Many organizations that are running mission-critical systems in highly virtualized private, public and hybrid clouds struggle to maintain a consistent method for assessing and remediating against industry best-practices for configuration or security management standards. Standards like VMware’s hardening guide(s), CIS Benchmarks, DISA STIGs, and even basic VMware host profiles are becoming an increasingly visible part of the industry movement of being able to call your enterprise “compliant.” Although “compliance” often doesn’t fall on the shoulders of virtual admins, configuration and security management squarely does. To further complicate this issue, it’s not always clear where security configuration management stops, and compliance starts. We see in the market that the dichotomy of configuration and security management and compliance adherence are becoming a single administrative function. This fact is becoming more apparent as we see compliance standards that are commonly derived from the hardening guidelines. For instance, take the VMware hardening guide. In recent years not only has it been renamed to the VMware Security Hardening Guide, but it’s also the basis for the latest guidance of NIST 800-53 for vSphere & NSX configuration and security management.

Automated, Continuous Assessment and Remediation
Many IT organizations use a mix of manual or semi-manual processes and procedures via scripts or point solutions to harden and secure the configuration of critical systems. However, as IT organizations continue to span infrastructure across dynamic, on-premises virtualized and cloud environments, it’s not going to get any easier. Implementing a solution that provides continuous monitoring and automated remediation of IT processes to support compliance efforts will provide significant benefits, mainly when operating at scale. Organizations can reduce compliance-related costs and minimize the attack surface of virtualized and cloud platforms considerably by implementing a solution that mandates frequent, ongoing testing, automated remediation, and reporting of IT systems.

"Costly resource intensive compliance requirements can be virtually eliminated with a continuous compliance solution.”

![Image: Benefits of Compliance Automation]

**Operational Cost Reduction**
- Reduce the cost of existing manual security controls
- Reduce resource overhead of repetitive tasks
- Reduce costs associated with manual task inconsistency

**Compliance Cost Reduction**
- Lower the cost of audits
- Reduce the likelihood of fines and penalties
- Avoid costs associated with multiple resources assigned to time intensive tasks

**Risk Reduction**
- Reduce the overall attack surface risk
- Reduce the risk of critical loss or compromise
- Reduce risk of incurring costs due to human error

**Process Improvement**
- Increase effectiveness and visibility of compliance initiatives
- Decrease time and increase reliability of task completion
- Increase leadership confidence in compliance activities

**Figure 1** - Organizations can streamline compliance efforts and reduce ROI by automating critical security processes and procedures.
Security Configuration Management - Simplified
Using HyTrust CloudControl can significantly improve an organization’s ability to identify, remediate, and report on configuration and security management drift. These capabilities lead to increasing visibility and decreasing the risk of misconfiguration, which can lead to unintended downtime or security exposure. Another added benefit of automation is improved personnel utilization and process optimization, which reduces operational costs while significantly increasing return on investment (ROI).

HyTrust CloudControl provides a solution that adheres to industry best-practices and compliance frameworks such as NIST 800-53, CIS Benchmark, PCI, DISA STIG, HIPAA, and customized requirements. CloudControl also provides frequent ongoing testing, automated remediation, and reporting of IT systems. These capabilities make it easy to view the overall compliance posture of your environment.

“Using a solution such as HyTrust CloudControl can significantly improve an organization’s ability to respond to, identify, remediate, and report on security configuration and compliance drift.”

Security Configuration Management and Compliance with HyTrust CloudControl
- Unified Visibility: Search, tag, inventory, and manage your vSphere infrastructure to understand your overall compliance posture.
- Security Configuration Hardening: Ensures your vSphere environments are configured according to industry security best practices to minimize risk.
- Security Configuration Hardening Templates: Use pre-defined templates based on the most common standards and frameworks such as NIST 800-53, PCI-DSS, and DISA STIG or create a custom template to meet your needs.
- Continuous Compliance: Continuously assess your infrastructure for configuration drift and remediate on a scheduled basis while also providing automatic remediation.

Figure 2 - HyTrust’s global compliance dashboard shows compliance status across a multi-cloud (AWS, Containers, VMware) environment.
Summary

Security configuration management and compliance automation enable commercial and government organizations to optimize their usage of virtualized and cloud environments while meeting the necessary operational and regulatory standards that ensure workload and data security. Using HyTrust CloudControl, IT security practitioners can effectively bridge the capability gaps found in cloud platforms to significantly reduce capital expenditure on legacy data center infrastructure, streamline resources, prove security and compliance, and assure a significant return on investment (ROI).

Figure 3 - View an assessment report and understand the details behind the report.