SafeNet

THE
DATA
PROTECTION
COMPANY

StorageSecure and KeySecure

Technological leadership in protecting the information lifecycle

Marko Bobinac

PreSales Engineer CEE, Russia & CIS

Actinet, June 2013

StorageSecure

SafeNet THE DATA PROTECTION COMPANY

Storage Types

Hard Drives

NetApp Storage

HP Storage

HP StorageWorks VLS9000
HP StorageWorks VLS9000 Capacity Module
DVD ROM
UID

Tape Library

- Tape Library is a storage device which contains one or more tape drives, a number of slots to hold tape cartridges, a barcode reader to identify tape cartridges and an automated method for loading tapes (a robot).

SafeNet THE DATA PROTECTION COMPANY

Network-Based Storage Encryption

Compliant, Fast, Transparent, Cost Effective

Meet Regulatory Requirements

- FIPS 140-2 Level 3 validation meets PCI, HIPAA, and government data security requirements for data at rest

No Performance Impact

- Encrypt data at wire speeds
- No impact to existing applications
- Have no requirement for additional CPU overhead

Ease of Installation

- Plug seamlessly into current IT environment
- Realize zero downtime or disruption to workflow

Scalability

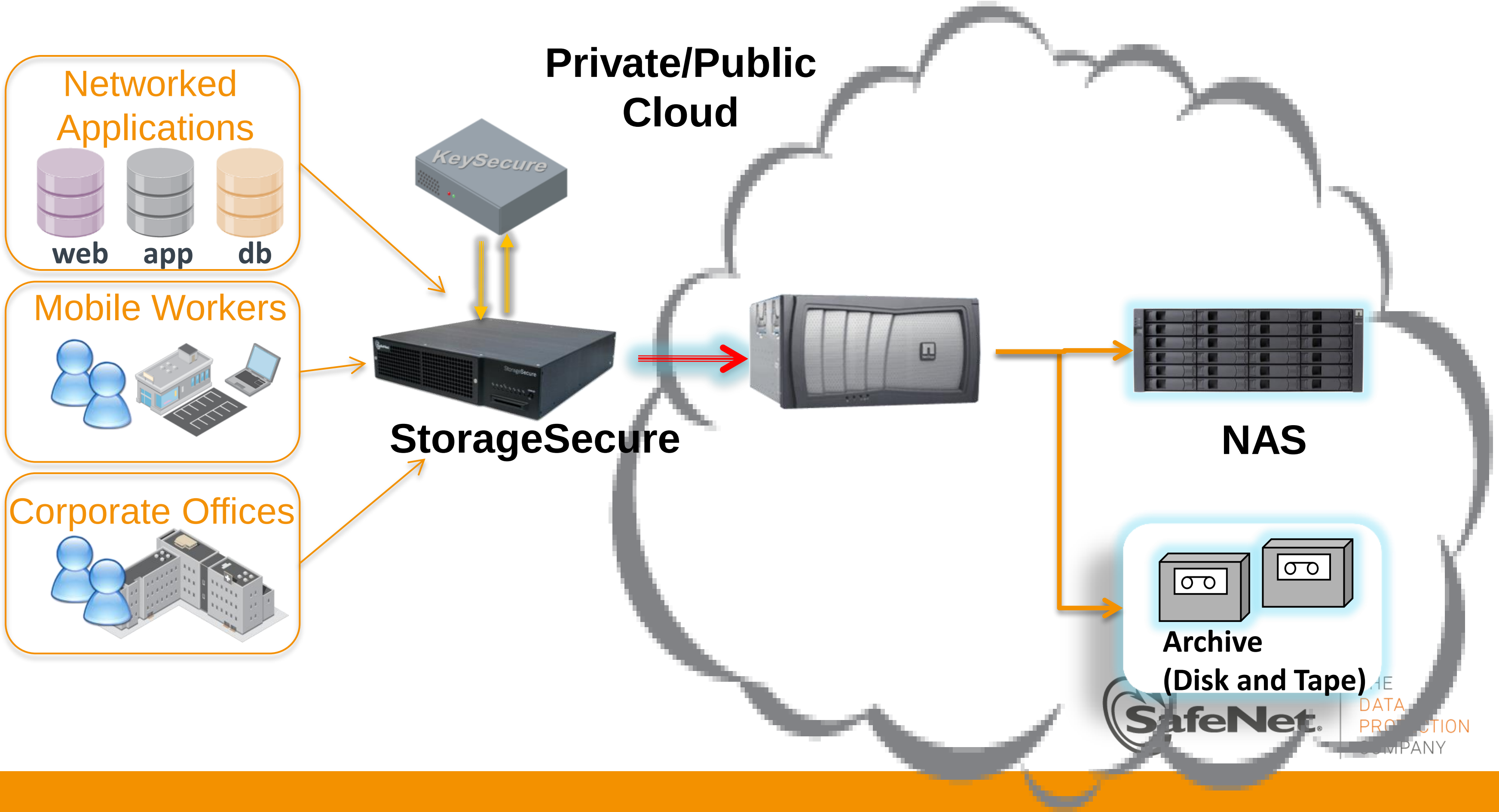
- No need for modifications to hosts, servers, applications, or forklift upgrades to storage
- As data grows, scale cost-effectively

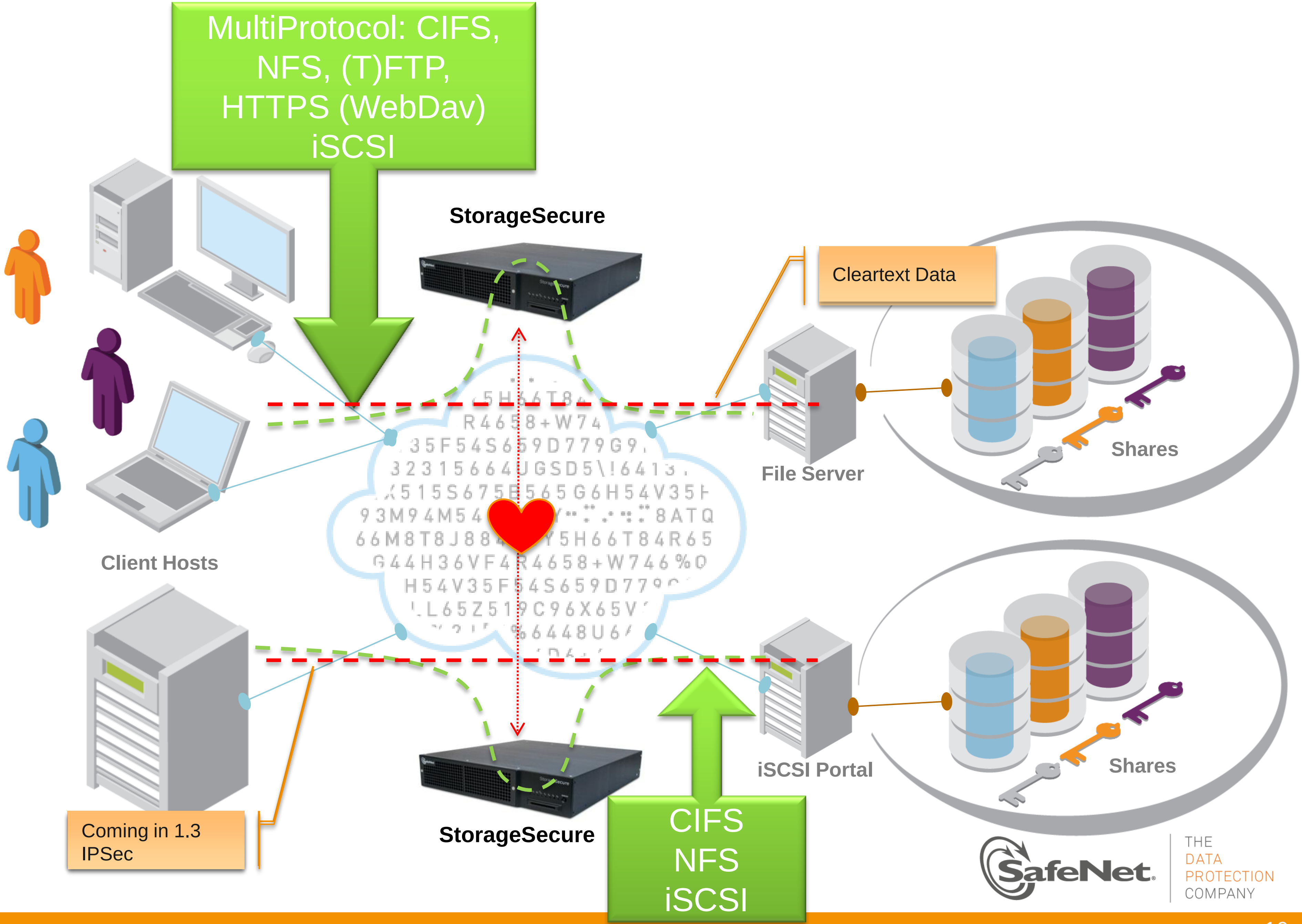
SafeNet THE DATA PROTECTION COMPANY

Secure IaaS - Virtual Storage

StorageSecure – what is it?

- Network appliance (StorageSecure) to encrypt data in storage devices
- Key manager (KeySecure) to manage the encryption keys





MultiProtocol: CIFS, NFS, (T)FTP, HTTPS (WebDav) iSCSI

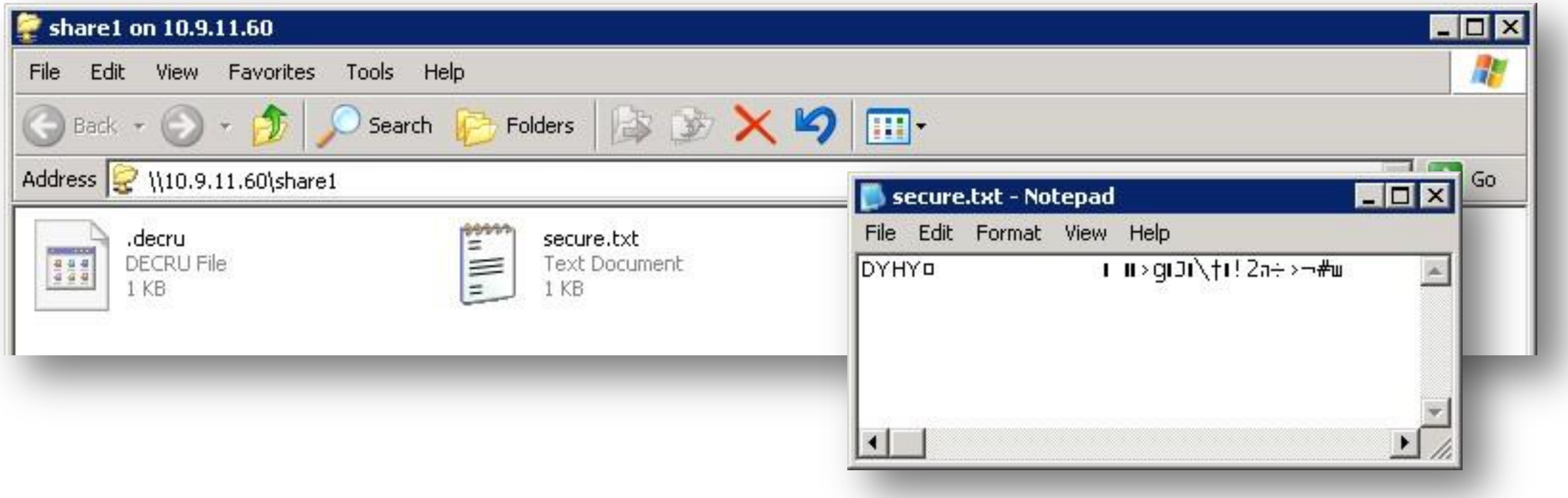
Coming in 1.3
IPSec

CIFS
NFS
iSCSI

SafeNet THE DATA PROTECTION COMPANY

Storage Vault Access through CIFS

Real Share



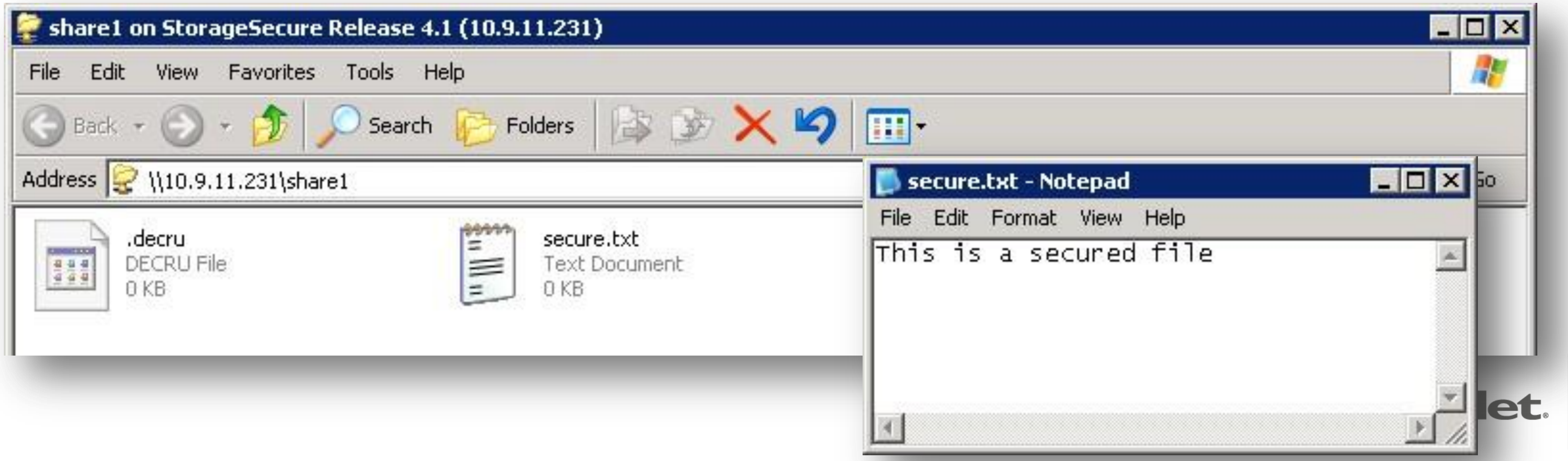
Address: \\10.9.11.60\share1

.decru
DECRU File
1 KB

secure.txt
Text Document
1 KB

```
DYHY□         ▮ ▮›gıJı\†ı!2ㅋ÷›¬#ш
```

Virtual Share – accessed via StorageSecure


share1 on StorageSecure Release 4.1 (10.9.11.231)
File Edit View Favorites Tools Help
Back Search Folders
Address
Go
secure.txt - Notepad
File Edit Format View Help

