Eliminate Compliance and Security Gaps in Your VMware Infrastructure with HyTrust CloudControl

By Jack Poller, Senior ESG Validation Analyst
July 2018

This ESG Lab Report was commissioned by HyTrust and is distributed under license from ESG.
Contents

Introduction ............................................................................................................................................. 3
Background ............................................................................................................................................... 3
HyTrust CloudControl ............................................................................................................................. 4
ESG Lab Validation ................................................................................................................................. 5
Visibility .................................................................................................................................................. 5
The Voice of the Customer ....................................................................................................................... 7
Control ................................................................................................................................................... 9
The Voice of the Customer ....................................................................................................................... 12
Compliance ............................................................................................................................................. 14
The Voice of the Customer ....................................................................................................................... 15
The Bigger Truth ..................................................................................................................................... 17

ESG Validation Reports

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team’s expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.
Introduction

This ESG Lab Validation report documents hands-on testing of HyTrust CloudControl with a goal of validating how CloudControl closes security gaps and automates compliance for VMware vSphere and NSX virtualized infrastructure.

Background

With the ever-increasing volume and publicity of cybersecurity threats, security teams struggle to improve the security posture of their infrastructure and stay up to date and in compliance with continuously evolving regulatory requirements. This is compounded by the global cybersecurity skills shortage and the technology change brought on by the adoption of cloud and virtualized infrastructures. To mitigate the associated risks, organizations are increasing security budgets and developing dedicated process and controls to improve security posture and efficiency of achieving compliance.

According to ESG research, the most important IT meta-trend is strengthening cybersecurity tools and processes (see Figure 1).¹

![Figure 1. Most Important 2018 IT Meta-trend](image)

The maturation of private cloud infrastructures results in increasing complexity, and maintaining the principles of information security confidentiality, integrity, and availability (CIA) becomes increasingly difficult. Forty-four percent of organizations said that strengthening cybersecurity was the most important business initiative driving spending. Within cybersecurity, 28% said that their organization will make their most significant investment in cloud infrastructure security.²

---

¹ Source: ESG Master Survey Results, 2018 IT Spending Intentions Survey, December 2017.
² ibid.
HyTrust CloudControl

HyTrust designed CloudControl to enhance and improve visibility, control, and compliance in VMware vSphere and NSX environments, strengthening security with privileged admin controls, forensic-level logging and compliance monitoring and hardening. CloudControl acts as the sole entry point for all virtual management actions. Any action taken by a privileged user through any of the management tools provided by VMware is proxied, evaluated, logged, and, if approved, forwarded to vCenter. Because CloudControl is implemented within the vSphere management network and only interacts with user actions, there is no impact on VM performance or network traffic (see Figure 2).

**Figure 2. HyTrust CloudControl in VMware Virtualized Infrastructures**

HyTrust originally designed CloudControl to address the security and compliance gaps that exist in VMware virtualized infrastructures. Organizations deploying CloudControl benefit from:

- **Strong authentication**—CloudControl supports multifactor authentication (MFA) including Duo, Octa, and RSA SecurID, and integrates with RADIUS and TACACS+ for remote authentication and related services for networked access control.

- **Separation of administrative duties**—CloudControl extends VMware’s role-based access controls (RBAC), increasing granularity to support separation of duties in multi-departmental or multi-tenant environments. Roles are fully customizable, and CloudControl includes 20 predefined vSphere roles and six predefined NSX roles.

- **Secondary approval process**—CloudControl enables organizations to add a secondary approval workflow for any action, providing an efficient and flexible way to grant privileged users temporary permissions. The secondary approval process enables greater control over powerful privileges and helps reduce human errors, such as inadvertently deleting or misconfiguring virtual machines.

- **Root password vaulting**—CloudControl generates a temporary root password for an ESXi server. All password transactions are logged, protecting root password integrity and providing an audit trail and accountability of activity.

- **Secure logging**—CloudControl generates granular, user-specific logs in human-readable format for all privileged user activity, including root access. Logs include both failed and successful actions, providing information to understand infrastructure change, detect and remediate security incidents, and implement compliance control activities.

