Product Brief

PGP® Command Line Encryption

Scriptable Encryption for Automated Data Workflows

At A Glance

Protect large volumes of sensitive data in automated workflows and file transfers with scriptable, policy-driven encryption.

Business Outcomes

- Reduce exposure in automated and high-volume data workflows
- Strengthen compliance and audit readiness
- Protect sensitive data with minimal disruption to existing systems
- Improve trust and integrity in machine-driven transactions

Solution Capabilities

- Scriptable encryption and digital signing
- Flexible integration with existing systems
- Protection for data in motion and at rest
- Centralized or local key management
- Authenticity, auditability, and secure handling

Overview

Organizations increasingly rely on automated workflows, scheduled jobs, and third-party applications to move, process, and generate large volumes of sensitive data. Many of these systems were not designed with built-in encryption, leaving information exposed during transfer between systems, when exchanged with partners, or when stored unencrypted after creation.

Symantec® PGP® Command Line helps organizations address these gaps by embedding strong encryption, decryption, signing, and verification into scripts and batch processes with minimal disruption to existing workflows. In addition to securing bulk data transfers, PGP Command Line can protect large volumes of stored data, such as files generated by third-party systems or archives that need to be encrypted once and retained securely over time. The result is more consistent protection for sensitive operational data, stronger compliance support, and a practical way to extend encryption into automated business processes.

Beyond Basic File Transfer Security

Many organizations focus on securing interactive file transfers or network connections, but leave the automated jobs and background processes that move and generate data with little or no protection. Scripts that pull reports, exchange files with partners, or move data to cloud services often run unattended, using legacy protocols that lack strong encryption or auditability. When those workflows handle regulated or business-critical data, they can become silent weak points in an otherwise modern security program.

To close these gaps, encryption has to be embedded directly into the processes that handle the data, not bolted on afterward. PGP Command Line enables teams to integrate encryption, decryption, and digital signing into scripts, schedulers, and third-party tools, so data is automatically protected whenever it is created, moved, or archived. That means bulk transfers, batch exports from third-party systems, and one-time encryption of archives such as email or log data can all be secured consistently, without re-engineering the applications that generate them.

Introducing PGP Command Line Encryption

PGP Command Line provides a flexible, scriptable approach to protecting sensitive data in automated workflows, batch processes, and large-scale operational environments. By enabling encryption, decryption, digital signing, and verification through command line scripts, it helps organizations secure data with minimal disruption to existing applications and business processes.

The solution can be integrated into a wide range of commercial and home-grown systems, making it practical for securing both data in motion and large volumes of stored data. PGP Command Line also supports local and centralized key management, digital signatures for authenticity and auditability, and broad integration with existing enterprise platforms, giving organizations a consistent way to extend strong encryption across automated services, file exchanges, archives, and other machine-driven workflows.

Solution Capabilities

PGP Command Line delivers core capabilities that help organizations extend strong encryption into automated workflows, large-scale data exchanges, and machine-driven storage processes.

- **Scriptable encryption and digital signing:** Encrypt, decrypt, sign, and verify individual files or collections of files through command-line scripts, helping secure batch jobs, automated transfers, and system-generated outputs without manual intervention.
- **Flexible integration with existing systems:** Add encryption commands to shell scripts and common scripting environments such as VB, .NET, Perl, and Python, or call the solution from other applications that can execute commands and pass parameters. This allows organizations to secure existing services and third-party workflows with minimal disruption to the applications themselves.
- **Protection for data in motion and at rest:** Use PGP Command Line not only to secure bulk data transfers between internal systems, customers, suppliers, and cloud services, but also to protect large volumes of stored data on servers, archives, backups, and other repositories. This supports use cases where files must be automatically encrypted upon creation or encrypted once for long-term retention.
- **Centralized or local key management:** Manage keys on a local keyring or integrate with the Symantec Encryption Management Server for centralized key management, reducing operational complexity and helping enforce stronger governance across automated environments.
- **Authenticity, auditability, and secure handling:** Apply digital signatures to verify sender authenticity and support audit trails, while also using capabilities such as secure file deletion and compression to improve how sensitive data is handled throughout its lifecycle.

Enterprise Use Cases

- **Secure automated data exchanges and integrations:** Embed encryption and digital signatures into scheduled jobs, ETL processes, and integration scripts that move large volumes of data between internal systems, partners, and cloud services. This helps prevent interception or tampering in machine-to-machine workflows that traditionally rely on unsecured file transfer protocols.
- **Protect system-generated files and archives at rest:** Automatically encrypt files produced by third-party applications or internal systems—such as reports, extracts, and log files—or apply one-time encryption to archives like email, backups, or historical data sets. This ensures that large volumes of stored data remain protected against unauthorized access, even if servers or repositories are compromised.

Why Symantec

Symantec combines proven PGP encryption technology with the flexibility enterprises need to secure automated workflows, high-volume data exchanges, and machine-driven processes at scale. With more than 30 years of experience protecting sensitive data, Symantec brings the maturity, cryptographic depth, and enterprise focus organizations need to extend encryption beyond user-driven workflows into operational systems and back-office environments.

PGP Command Line also fits within the broader Symantec encryption portfolio, enabling organizations to protect automated data flows as part of a more comprehensive strategy for endpoints, email, file shares, and data transfers. Support for centralized key management and integration with established enterprise environments helps organizations apply strong encryption with greater consistency, governance, and operational control across diverse systems.

- **Meet regulatory requirements for bulk and back-office processes:** Use PGP Command Line to apply auditable encryption and digital signatures to data involved in high-volume, back-office operations such as billing, claims processing, financial reporting, or records exchange. This helps organizations demonstrate that regulated data is protected in transit and at rest, and supports Safe Harbor positions when incidents involve encrypted information.

Business Outcomes

- **Reduce exposure in automated and high-volume data workflows:** Embedding encryption into scripts, batch jobs, and system-to-system processes helps protect sensitive data automatically protected as it is generated, transferred, archived, or processed, reducing the risk of exposure in unattended workflows.
- **Strengthen compliance and audit readiness:** PGP Command Line helps organizations apply auditable encryption and digital signatures to regulated data flows, supporting privacy and compliance requirements while helping reduce the impact of potential breach disclosure obligations.
- **Protect sensitive data with minimal disruption to existing systems:** Because the solution can be integrated into existing scripts, applications, and processing environments, organizations can extend strong encryption without reengineering the systems that generate or move the data.
- **Improve trust and integrity in machine-driven transactions:** Digital signing and verification help confirm the authenticity of data and its sender, while centralized or local key management supports more consistent governance across automated processes and large-scale operational environments.

BROADCOM®

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

PGP-CMD-PB104 July 21, 2026