

# CryptoStor™ FC

## High Performance Storage Security Appliance



### Complete Storage Security

- Remote Copy
- Backup and Restore
- Mirroring / Shadowing
- Enterprise Applications
- Managed Storage Services
- Shared Storage Facilities
- Disaster Recovery

### Designed for

- Large Enterprises
- Financial Services
- Healthcare / Insurance
- Government / Military
- Managed Service Providers
- Manufacturing / eCommerce

“Compliance to HIPAA and GLBA will require encryption of data all the way into storage devices.”

Christian Christiansen  
Vice President  
eBusiness Infrastructure and  
Internet Security Software,  
IDC Research

“Storage security practices and functionality are needed to assure SAN availability, integrity, and confidentiality.”

Paul Robinson  
Editor-In-Chief  
Secure Computing Magazine

NeoScale CryptoStor™ FC is the first gigabit speed, storage security appliance for total storage transport and media privacy. It is the only solution to meet the demanding needs of distributed storage infrastructures that can't compromise performance, security, or manageability. CryptoStor enables companies to readily achieve high-speed, end-to-end encryption, and policy-based security during data transport and media storage.

### Critical Storage Exposures

The migration from direct-attached storage (DAS) to sophisticated storage-area networks (SANs), network-attached storage (NAS), and geographically dispersed data storage availability introduces a host of security challenges.

Enterprise security has focused on front-end system exploits and network attacks, but it is not enough to protect back-end, distributed storage infrastructures. Storage management requires strong data transport and media protection to complement traditional configuration, monitoring, access controls, and zoning.

In the past, storage security gaps have been driven by cost and availability tradeoffs associated with performance impact, complexity, deployment constraints, and security strength. Now these risks can be cost-effectively addressed.

### Security Built for Storage

CryptoStor uniquely offers a platform and application independent means to readily secure both onsite and remote data storage mirroring, backup, and applications. Employing wire-speed, policy-based encryption over standard storage protocols, CryptoStor is the most flexible, scalable, and manageable solution for effective storage data confidentiality.

## Mitigating Storage Risks

Gartner and other research firms predict that the majority of server storage will be external and networked by 2005; this evolution is driven by the demand for storage capacity, business continuity, and managed availability. Unfortunately, the same physical and logical threats that exist in IP networks can also plague dedicated storage networks. This includes spoofing, denial of service, unauthorized access, data theft and modification, hi-jacking, device management breach, and internal abuse. How can companies protect their storage infrastructure investments – by implementing storage security best practices and a multi-tier defense strategy. Operational storage policies should be based on a risk assessment by storage function and business need. System and device configuration, testing, auditing and monitoring, access authentication, and zoning all reduce risk. Applying policy-based access and encryption of storage data during transport, on the storage subsystem, and on the media provides critical barriers against unauthorized disclosure and potential corruption.

## Security Appliance Advantages

CryptoStor provides reliable, wire-speed, policy-based enterprise storage security. Operating as an optimized, in-line storage appliance, CryptoStor inspects storage traffic and applies strong 3DES encryption at gigabit rates. Now storage data privacy policies can be centrally managed and conveniently modified to suit current and changing storage infrastructures. This approach dramatically simplifies the complexity associated with employing disparate storage data protection schemes. Since this solution is application and platform independent, deployment can be immediate and will not impact backup, replication, virtualization, or other storage applications such as Veritas Backup, EMC SRDF, or Oracle. Nor will it require SAN / NAS topology modification.

### Data Encryption Considerations

Alternative Approaches	Performance	Manageability	Cost	Deployment	Security
Application / File System	Server Impact / App Response	Difficult: Per App / Per OS	High	Difficult: Per App	Varies Per App
Storage Management S/W	Server Impact	Difficult: Per OS	Med	Difficult: Per Environment	Strength Varies
Fibre Channel or iSCSI Switch/Router	Network Impact	Varies by Vendor	High	Difficult: Per Device	FC Not Available
<b>NeoScale CryptoStor</b>	<b>Bump in Wire</b>	<b>Convenient</b>	<b>Low</b>	<b>Immediate</b>	<b>Strong</b>

## Policy-Based Storage Security

### Stateful Storage Processing™

Deep frame inspection allows for access and encryption policies to be dynamically and selectively applied at wire-speed based on user-defined storage security rules. Rule definition include WWN, SID, DID, LUN, SCSI Command, Block Range, and Time Period.

### Storage Media & Transport Privacy

On-the-fly, block level 3DES encryption/decryption of storage data with the ability to support different encrypt keys. Protects data through the fabric down to the subsystem and on the media; disk or tape.

### Storage Transport Privacy

End-to-end, native Fibre Channel tunneling/VPN using automated key exchange to protect both FCP routing and storage data.

### Storage Data Access Control

Automated safeguards for unauthorized or malicious actions against storage subsystems such as format or block overwrite commands.