- **Automated compliance process**—CloudControl includes a compliance engine, which automates the compliance checking process, and enables organizations to develop and implement a complete compliance lifecycle process.
ESG Lab Validation

ESG Lab tested HyTrust CloudControl with a focus on visibility, control, and compliance in VMware vSphere and NSX infrastructure. We validated our results with interviews with HyTrust Cloud Control experts and customers.

Visibility

Malicious actors often target privileged accounts, which can be compromised through session hijacking, spear phishing, and other techniques. Organizations limiting risk by implementing the principle of least privileged access—granting the least number of users the least amount of privileges to the least amount of resources, especially sensitive data—need to have visibility regarding each user’s privileges, and what actions each user has taken.

ESG Lab began by exploring the Admin Dashboard, which provides administrators with complete visibility into user privileges over time, as shown in Figure 3. The dashboard provides a high-level summary overview in a graphic form, enabling at-a-glance identification of the number and types of admins, as well as the distribution of admins over time.

We clicked on the admin categories graph, which brought up the detailed list of administrators, including name, group, role, category, and number of operations available to the user. Specific privileges for a role or user were available by clicking to drill down for more information.

The admin dashboard eliminates the effort of manually enumerating each user and her privileges and ensures that the organization can continuously maintain the principle of least privilege.

Figure 3. HyTrust ControlCenter Admin Dashboard

Next, we explored the Log Viewer, as shown in Figure 4. CloudControl maintains a record of every attempted operation. This ensures that administrators have visibility into both who made changes to the environment with successful operations, and what changes were attempted via unsuccessful operations. The log is comprehensive, including the user; his group membership, role, and privileges at the time of the operation; the operation attempted; and the privileges required to complete the operation.
Attempts to change the environment can fail for a variety of reasons, from human error to insufficient privileges; such failures can be indicators of compromise (IOC).

**Figure 4. CloudControl Log Viewer**

![CloudControl Log Viewer](image1)

Source: Enterprise Strategy Group

To aid in forensic investigations, the log viewer can show the state and configuration before and after the requested change, as shown in Figure 5. Using this information can help an investigator determine if an attempted operation is the result of human error, insufficient privileges, or potentially malicious activity.

**Figure 5. CloudControl Log Viewer Prior and Requested Changes**

![CloudControl Log Viewer Prior and Requested Changes](image2)

Source: Enterprise Strategy Group
Next, we examined the **Alert Viewer**, as shown in Figure 6. Administrators can configure CloudControl to send emails for any specific alert type. ASC alerts cover CloudControl operations and include compliance drift, template conflict, and trust status change. A host is considered trusted when CloudControl can verify the software, firmware, and hardware versions and status of a Trusted Platform Module (TPM)-enabled Intel Trusted Execution Technology (TXT) ESXi host. Resource alerts cover the vSphere environment and include critical PCI assets powered off or deleted, denial of service attacks, sensitive workloads moved, and VM/workload sprawl. The alert viewer provided a comprehensive list of every alert, and details were quickly available by highlighting the specific alert. These capabilities can improve the operational efficiency in VMware environments.

**Figure 6. CloudControl Alert Viewer**

![CloudControl Alert Viewer](image)

The **Voice of the Customer**

After reviewing HyTrust CloudControl in a controlled environment, we spoke with a large health care customer to understand how CloudControl works in a real-life scenario.

**Before:** Prior to implementing HyTrust CloudControl, a VMware administrator caused a major outage due to a simple typing error on a common script that lasted for several hours. Unfortunately, the IT management team was unable to trace the root of the problem due to the limited logging and reporting capabilities provided by VMware, which prolonged the outage by several hours.

**After:** By implementing HyTrust CloudControl’s Log Viewer to capture audit-quality logging details, the IT organization was able to view both approved and denied VMware administrator actions, which provided the granularity required to quickly respond to security incidents and outages. They have since been able to trace the root cause of any outage rapidly and respond accordingly—shortening the outage cycle significantly.

