

VaultCore Data Storage Use Case

» THE CHALLENGE

As necessity and demand for data center storage grows, so have client expectations that critical data remains securely encrypted, highly available, and well organized. As a result, data centers are tasked with taking proactive measures to secure their perimeter and infrastructure. Owners and operators must also ensure all hosted software applications adhere to industry standards, Security Best Practices, and their own enterprise security policies. Data at rest requires a key management system to meet these demands.

This complex mix of storage, encryption, and management requirements creates many challenges for securing data. Typically, these efforts are costly, limited by scale, require network downtime, and create multiple access points for control commands and reporting. All require more manpower, higher electrical capacity, and an increased footprint within the data center.

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."

Stéphane Nappo
Vice President Global Chief Information Security Officer
2018 Global CISO of the Year

» THE SOLUTION

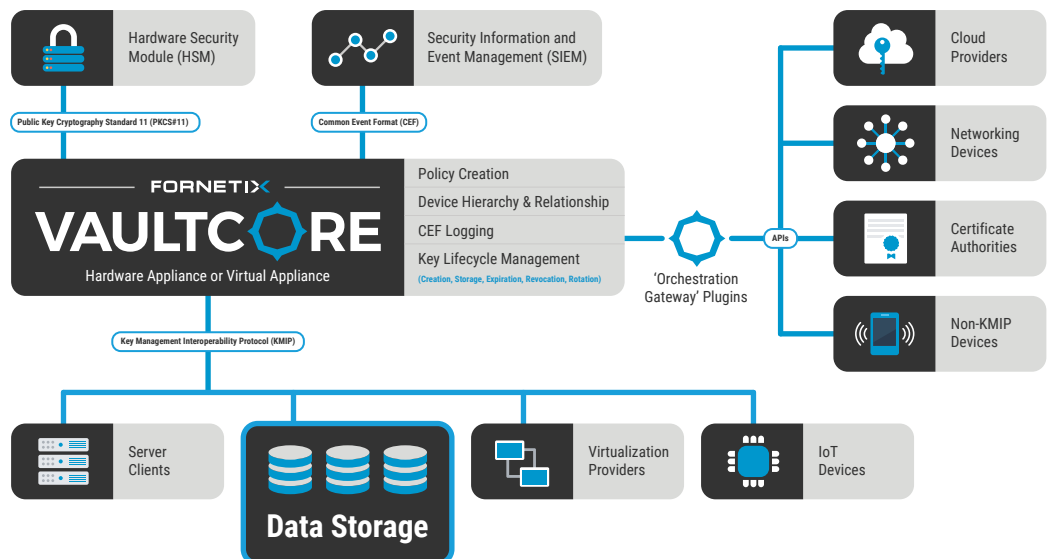
Fornetix recognizes the challenges data centers face when using multiple storage and data at rest encryption solutions. Limitations in integration, visibility, centralized control, access to reporting, and scalability can now be resolved by pairing any KMIP enabled storage product with Fornetix® VaultCore™. When paired together, they work cooperatively to create a superior storage/encryption solution that meets the growing security demands. This encryption key management solution alleviates data center struggles by:

1. Providing external key management for data at rest encryption to comply with Security Best Practices, including Separation of Duties
2. Offering simple KMIP integration that requires zero network downtime and no loss of keys
3. Allowing a centralized point for command and control with full access to audit reporting in one location



» HIGHLIGHT

Any KMIP-enabled storage product paired with Fornetix® VaultCore™ creates a powerful encryption solution for data centers. Together, they meet Security Best Practices through Separation of Duties ensuring the maximum protection available for sensitive data.



» 1. DATA AT REST ENCRYPTION – MEETING BEST PRACTICES

Many dedicated storage devices provide data protection through Self-Encrypting Drives (SEDs). However, where sensitive data is stored, Security Best Practices dictate that the data must be protected by a FIPS 140-2 Security Level 2 validated SED *and* for the encryption keys to be stored separately in an enterprise key management solution such as VaultCore.

Administrators strive to meet these best practices, including Separation of Duties. VaultCore creates Separation of Duties by splitting encryption keys from the data. This builds a safer environment, reduces human error, and offers protection with a FIPS 140-2 Level 2 validated solution (certification pending) that employs an HSM for a FIPS 140-2 Level 3 root of trust.

