

So schützt Proofpoint EFD jenseits von DMARC

Proofpoint EFD übertrifft autonome DMARC-Lösungen

Produkte

- Proofpoint Email Fraud Defense
- Proofpoint Targeted Attack Protection
- Proofpoint Email Protection
- Proofpoint Domain Discover
- Proofpoint Secure Email Relay

Wichtige Vorteile

- Allgemeine und detaillierte Einblicke in die Bedrohungslandschaft
- Machine Learning-Algorithmen zur intelligenten Klassifizierung von Identitäten
- Plattformbasierter Sicherheitsansatz mit leistungsstarken Integrationen mit anderen Proofpoint-Produkten und -Services

Da 96 % aller verdächtigen sozialen Interaktionen per E-Mail erfolgen¹, müssen Unternehmen ihre E-Mail-Anwender stärker schützen als je zuvor. Im Laufe der Jahre entstanden E-Mail-Authentifizierungsstandards wie SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) und DMARC (Domain-based Message Authentication, Reporting and Conformance), mit denen E-Mail-Spoofing und Betrugsversuche abgewehrt werden können.

DMARC kombiniert die Vorteile von SPF und DKIM und hat sich bei der Reduzierung von BEC-Attacks (Business Email Compromise), Phishing und Spoofing als effektiv erwiesen. Da DMARC jedoch auf den beiden anderen Standards basiert, kann die Einarbeitung in diesen Standard einige Zeit dauern. Die Implementierung einer DMARC-Strategie kann sich ebenfalls als kompliziert erweisen, zudem ist die Verarbeitung der DMARC-Berichte häufig schwierig.

Mittlerweile wurden zahlreiche Lösungen veröffentlicht, mit denen Unternehmen ihre DMARC-Strategien einrichten und verwalten können. Ebenso wie viele dieser Lösungen kann Proofpoint Email Fraud Defense (EFD) Sie bei der Bereitstellung Ihrer DMARC-Implementierungen zu unterstützen. Proofpoint EFD geht jedoch weit darüber hinaus: Die Lösung bietet einzigartige Einblicke in die Bedrohungslandschaft und nutzt Machine Learning, um Ihre Mitarbeiter intelligent und zuverlässig zu schützen. Der plattformbasierte Sicherheitsansatz integriert sich nahtlos mit anderen Proofpoint-Lösungen, damit Sie umfassenden und flexiblen Schutz erhalten.

¹ Verizon: „Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen), 2020.

Umfassende Erkenntnisse zu Bedrohungen

Proofpoint EFD bietet allgemeine und detaillierte Einblicke in die Bedrohungslandschaft. Die Lösung erfasst Telemetrie- und DMARC-Forensikdaten von mehr als 120 Messaging-Anbietern, die sich an Verbraucher richten. Proofpoint EFD verwendet all diese Daten, um Ihnen einen detaillierten Überblick über Bedrohungen zu bieten, die Ihre Marke oder Domäne imitieren.

Machine Learning-basierter Schutz

Proofpoint EFD nutzt Machine Learning-Algorithmen, mit denen Sie Ihre Lieferanten über eingehende Rechnungen an Proofpoint-E-Mail-Gateways identifizieren und bewerten können. Auf diese Weise behalten Sie problemlos Ihre Anbieter im Blick, von denen Sie abhängen. Zudem wird nach Lieferanten-bezogenen Bedrohungen gesucht, die gegen Sie gerichtet sind.

Schutz vor Risiken durch Lieferanten

Proofpoint EFD umfasst Nexus Supplier Risk Explorer. Dieses Tool identifiziert automatisch Ihre Lieferanten und die von ihnen verwendeten Domänen, identifiziert sowie priorisiert die Risiken der einzelnen Lieferanten in einer Dashboard-Ansicht und verifiziert deren DMARC-Datensätze.

Einblicke zu Domänenmissbrauch

Eine Proofpoint EFD-Standardfunktion ist Proofpoint Domain Discover. Diese Funktion findet Domänen, die Ihre Marke imitieren und häufig Ihre Mitarbeiter, Kunden und Partner angreifen. Mithilfe von Machine Learning und künstlicher Intelligenz analysiert Proofpoint Domain Discover umfangreiche Domänenendaten, um Domänenbetrug und betrügerische Domänen zu erkennen.

Stark integriertes Ökosystem

Proofpoint EFD ist unter den Fortune 1000-Unternehmen am weitesten verbreitet. Durch unseren plattformbasierten Ansatz können Sie viele unserer Service nahtlos nutzen und außerdem von den Vorteilen unserer starken Ökosystem-Integration zwischen Proofpoint-Erkennungssystemen und den DMARC-Berichten von Proofpoint EFD profitieren.

Integrationen von Proofpoint EFD:

- **Proofpoint Targeted Attack Protection (TAP):** Proofpoint TAP zeigt Bedrohungsmetriken an, die in den E-Mail-Gateways von mehr als 8.000 Proofpoint-Unternehmenskunden erfasst werden. Dadurch können Proofpoint EFD-Berichte reale Bedrohungserkennungsdaten von Unternehmen direkt korrelieren. Keine andere Lösung bietet einen so umfangreichen Überblick für Branchen und Regionen. Proofpoint EFD unterstützt im TAP-Dashboard Direktverknüpfungen mit Spoofing-Angriffen.
- **Proofpoint Email Protection:** Proofpoint EFD unterstützt die direkte Veröffentlichung schädlicher domänenbasierter Blockierungen in Proofpoint Email Protection-Appliances und Host-Services.
- **Proofpoint Virtual Takedown:** Mit den von Proofpoint Domain Discover erfassten Informationen können Sie einen Virtual Takedown auslösen, indem Sie Daten zu schädlichen und kriminellen Domänen übertragen. Dazu gehören zum Beispiel Domänen, die Phishing betreiben, schädliche Inhalte verbreiten oder an kriminellen Aktivitäten beteiligt sind. Außerdem ermöglicht die Funktion die Erstellung von Blocklists für verschiedenste ISPs, Geräte, Web-Dienste und Sicherheitsprodukte.
- **Proofpoint Secure Email Relay (SER):** Proofpoint SER verhindert, dass kompromittierte externe Versender schädliche E-Mails von der Anwenderdomäne senden können, und verringert das Bedrohungsrisiko, da nur autorisierte Versender den Service nutzen dürfen.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.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 mehr als die Hälfte der Fortune-1000-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, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.