



SECURING

NETWORKED

STORAGE™

WHITE PAPER

COMPLIANCE SOLUTIONS FOR THE
PAYMENT CARD INDUSTRY
SECURITY STANDARD (PCI)

DECRU SOLUTIONS FOR PCI COMPLIANCE

Decru DataFort™ storage security appliances provide turnkey encryption and access control enforcement to protect cardholder data, supporting compliance with Visa and MasterCard's Payment Card Industry Security Standards (PCI). Decru solutions can be deployed transparently in heterogeneous environments without modifying existing applications, databases, or workflow.

BACKGROUND

In April 2000, Visa launched its Cardholder Information Security Program (CISP) - a sweeping set of mandates designed to protect its cardholders from identity theft and other misuse. Visa outlined key security requirements, along with a program for validation and auditing. In December of 2004, Visa and MasterCard joined forces to simplify compliance for merchants and payment processors with the jointly-developed, 12 point PCI standard.

The scope of these requirements is quite broad, incorporating best practices for perimeter security, data privacy, and layered security. Storage security solutions from Decru can dramatically simplify PCI compliance by enabling organizations to create a secure, encrypted and auditable data storage environment without requiring costly or cumbersome changes to the existing infrastructure.

THE STORAGE FACTOR

PCI clearly instructs organizations to protect stored data from unauthorized access - a challenge that has become more difficult over the last several years, due to a number of trends. Enterprises have spent billions of dollars on firewalls, intrusion prevention, and anti-virus solutions, but these systems provide little or no protection against internal threats. This is a serious exposure, since research indicates a significant majority of security breaches originate inside the firewall, where security is weakest. Stored data is vulnerable to a wide variety of external and internal threats - from insider attacks and hacking, to misconfiguration of complex storage infrastructures that leaves data exposed, to lost or stolen backup media.

Consolidation of storage into massive shared arrays has dramatically increased the exposure of data at rest - a single breach can now compromise terabytes of data, and millions of records. Enterprises routinely maintain 5-10 copies of data to support availability, compliance, backup and disaster recovery requirements, further complicating attempts to limit access. In most organizations, cleartext customer data is regularly backed up to tape, handed to third party couriers, and archived in third party storage facilities, increasing the risk of theft or loss.

PCI REQUIREMENTS

PCI incorporates 12 basic requirements designed to secure and protect cardholder data from unauthorized access. Penalties for noncompliance can be significant: for example, companies that experience breaches and are found to be non-compliant can face fines of up to \$500,000 per incident, in addition to other restrictions from Visa and MasterCard.

"Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle."

From: Requirement 3 -- Protect Stored Data
Payment Card Industry Data Security Standard

Decru security solutions can help enterprises build a strong foundation of trust and control for overall data security, while addressing a range of PCI requirements, including:

- Requirement 3: Protect Stored Data
- Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks
- Requirement 7: Restrict access to data by business need to know
- Requirement 9: Destroy media containing cardholder information when it is no longer needed

When deployed appropriately, Decru technology can also provide security features to support PCI requirements such as access controls and auditing.

PROTECTING STORED DATA WITH DECRU

Requirement 3 of the PCI standards directs organizations to "render sensitive cardholder data unreadable anywhere it is stored (including data on portable media, backup media, in logs and data received from or stored by wireless networks.") Suggested approaches include strong cryptography, such as AES-256 with associated key management processes and procedures. Further, PCI specifically requires organizations take steps to protect encryption keys against disclosure and misuse, including creating separate roles for sensitive key recovery functions.

Decru DataFort™ storage security appliances provide a turnkey, military-grade solution for protecting stored data assets. DataFort secures data at rest using wire-speed AES-256 encryption, secure access controls, authentication, and secure logging. DataFort can be deployed transparently with no changes to applications, servers, desktops, storage, authentication, or user workflow, and negligible impact to overall performance. The Decru solution represents the first and only unified platform for securing stored data across the enterprise, with support for all storage infrastructures such as NAS, DAS, SAN, IP-SAN and Tape.

