Product Brief

PGP® Encryption Suite

Endpoint, Email, and File Protection

At a Glance

Protect sensitive data across endpoints, removable media, desktop email, and shared files with centralized key and policy management.

Business Outcomes

- Reduce breach impact and data exposure
- Strengthen compliance and audit readiness
- Support secure hybrid work and collaboration
- Simplify encryption operations

Solution Capabilities

- Full-disk and device encryption
- Removable media encryption
- Desktop email encryption
- File and folder encryption

Overview

Organizations need to protect sensitive information beyond endpoint drives. Data is now created, stored, shared, and sent from laptops, desktops, removable media, desktop email clients, and shared file environments, creating more opportunities for exposure through user error, device loss, or unauthorized access. Symantec® PGP® Encryption Suite addresses this challenge with a consolidated solution that combines full-disk and removable media encryption, desktop email encryption, and file and folder encryption, with centralized key and policy management. The result is broader protection for endpoint-centric data, stronger compliance support, and simpler administration than isolated encryption tools can provide.

Beyond Full-Disk Encryption

Full-disk encryption plays an important role in protecting lost or stolen devices, but it does not address every way sensitive data is exposed in modern work environments. Once a user is authenticated, files can still be copied to removable media, shared through desktop email, or placed in shared folders and cloud-synced repositories where they may be accessed by unintended recipients or malicious actors. Organizations that rely solely on drive encryption may still face protection gaps as data is used, shared, and moved across business workflows.

To reduce those gaps, enterprises need encryption that extends beyond the device itself. That means protecting files and folders in shared environments, securing email before it leaves the user's desktop, and applying centralized policies and key management across these different use cases. By extending protection beyond the drive, organizations can better contain risk, support compliance, and simplify how sensitive data is secured across hybrid work environments.

Introducing PGP Encryption Suite

PGP Encryption Suite delivers a unified approach to protecting endpoint-centric data by combining full-disk and removable media encryption, desktop email encryption, and file and folder encryption into a single solution. Built on proven PGP encryption technology, the suite helps organizations secure sensitive data at rest and in motion while simplifying administration through centralized key management, policy enforcement, and compliance-ready reporting. By consolidating these capabilities under a single management framework, PGP Encryption Suite helps enterprises protect data more consistently across devices, email, and shared storage than isolated tools can.

Solution Capabilities

PGP Encryption Suite delivers four core capabilities that work together to protect sensitive data on endpoints, in email, and across shared storage locations.

- **Full-disk and device encryption:** Protect laptops and desktops with strong encryption to help prevent data exposure if devices are lost, stolen, or decommissioned. Centralized policies and key management streamline deployment and recovery for IT teams.
- **Removable media encryption:** Automatically encrypt data written to USB drives and other removable media so sensitive files remain protected when they leave the endpoint. Policy-based controls can require encryption, block unapproved devices, or allow read-only access where needed.
- **Desktop email encryption:** Secure email content and attachments before they leave the user's desktop, with flexible options for policy-based, automatic, or user-initiated encryption. Integrated key and certificate management helps keep the user experience simple while maintaining strong security controls.
- **File and folder encryption:** Apply persistent encryption to specific files and folders on endpoints and in shared locations so access remains controlled even as data is copied, synced, or moved. This helps protect sensitive information in collaborative and hybrid work environments where traditional perimeter controls are less effective.

Enterprise Use Cases

- **Protecting remote and mobile endpoints:** Encrypt data on laptops, desktops, and removable media used by remote and hybrid workers so sensitive information stays protected if devices are lost, stolen, or accessed outside corporate networks. This protection helps to reduce the impact of common incidents like misplaced devices, stolen hardware, or use over unsecured connections.
- **Securing sensitive email and everyday collaboration:** Apply desktop email encryption to messages and attachments containing financial data, health information, or intellectual property before they leave the user's endpoint. This practice reduces the risk of accidental exposure through misdirected emails or overshared content while supporting secure collaboration with customers, partners, and internal teams.
- **Safeguarding shared files and workspaces:** Use file and folder encryption to protect sensitive data stored in shared locations, synced folders, and local project directories. Persistent encryption helps ensure that only authorized users can access critical information, even as it is copied, synced, or moved across on-premises and cloud-based environments.

Business Outcomes

- **Reduce the impact of data loss and exposure:** Protecting endpoints, removable media, email, and shared files with encryption helps make stolen, misplaced, or misdirected data far less useful to unauthorized parties, reducing the severity of common breach scenarios.
- **Strengthen compliance and audit readiness:** Centralized key management, policy enforcement, and reporting help organizations apply encryption more consistently and demonstrate controls that support regulatory and internal compliance requirements.
- **Support secure hybrid work and collaboration:** By extending encryption beyond the device to email, removable media, and shared files, organizations can protect sensitive information more consistently across remote users, distributed teams, and mixed on-premises and cloud-connected environments.
- **Simplify encryption operations:** Consolidating multiple encryption use cases into a single suite reduces administrative complexity, improves policy consistency, and avoids the inefficiencies of managing separate point tools for device, file, and email protection.

Why Symantec Software?

The Broadcom Symantec division brings together proven PGP encryption technology, broad coverage across key enterprise data protection use cases, and centralized policy and key management in a single platform. With more than 30 years of experience protecting sensitive data, Symantec software helps organizations consistently extend encryption across endpoints, email, file shares, and data transfers, rather than relying on disconnected tools.

Native integration with Symantec DLP and Email Security further strengthens the platform's value by turning policy decisions into enforceable protection actions. For organizations navigating hybrid work, regulatory pressure, and growing data exposure risks, Symantec software offers a scalable and governable approach to protecting sensitive information wherever it lives or moves.

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.

PGP-ES-PB100 July 21, 2026