

VMware VMLive

Encrypting sensitive data in VMware
Clouds with Fortanix Self-Defending KMS

April 2020

Agenda

VMware Cloud Director 10.1 update

VMware Cloud Director Encryption feature

Fortanix overview

Solution use cases for Cloud Providers

Questions

VMware Cloud Director

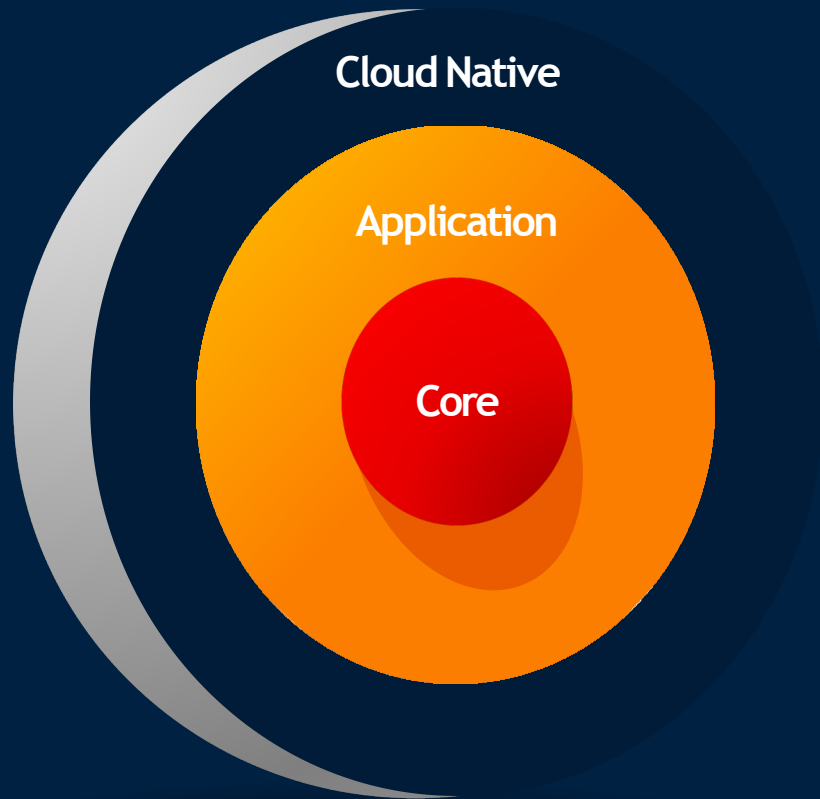
10.1 update

VMware Cloud Director

From edge-of-life to the World's Leading Cloud Provider Platform



Main themes for VCD 10.1



- CSE2.6 update
- Terraform 2.7 update
- Bitnami community catalog
- App Launchpad
- TenantApp 2.4 update
- NSXT enhancements
- NSX-T Migration Tool
- Object Storage Extension 1.5 update
- Encryption Service
- Tenant and Admin UI improvements

Encryption Service



Third Party Key Management Server



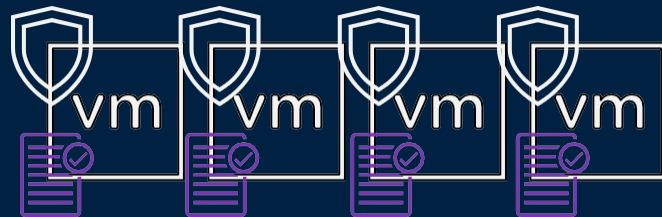
vSphere

vCenter Server

Managed VM key IDs



ESXi



Key Management Server - vCenter Server requests keys from an external KMS. The KMS generates and stores the keys, and passes them to vCenter Server for distribution.

vCenter Server - vCenter Server obtains keys from the KMS and pushes them to the ESXi hosts.

ESXi Hosts - vCenter Server pushes keys to an ESXi host when the host needs a key. This key is stored in memory of esxi host.

Virtual Machine Keys - Two types of keys are used for VM encryption:

- Data encryption key (DEK)
- Key encryption key (KEK)

3 new offerings for Cloud Provider

VM Encryption on Storage Policies of an Organization Virtual Data Center using vSphere Encryption policy covering VM, Disks & other Files

Provider Default Secure Cloud

Cloud Provider encrypts the VMs in their cloud environment in order to satisfy their own internal security compliance requirements.

All Tenants VMs / vApps are encrypted

Provider Managed VM Encryption

Tenants being able to enable and disable encryption on their VMs using Storage Profiles

Tenants rely on their Cloud Provider to manage their encryption keys

Cloud Provider needs a KMS solution to manage customers

Tenant Managed Dedicated vCenter VM Encryption

dedicated vCenter managing and accessing as an IaaS Virtual Datacenter through the vCD Tenant Portal

Tenant is able to supply, own and manage their own encryption certificates and KMS that is associated with their dedicated vCenter

Configure Encryption Storage Policy in vCenter

Import the Encryption SP into VCD PVDC

Import the Encryption SP into VCD orgVDC

The screenshot shows the vSphere Client interface for configuring VM Storage Policies. The left sidebar lists 'Policies and Profiles' with 'VM Storage Policies' selected. The main pane shows a list of policies: Development, Host-local FPMem Default Storage Policy, VM Encryption Policy (highlighted), vSAN Default Storage Policy, and VVol No Requirements Policy. Below the list, the 'Rules' tab is active, showing details for the 'VM Encryption Policy'.

Rules	VM Compliance	VM Template	Storage Compatibility
General			
Name			VM Encryption Policy
Description			Sample storage policy for VMware's VM and virtual disk encryption
Common rules			
Encryption > default encryption properties			
Name			Default encryption properties
Description			Storage policy component for VM and virtual disk encryption
Provider			VMware VM Encryption
Allow I/O filters before encryption			False

The screenshot shows the vCenter interface for a VDC named 'vc1-TestbedCluster-17:07:43'. The 'Storage Policies' section is expanded, showing a table of policies available in the VDC.

