



Enterprise-Wide Storage Security with  
Decru DataFort™ Appliances

white  
paper

**CONTENTS**

1. Executive Summary
2. Trends in Data Security and Privacy
3. Solution Overview: Decru DataFort™ Storage Security Appliances
4. 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, SAN, iSCSI and backup tapes that aggregate data for storage 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. Data replication, 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.

The Decru solution represents the first and only unified platform for securing stored data across the enterprise, with support for NAS, DAS, SAN, Tape, and iSCSI environments. Decru DataFort™ storage security appliances use wire-speed encryption, granular access controls, strong authentication, and cryptographically-signed auditing to protect stored data. DataFort can be deployed transparently with no changes to applications, servers, desktops, storage, authentication, or user workflow, and negligible impact to overall performance.

Key storage security applications for the enterprise include:

- Secure storage consolidation
- Insider threat mitigation
- Regulatory compliance
- Database security
- Secure tape backup and disaster recovery

With Decru DataFort, enterprises and government organizations 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

Recent, highly-visible security breaches are causing companies to rethink security practices for data at rest in databases, storage networks, and during backup and disaster recovery. Research organizations including Gartner, Enterprise Strategy Group (ESG) and the Computer Security Institute/FBI are closely following data security. They have published troubling statistics about the cost and impact of security breaches, as organizations grow increasingly dependent on digital storage of their corporate data assets. Trends include:

- Recent disclosures about the loss of backup tapes containing regulated customer data have led organizations to rethink their data protection strategies. Iron Mountain, the leading provider of outsourced records and information management services, has strongly recommended that companies encrypt sensitive data on backup tapes.
- Gartner predicts that “By year-end 2006, failure to encrypt credit card numbers stored in a database will be considered legal negligence in civil cases of unauthorized disclosures. (0.8 probability)” and “By year-end 2007, 80 percent of Fortune 1000 enterprises will encrypt most critical “data at rest” (0.8 probability).”
- Industry is starting to self-regulate. Visa, Mastercard, and other credit card companies now require merchants and payment card processors to comply with their jointly-developed Payment Card Industry (PCI) security standard. Requirement 3 of the standard mandates that organizations “Protect Stored Data” and defines encryption as “the ultimate protection mechanism.”

The risk of unauthorized data access only increases as enterprises adopt larger storage network deployments with expanded access, using file sharing protocols such as CIFS and NFS, Fibre Channel, 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:

<b><u>Industry</u></b>	<b><u>Initiative</u></b>
Healthcare	Health Insurance Portability and Accountability Act (HIPAA)
Financial Services	Gramm-Leach-Bliley Act (GLBA)
Credit Card Services	VISA/Mastercard Payment Card Industry Data Security Standard (PCI)
All businesses with customers in CA	Senate Bill 1386 (SB 1386)/ AB 1950
All businesses with customers in NY	A04254

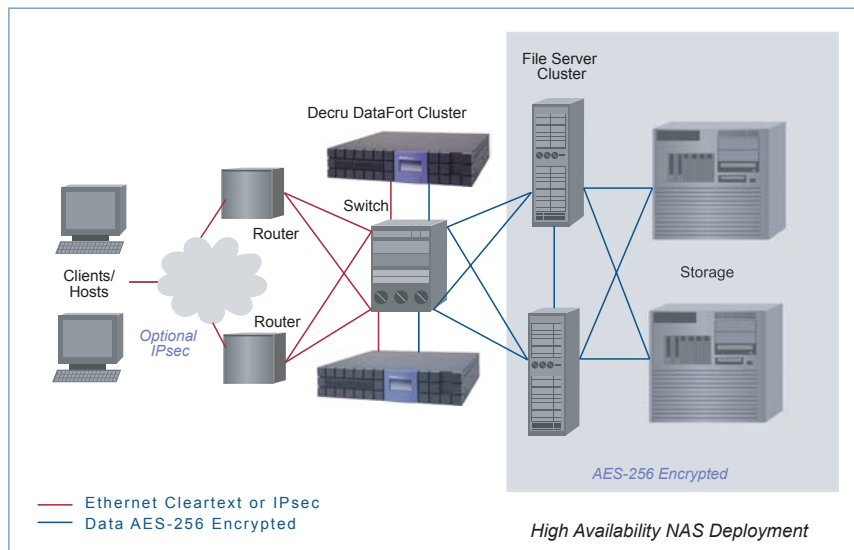
In the wake of the recent breaches, the US Congress has become even more involved in creating a national privacy initiative to protect consumers from identity theft. Proposed penalties for non-compliance include disclosure, fines, and in some proposed bills, jail time for the executives of the company responsible for data loss.