Address: \\10.9.11.231\share1

.decru
DECRU File
0 KB

secure.txt
Text Document
0 KB

```
This is a secured file
```

THE
DATA
PROTECTION
COMPANY

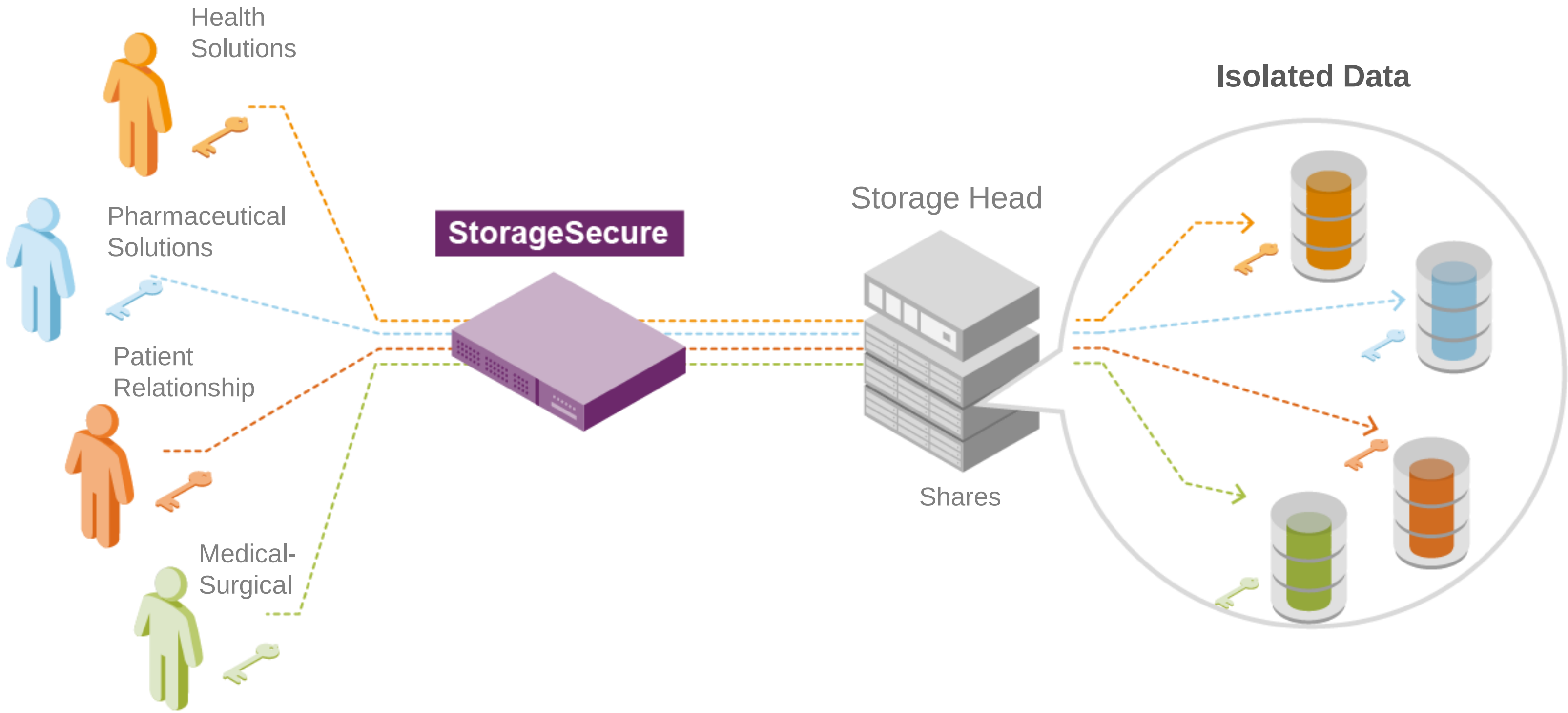
Storage Encryption Requirements

- Support all Protocols in SAN and NAS
  - CIFS, NFS, iSCSI
  - SAN Disk
  - SAN Tape
  - SCSI Tape

- Global Automated Key Management
  - Clear Separation of Rights & Roles
  - Hierarchical Key Structures
  - Keys stored centrally and secure in Hardware

StorageSecure use-cases

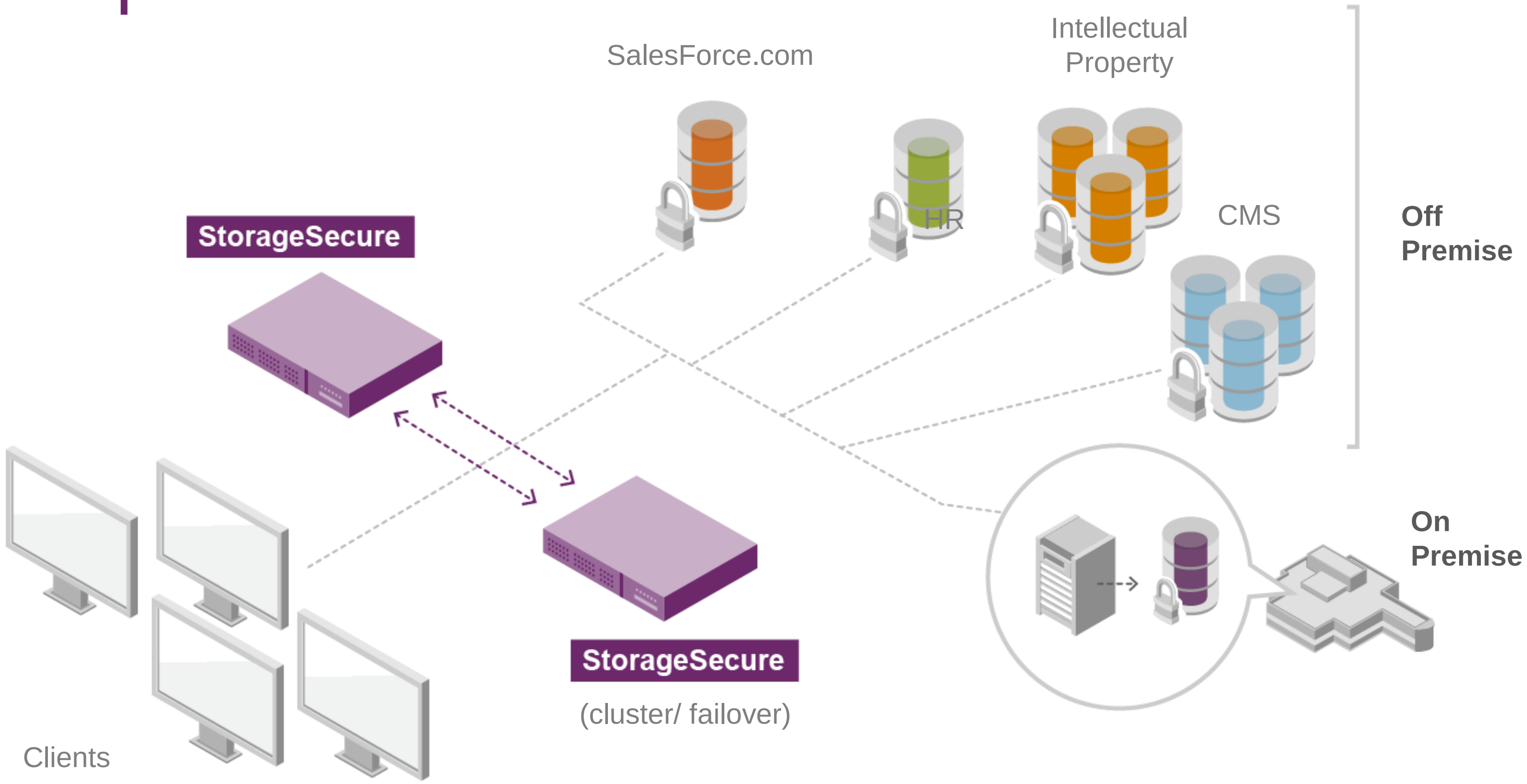
Isolate Data in Multi-tenant Environments



- •Encryption-enabled separation of data in shared virtual environments
- •Separation of departmental data
- •Protect data belonging to security sensitive departments
- •Enables hosting multiple customers on the same HW

SafeNet THE DATA PROTECTION COMPANY

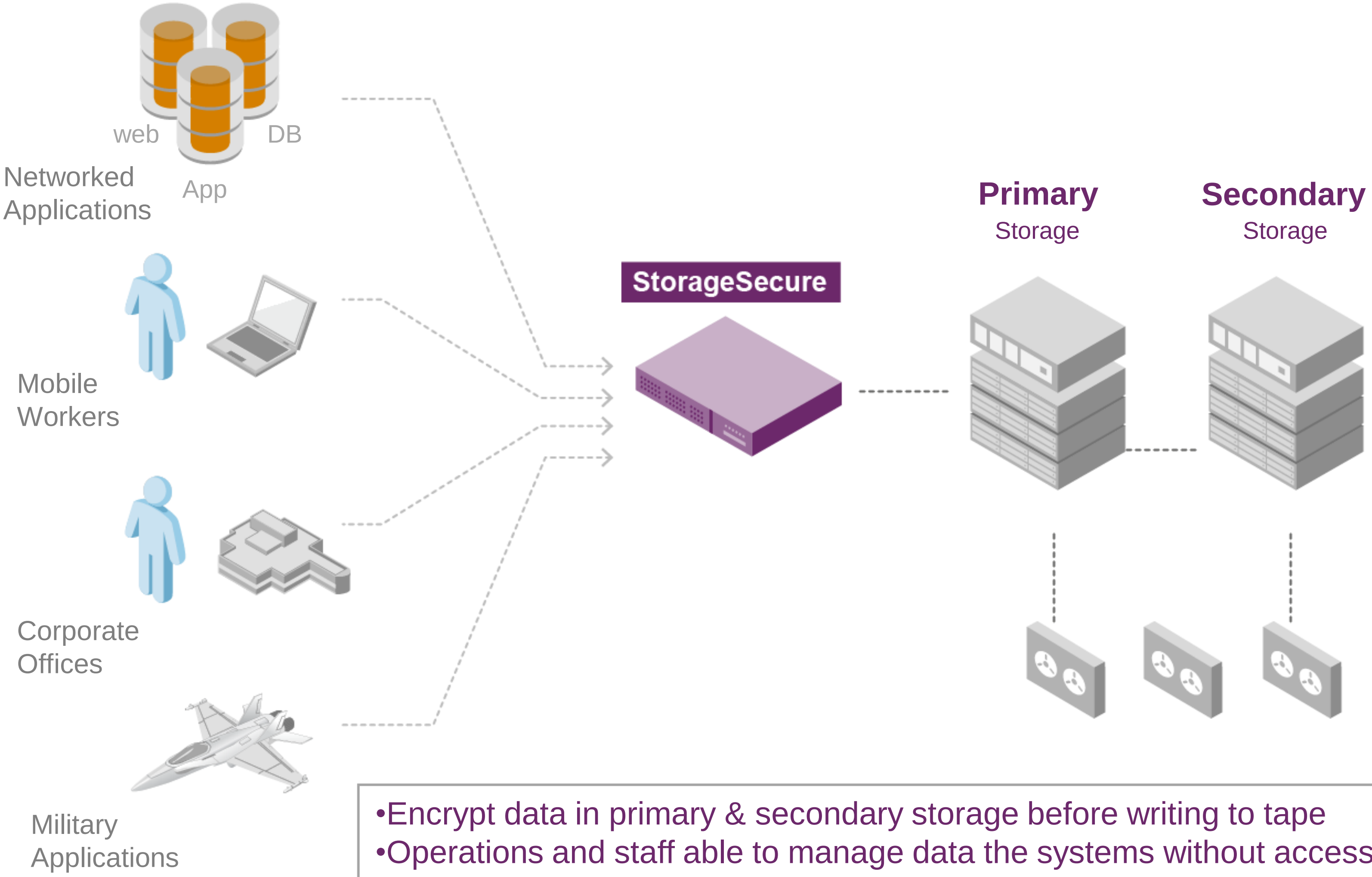
Compliant Data Protection



- Encrypt data in real-time at the point of capture/creation
- Secure, hardware based network storage (FIPS 140-2 Level 3)
- Encrypts data and renders it unreadable to unauthorized viewers
- Secure key management - clear text keys never leave the hardware
- Integrated with KeySecure for automated and centralized key lifecycle management

