



The Security Division of EMC

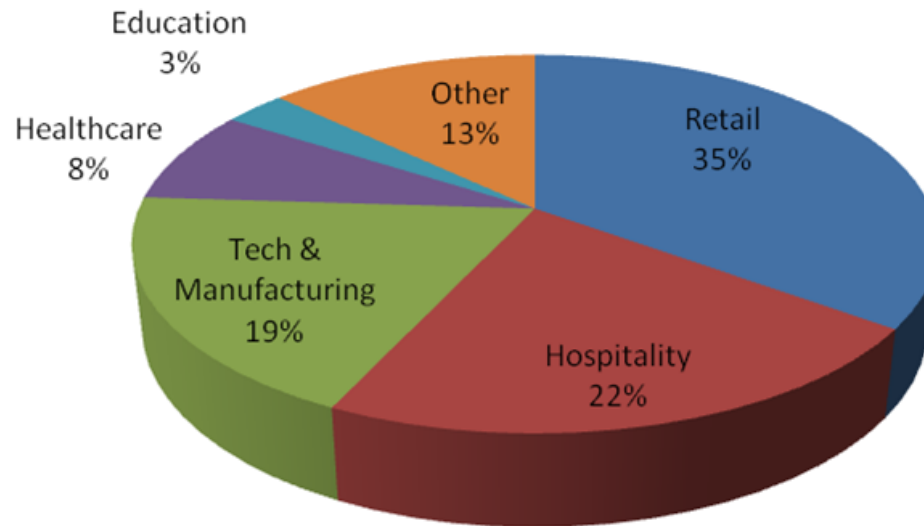
Securing Sensitive Data

EMC Forum 2010

What's Happening To Customer / Employee Data



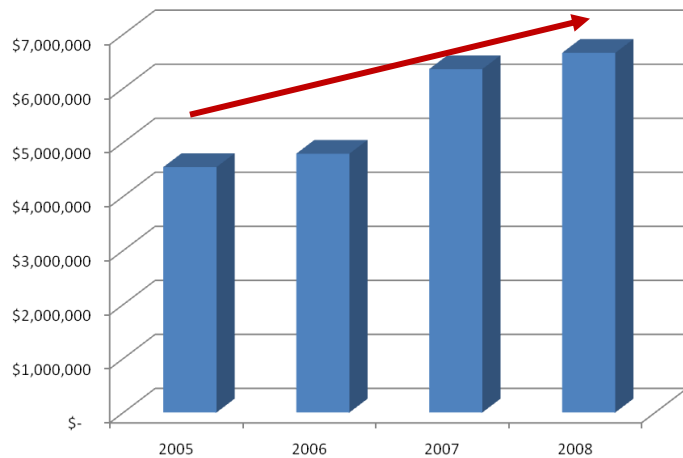
Data Leakage Incidents Between 2005-2008



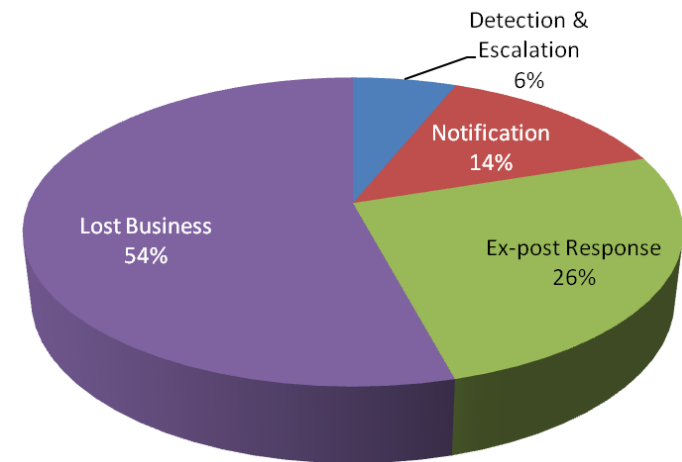
355,952,497 records reported to be lost since 2005

Cost of Data Breaches

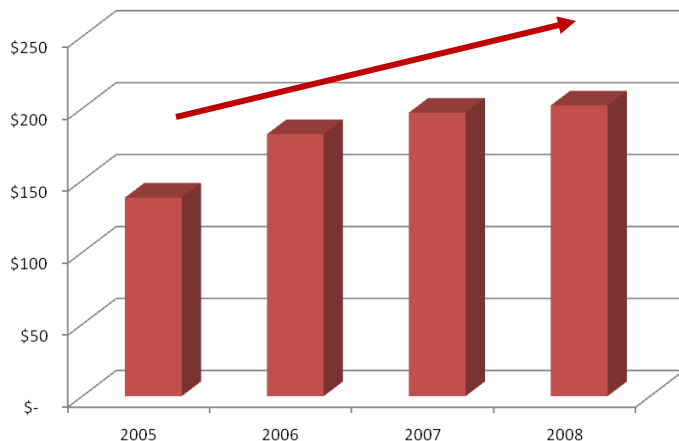
Average Cost Per Breach



Breach Costs Break Down



Average Cost Per Breached Record



- ➔ **Tangible financial impact**
- ➔ **Long-term damage to brand equity**
- ➔ **Total cost per breach is increasing**
- ➔ **44 US States have notification laws**
- ➔ **EU & Australia Data privacy policies**

