

# Unleash Encryption's Full Potential By Conquering Key Management

**VaultCore™ by Foretix® is a hyper-scalable cybersecurity solution that automates cryptography for dynamic asset protection.**

FORNETIX  
**VAULTCORE**



## Scalability

Store hundreds of millions of keys – orders of magnitude above existing tools



## Automation

Schedule and execute cryptographic operations on millions of keys at once



## Compatibility

Seamlessly integrate with legacy, existing, and future technology investments



## Compliance

Enable full reporting and auditing for today's ever-increasing regulations

**AS CRIPPLING DATA BREACHES BECOME AN ALMOST DAILY OCCURRENCE, IT'S CRITICAL FOR INFORMATION REQUIRING ENCRYPTION TO BE PROTECTED IN CREATION, IN USE, IN TRANSIT, AND AT REST.**

The methods of deploying and managing encryption keys on various devices and systems have traditionally taken a bottom-up approach. This disparate flow of control leads to a lack of fully-utilized encryption, breakdowns on networks that require encryption, and inadequate encryption key management.

The result is multiple systems or manual processes being utilized within the same organization to create and distribute encryption keys to isolated systems that may utilize an assortment of encryption key managers. The level of encryption and the adoption of methods for deploying encryption keys varies across industries based on need, the technologies in use, and the types of devices utilizing encryption.

Foretix recognizes the value and the necessity for businesses, organizations, and service providers to protect critical information, enable secure business transactions, and deliver trusted services to ensure the safety and confidentiality of their customers and business partners.

Best practices for enterprise systems management are top-down and centralized methods. While there are many different products and solutions available today that create encryption keys for organizations, the challenge becomes finding an approach that provides practical and affordable scalability.

Previously, there have been no options to easily manage, distribute, and federate encryption keys combined with the necessary conformance to organizational policies. Existing methodologies are often proprietary and device-specific. This approach does not support centralized control of enterprise applications, communications, and infrastructure.

**Fortunately, there's now a modern, scalable solution...**

## Centralize Key Management With VaultCore by Foretix

VaultCore (VC) solves these challenges by focusing on encryption key management, distribution, and federation. VaultCore helps coordinate encryption key lifecycle activities with applications, communications, and infrastructure management.

By coordinating these resources with the rest of the enterprise, the monitoring of key utilization becomes aligned with other components of policy, enterprise monitoring, and management functions. This makes encryption more accessible and operationalizes it as a service. Key management then becomes an integral component of mission management, placing encryption in line with other aspects of secure data and communication environments.

Encryption needs to be managed from the top down to ensure that organizational policy is followed and keys are securely generated and distributed within the organization's sphere of control. To achieve this goal, a standard method is needed to organize the communication of key management operations into a data contract so that management applications can control enrolled devices and those devices can receive and request key material in an automated fashion.



## Commitment to Standards: A Path Towards the Future

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).

As things like cryptography change over time, commitment to standards becomes a gate to transition, giving VaultCore users the ability to address change on enterprise scale with security and efficiency.

VaultCore functionality is grounded in providing enterprise-level interoperability, extensibility, scalability, and security. Emphasis on these qualities provides a framework for data-centric security that benefits an organization by aligning controls with the flow of information in the enterprise. By aligning encryption-based security controls, authorization definition, and management with an organization's business, it is possible to enforce the idea that "need-to-know" must follow a strict process.

When considering your organization's data-centric security needs, the emphasis on interoperability, extensibility, scalability, and security makes VaultCore a solution that allows you to unleash encryption's full potential.

## Interoperability

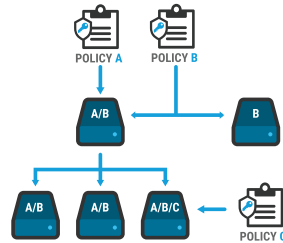
Foretix technology is driven by the motto "in standards we trust." This provides a strong foundation for extensibility and defines boundaries that impact how much VaultCore can grow (scalability) and how VaultCore provides protection to outside systems (security). VaultCore's policy engine is a decision point for cryptographic operations using the language of known standards as the baseline for policy definition.

### MAJOR FEATURES OF VAULTCORE INTEROPERABILITY

- Fully-compliant KMIP interface: KMIP 1.0–1.4
- KMIP services via TTLV, HTTPS, JSON, and XML
- CEF Logging to support rapid SIEM integration
- Ability to forward KMIP operations to other KMIP-compliant key managers
- PKCS#11 Interface for integrating HSMs to protect VC key store
- Encrypt and manage Virtual Machines via interoperability with VMware vSphere and vSAN

## Extensibility

The ability to expand capability while maintaining a highly interoperable and secure environment is a key feature of VaultCore. This feature includes integration of key management with other systems by translating protocol (NETCONF, F5, Microsoft Cryptographic Next Generation APIs) to support consolidation of user interfaces and supporting a dynamic, adaptive network defense inclusive of data-at-rest and data-in-motion security.



