

Who's Protecting



Your Keys?



Protecting the most vital data from the core to the cloud to the field

Trusted, U.S. based source for cyber security solutions...

We **develop, manufacture, sell** and **support** exclusive, trusted data security solutions in the U.S. that easily integrate into an existing cyber security infrastructure.

...from the core to the cloud to the field...

Our solutions enable agencies to deploy a **holistic data protection ecosystem** where data and cryptographic keys are secured and managed, and access and distribution are controlled.

...addressing the most pressing use cases.

Our solutions address many pressing use cases including **PKI, digital signatures, TLS Private Key Protection, data-at-rest and in motion protection, information sharing and authentication.**

Trusted, U.S. Based Source for Cyber Security Solutions

Support

Develop

Trusted data security solutions in the U.S. that easily integrate into an existing cyber security infrastructure

- Design core solutions for U.S. Federal agencies with code maintained and compiled by SafeNet AT
- Provide U.S. federal agencies with solutions that have a U.S. supply chain lifecycle
- Maintain required federal government approvals and certifications to develop, support and sell products to federal agencies

Sell

Manufacture

Agenda

- Cyber Security Landscape
- Key Management Fundamentals
- Enterprise Key Management

Cyber Security Landscape



THE REALITY OF DATA BREACHES

DATA RECORDS COMPROMISED IN FIRST HALF OF 2018

3,353,172,708

18,525,816
records lost or stolen
every day



771,909
records
every hour



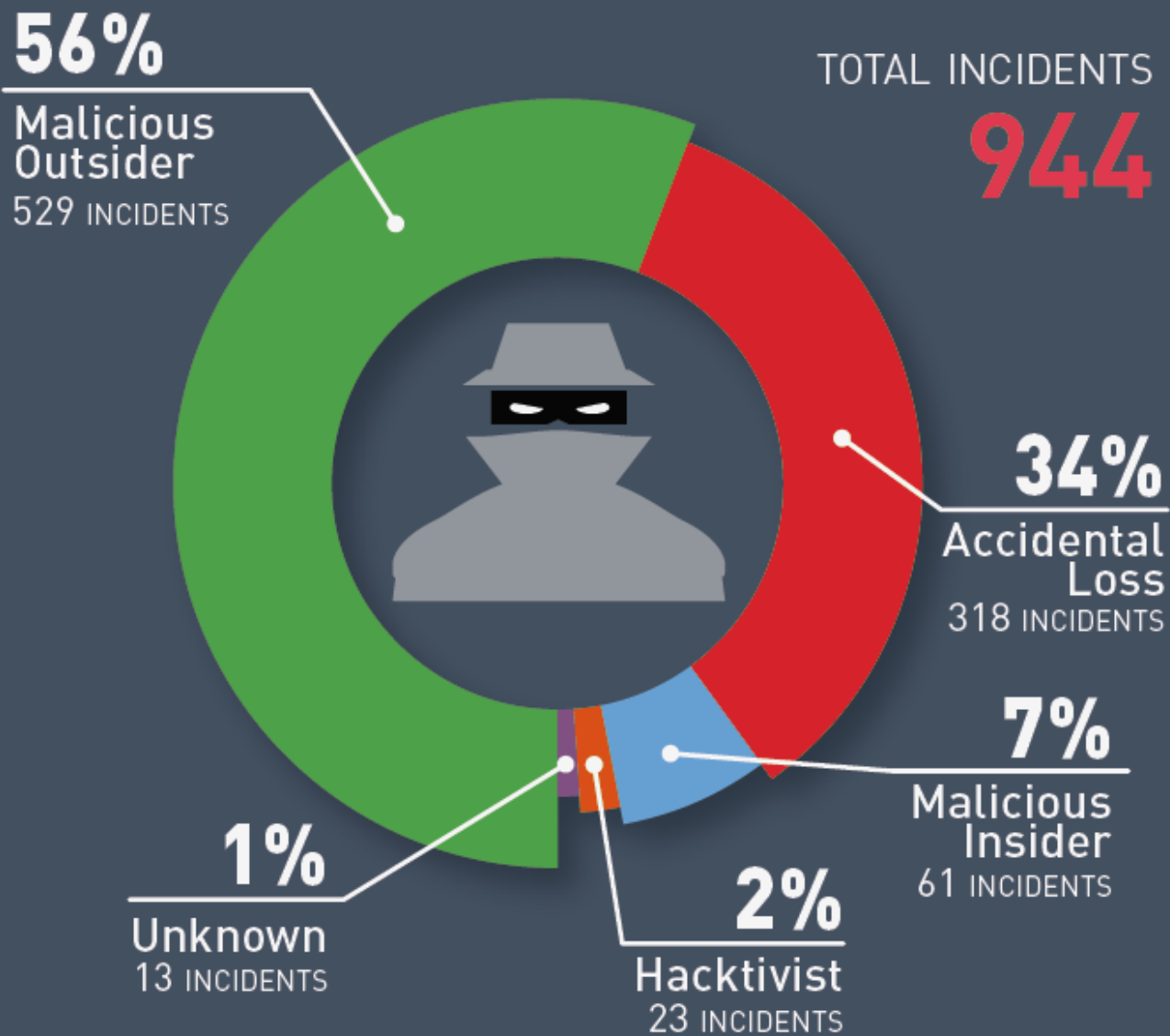
12,865
records
every minute



214
records
every second



Number of Breach Incidents by Source



Key Management Fundamentals



Importance of Cryptographic Keys

Encryption process generates cryptographic keys used to lock and unlock data.

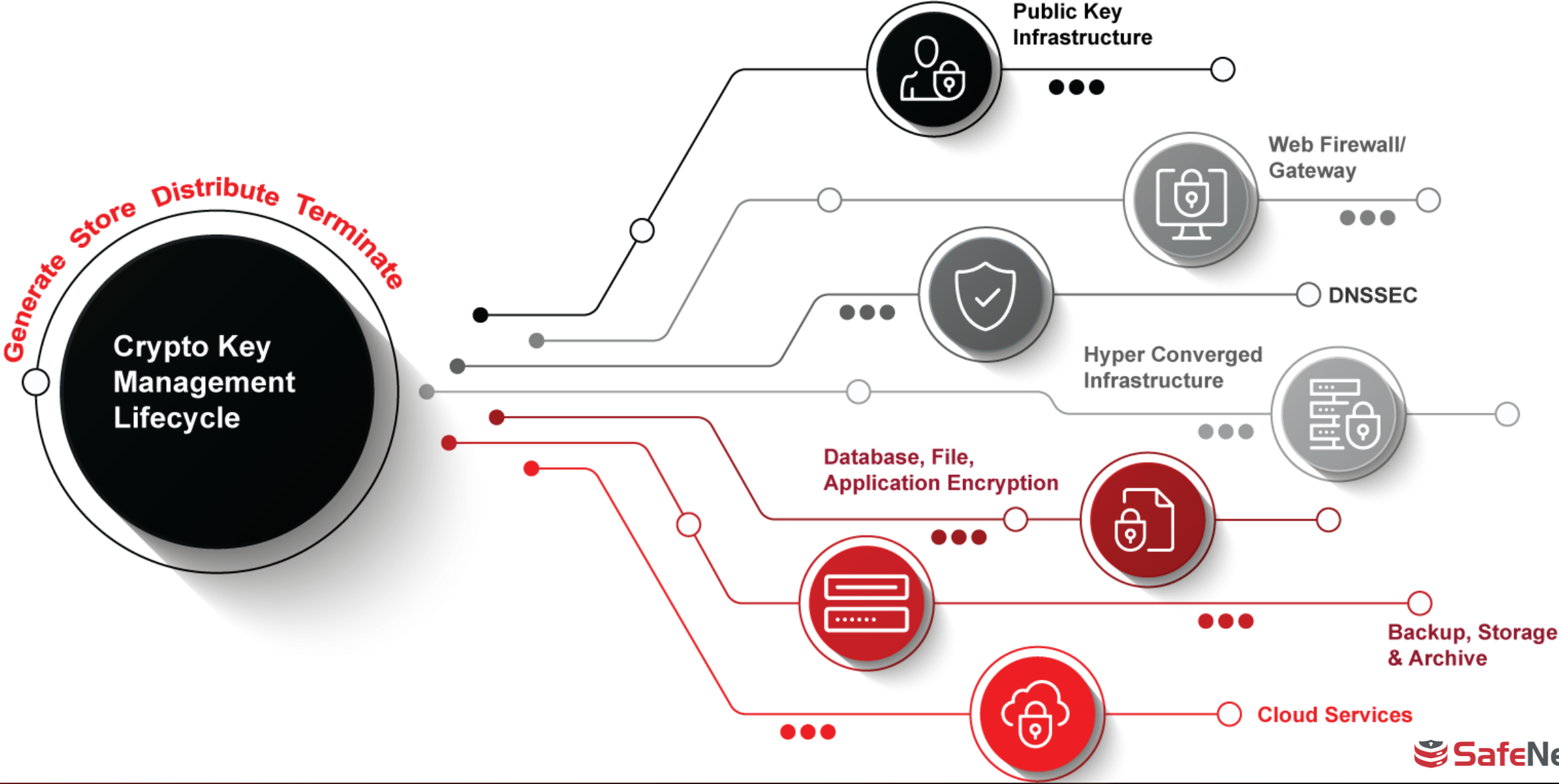
Cryptographic keys are the keys to the kingdom.