SafeNet. THE DATA PROTECTION COMPANY

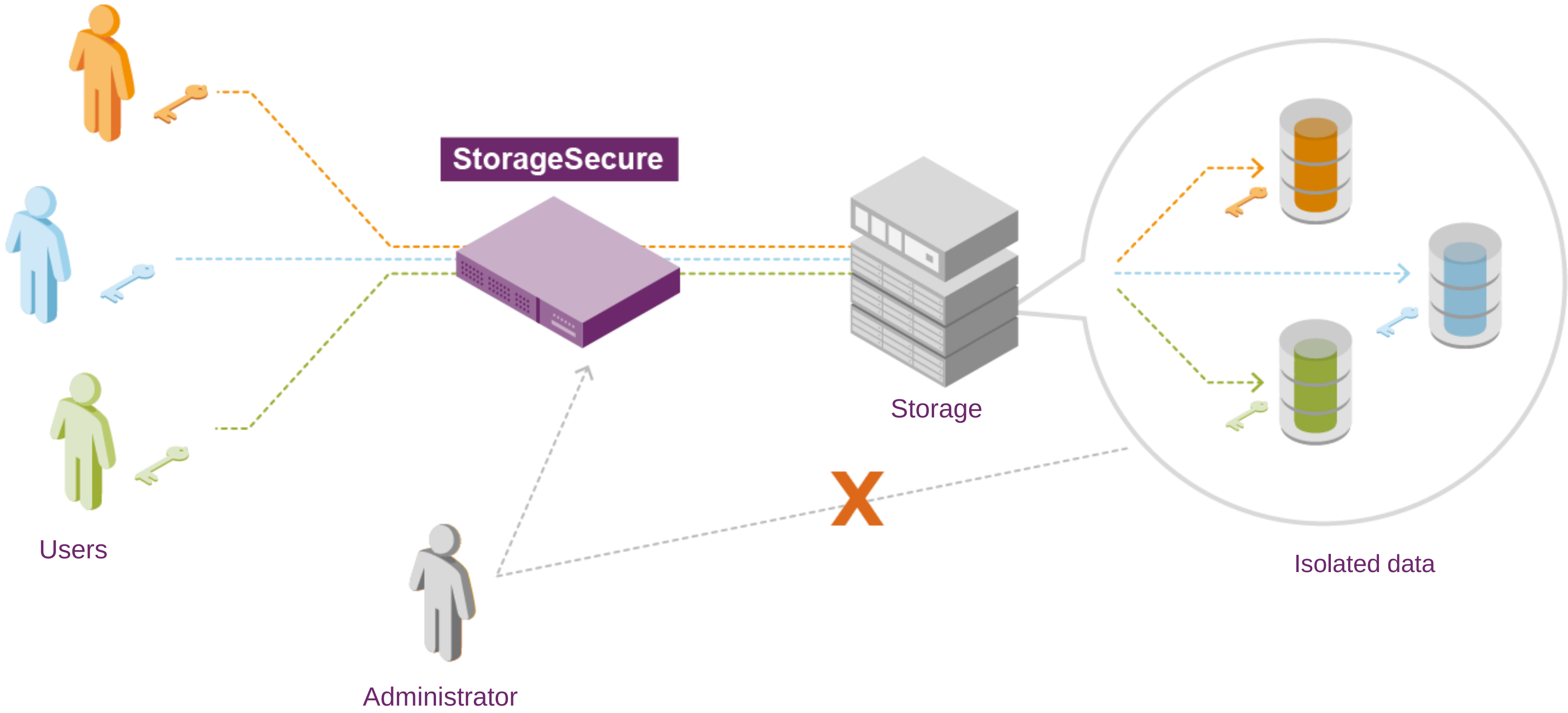
Archival Protection



- •Encrypt data in primary & secondary storage before writing to tape
- •Operations and staff able to manage data the systems without access to content
- •Transparent deployment - no agents, storage device changes or user behavior adjustments

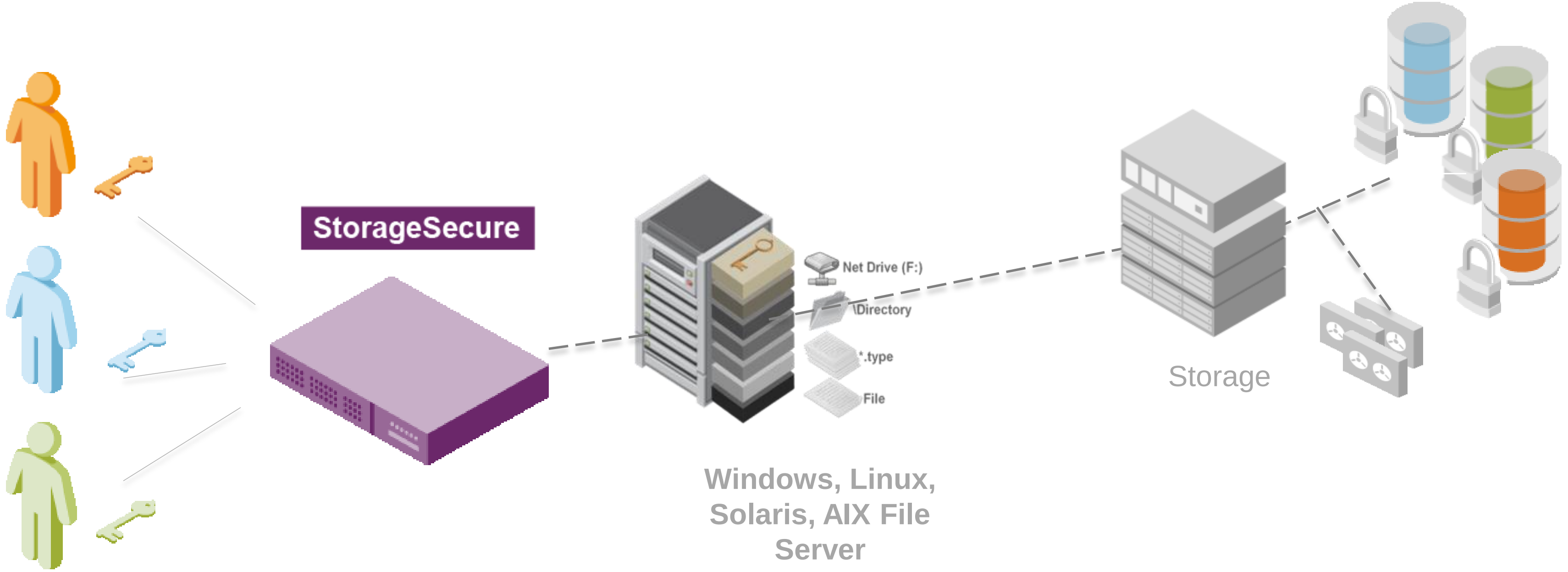
SafeNet THE DATA PROTECTION COMPANY

Privileged User Risk Mitigation



- •Ensures data isolation and granular, authorized access
- •Protects against unauthorized administrators/network administrators and users
- •Operations and staff able to manage data the systems without access to content
- •Integrated with existing Identity and access mgmt systems (LDAP, MS AD, NIS)
- •Instantiates additional layer of dual control to restrict access

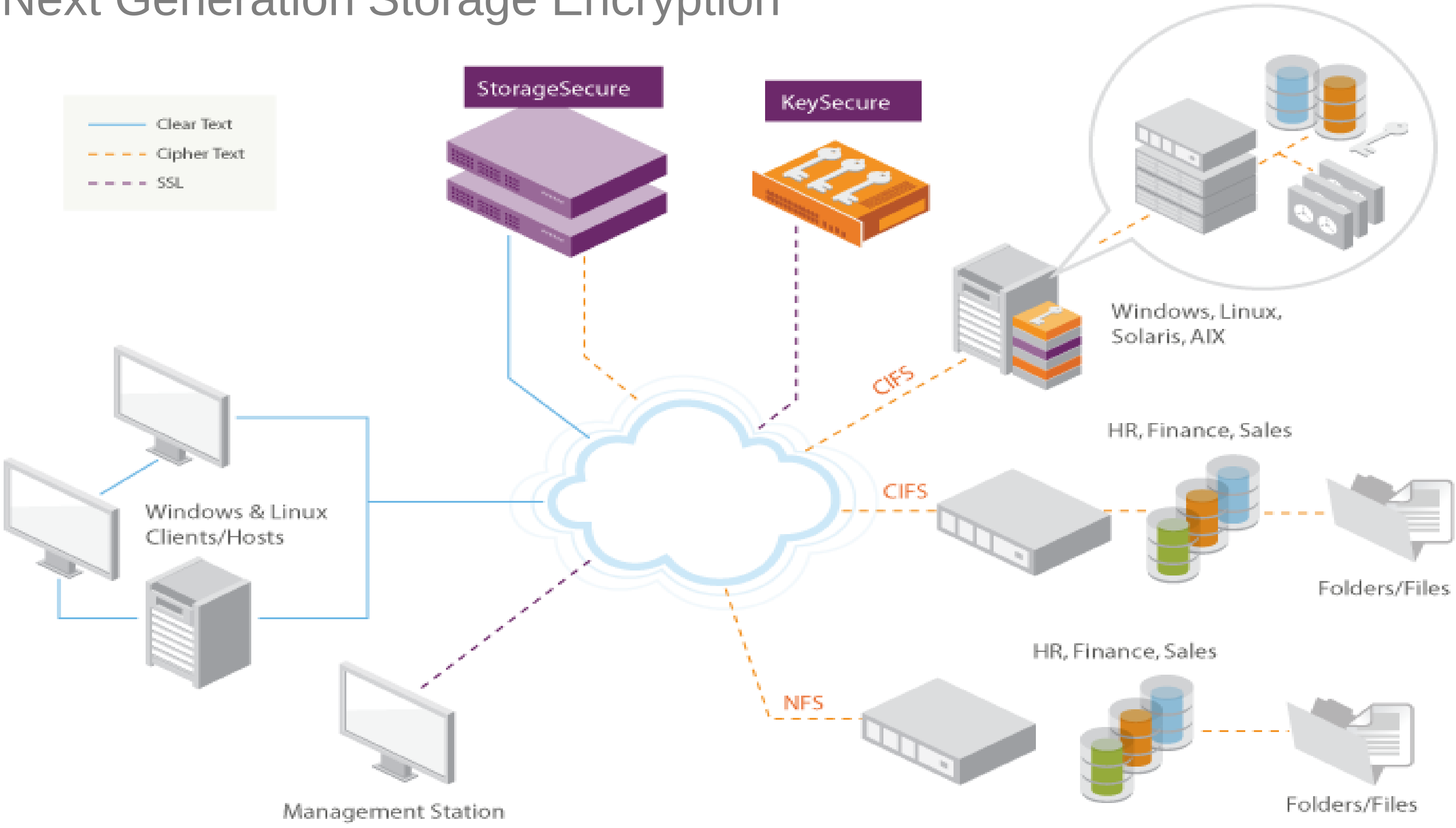
Protecting Backend SAN Environments



•Encrypt NAS applications on to protect backend block-level storage

SafeNet StorageSecure

Next Generation Storage Encryption



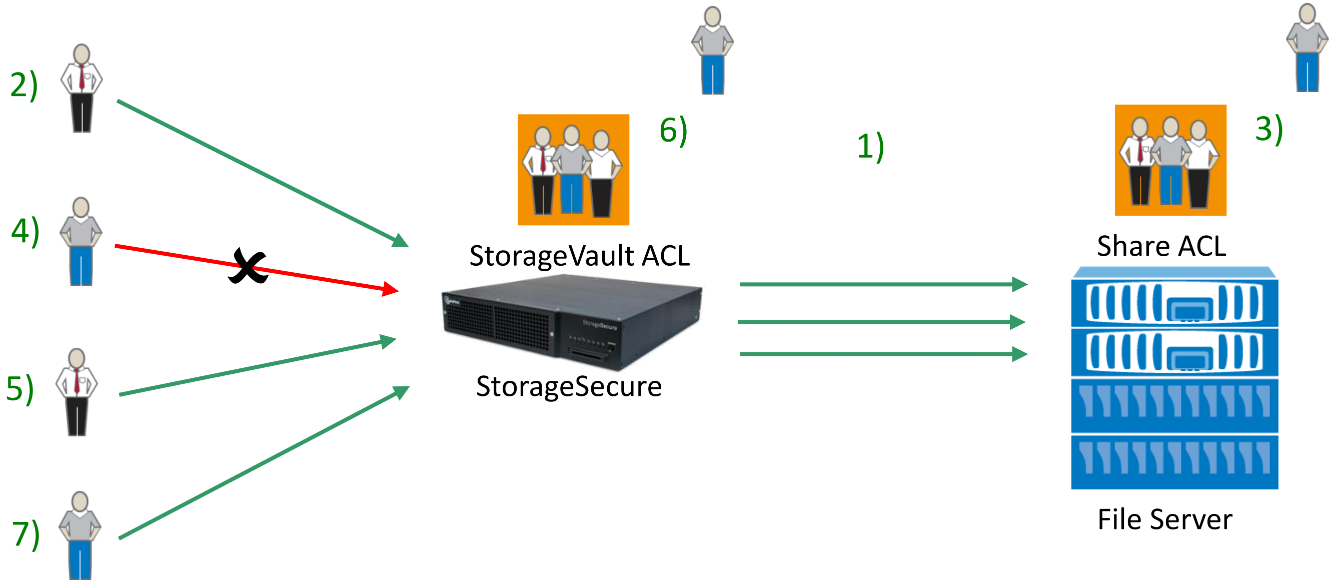
- •Transparent network-based encryption
- •Separation of duties and segregation of data
- •Clustering for high reliability and availability
- •Integrated with SafeNet KeySecure for centralized key management
- •Multi-gigabit speed support
- •Compatible with NetApp DataFort and LKM

StorageSecure

Separation of Duties

- Separation of administrator roles
  - Within in the StorageSecure device (9 administrator roles including "Full")
  - Between authentication and directory services and appliance and storage access
- Customers can separate roles to prevent compromise from a rogue administrator
  - Password resets, changed user credentials at the directory/authentication server can still require validation by the StorageSecure admin and/or share owner (Group Review)
- Simplest implementation - sync user and group directory data directly to the StorageSecure appliance

