DATA SHEET

HYTRUST
Cloud Under Control

HyTrust DataControl 2.6

Encryption and Key Management for the Cloud

HyTrust DataControl™ helps organizations lock down virtual machines and their data so they remain secure throughout their lifecycle, from creation until they are securely decommissioned, easily and automatically.

The Challenge

The public cloud can offload IT requirements and offer better business agility , but recent IT surveys show more than 50% of IT managers withhold sensitive data from the cloud because of security concerns. The reality is that virtualization introduces security concerns that escalate significantly as organizations move to private, hybrid or public clouds.

VM Encryption with HyTrust DataControl™

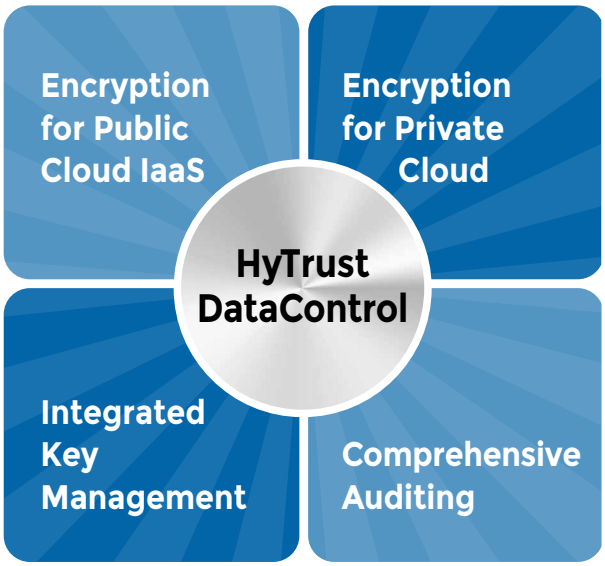
HyTrust DataControl™ encrypts stored data in any IaaS or private cloud. It is cloud-agnostic, and supports block storage encryption for Windows or Linux virtual machines. More importantly, the keys and encryption policies are retained by you – not your cloud service provider. With HyTrust DataControl, you can say 'yes' to your business units' public cloud demands.

The Features

HyTrust DataControl was purpose-built to secure data in virtualized and cloud environments.

On-the-Fly Encryption and Re-Key.

HyTrust DataControl encrypts data using NIST-approved AES-128/256 algorithms,



ensuring data remains private at rest in storage and in VM backups. HyTrust is uniquely able to encrypt and re-key without taking applications offline, eliminating disruption and enabling easier compliance with privacy regulations like PCI or internal mandates.

Simplified Key Management.

HyTrust KeyControl™ is a highly-available, security-hardened key management system that is simple to deploy and easy to use. KeyControl is fully multi-tenant and can be installed inside your firewall or at your service provider.

Role-based Policy Management.

HyTrust DataControl's policy-based encryption lets you segment encryption and administration by department, security-level, mission or other criteria. Unlike whole disk encryption, HyTrust DataControl policies and encryption travel with the VM, ensuring security regardless of where your VM is copied or instantiated.

Full RESTful API.

Leveraging HyTrust's API, you can easily automate any task such as provisioning new VMs or volumes, simplifying deployment and scalability.

Transparency.

Because of where the software sits in the virtualization stack, HyTrust DataControl is completely transparent to users and applications. Administrators can manage their virtual servers using the same tools they always have, with no change to their process.

Hardware-Accelerated Performance.

HyTrust DataControl will detect and automatically use the AES-NI hardware acceleration built into modern Intel and AMD chipsets, so you get maximum performance and minimal latency.

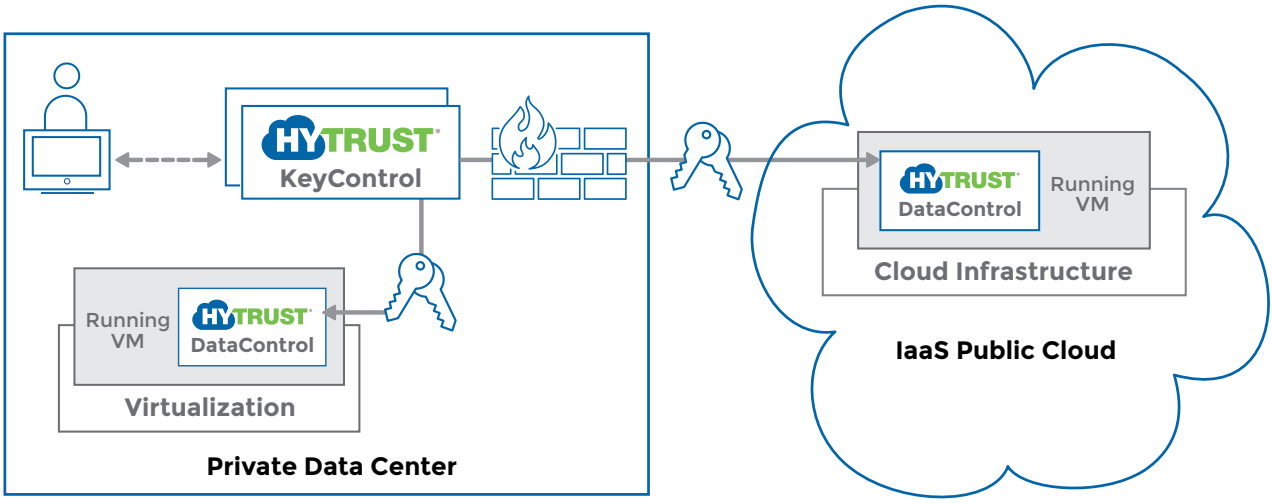
Rich Security Audit Stream.

HyTrust DataControl captures, logs and alerts on a broad range of activity to monitor and track administrative and system changes.

How It Works

The HyTrust DataControl Policy Agent can be installed in seconds into the Windows and Linux operating system of the VMs you wish to protect.

Once you have authenticated your VM with HyTrust KeyControl, you can start encryption. All data encrypted in the OS is protected it as it moves through the hypervisor and through to storage. When requested by authorized VMs, encryption keys are securely retrieved, and the data is decrypted and presented back to the application.



HyTrust DataControl encrypts data from within the OS of a virtual machine. Key management is policy-based and easy to deploy on premises or in the cloud.