DECRU®
A NetApp Company

DECRU DATAFORT™ STORAGE SECURITY APPLIANCES

Networked storage helps enterprises speed access to data and reduce administrative overhead, but can leave critical data vulnerable. Without the physical separation provided by traditional direct-attached storage, data assets become co-mingled in networked storage environments, putting them at much greater risk for unauthorized access, theft or misuse.

Technologies like firewalls and intrusion prevention systems seek to secure enterprise assets by protecting the perimeter of the network, but these approaches leave data at the storage core dangerously open to both internal and external attacks. Decru DataFort™ is a reliable, multi-gigabit-speed encryption appliance that integrates transparently into SAN, NAS, DAS, iSCSI and tape backup environments. By locking down stored data with strong encryption, and routing all access through secure hardware, DataFort radically simplifies the security model for networked storage.

performance

AT THE CRITICAL INTERSECTION OF DATA SECURITY AND NETWORKED STORAGE	THERE IS DATAFORT

MAXIMUM DATA SECURITY

Decru DataFort™ appliances combine secure access controls, authentication, storage encryption, and secure logging to provide unprecedented protection for sensitive stored data. Because DataFort protects data at rest and in flight with strong encryption, even organizations that outsource IT management can be sure their data assets are secure. In short, DataFort offers a powerful and cost-effective solution to address a broad range of external, internal, and physical threats to sensitive data.

HARDENED ARCHITECTURE: DataFort hardware was designed from the ground up for maximum security. At the heart of the system is Decru's Storage Encryption Processor (SEP) — a robust hardware engine enabling full-duplex, multi-gigabit-speed encryption and key management. Decru's SEP, clustering and key management been validated by the National Institute for Standards and Technology (NIST) for compliance with FIPS 140-2 level 3. DataFort's AES-256, SHA-256 and SHA-512 encryption implementations have also been certified.

ROBUST ENCRYPTION STANDARDS: DataFort appliances incorporate strong AES-256 encryption, optimized by Decru for protecting stored data. DataFort uses a True Random Number Generator (TRNG) to create keys, and cleartext keys never leave DataFort's secure hardware, offering the highest level of security against attacks.

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. DataFort also supports the creation of cleartext Cryptainer vaults, which enables administrators to enforce access controls centrally, but leave less sensitive data unencrypted.

LIFETIME KEY MANAGEMENT™: Decru's Lifetime Key Management™ system (LKM) securely automates the archiving and recovery of encryption keys across the enter-prise, ensuring data stored for decades can be decrypted. Data Decryption Software ensures access to data in the event that DataFort hardware is rendered inoperable.

AUTHENTICATION AND ACCESS CONTROLS: DataFort provides a powerful, single point of secure access controls and authentication for heterogeneous client and storage environments. DataFort integrates transparently with directory servers such as LDAP, Active Directory and NIS, and adds a layer of hardware-based policy enforcement that prevents common attacks. In SAN environments, DataFort can use Host Authentication to further lock down the fabric. DataFort also incorporates smart cards to ensure that only authorized administrators can configure and manage the DataFort.

Decru Smart Cards strengthen authentication for sensitive operations

STORAGE VPN: In Ethernet environments, DataFort can secure data in flight from the desktop or server with integrated Storage VPN features. DataFort supports IPsec or SSL with hardware-based acceleration, and WebDAV support enables secure, drag-and-drop access to networked storage for remote users or partners over the Internet.

SECURE LOGGING: Each DataFort keeps a cryptographically signed log of activities. Reports are fully customizable to track relevant events, including failed authentication attempts, Cryptainer access, administrative actions, or intrusion.

CRYPTOSHRED™ KEY DELETION: CryptoShred™ key deletion simplifies the process of permanently deleting data. By deleting an encryption key, all copies of associated data are instantly destroyed, regardless of physical location. CryptoShred provides vital functionality for a range of applications, including regulatory compliance, hardware redeployment or disposal, and protection for data in harm's way.

integrity

EASY TO DEPLOY

DataFort fits seamlessly into the existing storage infrastructure, adding critical security without impacting network performance or user workflow. Security advantages are realized without installing software on clients, servers or hosts, and authorized users can read, write and modify files as they always have, without changing their workflow.

OPERATIONAL TRANSPARENCY: DataFort can be deployed in-line or connected to a switch: to clients or hosts, DataFort looks like storage, and to storage, DataFort looks like clients or hosts. DataFort appliances support CIFS, NFS, iSCSI and Fibre Channel protocols for maximum transparency. Because only the payload is encrypted, existing applications - such as backups and restores - can function without modification.

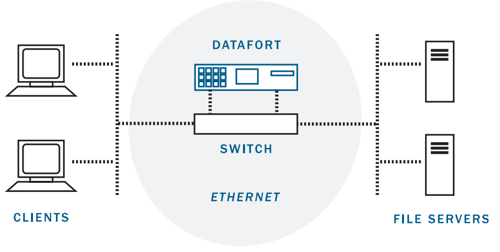
EASY TO MANAGE: DataFort can be installed in a matter of hours, and ongoing administration is simple and straightforward via a Web-based management interface. Industry-standard tools like SNMP and syslog can be used for monitoring, and DataFort's robust CLI allows scripting for common management tasks.

ENTERPRISE-CLASS RELIABILITY: DataFort hardware is built for maximum availability with minimal moving parts and no internal disks. DataFort can be installed in active-active clusters for automatic failover and linear scalability.

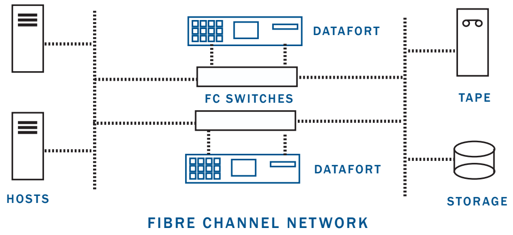
DEPLOYMENT OPTIONS

Decru DataFort is highly flexible and can be placed in a variety of locations within a storage network – either in-line or network-attached.

In a simplified example of a NAS environment, DataFort is shown on the IP network between department clients and the file servers. Clustered deployments are also supported.



In a basic SAN topology, DataFort can be connected to a Fibre Channel switch between the hosts and storage devices. A secondary DataFort can be installed for load balancing and failover, ensuring data will always be accessible.


DATAFORT
FC SWITCHES
DATAFORT
HOSTS
TAPE
STORAGE
FIBRE CHANNEL NETWORK