HYTRUST
Cloud Under Control

Solution Brief

Preventing Insider Threats with HyTrust's "Two-Person Rule"

Executive overview

The exposure of extremely confidential national security information by an N.S.A. systems administrator highlighted the catastrophic consequences of inadequate monitoring and access controls. Enterprises that virtualize mission critical applications and data without addressing this issue leave themselves open to similarly devastating outcomes. Securing VMware privileged user access to Tier 1 virtual machines is now viewed as essential; the challenge is controlling administrative access while maintaining user productivity.

The N.S.A. response to the Snowden breach includes closely monitoring privileged user activity and implementing the "two person rule" to stop rogue operations. HyTrust CloudControl™ enforces the two man rule for administrators in virtualized infrastructures, adding a critical layer of security to protect sensitive operations, in addition to providing real time, role-based monitoring and granular access controls. HyTrust's Secondary Approval automated workflow enables oversight of high impact administrative operations while keeping users productive and compliant with regulations.

HyTrust - Cloud Under Control

HyTrust has become the de facto standard for access control, logging, and policy enforcement in VMware environments. By filling gaps in virtual infrastructure security and compliance, HyTrust gives enterprises the assurance they need to virtualize their mission critical applications, implement private clouds, pass security audits, and reap the financial benefits of increased virtualization. HyTrust CloudControl enforces role-based and asset-based policies covering VMware privileged users, virtual resources, and management interfaces. It also secures the vSphere platform and virtualized workloads by providing virtual network segmentation; comprehensive, audit-quality access logs; strong authentication; and virtual infrastructure hardening. HyTrust DataControl™ provides strong encryption and integrated key management for virtual machines from the time they are created until they are securely decommissioned.

Your challenge

An N.S.A. systems administrator believed to be trustworthy dealt a devastating blow to U.S intelligence gathering, anti-terrorism efforts, and diplomatic relations. He gained access to some of the United States' most secret national intelligence, copied it, and provided it to both international media and the Chinese and Russian intelligence services. And he did this despite working as a contractor for one of the most security-conscious organizations in the world.

No enterprise with critical systems or data is immune to such an insider attack. Yet most enterprises are as vulnerable as the N.S.A. was, even though implementing two fundamental security measures can greatly mitigate the risk. A privileged user can't execute a successful attack if his administrative operations are continuously monitored and his access to sensitive information is strictly limited to need-to-know and need-to-manage.

Solutions to monitor privileged operations and control access to individual servers and applications have existed for years. However, administrators of the VMware virtualization platform typically have much greater administrative power than their counterparts who manage physical data center infrastructure. A single vSphere administrator can copy, power off, or delete hundreds or thousands of virtual machines (VMs) that host production applications – accidentally or intentionally – with a few clicks. The threat from this concentration of risk is not limited to national intelligence agencies. Highly publicized breaches at corporations including Gucci and pharmaceutical maker Shionogi - in which vSphere users destroyed production data center resources through a vSphere management interface - demonstrate that the risks are universal.

HyTrust access control policies based on "always on" rules provide very effective protection for critical applications and data in VMs. At the same time, data centers often want an efficient way to grant VMware users temporary administrative privileges needed to perform infrequent job duties. In other situations, managers want greater control over the use of powerful privileges by users who need those privileges to do their jobs every day.

Examples of these situations include:

- A contractor occasionally clones the virtual machine (VM) that hosts the enterprise email server in order to test patches and upgrades. The enterprise wants to ensure that the contractor cannot clone the VM for any other reason.

- A group of vSphere users conducts monthly scheduled reboots of VMs that run production workloads. Management wants to enable the reboots each month without having to approve exceptions, but also wants to require one-time approval for all other VM power-off and power-on operations.

- A virtualization operations group needs ongoing authorization to create and delete VMs used for non-production applications. However, their manager wants the ability to approve or deny any attempt to delete a production VM.