	Name	Enabled	Used
<input type="radio"/>	* (Any)	<input checked="" type="checkbox"/>	0.68%
<input type="radio"/>	> Development	<input checked="" type="checkbox"/>	0.15%
<input type="radio"/>	> VM Encryption Policy	<input checked="" type="checkbox"/>	0.68%

Capabilities: VSphere/Encryption

The screenshot shows the vCenter interface for an organization VDC named 'dev-vdc'. The 'Storage Policies' section is expanded, showing a table of policies available in the orgVDC.

	Storage Policy	State
<input type="radio"/>	> VM Encryption Policy	Enabled
<input type="radio"/>	> Development	Enabled
<input type="radio"/>	* (Any)	Enabled

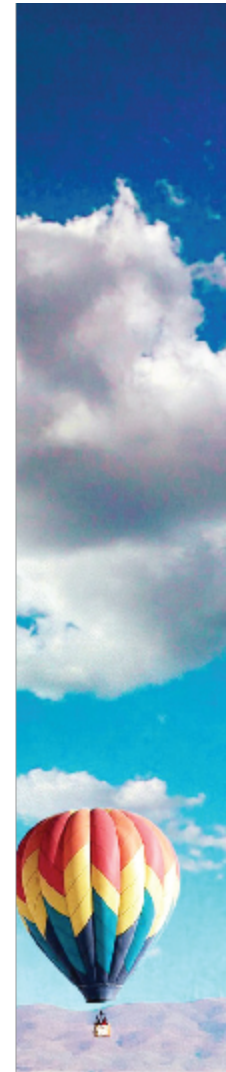
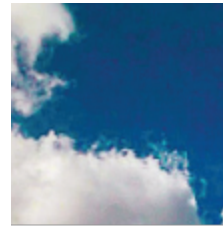
Then apply against VM

New Data Security Services Opportunities for Cloud Providers

April 16, 2020

VMLive

 **Fortanix**[®]  **vmware**[®]



Fortanix Self-Defending KMS for Cloud Partners

Presenters:

- Ambuj Kumar, CEO & Co-Founder
- Patrick Conte, VP of Business Development

Discussion Topics:

1. Fortanix – Cybersecurity Solutions for Cloud Providers
2. New Data Security Services Revenue Opportunities
3. Enabling New Multi-tenant Security Services
4. Working Together

The Challenges of Cloud-Scale Data Security

Cloud Application Complexity



75%

of Enterprise workloads
on public / private cloud

Source: IDC Data Age 2025 Study

Fortanix confidential. All rights reserved.

