

Data Encryption Service



Data Encryption is one of Fiberlink's Security Services, the industry's most extensive suite of endpoint security solutions. Together with the Fiberlink Extend360 Mobility Platform and Fiberlink Connectivity Services, they deliver:

Comprehensive Security

Enterprises can protect mobile devices – and the data they carry – from hackers, viruses, loss, theft, “data leakage” and many other hazards of mobile computing.

Simple Connectivity

Mobile workers can connect quickly and easily to the Internet and corporate networks from anywhere, using all types of wired and wireless networks.

Low-cost Administration and Compliance

Administrators can deploy, configure and manage security and connectivity services consistently across a global network, while ensuring compliance with enterprise policies

reported data breaches were the result of a device being lost or stolen.

Gartner estimates 90% of business mobile users have insufficient power-on protection and stored data encryption to withstand casual to moderate hacker attacks.

Laptops and other mobile devices are often lost or stolen in airports, in hotels, in cars, on public transportation, and at home. Gartner states that, “the loss and theft of mobile devices is the most common exposure to data leakage when data is taken outside the office.”

And today these devices contain increasing amounts of confidential information, including customer lists, employee data, financial information, business plans, and software code. A lost or stolen computer can lead to public embarrassment, high disclosure costs, severe regulatory fines, and the loss of customer confidence.

Fiberlink Data Encryption protects the enterprise brand, strengthens customer trust, and ensures compliance with regulatory mandates by securing valuable information on laptops, desktops and removable media against loss and unauthorized use. The solution utilizes a highly secure encryption process that protects vital information whether it is stored on a hard drive or external storage device.

According to the Privacy Rights Clearinghouse, 27% of



Features and Benefits

SECURITY, PERFORMANCE AND RELIABILITY

The Fiberlink Data Encryption service encrypts sensitive data on mobile devices, so confidential information is protected even if a system is lost or stolen. Information is encrypted wherever it is stored, including removable media and swap and temporary files. End users cannot disable or bypass the data encryption.

Instead of encrypting all data on the laptop's hard drive, which can slow performance, administrators can selectively encrypt data:

- Included in specific file types (for example spreadsheets, databases, or temporary files).
- Written by specific applications that handle sensitive data.
- Written to any fixed disk or removable media.
- Associated with a specific user (if a system is shared).

Because the Data Encryption service does not encrypt the operating system and program files, it does not suffer from the data corruption, recovery, and productivity loss typically associated with other encryption solutions. Existing corporate recovery processes are not affected, because the service is designed to avoid mandatory decryption of the entire disk in recovery and service scenarios.

EASE OF USE INCREASES USER ACCEPTANCE AND MINIMIZES IT OVERHEAD

The Data Encryption service requires no end-user training and the encryption process is transparent to end-users, lowering the cost of deployment. No additional passwords or password management processes are needed, because the service uses existing Windows login passwords. The service also provides administrators with comprehensive reporting on the status of encryption on remote devices.

COEXISTS WITH OTHER SECURITY SOLUTIONS

Many data encryption solutions interfere with other security technologies. The Fiberlink Data Encryption service works smoothly with other Fiberlink Security Services such as Patch Management, Vulnerability Management and Backup and Recovery.

Fiberlink can incorporate the Data Encryption service into its Network Access Control (NAC) capability. Mobile devices that are not running data encryption in compliance with corporate policies can be blocked from accessing corporate networks. This protects central networks and ensures that mobile employees comply with security policies.

Service Details

- » Centrally defined, policy-based encryption
- » Encrypts data on fixed disks and removable media
- » Encrypts at file type, application and user-level
- » Operates when connected and disconnected
- » Users cannot disable or bypass
- » Built-in hacker protections for windows domain password hash
- » FIPS 140-2 validated AES 256-bit encryption

System Requirements:

- Fiberlink Extend360 v 1.3 or later

FOR MORE INFORMATION

For more information on MaaS360's technology and services, see www.MaaS360.com or email aholmes@fiberlink.com.

Fiberlink Communications ; 1787 Sentry Parkway West, Building 18; Suite 200, Blue Bell, PA 19422. Phone 215.664.1600; Fax 215.664.1601