Data Loss Prevention

Encryption and Key
Management

The Business Case for DLP

Reduce Risk | Minimize Cost | Avoid Disruption

Reduce Risk

1. What data can you catch? Where?
2. What can you do about it?
3. Time to Value

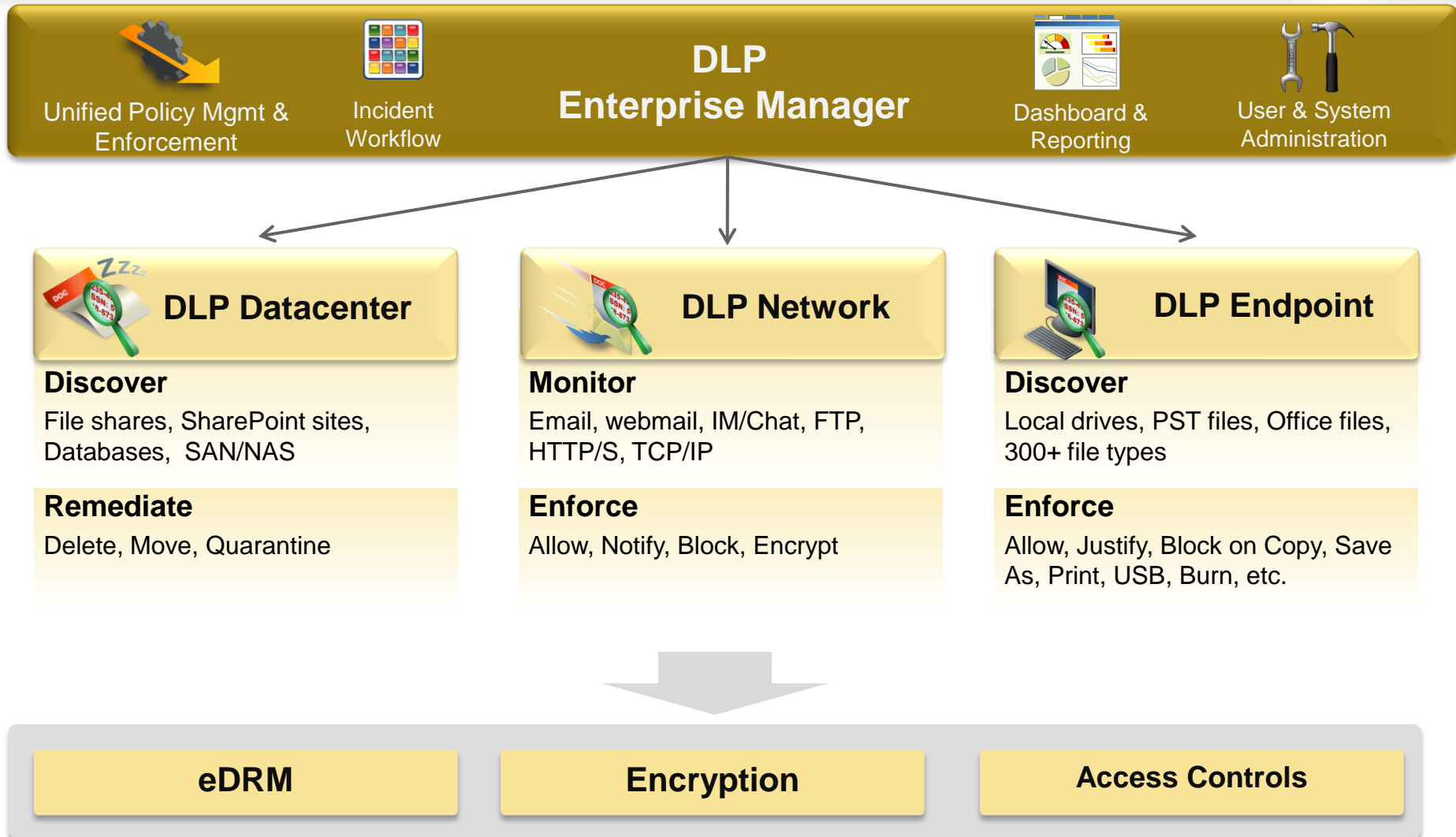
Minimize Cost

1. Product
2. People
 - a) Setup/Maintain
 - b) Investigations
 - c) Remediation
3. Infrastructure

Avoid Disruption

1. Consider the “who” not just “what”
2. Make controls transparent to users
3. Involve the data owners

RSA Data Loss Prevention Suite



Case Study: Technology Company

Microsoft®

Minimized risk by discovering all HBI data from 106K users

Driver

- Protect High Business Impact (HBI) Data
- PCI, PII and Intellectual Property

Situation

- 100 TB of data in file shares
- 30,000 file shares
- 120,000 SharePoint sites

Solution

- DLP Datacenter with site coordinators in Redmond, & India
- 12 machine Grid System

Results

- Selected for scalability, performance, accuracy
- Incremental scans in ½ day
- Managed by 2 people

Case Study: A Fortune 50 Retailer

LARGE ★ RETAILER

Identify and encrypt all emails containing credit card data

Driver

- Protect credit card data
- Payment Card Industry (PCI) Level 1 credit card processor

Situation

- Transmit 1 million plus emails per day
- ~2,000 contain sensitive data

Solution

- DLP Network integrated with Voltage IBE for encryption
- High availability configuration
- Installed in-between Exchange & Internet gateways

Results

- Higher accuracy than the competition with 2-3 False Positives per day
- No additional headcount allocated

Key Differentiators for the DLP Suite



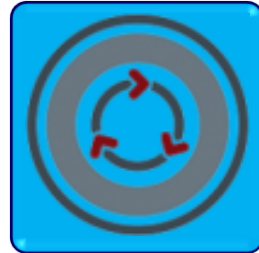
Policy & Classification

More policies and better policies for classification and risk mitigation



Identity Aware

Identity awareness for classification, controls and remediation



Incident Workflow

Consolidated alerts with the right information to the right people for the right actions



Enterprise Scalability

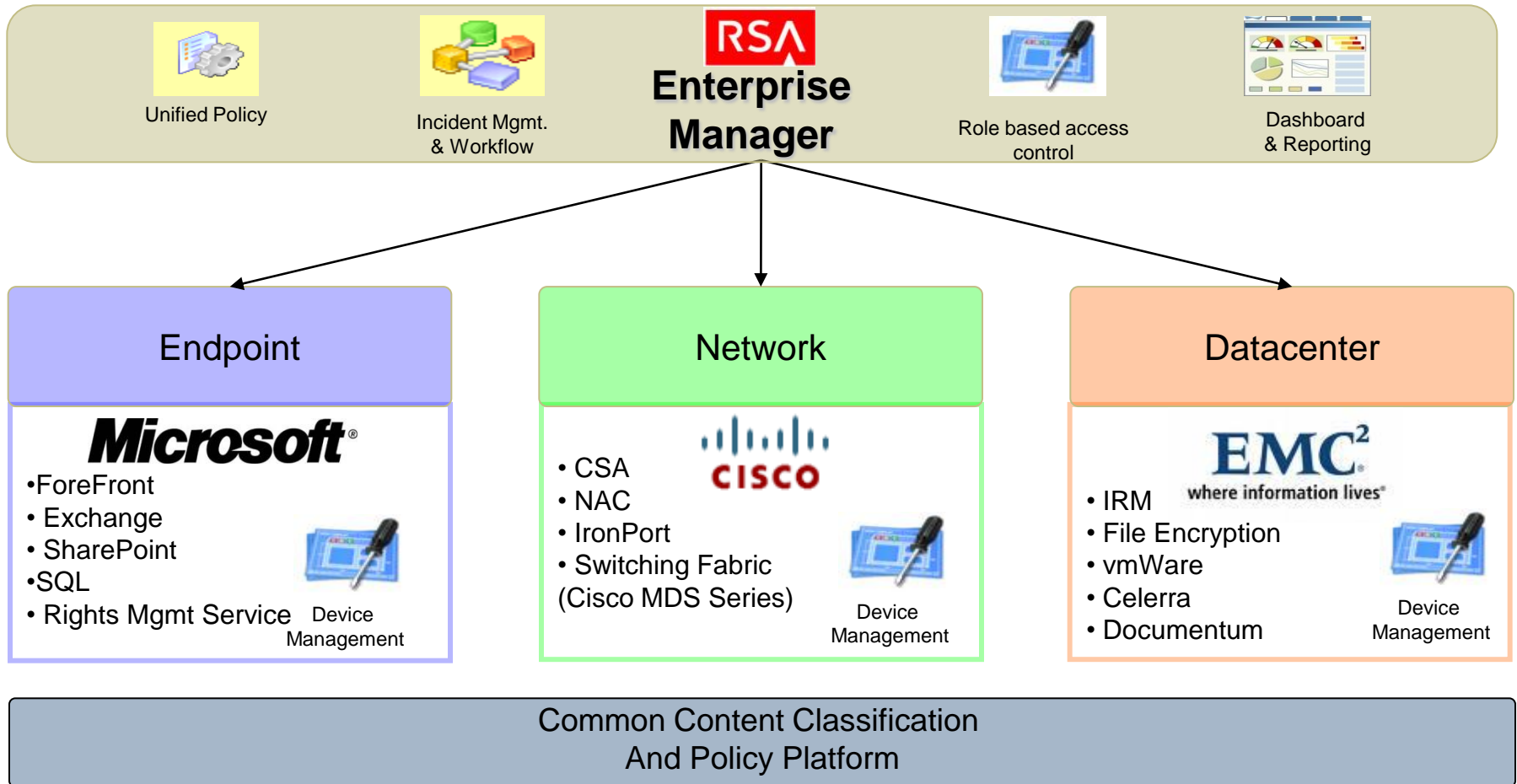
Scan more data faster with less hardware and resources



