PGP® Endpoint 4.3

Prevents data loss from removable storage and portable device connections

Part of the PGP® Encryption Platform

Benefits

- **Easy, automatic operation** – Permits safe and authorized removable storage use, without changing the user experience or reducing productivity.
- **Enforced security policies** – Enforces policies for device usage via USB, FireWire, WiFi, and Bluetooth connections; automatically encrypts removable storage based on policy; can also log usage and demonstrate compliance to auditors.
- **Accelerated deployment** – Reduces setup time and speeds enterprise protection without requiring user intervention and by leveraging existing enterprise directory infrastructure.
- **Reduced operation costs** – Result from fast deployment, ease of use, centralized management, and automated enforcement of security policies.

PGP Customer Spotlight

> "Our research showed that PGP Corporation was the one-stop-shop to secure our data."

Alex Clonaris
IT Security Analyst
Henry Davis York

Integrated data encryption and device policy enforcement for removable storage

Removable digital storage devices (such as USB flash drives and CD/DVD drives) and mobile connection technologies (such as WiFi, FireWire, and Bluetooth) are increasingly popular in the enterprise environment. They are convenient and enhance productivity, but present new security risks to the enterprise. The data on these removable endpoint devices and media may contain intellectual property or sensitive customer information.

Company policy and employee education can be insufficient to safeguard the data from insider threats and accidental data leakage. The exposure of sensitive data that results from the loss or theft of a removable storage device or medium can result in financial loss, legal ramifications, and brand damage.

PGP® Endpoint provides built-in security that detects, authorizes, and secures removable storage devices and media (such as USB drives, CDs, and DVDs). It enforces centrally defined device usage policy and stops data losses from network and peripheral connections (such as Bluetooth, WiFi, and FireWire). PGP Endpoint helps enterprises with their compliance and to monitor data exchanged between the endpoint, devices, and the network.

PGP Encryption Platform–Enabled

PGP Endpoint is a part of the PGP Encryption Platform, which provides an enterprise encryption framework for shared user management, policy, and provisioning that is automated across multiple, integrated encryption applications. Together with PGP® Whole Disk Encryption, PGP Endpoint provides the enterprise with an integrated endpoint data loss prevention solution.

Enforced Security Policies

PGP Endpoint transparently protects and secures data at rest or in motion. Advantages of enforcing enterprise security policies with PGP Endpoint include:

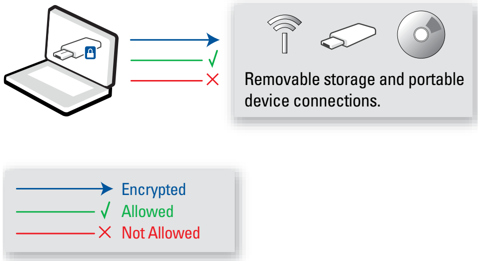
- **Granular Media Use Policies** – Blocks non-permitted devices. Authorizes company-standard media such as CDs and DVDs and specifies use with types of access, encryption, and more; access lists also specify user permissions.
- **Audit Trails** – Supports compliance by logging all device usage; can optionally record all information exchanged between devices and the network.
- **Detailed File and Data Protection** – Blocks PS/2 and USB keyloggers; specifies permitted file types; restricts size of data transfers.
- **Remote and Disconnected Users** – Enforces policy regardless of availability of network connection.
- **Encryption Flexibility** – Manages data encryption on removable media with flexible centralized or time-of-use options. Integrated with PGP Whole Disk Encryption.
- **User Applications Protection** – Available as an additional licensed option, Application Control provides policy-based enforcement of application use. It protects endpoints from malware, spyware, zero-day threats, and unwanted or unlicensed software.

Easy, Automatic Operation

With PGP Endpoint, data on removable devices is automatically protected without altering the user experience.

- **"On-the-Fly" Device Detection and Protection** – Automatically detects devices without disrupting the user.
- **Data Sharing** – Allows data to be shared across the enterprise, including by users without PGP software; access to data is enforced by policy.
- **Flexible User Permissions** – Reduces risk of unauthorized devices, without altering user flexibility. Provides multiple user permission settings, including type of access and specific device use.

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.



Prevent data loss from the endpoint.

Accelerated Deployment

Enterprises can quickly and easily deploy PGP Endpoint by:

- **Automated Installation** – Does not require administrator intervention to deploy; can use Microsoft® MSI.
- **Leverage the Enterprise Directory** – Transparently set user and device policy using the existing Microsoft Windows® Active Directory or Novell® eDirectory™ infrastructure.

Reduced Operational Costs

PGP Endpoint reduces deployment tasks and time, eliminates end-user training costs, and avoids any increase in help desk calls. With PGP Endpoint, organizations can centrally manage their security policies for users and encryption, reducing the operational costs of using disparate encryption applications.

Centralized Management

PGP Endpoint is centrally managed by the PGP Endpoint Administration Server. Its advantages include:

- **User and Device Management** – Can set granular policies, with multiple user and device options.
- **Recovery and Temporary Authentication** – Multiple lockout and recovery options, including temporary user permissions.
- **Infrastructure Independent** – Can be deployed on virtually any network, regardless of network complexity or size of user base.

Technical Specifications

PGP Endpoint supports Windows 2000 Professional (SP4 or later), Windows XP (32- and 64-bit editions), and Windows Vista® (32- and 64-bit editions). For complete technical specifications, please visit www.pgp.com.

PGP®

PGP Corporation
www.pgp.com

PGP Corporate Headquarters
Tel: +1 650 319 9000

PGP (GB) Ltd.
Tel: +44 (0)20 8606 6000

PGP Deutschland AG
Tel: +49 69 838310 0

PGP Japan K.K.
Tel: +81 03 4360 8308