HP NonStop Volume Level Encryption with DataFort
Agenda

- About NetApp
- Storage Security Background
- Introduction to DataFort
- Focus on Key Management
About NetApp
Delivering Customer Success

- Worldwide, enterprise customers
- Fastest growing storage company
  - Outpacing the industry by 3x
- Data Center proven solutions portfolio
- Industry-leading partners
- Comprehensive professional services
- Global support

- 6500+ Employees
- Distributed in 138+ countries
- 94,000+ installed systems

- Fortune 1000
- S&P 500
- NASDAQ 100
In August 2005 NetApp acquired Decru, an organization with an extensive security pedigree solely focused on Storage Security.

Decru was founded 2001 to solve emerging storage security problems:
- Regulatory compliance
- Identify theft and data privacy
- Insider threat

The acquisition of Decru has made NetApp the clear leader in storage security, with top tier enterprise and government customers.
Storage Security Background
Who Has Access to Sensitive Data?

- **CEO**
- **CFO**
- **General Counsel**

**Network Administrators**

- Customer Data
- Intellectual Property
- Salaries and Reviews
- Litigation Docs

**Storage Administrators**

- Storage
- Storage Repair/Service Staff
- Backup Administrators

**Outsourcing Vendors**

- DR Storage Administrators
- Tape Courier

**Salaries and Reviews**

- Storage Administrators

**Intellectual Property**

- Storage Administrators
Data Security Business Drivers

Best Practices

Compliance
Insider threat
Brand protection
Consolidation
Replication
Outsourcing
**Pros:**
- Granular options
- Encrypted at host
- Lower cost (SW)

**Cons:**
- CPU intensive, slow
- Weak Key Mgt
- Keys exposed in OS
- Complex to implement/manage
- Poor coverage for diverse environments

**Pros:**
- Transparent to host, storage, and apps
- Wire-speed encryption and compression
- Strong logging and Access Control
- HW-based - provides strong security

**Cons:**
- May require additional device

**Pros:**
- Transparent to host
- Bundled with HW

**Cons:**
- Immature key mgmt
- No support for diverse environments
- Lock-in to one vendor
- “Forklift upgrade”
- Not backwards compatible in many cases
Information Security Compromises

- High availability issues
- Performance degradation
- Key management complexity & security
- Application changes and downtime
- Database changes required
- Increased tape media usage
- Changes to desktops, servers, workflow

A proper solution must address all of these concerns.
DataFort is the industry’s only unified platform for securing data at rest across the entire enterprise.

DataFort integrates transparently into NAS, DAS, IP-SAN, FC-SAN & Tape (FC/SCSI/VTL) environments, and protect stored data with wire-speed encryption, strong access controls, authentication, and tamper-proof auditing.

**NAS/DAS/iSCSI:** *DataFort E-Series*
**SAN/Tape:** *DataFort FC-Series*
**SCSI Tape:** *DataFort S-Series*

*Lifetime Key Management™ system* for automated, secure enterprise-wide key management
**DataFort Storage Encryption**

**Data written to storage**

**Clients/Hosts**

**Data read from storage**

**Storage Encryption**

- **Cryptainer1**
- **Cryptainer2**
- **Cryptainer3**

**Authentication/Storage VPN**

- **ACL Enforcement**
- **IPSec/SSL (NAS)**
- **Supports AD/NIS/LDAP**
- **Crypto-signed logging**

**AES-256 Encrypted**

- **Compartmentalization**
- **Mitigates insider threats**
- **Information sharing**
- **Secure Key Management**
Example Deployment
Direct Attach Configuration: XP Array or FC Disk Module (FCDM)

HP Integrity NonStop server
(Also S-series NonStop)

NetApp DataFort FC-Series

NetApp LKM Appliance KM500

HP StorageWorks XP Arrays

Also supports:
HP FC Disk Module

* DataFort can also be deployed in-line with zero disruption to zones/WWNs
Example Deployment
XP Array configuration – with FC switches

HP Integrity NonStop server
(Also S-series NonStop)

NetApp DataFort FC-Series

NetApp LKM Appliance KM500

HP StorageWorks XP Arrays

Port Locking
SAN Host Authentication

AES-256 Encryption Cryptainer™ Vaults

* DataFort can also be deployed in-line with zero disruption to zones/WWNs
Future-Proof
- Industry’s only programmable encryption appliance
- Field-upgradeable with latest encryption algorithms and new features
- No hard disks

Secure
- Encryption boundary is physically encased in hardened epoxy
- Cleartext keys never leave SEP
- Hardware-based true random number generator (TRNG) enables high-entropy keys
DataFort Advantages

- **Transparent Deployment**
  - No application/database changes or downtime
  - Native support for NFS, CIFS, iSCSI, Fibre Channel, SCSI
  - No software agents required, appliance is OS-agnostic
  - Transparent rekeying enables zero downtime deployment

- **Wire-speed Performance**
  - Supports multi-gigabit line rate speeds
  - Less than 100 microsecond latency (FC) with ‘Cut-through Crypto’
  - Tape: Hardware-based compression before encryption