Built-In vs. Bolt-On

Common policies across the infrastructure - EMC, Cisco and Microsoft

Strategic Vision



How Can A DLP Solution Help?

Discover

- Identify and address sources of risk
- Identify broken business processes

Enforce

- Enforce data security policies for compliance
- Leverage third-party control solutions

Educate

- Educate employees on policy and risk
- Provide insight into violations & policies

Protect

- Monitor and protect all egress points
- Prevent sensitive data from leaking out

Data Loss Prevention

Encryption and Key
Management

Protection Methods

▶ Tokenization

- A PAN is “securely stored”, and a “token” is substituted
- Token can have similar characteristics to a card number
- Token has no cryptographic/mathematical relationship to the actual PAN

9837-4930-5838-3493

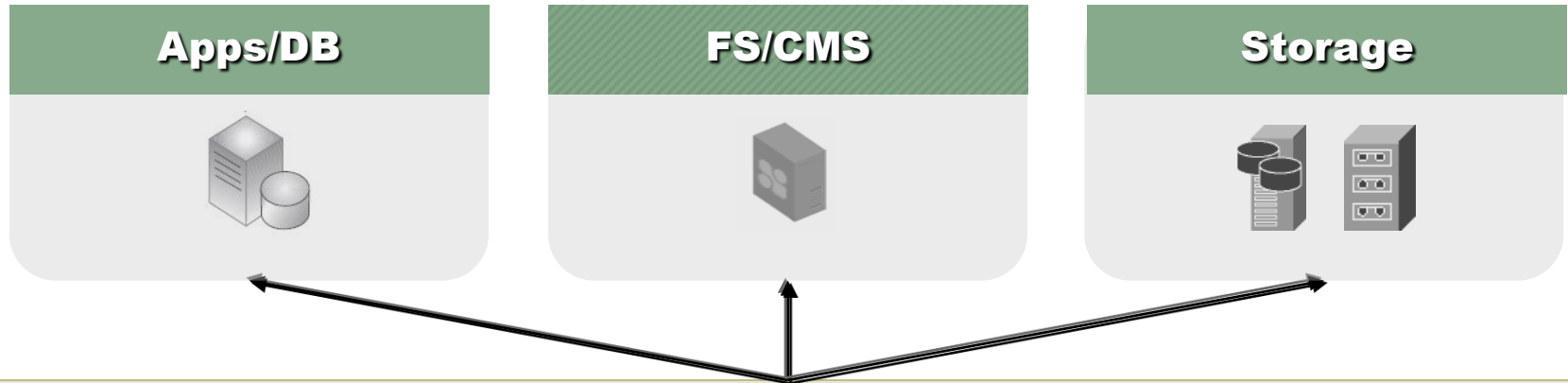
▶ Encryption

- PAN is encrypted, and can be stored anywhere
- Encryption keys must be securely managed

H&3Jk2)6\$m<L63qDs76mG* H&3Jk2)6\$w&qm<L63q
Ds7@mGlwv63lw&t3%m%m*w@q73Hte%nF29^!h1d=

RSA Key Manager

Enterprise-Wide Key Management



RSA Key Manager (RKM)

Policy-based Interface



1. Generate Keys



2. Securely Distribute Keys



3. Vault Keys



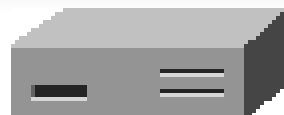
4. Expire / Turnover Keys



5. Monitor + Audit

RSA Key Manager

Enterprise-Wide Key Management



RKM Server

RSA Key Manager with Application Encryption



Application Encryption Client

- ▶ Sensitive data encrypted within applications at point of capture
- ▶ Application Encryption Clients- Comprehensive platform and language support
 - ▶ C, Java, .NET, Cobol, CICS
 - ▶ Linux, Mainframe, Unix, Windows

