SafeNet Enterprise Key Management – KeySecure

SafeNet
THE DATA PROTECTION COMPANY

Customer Problem

- Fragmented encryption solutions have proliferated through internal projects and compliance mandates, across multiple tiers and multiple vendor platforms, leaving organizations in a management and operational quandary. As the number of encryption solutions increase, the number of encryption keys grow proportionally.
- Security teams struggle with the administrative efforts of managing encryption deployments and associated key lifecycle operations.

SafeNet Solution/Value Proposition

- KeySecure is the industry's first high-assurance, FIPS validated, KMIP standards-based Enterprise Key Management (EKM) solution.
- KeySecure provides robust enterprise key lifecycle management, and enables centralized management of millions of encryption keys and key policies through a hardware-based platform, covering heterogeneous systems across the enterprise, from the data center to virtualized environments.

SafeNet Advantages

Heterogeneous Key Management Support

- Centralized key lifecycle capabilities from storage and archive systems to encryption in SAN switches to mixed databases and applications today and HSMs in the very near future.

KMIP Standards-based Interoperability

- Secures keys from KMIP-based solutions such as Quantum Tape Libraries today and more to come and easily expands interoperability.

Ensures Compliance

- Integrates with existing infrastructures to provide unified key lifecycle management, data isolation, and protect partitions in multi-tenant environments.

Next Generation Key Management

- Replaces NetApp LKM (Lifetime Key Manager)
- Manages encryption keys from self-encrypting drives (such as NetApp NSE), existing DataFort implementations, and Brocade SAN switches using encryption
- Supports keys for StorageSecure – the next generation DataFort solution.

Roadmap to Expansion

- Integrates with a variety of encryption devices (between KeySecure and HSMs, StorageSecure, and ProtectV) offers a powerful cross-selling tool.

Competitive Analysis

RSA Data Protection Manager (formerly RSA Key Manager):

- *What They Say:* Data Protection Manager leverages RSA's common enterprise key-management infrastructure to simplify the provisioning, distribution, and management of encryption keys and can be easily integrated with a number of host, database, SAN switch, and native tape-encryption solutions, among others.
- *What We Need to Say:* KeySecure is a hardware-based, out-of-the-box key management solution with the broadest coverage from storage & archive systems, SAN switches using encryption, Quantum Tape Libraries, NSE (self-encrypting drives), HSMs, databases, applications, and easily expands interoperability with 3rd party and legacy systems through KMIP.

IBM Tivoli Key Lifecycle Manager

- *What They Say:* Locking down data through key-based encryption with IBM Tivoli Key Lifecycle Manager
- *What We Need to Say:* KeySecure is a hardware-based, out-of-the-box key management solution. KeySecure offers the broadest system coverage, highest assurance and scalability for any key management solution.

Other Niche Vendors (Venafi, Vormetric, Voltage, Protegrity, NuBridges)

- *What They Say:* Varied from certificate , key & SSH mgmt, to key security expert, to stateless key mgmt, etc.
- *What We Need to Say:* Security is our core company strategy. More than 30 years of accumulated security .

Market Segments

All market segments including Banking and Investment, Insurance, Government, Healthcare, Manufacturing, Retail, Media, Energy & Utilities

Target Customer Profile

SafeNet KeySecure centralizes key lifecycle capabilities across heterogeneous environments—from storage and archive encryption systems, to SAN switches using encryption, to mixed databases and applications today and HSMs in the very near future.

- NAS, SAN & DAS storage customers
- Brocade BES storage customers
- Quantum Tape Libraries customers
- Large-scale Luna HSM customers
- KMIP standards-based systems
- Existing NetApp DataFort customers

Corporate Position of Strength

30 Years in Security: Since 1983, SafeNet has been solving complex security issues.

Large Enough to Scale, Small Enough to Adapt: SafeNet is a $500M company with over 1700 employees with a unique ability to respond to both customer requirements and the changing threat landscape.

