proofpoint.

Proofpoint Email Fraud Defense

KEY BENEFITS

- Simplify DMARC implementation by guiding you through each step of your rollout
- Protect your brand in email fraud attacks without blocking legitimate email
- Automatically identify your suppliers and the risk they pose
- Provide visibility into lookalike domains and emails sent using your trusted domains
- Integrate with industry-leading Proofpoint gateway to enforce DMARC with confidence and flexibility

Proofpoint Email Fraud Defense streamlines DMARC implementation with guided workflow and is supported by dedicated consultants. It protects your organization's reputation from email fraud attacks. And it provides full visibility into lookalike domains and emails being sent using your domain—including third-party senders. Email Fraud Defense also lets you mitigate risks posed by suppliers by automatically identifying your suppliers and lookalike domains registered by third parties.

Organizations of all sizes and industries have lost more than $26 billion in email fraud attacks since 2016. Attackers use a range of identity deception tactics, such as domain spoofing and lookalike domains, to lure victims into making fraudulent wire transfers. And among various types of email scams, supplier invoicing fraud often accounts for the most significant financial loss due to large B2B payments.

Deploying email authentication can help protect against impostor threats. But implementing DMARC (Domain-based Message Authentication, Reporting and Conformance) can be a lengthy, complex process. And it introduces the risk of interrupting legitimate mail flow.

Email Fraud Defense simplifies your DMARC journey by guiding you through your entire deployment. We authenticate all emails delivered to and sent from your organization without blocking legitimate email. We protect your brand from email fraud attacks and mitigate risks of inbound impostor threats. With Email Fraud Defense, you can better protect your customers, business partners and even employees against business email compromise (BEC) scams—restoring trust in your email.

Ease of Use

Dedicated consultants and guided workflow

As an Email Fraud Defense customer, you get an industry-leading solution with world-class support. From day one, we create a project for you with guided workflow. Our consultants who consistently receive superior Net Promoter Scores (NPS)[1] help you through every step of your rollout.

We work with you to identify all your legitimate senders—including third-party senders—to ensure they authenticate properly. Our consultants make recommendations to help you prioritize tasks based on your needs and criteria like email volume and top senders by analyzing your unique email environment. With our proven implementation plan, you can fully deploy email authentication without the usual headaches. And you can see the value from your Proofpoint investment sooner.

---

1 NPS is world's leading metric for measuring customer satisfaction and loyalty. According to global benchmark data, the average NPS score is +32. Proofpoint Email Fraud Defense consultants obtain an NPS of +90.

Hosted SPF

Email Fraud Defense includes the Hosted SPF service. It helps you overcome the traditional DNS lookup limit of 10 and reduces overhead of making changes to the SPF record. Rather than the traditional 72-hour delay for global propagation, Hosted SPF updates records in real-time. It also improves SPF security by preventing attackers from easily using your publicly discoverable SPF record to abuse your domain.

Comprehensive Brand Protection

Email spoofing and lookalike domains are common business email compromise attack tactics. Attackers use a company's brand to steal money or sensitive information from the victims. Email Fraud Defense prevents fraudulent emails from being sent using your trusted domains. We protect your brand and organization's reputation in email fraud attacks.

Identify lookalikes of your domain

Leveraging information from Proofpoint Domain Discover, Email Fraud Defense automatically identifies lookalikes of your domains. We dynamically detect newly registered domains posing as your brand in email attacks or by phishing websites. We analyze millions of domains and connect registration data with our own data on email activity and active attacks. And so we provide a full view of suspicious domains. We show you how attackers are impersonating your brand. You receive instant alerts when suspicious domains move from parked to a live, weaponized state.

With the Virtual Takedown add-on, you can quickly reduce consumer, business partner and employee exposure to malicious lookalike domains. And you can pursue removal of the domain with the registrar or hosting provider. You can also export domains to be blocked at the Proofpoint email gateway.

360-Degree visibility across your email ecosystem

Email Fraud Defense gives you unmatched visibility into all emails sent using your trusted domains. That includes those that are destined for consumer mailboxes, business gateways and your own gateway. None of other security tools or public data sources can provide such visibility.

Our comprehensive dashboard shows you:

- Which of your domains attackers have attempted to hijack
- The abuse rate of each domain
- Your DMARC, SPF and DKIM pass rate and policies
- Authorized senders and their DMARC records

Unlike other solutions that only show you numbers on a dashboard, Email Fraud Defense provides you with actionable insights and recommendations. You can better track, manage and take actions on open tasks. With Email Fraud Defense, you don't have to worry about failing DMARC or blocking valid emails while preventing attackers from spoofing your domains.

Visibility into Supplier Risks

Email Fraud Defense goes beyond DMARC implementation by providing visibility into your supplier risk. The Nexus Supplier Risk Explorer feature automatically identifies your suppliers, validates their DMARC records and uncovers the risk they pose to your organization. That includes impostor threats, phishing, malware and spam. We reveal the message volume and the messages delivered from the lookalikes of your suppliers' domain. And you can further investigate any potential threats. By prioritizing each supplier's domain's risk level, we help you focus on the most critical incidents.

Tight Integration with Proofpoint Email Gateway

We are the only security vendor that provides true integration between email authentication and secure email gateway. When combined with the industry-leading Proofpoint email gateway, Email Fraud Defense allows you to effectively mitigate risks of impostor threats by enforcing DMARC on your inbound traffic with confidence and flexibility. We help you verify the DMARC reputation of a specific domain, so your gateway doesn't block legitimate email that fails DMARC for whatever reason. We also help you create override policies for valid email without compromising your security posture. Together, your employees are better protected against email fraud attacks.

LEARN MORE

For more information, visit **proofpoint.com/us/products/email-fraud-defense**.

proofpoint.