

# Securing Networked Storage: Decru DataFort™ Appliance

## Contents

1. [Executive Summary](#)
2. [Trends in Data Security and Privacy](#)
3. [Current Approaches](#)
4. [Decru DataFort Security Appliance](#)
5. [Backup, Mirroring and Disaster Recovery](#)
6. [Conclusion](#)

## 1. Executive Summary

The advantages of networked data storage technologies such as Network Attached Storage (NAS) and Storage Area Networks (SAN) are well established, but storing an organization's data on a network creates significant security risks.

Technologies like NAS and SAN that aggregate data in a storage network can improve scalability, manageability and access to critical data, while substantially reducing the total cost of storage. Additionally, storage networks can simplify the process for enterprises seeking to implement comprehensive disaster recovery programs.

However, data in networked storage environments is significantly more vulnerable to unauthorized access, theft or misuse than data stored in more traditional, direct-attached storage. Aggregated storage is not designed to compartmentalize the data it contains, and data from different departments or divisions becomes co-mingled in the network. Data backup, off-site mirroring, and other disaster recovery techniques increase the risk of unauthorized access from people both inside and outside the enterprise. Partner access through firewalls and other legitimate business needs also create undesirable security risks. With storage networks, a single security breach can threaten the data assets of an entire organization.

Technologies such as firewalls, Intrusion Detection Systems (IDS), and Virtual Private Networks (VPN) seek to secure data assets by protecting the perimeter of the network. While important in their own right, these targeted approaches do not adequately secure storage. Consequently, they leave data at the core dangerously open to both internal and external attacks. Once these barriers are breached -- via stolen passwords, uncaught viruses, or simple misconfiguration -- data assets are fully exposed.

Decru secures networked storage by protecting data both in transit and stored on disk. Decru DataFort is an encryption appliance that fits transparently into NAS or SAN environments, securely encrypting and decrypting data at wire-speed. Built specifically to secure data storage, Decru DataFort combines custom, high-performance hardware with comprehensive key management, creating a powerful, yet manageable security solution. DataFort is application-independent, vendor-agnostic and fits seamlessly into the existing network infrastructure. With Decru DataFort, enterprises can fully leverage the benefits of networked storage, confident that their data assets are secure.

## 2. Trends in Data Security and Privacy

### 2.1. Data Security Concerns

Research organizations including the Computer Security Institute/FBI, Goldman Sachs, Information Security Magazine and RBC Capital Markets are closely following data security. They have recently published troubling statistics about the cost and impact of security breaches, as organizations grow increasingly dependent on digital storage of their corporate data assets. Statistics include:

- The 2002 CSI/FBI survey indicates 90% of 503 responding companies detected security breaches within the past 12 months. 80% acknowledged financial losses due to these attacks
- Industry researchers indicate that roughly 70% of security breaches come from inside the firewall, and organizations are becoming increasingly concerned about the ability of disgruntled employees, contractors or IT staff to access confidential information.
- A recent study by Network Computing indicated that the biggest factors preventing companies from outsourcing data storage were concerns about security and privacy.

While these statistics support the need for data security in general, organizations that use networked storage are even more vulnerable. Risks increase as enterprises adopt larger storage network deployments with expanded access, using file sharing protocols such as CIFS and NFS, Fibre Channel SANs and emerging storage protocols such as iSCSI. Advances in disk technology means more data can be stored on fewer, physically smaller disks, further increasing the risk and impact of theft.

### 2.2. Privacy Initiatives

A number of recently proposed initiatives and regulations will require many industries to implement security measures to ensure the confidentiality and privacy of their data, often by encrypting stored data. The following are just a few of these initiatives:

| <u>Industry</u>      | <u>Initiative</u>   |
|----------------------|---|
| Healthcare           | Health Insurance Portability and Accountability Act (HIPAA) |
| Financial Services   | Graham-Leach-Bliley Act (GLBA)                              |
| Credit Card Services | VISA USA Cardholder Information Security Program (CISP)     |

Compliance with the encryption requirements outlined in these initiatives is difficult in existing storage environments. While software-based encryption technologies are currently available, they incur significant performance penalties and provide inherently lower levels of security. Software encryption cannot address mandates for widespread data security in heterogeneous environments.