The forensic level of detail provided by LogViewer as well as the simple and easy to understand presentation of the information has helped the IT organization accelerate its time-to-resolution as well as the preparation of audit data for compliance reporting requirements.
Why This Matters

Organizations have been inundated with a plethora of endpoint and network security tools promising to protect their IT environments from attack. This can lead to a false sense of security provided by strong perimeter defenses that ignore the potential for harm caused by privileged administrators. Visibility into which users have access to which resources and what actions they take is critical to prevent errant or malicious damage. Obtaining this information in VMware virtualized environments is a challenging and time-consuming manual process.

ESG Lab validated that HyTrust CloudControl provided detailed information about each vSphere and NSX user’s access and privileges. The dashboard views aggregate vital details that can alert administrators to potential problems and enable remediation. All successful and unsuccessful activities are logged, providing an audit trail and information critical for forensic analysis, and alerts are triggered for critical activities, ensuring that administrators and security analysts have knowledge and oversight of any changes to the environment.

For VMware environments, HyTrust CloudControl:

- Reduces the time, resources, and overall costs to maintain a secure and compliant VMware environment.
- Accelerates time to resolution for unplanned outages with detailed logging of approved and denied admin actions.
- Enables tighter controls for privileged administrators, aligned to business needs.
Control

Organizations maintaining the cybersecurity triad of confidentiality, integrity, and availability need to enforce controls on their virtualized infrastructure. To aid this effort, HyTrust CloudControl provides strong authentication and authorization with multi-factor authentication (MFA), separation of admin duties and multi-tenancy with role-based access controls (RBAC), a secondary approval process to prevent admin errors, trusted computing, and superuser account protection with root password vaulting.

CloudControl supports a variety of MFA solutions including Duo, Okta, and RSA SecurID and can integrate with RADIUS and TACACS+ network authentication and authorization systems. ESG Lab used Duo to authenticate and authorize our test users when evaluating CloudControl.

Next, we examined how CloudControl provides granular admin controls that go beyond the basic VMware role-based access controls (RBAC) for better security and improved separation of duties. By default, vSphere supports four roles: Administrator, No Cryptography Administrator, No Access, and Read Only; NSX supports Enterprise Administrator, NSX Administrator, Security Administrator, and Auditor (read only).

CloudControl includes fully customizable roles, expanding VMware’s RBAC with 20 pre-defined vSphere roles and six pre-defined NSX roles. CloudControl’s RBAC system has object-level granularity, controlling access to any virtual resource managed by vCenter or NSX Manager. Custom labels, which are used to classify or categorize policy resources, can be included in RBAC rule definitions, and CloudControl’s pre-canned labels support a broad range of categories such as environment type (e.g., production, development, test, etc.), regulatory standards (e.g., PCI-DSS, NIST, etc.), security levels (e.g., trusted), or tenants. Combining fine-grained role definitions, access controls, labels, and rules enables separation of duties in complex and multi-tenant environments and provides for implementation of the security principle of least privileged access—granting the least amount of access to the smallest number of resources.

As part of our exploration of CloudControl’s RBAC, we examined the rules and constraints configuration, as shown in Figure 7. The rules editor enabled ESG to create new rules and modify existing rules. We created two rules for the Datacenter_Admin_Role, the first limited to hosts tagged with the label NIST, the second limited to hosts tagged with the label PCI, thus creating separate roles to manage PCI- or NIST-compliant hosts. Figure 7 shows the rule constraints for the Datacenter Admin - NIST rule, which requires that network and host labels match NIST.

Figure 7. CloudControl Role-based Access Control Rules and Constraints
Next, we edited the settings for the PCI-VM1 virtual machine. As shown in Figure 8, we attempted to add a network interface to the virtual machine, connecting the network interface to the NIST network. In a traditional vSphere environment, this operation would succeed because the user was granted add network privileges. However, CloudControl’s additional constraints prevented this operation—the VM was using networks with the PCI label, and the new network with the NIST label did not match.

