

Proofpoint SER + Amazon SES

Increase email security and control for AWS apps and AI agents

Integrate SER and SES Seamlessly

Secure Email Relay (SER) gives AWS developers one approved way to send email. It also gives security teams centralized visibility, policy enforcement, and compliance controls. The result is less complexity and better governance, with application- and AI-generated email that stays secure, authenticated, and aligned with your policies. Developers don't need to change their existing workflows.



AWS App

Approved identities and code paths



Amazon SES

Scalable SMTP or API submission



SES Mail Manager

Conditional routing to enterprise controls



Proofpoint SER

Threat, DLP, DKIM and policy controls



Recipients

Deliver directly or back via SES

Best Practice:

One approved path for AWS application email, with enterprise controls before delivery.

Benefits of Standardizing on Amazon SES + Proofpoint SER

Developer Velocity

Give teams a repeatable AWS-native pattern instead of custom relays and one-off SMTP configurations.



Centralized Governance

Control approved accounts, domains, senders, policies, and reporting from one enterprise layer.



Domain Protection

Limit corporate-domain sending to authorized sources and reduce abuse from vulnerable apps or third parties.



DMARC Readiness

Apply consistent DKIM signing and alignment to move application email toward DMARC enforcement.



Security Inspection

Scan for malware, spam, sensitive data, and policy violations before messages are delivered.



Cloud Modernization

Retire legacy on-prem relays while preserving control, scale, visibility, and compliance posture.



Customer Outcome

With this approach, developers keep using Amazon SES while security teams enforce Proofpoint SER controls for policy, authentication, data protection, and domain trust. The result is a scalable, AWS-native email standard built for both speed and security.

Take Control of Application Email