### **3. Current Approaches**

Whether the mandate for data security comes from within an organization or from the need to comply with external requirements, current technologies do not provide an acceptable solution. Technologies designed for network security were not designed specifically for the unique issues surrounding aggregated data storage.

#### ***3.1. Firewalls, Intrusion Detection Systems and Virtual Private Networks***

A firewall is designed to protect the perimeter of an enterprise network. If someone breaks through (or starts from inside), stored data is highly vulnerable. An Intrusion Detection System (IDS) will passively detect an intrusion and provide appropriate notification. A Virtual Private Network (VPN) provides data security for connections across public networks, but like a firewall, offers no protection against compromises from within.

These three technologies play an important role in network security, but they do not solve the unique security problems of networked storage. Today, management of the storage network means access to the data it contains. IT managers may wish to delegate management tasks, but are constrained by concerns about data access. Firewalls, IDS or VPN technologies cannot secure data against unauthorized access from insiders.

#### ***3.2. Software or Application-Level Encryption***

Software encryption can be useful to protect point-to-point communications, and for small projects such as a encrypting a single file or a diskette. Software-based encryption is too slow to provide scalability, and encryption keys are stored in software, making them more vulnerable. Additionally, software solutions are primarily OS or application-specific and do not work seamlessly across heterogeneous environments. Software encryption cannot scale for enterprise-wide implementation.

#### ***3.3. Logical Unit Number (LUN) Masking***

Physical devices in a SAN are often subdivided into a number of smaller pieces. For example, a RAID storage system that serves one terabyte of raw storage might be configured to present storage in 50 gigabyte chunks - a total of 20 virtual or logical disks. Each chunk is identified at the SCSI layer via its own Logical Unit Number (LUN). The SCSI layer is in turn encapsulated within the Fibre Channel protocols.

LUN masking is a storage management technique for limiting the number of LUNs presented to the higher-level software, such as a database server, on a given host. LUN masking is a cumbersome, vendor-specific process that can easily lead to errors or overly-broad access, further undermining the security value. This low-level management tool does not scale. Furthermore, LUN masking is a property of the storage device, not the data. Once the data moves to other devices (i.e., tapes), the access restrictions imposed by LUN masking disappear. It also does not adequately solve another facet of the storage security problem: when data is stored in cleartext, storage administrators have access to all data.

### 3.4. Zoning

Zoning resembles LUN masking, but is implemented by switches at the Fibre Channel layer. Zoning allows a switch to segregate devices into logical groups, much like Virtual LANs (VLANs) in an Ethernet environment. Devices must be members of the same zone in order to intercommunicate.

Zoning comes in two basic forms. *Hard zoning* or *Port Zoning* defines zones based on switch ports. If a connection to a device is moved from one port to another, it will no longer be in the same zone unless the switch configuration is updated. *Soft zoning* or *WWN Zoning* uses the World Wide Name (WWN) of a device or port, a 64-bit value (represented as eight hexadecimal pairs) uniquely assigned by the device vendor. This logical assignment allows a device to be moved from one switch port to another without affecting its zone membership.

Like LUN masking, zoning is vendor-specific, cumbersome to implement, and difficult to scale. It does not solve many of the security problems in networked storage, since the data is left in clear-text.

### 3.5. Comparison of Approaches

|   | <b>Decru<br/>DataFort</b> | <b>firewall</b> | <b>VPN</b> | <b>file encryption<br/>software</b> | <b>software from<br/>switch vendor</b> |
|---|---------------------------|-----------------|------------|-------------------------------------|--|
| Protects against outsider sniffing                                | ×                         | ×               | ×          | ×                                   | ×                                      |
| Protects against insider sniffing                                 | ×                         |                 |            | ×                                   | ×                                      |
| Can separate storage administration from access to cleartext data | ×                         |                 |            |                                     |  |
| Can secure data even if disk is stolen                            | ×                         |                 |            | ×                                   |  |
| Works in multi-vendor environment                                 | ×                         | ×               | ×          |                                     |  |
| Minimal impact on performance                                     | ×                         |                 |            |                                     | ×                                      |
| Compartmentalization of workgroup data                            | ×                         |                 |            |                                     |  |
| Backups are protected   | ×                         |                 |            |                                     |  |
| Secure remote access  | ×                         | ×               | ×          |                                     |  |

## 4. Decru DataFort Security Appliance

The DataFort encryption appliance combines comprehensive security features in a hardened hardware platform, optimized for performance and reliability. The DataFort interoperates seamlessly within existing environments. The Decru DataFort does not require changes to application and database servers or to switch or storage devices. It fits into the network as a “storage proxy”, appearing as a new server to storage clients while appearing as another client to storage servers. Figure 1 illustrates a simple deployment in a file server (NAS) environment.