Privacy and Regulations



71%

of Cloud Data
is sensitive

Source: Oracle and KPMG Cloud Threat Report 2019

Skills Gap



1.5M

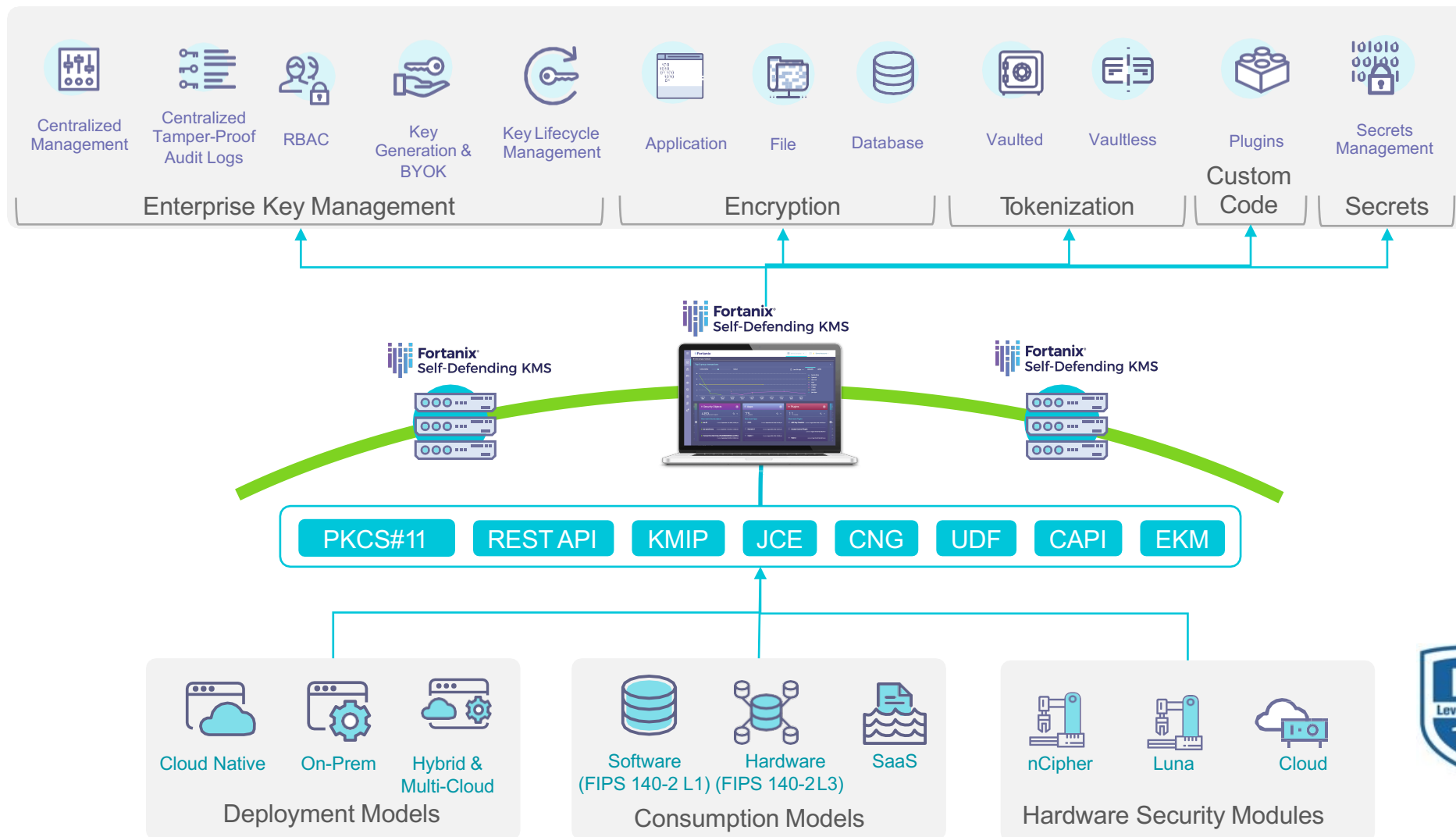
Unfilled Jobs
in cybersecurity

Source: Gartner (G00347310)

vmware®



Fortanix Self-Defending Key Management Service





New Data Security Services Revenue Opportunities

Offer a Portfolio of Profitable and Sticky Data Security Services

Basic Data Security Services For Every Customer



Key Management



VM Encryption



vSAN Encryption

Advanced High Margin Data Security Services



K8s Secrets Management



Database Encryption



HSM Service



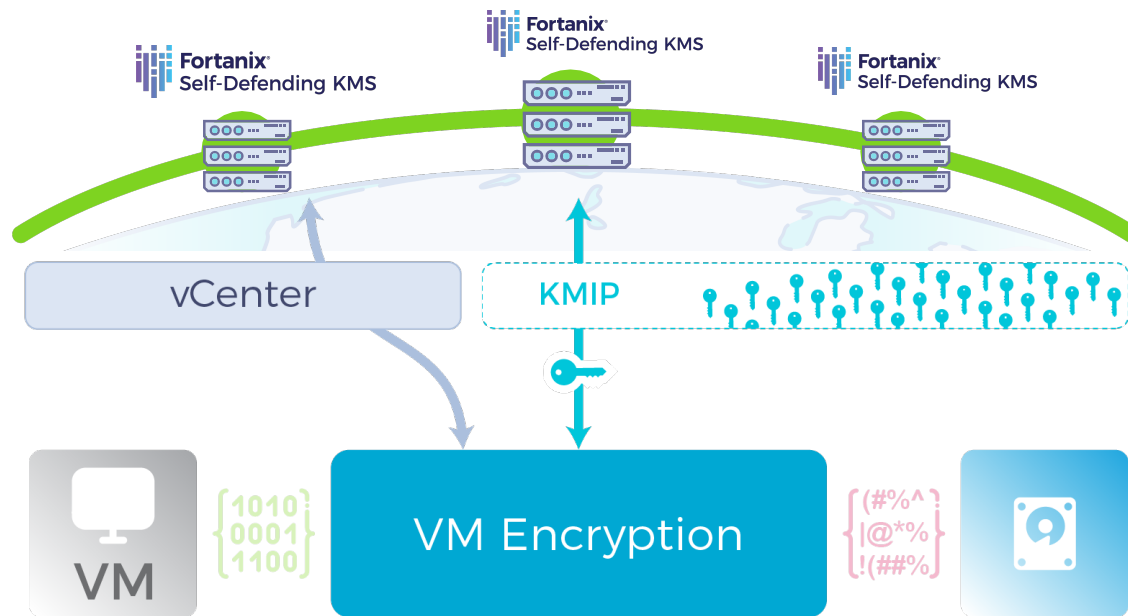
Tokenization



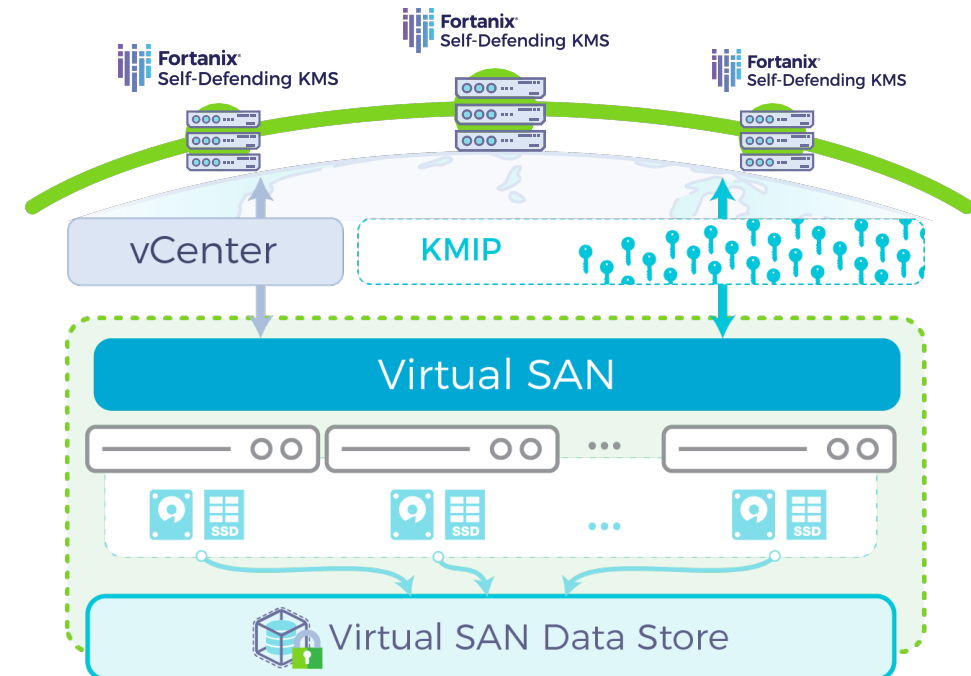
Multi-Cloud Data Security

VMware Encryption: Certified and Ready to Go!