- **Hardware-based Security**
  - Clear-text keys never leave secure hardware
  - Highest level certifications (FIPS 140-2 Level 3, CC EAL4+ underway, DoD 5015.2)
  - Trusted by sensitive military, intelligence, banking customers

- **Secure Enterprise-wide Key Management**
  - Secure key sharing among clusters for availability and information sharing
  - Lifetime Key Management™ system for automated enterprise-wide mgmt
**System Card**
Cryptographic “ignition key” to boot DataFort and access encryption keys
Once initialized, each is unique to a particular DataFort

**Admin Card**
Provides 2 factor authentication for admins
RBAC allows multiple admins & roles
Can be shared among DataForts

**Recovery Cards**
Recovery Cards are initialized during install, and can be shared among multiple appliances
Quorum of Recovery Cards (2/5, 3/5, 2/3) is required for sensitive key management and recovery operations, providing role separation
IEEE SISWG: P1619 Encryption standard
- Emerging standard for ‘data at rest’ encryption
- NetApp was the co-author and continues to lead

ANSI T10
- Key Management standards for transferring keys between storage devices over SCSI protocol
- NetApp is an active member on this committee

Trusted Computing Group (TCG)
- Broad standards efforts covering Trusted Processor Modules (TPM), disk-drive based encryption, and key management
- NetApp is an active member in the TCG

Industry: OpenKey™
- Co-operative efforts from leading companies to further key management standards
The IEEE Security in Storage workgroup (SISWG) is working on standards for encrypted storage media.

Members of the groups include:
- Brocade
- Cisco
- NetApp
- EMC
- Hifn
- Hitachi
- HP
- IBM
- Optica
- PGP
- Quantum
- Seagate
- Stanford
- SUN

- P1619 – **Disk** (based on NetApp’s implementation)
  - Ratified and awaiting final publication
- P1619.1 – **Tape** (based on NetApp’s implementation)
  - Ratified and awaiting final publication
- P1619.2 - **Wide block for disk**
  - Drafts in progress
- P1619.3 - **Key Management** - (based on NetApp’s implementation)
  - Draft 1 being worked
Focus on Key Management
1. Each DataFort appliance provides automated, self-contained key management.

2. Keys are automatically and securely replicated to additional cluster nodes.

3. All DataFort appliances across the enterprise replicate keys to NetApp Lifetime Key Management™ (LKM) system, providing automated, secure enterprise-wide key management. Recovery smart cards enforce quorum approval for sensitive operations.
Key management Objectives

- **Ensure Availability**
  - Keys must be available where and when you need them
  - Redundancy in Key Management System is crucial

- **Policy Considerations for Key Management**
  - Key Retention
  - Key Rotation

- Strong key generation requires the use of truly random numbers generated exclusively with hardware devices

- Keys must be properly protected to prevent unauthorized access yet ensuring availability when expected to guarantee access to encrypted data.

- A secure method to destroy key materials at the end of their usable lifetime is preferential
Hardened Appliance
- FIPS 140-2 level 3 physical security
- Administrator Role Based Administration Control
- Tamper evident auditing and logging

Storage Encryption Processor (SEP)
- System Card for Ignition and physical security
- Recovery Cards for LKM recovery
- High entropy key source (TRNG) for third-party encryption endpoint

RAID-1 Disk Storage
- Synchronous (response only after write completes)

Hardened OS
- Non-executable stack and heap
- Statically linked code
Open Interface
- OpenKey™: Open Interface into NetApp Key Manager
- Complete API
- Secure network interface

Available and Secure
- High Availability Clustered Key Manager
- Enables secure key distribution and key access controls
- Data Policy Management
- Robust LKM DR capability that facilitate Oracle DR use cases
- Hardware based key management access controls
Partner program that enables development of interoperable encryption and key management solutions

- **Proven** -- Builds on a mature and proven key management platform, with over three years of deployments, some spanning globally-dispersed data centers

- **Grounded in Standards** -- The NetApp program builds on deep security expertise
  - NetApp co-chair and co-author for P1619, the IEEE standard for storage encryption
  - Involved heavily with the Trusted Computing Group and ANSI T10.

- **Whole Solution** -- NetApp LKM appliance is a secure, highly-scalable, centrally managed platform, and is the only solution that will serve encryption end points for ALL open storage protocols

- **NetApp OpenKey™ API:**
  - Centralized management of enterprise-wide, distributed security domains
  - Secure communication channels
  - High entropy key generation with TRNG
  - Developers’ kit with system/application requirements, test plans, and deployment guidelines
Who has access to sensitive data?

- Customer Data
- Intellectual Property
- Salaries and Reviews
- Litigation Docs

- Network Administrators
- Storage Administrators
- Storage Repair/Service Staff
- Backup Administrators

- Outsourcing Vendors
- DR Storage Administrators
- Tape Courier

- CEO
- CFO
- General Counsel
- System Administrators
- Backup Administrators
- Storage Administrators
- Storage Repair/Service Staff
- Tape Courier