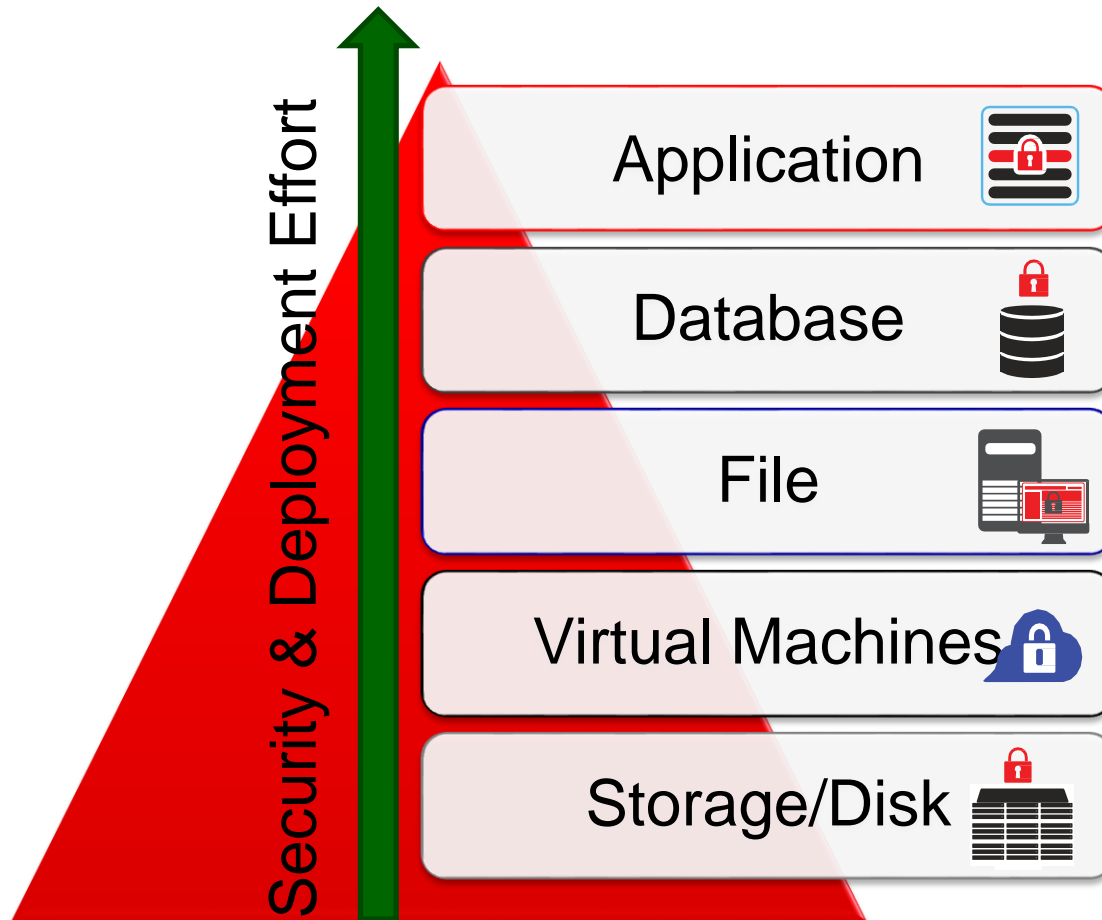
If these keys are stolen or copied, they can be used to decrypt sensitive data.

