Fornetix and VMware

Fornetix® VaultCore™ Brings Unified and Scalable Encryption Key Management to Virtual Environments

» HIGHLIGHTS

Securing virtual environments is a priority. Portability, versatility, efficiency, and cost effectiveness are just a few of the advantages of moving to virtualized environments. Virtualization allows organizations to shift from data centers full of equipment down to a just a few servers. A smaller footprint means less power consumption, lowered cost of ownership, and less overhead. Too often though, enterprises neglect security when it comes to implementing virtualization. VMware makes it possible for organizations to easily encrypt and manage virtual machines (VMs) in minutes.

» CONTACT INFO

Ready to secure your virtual environment? Request access to a complimentary version of Fornetix VaultCore and experience how easy it is to implement a key management system that works seamlessly in VMware production environments. Visit **www.fornetix.com** to learn more.

John W. Puente
VP of Commerical Sales
North and Latin America
jpuente@fornetix.com
(305) 298-6600

A Powerful and Smart Security Solution

- **Easily Meets Compliance Requirements**
- **Accelerates Deployment of Key Management Technology**
- **Maximizes ROI by Optimizing VMware's Encryption Capabilities**
- **Establishes Root of Trust for VMware Cloud Foundations**
- **Easily Secures Your Virtual Machines**
- **Utilizes Built-In Security Features Like TPM, Secure Boot, System Lockdown, FIPS Encryption, and Tamper Evident Chassis**
- **Designed, Engineered, and Manufactured by Trusted U.S. Supplier with Secure Supply Chain Protection**
- **Scales for Entire Enterprise — from the Datacenter, to the Edge, to the Cloud**
- **vTPM Emulates Physical TPM Capabilites and Protects Sensitive VM Data with VaultCore AES 256-XTS Key Material from VaultCore**

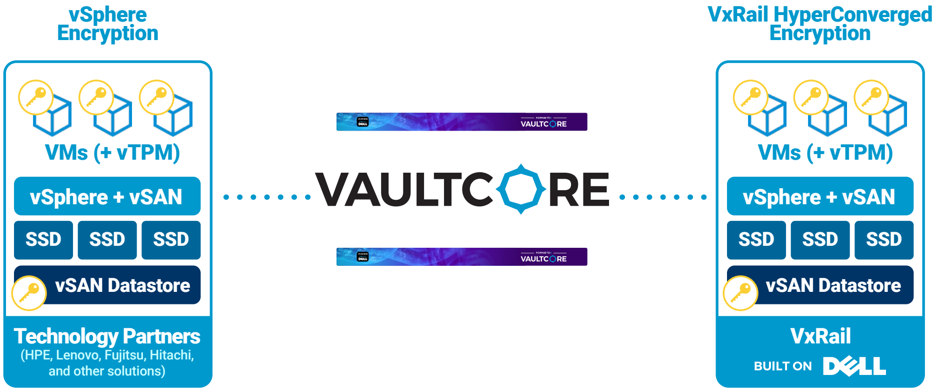
» HOW IT WORKS

Implementing Fornetix VaultCore with VMware is a seamless and secure process utilizing KMIP:

1. When a new or existing virtual machine is encrypted, the VMware host generates an internal AES key that is used to encrypt the virtualmachine.
2. The vCenter server then requests a new AES key from VaultCore that is used to encrypt the internally generated key.
3. The key from VaultCore used to encrypt the internal key is not saved anywhere in the VMware environment; only the UUID is stored.

» USE CASES

- **Encrypting Virtual Machines and the Data Within** — VMware requires the use of an approved KMS to enable encryption. VaultCore for VMware provides a lite and seamless solution.
- **Securing Your VxRail Hyperconverged Infrastructure** — Solve VMware encryption challenges with a simple, turnkey add-on appliance for any customer deploying VMware Cloud Foundations on VxRail or vSAN Ready Nodes.


vSphere Encryption
VMs (+ vTPM)
vSphere + vSAN
SSD
SSD
SSD
vSAN Datastore
Technology Partners
(HPE, Lenovo, Fujitsu, Hitachi, and other solutions)
VAULTCORE
VxRail HyperConverged Encryption
VMs (+ vTPM)
vSphere + vSAN
SSD
SSD
SSD
vSAN Datastore
VxRail
BUILT ON DELL