Datasheet

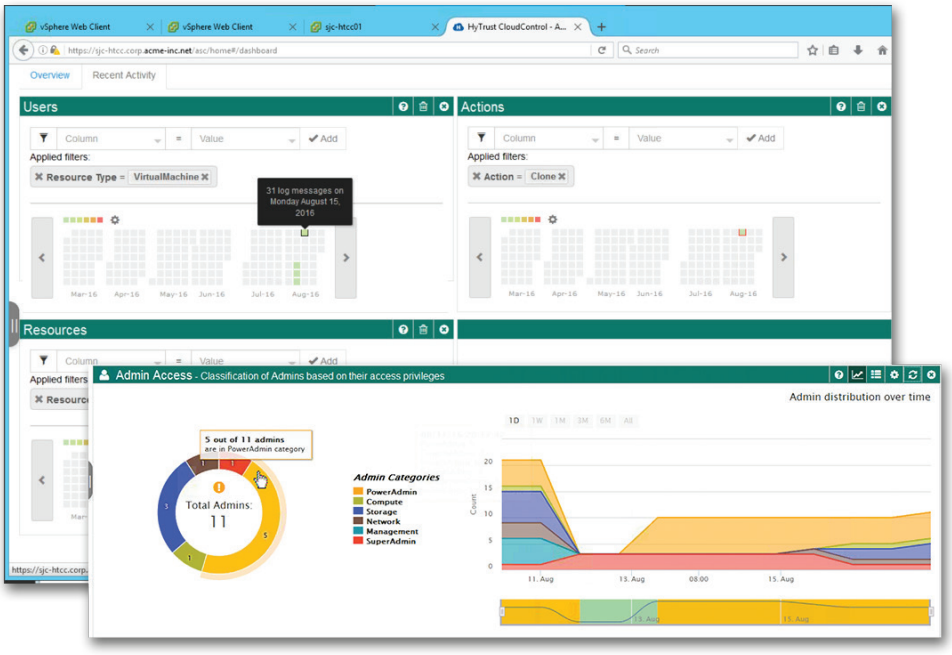
HyTrust CloudControl

Security, compliance, and control for virtual infrastructure

Introduction

Virtualization provides efficiency, flexibility, and cost savings. The average cost of a virtualized breach is $800,000—double the cost of a non-virtualized breach. Additional compliance mandates on virtualized infrastructure mean increased operational burden for virtual infrastructure administrators. Furthermore, such security and compliance concerns can limit further virtualization. In some cases, air-gapped hardware based on admin roles (network, server, etc.) or data classification (e.g. PCI, Top Secret, etc.) is used—reducing efficiency and increasing costs.

HyTrust CloudControl provides automated protection and compliance to allow hyper-convergence of virtual workloads on the smallest datacenter footprint all while minimizing time and resources associated with security and compliance.



Advanced dashboard provides enhanced visibility

"HyTrust CloudControl **provides automated protection and compliance to allow hyper-convergence of virtual workloads on the smallest datacenter footprint** all while minimizing time and resources associated with security and compliance."

No Gap Visibility

Virtualization should not be an obstacle to visibility nor should it interfere with audit trails. That's why HyTrust CloudControl provides a wide variety of capabilities enabling better visibility into and control over virtualized, private and software-defined data center environments.

- **Forensic level analysis**
  Whether you need to address a compliance violation or a security breach, HyTrust CloudControl provides detailed and user-friendly security posture dashboards that provide deep and rich analytics and trending of privileged user access, compliance status, and level of resource protection. With sophisticated analytical tools, your IT organization will have the ability to clearly understand how an administrative action was performed through the entire lifecycle of a virtual resource.
- **Solid audit trails**
  IT and security operations teams can now speed through compliance audits by leveraging our industry leading forensic level logging and reporting capabilities including heat maps, automatic capture of configuration changes, snapshot views for quick assessments and simplified logging data formats. HyTrust CloudControl also includes built-in integrations with all of the major SIEM vendors, making the process of exporting log data into other systems a matter of just a point and click.

Automated Security and Compliance

Security and compliance are most effective when they are automated and implemented in an "always on" model. Virtualization can challenge this model since VMs can be migrated, different administrator roles can overlap (server and network), and entire infrastructure changes can be executed in a few clicks.

- **Complete stack protection**
  First and foremost, the entire virtual stack must be protected and monitored. With HyTrust CloudControl, enterprises gain the confidence of being able to monitor and protect operating systems and valuable data. With built-in monitoring of security and compliance policies (with over thirty easy to use pre-defined templates), administrators can quickly see and remediate non-compliant activities with a single click. If necessary, administrators can even get a security health check of the VM hypervisor with built in security evaluation measurements. With the administrator's own policy or by leveraging security best practice or compliance templates, an instant check can be done to ensure the entire virtual stack remains protected at all times.
- **Fine-grained access control**
  Through detailed, fine-grained access controls, HyTrust CloudControl provides more control, security, and audit capability above and beyond traditional RBAC (role based access control) systems, including ones that are typically shipped with virtual hypervisors. This ensures that not only do server admins and network administrators stay in their own domains, but also administrators have defined scope. Through password vaulting, encryption (and automatic key management), and other features, these controls enforce administrator scope.
- **Secondary Authorization - The Two Person Rule**
  Many compliance and security best practices dictate that for certain actions, two administrators must mutually sign off on an action. This generally provides compliance with specific EU data directives and also guards against insider misuse. HyTrust CloudControl supports secondary authorization.

HyTrust CloudControl Enables Key Capabilities:

Complete Virtual Stack Protection

- Instant policy based protection for the hypervisor, VM, and data
- Continuous monitoring of hypervisor and VM for security and compliance
- One-click security and compliance remediation on vulnerable VMs

Visibility and Control

- Complete visibility of the entire security state, configurations, administrator actions, and compliance for all VMs running in virtualized, private or Software-Defined Data Centers (SDDC).

- **BoundaryControl Security and Data Sovereignty**
  To address the mobility of VMs, BoundaryControl, a solution enabled by DataControl and CloudControl, provides the ability to geofence VMs such that they can be permitted to only run on specific physical hosts. Leveraging either Intel TXT hardware or, alternatively, software-based tags, BoundaryControl enables you to create rules like "German VMs can only run on hosts located in Germany". Effective for data sovereignty as well as protection against theft of VMs, encryption ensures that VMs and the data they contain can run only on authorized hosts.

Easy to Deploy, Easy to Use

Most administrators have their hands full just keeping up basic infrastructure. With this understanding, HyTrust CloudControl was developed to be very fast to deploy with pre-integrations into VMware's ESXi, NSX and vCloud Air as well as VCE with additional platforms and features to come.

Policy based controls, and automated responses mean that the infrastructure group has minimal touch points with the HyTrust CloudControl system, leaving the security group to add/change policies as they need. And with bulletproof audit trails, no one has to fear an audit that grows in scope!

Authentication required? No worries – HyTrust CloudControl supports, built-in, a range of authentication schemes including TACACS+, Active Directory, RADIUS, Smart Cards (PKI), etc. Two-factor authentication is built-in so administrators don't have to struggle with their hypervisor vendor to try and create a custom solution.

Supported Platforms

- vSphere 5.5, 6.0, 6.5
- NSX 6.2, 6.
- ESXi 5.5, 6.0, 6.5

Supported Authentication Methods

- Active Directory
- RADIUS
- TACACS+
- RSA SecurID

Included Templates

- CIS ESXi, DISA vSphere, ICD 503 ESXi, NIST SP 800-53, PCI-DSS, SOX

Preconfigured Roles

- 26+ including admin, auditor

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.)

20180214-0068