## Enterprise-Class Protection

**More distributed secure data storage availability**

**Quicker / cost-effective storage security deployment**

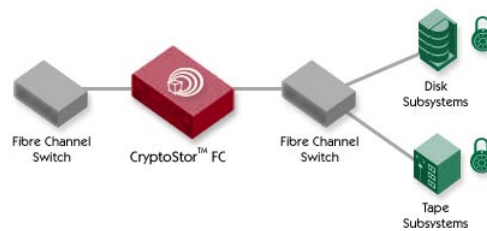
**Reduced storage security complexity**

### Key Features

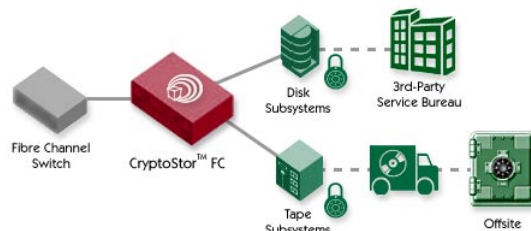
- Wire-speed, storage encryption for FC and GigE SANs
- Policy-based security using *Stateful Storage Processing™*
- Application, transport, and platform transparent media privacy
- Link protection and traffic blocking for FC SANs
- Less than 100 microsecond port-to-port latency
- Up to 4 modular 2-port channels (1 or 2 Gbps port config)
- Strong crypto key management / FIPS 140-2 compliant
- Multi-unit redundancy for fault-tolerant security
- Intuitive management and configuration (Web and CLI)
- Supports leading security, storage and network management standards, applications and frameworks

## Flexible, Rapid Deployment

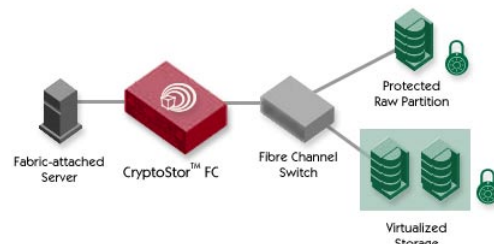
### Within Fabric



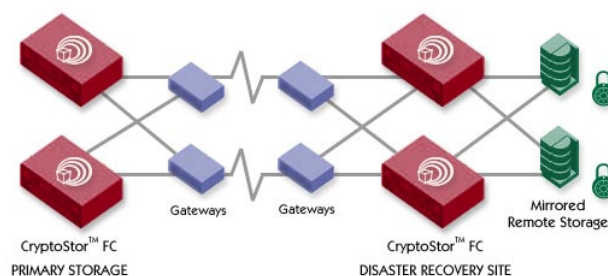
### Subsystem



### Application



### Gateway



## Storage Privacy Applications

<b>Remote Replication, Backup, and Disaster Recovery</b>	Availability <i>Means Risk</i> <sup>TM</sup> . Just as storage data can be sent to remote sites, so too can access policies and privacy controls be added at either the primary or secondary facilities.
<b>Managed / Shared Storage Resources</b>	Outsourced storage services provide great storage resource flexibility and cost-benefit. Storage data encryption eliminates risk of unauthorized third-party access. Zoning segregates but does not eliminate unauthorized storage data access. With the introduction of virtualization, both confidential and non-sensitive data can be stored on the same physical device. Storage data encryption extends access control provisions to complement virtualization and zoning.
<b>Enterprise Application Storage</b>	Data encryption which is enabled on backup and application servers that directly accessing storage subsystems typically has tremendous operational impact. Moving the encryption processing to a dedicated appliance eliminates such performance constraints and centralizes storage security functions.
<b>Valued / Regulated Storage Data</b>	Sweeping changes in privacy legislation such as HIPAA, the Gramm-Leach-Bliley Act, and EC Directives, are creating liabilities for enterprises that fail to ensure data protection within all levels of their storage function. Clearly, data encryption at the storage level adds to compliance due-diligence.
<b>Tape Media Management</b>	Tape management exposures increase exponentially with greater distributed backup, tape vaulting, and service bureau distribution. Media encryption can lower security burdens and costs associated with required tape controls.

## Highlight Specifications

### Security

- SecureStor<sup>TM</sup> block level media privacy, FCSec<sup>TM</sup> link protection
- SRP/FCAP key exchange and authentication
- 3DES, DES, RC4, MD5, and SHA-1 standards
- SSH/SSL/TLS secure remote access controls
- Built-in and remote SmartCard reader support
- Multiple key insertion and generation options
- FIPS 140-2 – Level 2 Certification (planned)

### Storage

- Line-rate Storage Routing / Data Classification
- WWN, SID/DID, LUN Address, SCSI Filter
- FC & GigE Interfaces, 2 Ports / Channel
- FC modes: E, F and null-port operation
- DNS, Zoning, ELS, and Fabric MIB support
- Major Storage Device and Application Support
- SANmark Certification (planned)

### Management

- In-line, redundant deployment with automated policy exchange for fail-over support
- Multiple data preparation/recovery options
- Secure command-line and web interface
- 3 user levels with security officer key control
- SNMP-based alerting and system monitoring
- Complete logging and alerting capabilities
- System hardening and tamper-resistant

### Physical

- 2U 19" rack mountable, industrial construction
- Redundant, hot-swappable power supplies/fans
- 100/240 VAC, 50/60Hz, 200W



**CryptoStor<sup>TM</sup> FC**