FORNETIX

The CISO's Guide to Understanding Encryption Key Management

Why Successful Security Strategies Must Go Beyond Just "Checking the Box" for Data Encryption

Chuck White
Chief Technology Officer

> *CISOs, CTOs, and others tasked with implementing enterprise security strategy are faced with the challenge of securing data across multiple environments — cloud, edge, IoT, datacenters, and even newer concepts like containers, mesh networks, and Dev Ops capabilities.*

Regulations and standards such as GDPR, Common Criteria, CMMC, CCPA, Shield Act, and FIPS all provide encryption guidance and validation. They also drive the commercial demand that encryption capabilities be embedded in most new technologies. However, ongoing data breaches across the globe continue to prove that encryption alone is not enough to reliably secure data.

The consensus from experts indicates encryption is the simplest and most effective means of securing data available by making data illegible to those without the correct deciphering key material. However, the explosive growth in data generation, the variety of new technologies, and the scope of enterprise endpoints has created more key material than can adequately and successfully be managed without a dedicated key management solution. Decision makers fail to realize that multiple encryption points create multiple weak links in their security strategy and become easy targets for bad actors.

Adding This One Security Best Practice May Be What Saves Your Data

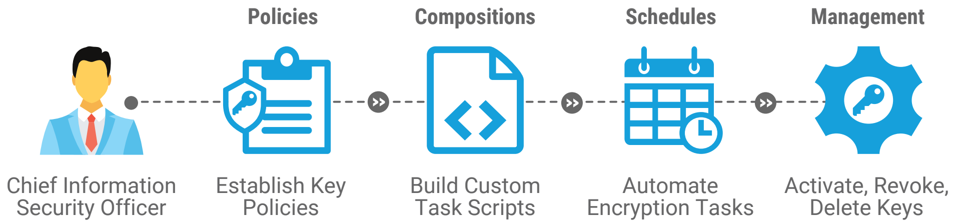
Historically, key management has been viewed as a daunting task. It either becomes spread across too many lines of responsibilities or gets overlooked completely in the security strategy and budget planning process. Yet security best practices make clear the need to separate encryption keys from the device where the data resides — an effective approach that requires a dedicated key management solution.

Key management works by enforcing separation of key material from the data source and further restricting access to the keys. It provides an independent, reliable source for delivering key material over a secure channel. Incorporating a key management solution renders most any breach of any duration inconsequential and leaves the attackers with nothing more than gibberish instead of your valuable data.

Recent innovations in key management technologies like Fornetix® VaultCore™ have made the once-difficult task of incorporating key management simple, affordable, and effective. It is time to end the bad habit of casually "checking the box" for encryption and instead begin to fully protect data by properly managing the encryption keys in a modern, automated, and policy-driven fashion.

> *"A court order is as ineffective at accessing encrypted data as a nuclear weapon.* ***Only the keyholder*** *can access that data, and that power resides exclusively with them."*
>
> **— Jacob Riggs**
>
> British crypto-anarchist, ethical hacker, and security expert

Effective key management becomes an important exercise in utilizing industry standards like the Key Management Interoperability Protocol (KMIP). The combination of encryption, KMIP, and a dedicated encryption key manager is arguably the most complete data security solution available to every enterprise, in any industry.


Policies
Compositions
Schedules
Management
Chief Information Security Officer
Establish Key Policies
Build Custom Task Scripts
Automate Encryption Tasks
Activate, Revoke, Delete Keys

Key lifecycle management workflow as part of Fornetix VaultCore.

Enterprise Policy and Automation for Encryption Keys

Having keys deployed in a broad range of environments (cloud, network, storage devices – keys everywhere) and being managed by different groups in your organization with varying levels of compliance quickly becomes problematic. The more a set of keys are used, the higher the odds an attacker will find a way to compromise them. Using a single set of keys across a highly dispersed environment creates opportunity for successful attacks.

The solution is to utilize an encryption key management system and create policy (different rules for keys based on the sensitivity of the data and/or the risk environment) and automate these policies based on your understanding of the following four points:

1. Unique Keys at a Granular Level

Unique keys should be employed with as much granularity as the enterprise can manage. Is it better to encrypt an enterprise or group with one key set? Or, does it make sense to have a more granular approach based on system components, classification, or location? Or, is a file or object-based approach more logical? Manually intensive key management techniques of the past were limited because highly granular data encryption schemes weren't feasible. The use of a single, long-lasting key set for large amounts of data suffered from a "keys to the kingdom" vulnerability. Simply put, if someone could obtain the key to the front door, they essentially held the key to every door in the house and could access anything they wished.

