The HyTrust CloudControl Solution

Today the boundary of the data center continues to be redefined and the Software Defined Data Center (SDDC) has clearly emerged as the next evolutionary step in cloud computing. Regardless of size or industry, organizations are adopting the SDDC vision into the roadmap for their next generation data center. Yet, despite its phenomenal growth, many IT organizations struggle to make the transition from virtualization to the SDDC, due to a multitude of challenges around security and compliance.

HyTrust empowers organizations to fully leverage their investment in the SDDC and overcome these challenges by delivering a unique and powerful set of controls for privileged user access, visibility and configuration policy and hardening. Specifically, HyTrust CloudControl (HTCC) was designed from the ground up to address the security and compliance gaps that exist in the virtual environment and is now the standard for policy-based access controls, enforcement and automated compliance for the virtual environment and SDDC.

The HTCC solution provides a robust set of capabilities, including granular Role-Based Access Controls (RBAC), Object-Based Access Controls (OBAC), Secondary Approval, Audit Quality Logging, Root Password Vaulting (RPV), Hypervisor Configuration Hardening, and Two-Factor Authentication (2FA). HTCC also includes visually appealing, user-friendly, and detailed management dashboards that can help organizations understand how privileged users’ actions were performed throughout the entire lifecycle of a virtual object.

**HyTrust CloudControl Architecture Overview**

HTCC is a virtual appliance deployed as a transparent proxy that allows for a single-entry point and non-intrusive application of security controls to all virtual user actions. Fundamentally, any action that is issued by a privileged user, through any of the management tools provided by VMware, is proxied, evaluated, logged, and forwarded to vCenter (if approved). The advantage of HTCC is that because it 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 1).

**HTCC Transparent Proxy**

The HTCC Transparent Proxy acts as a central point of control, seamlessly intercepting, monitoring, enforcing, and logging all privileged user requests originating from a variety of access mechanisms, including the vSphere Client, vSphere Web Client, vSphere HTML5 Web Client, and SSH. The HTCC proxy appliance can also be deployed in active-passive pairs so that if the primary (active) appliance fails, the secondary (passive) appliance takes over the network identity and serves as the primary HTCC appliance.

1. **HTCC Policy Engine**

   The HTCC Policy Engine is the enforcement mechanism that enables organizations to implement security best practices such as “separation of duties” policies that keep...
privileged users in their swim lanes or the implementation of the "principal of least-privilege access" which allows organizations to create secure multi-tenant private cloud environments. In either scenario, the HTCC Policy Engine allows organizations to control (through total customization) which privileged user roles can perform what operations on which objects in the virtual environment.

The HTCC Policy Engine also provides the ability to apply constraints, thereby, enabling organizations to limit privileged user access to objects with or without a certain label (e.g. PCI-DSS) or restrict privileged user access from a single or range of IP addresses, etc. This critical functionality allows organizations to logically segment their virtual and cloud environments by any defined boundary they choose, such as application type, regulatory standard, level of criticality, geography, data center, department, etc.

Role-Based Access Controls (RBAC)
The HTCC Role-Based Access Control (RBAC) capability encompasses five key elements: 1. Objects, 2. Groups, 3. Roles, 4. Labels and 5. Rules. Objects are defined as any virtual resource that falls under vCenter or the NSX management system such as

"HTCC delivers fully customizable roles, including 20 pre-defined vSphere roles and six pre-defined NSX roles. The ability to define roles at such a granular level enables organizations to enforce and maintain the 'separation of duties' between different areas of responsibility within an IT organization."

Figure 1: vSphere/NSX Architecture with HyTrust CloudControl

Figure 2: HyTrust CloudControl Architecture
virtual machines, PortGroups, virtual switches, ESXi hosts etc. Groups are defined in Active Directory (AD) and are made up of users who belong to one or more groups.

