HYTRUST

Datasheet

HyTrust DataControl

Workload encryption and scalable key management for any cloud

HyTrust DataControl offers powerful, military grade encryption with easy to use, scalable key management to secure the workload throughout its lifecycle from deployment and migration to sanctioned decommission. Used by some of the world's largest companies and government organizations, HyTrust DataControl has been built to be flexible and easy for any cloud deployment.

Deep security and automated compliance

HyTrust DataControl provides the best security capability and automates compliance enforcement to ensure no-gap security coverage for all workloads.

Complete stack protection

HyTrust DataControl ensures the entire workload, including the O/S, applications, and data are encrypted. Using block level technology (the most reliable), the entire system can be protected, without worrying about skipping boot or operating systems files that are always in use. HyTrust DataControl authorizes workloads to start only on approved conditions and locations. Authorized startup becomes critical when moving workloads to pubic cloud providers to ensure your data is protected at all times.

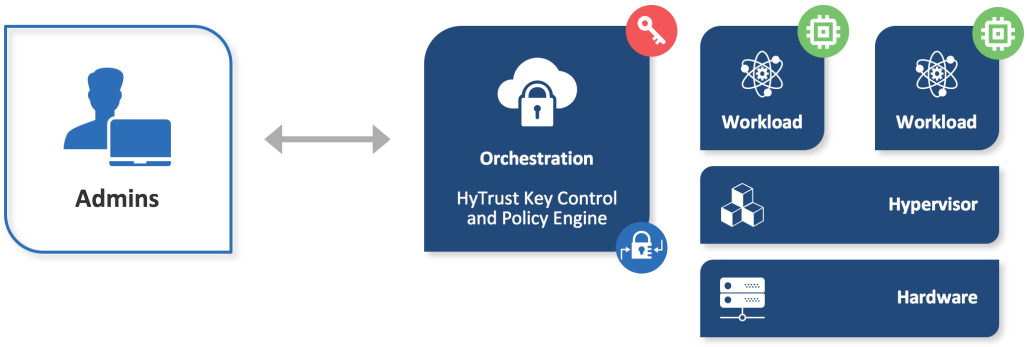
Any security posture supported

HyTrust DataControl provides users with a range of security postures, ranging from software-based protection to hardware-based protection, including HSM integration. HSM integration allows users to achieve the highest level of security (FIPS 140-2 Level 3) as their security needs require. With policy-based mechanisms, administrators can tune the level of security required quickly across the entire set of managed workloads.

HyTrust DataControl highlights:

Virtualization awareness
- Protects against counterfeit (stolen) workloads
- Secure decommissioning of workloads
- Portable encryption travels with workload for constant protection
- Protection of Active Domain Controllers
- VDI environment protection

Easy to use
- 15min from first click to full protection
- Always on—no downtime and no touch (via scheduling) encryption
- Encryption via API's, existing deployment platform systems, or even via GUI point and click encryption
- Graphical risk dashboard provides instant view of risk levels including unencrypted drives, out of date software, and other key operations and security metrics
- Fast to operate with policy based actions and fast encryption/ decryption leveraging hardware based support where available



KeyControl – the key manager that ensures enforcement of policy via key issuance and revocation

Policy Engine – ensure appropriate controls with context; enforces the right admins for creating/modifying encryption policies, identifies workloads and context for policies

Policy Agent – ties policy to workload and executes encryption and decryption

Key platforms

- Private clouds (vSphere, vCloud Air, VCE, VxRail, Nutanix, Simplivity, Pivot3, and others)
- Public clouds (AWS, IBM Cloud, Microsoft Azure, and others)
- Multi-hypervisor support (ESXi, Hyper-V, KVM, Xen)

Everywhere protection

Workloads are very mobile and thus need protection to follow. With portable encryption controls, workloads check with HyTrust DataControl's policy engine on when and where decryption of the workload is permitted.

Host security attestation

Workloads can move often, sometimes to hosts that may not be trusted. HyTrust DataControl integrates with HyTrust CloudControl to leverage Intel's TXT (Trusted Execution Technology) to provide proof of a hosts security state. With this capability, administrators can set policy and determine what to do if a workload is moved onto a host that does not have the appropriate level of security desired.

