proofpoint.

SOLUTION BRIEF

# Proofpoint Secure Email Relay

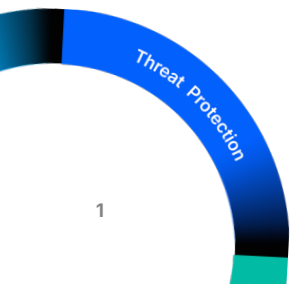
Advanced security and control for transactional emails



## Key Features

- Accepts email only from authorized applications, devices or third-party senders
- Performs antivirus and anti-spam scans on outbound emails to reduce the attack surface from application-generated traffic
- Automatically applies DKIM signatures and aligns SPF/DKIM so that your application emails pass DMARC, which is essential for authenticating email and protecting your brand
- Optionally supports encryption, data loss prevention (DLP) and archiving for handling sensitive data like PII and PHI
- Eliminates the need for on-premises relays by providing scalable, cloud-native email routing—ideal for SaaS-heavy environments
- Enables you to manage, monitor and disable email from third-party services using your domains

This solution set is part of Proofpoint's integrated human-centric security platform, mitigating the four key areas of people-based risks.




## Protecting your sending IPs is mission-critical

Whether to reduce costs, simplify infrastructure or as part of a cloud migration, email being generated by applications has made its way into your Proofpoint on Demand (PoD) environment—and it's putting your sending IPs at risk.

One of these risks is creating an open-relay situation that bad actors can exploit. Another is the risk of blocklisting, which can occur when application traffic is sent in large volumes over a short period of time, triggering spam detection systems. With your user and application emails merge, if your domains get blocklisted, then all your email traffic stops, and your business operations come to a halt.

## Use the right solution for the job

The most effective way to reduce risk and optimize performance is to use a separate environment that's built for handling application-generated email. That way, you get a high level of security plus enhanced features, such as the option of adding one-click unsubscribe as well as specialized reporting.

Proofpoint Secure Email Relay (SER) is a cloud-based solution that's designed for application-generated email. With Proofpoint SER, your organization gets a centralized solution to better manage all the applications and third-party SaaS partners that are sending email from your domains.

## Benefits of Proofpoint Secure Email Relay

**Protect deliverability.** You get separate, dedicated IPs that isolate your application-generated email from your user email environment. This not only improves performance, but it also reduces the risk of having all your email blocked. DKIM signing of all outbound messages ensures it meets email authentication requirements such as DMARC. And SER enables you to insert one-click unsubscribe links into message headers to meet requirements for Google, Yahoo, Apple and Microsoft bulk mail.

**Improve security.** All outbound emails are scanned for malicious content to reduce the attack surface from application-generated traffic. Optionally, SER supports encryption, data loss prevention (DLP), and archiving for handling sensitive data, such as personally identifiable information (PII) and personal health information (PHI).

**Centralize control**. SER provides centralized control for all application email, including messages that are sent on your behalf by third-party SaaS partners. All sending sources must be authorized, which eliminates an open relay situation. And with SER's cloud connector API, developers have a single, secure and consistent way to enable applications to send email.

**Enhance visibility.** You get separate reporting that's designed for application email. As a result, you get deeper insight into sending sources and volumes, as well as simplified troubleshooting.



©Proofpoint, Inc. 2025