HYTRUST

Datasheet

# HyTrust DataControl 4.2

## Secure Multi-Cloud Workloads

### The Need for Data Encryption

Many workloads contain critical data, which has to be protected. Your company's reputation is at stake, and after a data breach, lawsuits and loss of revenue is as good as guaranteed. Increased regulation and data security standards are there to guide organizations, but may impose heavy fines if your security measures are not up to par.

Encrypting your workloads is more than just another layer of cyber defense. It is, in fact, the foundation of a sound data security strategy, and a key component of most data protection regulations. Many regulations, including the GDPR, exempt you from reporting a data breach if data was encrypted.

#### The Multi-Cloud Conundrum

Managing encrypted workloads can get complex, especially in a multi-cloud environment. Workloads go through many life cycles, from staging to deployment, to backup and eventually have to be securely decommissioned. Each stage poses different risks of having the data stolen. Encrypting the data in each stage makes the data useless to the bad guy that stole it. Unfortunately, workload encryption is not a set-it-and-forget-it operation. It is critical to frequently re-key the data, increasing the complexity of key management.

Managing workload encryption from each cloud's management platform is complex and increases the risk of inconsistent policies, and mistakes. Migrating workloads between clouds means they are first decrypted, then migrated in clear-text, then have to be re-encrypted, introducing new risk factors.

### HyTrust DataControl

HyTrust DataControl secures multi-cloud workloads throughout their lifecycle for organizations seeking to protect critical and sensitive data. DataControl reduces the complexity of protecting workloads across multiple cloud platforms and helps your organization comply with industry regulations.

#### Managing Encrypted Workloads in a Multi-Cloud Infrastructure

HyTrust DataControl allows you to manage your encrypted workloads across different infrastructures. DataControl works on-premises and with the leading public cloud platforms, but also with hyperconvergence and storage solutions. With DataControl, you get a centralized and scalable solution to control all your encryption keys. DataControl includes the VMware certified HyTrust KeyControl Key Management Server (KMS).

#### Deep Workload Protection

Apply strong security and protection for workloads throughout their lifecycle, from boot to backup, and final decommissioning stage.

DataControl provides granular encryption for better security. The protection boundary does not stop at the hypervisor or at the data store; VMs are individually encrypted. Inside the VM, unique keys can be assigned to encrypt each partition, including the boot (OS) disk and swap partitions.

### HyTrust DataControl Benefits

- Complete workload lifecycle encryption management – from boot to decommissioning
- Key Management Server (KMS)
- Strong and granular VM encryption: live boot (OS) and data partition encryption
- Access controls for separation of duties among admins
- Easy to deploy and manage

### Platform Support

- Private cloud platforms: vSphere, vCloud Air (OVH), VCE, VxRail, Simplivity, Pivot3, NetApp, Nutanix
- Public cloud platforms: Amazon Web Services (AWS), IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS
- Hypervisor Support: ESXi, Hyper-V, Xen, AWS, Azure, KVM
- Deployment Platform Support: CentOS, Enterprise Linux, Ubuntu, SUSE Linux Enterprise Server, Oracle Linux, AWS Linux, Windows Server Core 2012 and 2016, Windows Server 2008, 2012, and 2016, Windows 7, 8, 8.1, and 10
- Deployment Media: ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services marketplace), or VHD (Microsoft Azure marketplace)

### Easy to Deploy and Manage

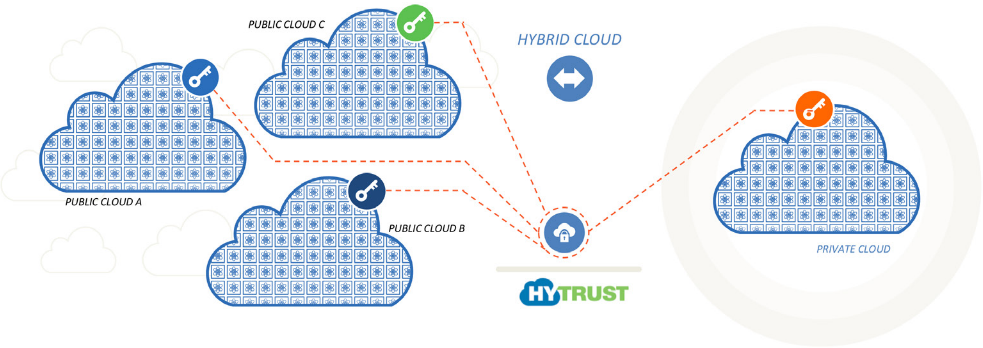
DataControl provides deployment flexibility with a single interface for all workload encryption, which eliminates the complexity of using each platform's own encryption feature separately. The user experience is great for administrators and zero downtime encryption allows for frequent and more secure re-keying while the workload remains accessible. High Availability clustering ensures your disaster recovery is not impaired by losing access to the critical key management system of DataControl.

### Access Controls

DataControl allows for robust policy-based access controls to enforce separation of duties across different user personas. Prevent root users or system administrators from accessing sensitive data by enforcing access controls on encrypted volumes. For hybrid cloud deployments, prevent your cloud service providers' administrators, often responsible for patching and other operational upkeep, from ever accessing encrypted data. DataControl allows for custom controls across a variety of use cases to enable greater security across multi-cloud deployments.

### Deduplication Support

Previously, the concern existed that encryption and deduplication could not co-exist, given that encrypting data makes every block different. HyTrust DataControl has now solved this problem so that customers can enjoy the data security afforded by encryption along with the cost savings offered by the deduplication capabilities of different storage platforms, including VMware vSAN storage. With this unique approach, HyTrust DataControl offers AES 256-bit encryption while maintaining 91% of the storage benefit of vSAN deduplication.



Centralized key management; encryption policy across clouds; VM never boots without key; security policy travels with the workload

## Extending Cloud Security with HyTrust CloudSPF

HyTrust DataControl is part of the HyTrust Cloud Security Policy Framework (CloudSPF), which includes HyTrust CloudControl, KeyControl, BoundaryControl and CloudAdvisor. The framework enables multi-cloud deployments with advanced access controls and audit capabilities, strong encryption, key management, workload geo-fencing and data discovery and classification solutions.

### Highlights

- Granular security for Windows and Linux VMs
  - Encrypt boot (OS), swap and data partitions
  - Use individual keys per partition
- Strong AES (128/256 bit) encryption with Intel hardware acceleration support
- FIPS 140-2 compliant Level 1 encryption key management. Works with Level 2/3 HSM
- Zero downtime encryption with automatic re-keying
- Dynamic partition resizing for Windows VMs
- Supports KMIP v1.1 - 1.4 (Key Management Interoperability Protocol) clients
- High Availability (HA) support with Active-Active cluster (up to 8 KMS servers per cluster)
- Single encryption key for deduplication support
- Certified for VMware vSphere and vSAN encryption
- Graphical dashboards visually identify risk including unencrypted workloads, out of date software, and other critical security metrics
- REST-based API integration for DevOps
- Protect encrypted workloads against unauthorized access with boot and clone protection
- Supports 3rd party Hardware Security Modules (HSM) for increased key security

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.)

© 2018 HyTrust, Inc. All rights reserved. HyTrust, and the HyTrust logo are trademarks and/or registered trademarks of HyTrust, Inc., and/or its subsidiaries in the United States and/or other countries. All other trademarks are properties of their respective owners.