HYTRUST

Datasheet

# HyTrust **KeyControl**

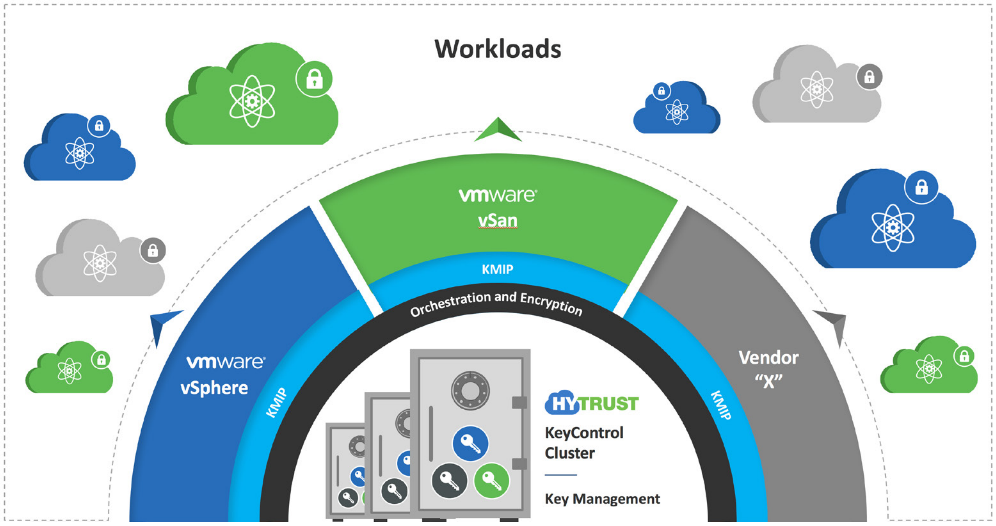
## Universal key management for encrypted workloads

### Key Challenges for an Encrypted Enterprise

Managing the security of workloads in a dynamic, virtualized environment is a time-consuming and complex challenge for administrators. Encrypting workloads helps to reduce your risk of data breaches; if data does fall into the wrong hands, it is unreadable. However, managing the keys for tens of thousands of encrypted workloads is not trivial. To ensure strong data security, keys have to be rotated frequently, and transported and stored securely.

Along with the high demand for strong data security, there is an ever-increasing business need to meet regulatory requirements for PCI-DSS, HIPAA, NIST-800-53, and GDPR compliance in virtual environments.

Many virtualization platforms such as VMware vSphere® lack native key management functionality, requiring a third-party external Key Manager Server (KMS). For multi-cloud environments, key management is even more complex as many key management systems cannot interoperate between different platforms.



### HyTrust KeyControl

With HyTrust KeyControl, businesses can easily manage encryption keys at scale. Using FIPS 140-2 compliant encryption, HyTrust KeyControl simplifies management of encrypted workloads by automating and simplifying the lifecycle of encryption keys; including key storage, distribution, rotation, and key revocation.

#### Universal Key Management for KMIP clients

HyTrust KeyControl is a VMware® certified, scalable, and feature-rich KMIP[1] server to simplify key management for encrypted workloads. It serves as a Key Management Server for VMware vSphere and vSAN encrypted clients, or other products that support KMIP.

### HyTrust KeyControl Benefits

- Pre-selected,validated solution by VMware
- Universal key management for KMIP-compatible encryption agents
- Rapid roll-out and easy to use:
  - Saves operational cost
  - Minimizes errors
  - Helps to rapidly meet security, compliance, or audit requirements
- Enterprise scale and availability
- High Availability (HA) in active-active cluster
- Easily upgradeable to HyTrust DataControl for complete, multi-cloud workload encryption