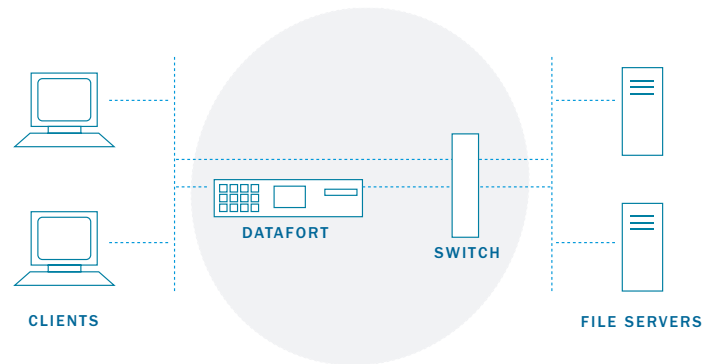


Figure 1

### 4.1. Wire-Speed Performance

The DataFort appliance was designed from the ground up to protect networked storage, using security-optimized hardware that is less vulnerable to attack than off-the-shelf hardware and software. At the heart of the appliance is the Storage Encryption Processor (SEP), a hardware engine that performs gigabit-speed, full-duplex encryption. This secure processor encrypts and decrypts data while ensuring both data and key security.

### Hardened Architecture

The SEP is fully protected within DataFort. DataFort is designed to meet Federal Information Processing Standard (FIPS) 140-2 Level 2 requirements. The SEP board, DataFort's encryption engine, is designed for even more secure FIPS 140-2 Level 3 compliance. Cleartext keys never leave the SEP hardware, making it extremely difficult for an attacker to compromise a key. A Decru-hardened operating system called DecruOS further strengthens secure operation.

## ***4.2. Security Features***

With Decru DataFort, data assets are secured without impeding workflow or requiring infrastructure changes. Incorporating a hardened architecture, two-factor authentication, secure key management and standard AES or 3DES encryption, Decru DataFort creates a transparent security solution that is powerful, yet still easy to use and manage. DataFort maintains a secure audit trail and enables secure backup and mirroring.

### ***Authentication***

Authentication plays a key role in the security provided by DataFort, ensuring only authorized users have access to stored data. DataFort can be configured to support a variety of authentication methods, which can be selected based on the security policies of an enterprise.

DataFort supports the predominant network authentication methods for network file sharing. DataFort can authenticate Microsoft Windows users with Active Directory and NT LAN Manager (NTLM), while Unix users can be authenticated via NIS and NIS+ (Network Information Service). In addition to Active Directory, NTLM and NIS/NIS+, DataFort supports additional layers of authentication. For example, DataFort administrators utilize a Decru-initialized Smart Card to add security for administrative roles.

### ***Advanced Key Management***

Decru DataFort utilizes an advanced, comprehensive key management system that ensures very high levels of security with no changes to user workflow. The Decru key management system is designed for operational efficiency, fully automating many administrative functions. In order to streamline key backups and restores, a hierarchical encryption method is employed. Data Encryption Keys (DEK), the keys used to encrypt the data, are themselves encrypted by a Master Key (MK). Even within the DataFort, DEKs are always held in encrypted form, ensuring exceptional security. In addition, since the DEKs are always encrypted, they can be backed up and restored easily and securely. The DataFort is designed such that the MK is always protected. For a complete explanation of the Decru key encryption system, contact [info@decru.com](mailto:info@decru.com).