CloudControl’s rules and constraints enabled us to easily restrict roles to operating on specific domains, and to enforce separation of domains and separation of duties, critical when operating in a multi-tenant environment.

**Figure 8. Protection from Crossing Domains**

![Figure 8. Protection from Crossing Domains](https://example.com/image)

Next, we explored how CloudControl’s secondary approval process provides additional controls to protect critical infrastructure from disruptive operations. vSphere and NSX permissions are absolute—users granted permission to execute an operation can execute that operation at any time. There is no mechanism to grant temporary privilege to perform an infrequent task, and there is no method to provide greater control over routine powerful privileges.

With CloudControl’s secondary approval process, a user can be required to obtain additional approval before they can perform sensitive or disruptive operations on specific virtual objects (e.g., delete or power off a VM, modify a firewall, or create an edge services gateway).

When a user attempts an operation requiring secondary approval, CloudControl informs the user that the operation has been blocked and alerts an approver group that a request requires review. Once an approver makes a decision, CloudControl notifies the user, and, if the request is approved, gives the user an approver-defined window of time to execute the operation.

We attempted to power off the PCI-VM3 virtual machine. As shown in Figure 9, CloudControl prevented this action because powering off the VM was protected through the secondary approval process. After our first attempt, an email was sent to the group responsible for approving the action. Clicking on the link in the email brought us to the secondary approval request list. We clicked on the request to see the request details and could approve or deny the request.
CloudControl’s secondary approval process adds security controls for vSphere and NSX environments, providing a workflow protecting critical systems from human error without blocking administrators from routine activities. Using secondary approvals, CloudControl can protect any part of the vSphere or NSX hierarchy from critical or destructive actions such as power cycles, snapshot reversions, VM deletions, or firewall reconfigurations.

Next, using the **Host Viewer**, we examined CloudControl’s trusted computing controls. Trusted computing attempts to ensure that there are no vulnerabilities in the infrastructure stack and relies on hardware components to store a fingerprint of the stack. This fingerprint can be used to verify that the stack has not been altered. By default, CloudControl automatically detects and updates the trust status of all TPM-enabled Intel TXT ESXi hosts on boot and re-verifies trust status daily.

As shown in Figure 10, CloudControl uses a green padlock to indicate hosts that have been trusted computing-verified. Hovering the mouse over the green padlock displayed a popup window providing the details, including the BIOS and VMM version, and the trust verification for the hardware, VMware, and HyTrust.
CloudControl automatically applies a **TRUSTED** label to trusted hosts, and this label can be used to enforce policies, such as critical VMs can only run on trusted hosts, or data can only be decrypted if the VM is running on a trusted host. This enables segregation of workloads and ensures that sensitive workloads only run on trusted hosts with no vulnerabilities.

Next, we examined root password vaulting, a feature that allows CloudControl to manage the root password of individual hosts. As shown in Figure 11, we selected the host **int-esx04.corp.acme-inc.net**, and clicked on **Issue Password**. CloudControl created and set a new random password for the local **root** user on the host. We then used that password to log in to that host using ssh. CloudControl expired the password after a timeout period and generated a new password. Thus, root password vaulting prevents a user from sharing or maintaining long-term root access to a host.

**Figure 11. Root Password Vaulting**

After reviewing HyTrust CloudControl, we spoke with a customer, one of the largest financial services institutions in the United States.

**Before:** An internal vulnerability assessment revealed that the biggest exposure to their security posture was the ability of their more than 1,000 virtual administrators to copy and delete any virtual machine or the entire virtual infrastructure within a matter of minutes. The escalation of administrative privileges due to the lack of access controls within the VMware environment had been an ongoing issue that was rapidly getting out of hand as the community of virtual administrators continued to grow.

