Industry Trends and Technology Perspective White Paper

Decrypting Enterprise Storage Security

"Trends and options for securing enterprise data and storage"

By Greg Schulz

Founder and Senior Analyst, the StorageIO Group

December 11th, 2006

With a growing awareness of existing and new threats to information coupled with increases in the amount of data being stored for longer periods of time, new and innovative approaches are needed to manage and secure data at rest. This paper looks at how to identify the level of security needed to apply to enterprise data while at rest and while in-flight as well as how to address the complexities associated with data storage security management.

Introduction

Public awareness of the importance of data protection and security continues to grow. With more data being reported lost or stolen, can any organization risk not having business information safe and secured?

Additionally, the public relations nightmare of a data loss or theft is something any business wants to avoid. Data loss and theft are not new topics; what is new are the growing options and points of exposure to ever-increasing amounts of data being generated, stored and retained for longer periods of time.

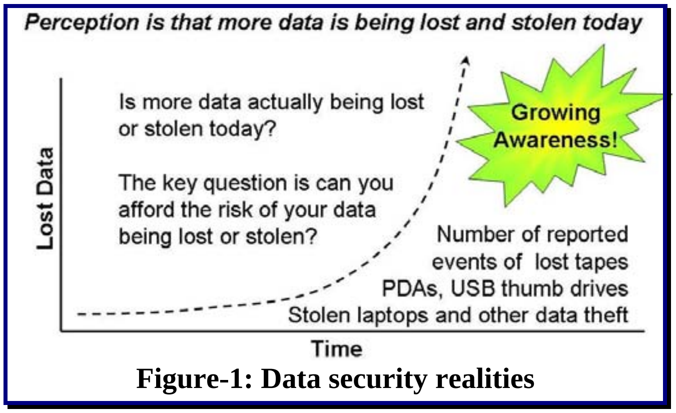

Figure-1: Data security realities

Issues and challenges

Regardless if more data is actually being lost or stolen today as compared to the past, a key question for any organization of any size is can it afford to risk the loss of any data or any exposure of critical information. Data and information security threats vary and are as diverse as each business and its applications. Data protection involves securing data while at rest on a storage device and while in-flight or being moved. In-flight data includes data being read or written by a server from a storage device, data being copied, mirrored or replicated over a network and removable media shipped off-site.

Common issues pertaining to securing data both at rest and in-flight include:

- Inadequate data protection and increased costs resulting from treating all data the same
- Determining where, when and how to deploy applicable level of storage security
- Striking a balance between worker productivity and exposure risk
- Meeting industry and government compliance regulation requirements
- Complexity of encryption and key management across different storage technologies
- Perceptions that encryption is needed only for data in-flight or removable media
- Growing awareness of the need for tiered security and data protection

Decrypting encryption options

Security and encryption issues:

- ✓ Key life cycle management
- ✓ Day-to-day as well as BC and DR
- ✓ Data at rest and in-flight or transit
- ✓ Application transparency
- ✓ Alignment of security to applicable threat
- ✓ Ease of use and granularity

There are many issues pertaining to data encryption including how and where to encrypt data for the particular needs at hand. Depending on the requirements and applicable threats, the applicable data protection and security strategy may involve multiple rings or tiers of protection. Data encryption options vary from host-based software to appliances that exist in the data path on a LAN, SAN, MAN or WAN to storage system-based solutions. Encryption capabilities vary by implementation and are suited for different purposes. For example, appliance-based encryption can support storage system to storage system remote mirroring and replication. Figure-2 shows three options for deploying data encryption to support different applications and types of data while at rest and while in-flight.

	Host Software	Appliance (In the	Storage System

	Based	data path) Based	Controller Based
Highly classified data	✓	✓	✓
Sensitive data	Emerging	✓	✓
Non sensitive data			Optional
Local and remote data mirroring and replication	If host involved in data movement	✓	✓
Network file servers		✓	✓
Desktops and laptops	✓		Emerging
Removable media		✓	Emerging

Figure-2: Where to implement what type of encryption for a tiered encryption strategy

Tiered data and storage security

Security and encryption, in particular, do not have to be all or nothing endeavors. Instead, by analyzing applications data and aligning the appropriate level of defense (known as tiered security) to counter applicable threats, data security will be enhanced while making security management more effective and transparent to users. Steps to secure data involve understanding applicable threats, aligning appropriate layers of defense, and continual monitoring of activity logs to take action as needed. The level of encryption will be based on what is necessary to counter applicable threats for specific applications.