### ***Compartmentalization***

A Cryptainer<sup>(tm)</sup> is an encrypted container of data, encrypted with its own, unique key. In a file server environment, each Cryptainer is manifested as an NFS export or CIFS share, and its contents (files, directories, folders) have their own keys that are further encrypted by the Cryptainer key. In a SAN environment, a Cryptainer is a separate LUN. Cryptainers are used to compartmentalize data within a storage device, so users from one workgroup cannot access data belonging to another workgroup unless explicitly authorized to do so. In addition to a unique key, each Cryptainer has an access control list (ACL) defining who may access and decrypt the data inside.

## *Encryption Standards, Optimized for Storage*

DataFort uses the following strong, proven encryption standards:

- **AES (Advanced Encryption Standard)** is a newer standard, selected by the US National Institute of Standards and Technology (NIST) to be a successor of 3DES and other cryptographic algorithms. As of May 26, 2002, the US Government requires AES for all of its sensitive communications. It is defined in Federal Information Processing Standard (FIPS) 197.
- **3DES (Triple Data Encryption Standard)** is an older US government standard, based on DES, which was developed by IBM with collaboration from the National Security Agency (NSA) and the National Bureau of Standards (NBS), a predecessor of the National Institute of Standards and Technology (NIST). The standard is defined in FIPS 46-3 and also in ANSI X9.32.

Some vendors' implementation of these standards can reduce the effectiveness of the security they provide. The Decru implementation of these standard algorithms is designed to maximize security for storage environments. Features include:

- **Long keys:** The longer the key, the more difficult it is for a hacker to break. With Decru's AES implementation, users can select up to 256-bit keys.
- **True random number generation:** Software-only solutions use pseudo-random number generators, the output of which can be guessed given knowledge of the seed and algorithm. This compromises the quality of keys based on these numbers. DataFort hardware incorporates a true random number generator (TRNG), ensuring that keys are truly unpredictable.
- **Avoiding predictable patterns:** Similarities or patterns in encrypted data may be exploited if identical files encrypt to identical ciphertext. DataFort uses a value, computed from the logical offset of the encryption block, as an additional input to the encryption function. DataFort also employs a different key for each file in file sharing environments, so identical data in different encryption blocks will result in different ciphertext.

## *Audit Trail*

Decru DataFort maintains an activity log, which is encrypted and cryptographically signed to ensure that it cannot be modified without detection. Administrators can elect to maintain a log of a large variety of activities, including:

- System configuration changes
- Administrator and user logins
- File access attempts
- Cryptainer accesses
- Amount of data transferred

The audit trail can be exported/saved through syslog to different devices on the network.

## 4.2. Usability Features

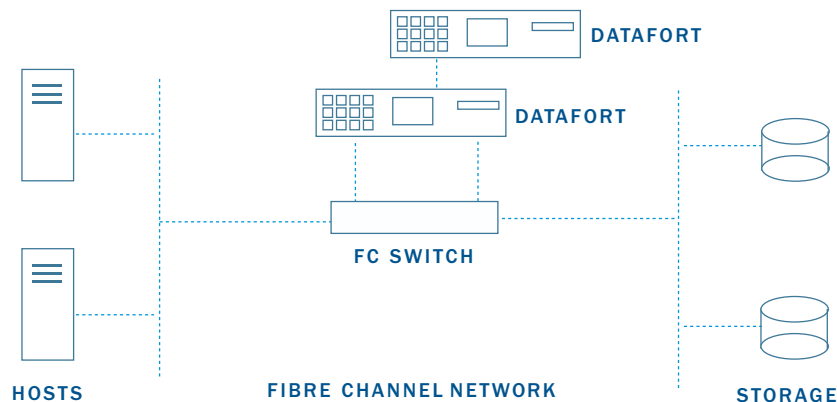
A DataFort appliance is an easy-to-deploy device that integrates into any SAN or NAS storage network. It is scalable, installs in less than 30 minutes, and does not require additional user or server software. Installed between clients or hosts and the storage device, the DataFort appliance functions as a proxy. It accepts data from the client, encrypts it using standard AES or 3DES algorithms, and sends it to storage. When a user requests data, the DataFort authenticates the user, retrieves the data from storage, decrypts it and presents it to the user -- all at wire speed. The DataFort works seamlessly within both block-based (SAN) and file-based (NAS) networked storage environments. Security of the stored data is ensured while user workflow is not changed.

