IBM Data Security Services for endpoint data protection—endpoint encryption solution

Managing data security for the growing number and variety of endpoint devices

In today’s highly mobile and competitive business environment, data knows no boundaries. While information is consumed, transferred, and stored between an organization’s suppliers, customers, partners, and employees, it is susceptible to compromise. Laptops, USB flash drives, and PDAs are ready-made targets for loss or theft. People take them everywhere—home, airport, hotels, and beyond. Easily transported, laptops provide the freedom to work anywhere, but this freedom increases the likelihood of theft and inadvertent compromise of sensitive customer records and intellectual property. IBM® offers an endpoint encryption solution that enables your workforce to transport, share, and circulate critical data while defending your business from a potential breach. IBM Data Security Services offerings ensure that your organization benefits from the latest encryption technologies—liberating your team from the fear of data loss and exposure.

Highlights

- Secure data on endpoint devices across the enterprise to prevent data exposure and protect your corporate brand and reputation
- Protect sensitive information on mobile computers, handhelds, and removable storage devices even if a device is lost or stolen
- Leverage market-leading encryption technologies, services expertise, and proven methodologies to deploy an integrated security solution
- Reap benefits such as lower total cost of ownership and accelerated deployments from an extensible platform and scalable solutions
- Ensure optimized protection through professional security services and support desk
Widespread reports of lost notebook computers and other mobile devices communicate the growing risk of data breaches for all organizations. The cost of a single breach can exceed millions of dollars and permanently damage brand equity as well as customer trust. That is why protecting data in the modern enterprise requires a comprehensive approach. IBM’s endpoint protection solution is an evolutionary combination of technologies and services to manage sensitive data, control access, and detect information at risk to protect the value of sensitive data.

**Protecting data wherever it goes**
Data is always in motion—constantly traveling on devices inside and outside an organization’s main facilities. Although this movement creates risk, sharing and portability increases the value contribution of an organization’s most valuable assets. Effective organizations promote a collaborative business model by ensuring that data is protected even as it is moved around. Increasingly, encryption is required for regulatory compliance and to compete in today’s market. IBM’s endpoint encryption solution ensures that you can collaborate while mitigating risk.

IBM implements endpoint encryption solutions with your needs in mind to:

- Establish an enterprise encryption framework for your organization
- Deploy market-leading encryption technology using a proven implementation methodology
- Enforce corporate data security policies
- Define and deliver reliable management and support services

IBM Data Security Services address the challenges associated with deploying a comprehensive solution by managing cost and scope, accelerating implementation, leveraging IBM’s information security expertise, and eliminating the need for additional headcount.

**Leveraging encryption technology to protect data on endpoints and removable media**
The need to manage and control access to data has led to an evolution in data security. Because data is increasingly transferred across multiple systems and networks, organizations must now detect when information is at risk and secure it automatically using persistent protection that works both inside and outside the enterprise. The most effective way to meet this enterprise data protection goal is with a centrally managed solution that controls policy and data access without requiring end users to make enforcement decisions or burdening administrators with complicated and resource-intensive tasks. A comprehensive approach ties security to the data.

IBM’s endpoint encryption solution ensures centralized policy and compliance management by enforcing data protection policies on endpoints and alerts when deviations and tampering are detected so that mitigating actions can be taken. Utilizing IBM services to assess requirements, design architecture, plan implementation, and manage deployment, ensures that data protection policies are configured optimally for your environment and specific business needs.

With IBM’s endpoint encryption solution, built-in data protection separates how data is transferred, stored, and used from the security controls, reducing the risk incurred by human decision—making and increasing usability for people throughout the organization.
Enabling authorized users to move, share, and store data throughout the enterprise and beyond

At the core of enterprise data protection, encryption serves to provide the encompassing protection layer that obscures data from unauthorized access. If encrypted data is somehow lost or stolen, it remains unusable. Even if someone violates access controls, encrypted data will still be protected. This level of critical protection is why more than 30 U.S. states provide safe harbor from mandated consumer notification in the event of a data breach involving encrypted data. In countries such as the U.K., where the need for breach mitigation is just emerging, protecting brand and reputation is the major reason enterprises adopt encryption solutions. IBM’s endpoint encryption solution segments access as needed, maintaining separation of duties and roles. This separation, for example, means confidential information in emails cannot be read by an IT administrator. Our expertise in the area of governance and risk management reduces the complexity required to translate and enforce your authorization policies.

Leveraging enterprise encryption solutions

Today, the process of protecting data with leading, strategically focused encryption is largely automated and operates in the background, transparent to end users. Encryption is enforced by centrally managed policy while corporate access to data is always maintained. Most importantly, key management is integrated and automated, enabling administrators to focus on user and policy management instead of key maintenance. Point encryption applications that protect only one type of data or one locale are rapidly being replaced by a platform solution that scales to provide a range of security options, depending on where data is stored, how it is shared, and who needs access. IBM’s platform approach provides operational and management efficiencies as well as consistent data security that can scale to meet needs as they emerge and evolve.

