NetApp
Go further, faster

Infrastructure Solutions

NetApp DataFort Storage Security Systems

Secure valuable data without compromising simplicity

KEY BENEFITS

Maximize storage security
Get deep security for your most sensitive data using our layered security model.

Speed time to deployment
Install NetApp® DataFort appliances in hours without impacting network performance, availability, or user workflow.

Lower impact for users
Authorized users can read, write, and modify files as they always have, without changing how they work.

Simplify key management
Easily enforce security policies by associating keys to data sets using different levels of granularity.

Lower total cost of ownership
Reduce operational overhead by combining dedicated encryption appliances with preconfigured security policies and automated key management.

THE CHALLENGE

Electronic data is the lifeblood of business today. Keeping intellectual property and personal information safe becomes more difficult by the day. Storage consolidation increases the amount of data at risk from a single breach. At the same time, attacks are increasingly sophisticated, and the penalties associated with security breaches are more severe. Regulations regarding data integrity and data privacy impose high costs when companies fail to protect their data. One lost tape can compromise the personal information of millions of people and could cost a company billions of dollars in penalties and lost trust.

There is an easy way for you to meet this challenge: encryption. All encryption solutions, however, are not created equal. They differ in the depth of the security they provide, the speed with which they can be deployed, the ease of use for security administrators and end users, and their cost effectiveness. You need a storage security solution that will work seamlessly with your storage infrastructure without affecting network performance and data availability.

THE SOLUTION

You can secure data across your organization with a storage security solution that won't compromise ongoing operations. With our NetApp DataFort storage security appliances you can secure networked storage by locking down stored data with strong encryption and by routing access for your secured data through secure hardware. NetApp DataFort appliances are designed to maximize security without impacting network performance or user workflows. As a result, you can confidently and quickly encrypt all your sensitive data, whether it resides on NAS file servers, SAN and IP SAN storage systems, or tape media (FC and SCSI).

The NetApp DataFort Appliance Family

STORAGE TYPE	DATAFORT MODEL	INTERFACE
NAS/iSCSI	DataFort E-Series	Ethernet
Fibre Channel for SAN/Tape	DataFort FC-Series	Fibre Channel
SCSI Tape	DataFort S-Series	LVD SCSI

> "DataFort sold itself for a number of reasons, the most important being its ability to integrate into our current IT system, the transparency of DataFort to end users, and the data protection and reliability offered by DataFort hardware. NetApp DataFort offered us the ultimate security solution."

Vincent J. Fusca III, Project Manager, Dartmouth Atlas of Health Care and Operations Director, CECS

From Decru case study "Privacy and HIPAA Compliance at Dartmouth Medical School" (www.decru.com/solutions/pdf/dartmouthCS.pdf).

NetApp DataFort appliances are especially well suited for use in consolidated and virtualized storage environments across your entire storage infrastructure, including:

- Primary
- Backup
- Archival
- Compliance
- Disaster recovery

To prevent users from accessing the data of other workgroups, you can compartmentalize data in shared storage. Using our Cryptainer® storage vaults, data in each vault is encrypted using a different key. Further, you can use a central interface to manage access controls for all your data—whether it is encrypted or not.

MAXIMIZE SECURITY

NetApp DataFort storage security systems protect your data from a broad range of internal and external attacks. You get deep security for your sensitive data as a result of our layered security model.

Protect data at rest
At the heart of our NetApp DataFort appliance is our storage encryption processor (SEP), which enables full-duplex, multi-gigabit-speed encryption and key management. The National Institute for Standards and Technology has awarded our processor FIPS 140-2 level 3 certification—one of the highest levels awarded for security products. The SEP uses the AES-256 encryption algorithm as well as SHA-256 and SHA-512 hashing algorithms. All NetApp DataFort appliances use a hardware-generated true random number generator (TRNG) to create keys.

Protect data in flight
With our NetApp DataFort E-Series appliance, you can protect data in transit between authorized client machines and the NetApp DataFort appliances using an optional storage VPN feature. NetApp DataFort supports IPSec or SSL with a hardware-based acceleration card.

Protect against theft and tampering
Your NetApp DataFort appliance is secure—even if it is stolen. It will not power up without insertion of the required system card. If someone tries to physically probe the NetApp DataFort appliance in an attempt to access encrypted data, the appliance disables all encryption and decryption services and deletes all encryption keys, making the protected data unavailable.

For added security, you can protect your DataFort appliance from unauthorized administrative access by requiring two-factor authentication with smart cards. For sensitive recovery operations, a quorum of cards is required to make sure no single administrator can compromise your security environment.

Protect against attacks on your file server
If a malicious user takes control of your file server and tries to change access controls, your NetApp DataFort E-Series appliance will reject those changes until a security administrator explicitly grants access using the appliance.

Protect against attacks on your windows active directory server
If a malicious user takes control of your Active Directory server and makes changes to passwords or group memberships, your NetApp DataFort E-Series appliance will automatically reject those changes unless the security administrator configures the DataFort appliance to accept them.

The Group Review feature augments access control by requiring your NetApp DataFort administrator to review and accept or reject newcomers to groups in any domain. Users added to a Windows® group are not automatically given permission to access the encrypted share through the NetApp DataFort appliance.

