How Proofpoint EFD Is More Than Just DMARC

EFD outshines standalone DMARC solutions

Products

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

Key Benefits

- Get broad and deep insight into the threat landscape
- Leverage machine learning algorithms for intelligent identity classification
- Enjoy a platform-based approach to security, using powerful integrations with other Proofpoint products and services

With 96% of all suspicious social interactions arriving through email,[1] organisations must protect their email users more than ever. Over the years, email-authentication standards such as Sender Policy Framework (SPF); DomainKeys Identified Mail (DKIM); and the Domain-based Message Authentication, and Conformance (DMARC) have sprung up to help defend against email spoofing and fraud attacks.

DMARC brings together the power of SPF and DKIM. It has proven to be quite effective at reducing business email compromise (BEC), phishing and spoofing attacks. A common problem, however, is that being based on two other standards, DMARC can take some time to understand. Implementing a DMARC strategy can also be complex. And DMARC reports are often difficult to parse.

A raft of solutions have sprung up to help organisations set up and manage their DMARC strategies. Like many of these solutions, Proofpoint Email Fraud Defense (EFD) can help you streamline the deployment of your DMARC implementations. Proofpoint EFD, however, offers so much more than this. It provides you with unparalleled insight into the threat landscape. It also leverages machine learning to help defend your people intelligently and thoroughly. And its platform-based approach to security integrates seamlessly with other Proofpoint solutions for comprehensive and flexible protection.

1 Verizon. “Data Breach Investigations Report.” 2020.

Comprehensive Threat Insight

Proofpoint EFD offers broad and deep insight into the threat landscape. It collects telemetry and DMARC forensic data from more than 120 consumer messaging providers. EFD uses this wealth of data to provide you with a detailed view of brand- and domain-impersonation threats.

Machine Learning Defence

Proofpoint EFD employs machine learning algorithms. These help you identify and score your suppliers through inbound invoice detection via Proofpoint email gateways. This way you can easily keep track of the third parties that you depend on. It also screens for threats directed toward you that may be associated with suppliers.

Protect Against Supplier Risk

Proofpoint EFD includes Nexus Supplier Risk Explorer. This tool automatically identifies your suppliers and the domains they use to send to your users. It then identifies and prioritises the risk each supplier poses into a dashboard view and verifies their DMARC records.

Gain Insight Into Domain Abuse

A standard feature of Proofpoint EFD is Proofpoint Domain Discover, which finds domains that are posing as your brand. These domains often target your employees, customers and partners. Using machine learning and artificial intelligence, Domain Discover analyses a vast body of domain data to uncover domain fraud and infringing domains.

Tight Ecosystem and Integrations

Proofpoint EFD has the broadest deployment in the Fortune 1000. Our platform-based approach lets you leverage many of our services seamlessly. It also lets you enjoy the benefits of tight ecosystem integration between Proofpoint detection systems and EFD's DMARC reporting.

Proofpoint EFD integrations include:

- **Proofpoint Targeted Attack Protection (TAP).** Proofpoint TAP provides threat metrics observed by more than 8,000 Proofpoint enterprise customer email gateways. This gives EFD reports a direct correlation to real world enterprise threat-detection data. No other solution offers such a broad visibility into threat visibility across industry verticals and regions. EFD supports direct linking to spoofing attacks within the TAP dashboard.
- **Proofpoint Email Protection.** Proofpoint EFD supports the publishing of malicious domain-based blocking directly to Proofpoint Email Protection appliances and hosted services.
- **Proofpoint Virtual Takedown.** Information gathered from Proofpoint Domain Discover can be used to initiate a Virtual Takedown by submitting malicious and criminal domains. These domains can include those engaged in phishing, propagation of malicious content in criminal activity. They can also include domains found in blocklists used by a wide array of ISPs, devices, web services and security products.
- **Proofpoint Secure Email Relay (SER).** Proofpoint SER prevents compromised third-party senders from sending malicious email using the users' domain. It reduces threat risk by letting only credentialed senders use the service.

LEARN MORE

For more information, visit **proofpoint.com**.