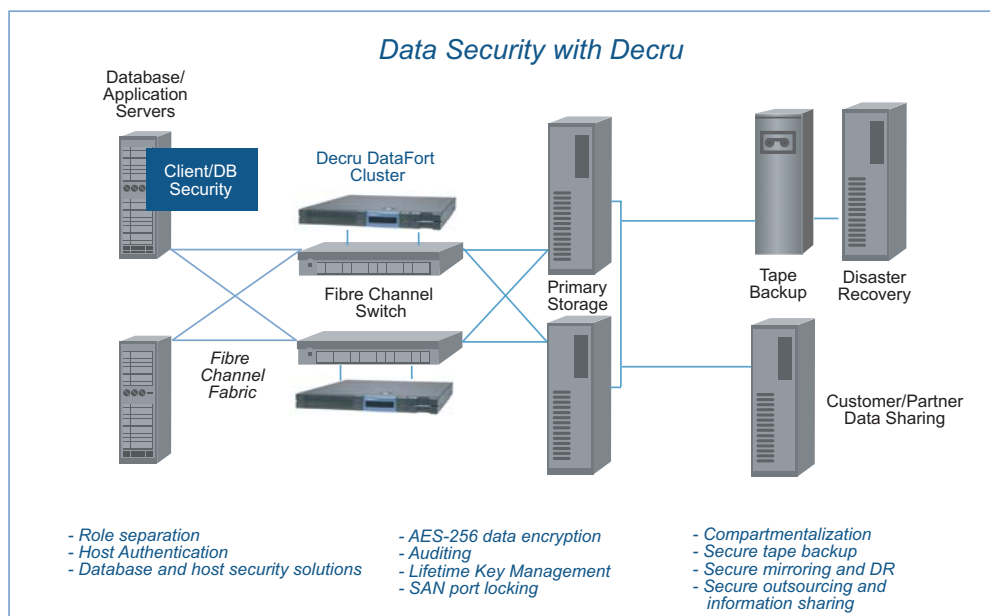


Figure 1: End-to-end security with Decru DataFort in Fibre Channel storage environment

DATAFORT FEATURES

Hardened Appliance: At the heart of the DataFort system is Decru's Storage Encryption Processor (SEP) - a robust hardware engine enabling full-duplex, multi-gigabit-speed encryption and key management. Decru DataFort incorporates strong AES-256 encryption, optimized by Decru for protecting stored data. Decru's SEP, clustering and key management have been validated by the National Institute for Standards and Technology (NIST) for compliance with FIPS 140-2 level 3. By incorporating all encryption and key management into the SEP, DataFort provides robust key security and removes the traditional complexity associated with software-based encryption technologies.

Compartmentalization: Security administrators can compartmentalize data in shared storage using Cryptainer[®] storage vaults. Cryptainer vaults cryptographically partition stored data, and provide an additional layer of threat containment. Cryptainers can be tied to access controls and authentication, supporting "need to know" access policies.

Lifetime Key Management™: Decru's Lifetime Key Management system (LKM) securely automates the archiving and recovery of encryption keys across the enterprise, ensuring data stored for decades can be decrypted. A software-based decryption utility ensures access to data in the event that DataFort hardware is unavailable.

Secure Logging: DataFort generates a tamper-evident, cryptographically-signed log of activities. Reports are customizable to track relevant events, including failed authentication attempts, Cryptainer access, administrative actions, or intrusion.

Endpoint security: Decru Host Authentication and port locking prevent host-based spoofing attacks, and Decru has been tested for interoperability with a range of endpoint and database security solutions. For example, the Cisco Security Agent consolidates multiple endpoint security functions in a single agent, including host intrusion prevention, spyware protection, malicious code protection, operating system integrity, and auditing. Decru has also been certified for interoperability with Oracle databases and Oracle's DataVault security features.

Operational Transparency: DataFort can be deployed in-line or connected to a switch, without changing the existing infrastructure. DataFort appliances natively support CIFS, NFS, Fibre Channel and iSCSI protocols for maximum transparency. Because only the data payload is encrypted, existing applications and management utilities can function without modification.

"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 (probability 0.8)."

When and How to Use Database Encryption
Feb, 2004 -- Rich Mogull -- Gartner Research

Media Disposal: If data is encrypted before it is written to disk or tape, and keys are stored in secure hardware, there is no risk of data being compromised if that media is lost or stolen. Encryption dramatically simplifies the process for media disposal, as there is no need to scrub or physically destroy the media. Further, the scheduled deletion of expired data becomes much easier. By simply deleting the key used to encrypt the data, organizations can immediately "shred" expired data - no matter where the data is stored, or how many copies have been made.

HOW DECROU DATAFORT APPLIANCES ADDRESS REQUIREMENT 3 OF PCI

Requirement 3 of PCI mandates that merchants and processors protect stored data. Decru appliances enable encryption for credit card numbers, and other sensitive cardholder data, with military-grade hardware that is in keeping with a range of PCI best practices.

For example:

Section 3.4 “Render sensitive cardholder data unreadable anywhere it is stored”

Decru DataFort appliances render data unreadable wherever it is stored (ie., on disk or tape) using FIPS-certified AES-256 bit encryption. A comprehensive, automated and secure system for key management is built in to the system.