The Data Protection Company: SafeNet protects its customers' most valuable asset - data. More than 25,000 customers, from commercial to government, In over 100 countries - - trust SafeNet.

Trust Is Earned: Security is SafeNet's core company strategy. We have accumulated extensive knowledge and understanding of the challenges facing enterprises and have answered those challenges through our broad product solutions.

SafeNet Enterprise Key Management – KeySecure

THE
DATA
PROTECTION
COMPANY

Qualifying Questions

- Do you have sensitive data?
- Where do you store your sensitive data?
- Do you use encryption to protect your data?
- Do you have more than one encryption solution &/or encryption vendor in your organization?
- Where do you store the keys?
- Do you use storage encryption to protect your data-at-rest?
- Do you your backup / archive data? How do you store the keys? Do you store the keys with the tape?
- How do you verify data is not accessible to unauthorized users?
- How do you provide key lifecycle management (key rollover, key versioning, policy management) for your existing encryption solutions?
- How are you validating compliance for your encryption keys (auditing, logging, and alerting on key state changes)?
- How do you handle a compelling event such as an upcoming audit to prove compliance for your encryption keys?
- Are you planning on migrating your data to the cloud?

Objection Handling

Hardware is more expensive. Why would I want to pay more when I will need to do more for installation (find datacenter space, rack the unit, obtain an IP address, etc)?
Hardware-based solutions are more secure. KeySecure is a high assurance, FIPS, solution-in-a-box that controls the way encryption is used for compliance, audit control, policy management, separation of duties, and dual control. KeySecure embeds a SafeNet HSM card to provide secure repository and FIPS boundary for critical keys.

My enterprise has a mixture of encryption vendors including native hardware and software systems. There isn't a key management solution that can handle the different types of native encryption.
KeySecure can. KeySecure is a hardware-based, out-of-the-box key management solution with the broadest coverage from mixed databases and applications, to storage & archive systems, to HSMs, to encryption in SAN switches, and interoperability with 3rd party and legacy systems through KMIP. KeySecure can grow as the business expands and transactions grow.

Aren't hardware solutions slower than software? Why would I want to buy a hardware platform?
Having a single, dedicated hardware-based key management platform eliminates the need to deploy multiple systems and software. Centrally managing all of your encryption keys with one system gives IT one company to contact and one company for support.

When I move to the cloud, I want a virtualized appliance. Why would I want a physical appliance now?
You want physical ownership of your keys to maintain ownership and control of data as you migrate to the cloud. KeySecure maintains your root of trust in the cloud. KeySecure evolves with you as you extend into the cloud.

If I centralize all of my keys, why shouldn't I be concerned that this is a central point of failure?
KeySecure has high availability and load balancing with key and policy management distributed globally. Keys are synchronized with all of the clustered KeySecure platforms preventing the concern if one system is unreachable, users are unable to access data. KeySecure automatically backs up keys and policies for disaster recovery.

SafeNet References and Tools

- Product Brief
- Customer Presentation
- Sales Presentation & Use Cases
- Quantum Solution Brief
- Competitive
- Key Management Blog
- Press Release and more

http://sno/dps/Product%20Management/Pages/KeySecure.aspx

Certification, Reviews, and Awards SafeNet References and Tools

Gartner
"As the use of encryption grows and various solutions are deployed, key management becomes exponentially critical and complex. Mismanagement of keys can expose an organization to unnecessary risks."

FIPS 140-2 level 3 (in process)

SafeNet Cross-Sell/Up-Sell

KMIP: As a interoperability protocol for legacy systems with KeySecure centrally managing KMIP based systems

StorageSecure: As storage encryption solution with KeySecure centralizing key management

HSM: KeySecure provides centralized monitoring of all the keys for each HSM partitions in an enterprise. Additionally KeySecure supports remote key foundry where an administrator can control key creation process centrally but actual keys are generated in local HSMs