RSA Key Manager for the Datacenter

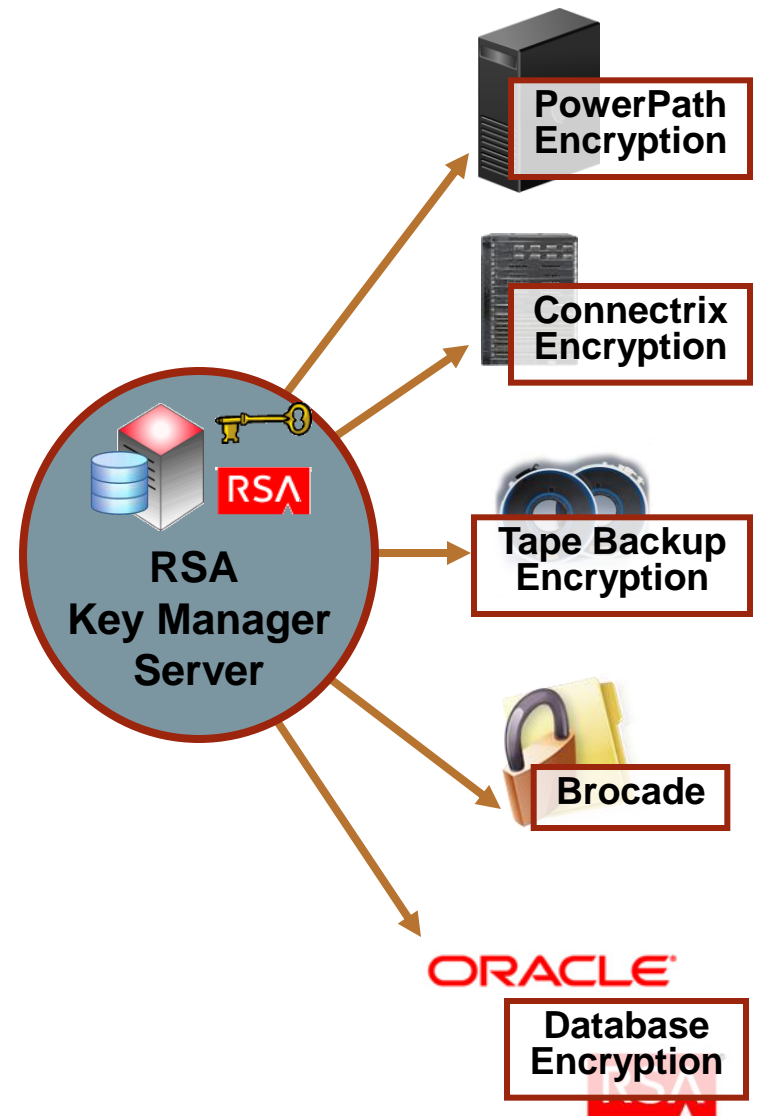


Integration modules EMC & 3rd party encryption

- ▶ Integrates with host, SAN switch, and native tape encryption solutions from RSA, EMC, and third parties
- ▶ Current integrations include , PowerPath, Connectrix/Brocade, Oracle and Native Tape

RSA Key Manager for the Datacenter

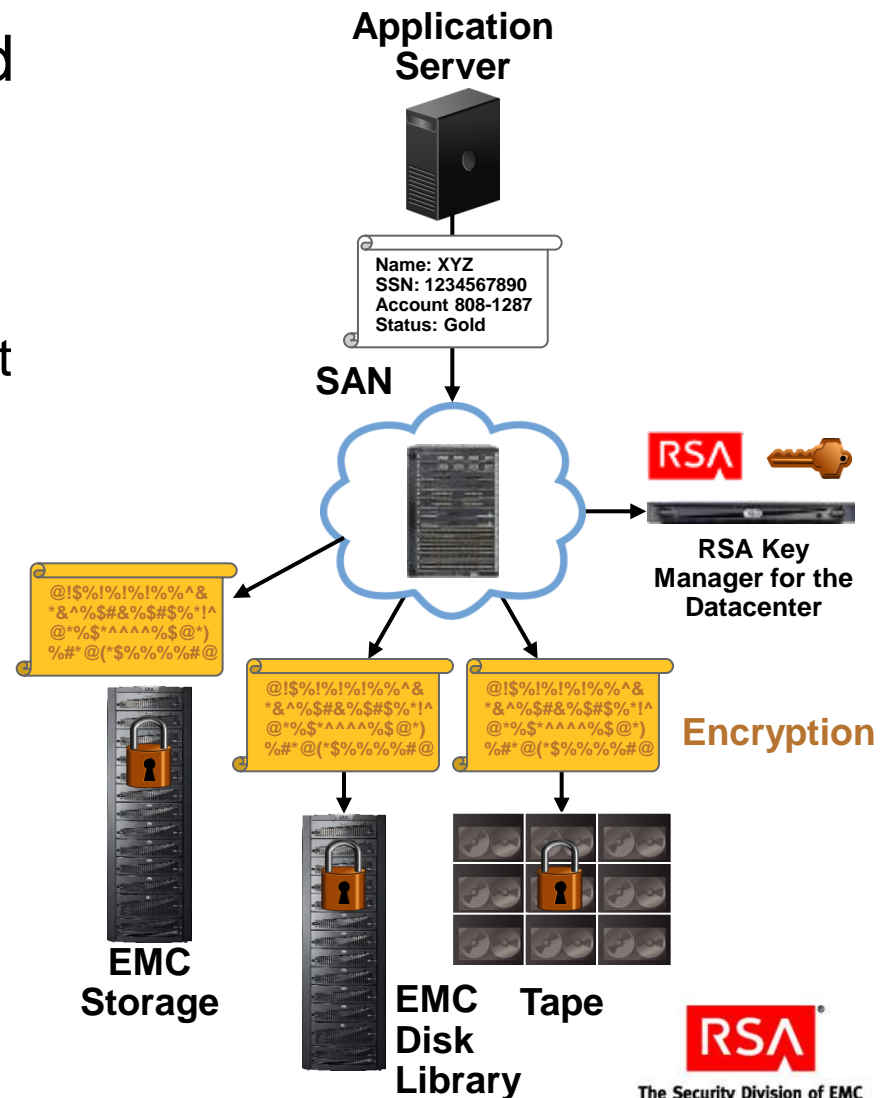
- ▶ Provides security over the long term
 - Vaults and protects encryption keys
- ▶ Scales across the enterprise
 - Centralized key management of encryption solutions across the IT stack
- ▶ Reduces cost and complexity over point key management solutions



EMC[®] Connectrix Storage Media Encryption with RSA[®] Key Manager for the Datacenter

SAN-Based Data Encryption for Tape and EMC Disk Libraries

- ▶ Requires encryption-enabled EMC Connectrix blade/modular switch
 - Nondisruptive installation
 - Implemented via a transparent fabric service
 - RKM provides enterprise key management