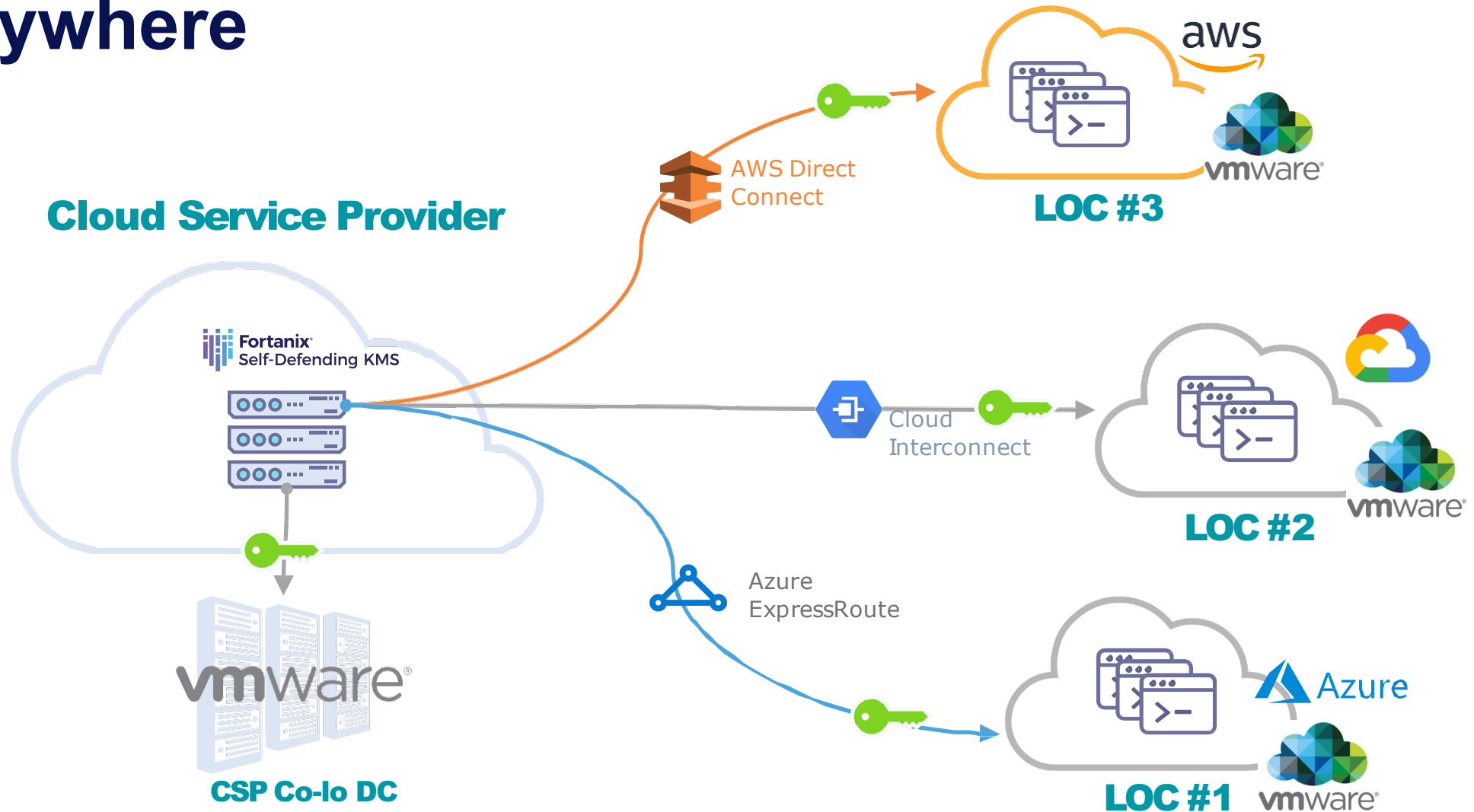
SDKMS for vSphere VM Encryption



SDKMS for vSAN Encryption



Expand your service to protect customers' data everywhere



Case Study: Major Service Provider

“By collaborating with a leading technology partner Fortanix, our CSP is providing our customers with a solution that meets the demands of today’s changing data landscape.”