### *Operational Transparency*

Decru DataFort was designed to protect existing infrastructure investments, integrating seamlessly with databases, mail servers, and other applications layered upon various operating systems, file systems, and storage virtualization products in both SAN and NAS environments. No special software is required for either the application hosts or the storage devices, making the appliance easy to install and support. A sophisticated encryption key management system maximizes security with minimal administrative effort. DataFort also works with existing security technologies like firewalls, IDS, or VPNs, but with dramatically increased security for data.

### *Deployment and Reliability*

The DataFort appliance is available in two models. The DataFort FC440 uses Fibre Channel for SAN applications, while the DataFort E440 uses Gigabit Ethernet for NAS environments. DataFort can be deployed to provide an optimal level of data security within a given network topology. A DataFort appliance can operate as an in-line proxy within the traffic flow between application servers (mail servers, database servers, etc.) and the storage devices, whether SAN or NAS. A sample deployment is depicted in [Figure 2](#). DataFort appliances will usually be deployed in fail-over pairs to provide a system without a single point of failure.



**Figure 2:** Sample clustered deployment of Decru DataFort<sup>(tm)</sup> appliances

Although Fig. 2. shows the DataFort as connected physically in-line, that is not a requirement. For example, in a small installation with a single switch, the application server(s), DataFort, and storage server could all be attached to the same switch. The DataFort is logically in-line for storage access, and non-storage traffic (i.e. web) bypasses the DataFort.

### ***File System Transparency -- NFS, CIFS, Databases***

Decru DataFort works transparently in both NFS and CIFS environments, and authorized users can apply all operations to directories and files. All versions of NFS (V2 and V3, using either UDP or TCP) and CIFS (the dialects used by Windows NT, 98, 2000, and XP) protocols are supported.

### ***Migration of Unencrypted Data and Re-keying***

Once DataFort is physically connected, the process of data encryption can begin. Using unique patent pending technology, DataFort can transparently encrypt existing data while the data remains accessible to users. This allows organizations to encrypt their data for the first time without disruption. The same technology is used to re-encrypt data with a new key.

## **5. Disaster recovery, secure backup and mirroring**

Physical security of backup media has been a major concern for enterprises, because data is often stored on the backup media in cleartext, readable by anyone who can get access to it. Some newer devices offer encryption of this media, but performance can suffer and key management is simplistic. Because a single key is used, media containing a mix of data from multiple workgroups exposes all groups with a single compromise.

With DataFort installed, the physical security of backup media is not an issue because the data is indecipherable without the appropriate decryption keys -- which never leave the SEP hardware inside DataFort.

As enterprises exponentially increase the amount of data that requires backup, the backup process can become cumbersome and resource consuming. Consequently, mirroring data for backup and for disaster recovery is growing in popularity. The main advantage is quick data recovery, but the security issues are significant. Not only does an enterprise have two physical premises to secure, but there are more people with administrative privileges able to access the data. In addition, the data must travel across a wide-area network connection, which raises even more security issues.

Once DataFort is installed, mirrored data is secured. If the original data is stored in encrypted form, then the mirror of that data is also encrypted at the remote site. In addition, the data that travels across the wide-area link is encrypted, so any unauthorized access within the wide-area connection cannot compromise the privacy of the data.

Eliminating the risk of data exposure allows the use of shared disaster recovery facilities, reducing the expense of disaster recovery provisions. Consequently, more affordable disaster recovery may make it feasible to protect a larger portion of an enterprise's data.

## 6. Conclusion

As organizations seek to save money and improve access to data by implementing aggregated storage technologies such as file servers (NAS) and SANs, they have opened the door to much greater risks. New privacy initiatives are mandating greater attention to the security of stored data. Backup, mirroring, and disaster recovery requirements require a more sophisticated approach to data security.

While some common existing security technologies play an important role, they do not adequately meet the needs of storage security. Software-based storage security solutions are slow, limited in scope, and are not fully secure.

Decru offers a comprehensive solution to the storage security problem. Decru DataFort is a powerful, scalable, network appliance that is designed specifically for the task of securing stored data. DataFort enables organizations to reap the full benefits of networked storage, while ensuring that the data remains private and secure.