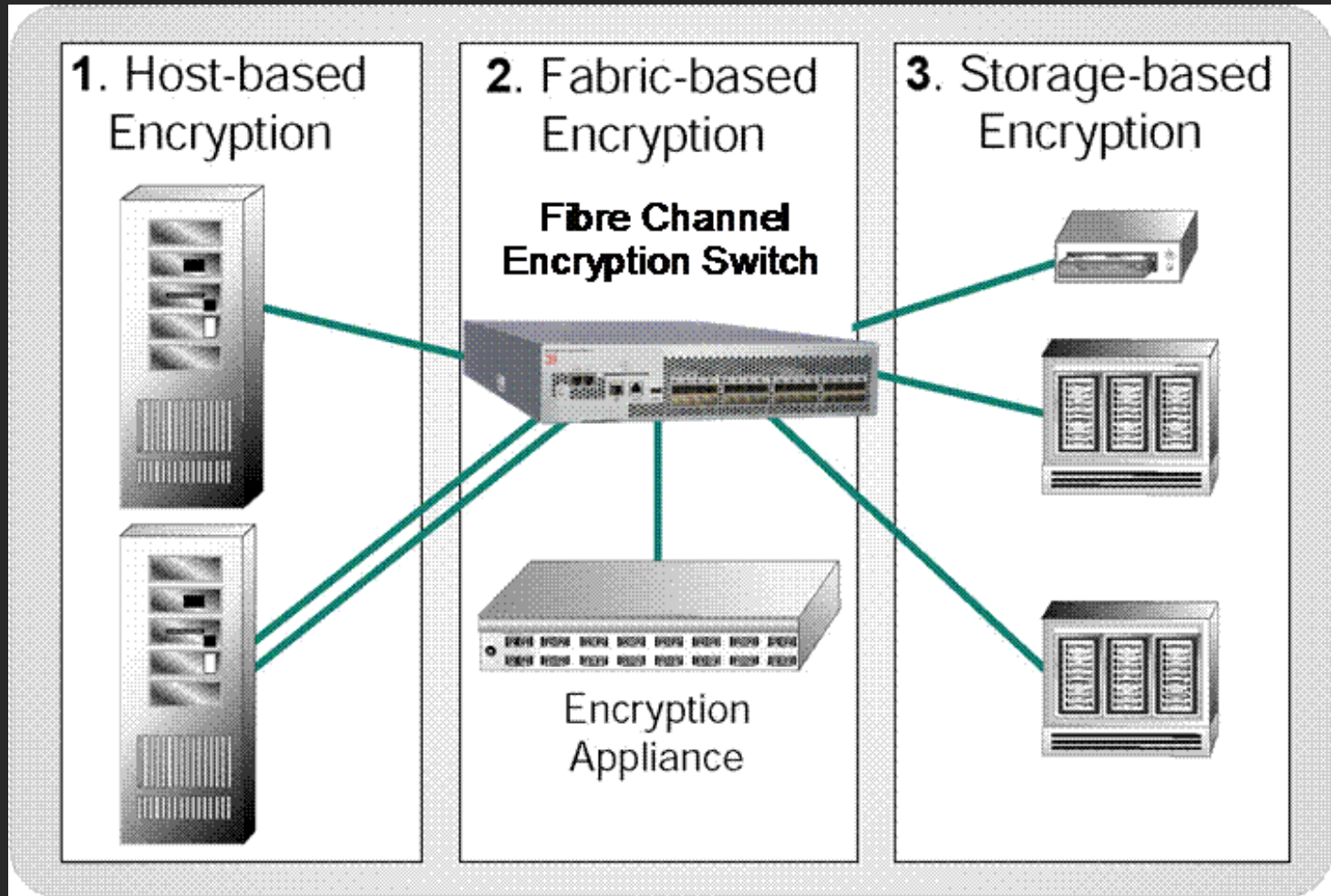


Brocade delivers encryption for data-at-rest today



Considering Encryption for Data-at-Rest

Three locations for block-based encryption



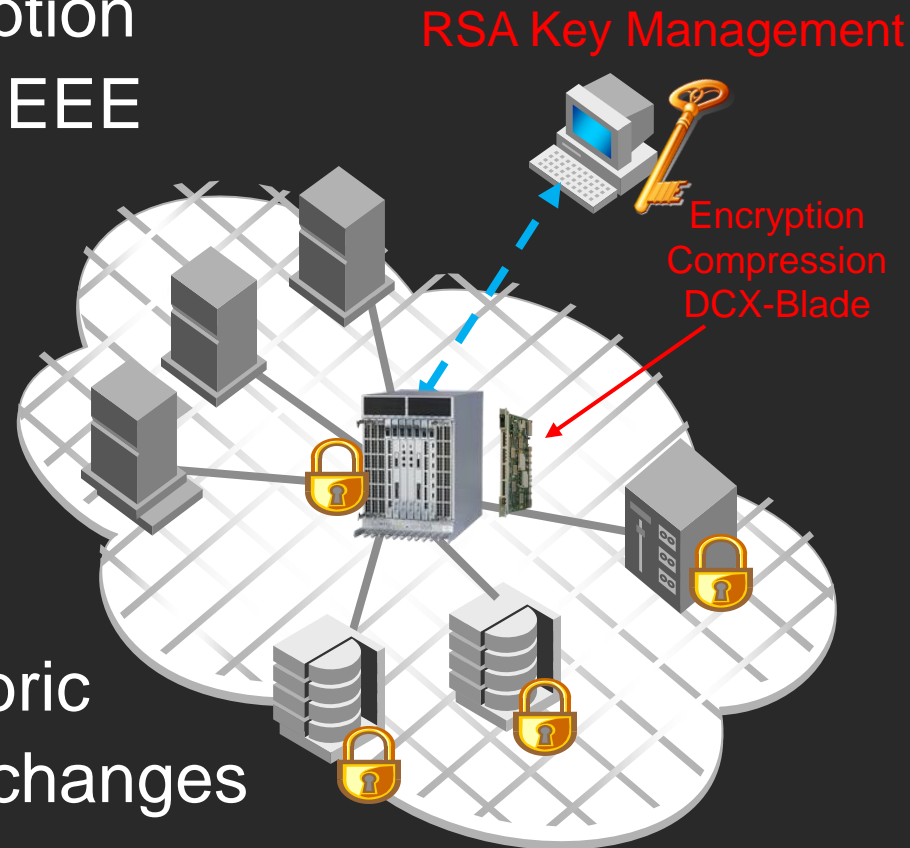
Fabric-Based Encryption for Data-at-Rest



- Connectrix B-series Solution
 - All data moves through the SAN
 - Central point of management
 - Plug-in encryption service
 - Centralized key management service
 - Highly scalable solution via Encryption Switch or Blade
 - Up to 96 Gbps disk encryption processing and 48 Gbps tape encryption with compression processing

Fabric-Based Encryption Solution

- Highest performance encryption processing available using IEEE 1619.x standard AES
 - AES-256 XTS for disk
 - AES-256 GCM for tape
- Wire speed compression prior to encrypting
- Easy installation into the fabric eliminates rezoning or PID changes
- Support for heterogeneous storage and tape systems