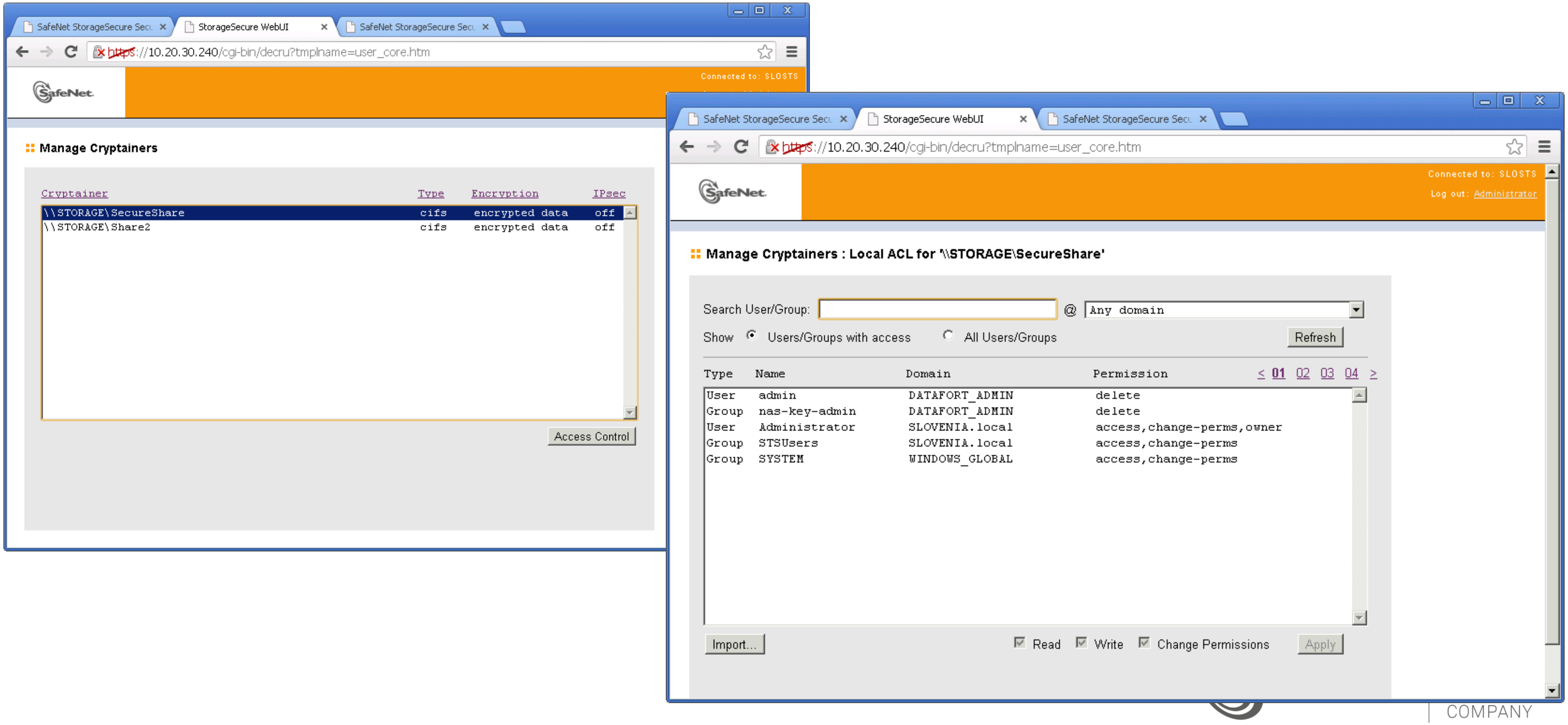
Local ACL and Access Control



1) Filer Server ACLs in sync with StorageSecure
2) User 1 allowed access by the StorageSecure
3) Filer Server ACLs is modified – user 3 added
4) User 3 denied access by StorageSecure
5) User 1 still allowed access by StorageSecure
6) StorageSecure Admin adds user 3 to StorageVault ACL
7) User 3 allowed access by the StorageSecure

WebUI Storage Vault Management

- End users can log in to the SafeNet StorageSecure WebUI to view and manage the Storage Vaults they own.



SafeNet StorageSecure Secu
StorageSecure WebUI
SafeNet StorageSecure Secu
https://10.20.30.240/cgi-bin/decru?tmplname=user_core.htm
SafeNet
Connected to: SLOSTS

Manage Cryptainers

Cryptainer	Type	Encryption	IPsec
\\STORAGE\SecureShare	cifs	encrypted data	off
\\STORAGE\Share2	cifs	encrypted data	off

SafeNet StorageSecure Secu
StorageSecure WebUI
SafeNet StorageSecure Secu
https://10.20.30.240/cgi-bin/decru?tmplname=user_core.htm
SafeNet
Connected to: SLOSTS
Log out: Administrator

Manage Cryptainers : Local ACL for '\\STORAGE\SecureShare'

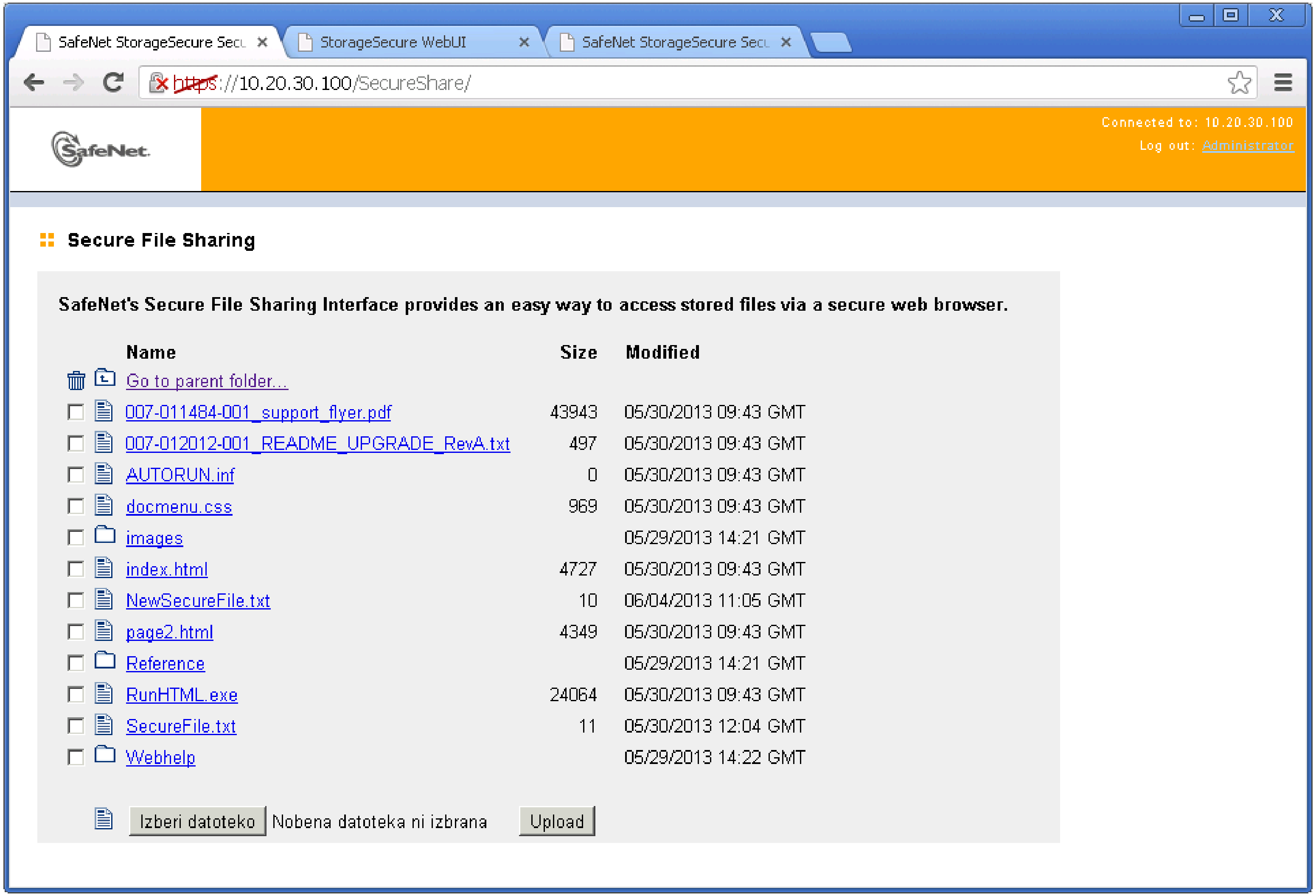
Search User/Group: @ Any domain

Show ● Users/Groups with access ○ All Users/Groups

Type	Name	Domain	Permission
User	admin	DATAFORT_ADMIN	delete
Group	nas-key-admin	DATAFORT_ADMIN	delete
User	Administrator	SLOVENIA.local	access,change-perms,owner
Group	STSUsers	SLOVENIA.local	access,change-perms
Group	SYSTEM	WINDOWS_GLOBAL	access,change-perms

☑ Read ☑ Write ☑ Change Permissions

Secure Web Access



SafeNet StorageSecure Secu
StorageSecure WebUI
SafeNet StorageSecure Secu
~~https~~://10.20.30.100/SecureShare/
SafeNet

Connected to: 10.20.30.100
Log out: Administrator

Secure File Sharing

SafeNet's Secure File Sharing Interface provides an easy way to access stored files via a secure web browser.

	Name	Size	Modified
	Go to parent folder...		
□	007-011484-001_support_flyer.pdf	43943	05/30/2013 09:43 GMT
□	007-012012-001_README_UPGRADE_RevA.txt	497	05/30/2013 09:43 GMT
□	AUTORUN.inf	0	05/30/2013 09:43 GMT
□	docmenu.css	969	05/30/2013 09:43 GMT
□	images		05/29/2013 14:21 GMT
□	index.html	4727	05/30/2013 09:43 GMT
□	NewSecureFile.txt	10	06/04/2013 11:05 GMT
□	page2.html	4349	05/30/2013 09:43 GMT
□	Reference		05/29/2013 14:21 GMT
□	RunHTML.exe	24064	05/30/2013 09:43 GMT
□	SecureFile.txt	11	05/30/2013 12:04 GMT
□	Webhelp		05/29/2013 14:22 GMT

Nobena datoteka ni izbrana

FTP Access

- Clients can access encrypted data using FTP
  - Clients can log in to virtual servers from an FTP client, authenticated by their username and password
  - FTP is disabled by default and must be enabled per VIP through the command-line interface
  - Users can only access data for which their CIFS / NFS credentials are valid
  - FTP supports the concept of a home directory
  - If a home directory is set up for a client; rather than starting at the top level, the client starts in his home directory
  - `user home set [<user>]@<domain><real_path>`

KeySecure

Enterprise Key Management solution

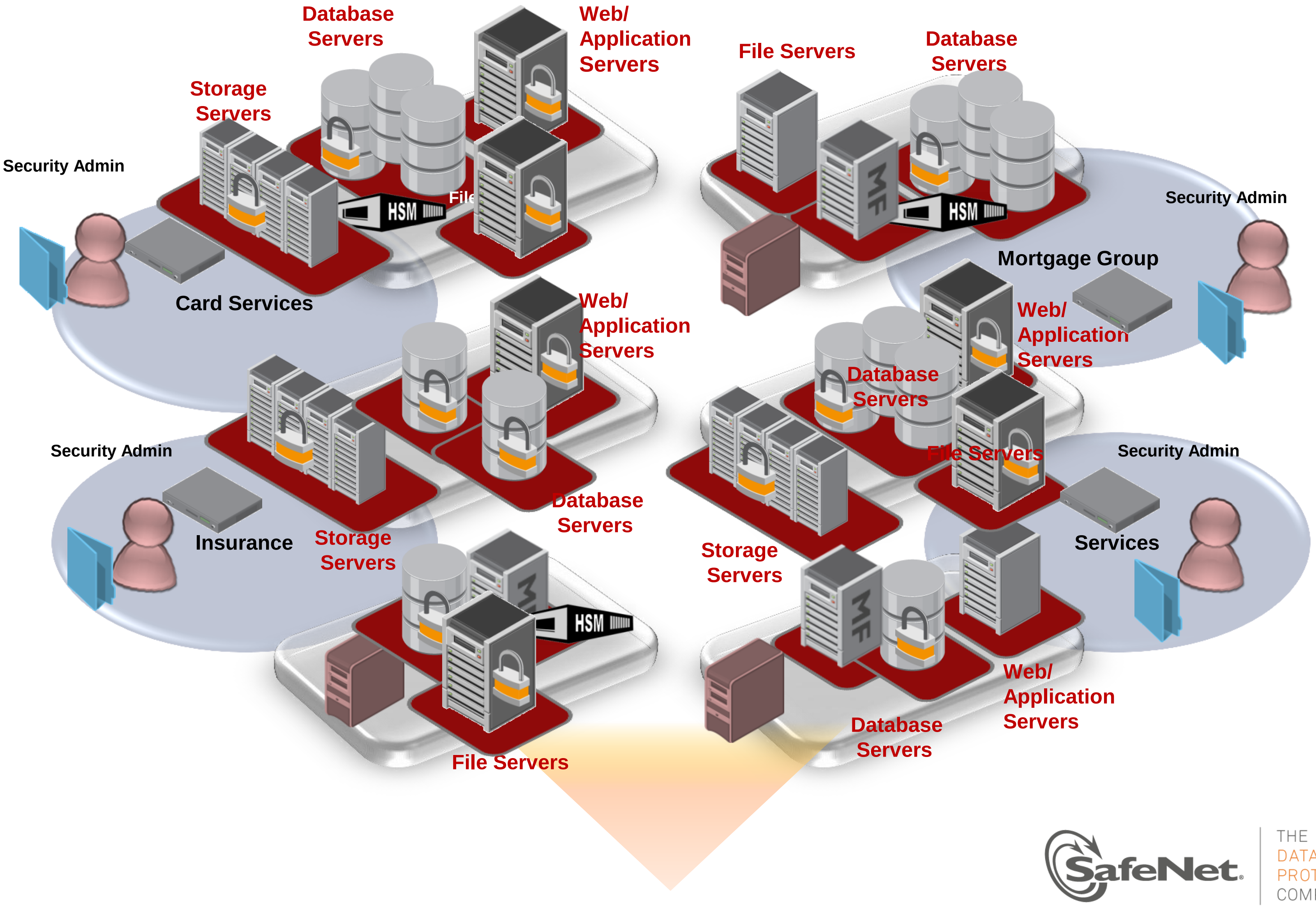
THE
DATA
PROTECTION
COMPANY

The Unmanageable Cost of Disparate Encryption Keys

- Time:
  - Managing disparate keys manually, decreases operational effectiveness while increasing risks
- Data Loss / Operational Disruptions:
  - Up to 39 percent of organizations who have experienced key loss also lose data permanently or disrupt business operations.
- Compliance Proof:
  - Demonstrate which appliances, devices, applications are using encryption keys and where they are geographically located
- Maintenance Costs:
  - Disparate systems mean no economy of scale for maintenance costs. Each encryption system and key management solution could have 15-20% annual maintenance fees.