**After:** By implementing HyTrust CloudControl’s customizable and granular attribute-based access controls (ABAC) across both their vSphere and NSX environments, the IT management team was able to quickly enforce the separation of administrator duties and the principle of least privileged access. By the time they had completed the deployment of HyTrust CloudControl, the IT management team had successfully “privilege rightsized” the more than 1,000 virtual administrators—putting a stop to the practice of uncontrolled granting of administrator privileges.

The IT organization also implemented secondary approval escalation workflows using CloudControl, enabling IT managers to oversee critical and sensitive operations without impacting VMware administrator productivity. As a result, they were able to effectively transition their virtual infrastructure to a new private cloud environment on time and on budget without compromising security or uptime.
Why This Matters

According to ESG research, more than two-thirds of organizations said their IT environment has become more complex over the last two years.³ Complex environments have large attack surfaces, increasing the security risk.

ESG Lab validated that HyTrust CloudControl, acting as a proxy for all vSphere and NSX administrative operations, only allowed authenticated and authorized users to control the environment. CloudControl expands the basic RBAC provided by VMware with the additional granularity necessary for strict policy compliance and separation of roles, especially in multi-tenant environments. We also validated the utility of additional security controls, including a secondary approval process to prevent errant or malicious destruction of workloads and VMs, enforcement of trusted computing compliance, and root password vaulting.

CloudControl security controls work together to increase security effectiveness, and as an added benefit, improve operational efficiency. This helps minimize the risks of insider threats in complex vSphere and NSX environments with large attack surfaces.

For VMware environments, HyTrust CloudControl:

- Enables necessary security controls and multi-tenant separation that complex VMware environments require, streamlining IT operations and reducing the risk of over-provisioned admin rights.
- Provides automation of security controls to improve operational efficiencies.
- Reduces the attack surface for VMware deployments, especially privileged admins and weak controls.
- Enables rapid deployment of the latest VMware infrastructure innovations without security or compliance gaps.

³ ibid.
Compliance

In addition to self-developed policies to ensure confidentiality, integrity, and availability, many organizations must adhere to external policies such as VMware’s hardening guide, as well as standards including NIST, PCI, HIPAA, and GDPR. Ensuring that every host and network object is in compliance can be an arduous task, especially for large enterprises and service providers with thousands of hosts, network segments, firewalls, switches. As a result, many organizations only check for compliance during a yearly audit cycle; for the remainder of the year, hosts can drift out of compliance.

VMware provides limited compliance checking functionality for vSphere and NSX environments, primarily centered around comparing a host’s configuration against a reference host. This requires manually creating and maintaining references for each compliance standard, and manually running the compliance check against each host in the environment, which is both labor-intensive and time-consuming.

CloudControl enhances vSphere and NSX environments with automated compliance checking, reporting, and remediation. Compliance processes can be scheduled to execute on a regular basis, helping administrators prevent compliance drift. CloudControl provides four compliance processes that can be applied to any object in the environment:

- **Assessment**—compare the object configuration against a reference template
- **Remediation**—modify configuration parameters to match a reference template
- **Rollback to previous**—reset the configuration values to the state prior to the last remediation
- **Revert to initial**—reset the configuration values to the baseline values

Users can customize the default templates provided by CloudControl for VMware hardening, CIS, PCI-DSS, NIST, SOX, and other standards, and can create their own compliance templates. CloudControl maintains a history of compliance testing for automated reporting and auditing.

ESG Lab examined the **Compliance Dashboard**, as shown in Figure 12. Like the admin dashboard, the compliance dashboard shows the current state of compliance and the state of compliance over time. We clicked on the portion of the pie chart representing the hosts out of compliance. This brought up the list of noncompliant hosts, and provided details for the compliance template, when the host was last checked, and the percentage of checks that passed or failed.

**Figure 12. Compliance Dashboard**
Next, we clicked on the host *evo2.testdrive.HyTrust.com*, which brought up the details for that host, as shown in Figure 13. This showed a list of the results for every check in the policy templates *PCI DSS 3.0* and *3.1 ESXi*. Using this list enables an administrator to update the configuration and bring the host into compliance. Auditors can combine the failed checks with the configuration delta information captured in CloudControl logs to determine who made the noncompliant changes to the host.

