Product Brief

PGP® Gateway Email Encryption

Policy-Based Protection for Outbound Email

At a Glance

Protect sensitive outbound email with policy-based encryption and no client-side software required.

Business Outcomes

- Reduce the risk and impact of outbound email exposure
- Strengthen compliance and audit readiness
- Enable secure collaboration without adding user friction
- Improve email security through integrated protection workflows

Solution Capabilities

- Policy-based gateway encryption
- No client-side software required
- Secure external recipient access
- Integrated policy enforcement and threat protection

Overview

Email remains one of the most common ways sensitive information leaves the organization, whether through everyday collaboration with customers and partners or simple user errors such as misdirected messages or incorrect attachments. While traditional email security focuses on inbound threats, many organizations still lack consistent, automated protection for outbound messages containing regulated or confidential data. Symantec® PGP® Gateway Email Encryption addresses this gap by encrypting email at the gateway based on centrally managed policies, without requiring client-side software or changing how users work. The result is stronger protection for sensitive email, simpler compliance with data privacy regulations, and more seamless secure collaboration with external recipients.

Beyond Basic Email Protection

Some organizations respond to email risk by encrypting every outbound message, but that approach can create unnecessary friction for users and recipients while still failing to focus protection where it matters most. Blanket encryption does not distinguish between everyday traffic and emails that contain regulated data, confidential financial information, or sensitive customer records, and it can complicate collaboration with external recipients who do not have compatible tools.

To reduce risk without disrupting normal business communication, enterprises need email encryption that is both automatic and selective. Policy-based controls in PGP Gateway Email Encryption allow outbound messages to be encrypted based on content, sender, recipient, or other criteria, eliminating the need for end users to make the right choice each time they send an email. This criteria helps ensure that messages carrying sensitive information receive strong protection, while routine email continues to flow with minimal change to user experience.

Introducing PGP Gateway Email Encryption

PGP Gateway Email Encryption provides a centralized, policy-based approach for securing outbound email communications. There are no requirements for client-side software or a need for users to encrypt messages manually. By applying customizable rules at the email gateway, the solution helps organizations automatically protect sensitive content as messages leave the environment.

The solution is designed to support secure collaboration both inside and outside the organization. Recipients can access protected messages through a web inbox or other supported delivery methods without needing PGP software, making it easier to secure communications with customers, partners, and other external stakeholders. When integrated with Symantec Data Loss Prevention and Symantec Messaging Gateway, PGP Gateway Email Encryption can also strengthen policy enforcement and add protection against malware, spam, and other email-borne threats.

Solution Capabilities

PGP Gateway Email Encryption delivers several core capabilities that work together to protect sensitive outbound email without disrupting how users work:

- **Policy-based gateway encryption:** Automatically encrypt outbound messages based on configurable rules that consider content, sender, recipient, and other criteria, reducing reliance on users to decide when to encrypt. Encryption and decryption occur at the gateway, helping to ensure consistent protection as email leaves the organization.
- **No client-side software required:** Apply strong email encryption without installing software on user devices or changing their everyday workflows. Users continue to send email as usual while the gateway enforces encryption policies behind the scenes.
- **Secure external recipient access:** Allow external recipients to view encrypted messages through a secure web inbox or as protected PDFs, without needing PGP software or preshared keys. This supports secure collaboration with customers, partners, and other third parties while keeping the user experience straightforward.
- **Integrated policy enforcement and threat protection:** When paired with Symantec Data Loss Prevention and Symantec Messaging Gateway, PGP Gateway Email Encryption can automatically encrypt messages that match DLP policies and combine that protection with antivirus, malware, and spam filtering. This integration helps organizations strengthen policy enforcement and maintain a more complete audit trail for compliance and security investigations.

Enterprise Use Cases

- **Protecting sensitive outbound communications:** Automatically encrypt emails containing financial information, health data, customer records, legal documents, or other sensitive content before they leave the organization. This automation helps to reduce the risk of exposure caused by user error, misdirected messages, or inconsistent manual encryption practices.
- **Enabling secure collaboration with external recipients:** Secure communications with customers, partners, suppliers, and other third parties without requiring them to install PGP software or exchange keys in advance. Web inbox and protected PDF access options make encrypted communication easier for a wide range of recipients.
- **Enforcing policy-driven email protection at the gateway:** Integrate with Symantec Data Loss Prevention and email security controls to automatically inspect outbound messages and apply encryption when policy conditions are met. This integration helps organizations protect sensitive data more consistently while strengthening auditability and reducing dependence on end-user decisions.

Business Outcomes

- **Reduce the risk and impact of outbound email exposure:** Automatically encrypting sensitive messages at the gateway helps reduce the likelihood that misdirected emails, user error, or inconsistent encryption practices will expose confidential information.
- **Strengthen compliance and audit readiness:** Policy-based encryption, centralized control, and integration with a FIPS 140-2-validated cryptographic module help organizations apply consistent protections and meet regulatory and audit requirements for sensitive email communications.
- **Enable secure collaboration without adding user friction:** By encrypting email without client-side software and giving recipients access through a web inbox or protected PDFs, organizations can protect sensitive communications while keeping interactions with customers, partners, and other external stakeholders straightforward.
- **Improve email security through integrated protection workflows:** When combined with Symantec DLP and Symantec Messaging Gateway, PGP Gateway Email Encryption can help organizations automate policy enforcement and add antivirus, malware, and spam protection to outbound email workflows.

Why Symantec Software?

The Broadcom Symantec division combines proven PGP encryption technology with a scalable, policy-driven approach for protecting sensitive communications across enterprise environments. With more than 30 years of experience protecting sensitive data, Symantec software brings the maturity, operational depth, and enterprise focus organizations need to secure high-risk communication channels such as outbound email.

PGP Gateway Email Encryption also fits into a broader Symantec encryption and data protection portfolio, allowing organizations to extend protection beyond email when needed while maintaining centralized policy control and stronger governance. Native integration with Symantec Data Loss Prevention and Symantec Messaging Gateway further strengthen the platform by combining automated encryption with policy enforcement, auditability, and protection against spam, malware, and other email-borne threats.

BROADCOM®

For more information, visit our website at: www.broadcom.com

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

EMA-ENC-PB100 July 21, 2026