The more you encrypt, the more encryption keys you have to store & manage.

What is Cryptographic Key Management

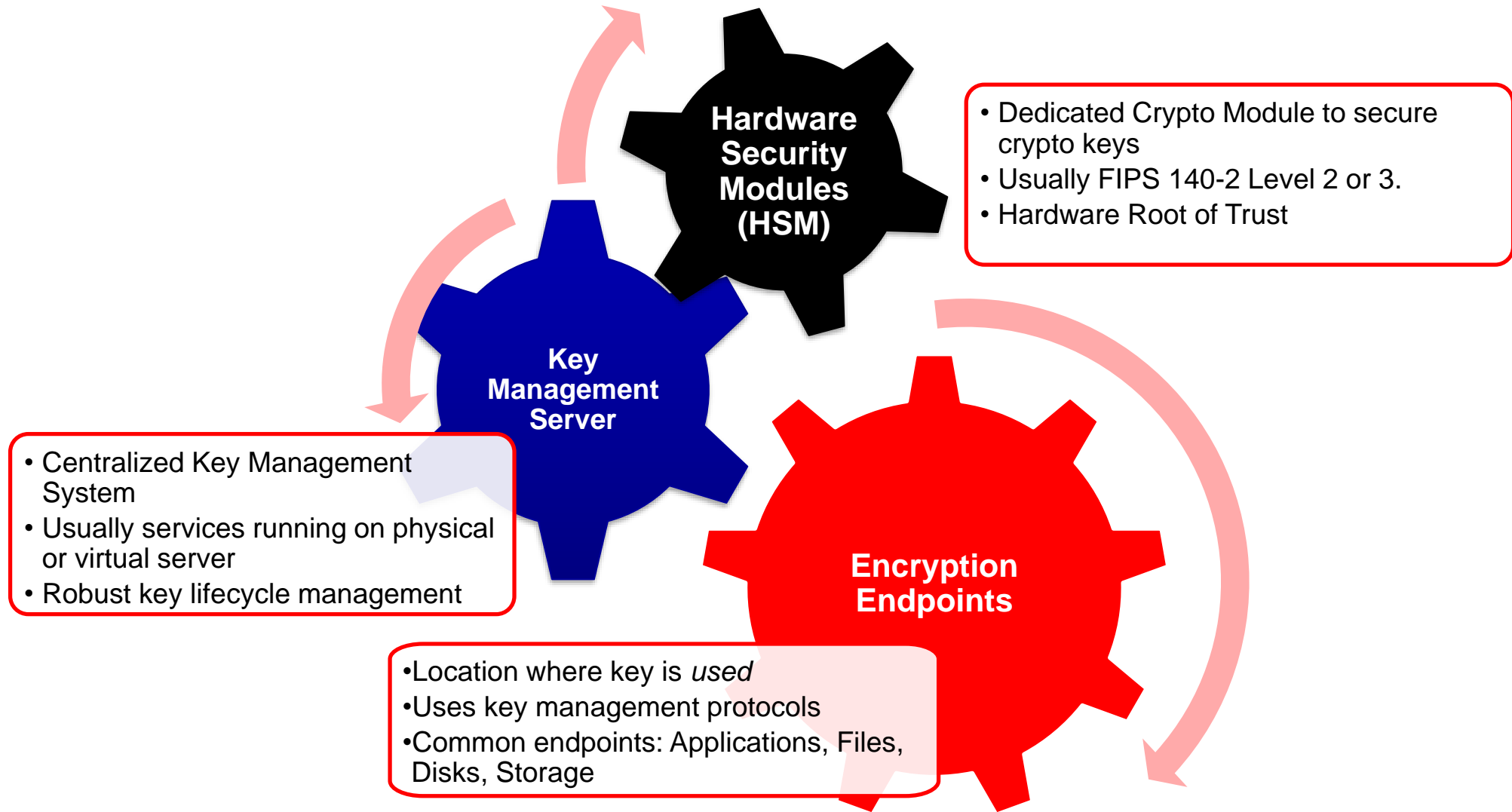


Encryption Layers



- There is not a “best” layer to do encryption
- Depends on the threat vector
- Complexity varies
- Often encrypt at multiple layers
- Principles of CSfC
- **They ALL need key management!**

Key Management Components



Important Standards

NIST 800-57

- SP 800-57 Recommendation for Key Management
- 3 Parts: General, Organization, Implementation

NIST 800-152

- SP 800-152 A Profile for US Federal Cryptographic Key Management Systems
- Requirements for design, implementation, management, etc.