- An attacker may be able to compromise a vCenter user's log-in credentials via a sophisticated phishing exploit. With the authorized user's privileges, the attacker can copy critical data or suspend a security appliance in order to perpetrate other damage. The enterprise wants a way to prevent this scenario without reducing the operations team's productivity.

The VMware platform does not provide a viable way to enable one-time authorization of a particular operation attempted by a particular user. Consequently, many enterprises have been hesitant to virtualize their critical workloads and have missed the economic gains available from greater virtualization.

The HyTrust solution

Following the Snowden breach, the director of the N.S.A. said his agency would institute a "two-man rule" to limit the ability of each of its 1,000 system administrators to gain unfettered access to the entire infrastructure. The New York Times reported that "the rule, which would require a second check on each attempt to access sensitive

information, is already in place in some intelligence agencies ... in effect, two sets of keys are required to unlock a safe." ("N.S.A. Leak Puts Focus on System Administration", June 24, 2013).

The two-man rule is an implementation of the adage "trust but verify". It has been applied for years in situations and environments where a rogue privileged user acting alone could cause great damage. For example, according to US Air Force Instruction (AFI) 91-104, the two- person rule is designed to prevent accidental or malicious launch of nuclear weapons by a single individual.

HyTrust CloudControl enables efficient implementation of the two-man rule in virtualized environments. The automated Secondary Approval process available with HyTrust CloudControl requires that a designated approver authorize an administrative operation attempted by a privileged user before the VMware platform allows the operation to proceed.

The workflow is simple and efficient, making it easy for operations groups to implement. It begins when a user attempts a VMware platform operation requiring authorization, in accordance with data center policy. HyTrust CloudControl blocks execution and tells the user that Secondary Approval has been requested for the operation. HyTrust CloudControl simultaneously alerts an approver group that a user request requires review, and it provides the details of the request. When an approver makes a decision, CloudControl notifies the user and – if the request is approved - gives the user an approver-defined window of time in which to execute the approved operation.

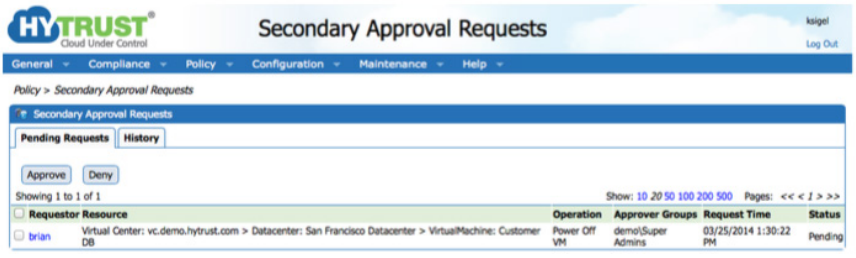
Applying Secondary Approval to the following use cases illustrate its value:

- Attempts by the contractor to clone the email server VM are blocked until an approver grants permission. When a patch or upgrade has been scheduled, the approver gives the contractor a limited period of time in which to clone the VM.

- Outside of scheduled monthly reboot times, a vSphere user's attempt to reboot a production workload triggers the Secondary Approval process. A manager toggles off the rule each month while vSphere users reboot the appropriate VMs.

- Virtualization operations team members are able to create or delete a production VM only when a manager authorizes the request in HyTrust.

An attacker's attempt to use stolen log-in credentials to conduct a damaging operation is blocked, logged, and immediately reported to secondary approvers.



Approvers review the details of an attempted VMware operation and approve or deny it in seconds within a browser-based management dashboard

The HyTrust CloudControl "two person rule" workflow is not available from the VMware platform or any other source. By deploying HyTrust CloudControl with Secondary Approval, IT organizations take an essential step toward virtualizing their critical workloads and increasing their virtualization ROI without sacrificing security, compliance, or productivity.

For more information on how HyTrust enables greater virtualization of workloads that must stay compliant, visit www.hytrust.com, email questions to sales@hytrust.com, or call HyTrust at 650-681-8100 for a free consultation.

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