Connectrix ES-5832B

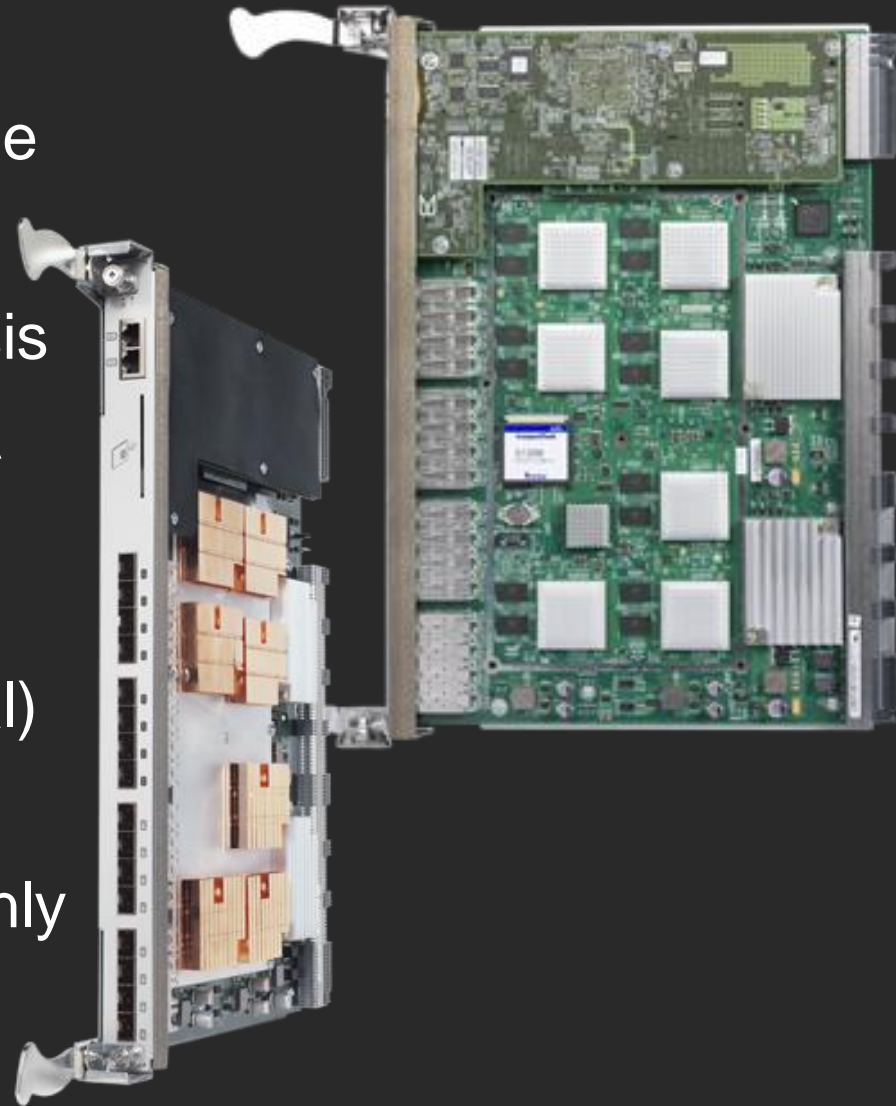
Hardware Overview

- 2U, 32-port 8 Gbps encryption standalone switch
 - 96 Gbps of encryption bandwidth for disk
 - 48 Gbps of encryption and compression bandwidth for tape
- Dual Ethernet ports for rekeying / HA synchronization
- Smart Card reader for crypto ignition function (optional)
- Dual hot-plug fans and power supplies
- FIPS 140-2 Level 3 Validated



Brocade FS8-18 (PB-DCX-16EB) Encryption Blade Overview

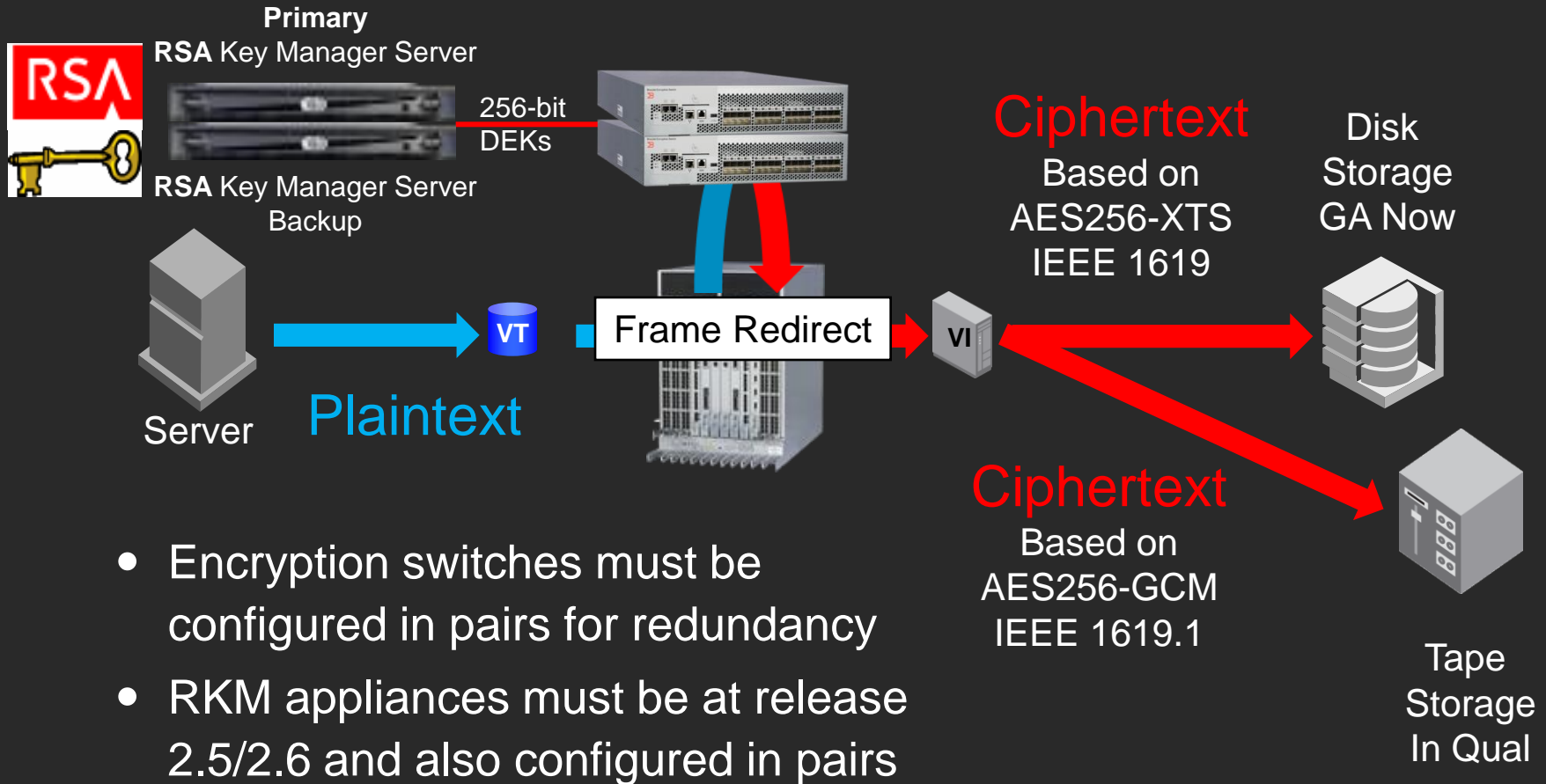
- 16-port 8 Gbps Encryption blade for DCX and DCX-4S
- Support for 1-4 blades in chassis
- Dual Ethernet for rekeying / HA synchronization
- Smart Card reader for crypto ignition function (optional)
- FIPS 140-2 Level 3 Validated
- DCX Backbone and DCX-4S only



