

Proofpoint Secure Email Relay

A better solution for controlling and securing transactional emails from applications and SaaS partners

Key Benefits

- Secures transactional email from internal applications as well as SaaS providers such as Salesforce, ServiceNow and Workday.
- Accelerates DMARC implementation by enabling DKIM signing of emails from all sources prior to sending
- 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 emails, such as personally identifiable information (PII) and personal health information (PHI), 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

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



Proofpoint Secure Email Relay (SER) consolidates and secures transactional emails. It prevents compromised third-party senders from sending malicious email using your domains and enables DKIM signing to help you meet DMARC compliance. As a hosted solution, Proofpoint SER helps you achieve your cloud migration initiatives.

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

Proofpoint SER brings our security and compliance controls to bear on application transactional emails that use your identity. These kinds of emails originate from internal apps or third-party SaaS partners such as Salesforce, ServiceNow and Workday. They include invoices, authentication codes, confirmations and the like. They may be isolated from user-generated email, but Proofpoint SER still affords them the same levels of protection.

Proofpoint Secure Email Relay

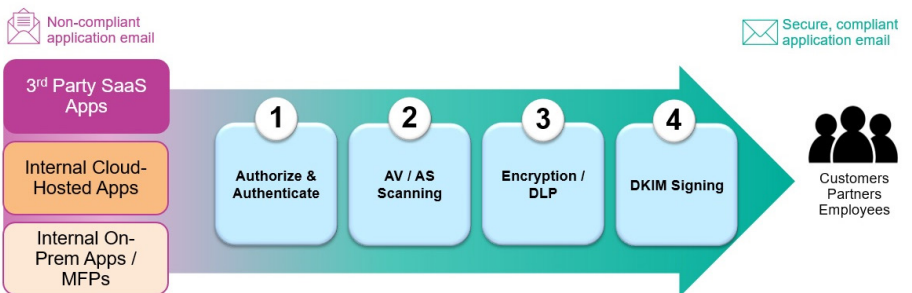


Figure 1: Ensure secure, clean and compliant transactional email.

Other 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 authorized 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 authorized 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 authorized 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 application or 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 required authentication redundancy. This makes it hard to survive forwarding, for example. Proofpoint SER enables these transactional emails to fully meet DMARC compliance by DKIM-signing messages prior to sending. 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, organizations 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.

Proofpoint offers optional application owner support, migration planning and execution, and post implementation deliverability services for Secure Email Relay.

LEARN MORE

For more information, visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. [Proofpoint.com](https://proofpoint.com)