### 3. SOLUTION OVERVIEW: DECRU DATAFORT™ STORAGE SECURITY APPLIANCES

Decru DataFort™ appliances provide the only unified platform available to secure data at rest across the enterprise. DataFort appliances combine AES-256 encryption, authentication, strong access controls, and crypto-signed logging in a hardened platform, optimized for performance and reliability. DataFort fits transparently within SAN, NAS, DAS, iSCSI and Tape backup environments, and does not require any software to be installed on clients, servers, or storage devices.

DataFort can be deployed in the data path between clients or hosts and the storage device, either inline or attached to a switch. DataFort doesn't store data – it simply accepts data from the client/host, encrypts it using the AES algorithm, and sends it on to storage. When an authorized user or application requests data, DataFort authenticates the user or application, retrieves the data from storage, decrypts it and presents it back — all at wire speed. DataFort works seamlessly within both block-based (SAN/iSCSI) and file-based (NAS) networked storage environments. Security of the stored data is ensured while user or application workflow is not changed.

Figure 1 illustrates a simple, high-availability deployment in a file server (NAS) environment.



**Figure 1**

By encrypting data, and routing all access through secure hardware, Decru DataFort makes it easier for organizations to control and track data access. Encryption effectively blocks all back doors to data - protecting sensitive information on disk or tape against theft or misuse. Even if an unauthorized person gains access to the media, all they'll see are meaningless characters. Implemented correctly, encryption is a powerful tool that dramatically simplifies data security.

**But all encryption is not created equal.** There are a number of capabilities organizations should consider when evaluating encryption technologies:

#### 3.1. PERFORMANCE

One of the many advantages of using dedicated hardware for encryption is exceptional performance. Strong encryption is computationally expensive, and traditional, software-based encryption

methods are notoriously slow, as well as cumbersome to implement. In contrast, DataFort appliances can be deployed into an existing infrastructure in a matter of hours, without ever taking the data offline. Further, DataFort encrypts and decrypts at over 4 gigabits per second, easily keeping up with Gigabit Ethernet and 2 Gigabit Fibre Channel storage networks. Using unique “Cut-through Crypto” functionality (similar to data pipelining in a switch), DataFort delivers a port to port latency as low as 50-100 microseconds.

DataFort can be placed in a broad variety of locations within the network, depending on the desired security and throughput requirements. Because many storage networks do not consistently maximize the 2Gig pipe, it is quite feasible for one DataFort to handle many hosts and many storage devices simultaneously.

DataFort appliances can be deployed in active-active clusters for availability and failover, and additional appliances can be added to address higher throughput requirements.

### **3.2 TRANSPARENCY**

Decru DataFort was designed to secure data while protecting existing infrastructure investments. The system integrates seamlessly with databases, mail servers, storage management, backup and other applications layered upon various operating systems in all storage environments. Because DataFort speaks CIFS, NFS, iSCSI and Fibre Channel natively, no software or agents are required for either the application hosts or clients, making the appliance easy to install and support. DataFort also works with existing security technologies like firewalls, authentication schemes, IPS, and VPNs.

#### ***OS-Independence***

Software or database encryption solutions are operating-system dependent. They must be integrated into each client or application, and it's important to consider that security may be compromised when application or operating systems are upgraded. Because DataFort speaks the native protocols of the storage environment, it works with all operating systems, applications and versions, providing much greater security, and flexibility.

#### ***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 encrypt existing data in place without ever taking it offline. This allows organizations to encrypt their data for the first time without disrupting user or application workflow. The same technology is used to re-encrypt data with a new key in accordance with any rekeying policies, or even to return data to cleartext, should this be desired at some point in the future.

### **3.3 SECURITY**

While performance and easy implementation are important, perhaps the most crucial consideration for an encryption solution is the security of the system itself.

#### ***Hardened Architecture***

Software-based or application-level encryption solutions typically do not have a secure method for storing encryption keys: keys are kept in cleartext in an open operating system. This is a recipe for disaster if someone gains access to that machine.

DataFort appliances are designed from the ground up to protect data in networked storage, using security-optimized hardware that is less vulnerable to attack than off-the-shelf hardware and software solutions. At the heart of the appliance is the Storage Encryption Processor (SEP), a hardware engine that performs multi-gigabit-speed, full-

duplex encryption and decryption, while ensuring both data and key security.

Fully protected within DataFort's hardened chassis, complete with intrusion detection, the SEP has been certified by the National Institute of Standards and Technology (NIST) to meet the stringent security requirements of FIPS 140-2 Level 3 (Cert #439), and is in process for Common Criteria certification with a target of EAL-4+. Cleartext keys never leave the SEP hardware, making it extremely difficult for an attacker to compromise a key. A hardened operating system called DecruOS further strengthens secure operation.