The more critical and sensitive data, the stricter and more comprehensive the corresponding security response should be, involving multiple layers to counter internal and external threats. Multiple layers of defense (Figure-3) isolate and protect data should one of the defense perimeters be compromised.

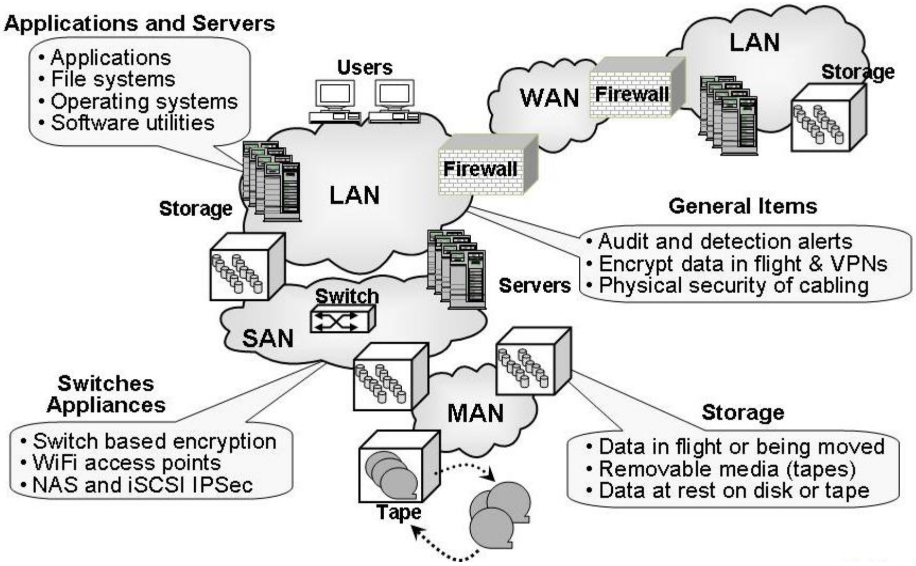

Figure-3: Areas of data security focus

Figure-3 shows common areas of focus pertaining to securing stored data while at rest and in-flight. Data movement is required for authorized general access, business continuance (BC), disaster recovery (DR), and general data protection. Archiving is also necessary for data preservation and compliance.

Tips for implementing a tiered storage security strategy include:

- Enable storage system based encryption as a basic layer of defense and avoid treating all data the same from a data security and protection standpoint
- Protect data at rest using storage system-based encryption when available; use appliances to protect data in-flight or when storage system-based encryption is not available for data at rest
- Key management can add complexity for heterogeneous environments, instead, look for solutions that support granularity without being intrusive to productivity or that compromise data security
- Identify how keys will be managed and handled if applicable for off-site BC and DR needs
- Understand any applicable applications interoperability and performance transparency issues
- Leverage eDiscovery, indexing, search and data classification tools to assist with identify data and applying applicable security to counter relevant risks

Fujitsu ETERNUS Security Features

Tiered data protection and security strategies can be deployed leveraging storage system-based encryption for data at rest combined with appliance-based encryption to protect data in-flight for local and remote mirror, replication and electronic tape vaulting. The Fujitsu ETERNUS with storage system-based encryption protects data with encryption on an individual LUN or using volume granularity enabling the user to avoid treating all data the same. In other words, the ETERNUS enables the alignment of the appropriate level of security and encryption to counter applicable threat risks to the data.

The Fujitsu ETERNUS storage system addresses complexities traditionally associated with securing stored data with built-in storage controller-based encryption. By utilizing a persistent system-based key combined with storage system controller based-encryption, the ETERNUS removes the complexities associated with key management when applying encryption on a granular LUN or volume basis.