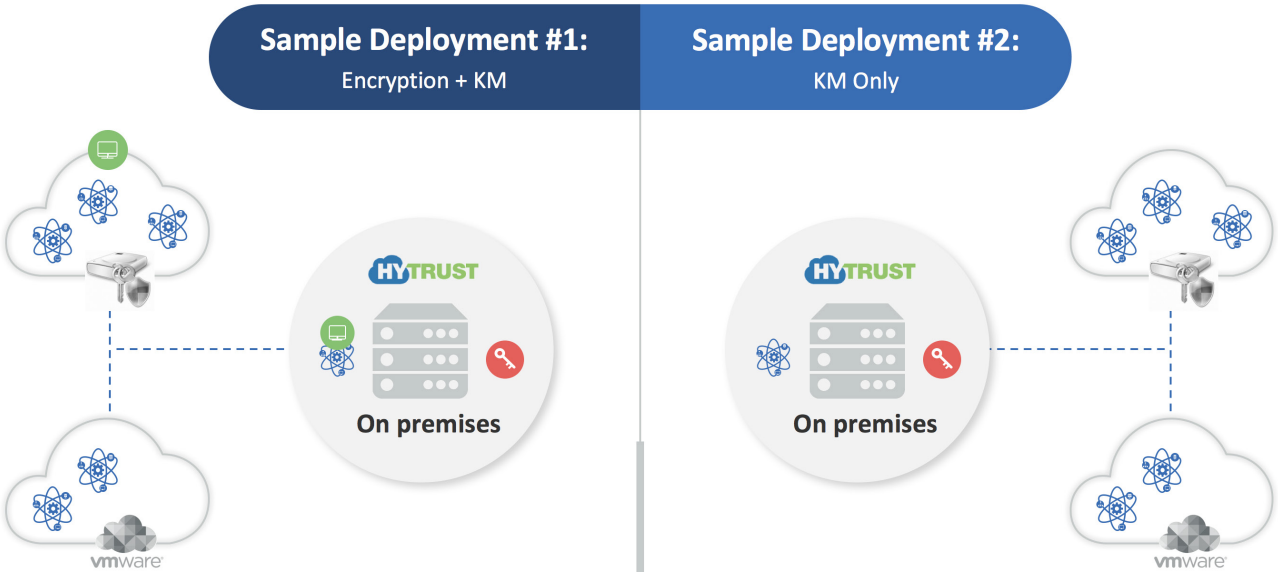
Counterfeit workload protection

Clones of workloads (e.g. copies of virtual machines) may be created accidently or maliciously (to steal them) and should not be allowed to be used. In other cases, administrators may want to create a "gold master" and allow for a copy of a workload. Leveraging HyTrust DataControl's intelligent policy engine – administrators can set scenarios to ensure counterfeit workloads are never decrypted, but authorized copies can be used to speed up IT deployments while maintaining separate and unique encryption keys.

Multi-tenancy administrator protection

HyTrust DataControl not only protects the workload, but also protects an organization by ensuring appropriate accesses

Flexibility in deployment model – you choose



Key security features

- FIPS 140-2 Level 3 support with HSM (or FIPS 140-2 Level 1 certified without)
- Secure workload startup protection
- KMIP support (including VMware's VMcrypt)
- Dashboard and log based forensic analytics
- RBAC for administrative controls over policy and key access
- Cross-cloud (public and private) key management
- Secure decommissioning
- Pre-integration with HyTrust CloudControl and HyTrust BoundaryControl to provide automated data geo-fencing of workloads
- File/Folder level encryption (on select operating systems)
- Pre-integration with Intel TXT/TPM for hardware host attestation
- workloads
- Pre-integration with Intel TXT/TPM for hardware host attestation

to the administrative functions are also controlled – critical in a multi-tenant environment. With role hierarchy and detailed transactional controls (e.g. policy creation, key issuance, etc.) organizations can rest assured that even the administrators have provable audit trails and protection.

Scalable and reliable

Organizations demand the highest level of service availability without sacrificing security and no extra cost. HyTrust DataControl ensures workload protection always works, all the time.

Zero downtime, zero touch

Most organizations schedule changes of encryption keys on a regular basis for best practices as well as to meet specific compliance requirements. HyTrust DataControl is the only product on the market that can allow for rekeying of encryption keys without any downtime. In addition, with scheduled based re-keying, administrators can literally "set and forget" – making the process very easy with no burden on operations.

System resilience

Should the corruption of a workload occur or the encryption process be interrupted – HyTrust DataControl can immediate pick up where it left off. This ensures minimal risk with exposed (unencrypted data) and ensures no data corruption. For large disks – this could save days or even weeks of time for operations.

RESTful APIs for unlimited expansion

While not required, organization can choose to further enhance their automation and scale through interacting with HyTrust DataControl's APIs and build data protection into a Devops or production flow.

Active-active fault tolerance included

With no additional cost for additional servers for key issuance and control, organizations can provide any number of backup (active-active) virtual images to ensure all key operations remain online, all the time.

Fast deployment, easy operation

HyTrust DataControl has been designed to be a minimal touch, easy to implement security solution and can also be leveraged for sophisticated workflows through graphical interfaces, policy definitions, and even API integration.

Risk exposure dashboard

With visual dashboards, administrators can quickly identify risk exposure through unencrypted disks or track how much data remain encrypted. All encrypted tasks are shown visually on the dashboard so operations personnel can plan or respond in real-time.

Point and click encryption

While HyTrust DataControl's powerful encryption engine provides for a range of capability, administrator can also select individual workloads manually to encrypt on demand. This point and click encryption can be helpful for smaller deployments, breach mitigation, or even test/development scenarios.

Powerful and easy logging

Unlike many other virtual administration software, HyTrust DataControl provides forensic level details – in an easy to consume format for humans and machines. Security response or compliance teams can use this information to quickly mitigate issues.

Pre-integration and compatibility

HyTrust DataControl provides the highest level of security and easiest to use solution on the market by ensuring workload work on any chosen deployment model. With established integrations or tested compatibility with environments such as private cloud offerings, including hyper-convergence platforms, and numerous public cloud offerings, no matter where the workload goes – HyTrust DataControl will be ready to secure it.

To learn more about HyTrust DataControl, as well as other HyTrust products and services, visit:

www.hytrust.com/products/datacontrol/

HyTrust - Cloud Under Control.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100