– **Roles**

Roles are a collection of privileges or permissions that define authorized operations, usually defined along the same lines as roles or duties that users perform within an organization. Roles are defined within HTCC; but the privileges are mapped to specific vSphere or NSX operations. For example, the “VirtualMachine.Interact.PowerOn” privilege is mapped to the “power on VM” operation in vSphere. This privilege can belong to one or more roles, such as the “ASC_VMPowerUser” and/or the “ASC_SuperAdmin.”

HTCC delivers fully customizable roles, including 20 pre-defined vSphere roles and six pre-defined NSX roles. The ability to define roles at such a granular level enables organizations to enforce and maintain the “separation of duties” between different areas of responsibility within an IT organization. For example, vSphere administrator, NSX administrator, and storage administrator may be separated into roles so that each group may only perform actions on objects assigned to their groups.

– **Labels**

Labels are used to classify or categorize policy resources. Labels are useful when defining rule constraints or restrictions. For example, virtual machines can be constrained or restricted to start only on the hosts with a specific label (e.g. production, PCI-DSS). HTCC includes fully customizable and pre-canned labels that support a broad range of categories, including but not limited to environment types (e.g. PROD), regulatory standards (e.g. PCI-DSS), and security levels (TRUSTED), etc.

– **Rules**

Rules are relationships between user groups, objects, and entitled operations for a specific role and label. A rule must have an object, group, and role, however, labels are optional and may be used to further control access to objects. For example, if virtual administrators are given full rights to all virtual machines the “rule” would grant ASC_SuperAdmin to VirtualAdministrators on all virtual machines. To take this example further, if “Kevin” is the user and he tries to power on a virtual machine, the HTCC Policy Engine will check the following: Is “Kevin” a member of the group “VirtualAdministrators” in Active Directory? Is the operation “PowerOnVM” permitted in the “ASC_SuperAdmin” role? What object is “Kevin” performing the operation “PowerOnVM” on? Is this object associated with the rule? If all answers are yes, the HTCC rule authorizes the operation.

As mentioned, with HTCC, organizations can build constraints into the rule. For example, if “VirtualAdministrators” are given full rights to all virtual machines unless the virtual machine is labeled “SPECIAL,” the “rule” would grant ASC_SuperAdmin to VirtualAdministrators on all virtual machines unless LABEL = SPECIAL. Using the example from above, if the user “Kevin” tries to power on a virtual machine that is labeled “SPECIAL,” the HTCC policy engine will check the following: Is “Kevin” a member of the group “VirtualAdministrators” in Active Directory? Is the operation “PowerOnVM” permitted in the “ASC_SuperAdmin” role? Is the object associated with the rule? Does the VM have a label that matches the constraint? If all answers are yes, the operation will be denied based on the constraint of excluding a VM by a label (see Figure 3).

**Secondary Approval Workflows**

Beyond RBAC, most organizations also require an efficient and flexible way to: 1) grant privileged users temporary permissions needed to perform infrequent job duties, and 2) have greater control over the use of powerful privileges by users who need those...
privileges to do their daily jobs. For example, a virtualization operations group needs ongoing authorization to create and delete VMs used for non-production applications, but management also wants the ability to approve or deny any attempt by this group to delete a production virtual machine.

Because the VMware platform does not provide a viable way to enable one-time approval of a specific operation attempted by a specific privileged user, organizations have turned to HTCC’s Secondary Approval capability for both vSphere and NSX operations. From a workflow perspective, this feature allows authorized users to configure HTCC to require additional approval before privileged users can perform sensitive or disruptive operations on specific virtual objects (e.g., delete or power off a virtual machine, edit a firewall or create an edge services gateway). The process requires that a designated group of approvers authorize an operation attempted by a privileged user before that operation can proceed.

The workflow is simple and efficient, making it easy for operations groups to implement. It begins when a privileged user attempts an operation requiring secondary approval in accordance with the organization’s policy. HTCC blocks execution and informs the privileged user that a secondary approval has been requested for the operation. HTCC simultaneously alerts an approver group that a request requires review, and provides the details of the request. Once the approver makes the decision, HTCC notifies the privileged user and, if the request is approved, gives the privileged user an approver-defined window of time in which to execute the approved operation.