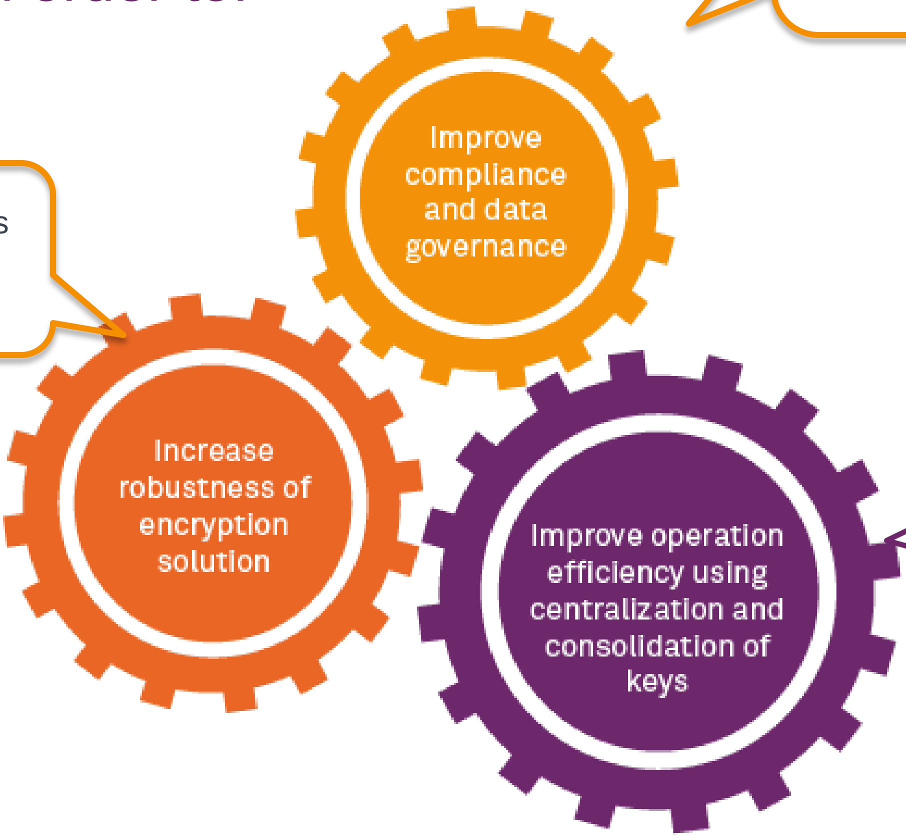
* Source: trust catalyst, 2009 Encryption & Key Management Industry Benchmark Report

Encryption Domains



As the need for more widespread encryption becomes the norm, enterprises will look to aggregate key management into a centralized solutions in order to:

- True enterprise key management enables uniform, consistent key management and policy management across heterogeneous environments.



Improve compliance and data governance

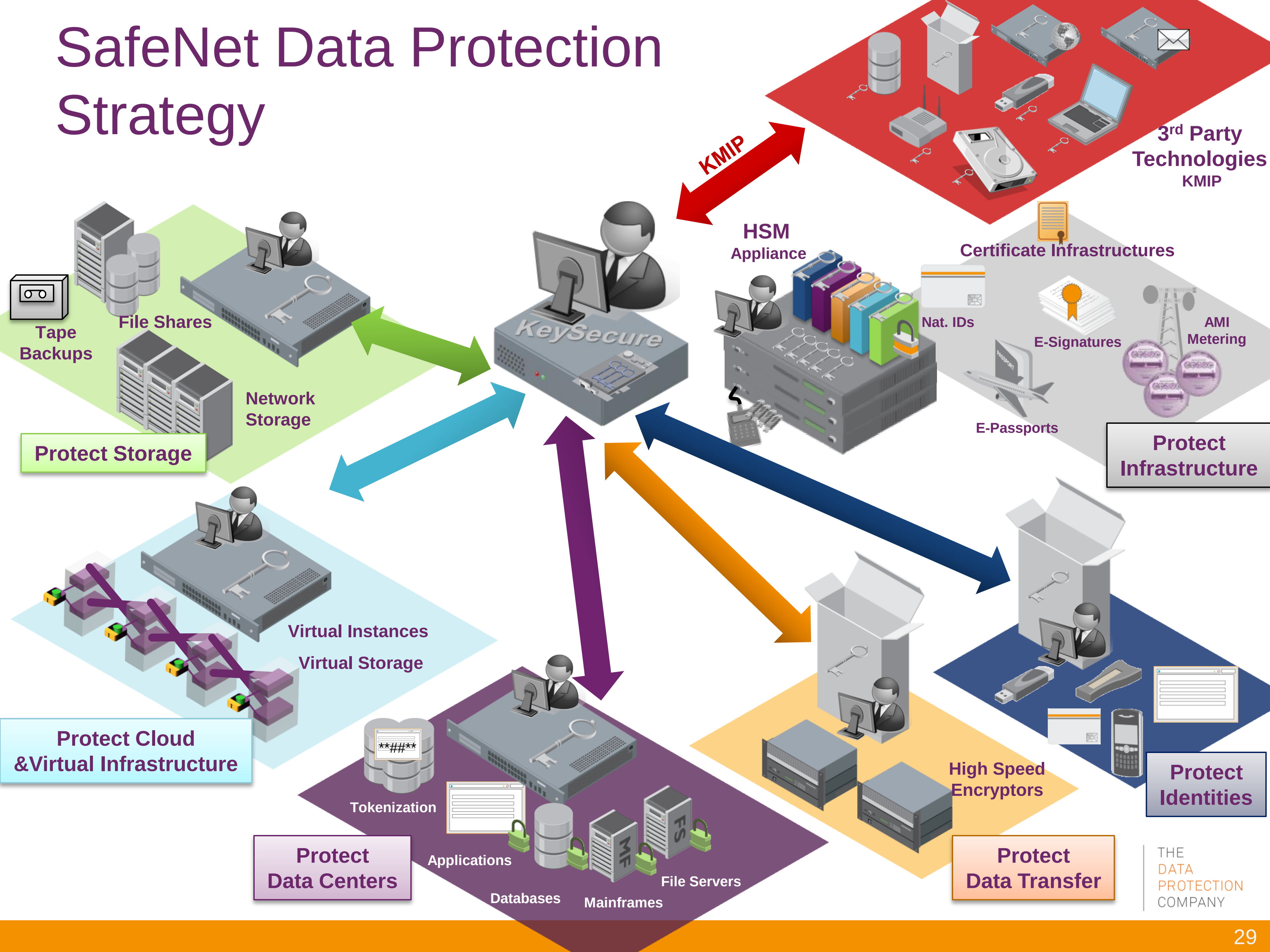
Increase robustness of encryption solution

Improve operation efficiency using centralization and consolidation of keys

- Separation of duties
- Unique keys

- Centralize key management lifecycle
- Reduces operational costs
- Strong protection for heterogeneous systems

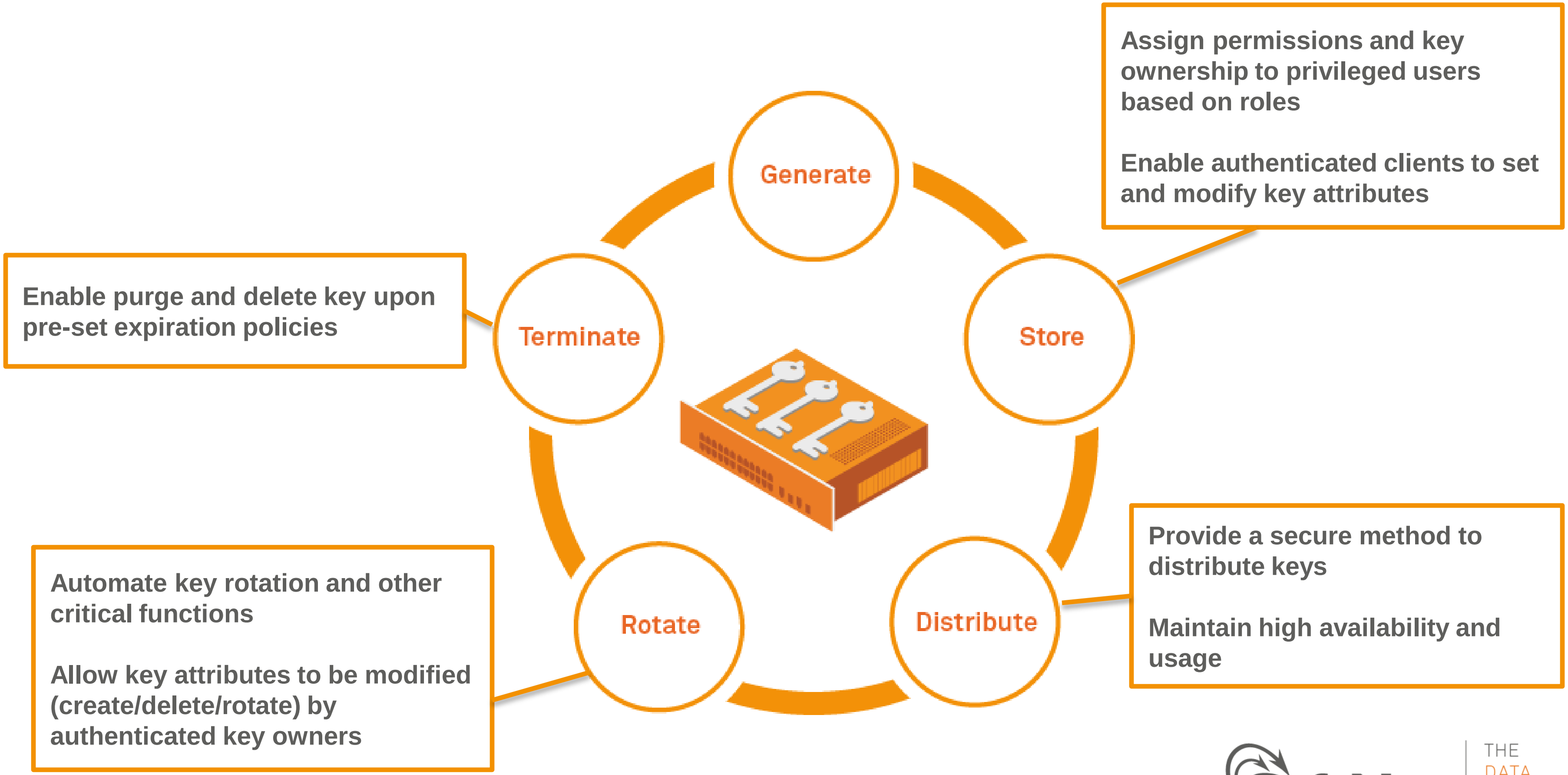
SafeNet Data Protection Strategy



KeySecure: How it works

KeySecure handles every aspect of key management.

An Admin Console allows central definition, management and monitoring of key ownership and user access controls.



