HyTrust® CloudControl™ 3.6

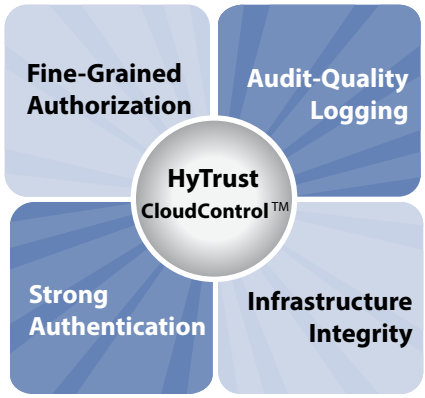
HyTrust CloudControl ™ serves as a gateway to mitigate the concentration of risk and potential for catastrophic data center outages inherent in virtualization. Enterprises now have the visibility and controls they need to securely virtualize all workloads and deploy multi-tenant private clouds.

THE CHALLENGE

Virtualization provides large operating and financial benefits by consolidating thousands of servers, routers, and switches into a single software layer. It has delivered dramatic increases in capacity utilization and increased IT administration efficiency. One consequence of consolidation is that virtualization administrator accounts have unprecedented power and spans of control: a privileged user with administrative access to the virtual infrastructure can reconfigure, power off, or delete scores of mission critical applications and network adapters – accidentally or intentionally – with a few clicks.

With the cloud's proliferation of highly privileged accounts that can control most of an organization's production and mission critical applications, risk becomes highly concentrated. The lack of continuous monitoring, audit trails, and accountability for administrative activity in the virtual environment only magnifies the risk. Without the controls needed to ensure separation of duties and least privilege access to virtualized and private cloud infrastructure, the potential for catastrophic outage is real.

Unauthorized access to privileged user accounts by bad actors outside or inside the enterprise is, if anything, a greater threat than misuse by authorized users. Weak authentication, inadequate logs, host configuration vulnerabilities, and the absence of threat detection all contribute to a breakdown in data center governance. The consequences of insider and external breaches in the virtual infrastructure can be catastrophic – leaks of sensitive data, theft of IP or financial data, and malicious destruction of the datacenter are all possible.



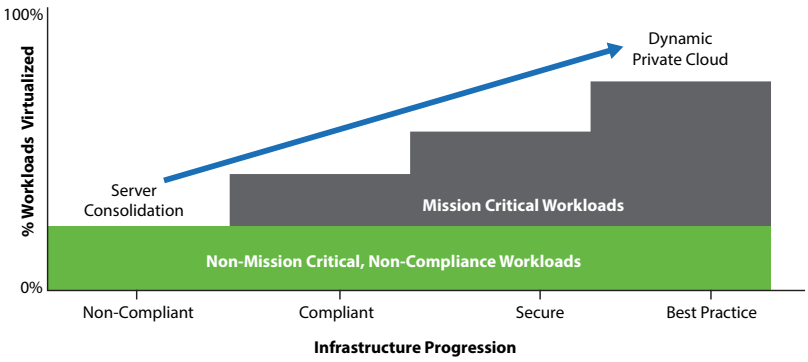
THE SOLUTION

HyTrust CloudControl ™ enables enterprises to virtualize mission critical applications and deploy multi-tenant private clouds without taking on large, unacceptable risks. It establishes visibility and accountability, defeats sophisticated attacks, and limits the impact of administrative mistakes by providing:

- Real time monitoring, threat detection, and alerting of suspicious vCenter account activity
- Fine-grained role-based and resource-based authorization, enforcing separation of duties and least privilege, need-to-know access
- Audit-quality logs that enable complete audit trails tied to individual users' activity
- Strong, multi-factor authentication to protect access to the virtualization platform
- Hypervisor configuration hardening to ensure platform integrity

THE BENEFITS

- Gain operational and financial benefits of virtualizing critical applications without added risk
- Mitigate risks of extended data center downtime and theft of confidential information
- Achieve constant visibility and privileged user accountability
- Contain and prevent damage due to privileged account misuse
- Isolate each tenant's resources in a private cloud without costly air gaps
- Assure internal and external auditors that administration risk is effectively managed
- Harden privileged accounts against compromise



VIRTUALIZATION MATURES

Organizations have expanded their use of virtualization from lower tier workloads to production and other mission-critical applications. HyTrust CloudControl™ mitigates the increasing concentration of risk in next generation data centers, enabling greater virtualization and faster adoption of private clouds.

HOW IT WORKS

Fine-Grained Authorization

- Limits or prevents harm to critical workloads by enforcing enterprise-defined policies
- Applies both role-based and asset-based access control rules to achieve separation of duties and resource isolation, with no changes to user workflows
- Automates secondary approval requested policy exceptions
- Integrates with Active Directory for efficient role definition

Audit Quality Logs

- Compiles complete audit trails required for compliance and fast incident response
- Provides a unique user ID for every attempted operation using root password vaulting
- Records essential audit data including denied operations, source IP addresses, and details of VM reconfigurations
- Automatically sends log data to SIEM and security management systems including McAfee ePolicy Orchestrator, Symantec Control Compliance Suite, RSA enVision and HP ArcSight

Strong, Multi-Factor Authentication

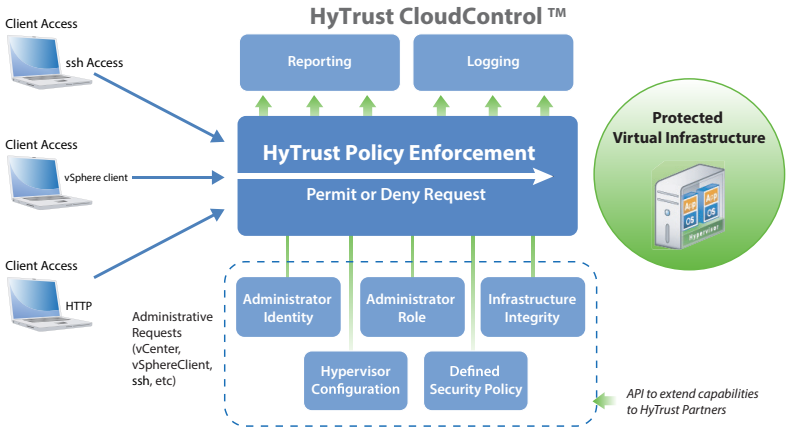
- Prevents damage to enterprise resulting from compromised administrative password
- Integrates with RSA SecurID and CA ArcotID

Hypervisor Configuration Hardening

- Mitigates risk of catastrophic loss made possible by host misconfiguration vulnerabilities
- Automates configuration policy definition, enforcement, and remediation
- Defeats rootkit attacks by verifying host root of trust with Intel TXT technology

HyTrust CloudControl also enforces access and governance policy for VCE Vblock converged infrastructure's virtual environment.

To learn more about how HyTrust mitigates the increasing concentration of risk and potential for catastrophic failure in virtualized and private cloud environments, visit hytrust.com/product



To learn more... hytrust.com/product

HyTrust, Inc. 1975 W. El Camino Real, Suite 203 Mountain View, CA 94040 sales@hytrust.com | www.hytrust.com Phone: 650-681-8100