### **Encryption Standards, Optimized for Storage**

DataFort uses strong, proven encryption standards. **AES (Advanced Encryption Standard)** is the strongest commercially-available encryption standard, identified by the US National Institute of Standards and Technology (NIST) as the successor to 3DES. It has recently been approved for use in Top Secret classified systems. Additional features of Decru's implementation include:

**Long keys:** The longer the key, the more difficult it is for an attacker to break. With Decru's AES encryption, users get the strength of 256-bit keys, while still achieving wire-speed performance.

**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 can 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.

It's also important to note that DataFort encryption does not increase the size of the stored data. In a SAN environment, DataFort does not change the size of data at all. For tape encryption, DataFort employs hardware-based compression before writing data to tape, resulting in a compression ratio of approximately 2:1. In a NAS environment, DataFort appends 512 bytes of data to each file header, a small addition that allows DataFort to track key information on a per-file basis.

### **Compartmentalization:**

DataFort uses Cryptainer<sup>®</sup> vaults to compartmentalize data within a storage device, so users from one workgroup cannot access data belonging to another unless explicitly authorized to do so. Data in each Cryptainer vault can be encrypted using a different key, providing for separation. In a file server/NAS environment, Cryptainer vaults can be defined using existing or new NFS exports or CIFS shares. In a SAN, Cryptainer vaults are defined on a LUN by LUN basis. For tape, encryption can be applied per host, per tape or per tape pool. Each Cryptainer vault is tied to an access control list (ACL) defining who may access and decrypt the data inside. DataFort also supports the deployment of "cleartext" Cryptainer vaults, so organizations can choose to encrypt only sensitive data, but still maintain a centralized interface for access control. Decru Cryptainer vaults enable organizations to securely consolidate storage.

### 3.4 KEY MANAGEMENT

When encrypting data that may be stored for months or years, secure, effective key management is crucial. Key management has always been a weakness in traditional encryption systems - requiring users or administrators to keep track of this important and highly sensitive information. Further, keys were often stored in cleartext on open operating systems, leading to a much higher likelihood of compromise.

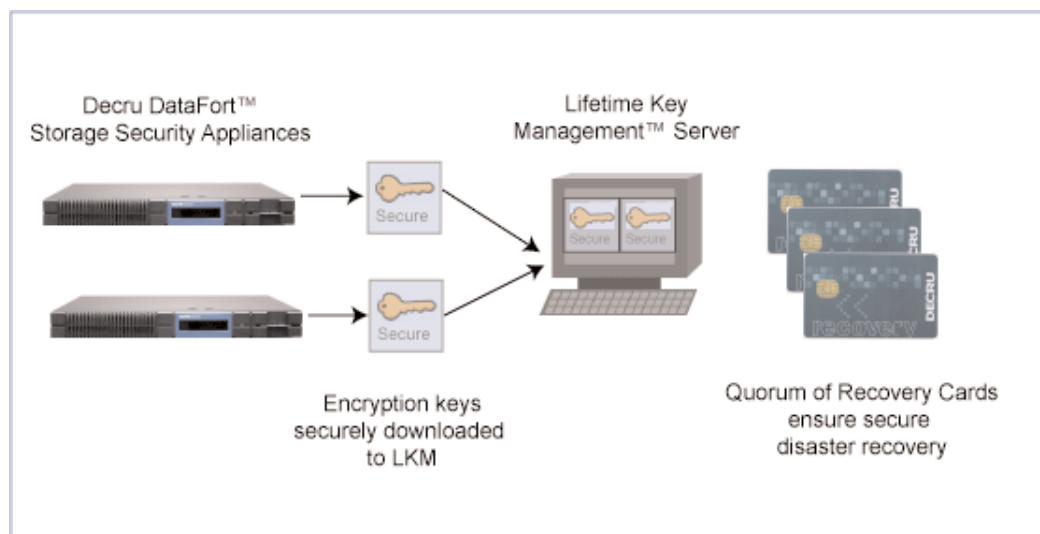
Decru changes this legacy with an innovative, layered key management system that removes the complexity commonly associated with encryption, yet ensures that the keys are fully protected and data can be restored, regardless of location.

Data is encrypted at the file level with a File Key, which ensures that even identical documents will result in different ciphertext. Further, each Cryptainer vault has its own encryption key, so aggregated storage can be cryptographically partitioned. Finally, these keys are wrapped in an additional layer of AES-256 encryption so they can be securely backed up outside DataFort.

**Runtime Key Management:** During normal operation, all keys are generated and maintained in a Configuration Database, inside DataFort's Storage Encryption Processor (SEP). Each DataFort keeps track of the key used to encrypt each piece of data, completely hiding this complex operation from users or administrators. DataFort appliances can be deployed in active-active clusters for availability, securely sharing keys via an IPsec tunnel.

