Many organizations live and die by their data. A host of problems, ranging from legal issues to financial penalties, may be at stake if an organization’s data is stolen. If your customer uses encryption to secure data access against unauthorized use, they have already taken some important steps to mitigate those risks. Although encryption does render data unreadable if files are copied or disk drives stolen, data can still be compromised if the encryption keys fall into the wrong hands.

SafeNet KeySecure from Gemalto provides security teams with the critical capabilities to securely store encryption keys. Encryption keys that are stored in hardware effectively and persistently help meet governance, compliance, and data protection mandates. This document identifies common business uses cases for SafeNet KeySecure, which interoperates as a key management solution for industry-leading encrypted storage solutions, including NetApp Storage Encryption (NSE), Dell SC and XC Storage solutions, Hitachi HUS and VSP solutions, IBM XIV storage, and dozens of other products.

Business Case 1: Protection against physical theft of disk drives
To protect data against the unauthorized removal of disk drives, many organizations are turning to self-encrypting disk drives. Without access to the associated encryption key, the data is rendered unreadable, and protects the customer’s data from theft. However, best practices also recommend a centralized approach to key management, in order to easily keep pace with the growing volume of encryption keys associated with self-encrypting drives.

Can your organization demonstrate that it can protect data against physical theft of disk drives?
SafeNet KeySecure protects data from physical theft of disk drives when used with standards-based Key Management Interoperability Protocol (KMIP) encryption systems that are deployed with full-drive encryption.

For many full-drive encryption solutions, during configuration SafeNet KeySecure generates a unique authentication key and encryption key for each self-encrypting disk drive. When the shelf is powered up, the authentication key is requested and sent to the disk drive, allowing it to unwrap its unique encryption key. Unless the disk, shelf, and key manager all agree, the data on the drive cannot be accessed.

> This approach strengthens the customer’s control over data access, while centralizing key management across the enterprise.
> Customers can rest assured that stored data remains protected against unauthorized access, even if disk drives are stolen.

Business Case 2: Meet compliance and/or audit mandates
Encryption solutions can provide many benefits in protecting your customer’s corporate data. However, management complexity of both data and encryption keys can become overwhelming when multiple encryption solutions are deployed across applications or departments. As encryption solutions increase, so do the number of encryption keys that need to be managed. And when encryption solutions have been deployed in a piece-meal approach, each discrete encryption deployment has the potential to become a weak link in the security chain, and could provide an entry point for compromise.

Can your organization demonstrate that its key management meets compliance and/or audit mandates?
SafeNet KeySecure helps customers meet compliance and/or audit mandates by consolidating key security policies across multiple, disparate KMIP-based encryption systems.

Gemalto products provide a high-assurance, FIPS-compliant, solution that controls the way encryption is used for compliance, audit control, policy management, separation of duties, and dual control. This approach simplifies and strengthens your control over data access by authorized users, and prevents access by non-authorized personnel or outside threats.

> Provides verifiable audit trail for all key management actions to address compliance requirements.
> Guard against insider threats (rogue admins) through separation of duties, with individual or group-level authorization and defined key validity time frames.
> Benefit from a non-repudiative audit trail of key state changes with built in auditing, logging, and alerting. Administrators are informed if attempts to breach occur.

Business Case 3: Protect intellectual property in multi-tenant environments
Organizations are increasingly taking advantage of the cost efficiencies afforded by multi-tenant and cloud computing environments. While sharing resources provides many cost, usage, and operational benefits, new issues regarding data separation and security must be addressed.
Can your organization demonstrate that it adequately protects intellectual property in multi-tenant environments against unauthorized disclosure?

SafeNet KeySecure provides centralized and consistent enterprise key management that integrates with existing infrastructures. This allows customers to protect intellectual property with a unified key lifecycle management solution that protects data across multi-tenant or cloud environments with isolation and granular access to data.

This is achieved by separating the administrative duties, requiring individual or group-level authorization combined with defined key validity time frames so that disk and security administration can be handled by different IT professionals. In addition, SafeNet KeySecure provides a verifiable audit trail for all key management actions so you can make sure to address any compliance requirements in your shared infrastructure environment.

- Isolate data and protect existing partitions in multi-tenant environments.
- Protect data belonging to security-sensitive departments.
- Restrict access, only allowing authorized administrators to perform specific tasks. Access, administration, and encryption keys are tightly controlled by security mechanisms including multi-factor authentication.

Business Case 4: Secure data in disaster recovery sites

To protect against natural or man-made disasters, many organizations backup or replicate their production environment to an offsite disaster recovery location. To protect sensitive data as it travels between sites, encryption will render the data unreadable if an unauthorized interception or access attempt occurs. In addition, implementing a centralized key management solution will protect and manage the data as it is being replicated across sites, eliminating replication as a potential weak link in the security chain.

Can your customer demonstrate that all of its data, including data at disaster recovery sites, is secure?

SafeNet KeySecure secures the customer’s disaster recovery data through centralized and consistent enterprise-wide key management. It consolidates key security policies across multiple disparate KMIP-based encryption systems to simplify and strengthen control over data access even at remote locations.

- Separate keys from backup tapes or drives to maintain cross-enterprise control of millions of encryption keys and key policies with centralized key management.
- Protect disaster recovery data against unauthorized disclosure, and maintain control even when it is located off-site in a primary data center.

Business Case 5: Maintain high performance and availability of data

Downtime is not an option in business today. As organizations use distributed resources to meet storage needs, encryption solutions must maintain performance, ease-of-access, and an invisible impact on user workflows – all while restricting access to authorized users. Unified key management minimizes the complexity across heterogeneous encryption solutions, streamlining the management of the growing number of encryption keys.

Can your customer demonstrate that it maintains high performance and availability of user files while providing the highest level of protection?

SafeNet KeySecure delivers high performance and availability of user files through an easy-to-use, self-contained, hardened hardware solution that makes sure encrypted data is continuously secure and available to users.

The security appliance delivers robust enterprise key lifecycle management, and shares configuration setting in active-active mode to improve failover capabilities and resiliency in distributed environments.

- Protect sensitive corporate data while simultaneously delivering high performance and availability.

Business Case 6: Technology refresh of legacy key management solution

As technology advances, organizations that have long embraced data encryption as part of their security portfolio will be faced with product upgrades in order to maintain access to continued support. Customers with legacy solutions from NetApp and RSA have already received end-of-sale or end-of-life notifications, signaling that support will soon end. In addition, legacy encryption solutions may not be supported by the current operating systems, also signaling a need for a tech refresh.

End of support for legacy solutions can raise a flag for internal and external auditors, especially if those unsupported products are managing a function as critical as key management. Therefore, continued use of such products can complicate audits, adding time and cost to each audit cycle.

Does your organization have a plan to refresh its legacy key management solution with one that is state-of-the-art?

SafeNet KeySecure can easily refresh a legacy key management environment, as it is the industry’s first high-assurance, FIPS-validated, KMIP standards-based enterprise key management solution. With SafeNet KeySecure, customers can seamlessly upgrade legacy key management technology.

With SafeNet KeySecure, customers can manage encryption keys across a broad range of encryption solutions. As a result, your organization will be able to refresh its key management technology while leveraging existing security-related investments.

- Manage encryption keys across a broad range of encryption solutions.
- Refresh your management technology while leveraging existing security-related investments.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com
Follow Us: blog.gemalto.com/security

©Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. UC (EN)-Nov.15.2016 - Design: FR