– VP Product Strategy



Customer Wins Include

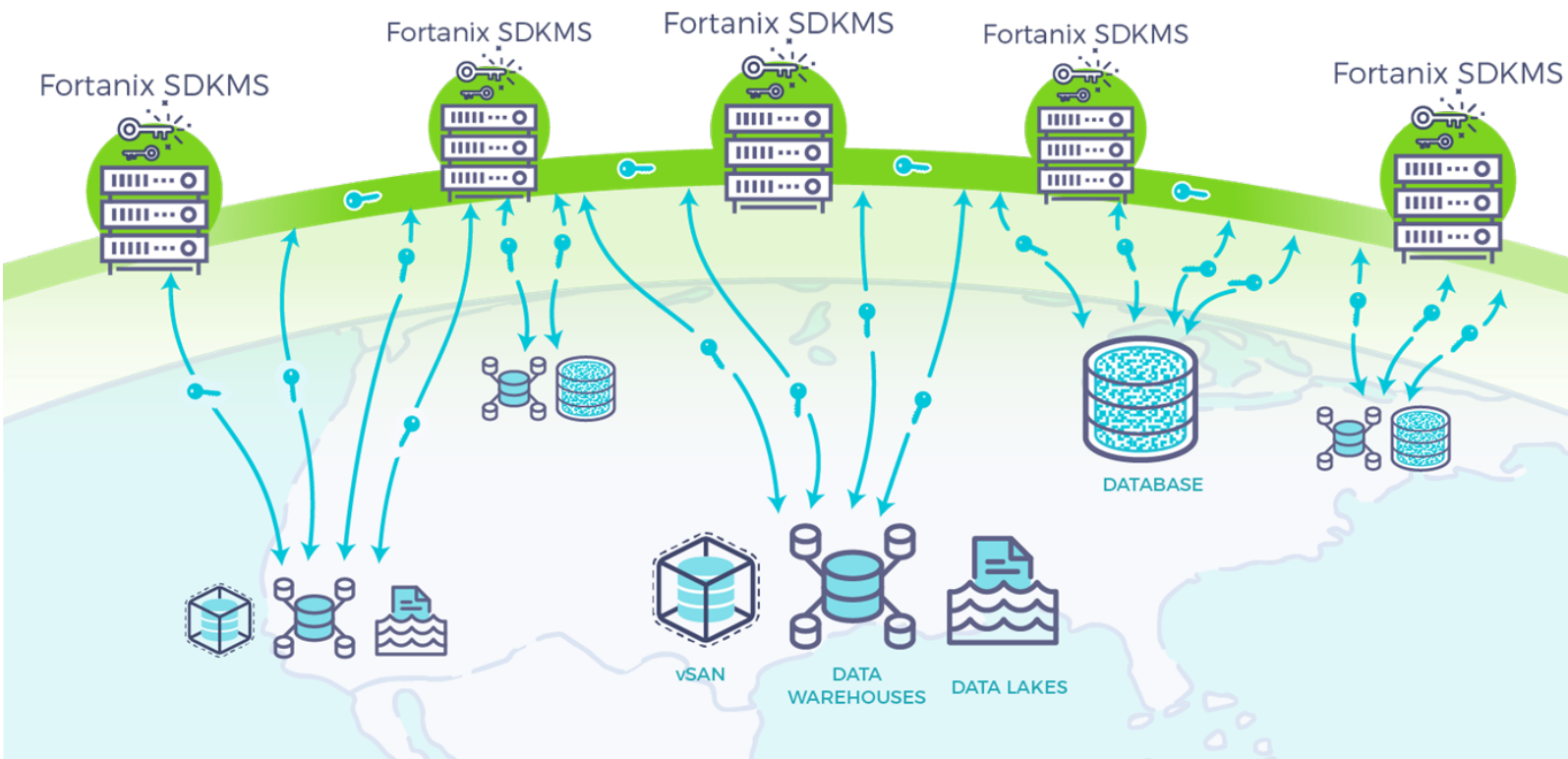
- Global ERP provider
- Multi-national restaurant chain
- National e-Health records system

Benefits

- Increased margin and customer retention
- \$10K-\$15K average new MRR revenue stream per customer
- Differentiation against hyperscale providers

Case Study: CSP's Global FSI Customer

Enterprise Data Protection as a Service



Company Profile

- Top 10 Global Wealth Management Firm

Requirements

- Encryption, KMS, and FIPS level 3 HSM for 1000s of VMware VMs, vSANs, databases
- Separate Tokenization solution needed

Solution and MRR Growth

- Added new use cases of Database Encryption, Tokenization
- **Grew MRR from \$6K to \$18K**
- Additional Upsells – Secrets, Multi-cloud