Assign permissions and key ownership to privileged users based on roles

Enable authenticated clients to set and modify key attributes

Enable purge and delete key upon pre-set expiration policies

Provide a secure method to distribute keys

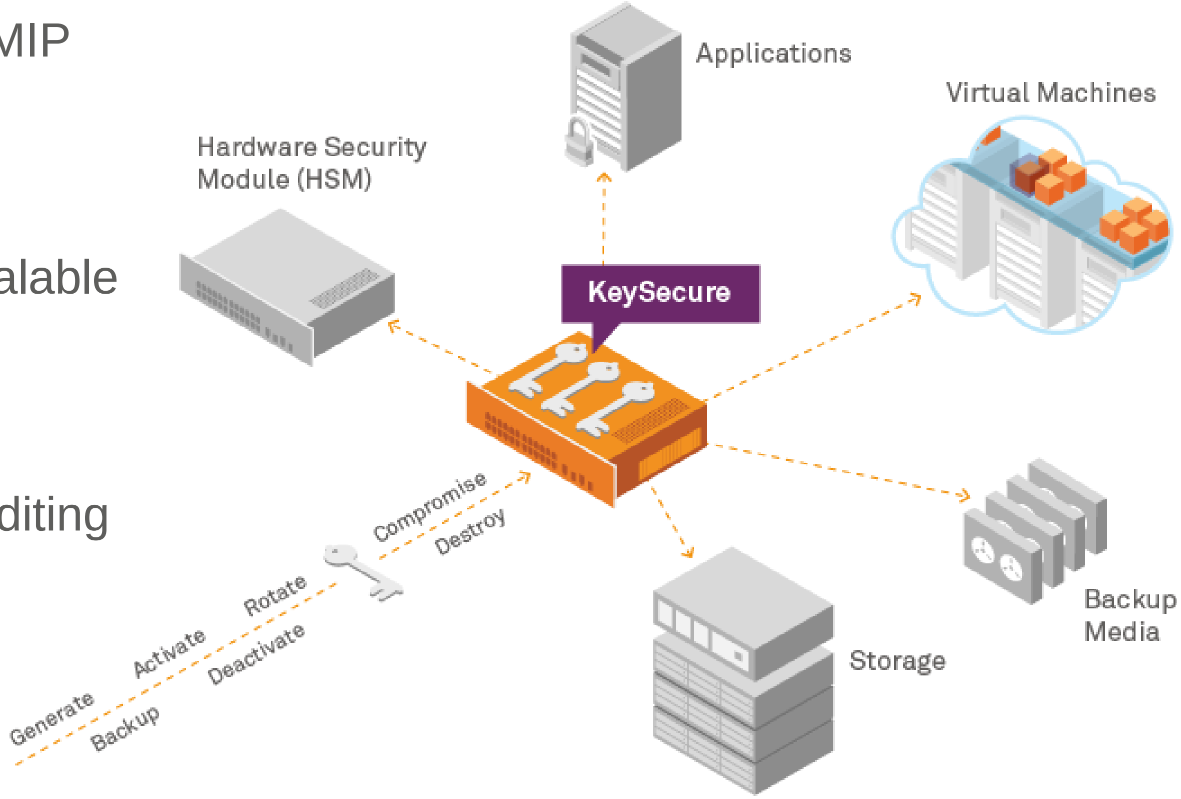
Maintain high availability and usage

Automate key rotation and other critical functions

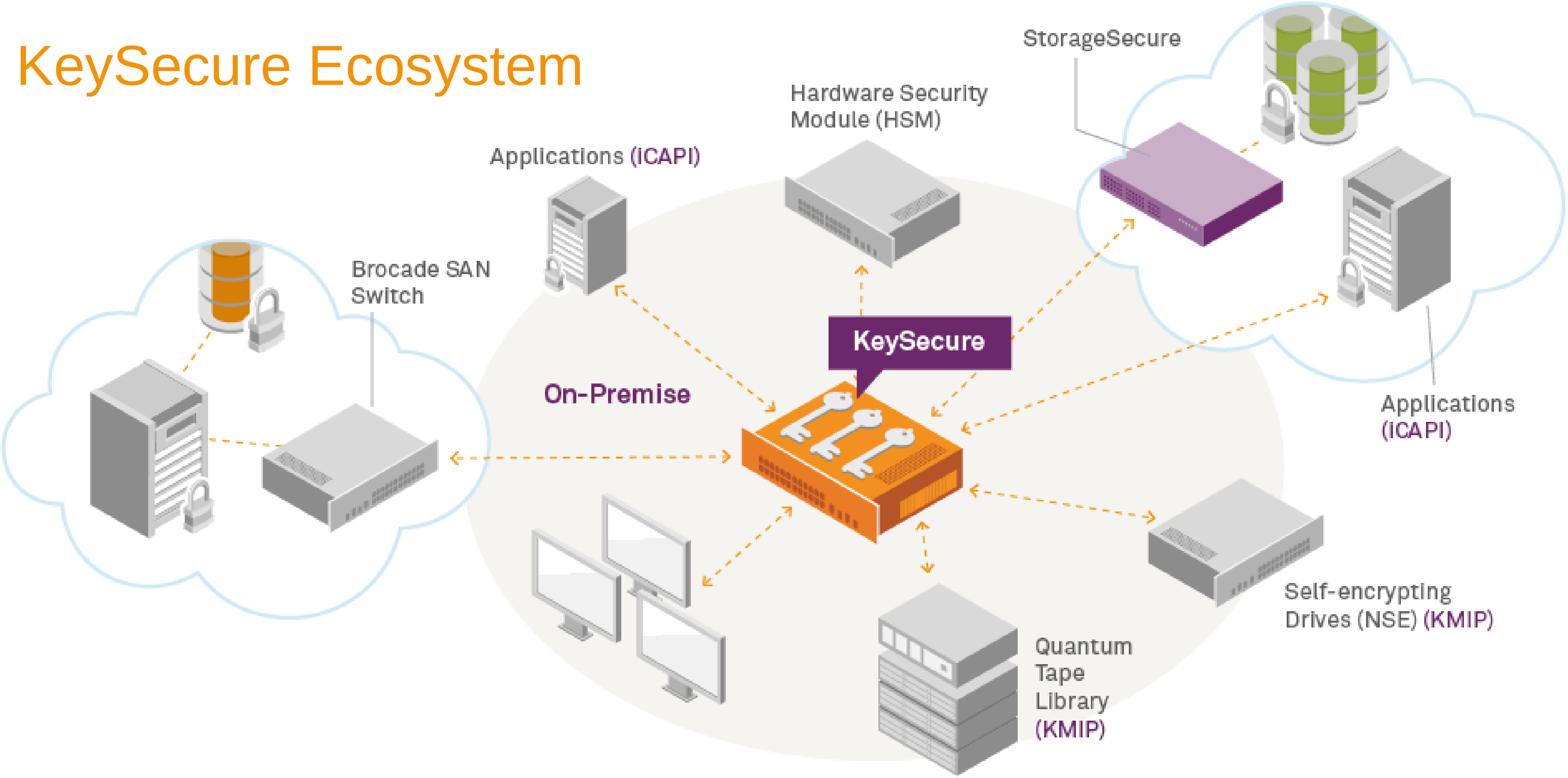
Allow key attributes to be modified (create/delete/rotate) by authenticated key owners

KeySecure: How it works

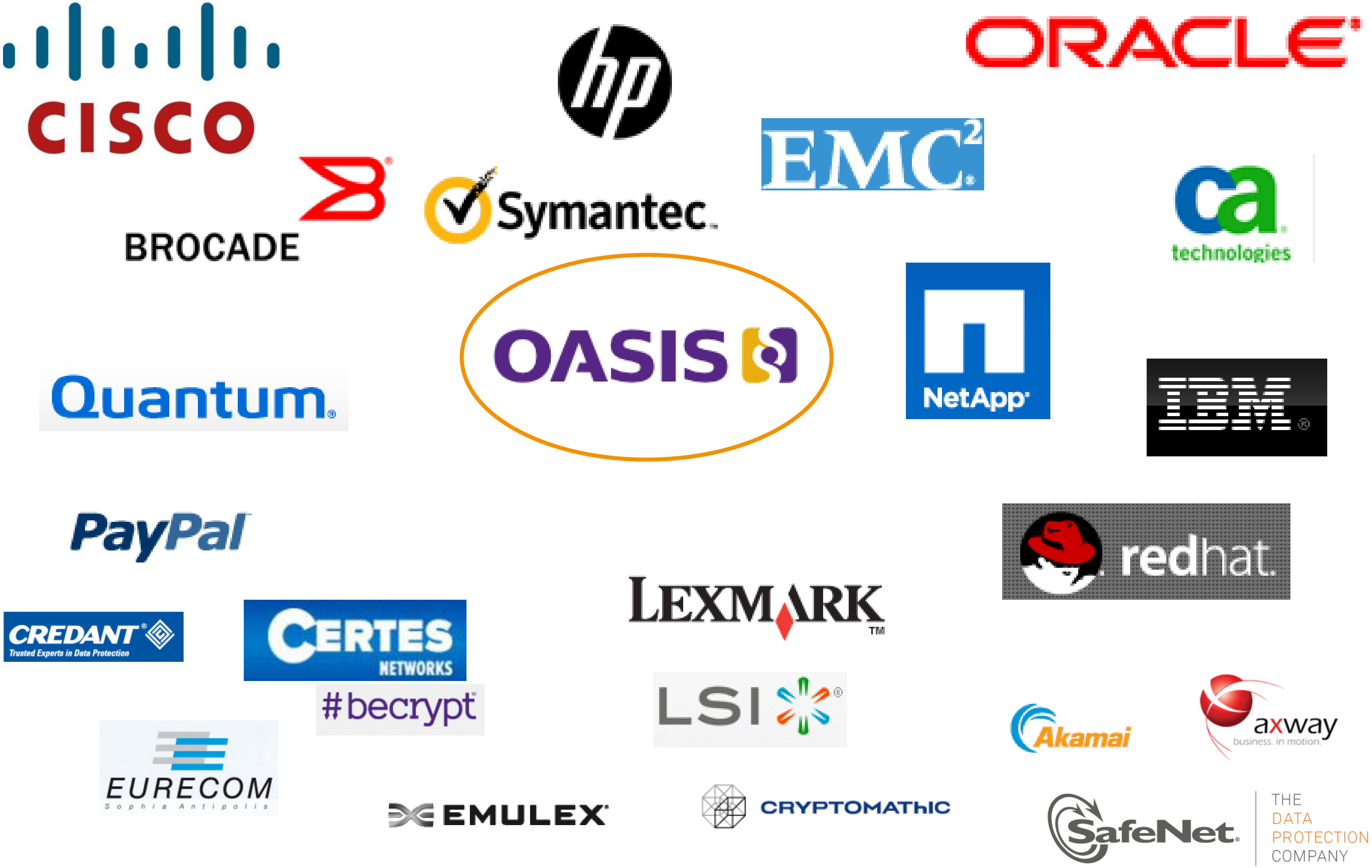
- Secure, centralized key management
- Standards-based via KMIP
- Data-centric policy management
- Highly available and scalable
- Identity and access management
- Visibility via logging, auditing and reporting



KeySecure Ecosystem


StorageSecure
Hardware Security Module (HSM)
Applications (ICAPI)
Brocade SAN Switch
KeySecure
On-Premise
Applications (ICAPI)
Self-encrypting Drives (NSE) (KMIP)
Quantum Tape Library (KMIP)

Oasis KMIP Members



SafeNet KeySecure

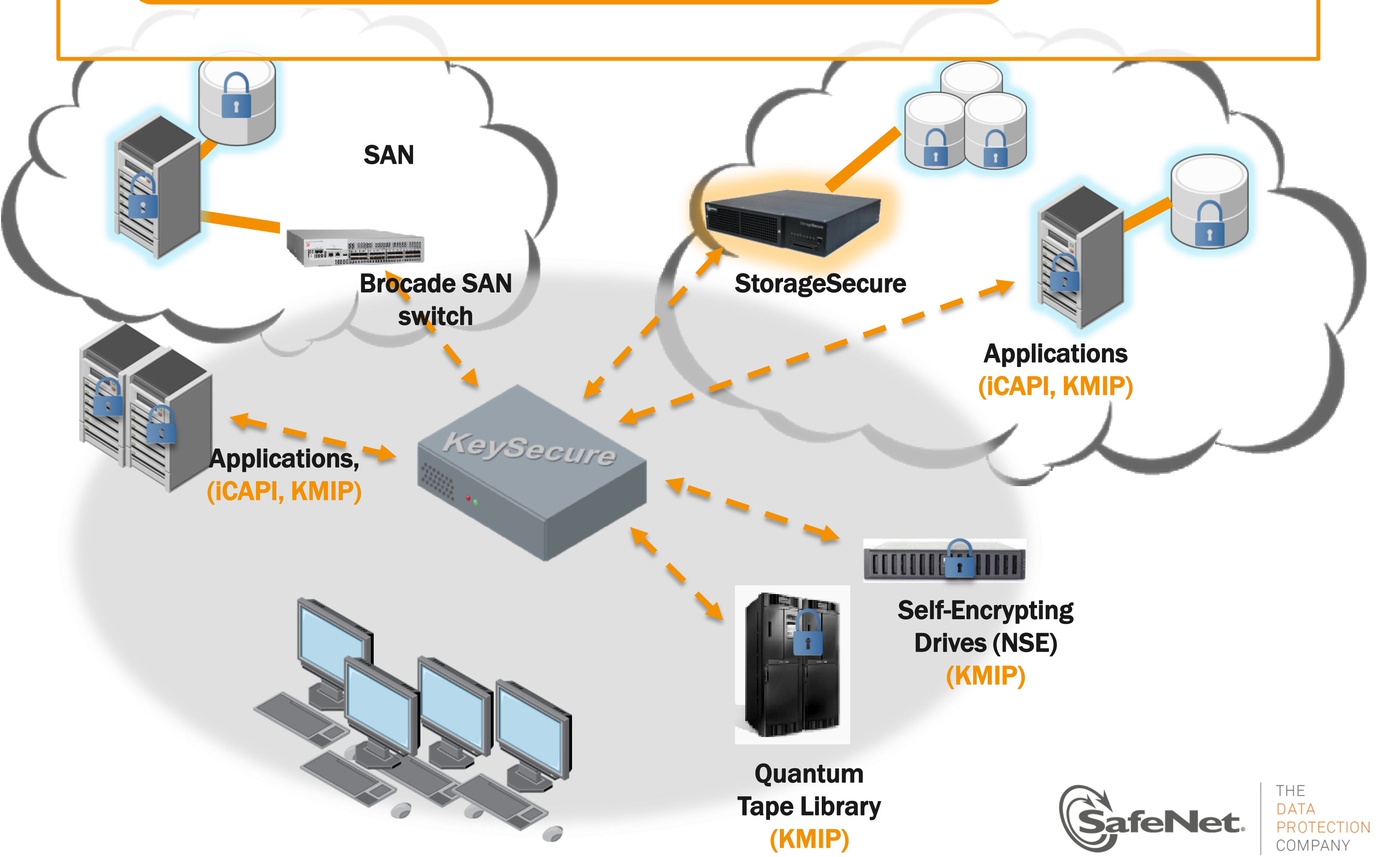
Enterprise Key Management

- Enterprise Key Lifecycle Management
  - Centrally managed, consolidation of keys
    - store, manage, generate, distribute, rotate, backup, activate, deactivate, and destroy
  - Up to 1 million keys per cluster
  - High Assurance Level
- Standard based approach – OASIS KMIP
- Broadest Coverage in Industry
  - NAS – StorageSecure
  - SAN - Brocade Encryption Solutions (BES and FS8/18)
  - KMIP support (NSE/FDE, Quantum Tape Library and other 3rd Party support)
  - Cloud-enabled (KMIP-based)
- SafeNet LUNA SA (HSM) and PCI Card Management
- ProtectV

•Hardware- based ,secure key replication across multiple appliances
•Active-Active mode of clustering
•Geo distribution support
•Highly scalable for cloud implementations
•LDAP/Active Directory Integration and Syslog forwarding
•Heterogeneous solutions: SFNT and non-SFNT devices, applications, databases, storage devices, SAN switches, tape libraries, HSM, network and endpoint devices, etc.

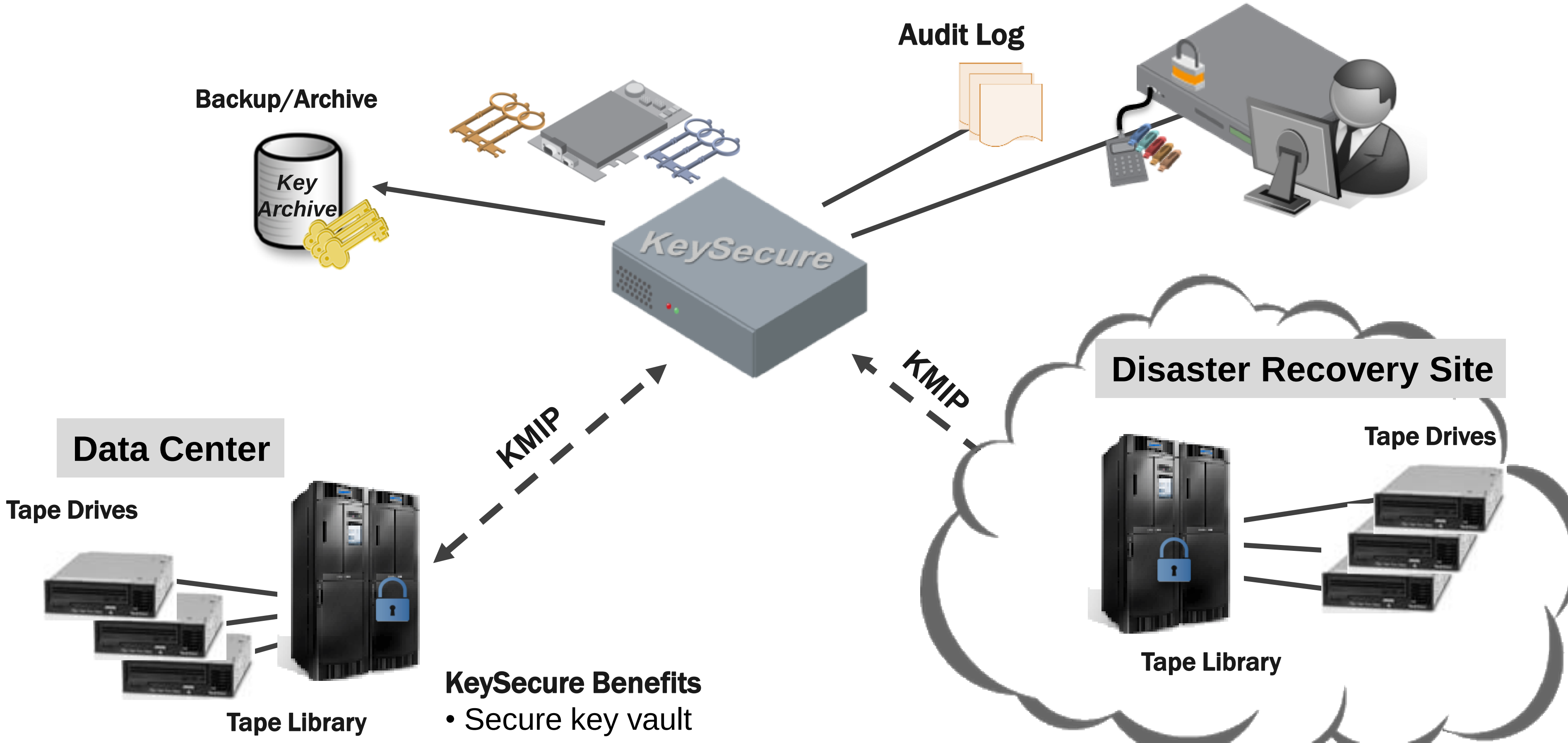
SafeNet
THE
DATA
PROTECTION
COMPANY

Ecosystem



SafeNet THE DATA PROTECTION COMPANY

Storage & Archive (Tape Libraries)

