PGP® Whole Disk Encryption for Enterprises

Centrally managed, automatic full disk encryption solution for the enterprise

Comprehensive disk encryption for securing all files on desktops, laptops, or removable disk drives

Mobile computers are emerging as the industry standard for increasing user productivity and efficiency. The portable nature of these devices increases the possibility of loss or theft. Without strong data protection, an enterprise may be exposed to significant financial loss, legal penalties, and brand damage.

PGP Whole Disk Encryption for Enterprises provides comprehensive, non-stop disk encryption. The solution is centrally deployed and managed, enabling organizations to quickly and cost-effectively safeguard sensitive data from unauthorized access.

Full Disk Protection

PGP Whole Disk Encryption for Enterprises locks down the entire contents of a laptop, desktop, external, or USB flash drive, including boot sectors plus system and swap files. The encryption is transparent to the user, automatically protecting data.

Scalable Security

PGP Whole Disk Encryption for Enterprises includes enterprise-class tools for user management, IT configuration, rapid deployment, and data recovery.

Seamless Integration

PGP Whole Disk Encryption for Enterprises is interoperable with all the solutions in the PGP security suite.

- Other PGP solutions can be added with simple, centralized administrative license updates.
- Administrators can incrementally add features for email and messaging security.

Overview

Rapid Deployment

- Leverages an existing LDAP/Microsoft Active Directory to automatically assign security policies for user groups.
- Facilitates creation, deployment, and updates of pre-configured clients using Microsoft MSI.
- Provides silent installation with Microsoft MSI tools.
- Integrates with PKI deployments via compatible tokens.
- Operates in the background so users remain fully productive, even during initial disk encryption.

Simple Administration

The unified, Web-enabled management console provides easy access to administer and manage PGP Whole Disk Encryption for Enterprises clients.

- Simple, push-based management of updates.
- Recovery passphrases reduce help desk overhead by enabling user access to secured disks in the event of a lost token or forgotten passphrase.
- Role-based administrative access enables administrative separation of duties.
- Comprehensive audit log.

Centralized Policy Enforcement

IT administrators can specify and centrally enforce granular security policies based on requirements.

- Centralized enforcement of full disk encryption.
- Specification of passphrase, authentication, and recovery token requirements.
- Centralized policy prevents users from decrypting the disk or uninstalling the software.

Trusted, Proven PGP Encryption

PGP Whole Disk Encryption for Enterprises is based on the same mature PGP technology that has been proven effective by millions of users worldwide. PGP Corporation is the only commercial security vendor that publishes source code for peer review, ensuring the integrity of its encryption implementation.

- Provides strong encryption based on industry-standard, trusted security technology.
- Used and tested by enterprises, government agencies, individuals, and cryptographers for the last 10 years.

Components

High-Performance Encryption Engine

The high-performance encryption engine transparently performs on-the-fly encryption and decryption with no impact on system usability.

Multiple Pre-Boot Authentication Options

PGP Whole Disk Encryption for Enterprises can be secured using a unique passphrase as well as a PGP or X.509 key stored on an Aladdin eToken. With a single passphrase or token, users can secure full disks, files, archives, and virtual drives.

Recovery Passphrases

Unique to each user, PGP Whole Disk Encryption for Enterprises automatically generates and centrally stores a one-time-use recovery passphrase.

- Enables remote assistance for users with lost tokens or forgotten passphrases.
- Automatically resets after each use, reducing administrative overhead.
- Does not rely on use of a single, global administrative password.

Multi-User Workstation Login

Multiple users may access a PGP-encrypted drive using separate credentials, allowing them to securely share workstations without sharing authentication credentials.

Additional Features

PGP Virtual Disk

PGP Virtual Disk enables users to create personal volumes whose contents are encrypted when not in use, allowing them to create a unique, secured storage space on a PGP-encrypted disk.

PGP Zip

PGP Zip enables single-step creation of secure, encrypted, compressed archives.

Self-Decrypting Archives

Self-Decrypting Archives can be decrypted on any Microsoft Windows system, making them ideal for securing files intended for non-PGP users.

PGP Shredder and PGP Wipe

The PGP Shredder and PGP Wipe tools allow users to securely and permanently eliminate all traces of files from a disk.

Technical specifications

Desktop Systems Supported

- Windows 2000 Professional SP4, Windows XP SP1 & SP2
- English, Japanese, & German languages

Storage Devices Supported

- Internal hard drives
- External hard drives (FireWire [IEEE 1394], USB)
- USB flash drives

Authentication Options

- OpenPGP RFC 2440 key (on Aladdin eToken cryptographic token)
- User-defined passphrase

Symmetric Key Algorithms

- AES 256-bit keys

(See http://www.pgp.com/products/desktop/professional/techspecs.html for current product specifications.)