Proofpoint Email Fraud Defense

Key Benefits

- Makes DMARC implementation easier with guidance through each step of your rollout
- Protects your brand from being used in email fraud attacks, without blocking legitimate email
- Automatically identifies your suppliers and the risks they pose
- Shows all email sent using your trusted domains and from lookalikes
- Ensures reliable SPF, DKIM and DMARC record hosting with Proofpoint-hosted authentication services
- Integrates with industry-leading Proofpoint email gateway to help you enforce DMARC with confidence and flexibility
- Shows DMARC pass rates for company-owned domains that are managed on Microsoft 365

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

Proofpoint Email Fraud Defense streamlines your DMARC implementation with guided workflows and support from skilled consultants. Our product protects your company's reputation from email fraud attacks. It shows the sources of emails sent using your domains and from lookalikes. It also reduces supplier risk by identifying your suppliers and lookalikes of their domains registered by third parties.

Email Fraud Defense guides you through DMARC deployment. It helps protect your customers, business partners and employees from business email compromise (BEC) scams. With Email Fraud Defense, Proofpoint protects your brand from being used in email fraud attacks and reduces the risk of inbound impostor threats. We authenticate all emails delivered to and sent from your organisation. And we do this without blocking legitimate email.

Ease of Use

Dedicated consultants and expert guidance

To help you set up email authentication, Proofpoint creates a project plan for you. The plan has guided workflows that simplify the setup process. Our consultants help you through every step of the plan. We work with you to identify all your legitimate senders – including third parties and shadow IT – to make sure they authenticate properly. We also analyse your email environment to help you prioritise tasks based on your needs, such as email volume and top senders.

Hosted authentication services

Email Fraud Defense includes Proofpoint's Hosted SPF, Hosted DKIM and Hosted DMARC services. These hosted services help you set up and manage policies for Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and DMARC. They are also geographically distributed, fault-tolerant services that ensure reliability.

Hosted SPF

- Helps you overcome the 10 DNS lookup limit imposed by SPF
- Reduces the work of updating SPF records
- Updates records in real time, with proper syntax validation
- Improves SPF security by obfuscating your sending infrastructure
- Eases bulk management of multiple domains that use the same sending infrastructure

Hosted DKIM

- Simplifies configuration and management of DKIM selectors and keys
- Provides flexible hosting options for DKIM selectors (delegated or non-delegated)
- Supports DNS Security Extensions (DNSSEC)
- Allows simple import of DKIM selectors and public keys

Hosted DMARC

- Simplifies configuration and management of DMARC records for your domains
- Supports DNSSEC
- Allows simple import of existing DMARC records

Comprehensive Brand Protection

To protect your brand, Email Fraud Defense stops fraudulent emails from being sent using your trusted domains.

Identify lookalikes of your domains

Email Fraud Defense uses domain registration information from Proofpoint Domain Discover. It detects domains posing as your brand in email attacks or on phishing websites. Proofpoint analyses millions of domains and connects registration data with our own data on email activity and attacks. We show you suspicious domains and how attackers are spoofing your brand. We also alert you when suspicious domains become active.

The Proofpoint Takedown add-on reduces exposure of your consumers, partners and employees to lookalike domains. You can pursue removal of a malicious domain with the domain registrar or the hosting, content delivery network (CDN) or email provider. You can also export domains to be blocked at the Proofpoint email gateway.

360-degree visibility across your email ecosystem

Email Fraud Defense shows all emails sent using your trusted domains. These include emails to consumer mailboxes, business gateways, and your own gateway.

Our dashboard shows which of your domains attackers have tried to hijack and the abuse rate of each one. It shows authorised senders and their DMARC records as well as your policies and pass rates for SPF, DKIM and DMARC.

Email Fraud Defense gives you actionable insights and recommendations. You don't have to worry about failing DMARC or blocking valid emails while stopping attackers.

Visibility of Supplier Risks

Email Fraud Defense goes beyond DMARC setup to also show your supplier risks. Nexus Supplier Risk Explorer identifies your suppliers, checks their DMARC records and shows their risks. Our product shows you messages delivered from lookalike domains. By prioritising alerts based on risk levels, we help you to focus on the most critical incidents.

Integration with Proofpoint Email Gateway

Email Fraud Defense works with the Proofpoint email gateway to enforce DMARC on inbound traffic. It helps you verify the DMARC reputation of a domain, so your gateway doesn't block valid email that failed DMARC. It also helps you create override policies for valid email without reducing your security posture.

DMARC Visibility for Microsoft 365

If you use Microsoft 365 with your mail exchange (MX) records pointed to Microsoft's inbound servers, Email Fraud Defense can still show the DMARC compliance of your domains. This visibility helps you to enforce DMARC on inbound traffic from your domains with confidence.

LEARN MORE

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