**Separation of Duties Dashboard**

The HTCC Separation of Duties dashboard provides current and trending data regarding the distribution of privileged user access throughout the virtual environment. Organizations can view the number of privileged users per category (categories are based on privileges) to get a better understanding of whether users have more privileges than necessary to perform their jobs or if privileged user access has changed over time. Having quick access to this information can help organizations redistribute roles and privileges in accordance with security best practices and prevent privilege creep in the future (see Figure 4).

**2. HTCC Logging Engine**

A solid audit trail of privileged user activity is necessary to understand infrastructure change, implement numerous compliance control activities, and to detect and remediate security incidents. A good log will reveal exactly what was done or attempted, by whom, from where, and when. Logging privileged user activity is important, because privileged users have far greater capabilities than other users and can perform a wide
variety of potentially risky activities, such as shutting down or otherwise disrupting critical applications, bypassing access controls to copy or corrupt sensitive data, or tampering with or deleting log data.

For these reasons, privileged accounts are commonly the target of malware and advanced persistent threats. An attacker that can obtain privileged user credentials through session hijacking or spear phishing immediately gains the perfect vector to deposit a malware payload into the infrastructure. It should be clear, therefore, that not only does the privileged user activity need to be logged, it must be logged in such a way that the privileged user credentials cannot be used to tamper with the logs.

Despite the clear need for robust logging, many IT systems do not provide this capability. Often the system does not log all events that may be important or required to support security best practices and compliance. For example, a system may log all approved logins, but will not capture denied login attempts. In some cases, the data within the log entry may also be lacking. The entry may contain the obvious elements, like the system name and address and the timestamp, but no other critical information such as exactly which change was performed on what object.

It should be noted that, contrary to popular belief, the log collection systems and SIEMs do not help solve the problem because these products consume log data; they do not create it on behalf of the mentioned system. If an IT system does not send the SIEM log information with a sufficient level of detail, the SIEM cannot possibly compensate for the deficiency, because it has no insight about what is going on within the IT system. It’s only as good as the log data being sent to it. HTCC solves this problem by logging every single privileged user action performed, without affecting application availability or performance. The HTCC Logging Engine generates granular, user-specific logs in human-readable form for all privileged user activity, including root access.

HTCC’s logging functionality also allows organizations to capture attempted actions that have been denied by security policy, which significantly improves visibility and detection of anomalies in a virtualized or cloud environment. In contrast, privileged user actions that are attempted but denied are never captured or logged with vCenter’s native logging function. Additionally, the HTCC Logging Engine seamlessly pushes log entries to most log analysis/SIEM tools via a standard syslog format or Common Event Format (CEF), allowing IT organizations to easily leverage existing log management and alerting operational processes (see Figure 5).
HTCC Log Viewer
For every administrative action and event, detailed information about the operation performed and changes made to the environment are presented in the HTCC Log Viewer. For example, if a privileged user deleted a virtual hard drive from a virtual machine, the HTCC Log Viewer would provide detailed information about the specific hard drive that was deleted. What’s more, it will also provide the delta of change(s) that occurred.

To help IT teams rationalize the amount of information captured in the HTCC logs, a graphical depiction of key risk metrics is conveyed through visual heatmaps. The customizable heatmap shows daily activity by representing the # of logs on a particular day with a colored square corresponding to high or low activity (see Figure 6).

3. HTCC Compliance Engine
Security and compliance are most effective when they are automated and implemented in an always-on model. However, virtualization challenges this model since VMs can be migrated, different privileged user roles can overlap, and entire infrastructure changes can be executed in just a few clicks. Further, with all aspects of infrastructure (compute, network, storage) being virtualized, privileged user power is now heavily concentrated at the hypervisor layer, which introduces a whole new set of security and compliance challenges.