New tools that are automated and policy-based can greatly improve the segmentation and granularity of data encryption in the modern enterprise. VaultCore's Attribute Based Access Control Policy (ABAC), with automation through Compositions and Schedules provides a standards-based approach for implementing policy. This makes it possible to associate unique key material at the most granular level.

2. Key Distribution

Key distribution has also been a difficult problem in the past. Specifically, the ability to deliver cryptographic objects (certificates, key pairs, symmetric keys) used to build trust quickly and securely throughout the enterprise. Most of this difficulty can now be alleviated due to the wide adoption of standards such as KMIP and the use of storage and authentication techniques for key protection communicating over TLS and other encapsulated key delivery mechanisms.

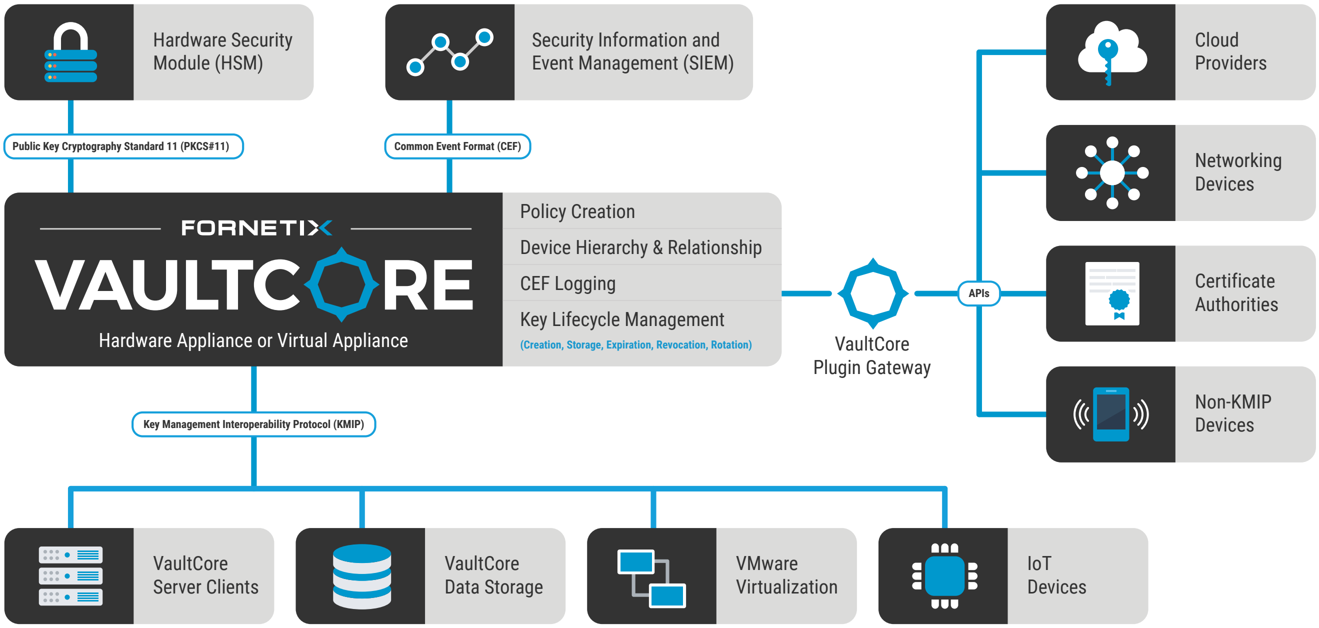
This powerful control and distribution of key material provides trust in secure network connections, validates trust during encrypted traffic inspection, and can remove trust when an attacker is detected through revocation and rekeying of network segments.

3. Secure Key Storage

Key storage was once an intractable problem. Because keys are digital data, they are commonly stored in places that were vulnerable to attack themselves. Fortunately, for most applications in the modern world, this problem has almost completely disappeared thanks to the rise and relative ubiquity of Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs), and other dedicated cryptographic hardware components. VaultCore is "secure by design" with sufficient storage capabilities but can also be augmented further by integrating HSM technologies to create additional secure enclaves for key storage at FIPS 140-2 Level 3.