OASIS KMIP

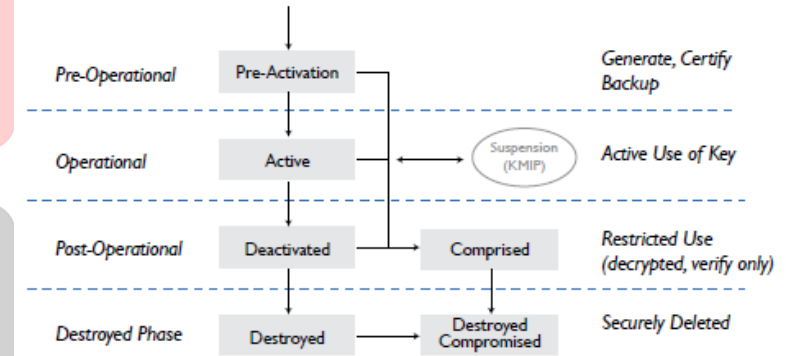
- Key Management Interoperability Protocol (KMIP)
- Specification, Profiles, Usage Guides

PKCS

- Public Key Cryptography Standards (PKCS)
- OASIS PKCS#11 Crypto Token Interface

FIPS 140-2

- Security Requirements for Cryptographic Modules
- Four Security Levels



SP800-57 Key Lifecycle

Enterprise Key Management



Encryption in Today's Enterprise: The Current Situation

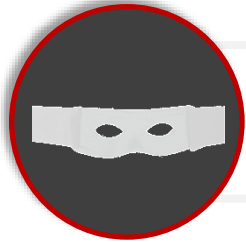
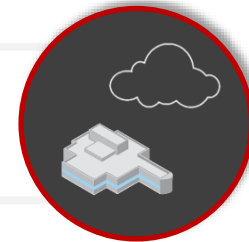