"Hypervisor configuration can easily drift over time. Having an automated process for tracking these changes and remediating when needed helps organizations maintain compliance."
Hypervisor configuration can easily drift over time. Having an automated process for tracking these changes and remediating when needed helps organizations maintain compliance. Unfortunately, solutions for keeping the hypervisor secure and compliant has remained relatively stagnant over the years. As a result, most organizations continue to rely on costly, time-consuming, and error-prone manual processes, which simply can’t keep up with the constantly changing threat landscape and regulatory environment.

The HTCC approach to protecting virtual infrastructure is different, because the focus is on automation for each phase of the compliance lifecycle. HyTrust provides compliance templates for various regulatory and government standards (e.g. PCI-DSS, HIPAA, DISA), as well as industry best practice guidelines (e.g. VMW hardening guide). These templates assist in creating an accepted baseline configuration for virtual infrastructures, which can be leveraged to automate the assessment, remediation, and continuous monitoring of the organization’s virtual security posture. HyTrust uses a four-phase lifecycle approach to achieve and maintain compliance in the virtual environment.

**HTCC Compliance Lifecycle Process**

– **Phase 1: Defining ESXi Configuration Standards**
  The first phase is about determining which standard or custom templates (a collection of host configuration parameters and their defined correct values) will be applied to perform the compliance configuration assessment on both the ESXi host and the VM container. There are two types of templates: 1) system templates and 2) custom templates. System templates are pre-packaged templates installed automatically with the appliance, such as PCI-DSS, HIPAA, NIST, which are provided as a starting point to help meet an organization’s compliance requirements. Customizable templates are available for organizations that prefer to customize compliance templates to align more closely with their security and operational requirements.

– **Phase 2: Assessing the Virtual Infrastructure**
  The second phase of the compliance lifecycle is the assessment—the process of running operations or tests on the host to compare the parameter value specified in the template with the actual value configured on the host. Compliance template operations on the protected hosts can occur as scheduled events or ad hoc. Ad hoc operations are performed immediately, whereas scheduled operations are performed at a specified date and time in the future.

  A compliance check is considered “failed” when the configured value is different from the value specified in the template. HTCC presents assessment results in the form of a compliance percentage. The compliance percentage of an assessment is calculated by dividing the number of successful operations (e.g. the configured value matched the desired value in the template) by the total number of operations run against the host. For example, if 50 parameter values in a template are assessed against the configured values on a host and 40 pass (the values match the template), the compliance percentage of that assessment is 80 percent.

– **Phase 3: Remediating the Virtual Infrastructure**
  The third phase of the compliance lifecycle is the remediation phase. HTCC is also able to perform remediation operations to bring the virtual infrastructure back into compliance. Remediation modifies parameter values on the ESXi hosts based on the desired values defined in templates (in contrast to assessment, which evaluates, but does not change values). A remediation action will first run the assessment operation
against the target host. If the assessment operation fails, HTCC will modify the host parameter value(s) to match the value(s) defined in the template.

**Phase 4: Refining the Configuration Standard**
The fourth phase of the compliance lifecycle allows organizations to review past compliance reports, modify security controls, and update their customized templates to reflect changes in the organization’s security posture. Further, HTCC includes ongoing updates to system templates to reflect the latest regulatory standard changes.

**Compliance Dashboard**
Users can view the current and trending state of the virtual infrastructure host's compliance in regards to the currently enforced templates. A template is enforced if it is associated with a host’s last compliance event (either assessment or remediation). The current state of compliance is represented by the number of hosts that are in compliance with an enforced template, out of compliance with an enforced template, or have not been assessed yet (see Figure 7).

**Root Password Vaulting (RPV)**
HTCC provides a root password vaulting capability to protect the integrity of the root account and provide an audit trail for those occasional situations when root access is required to perform specific actions or troubleshoot activities on ESXi servers. Because the management of root passwords is critical from both an operational and security perspective, HTCC owns the root password of every host under its protection. When a privileged user requests root access through HTCC, a root password is randomly generated at the time of request and an expiration time is set (e.g. valid for two hours). Once the root password expires, HTCC automatically generates a new root password and executes the password change on the ESXi host. All password transactions are logged by the HTCC Logging Engine for future audits and reporting (see Figure 8).

