



Proofpoint Smart Send

Self-Remediation for Email Policy Violations

Proofpoint Smart Send™—included in the Proofpoint Enterprise Protection™ and Proofpoint Enterprise Privacy™ email security and data loss prevention solution suites—provides a powerful, easy-to-administer self-remediation tool that lets email end users remediate outbound email policy violations, such as inadvertent violations of data loss prevention or outbound spam detection policies.

About Proofpoint Smart Send

An integral feature of both Proofpoint Enterprise Suites, Proofpoint Smart Send provides powerful self-remediation tools for DLP and outbound spam detection.

Proofpoint Enterprise Privacy Suite

- Email Firewall
- Regulatory Compliance
- Digital Asset Security
- Encryption

Proofpoint Enterprise Protection Suite

- Dynamic Reputation
- Email Firewall
- Spam Detection
- Zero-Hour Anti-Virus
- Virus Protection

Outbound email policies and the need for self-remediation

The vast majority of data loss incidents are non-malicious and inadvertent. Many organizations that enforce various outbound email policies (including data loss prevention, regulatory compliance, and outbound spam/virus scanning policies) desire a way to let email senders remediate their own policy violations in certain situations.

Allowing this type of “self-remediation” can save significant IT and compliance resources, as administrators do not have to review each incident. At the same time, self-remediation techniques help to educate email senders about their organization’s outbound email policies and empower them to correct common errors.

Self-remediation features are also useful for organizations that use Proofpoint products for outbound spam and virus scanning features. In the case of outbound false positives (legitimate outbound email messages that are inadvertently marked as spam), senders need a convenient way to release such messages, without administrator intervention.

Proofpoint Smart Send: Flexible self-remediation features

Proofpoint Smart Send allows administrators to easily create customizable self-remediation policies. Policies can be configured to notify email senders when a message that they have sent violates a data loss prevention policy. The original message is temporarily held in quarantine until the end user has the opportunity to take a remediation action, such as reviewing and approving the message for release, choosing to send the message encrypted, or accepting that the message was in violation (blocking the message).

If Proofpoint Smart Send is enabled for outbound spam scanning rules, email senders can be notified if a message they have sent was flagged as spam and can release such messages, as appropriate.

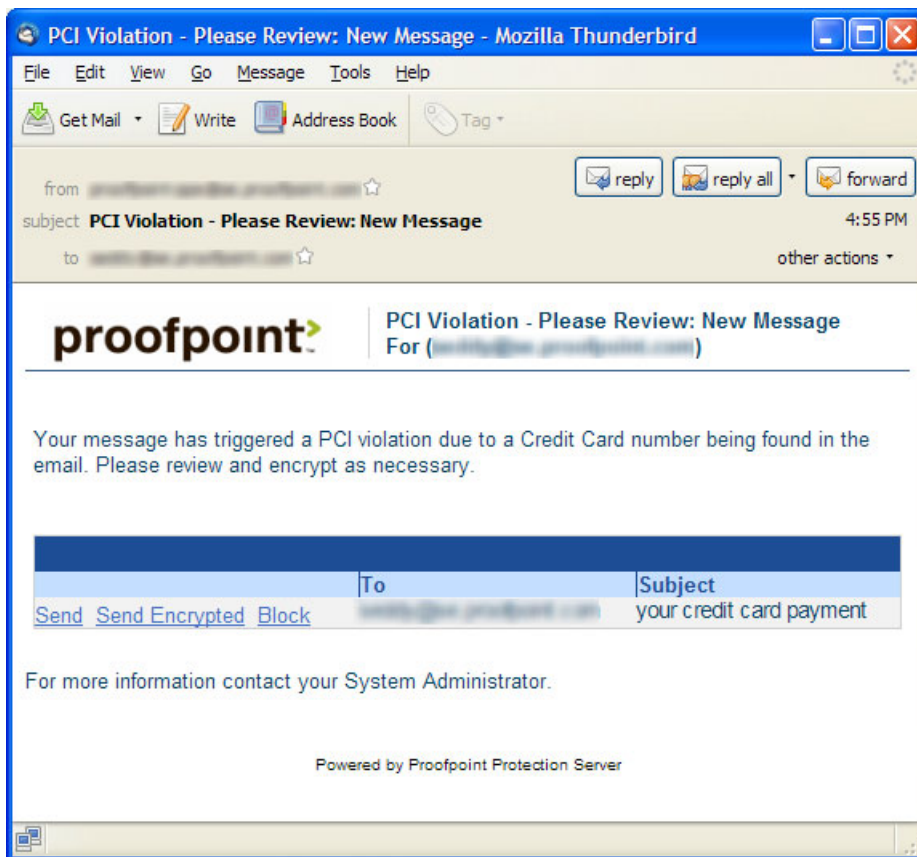
Simple to administer, with full control

As with all of Proofpoint’s email security product features, self-remediation policies are managed and enforced on an enterprise level from a single location. Once defined, these policies are applied automatically at the gateway, eliminating the risk of user error.

Proofpoint Smart Send

Administrators have complete control over Proofpoint Smart Send features and can choose whether or not self-remediation should be allowed for any given outbound policy rule. Additionally, administrators can ensure that certain users or groups of users can never remediate their own violations, regardless of how a given rule is configured.

Configuration options also allow administrators to control how long a message is temporarily quarantined and what happens to quarantined messages if users do not take any self-remediation actions.



Administrators may opt to encrypt messages on-the-fly with policy-based encryption or enable Proofpoint Smart Send to allow the end user to determine the final remediation.

Auditing features provide complete visibility into Proofpoint Smart Send actions

Allowing email senders to remediate their own policy violations doesn't mean loss of control. Built-in auditing features give administrators complete visibility into how email senders are using the self-remediation features.

All sender-remediated messages can be stored in a separate folder for administrators to review, depending upon their organization's customized policies.

Included in Proofpoint Enterprise Protection and Proofpoint Enterprise Privacy

Proofpoint Smart Send features are included in the Proofpoint Enterprise Protection email security and Proofpoint Enterprise Privacy data loss prevention suites at no extra charge.

About Proofpoint

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.

Proofpoint, Inc.
892 Ross Drive
Sunnyvale, CA
94089

1.877.647.6488