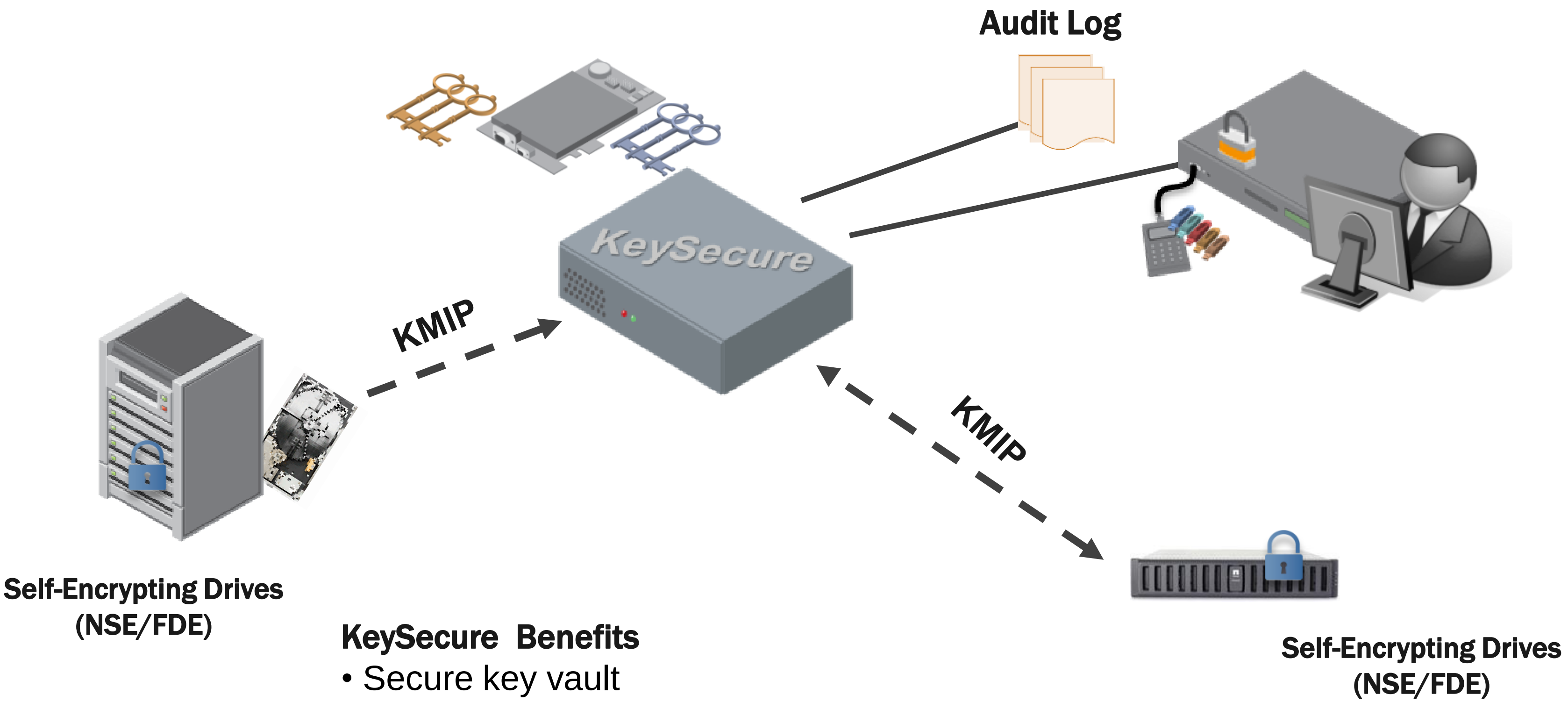


KeySecure Benefits

- Secure key vault
- Centralize key mgmt for backup and recovery
- High availability and clustering between geo-locations (e.g., HQ and Disaster Recovery sites)
- Key lifecycle management auditing and logging

SafeNet THE DATA PROTECTION COMPANY

Storage & Archive (NSE/FDE)

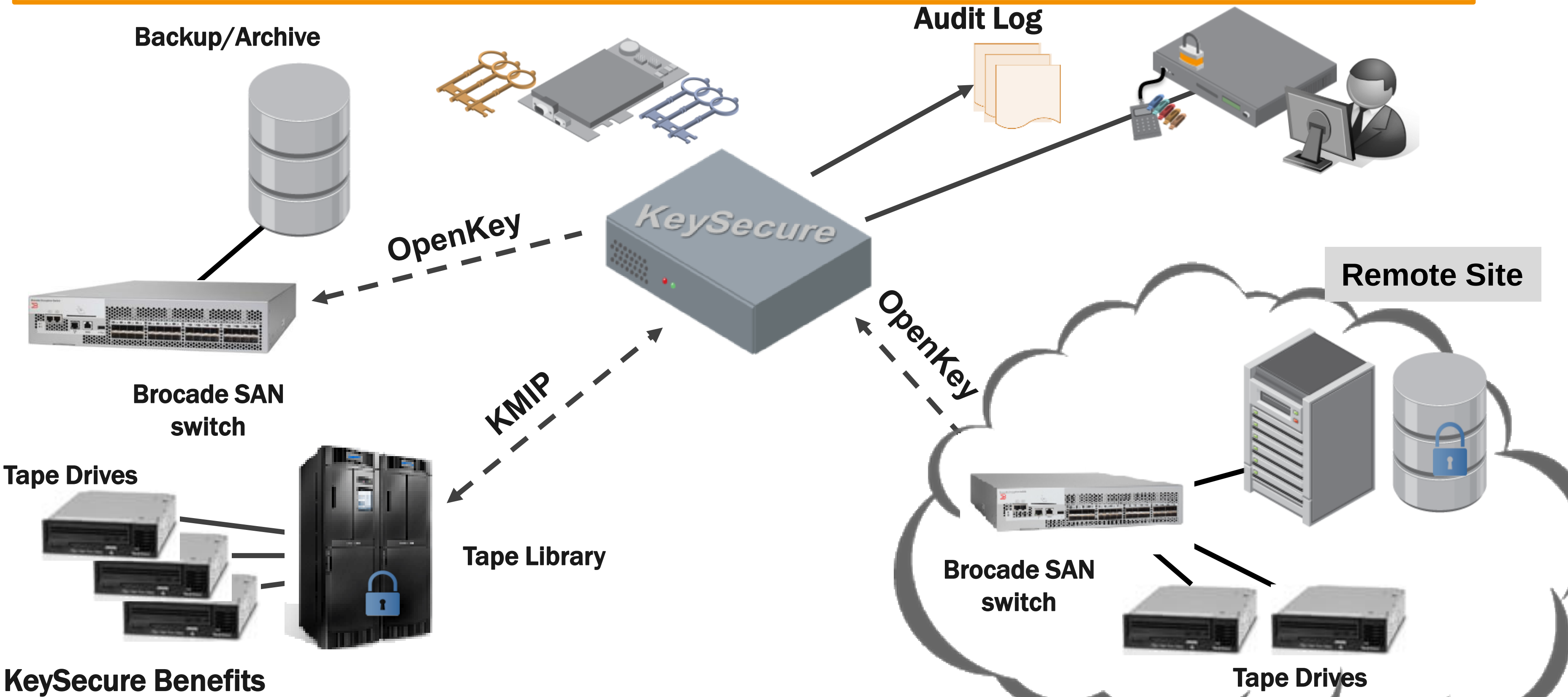


KeySecure Benefits

- Secure key vault
- Centralized policy management
- Secure key sharing, provisioning and storage
- Granular policy access controls provide separation of duties
- Secure data disposal
- Key lifecycle management auditing and logging

SafeNet THE DATA PROTECTION COMPANY

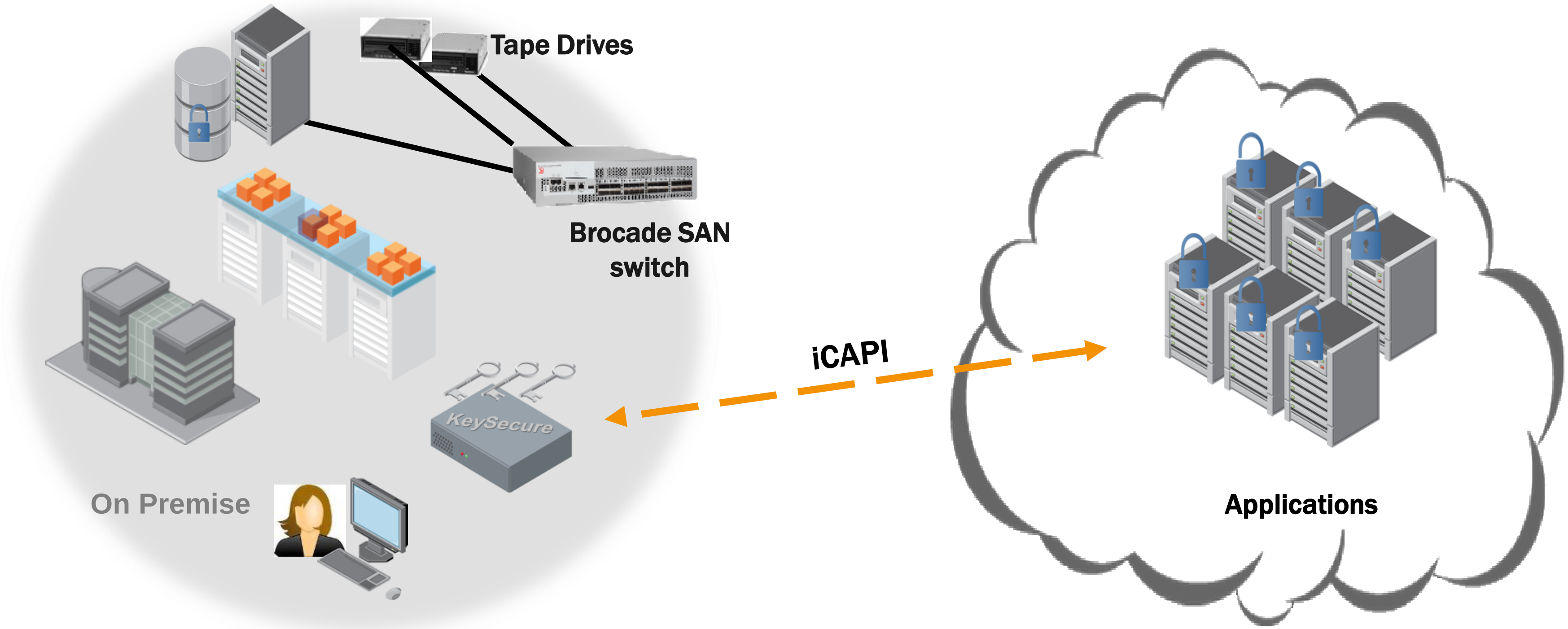
Storage & Archive (SAN)



KeySecure Benefits

- Centralized cryptographic key mgmt for SAN appliances & KMIP clients
- Automatic key sharing between sites to ensure encrypted data mirroring
- Centralized policy management
- Granular access controls for separation of duties
- Key lifecycle management auditing and logging
- Secure movement of keys across geographic boundaries (individual tapes)