### MAJOR FEATURES OF VAULTCORE EXTENSIBILITY

- RESTful Services to integrate VaultCore with existing enterprise services
- VaultCore custom scripting to automate complex encryption and key management operations
- VaultCore scheduling to run automation scripts
- Windows and Linux Orchestrators for KMIP-driven protocol translation of Microsoft Services, Certificate Authorities, NETCONF, and other protocols
- VaultCore Policy for defining authorization rules outside of key management operations

## Scalability

VaultCore has the capacity to support hundreds of millions of keys while supporting mobile adhoc networking, tactical communications, and file or object-level encryption. VaultCore Compositions and Jobs give organizations the ability to define complex key management operations in bulk. This allows customers to orchestrate key management, encryption, network security, and business systems with the assurance the keys used are safe and will not be lost.

### MAJOR FEATURES OF VAULTCORE SCALABILITY

- VaultCore Data Store is designed to maintain a repository of hundreds of millions of keys
- High Availability and full backups using encrypted replication with geo-separated VC appliances to ensure you never lose keys
- Ability to integrate embedded or network-based Hardware Security Modules (HSMs) to protect key stores while in a high availability configuration
- Pricing Structure that encourages – not penalizes – organizations to utilize the greatest number of keys possible

## Security

VaultCore enables mandatory access controls through positional security and policy. Discretionary access controls through KMIP grouping allows the VaultCore server to provide secure key lifecycle from the data center to the tactical edge.

### MAJOR FEATURES OF VAULTCORE SECURITY

- VaultCore Appliances run with SELinux in enforcing mode to protect running processes and enforce strict behaviors
- User Roles for key management and policy management allowing for separation of controls between key management and policy management
- VaultCore Policy Engine enables defining cryptographic decision point services for IoT-scale two-person integrity
- Mutual TLS Connections for distribution of keys, management objects, effective policy, and orchestration instructions
- Positional Security enforces mandatory access controls based on where a given client connection is associated in VC hierarchy
- Every VC appliance uses FIPS-certified Self-Encrypting Drives to ensure data security if a drive is physically removed
- Hardware Security Modules available to protect key stores in stand-alone and high-availability configurations
- The entirety of VaultCore is owned, designed, and assembled in the U.S. to comply with the Buy American Act



VCH260 (1U)

VCH760 (2U)

VCH460 (1U)

## Deployment Options

From small businesses to global enterprises with massive IoT infrastructure, there’s a VaultCore deployment solution that perfectly meets the unique needs of your organization. VaultCore is designed to grow with you as your encryption usage increases. A small deployment of software-based VaultCore appliances can rapidly and seamlessly be upgraded to the industry-leading horsepower and capacity of our rack-mounted hardware appliances. Additionally, the VCH760HSM embeds a FIPS 140-2 Level 3 certified Hardware Security Module (HSM) for added security.

## Hardware Appliances

### POWER SUPPLY

VCH260	Single fixed
VCH460	Dual hot-swap
VCH760	Dual hot-swap

### INTERFACES

VCH260	(2) 1GB RJ45
VCH460	(6) 1GB RJ45
VCH760	(6) 1GB RJ45 + (2) 10GB SFP

Graphical User Interface (GUI)  
 KMIP API  
 Command Line Interface  
 VaultCore Client, Agent, and RESTful Services  
 HSM (PKCS #11)

### KEY CAPACITY

VCH260	500,000
VCH460 / 460H	10,000,000
VCH760 / 760H	100,000,000+

### CERTIFICATIONS AND INTEROPERABILITY

- VCH260** — FIPS 140-2 Level 2 Compliant; FIPS 140-3 Certification Pending
- VCH460** — FIPS 140-2 Level 2 Compliant; FIPS 140-3 Certification Pending
- VCH460H** — FIPS 140-2 Level 2 Compliant with FIPS 140-2 Level 3 Certified HSM; FIPS 140-3 Certification Pending
- VCH760** — FIPS 140-2 Level 2 Compliant; FIPS 140-3 Certification Pending
- VCH760H** — FIPS 140-2 Level 2 Compliant with FIPS 140-2 Level 3 Certified HSM; FIPS 140-3 Certification Pending

KMIP 1.0, 1.1, 1.2, 1.3, 1.4, and 2.0 compliant

### SCALABILITY AND FAILOVER

Fully distributable  
 Clustering support  
 High availability / zero failover interruption  
 Backup / restore process

## Virtual Appliances

### VIRTUAL STORAGE

VCV160	20GB
VCV260	32GB
VCV460	64GB
VCV760	96GB

### VIRTUAL CPU / RAM

<b>All Models</b>	2 CPU / 4GB RAM
-------------------	-----------------

### KEY CAPACITY

VCV160	125,000
VCV260	250,000
VCV460	500,000
VCV760	1,000,000

### CERTIFICATIONS AND INTEROPERABILITY

FIPS 140-2 Level 1 compliant  
 KMIP 1.0, 1.1, 1.2, 1.3, 1.4, and 2.0 compliant

### SCALABILITY AND FAILOVER

Fully distributable  
 Clustering support  
 High availability / zero failover interruption  
 Backup / restore process

### INTERFACES

Graphical User Interface (GUI)  
 KMIP API  
 Command Line Interface  
 VaultCore Client, Agent, and RESTful Services  
 HSM (PKCS #11)