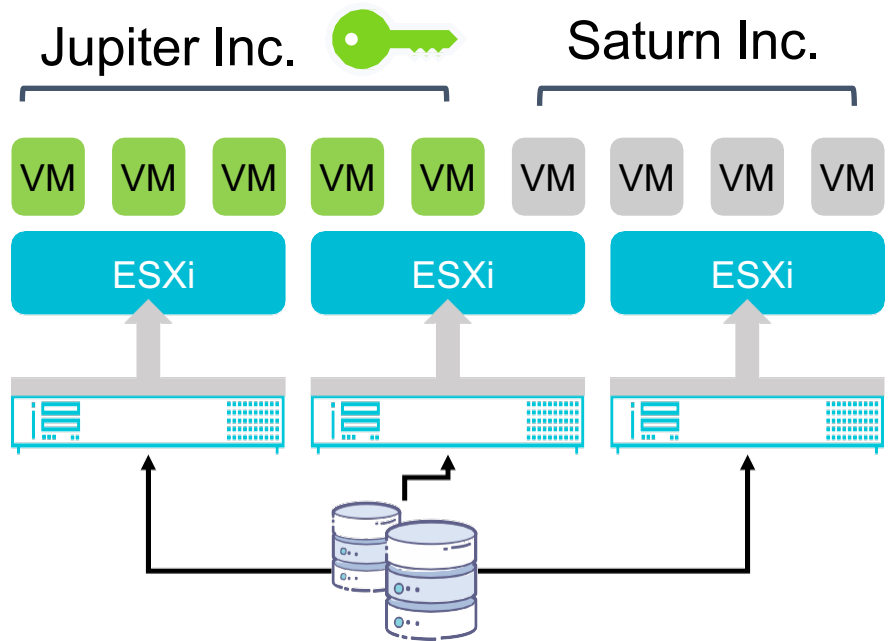
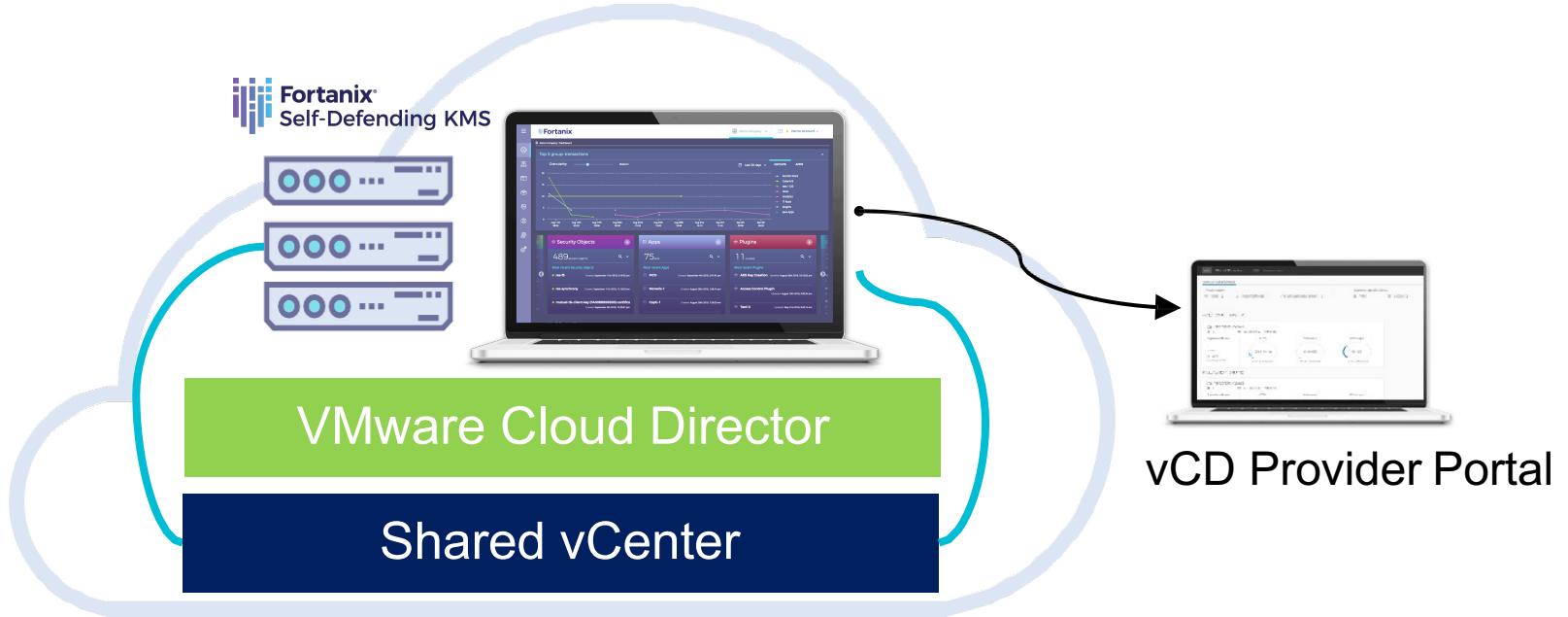


Enabling New Multi-Tenant Services

Multi-tenancy Models

- 1 CSP - Fully Managed Data Security Service
- 2 Data Security as a Service

1 CSP - Fully Managed Data Security Service

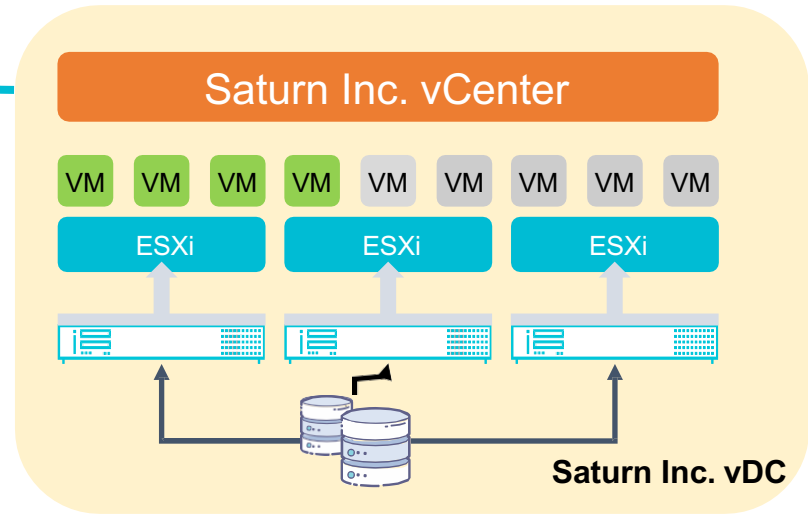
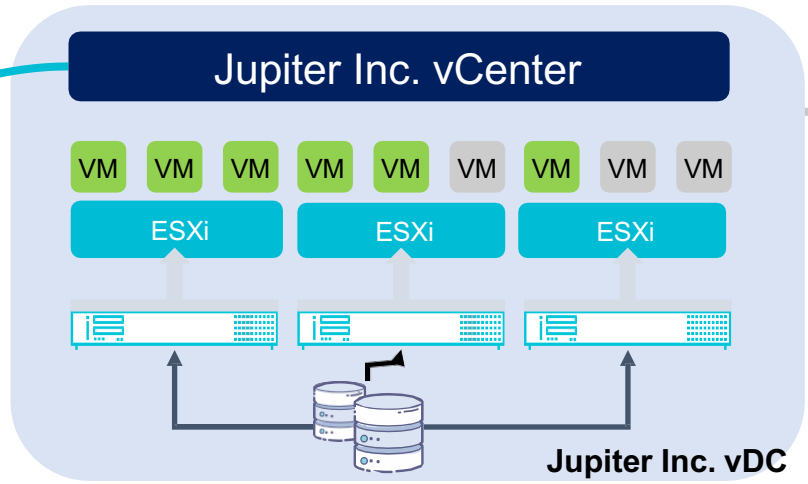


2 Data Security as a Service

Fortanix
Self-Defending KMS



VMWare Cloud Director



The background features a light blue and white color palette. On the right side, there is a graphic of a staircase with white steps and a teal railing, receding into the distance. A solid teal horizontal bar spans across the middle of the image. The word "Demo" is written in white, bold, sans-serif font on the left side of this bar.

