Proofpoint Secure Email Relay

Prevent compromised third-party senders from sending suspect email from your domain

Key Benefits

- Secures application email from SaaS providers, such as ServiceNow, Salesforce, and Workday, that send on your behalf
- Accelerates DMARC implementation by enabling third-party senders to achieve DMARC compliance
- Secures your trusted domain from abuse involving compromised senders and vulnerable email service providers whose IPs are in your SPF records
- Protects sensitive data in application email with payload encryption and DLP
- Replaces on-premises relays with a secure, cloud-based alternative
- Prevents disruption of user mail by isolating it from your application mail
- Lets you send your own invoices securely

Proofpoint Secure Email Relay (SER) secures cloud applications that send emails on your behalf. A hosted solution, it shrinks the attack surface around identity takeover by scanning every application email that flows through the system before it sends them out to the internet. Proofpoint SER prevents compromised third-party senders from sending malicious email using your domain. And it reduces threat risk by letting only credentialed senders use the service. By streamlining cloud application sender authorisation, Proofpoint SER lets you meet DMARC compliance more efficiently.

Applications are moving from on-premises systems to the cloud. This migration can expand the attack surface of your organisation. Emails sent "as you" can come from third-party app senders that you do not control. The setup leaves email identities vulnerable to spoofing. Without proper controls in place, attackers can easily steal your company's identity. They can abuse the authorised senders' cloud environments. Afterward, they can send malicious email authorised as you. These messages would pass SPF/DKIM/DMARC. And they can be sent directly to your customers, partners and employees.

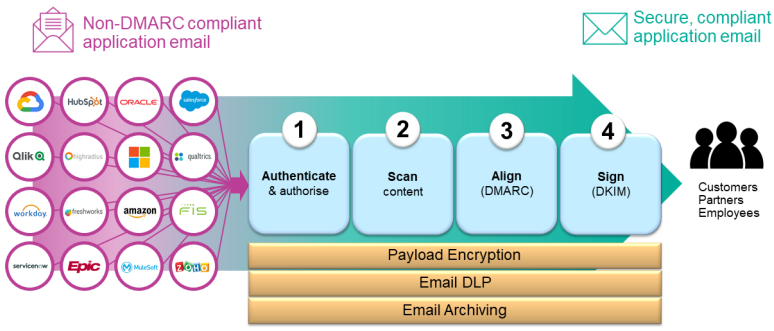

Figure 1: Proofpoint Secure Email Relay secures cloud apps that send transactional email as you and lets you apply security controls such as encryption and DLP to your application email.

Proofpoint SER brings our security and compliance controls to bear on application transactional emails that use your identity.

Examples of transactional email include:

- Statement notifications
- Package delivery notifications
- Order confirmations
- Electronic sales receipts
- Generated insurance quotes
- Experience or feedback requests
- Task notifications
- IoT or device alarm notifications
- Alerts/emergency management

Proofpoint SER makes DMARC easier by DKIM-signing all email. It evaluates emails using anti-spam/virus technology. And it reduces risk with sensitive data by letting you apply payload encryption and email DLP. Proofpoint SER puts you in control of your email identity. It ensures your customers, partners and employees only receive authentic email from you.

Secure Email from Vulnerable Environments

Application email and email service providers can be authorised to send email using your domains. But they often don't adhere to security best practices. This could lead to account compromise or platform abuse. And in both cases, bad actors can use your trusted domains to send malicious email that passes email authentication.

Proofpoint SER adopts a closed system that lets only verified business entities use our email relay service. Random users can't register for free accounts on our platform. This greatly reduces the risk posed by vulnerable or compromised email service providers.

Proofpoint SER also securely accepts email from your authorised applications via SMTP Authentication and TLS (STARTTLS). It applies Proofpoint anti-spam/virus measures to each message. Proofpoint SER blocks any email that wants to send authorised malicious email as you. You can also consolidate application email behind trusted, reputable IPs. These can obfuscate application senders who send email as you from bad actors.

Accelerate DMARC Implementation

Some SaaS providers don't support DKIM-signing. You can have single-passing DMARC based on SPF alone. But without DKIM, your legitimate email lacks the authentication redundancy required. This makes it hard to survive forwarding, for example. Proofpoint SER enables SaaS providers to meet DMARC compliance by DKIM-signing their email and distributing it to the Internet in a DMARC-compliant fashion. This lets you achieve DMARC reject policies on your domains more rapidly so bad actors can no longer spoof them.

Adhere to Application Email Regulatory Compliance

Applications are migrating to the cloud. As they do, organisations are often left with less-than-ideal email options from a regulatory-compliance point of view. Some route application email through on-premises systems. But doing so exposes them to vulnerable external environments. Some cobble together cloud-based point solutions. But these often lack a consolidated view into activities.

Proofpoint SER lets you meet regulatory compliance standards with your application email. Email from applications with access to personally identifiable information (PII) and personal health information (PHI) can be transport- and/or payload-encrypted. SER also lets you apply data loss prevention (DLP) and archiving solutions to your application email, so it complies with SEC/FINRA regulations.

LEARN MORE

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