MORE SENSITIVE DATA

Produced, processed, stored, and shared in more places

MORE DEPLOYMENTS

On-premises and in the public cloud



MORE THREATS

Malicious internal or external threats and breaches

MORE "ISLANDS" OF SECURITY

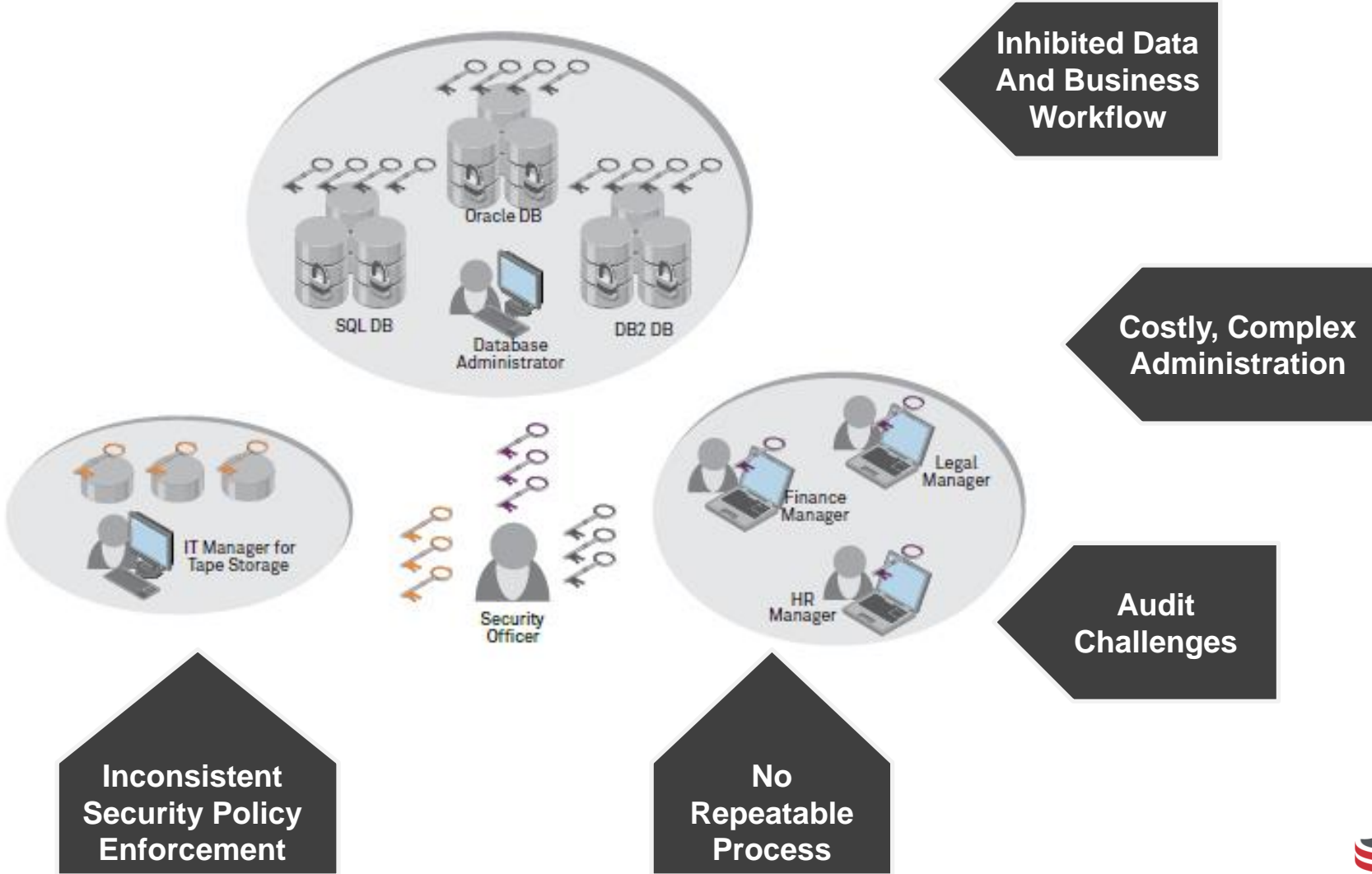
Disparate, isolated encryption projects and approaches



MORE OVERLAP

Multiple encryption platforms deployed across the enterprise

The Result: Isolated Islands of Encryption



Implementing an Effective Encryption Strategy

Identify Sensitive Data Where it Resides

- Check data-at-rest in storage, file servers, applications, databases, removable media.
- Look both on-premises and in the cloud.
- Don't forget data-in-transit.
- Identify which users should have data access rights