Demo

Accounts

Earth Inc.

Jupiter Inc.

Mars Inc.

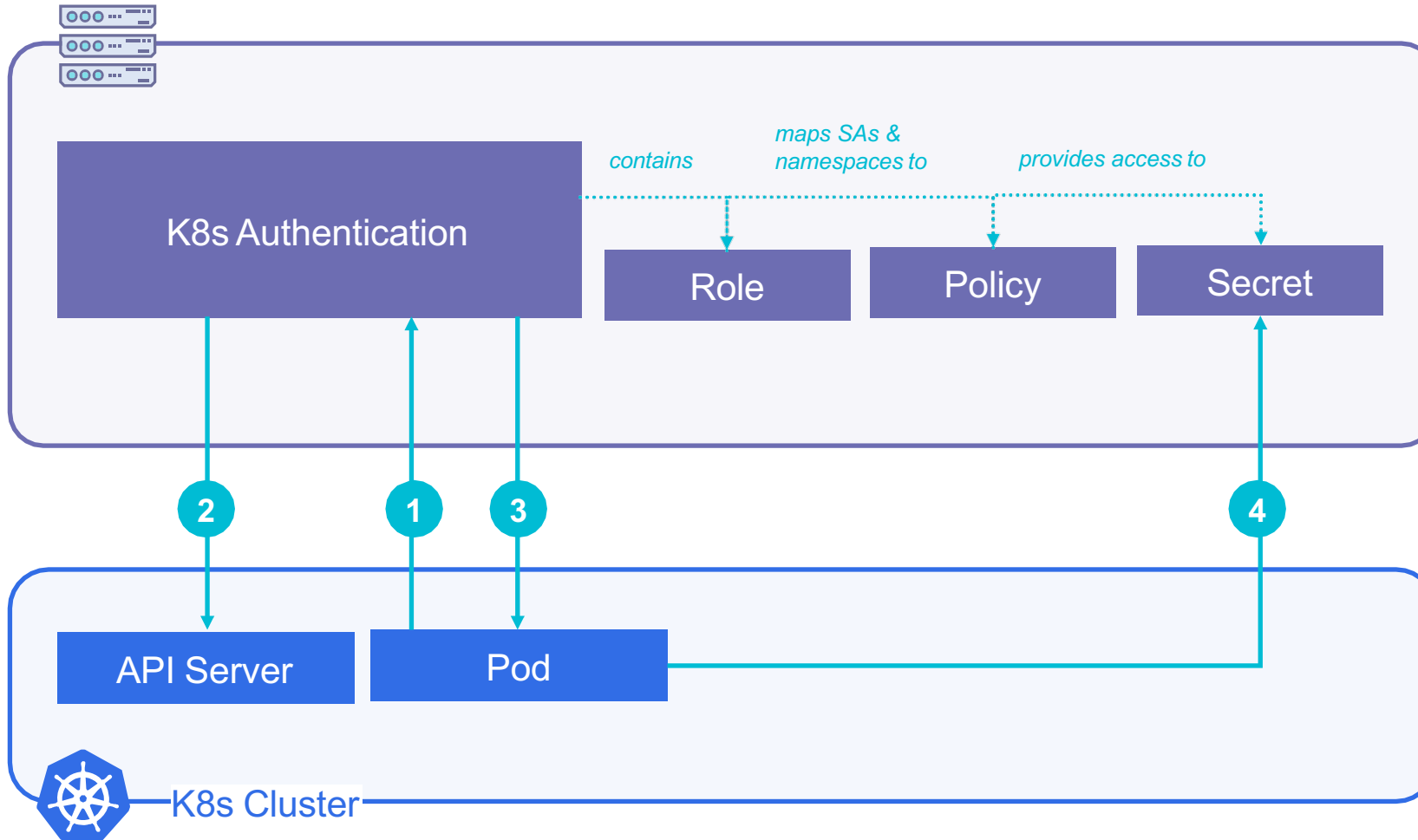
Saturn Inc.

 **CREATE NEW**




To join an existing account, please contact its account administrator.