**Lifetime Key Management System:** Decru also offers a software utility called Lifetime Key Management (LKM) which automates key archiving and management for all DataFort appliances across an enterprise. Any time a change is made to a DataFort (ie., a new key is generated, or a new host is added,) the appliance will make a copy of its ConfigDB, encrypt it, and push it securely to the LKM server. This ensures that LKM always has a current copy of every encryption key. LKM is typically used for information sharing and disaster recovery operations.

Figure 2 illustrates the automated archiving of encryption keys into the LKM server.



**Figure 2**

**Disaster Recovery:** DataFort key hierarchy comes into play during the event of a disaster, where a DataFort is destroyed or rendered inoperable. As previously mentioned, all DataFort appliances maintain a Configuration Database of all key material.

When DataFort is first deployed, the DataFort administrator will initialize a series of smart cards, called Recovery Cards. These 5 cards are typically distributed to trusted individuals within the organization, who create a username and password associated with each card. Note: these cards can also be placed in a safe, or several of the cards can be put into escrow, depending on the security policies of the organization. For the most secure deployment, these cards are used in a quorum, to prevent any one person from having complete access to sensitive operations. For example, 2/5 or 3/5 of the cards would be required to come together to support activities such as cloning a new DataFort, or replacing a smart card.

In the event of a disaster, there are three key ways to ensure that data can always be decrypted.

- 1) **Clustering:** First, DataFort appliances can be deployed in clusters, sharing key material and failing over if one path or device goes down. In the event that a complete cluster is destroyed, there are several recovery options:
- 2) **DataFort Cloning:** By combining a quorum of Recovery Cards with a Configuration Database (either stored independently or in the Lifetime Key Management system), a clone of the failed DataFort can be quickly configured.
- 3) **Software-based Recovery:** Decru also provides a Software Recovery Tool within the LKM, which allows an administrator to decrypt necessary data from a file, a Cryptainer, or a full DataFort using a standard server.

For a complete overview of DataFort Key Management, contact [info@decru.com](mailto:info@decru.com).

### **3.5 EXTENSIBILITY**

Data privacy should not be solved with point solutions. Sensitive data is frequently maintained in many different formats, from files to block-based data to backup tapes. With application-based encryption, organizations must manage separate implementations for each application, OS and environment. In contrast, Decru appliances provide a unified platform that create a foundation for security and compliance across the enterprise.

Decru is the only storage security vendor with appliances that can be field upgraded. The Decru SEP cryptographic module is based on Field Programmable Gate Array (FPGA) technology that can be adapted to modify algorithms, key management and other critical functionality. This gives Decru better control to adapt to emerging security trends and update the appliances in the field. Other solutions use off-the-shelf chips from third parties, and will be reliant on the original chip manufacturer's schedules and priorities.

### **3.6 ADDITIONAL SECURITY CAPABILITIES**

**Audit Trail:** Decru DataFort maintains an activity log, which is 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
- Cryptainer creations/deletions

- Security policy changes and rekeying functions
- File read/write access

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

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

In NAS environments, DataFort provides significant enhancements to existing enterprise access controls, with greater security and a single point of management. DataFort appliances support and enforce the predominant network authentication methods for CIFS and NFS network file sharing. DataFort can transparently authenticate Microsoft Windows users with Active Directory, NT LAN Manager (NTLM) and LDAP, while Unix users can be authenticated via LDAP and NIS (Network Information Service).

For Unix environments in particular, DataFort's granular and flexible access control lists (ACLs) represent a dramatic improvement over NIS directory capabilities. DataFort enforces access controls based on any combination of userID, group, IP address and directory, and fully supports multiple nested groups. DataFort's Group Review feature creates role separation, giving DataFort administrators the ability to approve or deny permissions granted by system admins via directory services. In SAN environments, Decru's host authentication features provide protection against WWN spoofing and other fabric-level attacks.

***Decru Client Security Module (DCS):*** Decru Client Security Module™ (DCS) enables end-to-end application security and policy enforcement, extending from desktops and host servers to the entire storage infrastructure. DCS software is optional, and can be deployed in conjunction with DataFort appliances to prevent unauthorized users, administrators, and viruses from accessing sensitive stored data.

#### 4. CONCLUSION

As organizations seek to save money and improve access to data by implementing aggregated storage technologies such as file servers (NAS) and SANs, and replicating this data for backup and disaster recovery, they have opened the door to much greater risks. Identity theft is costing companies and government organizations billions of dollars, and new privacy initiatives are mandating greater attention to the security of stored data.

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, enabling organizations to build defense in depth. 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.

#### **For more information on storage security solutions, contact:**

Decru, A NetApp Company  
275 Shoreline Drive, Fourth Floor  
Redwood City, CA 94065  
Tel: 1-877-22DECRO  
Email: info@decru.com