proofpoint

SOLUTION BRIEF

Proofpoint Impersonation Protection

Protect your communications with trusted partners, customers, and suppliers

Key Highlights

- **Protect your trusted business communications from impersonation threats**
- **Prevent you and your brand from impersonation abuse**
- **Monitor for malicious lookalike domains and get them shut down**
- **Detect and defend against risky suppliers, including compromised supplier accounts**
- **Secure email sent on your behalf by applications, devices, SaaS platforms, and AI agents**
- **Powered by Nexus® AI, machine learning, LLMs, and behavioral analysis**

Most organizations rely on email to do business. But attackers have figured out how to hijack trusted business communications, and generative AI has made those attacks faster, more convincing, and easier to scale. They can impersonate your organization, your brand, or your business partners and create credible messages and websites in minutes instead of hours.

According to the FBI's Internet Crime Complaint Center, business email compromise (BEC) consistently generates billions of dollars in losses each year, with losses continuing to climb year over year. The FBI has also begun tracking AI as a distinct threat factor, attributing tens of millions of dollars in BEC losses specifically to attacks with a confirmed AI component—and cautions that this figure likely understates the true scope.

These attacks often combine multiple impersonation tactics, including spoofed domains, lookalike domains, and compromised supplier accounts. Together, they put communications with trusted partners, customers, and suppliers at risk—and make it harder for recipients to distinguish legitimate messages from fraudulent ones.

Proofpoint takes a holistic, multilayered approach to protecting your organization and brand from impersonation abuse. We provide the tools, technology, and resources to authenticate user-generated and application email, secure messages sent on your behalf, identify risky or potentially compromised supplier accounts, and monitor for malicious lookalike domains so they can be taken down.

Protect Your Brand from Impersonation

One of the most common impersonation tactics is domain spoofing, and generative AI has made spoofed messages faster to produce and harder to distinguish from the real thing. Without the right security controls in place, attackers can easily steal your trusted domains and use AI to craft highly convincing messages at scale. This allows them to target your customers, partners, and even your employees with a level of speed and polish that didn't exist even a year ago. Email authentication is the most effective way to stop it.

Proofpoint Impersonation Protection simplifies DMARC implementation by guiding you through each step of your rollout and enables both your user and application email to be authenticated. Our experts work with you to identify your legitimate senders. They also ensure that all of your email—including those from third-party authorized senders—authenticates properly.

Integration with Proofpoint Threat Protection allows you to enforce DMARC authentication for inbound messages with confidence. It adds a layer of defense against AI-generated impersonation attempts that spoof your trusted domains. It also lets you override DMARC policies without blocking legitimate email or compromising security with safelisting. This integration gives you visibility into both inbound and outbound email traffic. You can see all the emails sent that use your trusted domains, including those sent by third parties and, increasingly, by AI agents acting on your behalf.

Defend Against Compromised Supplier Accounts

Attackers are increasingly exploiting the supply chain to compromise trusted business communications. They often use compromised supplier accounts to hijack email threads between you and your business partners. Generative AI can help them study prior conversations and mimic a supplier's writing style, making fraudulent messages harder to detect. And because these emails may come from legitimate supplier accounts and contain no malicious payload, they can evade traditional authentication and detection controls. The result can be significant financial loss, data theft, extortion, or ransomware.

Proofpoint Impersonation Protection helps you detect and defend against risky suppliers, including potentially compromised accounts. It uses behavioral AI, machine learning, and threat intelligence from across Proofpoint's large customer footprint to uncover signs of supplier compromise, including attacks where generative AI is used to craft more convincing lures. Adaptive controls, such as automatic URL isolation, help reduce exposure to threats from compromised senders. And integration with Proofpoint Threat Protection, combined with context around sender-recipient relationships, helps streamline third-party incident response and investigation.

Detect and Remove Malicious Sites, Including Lookalikes

Bad actors build websites that are purpose-built for attacks. Some impersonate other organizations, brands, or institutions to trick your employees, customers, or partners into trusting them. Others imitate your own organization, using domains and pages that closely mirror your logo, layout, and brand experience. Generative AI has made both kinds of attacks easier to produce, harder to spot, and faster to scale. Bad actors use these sites in credential phishing, BEC, telephone-oriented attack delivery (TOAD), and other schemes that depend on a convincing digital presence.

With Proofpoint Impersonation Protection, we continuously monitor for newly registered domains that may impersonate your organization and provide the context needed to assess potential risk.

Detection is just the first step. When you submit a suspicious site to our Takedown Team, we investigate it, collect available evidence, and work to mitigate malicious activity and remove the site. We maintain relationships across a broad network of internet infrastructure providers and trusted partners, including registrars, hosting providers, email service providers, blocklist partners, and more.

Our team manages the takedown process on your behalf, so you don't have to determine whom to contact or what documentation is required. Our takedown services extend beyond lookalike domains to support mitigation for malicious subdomains and URLs, as well as non-lookalike domains.