Section 3.5 “Protect encryption keys against both disclosure and misuse”

DataFort encryption keys are generated, managed and maintained inside Decru’s secure hardware. They never leave the appliance in cleartext, and even management of encrypted keys is limited to certain DataFort administrators. Keys are stored securely inside the appliance, and can be encrypted and backed up to the Decru Lifetime Key Management system, used for centralized key management and disaster recovery.

“Protecting data at rest is a growing concern for many customers. The combination of Oracle’s proven security features with Decru DataFort’s hardware-based storage encryption provides a powerful secure platform. The Oracle-Decru solution provides a transparent and simple approach to protecting sensitive data..”

- Bronwyn Hastings, Vice President
Worldwide Alliances and Channels at Oracle

Section 3.6 “Fully document and implement all key management processes and procedures...”

Decru DataFort appliances address every requirement in this category:

- All keys are AES-256.
- Keys are encrypted before they leave a DataFort appliance, so they cannot be compromised during distribution or archiving.
- DataFort can rekey data in place on disk, without ever taking it offline, and for tape, keys can be changed on a per tape basis.
- No single administrator has the ability to recreate keys - this is divided among a quorum of Recovery Officers, and enforced by two factor authentication of a username/password associated with a smart card.
- DataFort appliances use DecruOS, a hardened operating system that further strengthens the security of the appliance.
- Keys are cryptographically signed when they are generated, so an unauthorized key will not be accepted by the system.
- It is possible to purge and replace any keys that may be compromised.

DATAFORT ADVANTAGES OVER APPLICATION-LEVEL SECURITY SOLUTIONS

Legacy encryption solutions have typically required modifications at the application or database level, and encryption has been limited to selected database columns due to performance restrictions. In contrast, DataFort’s transparent deployment model and wire-speed throughput enable much stronger security without trading off performance or simplicity.

DataFort advantages include:

Wire-speed performance: Strong encryption is computationally expensive, and application or column-level encryption solutions can have a significant performance impact. Software-based encryption steals cycles from the application server or host. Other solutions are deployed using out-of-band encryption appliances, which impose a round trip latency penalty with every read and write, severely limiting overall system performance. In contrast, DataFort appliances support 2 Gbps Fibre Channel and 1 Gbps Ethernet networks at wire-speed, and are deployed in-band within the existing infrastructure.

OS and Vendor Independence: DataFort speaks the native protocols of storage - so it works with all major OS versions, storage hardware, databases and software applications. Because software-based solutions integrate at the application layer, they are OS-dependent and may require customized installation for each environment.

Storage-Optimized Encryption: Unlike many column-level solutions, DataFort encryption does not increase the size of the data when encrypted. Further, DataFort FC-series appliances for tape have built-in hardware compression, so backup windows are not increased.

Easy to install, manage and upgrade: DataFort is typically installed in a few hours, enabling enterprises to immediately address a wide range of threats to stored data. To achieve comprehensive security at an application level requires significant custom integration, which must be taken into consideration any time changes are made to the storage or application environment. Moreover, column-level encryption often requires many fields to be left in cleartext, for example customer names and addresses that are needed for billing and customer service. DataFort protects all database fields and metadata from unauthorized disclosure.

Centralized, enterprise-wide key management: DataFort's key management is centralized and fully automated across clusters of DataFort appliances, providing strong security and high availability. Keys never leave DataFort's secure hardware in cleartext, and a quorum of recovery smart cards is required for sensitive key management operations. This ensures that no individual can override system security or compromise key management. In contrast, software-based solutions manage encryption keys locally in the operating system, leaving them vulnerable to a broad range of attacks.

Extensibility: Data privacy should not be solved with point solutions. DataFort offers a unified platform that can create a foundation for security and compliance across the entire enterprise. Sensitive data is frequently maintained in many different formats, from files to backup tapes. DataFort is the only solution that can address data security across all these formats.

SUMMARY

PCI is one of many emerging mandates designed to address data privacy and identity theft. HIPAA, GLBA, Basel II and California's SB1386 all identify encryption as a technology to support compliance with expanding privacy requirements. In fact, Gartner analysts recently estimated that "By year-end 2007, 80 percent of Fortune 1000 enterprises will encrypt most critical 'data at rest' (0.8 probability)." Decru's powerful, easy-to-deploy security solutions give organizations a strong, cost-effective method to address a wide range of privacy regulations, without trading off performance or simplicity.

For more information about Decru Storage Security solutions:

Visit: www.decru.com | Call: 1-888-22DECRO | Email: info@decru.com