Protect against operating system runtime attacks
All security-related tasks are performed in the security-hardened NetApp DataFort appliance, not in the operating system. As a result, your DataFort appliance is immune from OS runtime attacks.

Secure logs
All log functions are secure on NetApp DataFort appliances. Audit logs are tamper proof, and NetApp DataFort appliances keep a cryptographically signed log of all activities. Your NetApp DataFort appliance can help you enforce compliance through nonrepudiative logs. It generates cryptographically signed logs of all activities, making it impossible for someone to modify or delete a log without the knowledge of your DataFort appliance administrator.

LOWER IMPACT FOR USERS

You can install NetApp DataFort appliances—in-line or connected to a switch—in a matter of hours. NetApp DataFort appliances support all standard storage protocols to integrate transparently into your SAN, NAS, iSCSI, and tape environments. With NetApp DataFort appliances, you can add critical storage security without impacting network performance, availability, or user workflow. You can realize our security advantages without having to install software on clients, servers, or hosts. Your authorized users can read, write, and modify files as they always have, without changing how they work.

High availability
To help make sure that your encrypted data is always accessible to users and applications, you can set up NetApp DataFort appliances in clusters. All keys and configuration information is shared among the appliances in the cluster. If one DataFort appliance fails, others in the cluster will take over.

REDUCE MANAGEMENT COMPLEXITY

With NetApp Lifetime Key Management™ appliances, our centralized administration console, and SecureView software, you can manage all NetApp DataFort appliances in your environment from a single machine. You can work the way you want: use industry-standard tools such as SNMP and syslog for monitoring or use a command-line interface for scripting common management tasks.

Simplified key management
Basic key management for reading and writing data is completely transparent and fully automated. In addition, NetApp DataFort encryption provides greater functionality for secure information sharing or data scrubbing applications. For example, with backup applications, you can apply encryption per tape, per tape pool, or simply use one key for all tapes. You can also apply key expiration dates so that keys are automatically deleted in accordance with your data retention policies.

Securely share data with trusted partners
Share sensitive data with a trusted partner by encrypting that data with a unique encryption key. Partners can decrypt the data using a NetApp DataFort appliance or with NetApp data decryption software.

Nondisruptive rekeying of data
Our background encryption function allows you to periodically rekey your encrypted data for additional security and still maintain access to your encrypted data during the process.

LOWER TOTAL COST OF OWNERSHIP

Calculating total cost of ownership for a storage security solution involves more than the purchase price of the solution. We can help lower your total cost of ownership in several ways:

- You can leverage your DataFort storage security appliances by connecting them with a switch and using them for multiple hosts.
- You can save on administrative staff by using a single security platform to

protect data wherever it resides in your organization and managing it from a central location using a single management system. Managing a different security system for each different type of storage adds complexity and raises operational costs.

- You can save your administrators' time and save money with our simplified security management and automation of common tasks.
- You can protect your existing infrastructure investments because the DataFort appliances are designed to integrate seamlessly into your existing infrastructure.

SPEED TIME TO DEPLOYMENT

Our fixed-price, fixed-scope DataFort Design and Implementation service can help you quickly and efficiently deploy your DataFort storage security appliances with minimal impact to ongoing operations. Our service provides an optimal design based on best-in-class NetApp storage security technology that facilitates a smooth and efficient deployment into complex, distributed environments. Our highly trained and experienced NetApp or partner Professional Services engineers can help you reduce the risk of downtime and performance problems that might result from storage or software misconfigurations.

PARTNER FOR SUCCESS

When you partner with our Professional Services and Global Support teams, you gain access to our extensive storage security expertise, innovative technologies, and best practices. Our team works in partnership with you to solve your information security challenges so you can accelerate the return on your infrastructure investments and get the most business benefit from them. We share with you the experience we have gained by working with hundreds of organizations just like yours. We respond quickly to your problems, no matter where in the world they occur, and with one of the most flexible support programs in the industry, you always get just the support you need for your unique IT and business requirements.

DATAFORT STORAGE SECURITY APPLIANCE KEY FEATURES

FEATURE	DATAFORT E-SERIES	DATAFORT FC-SERIES	DATAFORT S-SERIES
ENCRYPTION			
FIPS 140-2 level 3 certification	•	•	•
Creates strong keys using AES-256 encryption and TRNG	•	•	•
Permanently delete data when you delete an encryption key using CryptoShred® key deletion	•	•	•
Background encryption keeps data available during rekey process	•	•	Not applicable
ACCESS			
Quorum-based authentication for sensitive security operations	•	•	•
Two-factor authentication with role-based admin control (optional)	•	•	•
Hardware-based secure VPN secures data in flight between client/host and DataFort appliance	•		
Host authentication		•	
Access controls	•		
Group review forces the DataFort appliance administrator to approve all newcomers to groups.	•		
User registration	•		
MANAGEMENT			
Remote authorization	•	•	•
Secure logging	•	•	•

NetApp creates innovative storage and data management solutions that accelerate business breakthroughs and deliver outstanding cost efficiency. Discover our passion for helping companies around the world go further, faster at NetApp.com.

© 2008 NetApp. All rights reserved. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, Cryptainer, CryptoShred, and Lifetime Key Management are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Windows is a registered trademark of Microsoft Corporation. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.
DS-2825-0708

NetApp™

www.netapp.com