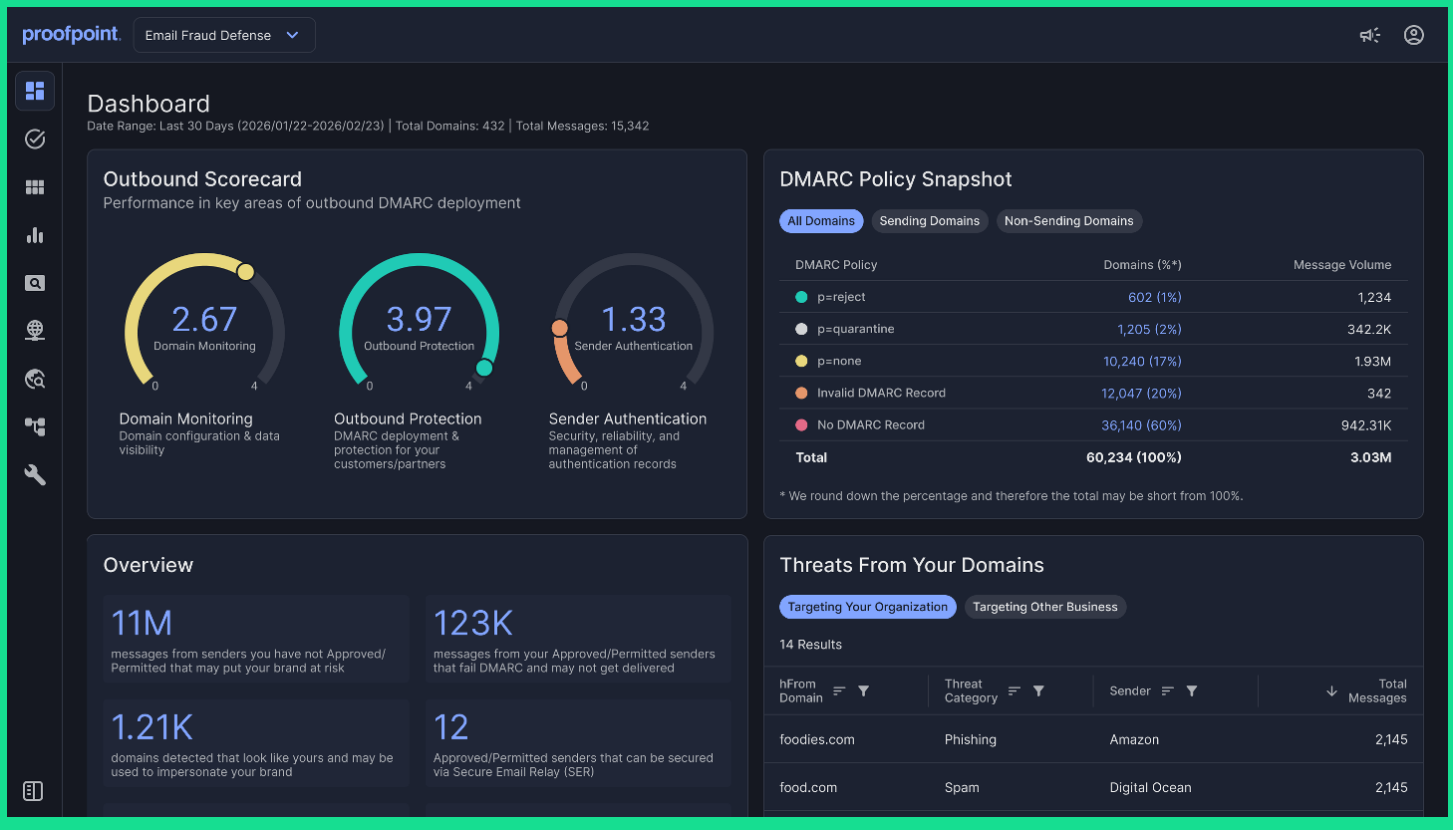

Figure 1.Proofpoint gives you visibility into domain spoofing threats, malicious lookalikes of your domains, as well as emails being sent using your trusted domains.

Secure Email Sent on Your Behalf

Not all email leaving your domain comes from a person typing a message. HR platforms send payroll notices, CRM tools send customer receipts, office devices send scan-to-email and fax notifications, and AI agents are beginning to generate messages on your behalf. Each source can become an opening for abuse. If an application, device, or sending service is compromised, attackers can use that trusted channel to send malicious email that appears to come from you, passes authentication checks, and—when enhanced with generative AI—looks more convincing than ever.

Proofpoint Impersonation Protection closes this gap with a secure, dedicated relay for automated senders that use your domains, from internal apps and office devices to SaaS platforms and AI agents. It accepts mail only from verified, authenticated sources, applies advanced anti-spam and antivirus scanning to every message, and DKIM-signs approved mail. This helps your outbound sources support DMARC alignment and SPF compliance without disrupting legitimate mail flow. SER also isolates this traffic behind dedicated, reputable IPs, helping protect your sending infrastructure and brand reputation from bad actors who might otherwise piggyback on your domain's trust.

Gain Visibility, Control, and Compliance Support

Proofpoint Impersonation Protection gives you centralized visibility and control over high-volume sending services, such as Amazon SES. You can see what is leaving your domain in bulk and trace messages back to the application, device, or AI agent that sent them. Optional encryption and data loss prevention help safeguard sensitive data, including personally identifiable information (PII) and protected health information (PHI), in transactional messages. These controls can support compliance with frameworks and regulations such as HIPAA, SEC, and FINRA requirements.

Proofpoint Impersonation Protection also helps you align with major inbox-provider requirements for sender identity and message integrity for bulk senders. With support for unsubscribe headers and centralized list management, it helps legitimate email continue reaching the inbox.

Learn More

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

proofpoint.