Protect Sensitive Data

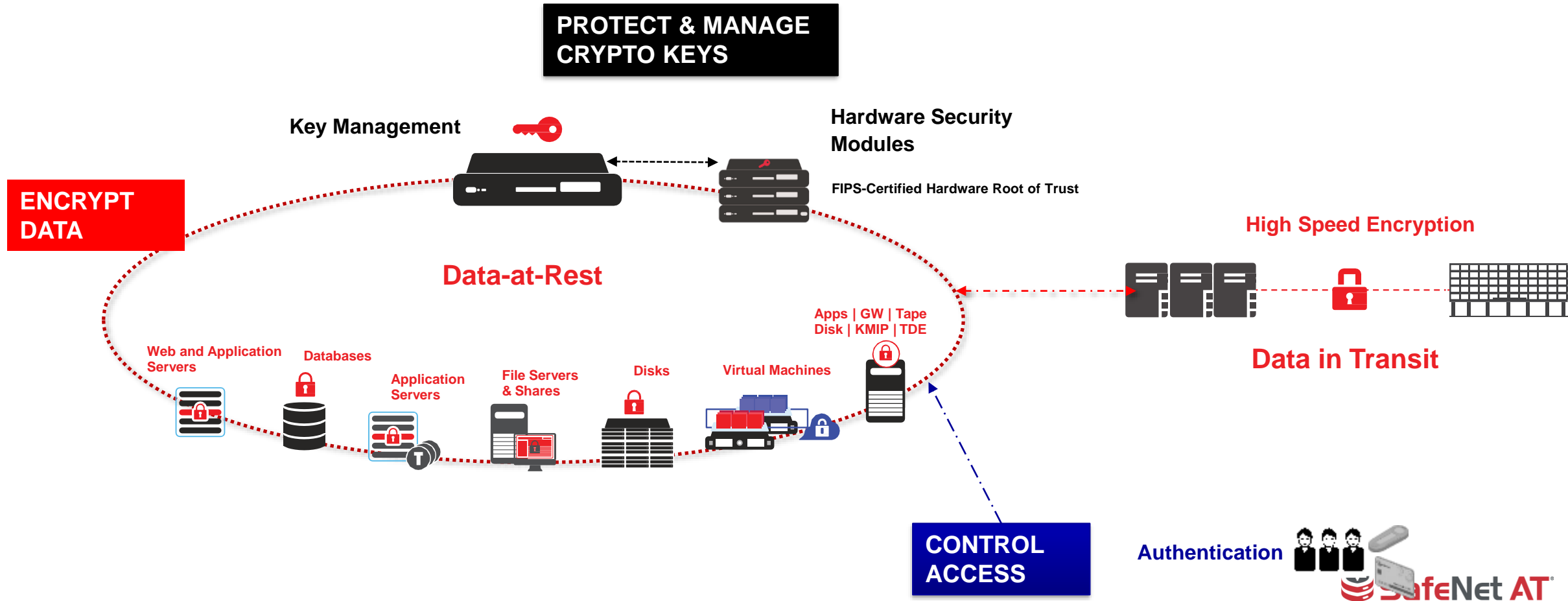
- **Encrypt data-at-rest** - Apply granular encryption and role-based access control for data residing in databases, applications, files and storage both on-premises and in the cloud.
- **Encrypt data-in-transit** - Secure data as it travels across the network with high speed encryption.
- **Control access to data** – Use strong authentication, especially for “privileged users”.

Manage the Protection

- Cryptographic keys should be treated with the same level of care.
- For maximum security, dedicated hardware key management protects sensitive cryptographic keys from attack.
- Prepare for compliance audits by using centralized logging for data and key access.

Holistic Data Protection Architecture

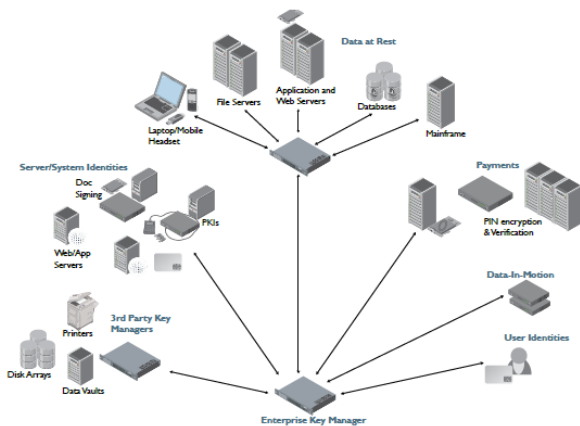
Encrypt Everything
Manage the Keys
Control User Access



Enterprise Key Management Advantages

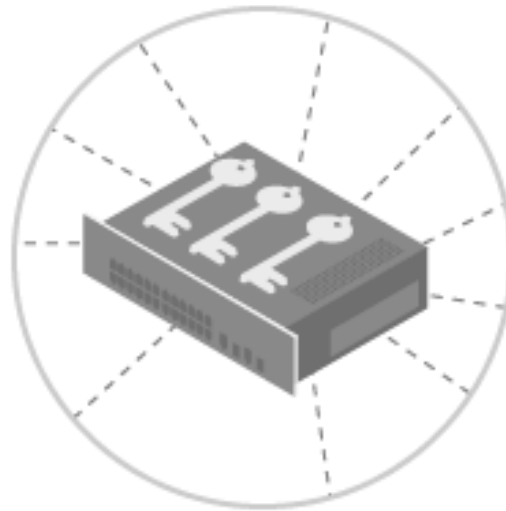
Crypto Management & Encryption Portfolio

Consolidates and centrally manages cryptographic objects and policies from multiple, disparate encryption platforms.



Scalability & High Availability

Automatically synchronizes and replicates keys to ensure data availability – eliminating key/data connectivity concerns.



Centralized Audit and Reporting for Compliance

Captures key lifecycle management activity to provide a single audit point for compliance validation



Thank You