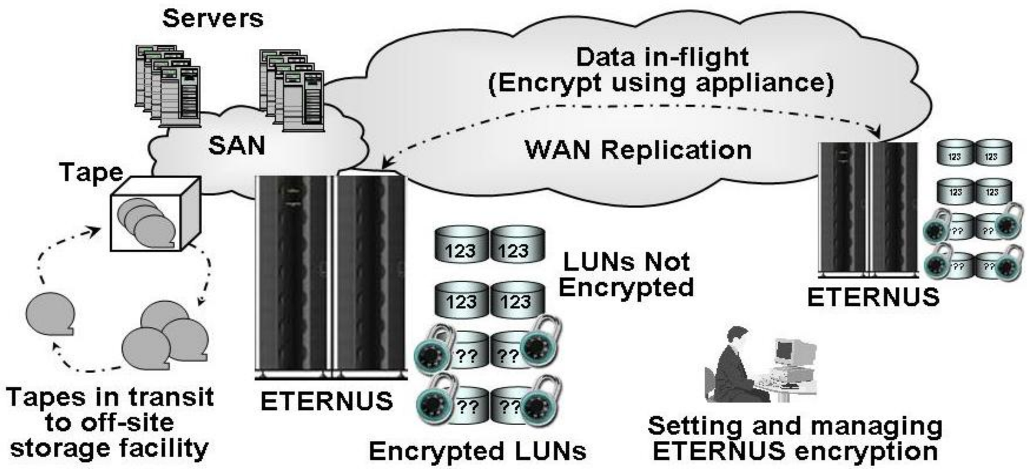
Servers
SAN
Data in-flight
(Encrypt using appliance)
WAN Replication
Tape
LUNs Not Encrypted
ETERNUS
Tapes in transit to off-site storage facility
ETERNUS
Encrypted LUNs
Setting and managing ETERNUS encryption

Figure-4: Tiered data storage protection using ETERNUS encryption for data at rest

As part of a tiered data security strategy, as shown in Figure-4, IT organizations have the flexibility of enabling encryption on a LUN-by-LUN or volume basis for data at rest protection in the ETERNUS storage system. Co-existence and interoperability without compromise is important to simplifying management and maintaining data protection in a tiered data security environment. Figure-4 shows how the ETERNUS storage system-based encryption for data at rest co-exists with other external encryption technologies to protect and encrypt data in-flight for backup using removable tape or other media, as well as maintaining functionality support for local mirroring and remote replication between ETERNUS storage systems.

Data is encrypted using AES 128 bit cryptography when it is written from cache to disk and decrypted when read back from disk to cache in order to be compatible with and transparent to host I/O accesses. For additional data security, the Fujitsu ETERNUS also encrypts cached data flushed to systems disks in the event of a power loss. To insure uniquely encrypted data, even when redundant data is found, the encryption is seeded with LUN and block address, strengthening the encryption algorithm.

Summary of ETERNUS storage system-based encryption features include:

- Storage system-based encryption implemented in microcode for application transparency
- Granularity to support encryption on an individual LUN or volume basis
- Simplified built-in key management to enable 128 bit AES based encryption
- Data consistency, including encrypting data flushed from cache during power loss
- Automatic encryption of destination volumes for replicated and snapshot encrypted LUNs
- Elimination of complex management of individual keys of disk drive based encryption
- Compatibility with external encryption appliances for remote mirroring and replication
- Fujitsu encryption features are implemented to be transparent to other ETERNUS functions

Trends moving forward

Insuring that data is secured utilizing encryption has become an IT best practice. Another trend is movement away from treating all data the same by implementing a tiered security and data protection strategy. A tiered data storage security strategy combines multiple layers or rings of defense, including access controls and encryption of data at rest or while in-flight. Enabling storage system-based encryption is a good starting point for implementing a tiered data security strategy.

Storage security features to look for:

- ✓ Flexible and easy to use
- ✓ LUN or volume level granularity
- ✓ Compatible with other technologies
- ✓ Transparent to applications
- ✓ Robust AES 128 bit encryption

Conclusion

It is important to avoid having data security become a bottleneck to productivity while taking the appropriate steps to secure all data based on applicable threat risks. To avoid treating all data the same, leverage storage system-based volume or LUN level encryption as part of an overall tiered storage security strategy. The more transparent the effective security is to those authorized to use the data, the less likely those users will try to circumvent security efforts. For security and compliance conscious environments and impacted data, Fujitsu's new paradigm of storage system-based data encryption reduces the cost and simplifies the management of sensitive data.

About the author:

Greg Schulz is founder and Senior Analyst of the StorageIO group and author of the book *"Resilient Storage Networks - Designing Flexible Scalable Data Infrastructures"* (Elsevier / Digital Press).

All trademarks are the property of their respective companies and owners. The StorageIO group makes no expressed or implied warranties in this document relating to the use or operation of the products and techniques described herein. The StorageIO group in no event shall be liable for any indirect, inconsequential, special, incidental or other damages arising out of or associated with any aspect of this document, its use, reliance upon the information, recommendations, or inadvertent errors contained herein. Information and recommendations made by the StorageIO group are based upon public information believed to be accurate, reliable, and subject to change.