**Figure 13. Compliance Check Results for a Host**

![Compliance Test Results](image)

*Source: Enterprise Strategy Group*

The **Voice of the Customer**

After reviewing HyTrust CloudControl, we spoke with a large government agency that deployed HyTrust CloudControl for its Virtual Desktop Infrastructure (VDI).

**Before**: The agency’s VDI environment lacked sufficient controls and automation to meet the stringent requirements of a number of government compliance mandates and effectively protect sensitive data.

**After**: The agency deployed HyTrust CloudControl’s configuration hardening functionality in record time across multiple data center VDI installations. Within a very short period, the agency’s IT team was able to markedly reduce the overhead and resources required to perform repetitive compliance tasks and the costs associated with inconsistencies from manual compliance efforts. They were also able to significantly lower the costs of audits and the likelihood of penalties associated with non-compliance.
Why This Matters

In vSphere and NSX environments, organizations must expend time and effort to manually check that their virtual machines comply with security and regulatory policies. This challenge is greater for larger organizations with more complex environments. Organizations often leave compliance checks until their annual audits, allowing users to make noncompliant changes to the environment for the remainder of the year, which increases risk.

ESG Lab validated that HyTrust CloudControl simplifies the security compliance process, automatically checking each object in the environment. Objects are checked daily for compliance with multiple policies, helping to eliminate compliance drift. The results are shown on a dashboard, providing administrators and auditors up-to-date compliance status. Investigators can quickly determine reasons for noncompliance, and which users made noncompliant changes to configurations, enabling remediation and process changes to prevent future drift.

For VMware environments, HyTrust CloudControl:

- Reduces the cost and resources required to achieve compliance across VMware deployments.
- Automates redundant tasks, preventing downtime from errors and inconsistencies, enabling resources to focus on other mission-critical tasks.
- Achieves ongoing continuous compliance and lowers the risk and exposure of penalties and incremental IT tasks due to non-compliance.
The Bigger Truth

More than half of organizations report that they have a problematic shortage of cybersecurity skills, according to ESG research, challenging organizations to maintain or improve their security posture as they build ever larger and more complex virtualization infrastructures. This, along with the adoption of new cloud infrastructures, makes automation of security and compliance tasks for private and public cloud infrastructure increasingly important.

HyTrust initially designed CloudControl to enhance and improve visibility, control, and compliance in VMware vSphere and NSX environments, strengthening security with privileged admin controls, forensic-level logging, and compliance monitoring and hardening.

ESG Lab confirmed HyTrust CloudControl automates many manual processes, providing critical data in easy-to-use dashboards and eliminating the time and effort associated with security and compliance tasks. CloudControl aggregates user privileges and actions, providing administrators with knowledge and oversight of changes to the virtualization environment. Automation extends to running daily compliance checks, effectively eliminating compliance drift over time, and providing audit trails and forensics for remediation.

Fine-grained visibility and controls go beyond the basic VMware RBAC capabilities to provide the granularity necessary for separation of roles, especially in multi-department and multi-tenant environments. CloudControl provides additional controls supporting multi-factor authentication, root password vaulting, and a secondary approval process to prevent human error or malicious activity from destroying critical workloads, virtual machines, or networks.

A Hytrust customer summed it up well when he said, “We’re no longer concerned about significant outages cutting into the bottom-line. And with the ability to complete audits more quickly, we’re avoiding potential fines and other consequences of noncompliance.” Another customer stated, “With HyTrust, we don’t have to worry about an administrator inadvertently shutting down a critical virtual machine and interrupting our business, nor do we have to worry about a rogue insider exporting or deleting VMs.”

ESG Lab recommends that organizations with large or complex vSphere and NSX environments take a close look at how implementing HyTrust CloudControl can expand the capabilities provided by VMware with the needed capabilities to strengthen security and automate compliance to enhance their environment and have an immediate beneficial impact reducing their cybersecurity risk.

---

4 ibid.