BES/FS8-18 - Disk Encryption Rekeying

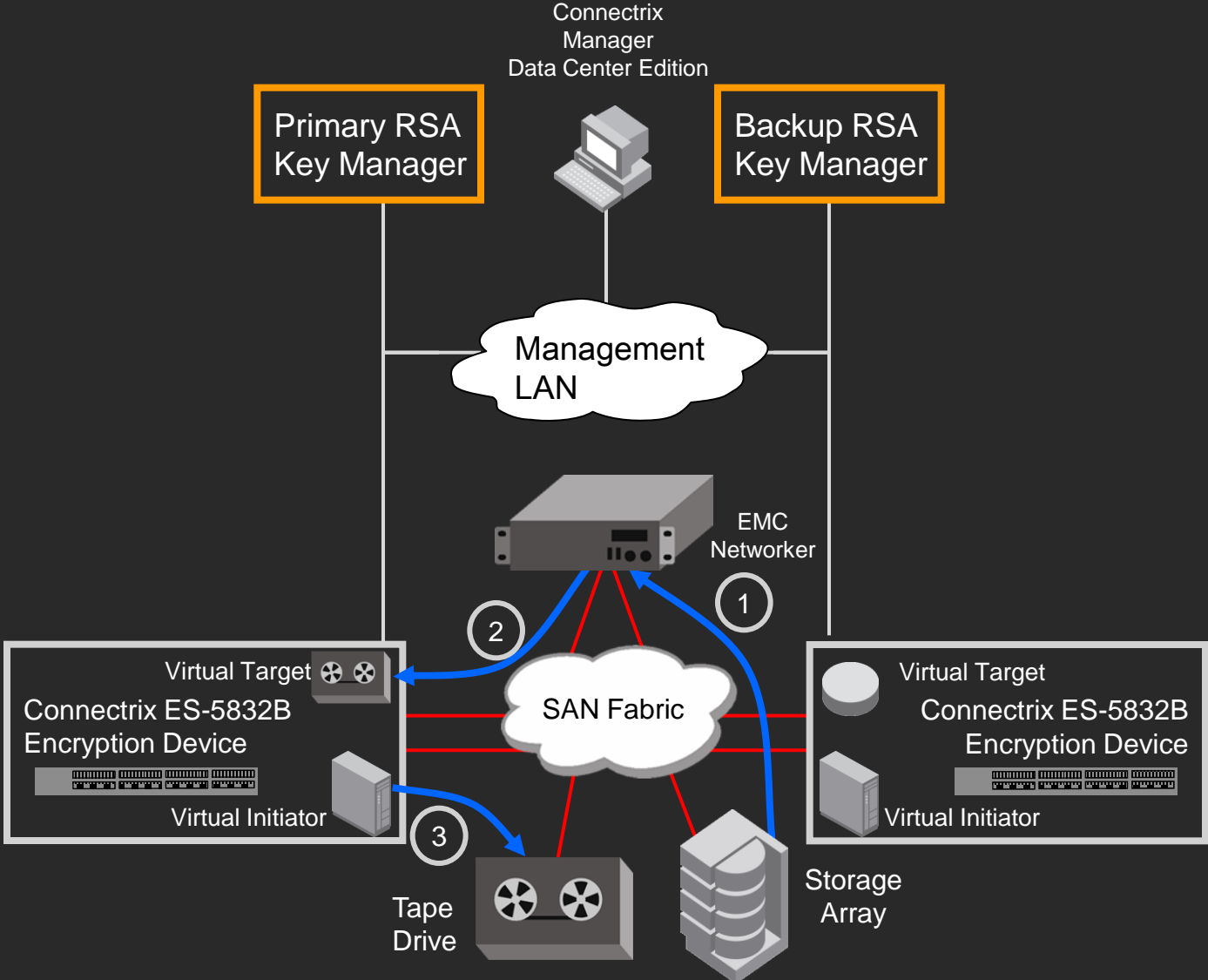
- First time encryption (FTE): Conversion of existing cleartext to ciphertext
- Rekey – Reading existing data, decrypting with expired/old key, re-encrypting with new key and writing the encrypted data back to the LUN
 - In-place rekey – Re-encrypting the existing data & writing back to the same LUN at same location
 - Online rekey – Host I/Os in progress
 - Offline rekey – Host I/Os not in progress or host offline
- Automatic rekey upon key expiry preconfigured by user
- Manual rekey can be invoked in case of key compromise or key policy change

