

## Enhancing VDI with HyTrust DataControl

- 
- **Securely encrypt VDI workloads**
  - **Securely decommission VDI workloads**
  - **Automate and script encryption key management**
  - **Protect against insider theft**
- 

Many organizations, particularly those in industries/verticals with a heavy emphasis on regulations, are turning to virtual desktop infrastructure (VDI). These organizations include the government, military, educational institutes, finance corporations and medical/healthcare establishments - generally speaking, environments where standardization and consistency are important.

One of the benefits of VDI is that virtual endpoint data resides in the data center. This reduces the risk of lost or stolen end point devices since only a representation of a screen image (think VNC or RDP) is sent to the end client, not the data. That said, these virtual machines need the protection of encryption.

Beyond just fundamental encryption, HyTrust DataControl includes advanced key management capabilities that allow secure decommissioning of workloads, automated key rotation and secure clone management. All these factors help provide a better security stance while making compliance faster, easier and more certain.

### **VDI encryption**

HyTrust offers organizations the ability to encrypt VDI desktops. With FIPS 140-2 certification, HyTrust DataControl brings military strength encryption to virtualized hosts located on-prem or in the public cloud.

### **Rapid deployment**

HyTrust DataControl is fast to install and fast to deploy, up and running in as little as 30 minutes in small/simple environments. Obviously larger, more complex environments will require a little planning, but you can count on a fast, easy initial install and configuration experience.

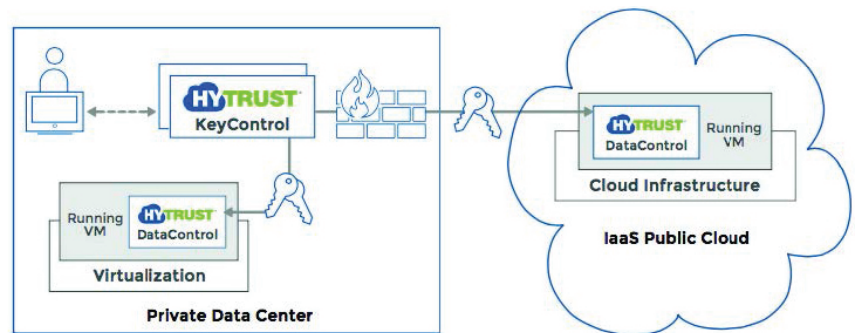
### **Central key management**

HyTrust DataControl brings sophisticated key management capabilities, such as automating complex tasks (ex. key rotation and compliance), which in turn save a considerable amount of time and money. It can also support KMIP,

symmetric keys, certs, PGP keys, split keys and more. Key management automation can be scripted, aiding operations and compliance.

### Secure decommissioning of VMs

When desktop VMs are encrypted, control of the encryption key remains with the central KeyControl server. When a VM is to be retired, the KeyControl server can just pull the key and the VM will no longer be decryptable nor will it be executable.



### Cloning and controls

With HyTrust DataControl you can create a golden master image complete with encryption for enterprise-wide deployment, saving time. Similarly, illegitimate clones never receive encryption keys, rendering them useless.

### Insider threat protection

With tight control over encryption keys, even if an insider were to get his hands on a VM, it will be of little use for data exfiltration because the files composing the VM are all encrypted.

### Role-based access control

Granular RBAC security ensures administrators have the access they need to do the job, not more.

### Rekey without downtime

Unlike traditional encryption systems, HyTrust DataControl allows zero downtime encryption rekeying. This enables organizations to maintain the strictest compliance requirements while minimizing impact on end users.

### Plays well with others

RESTful APIs allow for easy integration with other enterprise applications including SIEM and other security packages.

Ready for next steps? Get in touch with us at [www.hytrust.com/contact/](http://www.hytrust.com/contact/) or by phone at 844 681-8100. We hope to hear from you soon.