> • Interaktive Schulungen, um eine Verhaltensänderung beim Endanwender zu erreichen <i>Security Awareness-Training</i> • Erfahren Sie, wie es um den Kenntnisstand der Anwender vor Start der Trainings bestellt ist. Schulen Sie Ihre Mitarbeiter, so dass diese Sicherheitsrisiken erkennen und vermeiden. Überwachen sie die Fortschritte Ihrer Anwender <i>CyberStrength</i> 	•	•	•	•	•
Schutz Ihrer Informationen	<ul style="list-style-type: none"> • Regular Expression für E-Mail-DLP; E-Mail-Verschlüsselung per TLS <i>Email Protection (RegEx)</i> • Integrierte Richtlinien, File Fingerprinting und „Smart Send“ zum Schutz vor Compliance-Verstößen; TLS-Fallback für Push/Pull-Verschlüsselung einschließlich Web-Portal <i>Email DLP und Email Encryption</i> • Schutz vor Cloud-Bedrohungen; DLP, einschließlich dem Schutz vor zu freizügigem Teilen vertraulicher Daten, Kontrolle von Drittanbieter-Anwendungen und Schatten-IT <i>CASB</i> 	•	•	•	•	•

P1 Erweiterte E-Mail-Sicherheit

P1+ Abwehr von BEC (Business Email Compromise)

P2 Abwehr von EAC (kompromittierte E-Mail-Konten) und BEC

P2+ Schutz von Cloudanwendungen

P3 Umfassende personenorientierte Sicherheit

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter proofpoint.com/de.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. 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 mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten 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, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.