

On Target Security – IBM System Storage™ DS3500 Encryption Manager

Negative impacts of data breaches:

- *Loss of customers and revenue*
- *Unplanned expenses*
- *Legal implications, penalties, and fines*
- *Negative press and tarnished reputation*
- *Lost goodwill and undermining of other corporate relationships*

Whether it is to sensitive customer information, intellectual property, or proprietary data that helps a company reach its strategic objectives, a company's data may be its most valuable asset. If this data is misplaced or stolen, organizations run the risk of lost revenue, legal implications, and a tarnished reputation. The unfortunate truth is that an organization's data is becoming increasingly vulnerable as lost, accidentally exposed, or breached data is becoming more and more commonplace in today's environment. With data security risks on the rise, an influx of government mandates and regulations for securing data have been implemented, which are becoming part of the corporate landscape for many. Eliminating exposure of private data is now viewed as a sound business practice.

To avoid the high costs associated with data exposures such as these, organizations must put into place a comprehensive security strategy. While each point in the storage infrastructure provides unique threat models, data-at-rest presents one of the highest security vulnerabilities.

Data, in fact, spends most of its life at rest on drives within the data center. As these drives will eventually leave the data center either for repair, retirement, relocation, or maintenance, it is at this time that drives—and the data contained on these drives—are most vulnerable to being lost or stolen.

The emergence of self-encrypting drives (SEDs) is timely in mitigating the security vulnerabilities of data-at-rest. With SEDs both the data and the encryption key use the Advanced Encryption Standard (AES) 128 encryption algorithm, the same encryption algorithm approved by the United States government for protecting secret-level classified information. With SEDs if a disk drive is removed from its storage system in which it is housed, the data on that disk drive is encrypted and useless to anyone who attempts to access it without the appropriate security authorization. Many safe-harbor laws protect organizations that store data in compliance with security encryption requirements. In fact, an organization may not have to notify a customer of lost data if that data was stored on secured SEDs.

IBM Disk Encryption Manager

Simple, secure and cost-effective full disk encryption.

While the encryption capabilities of the disk drives are the primary level of security, management of the SEDs is critical to their execution. In fact, the security capabilities offered with disk-level encryption are only as good as the management tool used to implement and manage them.

As a leader in storage technologies, IBM offers disk encryption management with the System Storage DS3500, which combines local key management with SEDs. This capability represents a significant step forward in securing a disk drive and ensuring that the data is not compromised. The DS3500 maintains and controls the key linkage and communications with the SEDs, secures user-selected storage volumes, and authorizes the disk drives to encrypt and decrypt data with a pass phrase and security key management. The DS3500 uses simple and intuitive configuration menus to effectively protect data from any unauthorized access or modification resulting from theft, loss, or repurposing of the disk drives.

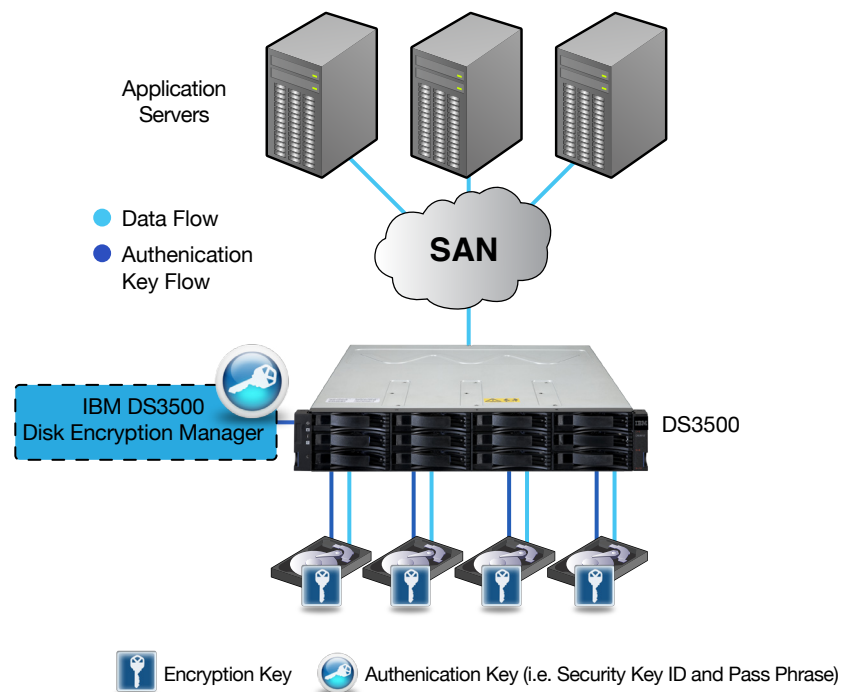
Secure

By embedding the intelligence to manage SEDs in the IBM System Storage DS3500, the IBM DS Storage Manager removes the administrator from most of the daily tasks of managing disk drive security, thereby reducing user error or the compromising of data. The IBM System Storage DS3500 also supports instant secure erase of disk

drives that permanently removes data when repurposing or decommissioning disk drives. This capability provides a much more secure level of data erasure than other common erasure methods, such as overwriting or degaussing.

High performance

The IBM System Storage DS3500's performance-optimized architecture with SEDs allow for exceptional data security with virtually no performance impact. While other encryption methods may take place at the software or host level, which can negatively impact processing resources, encryption resides on the disk drive itself. With SEDs within the IBM System Storage DS3500, no CPU cycles from the host are necessary, and the transfer of I/Os can occur without interruption.



Cost-effective

The IBM System Storage DS3500 management of SEDs provides protection from the high costs associated with a breach in data. In fact, a 2008 study found that a breach can cost up to \$202 per exposed record and more than \$6.6 million per total reporting company on average. At only a small percentage of the total cost of the storage system that can house hundreds of thousands of records, the IBM System Storage DS3500 and SEDs can save an organization up to millions of dollars by avoiding an unexpected breach.

Alternative and costly methods of data erasure can be avoided with the instant secure erase feature, which does not require hefty transportation and service expenses to erase or deconstruct the disk drive's data. In addition, instant secure erase reduces overall hardware expenditures by re-provisioning existing disk drives instead of the alternative of replacing destroyed or disposed-of disk drives for which additional hardware purchases are needed.

Simple

The IBM System Storage DS3500 provides the necessary management and protection of SEDs by using a set of security authorizations that can be set and applied to all SEDs within an IBM Storage System DS3500. This process removes the complexity of managing each SED's unique encryption key (which encrypts and decrypts data on the disk drive). Because the DS3500 manages the key linkage and communication, the process is transparent to the system administrator and no modifications to existing operating systems or applications are necessary. As well, migrating SEDs from one device to another is secure and simple.

Flexible

For maximum utilization of disk drive inventory, organizations may choose to continue to use their non-SEDs for data that they determine does not have to be secured. Having the flexibility to support SEDs and non-SEDs, IBM addresses the needs of tiered and classified data with a single storage device. And when it becomes

necessary to secure data residing on a non-SED the data can be simply migrated to an SED.

While the idea of fully securing data across a company's entire range of offices, laptops, networks, and datacenters can be overwhelming, IBM provides a powerful tool for securing critical information and protecting against the ever-present threat to data-at-rest. As disk drives will inevitably be moved from the data center, the DS3500 with SEDs mitigate the risks associated with data loss and breaches and is a critical component to a successful end-to-end security solution with minimal cost and complexity.