vmware® READY
APPLICATION SOFTWARE

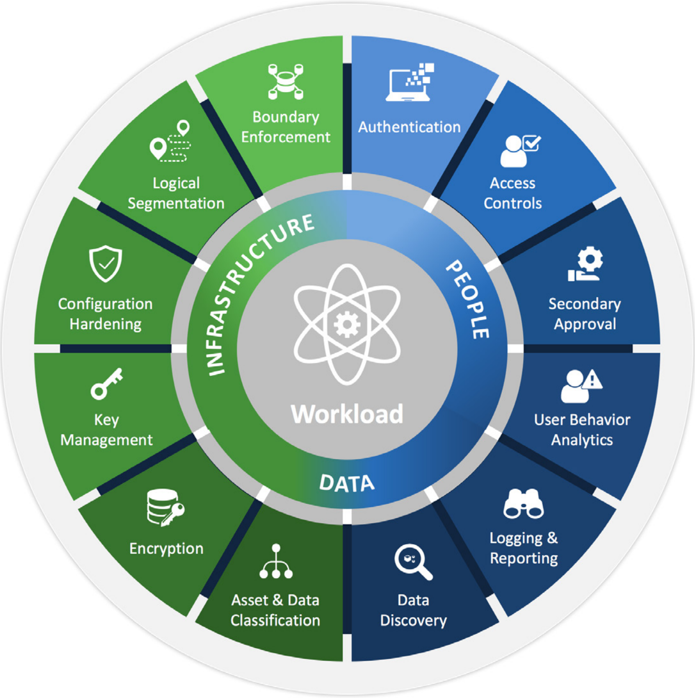
[1] The Key Management Interoperability Protocol (KMIP) standard was introduced in 2010, by an alliance of vendors led by Hewlett-Packard, IBM, and EMC/RSA Security, in order to simplify the interoperability of encryption keys.

### Enterprise Scalability and Performance

HyTrust KeyControl manages the encryption keys for all your virtual machines and encrypted data stores and can scale to support thousands of encrypted workloads in large deployments. Up to eight key managers can be added to a cluster to increase availability and resiliency in high volume key request environments.

### Enhanced Multi-Cloud Workload Encryption

HyTrust KeyControl is easily upgraded to HyTrust DataControl, which enables multi-cloud workload encryption, and policy-based key management. It ensures policies are enforced, even when moving workloads across cloud platforms such as VMware, Microsoft Azure and Amazon AWS. HyTrust DataControl ensures that data within each VM is securely encrypted (AES-128/256-bit) throughout its lifecycle: from installation, upon boot, until each workload is securely decommissioned.



### Extending Cloud Security with HyTrust CloudSPF

HyTrust KeyControl is part of the HyTrust Cloud Security Policy Framework (CloudSPF), which includes HyTrust CloudControl, DataControl and BoundaryControl. The framework enables cross-platform virtualization platforms with advanced security and audit controls, strong encryption, key management, and workload geo-fencing solutions.

### Highlights

- VMware Certified Key Manager Server (KMS) for:
  - vSphere 6.5, 6.7 and 7.0
  - vSAN 6.6, 6.7 and 7.0
  - vSphere Trust Authority 7.0
- Supports KMIP 1.1 – 1.4
- High Availability (HA) support with Active-Active cluster (up to 8 KMS servers per cluster)
- FIPS 140-2 Level 1 validated. FIPS 140-2 Level 3 compliance via HSM support
- Enables the use of Virtual Trusted Platform Module (vTPM) crypto-processors in your VMs
- Supports the use of TLS 1.2 between all registered clients

### Platform Support

- Private cloud platforms: vSphere, vCloud Air (OVH), VCE, VxRail, Pivot3, NetApp, Nutanix–Public cloud platforms: Amazon Web Services (AWS), IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS
- Hypervisor Support: VMware ESXi, Microsoft Hyper-V, AWS, Azure
- Deployment Media: ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services marketplace), or VHD (Microsoft Azure marketplace)

To learn more about HyTrust products and services, visit: www.hytrust.com/products/

**HyTrust**
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
1-844-681-8100 (US)
1-650-681-8100 (Intl.)