**Figure 7: Compliance Dashboard**

account and provide an audit trail for those occasional situations when root access is required to perform specific actions or troubleshoot activities on ESXi servers. Because the management of root passwords is critical from both an operational and security perspective, HTCC owns the root password of every host under its protection. When a privileged user requests root access through HTCC, a root password is randomly generated at the time of request and an expiration time is set (e.g. valid for two hours). Once the root password expires, HTCC automatically generates a new root password and executes the password change on the ESXi host. All password transactions are logged by the HTCC Logging Engine for future audits and reporting (see Figure 8).

**4. HTCC Authentication Engine**
The HTCC Authentication Engine provides an extra layer of security along with the usual username and password by validating privileged user access requests made through the HTCC Transparent Proxy using Active Directory or by leveraging 2FA solutions that already exist in the customer environment, such as RSA SecureID, RADIUS-based authentication, or TACACS+ (see Figure 9).
Alerts
The HTCC alert feature provides a method to receive immediate notifications based on the operations performed by privileged users or by HTCC itself. When HTCC or a privileged user performs an operation matching an alert, the appliance generates that particular alert. If configured, an email with the activity details is sent to the user. Apart from the built-in alerts, users can also customize and add alerts for any role, label, resource type, or operation. There are two key types of alerts in HTCC: 1) host configuration and 2) user actions or virtual object events.

Host configuration based alerts are generated when there are changes to the host, such as the security configuration of a host drifting below a customizable compliance threshold. Secondly, alerts can be triggered when the trust status of any protected host changes, such as a BIOS update (planned or malicious) or hypervisor version change. This feature leverages Intel’s Trusted Execution Technology (TXT).
Privileged user action based alerts are generated when an event or series of events happens. Alerts are flexible and customizable to instantly warn of VM sprawl, attempted and denied actions, possible denial of service attacks against hosts, or only when an interaction occurs with a specific/critical virtual object. For example, an alert could be generated when a VM is (or action is attempted) powered off, deleted, or cloned.

Trust Attestation Service (TAS)
TAS is a HTCC feature that leverages Intel TXT to establish comprehensive hardware-based trust on managed ESXi hosts. A feature of the Intel Xeon processor, Intel TXT establishes a root of trust through measurements when the hardware and pre-launch software components are in a known good state. Once the organization knows which hosts can be trusted, HTCC can be leveraged to group those hosts into trusted compute pools. For example, organizations can now apply policies to VMs so that different sensitive VMs run only on specific, trusted servers in specific trusted groups.

About HyTrust
HyTrust’s mission is to make private, public, and hybrid cloud infrastructure more secure for enterprises, service providers, and government agencies. HyTrust provides solutions that automate security controls for software-defined computing, networking, and storage workloads to achieve the highest levels of visibility, granular policy control, and data protection. HyTrust customers benefit from being able to fully realize the cost savings associated with virtualization and cloud technologies without sacrificing their security posture by automating and enforcing security policies in real time, adapting quickly to compliance requirements, and minimizing disruption to their business.

Headquartered in Mountain View, CA, HyTrust is backed by the leading providers of strategic IT infrastructure, including VMware, Cisco, Intel, and Fortinet; by the vanguard of innovative solutions for the intelligence community, In-Q-Tel; and by a world-class group of financial investors, including AIT Ventures, Granite Ventures, Trident Capital, and Vanedge Capital. HyTrust was recently named one of CRN’s “20 Coolest Cloud Security Vendors,” a recipient of VMworld’s 2015 Gold Award for Security/Compliance and Virtualization, and the Most Innovative Cloud Company at Intel Security Focus 2015.

For More Information
Contact HyTrust at 1-844-681-8100 to discuss your cloud security requirements or to schedule a demonstration.