IBM’s comprehensive endpoint encryption platform includes:

- Whole disk encryption
- External USB storage device policy-enforced encryption
- Network-based shared file encryption
- Transparent email encryption performed at the desktop or email gateway

IBM partners with PGP Corporation to combine professional security services with comprehensive technology for a complete endpoint encryption solution. This partnership ensures that every step of the solution lifecycle is backed by proven experience and market leading technology.

Enabling a strategic approach

IBM’s solution for endpoint encryption leverages an extensible platform with modular applications. This approach makes it unnecessary to install a separate or additional infrastructure as business needs change. As part of the initial installation, IBM deploys the PGP® Encryption Platform. Subsequently, additional encryption applications then leverage this framework, expediting deployment, lowering operational costs, and freeing administrative resources. Most importantly, this modular platform provides the automated services, centralized management, provisioning, consistent policy enforcement, and extensible framework needed to support a robust encryption strategy.

---

The key components of IBM’s endpoint encryption solution include:

- **PGP Universal™ Server**—Delivers an extensible framework that supports scalable, centralized gateway and desktop encryption management, deployment automation, and policy enforcement across applications.

- **PGP® Whole Disk Encryption**—Provides comprehensive, nonstop encryption for securing all files on desktops, laptops, and removable media, transparently securing all disk contents, including system and temporary files, and enabling quick, cost-effective protection for sensitive data.

- **PGP® NetShare**—Enables teams to securely share documents on file servers by automatically and transparently encrypting the files for fine-grained group access.

- **PGP® Desktop Email**—Secures email communications from the sender’s email client to the recipient’s—and all points in between—automatically, using centrally defined, policy-based encryption leveraging industry standards for maximum interoperability and transparency.

- **PGP Universal™ Gateway Email**—Delivers standards-based enterprise email encryption and digital signatures without client software.

- **PGP® Endpoint**—Enforces device usage policy and stops data losses from removable storage devices (such as USB drives, CDs, and DVDs) and network/peripheral connections (such as Bluetooth, WiFi, and FireWire).

- **PGP® Mobile**—Protects individual files, entire data volumes, archives, or directories with comprehensive data encryption for mobile devices, enabling quick protection for the data stored, in use, and shared with other users.

- **PGP® Support Package for BlackBerry®**—Enables BlackBerry smartphone users to seamlessly send and receive PGP-protected email using policy and key management provided by PGP Universal Server.
IBM's approach enables IT management to execute on business needs without making security a separate project or an afterthought. Our endpoint encryption solution builds security into the most commonly used applications, protecting data wherever it exists—from outbound email, to file servers, to removable storage devices such as USB flash drives and PDAs.

**Adopting an endpoint encryption solution**

IBM understands data security at the enterprise level, through interaction with customers and utilization of data security solutions in our own internal networks. Our consultants and specialists have experience with a wide range of industry solutions and IT architectures to help you adopt an endpoint encryption solution. Our professional security services help:

- **Conduct a Requirements and Planning Workshop** to assist in assessing environment, business, compliance and IT requirements, preparedness for implementation of controls, and developing an all-encompassing approach for integration

- **Determine your Policy Design** by defining encryption policies and deployment priorities to be used in implementation and testing

- **Understand the Implementation** aspects of a successful deployment including:
  - Implementation planning and project management
  - Solution architecture and design
  - Installation of primary components
  - Testing of primary components
  - Pilot deployments
  - Production roll-out of controls to endpoints
  - Project documentation
  - Help desk deployment assistance
  - Technical training and skills transfer
  - Project close-out and hand-off

- **Ensure a single point of contact for technical assistance with a Support Desk** for all encryption products licensed and deployed in the solution with escalation to PGP for break/fix or insolvable issues. IBM Support Desk will own and help manage, track, and resolve problems related to the endpoint encryption solution.

IBM combines the use of refined methods and extensive skills so that you can realize the full value of your encryption investment. Our services are designed to optimize productivity, manageability, and cost-effectiveness within your organization.

**Why IBM and PGP Corporation?**

IBM and PGP Corporation come together to bring a complete, trusted, and transparent endpoint encryption solution to market. Clients can confidently deploy PGP Corporation’s market leading products by leveraging IBM Global Services experience, global reach, and scale. The IBM endpoint encryption solution, powered by products from PGP Corporation, is a complete, integrated security solution encompassing the entire security lifecycle, from strategic consulting and risk analysis, to deployment, support and solution management. IBM provides experienced practitioners, proven methodologies, and innovative approaches to allow rapid adoption with less risk than deploying encryption technology yourself. IBM will partner with you to stay on top of your evolving security and endpoint data encryption requirements.
For more information
To learn more about the IBM Data Security Services for endpoint data protection—endpoint encryption solution, contact your IBM representative or visit:

ibm.com/services