Virtualization & Cloud

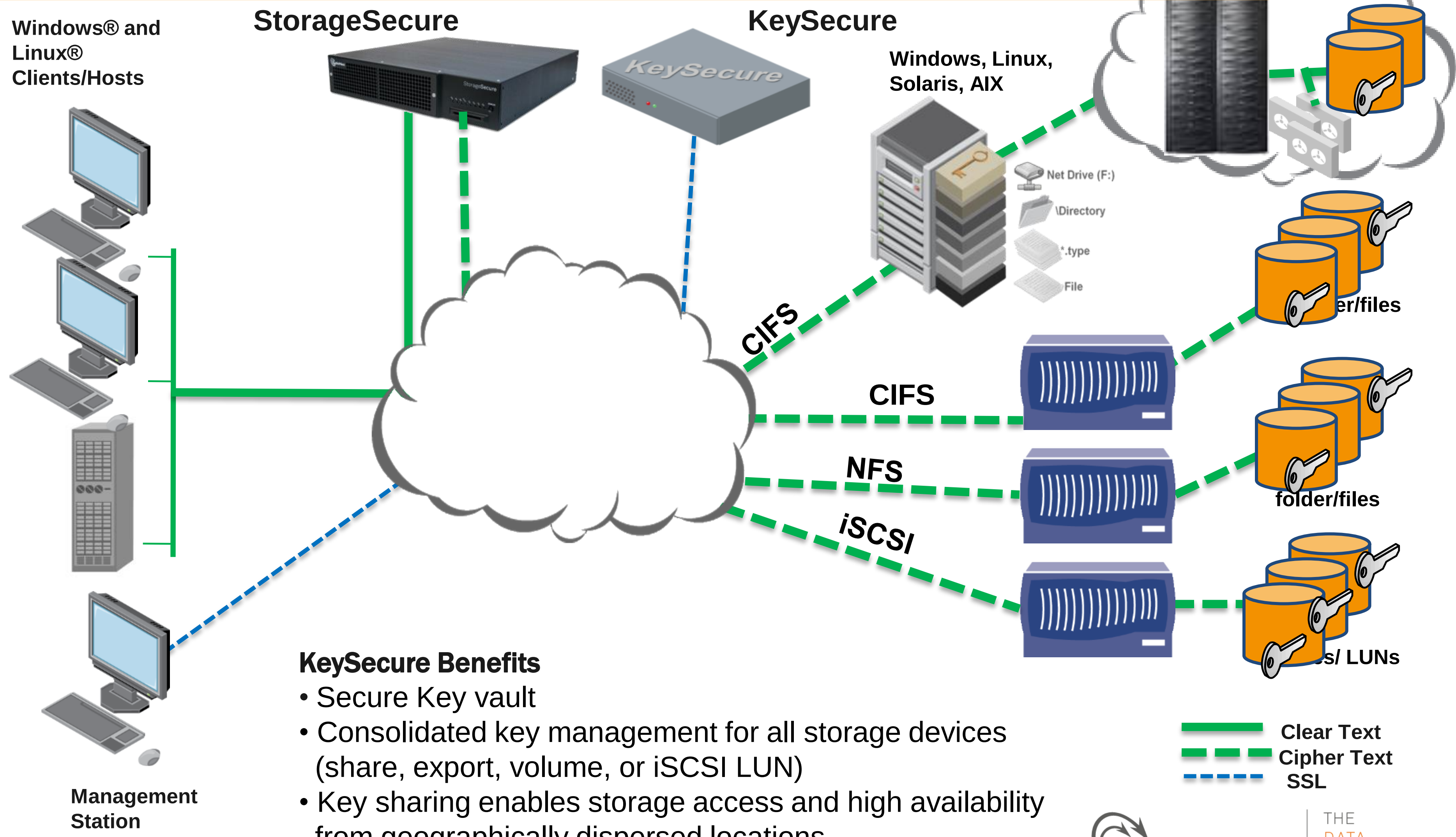


KeySecure Benefits

- Centralized key management for persistence and flexibility
- On-premise key vault – extends trust to the cloud
- Secure key creation , storage and vault
- Key archiving and shredding

SafeNet THE DATA PROTECTION COMPANY

StorageSecure



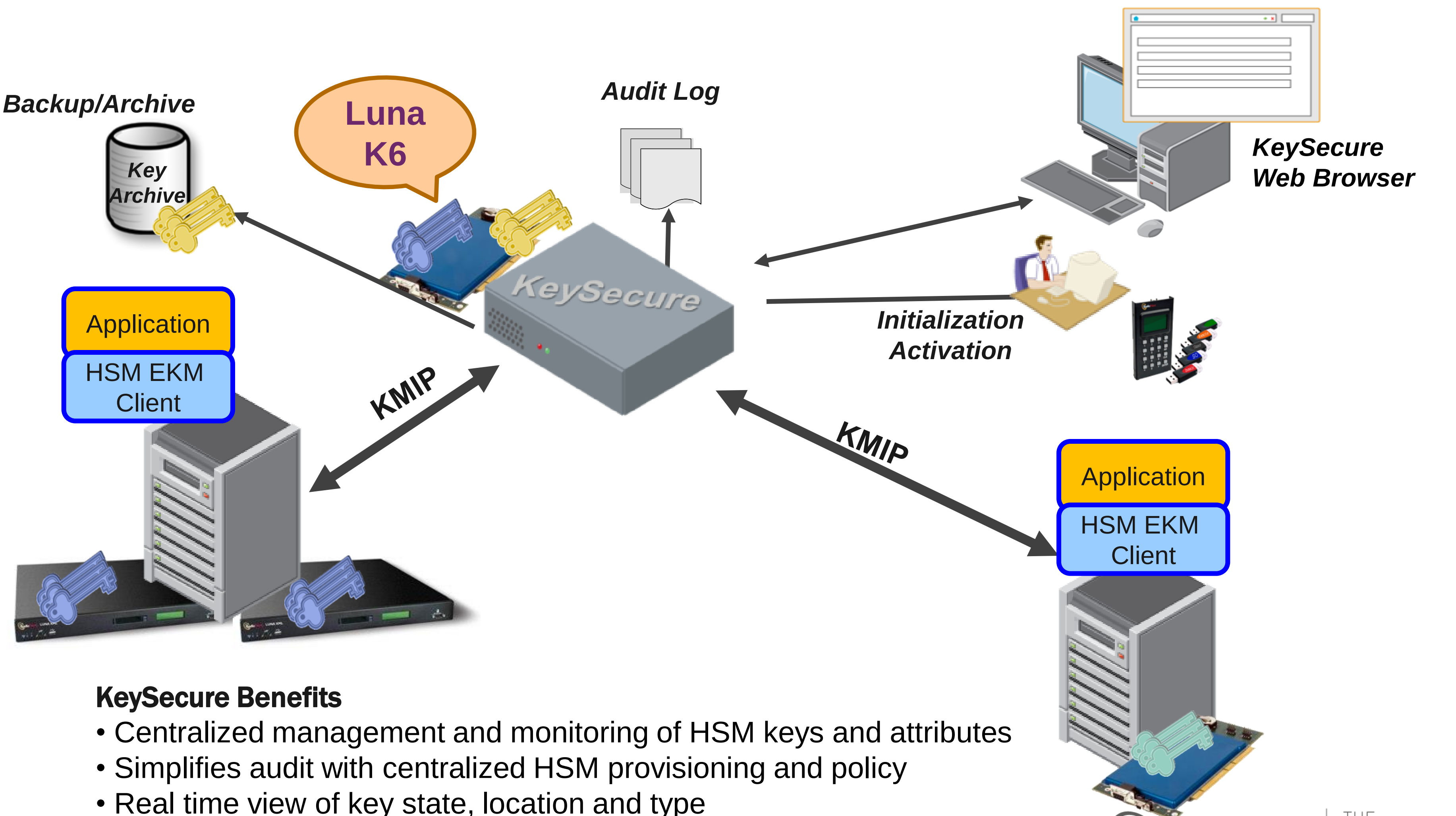
KeySecure Benefits

- Secure Key vault
- Consolidated key management for all storage devices (share, export, volume, or iSCSI LUN)
- Key sharing enables storage access and high availability from geographically dispersed locations
- Granular policy management provides separation of duties

SafeNet THE DATA PROTECTION COMPANY

HSM Key Management (KMIP)

Coming Soon (Q1 2012)

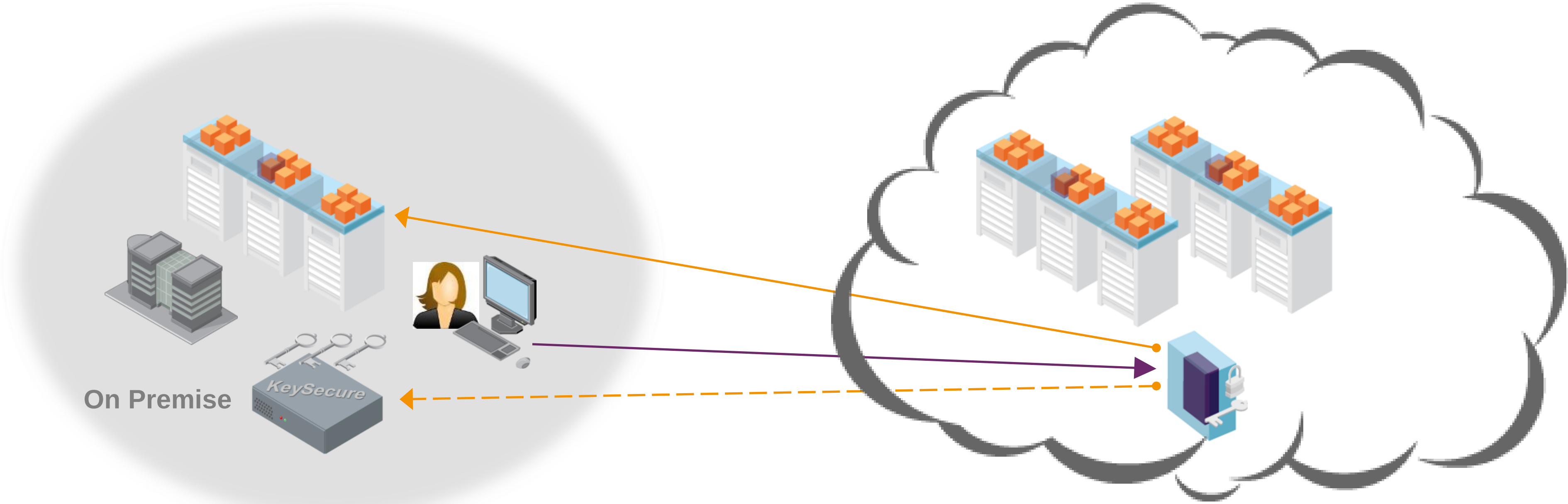


KeySecure Benefits

- Centralized management and monitoring of HSM keys and attributes
- Simplifies audit with centralized HSM provisioning and policy
- Real time view of key state, location and type
- Consistent security policy enforcement across all HSMs
- Key lifecycle management auditing and logging of key state changes

SafeNet THE DATA PROTECTION COMPANY

ProtectV

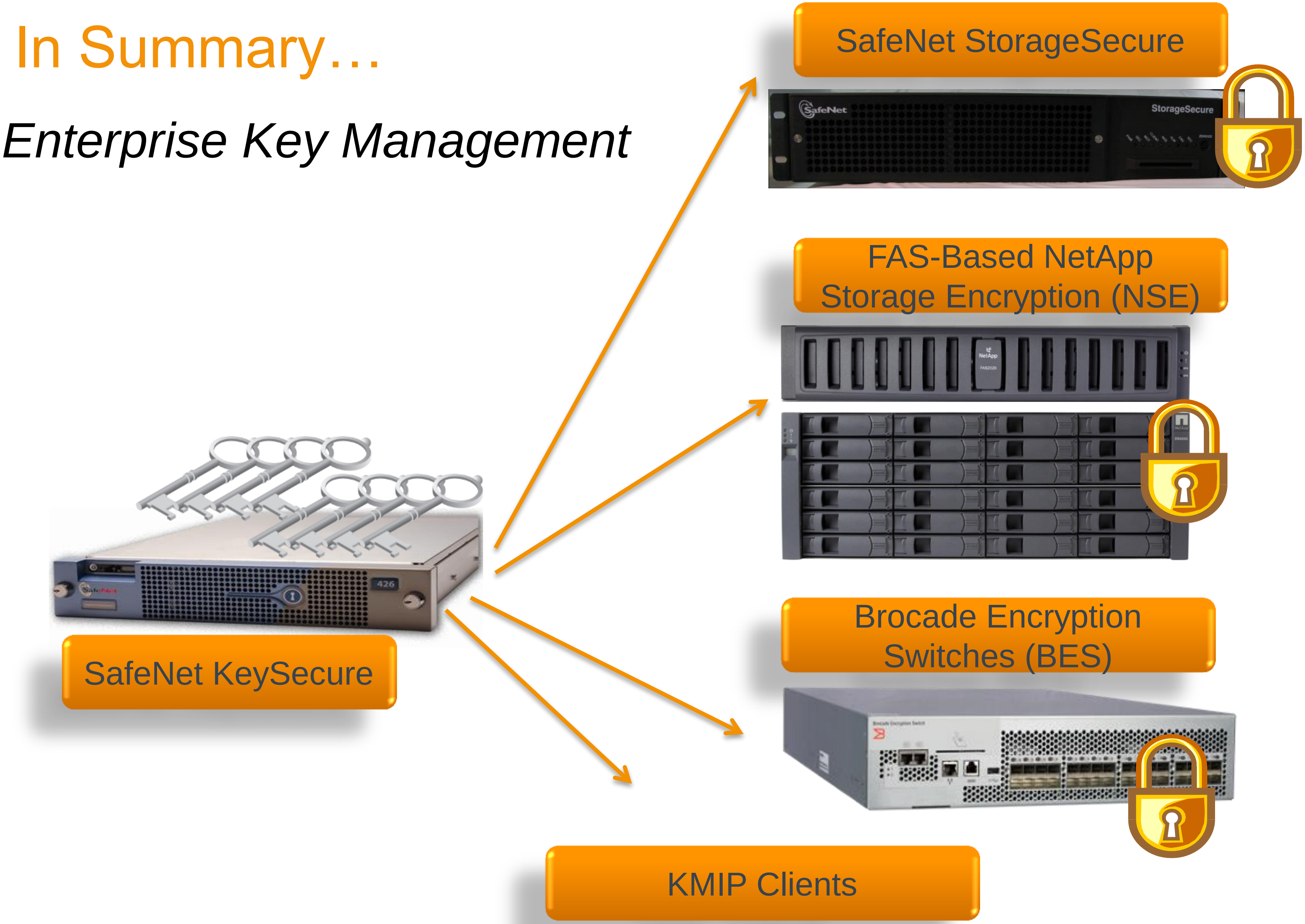


KeySecure Benefits

- Centralized key management for persistence and flexibility
- On-premise key vault – extends trust to the cloud
- Secure key creation , storage and vault
- Key archiving and shredding

In Summary…

Enterprise Key Management



SafeNet KeySecure

SafeNet StorageSecure

FAS-Based NetApp Storage Encryption (NSE)

Brocade Encryption Switches (BES)

KMIP Clients

OASIS

Advancing open standards for the information society

KeySecure Options

	KeySecure k460	KeySecure k150
Max keys (symmetric & asymmetric keys stored per cluster	1,000,000	25,000
Max concurrent clients	1,000	100
Redundant, hot-swappable hard drives & fans	Yes	No
Scalability	Unlimited	Unlimited
FIPS 140-2 level 3	Embedded LUNA K6 card (in process)	No
Supported Appliances		
KMIP compliant	Yes	Yes
Cloud Encryption/Virtualization	Cloud Enabled ProtectV (Q2 2012)	Cloud Enabled ProtectV (Q2 2012)
Tape Libraries	Quantum Tape Libraries	Quantum Tape Libraries
NAS, SAN Storage appliances	SafeNet StorageSecure (Q1 2012) NetApp DataFort and LKM NetApp NSE Brocade Encryption SAN Switch (BES)	
Hardware Security Modules (HSM)	SafeNet LUNA SA (Q1 2012) SafeNet LUNA PCI (Q1 2012)	