With policy and positional security, VaultCore ensures storage servers can only request the keys, certificates, and data intended for them while working to define permissions for the key administrators and key users. Through High Availability and Sync Services, VaultCore supports global synchronization of encryption keys across the entire enterprise. This ensures only the right encryption keys get to the right devices, at the right time, and under the right circumstances.

Any KMIP enabled storage product coupled with VaultCore creates a complete data at rest security solution for unifying and automating an organization's encryption controls. The pair works to securely create, protect, serve, control, and audit encryption keys, all while in compliance with Security Best Practices and ensuring Separation of Duties.

» 2. SIMPLE INTEGRATION ENSURES NO NETWORK DOWNTIME OR LOSS OF KEYS

VaultCore's simple workflow allows for swift integration with any KMIP enabled storage product. The VaultCore Team completes pre-condition requirements followed by these simple steps:

1. Create VaultCore as a new Client on the storage device
2. Generate PEM and Private Key PEM Client Credentials and upload into the storage platform interface
3. Setup each VaultCore appliance to High Availability Mode on the storage system
4. Turn on storage system's encryption feature

At this point, the storage device will connect to VaultCore and begin creating, activating, and retrieving key material to support all the data center's Self-Encrypting Drives. This simple out-of-the-box solution typically takes less than 10 minutes to deploy, requires no network downtime, and no loss of keys.

» 3. SCALABLE, STRAIGHTFORWARD, CENTRALIZED APPROACH TO ACCESS CONTROL AND REPORTING

In addition to a simple integration, VaultCore delivers the capacity to support over one hundred million keys – ample room for data center storage growth.

VaultCore's Mandatory Access Controls (MAC) provides a unique, hybrid Attribute-Based Access Control (ABAC) that utilizes both Role-Based Access Control (RBAC) and ABAC. This unique, proactive, centralized approach to data security allows organizations – at any point – to review and control who has access to keys *and* how the keys are being used. This is a perfect solution for securing large volumes of storage center devices.

VaultCore streamlines audit reporting with a centralized control panel accessed via a simple web interface. Administrators have clear visibility of all encrypted devices utilizing KMIP, and are provided signed, validated audit log information on key management and key consumption. These logs include who accessed the key, the event time, and the success or failure of the operation. The hassles of collecting access reports, locating client credentials, and organizing reporting from multiple locations become a thing of the past.



» OUR COMMITMENT TO STANDARDS

VaultCore leverages Key Management Interoperability Protocol (KMIP), Public Key Cryptography Standards #11 (PKCS#11), and Common Event Format (CEF) as standards-based approaches for key management, command and control, hardware security module integration, and security incident event management (SIEM) integration. KMIP and PKCS#11 are technical specifications defined by the Organization for Advancement of Structured Information Standards (OASIS). Both KMIP and PKCS#11 are directly associated with standards provided by National Institute of Standards and Technology (NIST).


SUMMARY


Securing data has become exponentially complex as companies continue to migrate all or part of their data into virtual data centers or cloud environments. As a result, security and risk management leaders struggle to support secure access to encrypted data while also meeting data residency, privacy, crypto-agility, compliance, and business needs. Fernetix VaultCore provides a simple solution that works with an organization's existing investments – whether the data is in the cloud, hyperconverged, or on-prem environments. Through a simple KMIP connection, VaultCore can provide enterprise level key management to fully protect sensitive data. Remember, any security strategy that does not include a centralized encryption key management solution is putting data at risk.

ABOUT FORNETIX

Fernetix, a pioneer in encryption key management, understands that securing data in today's complex environment can seem like an impossible task. VaultCore™ by Fernetix is a patented solution designed to simplify the encryption key management process across the entire enterprise. VaultCore provides a centralized system to automate the full key lifecycle and enable compliance policy enforcement. Scalable to over one hundred million keys for data storage environments including multi-cloud and hyperconverged infrastructures, VaultCore allows you to leverage existing technology investments and take complete ownership of your keys ensuring that critical data is safeguarded no matter where it resides.

FREE TRIAL: www.fornetix.com/freetrial
FREE DEMO: www.fornetix.com/demo

 **1-844-539-6724**

 **5123 Pegasus Court, Suite X
Frederick, MD 21704**