SUPPORTING VMWARE ENCRYPTION WITH FORNETIX KEY ORCHESTRATION

Bringing Unified and Scalable Encryption Key Management to Virtual Machines

"With the combined Fornetix and VMware integration, encrypting our virtual machines has been seamless. It empowers our organization to protect our clients' data via a transparent security layer that can be deployed with minimal disruption and, critically, requires near-zero maintenance allowing us to deliver exceptional reliability and scale on-demand."

LEE ADAMS
MANAGING DIRECTOR
CANTARUS

VMWARE vSPHERE 6.5 AND 6.7

VMware vSphere, the industry-leading virtualization and cloud platform, is the efficient and secure platform for hybrid clouds, accelerating digital transformation by delivering simple and efficient management at scale, comprehensive built-in security, a universal application platform, and seamless hybrid cloud experience.

Make Securing Virtual Environments a Priority

Portability, versatility, efficiency, and cost effectiveness—these 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. Now, with the release of VMware vSphere® 6.5, VMware makes it possible for organizations to easily encrypt and manage virtual machines (VMs) in minutes.

Flexibility Without Compromising Security

Fornetix Key Orchestration™ can centrally store and manage the lifecycle of hundreds of millions of encryption keys, maximizing ROI on VMware encryption. Volume and location of encryption keys and certificates, along with the ongoing efforts it takes to manage them, are no longer inhibitors to increased usage and functionality.

To ensure that keys can be managed without negative operational impact, VMware has taken the burden of disk image encryption out of the VM and has located it in the hypervisor, "beneath" the virtual machine. To better protect privileged access for encrypted images, VM keys do not persist in VMware vCenter®. With Fornetix Key Orchestration for VMware, key management functions are performed via a seamless and secure process. Using the industry standard Key Management Interoperability Protocol (KMIP). This allows for simple integration and extends Key Orchestration's ability to provide hardware solutions validated up to FIPS 140-2 level 3 and a FIPS 140-2 compliant virtual solution.

A Powerful and Smart Security Solution

Together, VMware and Fornetix Key Orchestration create a powerful and effective solution that:

- Meets compliance requirements
- Accelerates deployment of key management technology
- Optimizes VMware's encryption capabilities, maximizing ROI
- Adds VMware to an enterprise wide encryption strategy for key management unification

vmware® | FORNETIX®

FORNETIX KEY ORCHESTRATION

Fornetix Key Orchestration is an advanced encryption key management ecosystem that automates the key lifecycle across the entire enterprise with groundbreaking precision and speed. Key Management Interoperability Protocol (KMIP) allows for simple integration and extends Key Orchestration's ability to provide hardware solutions validated up to FIPS 140-2 level 3 and a FIPS 140-2 compliant virtual solution.

FORNETIX COMPANY DESCRIPTION

Fornetix empowers organizations to build a data security strategy with encryption as the strong foundation. Fornetix Key Orchestration enables enterprises to safeguard sensitive information with a system backed by granular policy tools, user access controls, and powerful automation.

CASE STUDY

Cantarus, an MSP based in the UK, was challenged to meet the impending deadline for GDPR by protecting client data and internal data within a virtual environment. The solution was to implement a KMIP integration between Fornetix Key Orchestration and VMware virtual machines providing encryption key management through the hypervisor. The result is an efficient, reliable, and easily implemented data-at-rest encryption that is transparent to operating systems, applications and storage while maintaining future scalability.