Coming: Protecting Kubernetes secrets in TANZU

 Fortanix
Self-Defending KMS

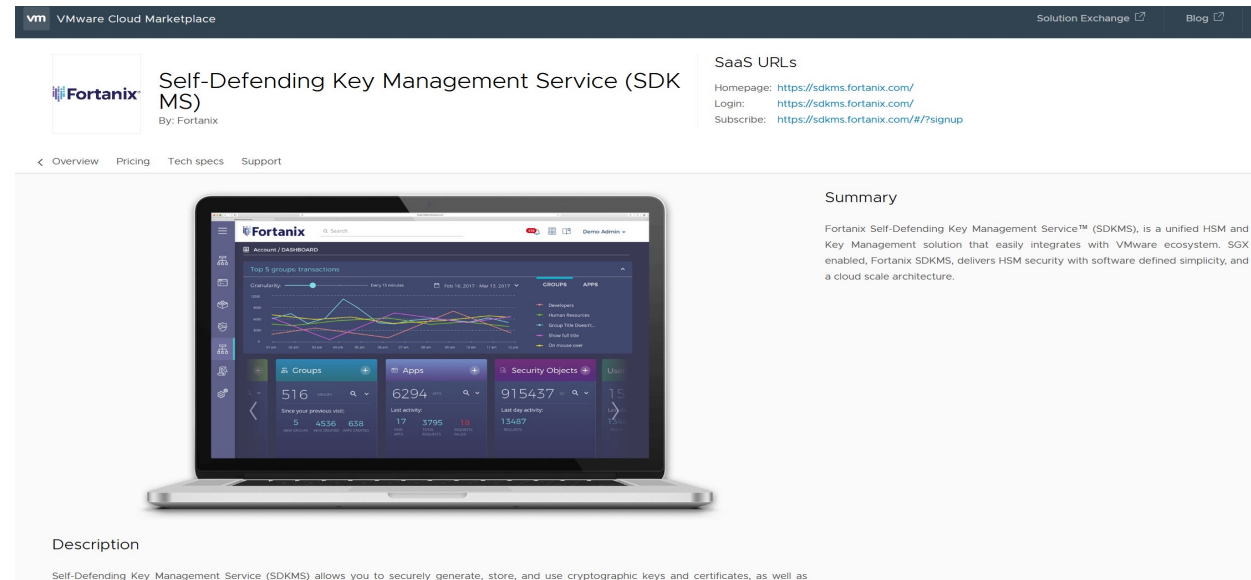


How to engage with us?

Who	Contribution
<p>Fortanix Provides</p> 	<ul style="list-style-type: none">• Knowledge transfer, collaterals, marketing, and sales assistance• Software and appliances certified at FIPS 140-2 Level 3• Training & engineering support for initial period• Level 2 & 3 support
<p>You Provide</p> 	<ul style="list-style-type: none">• Cloud and VMware infrastructure• Acquisition of Fortanix software and appliances• Level 1 support
<p>Commercials</p> 	<ul style="list-style-type: none">• Direct Partnership to start – will be available in marketplace over time• Billing consistent with what you do it today<ul style="list-style-type: none">• Monthly Per Customer Billing of VMs, VSAN, Tokens and Secrets

Where to find us?

VMware Cloud Marketplace



vm VMware Cloud Marketplace Solution Exchange Blog

Fortanix Self-Defending Key Management Service (SDKMS)
By: Fortanix

SaaS URLs
Homepage: <https://sdkms.fortanix.com/>
Login: <https://sdkms.fortanix.com/>
Subscribe: <https://sdkms.fortanix.com/#/?signup>

Overview Pricing Tech specs Support

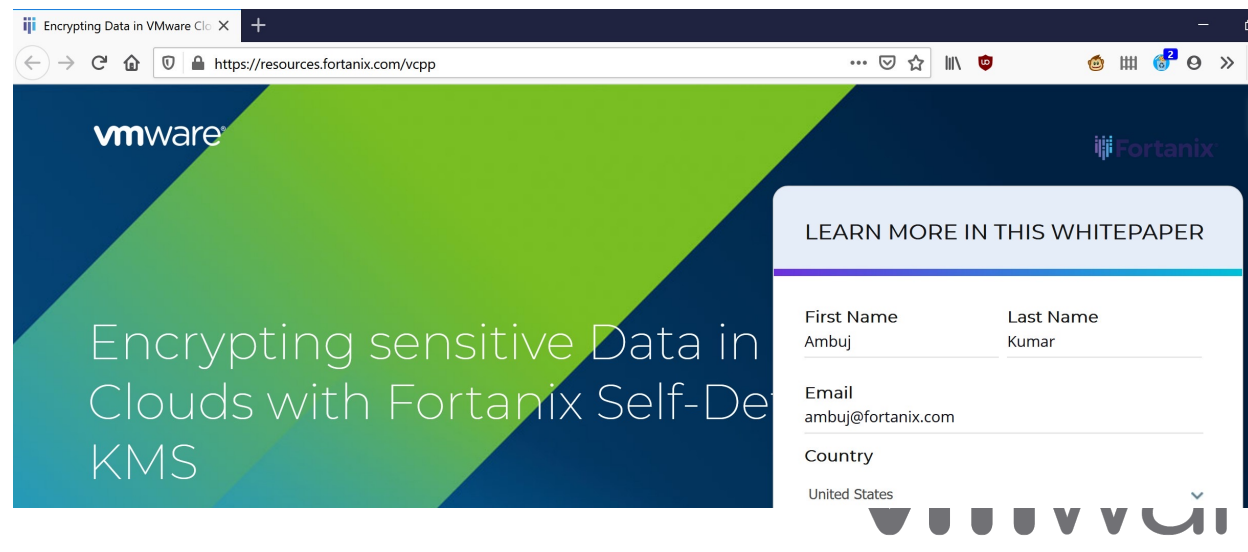
Summary

Fortanix Self-Defending Key Management Service™ (SDKMS), is a unified HSM and Key Management solution that easily integrates with VMware ecosystem, SGX enabled. Fortanix SDKMS, delivers HSM security with software defined simplicity, and a cloud scale architecture.

Description

Self-Defending Key Management Service (SDKMS) allows you to securely generate, store, and use cryptographic keys and certificates, as well as

Dedicated page for you [fortanix.com/vcpp](https://resources.fortanix.com/vcpp)



Encrypting Data in VMware Cloud Marketplace

<https://resources.fortanix.com/vcpp>

vmware Fortanix

LEARN MORE IN THIS WHITEPAPER

First Name: Ambuj Last Name: Kumar

Email: ambuj@fortanix.com

Country: United States

vmware



Takeaways

1

Cloud Partners expect leading edge technology to solve the latest security problems. Fortanix delivers this with Services-ready technology.

2

Fortanix is designed for true multi-cloud scale data security - On Premises, Private Cloud, Hybrid and Public Cloud. Your customers expect you to provide this access and security.

3

New security focused cloud services can result in net new bookings and \$100Ks more margin dollars *per Customer*. Contact us directly to get started.

fortanix.com/vcpp

Q & A

ambuj@fortanix.com

patrick.conte@fortanix.com

 fortanix.com

 info@fortanix.com

 [@fortanix](https://twitter.com/fortanix)

 [Fortanix](https://www.linkedin.com/company/fortanix)

 **Fortanix**[®]