How Fabric-Based Encryption Works

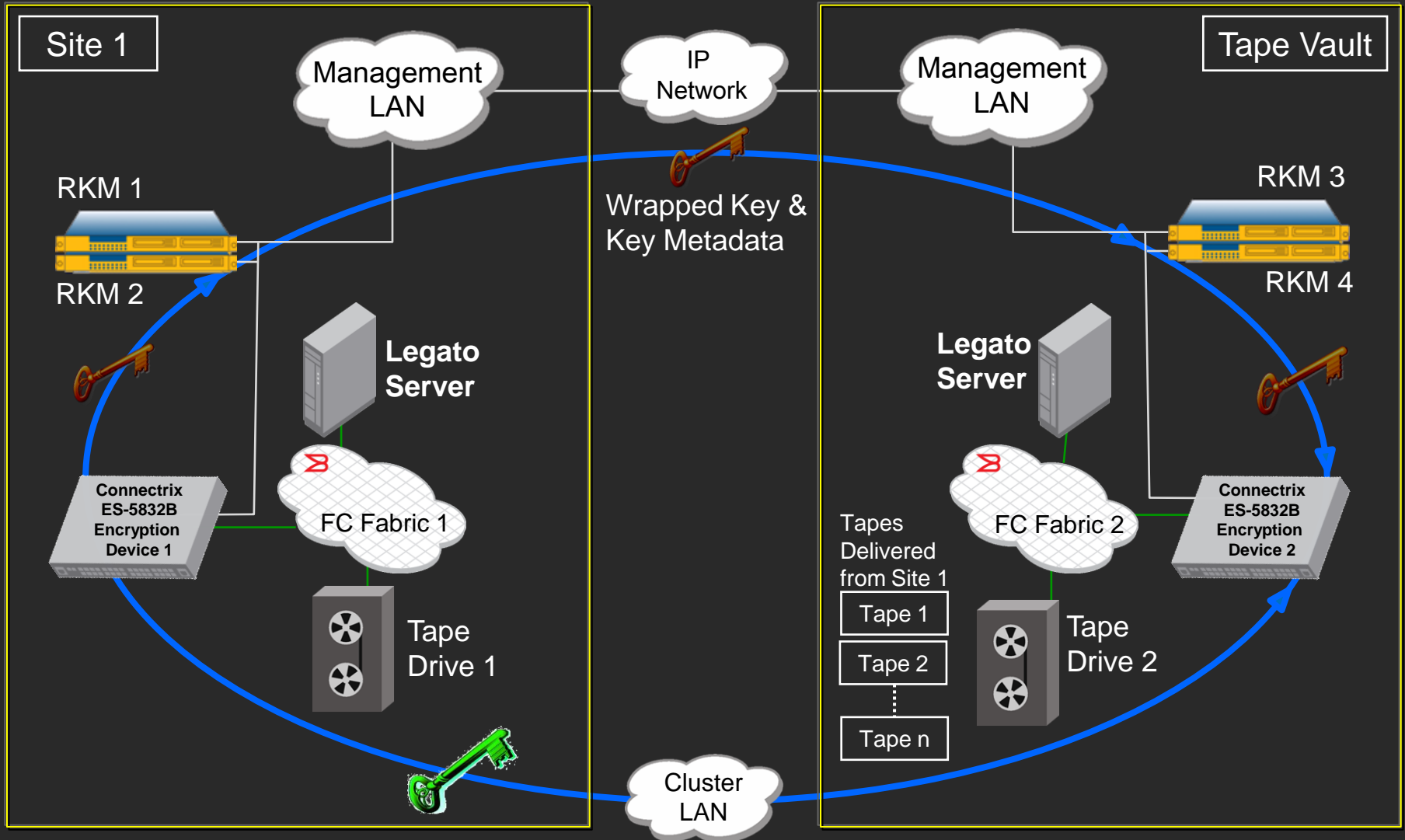


- Encryption switches must be configured in pairs for redundancy
- RKM appliances must be at release 2.5/2.6 and also configured in pairs
 - DEKs - Data Encryption Keys

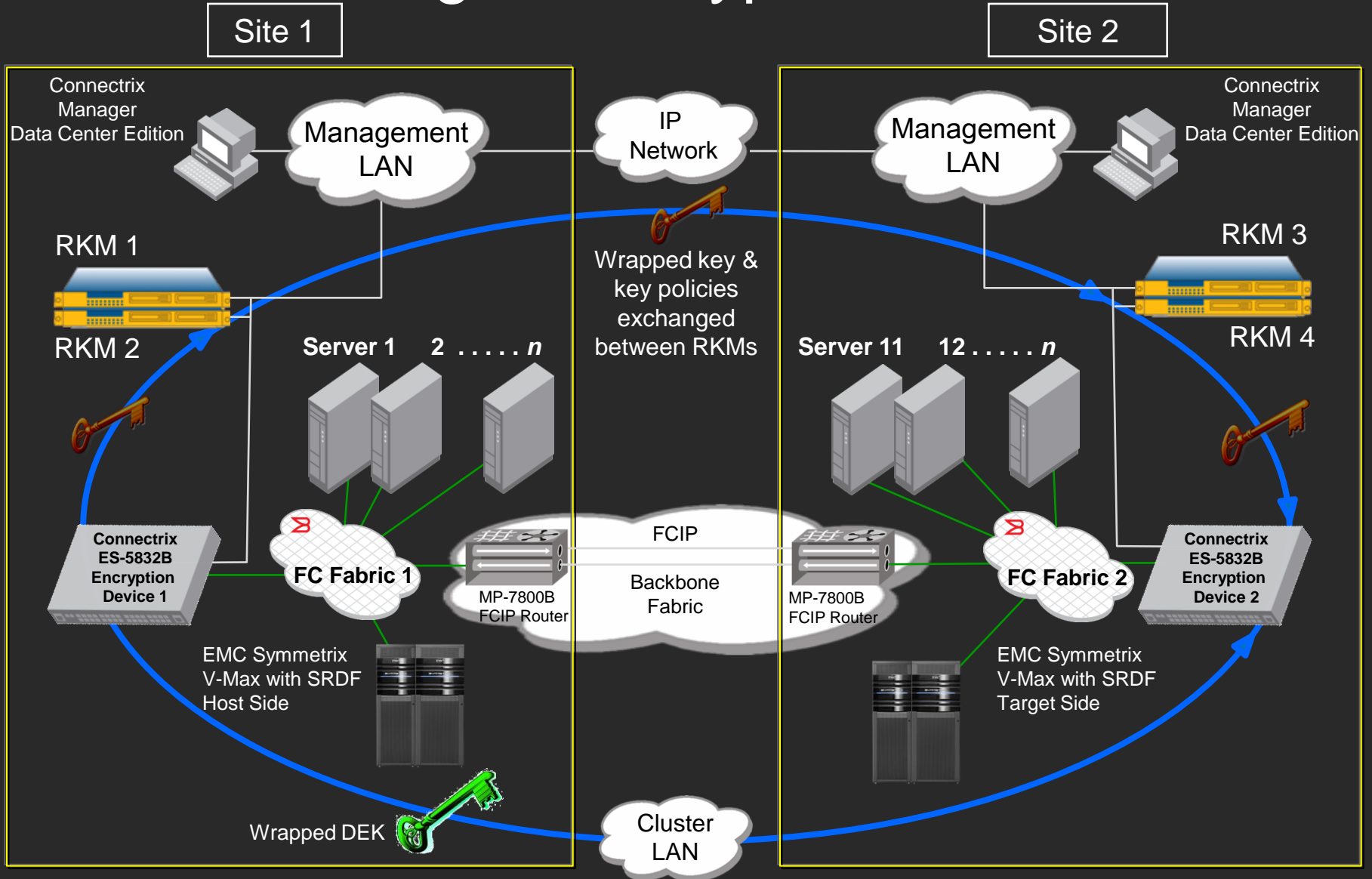
Encrypting Tapes



Key Exchange Example Between Sites



SRDF Mirroring of Encrypted Data



SRDF = Symmetrix Remote Data Facility

How RSA RKM and Aliasing System Help

-
- | | | |
|---|-------------------------|---|
| 1 | Holistic Solution | We designed a holistic solution, integrating products and services from RSA and our partners |
| 2 | Best Practice Framework | Our solution is built around a best practice process for securing enterprise data |
| 3 | Policy-based Management | Our solution not only centralizes management, but elevates control to policy-based management |
| 4 | Partner Ecosystem | A partner ecosystem of leading security and infrastructure vendors. Involvement on major standards boards. |
| 5 | Strategic Services | A suite of services that extends from strategy, to process through implementation, all designed a single framework. |
-



EMC Services to Secure Information

EMC Certified Data Erasure Services

- ▶ Proprietary process to overwrite at the lowest application addressable level to rigid hard disk drives
- ▶ Minimum 3x overwrite (default) with 5x and 7x options at no additional cost
- ▶ Full report, showing erasure results with an EMC Certificate of Completion
- ▶ Aligns with U.S. Department of Defense standard, 5220.22-M, NISPOM (2/28/06) for “clearing”/”eradicating” addressable data on hard disks
- ▶ Flexible options covering full-frame and single disk erasure*

EMC Disk Retention Services

- ▶ Enables you to maintain ownership of drives that must be returned to EMC as part of corrective maintenance
- ▶ Ensures information security
- ▶ Supports compliance mandates
- ▶ Flexible service options:
 - Contracts available for 12, 24, and 36 months
 - Purchase drives as they fail, with no contractual obligation

* Options differ per product line





The Security Division of EMC

Thank you!