4. Key Lifecycle Management

The more keys that are used, the higher the odds an attacker will find a way to compromise them. Just like passwords on our computers, encryption keys must be rotated as frequently as possible. The rotation of keys increases the complexity of key management exponentially and greatly reduces any negative consequences from an interior or exterior attack. Key lifecycle management provides the ability to store and control all encryption keys across all environments (whether on-premise storage, virtualized, or cloud), strengthens data security, and greatly decreases the probability of a successful attack.


Hardware Security Module (HSM)
Security Information and Event Management (SIEM)
Public Key Cryptography Standard 11 (PKCS#11)
Common Event Format (CEF)
FORNETIX
VAULTCORE
Hardware Appliance or Virtual Appliance
Policy Creation
Device Hierarchy & Relationship
CEF Logging
Key Lifecycle Management
(Creation, Storage, Expiration, Revocation, Rotation)
VaultCore Plugin Gateway
APIs
Cloud Providers
Networking Devices
Certificate Authorities
Non-KMIP Devices
Key Management Interoperability Protocol (KMIP)
VaultCore Server Clients
VaultCore Data Storage
VMware Virtualization
IoT Devices

SCENARIO: Enterprise Key Management at Work

Let us consider a scenario in which your organization, a general contractor utilizing at least one subcontractor, implements a production chain security strategy powered by encryption key management to protect against a next-generation attack:

You implement standards-based encryption key management and provide a common software platform to your supply chain partners, allowing for data-in-motion and data-at-rest encryption with short-life periodic key rotations. The key management system is tied to identity services, applications, and storage services used in the development of your product. This enables the release of encryption keys to process information for engineers, testers, machinists, procurement specialists, facility security officers, program managers, and others. Your organization now has insight into when keys are created and requested and you control key rotations as governed by your organization's and your subcontractor's various policies, standards, and guidelines.

With the above scenario in mind, even when an attack breaches the perimeter of one of your subcontractors, the breach attempts to access content that requires key material centrally controlled by you.

Assume the attacker obtains a credential that allows access to your data file system. After grabbing files, they hit their first roadblock: The files are encrypted, and they can't decipher the content of the files because they don't have the keys necessary to decrypt the information. Furthermore, even if it is an insider attack, the drives remain encrypted, rendering the content useless.

This means the attacker now must pivot to a new attack vector and attempt to request that the key manager release the appropriate keys associated with the content.

This requires access to the key manager which is always under your direct control and initiates a Mutual TLS request to the key manager. This leads to yet another pivot to attempt accessing client TLS credentials, which may be stored on smart cards or other physical tokens rendering them completely inaccessible.

Each pivot executed by the attacker increases the complexity of the attack. It increases the risk of discovery and counterattacks by requiring simultaneous access to more systems which are even more secure than the last. The situation becomes critical for the attacker as the key manager reports requests for key material to monitoring systems such as Security Information and Event Management (SIEM) providers.

When your organization notices the unusual activity from one of your subcontractors' networks, you may temporarily or permanently disable access to the relevant encryption keys so that the data remains secure. It may also provide the time needed to apprehend the attacker. This ultimately gives the attacker a harsh choice: Leave with the unreadable, useless data or risk discovery while trying to retrieve keys. The "easy" target is now virtually unassailable.

Summary

Encryption key management provides a consistent platform for extending the reach and power of encryption and reporting information based on encryption use. Addressing the overall security of the enterprise (or supply and distribution chain) with automated, policy-based key management tools reduces the impact of even the most complex network security breach.

In conclusion, it is readily apparent that a protection-centric approach, bolstered by a modern encryption key management system, is the most cost-effective and simple solution for truly protecting data.

How Fornetix® and VaultCore™ Can Help

Fornetix's VaultCore is helping organizations across the globe unleash the full potential of encryption by conquering the key management challenge and working to secure some of the world's most vital secrets by automating the key lifecycle from enterprise to edge with groundbreaking precision, speed, and accuracy.

As global use of encryption rapidly expands, be prepared for the future with VaultCore's unmatched scalability. Fornetix's commitment to standards-based interoperability ensures your existing investments in encryption can be utilized and will continue to integrate seamlessly as your organization grows. Policy-driven automation of the key rotation lifecycle reduces human error and empowers your organization to remain secure while avoiding the costly expenses associated with a data breach.

If you are ready to add easily managed and fully automated encryption key management to your security checklist to ensure your data remains secure, we'd love to hear from you. Please call 1-844-539-6724 or visit www.fornetix.com for more information.

Find Out More About VaultCore

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

☎ **1-844-539-6724**

5728 Industry Lane
Frederick, MD 21704