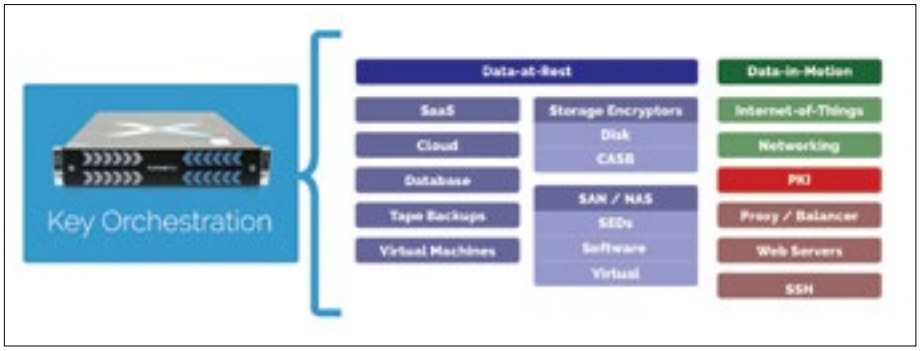

Figure 1. Fornetix Key Orchestration enables a unification strategy, which allows for centralized governance and control of all encryption keys throughout the enterprise.

Securing VMs in Five Minutes

VMware and Fornetix Key Orchestration work together to enable easy encryption of VMs with just a few clicks from the management console. vSphere virtual machines sitting on the disk (data-at-rest) or moving between hosts (data-in-motion with VMware vSphere vMotion®) are now able to be encrypted. vSphere allows you to encrypt the home folder (containing sensitive configuration information) and the virtual machine disk (VMDK file) with the same key or separate keys with ease. Encryption keys can be stored in a virtual appliance, or in a physical appliance with the ability to achieve up to FIPS 140-2 level 3 security controls.

How It Works

Implementing Fornetix Key Orchestration with VMware vSphere 6.5 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 virtual machine.
2. The vCenter server then requests a new AES key from Key Orchestration that is used to encrypt the internally generated key.
3. The key from Key Orchestration used to encrypt the internal key is not saved anywhere in the VMware environment; only the UUID is stored.

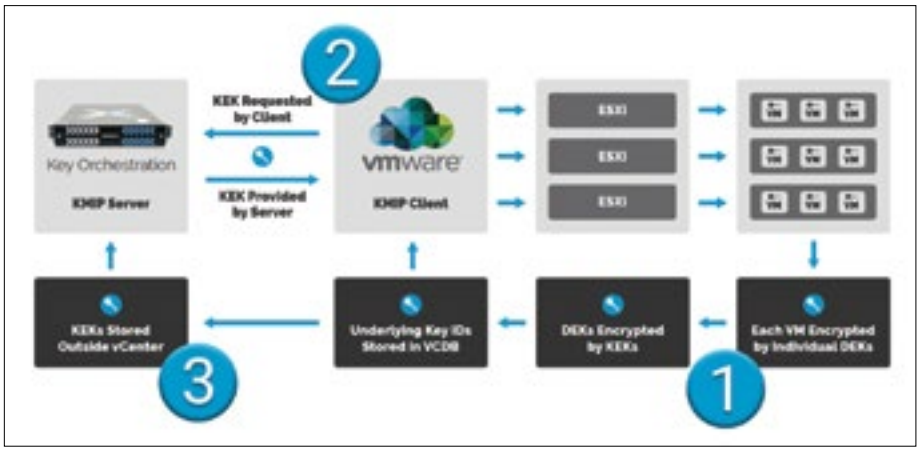

Figure 2. The integration between Key Orchestration and vSphere 6.5 is made possible through KMIP, and the workflow is illustrated in the above figure.

SEE OUR SOLUTIONS IN THE VMWARE SOLUTION EXCHANGE
https://marketplace.vmware.com/vsx/solutions/fornetix-key-orchestration

Maintaining security posture is assured, even when moving virtual machines from one encrypted host to another. By utilizing vMotion encryption, all relevant hosts and the virtual machine are secured.

Not using an encrypted virtual machine? vMotion encryption can be used on unencrypted virtual machines as well. Additionally, because all encryption operation happens outside of the virtual machine at the hypervisor level, the guest operating system or the data on the VMDK does not constrain these capabilities; all encryption of the virtual machine is OS agnostic.

Ready to Secure Your Virtual Environment?

Request access to a complimentary version of Fornetix Key Orchestration 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.

vmware® | FORNETIX®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com