



Scaling Security Configuration Assessment and Remediation

Mitigating risk and achieving security management nirvana with Entrust CloudControl



ENTRUST

SECURING A WORLD IN MOTION

Introduction

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 of security management standards. Standards like VMware's hardening guide(s), Center for Internet Security (CIS) Benchmarks, Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs), and even basic VMware host profiles are central to the growing need to define your enterprise as "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. Rather, these two elements are increasingly combined in a single administrative function. This line-blurring stems, in part, from compliance standards that are frequently derived from the hardening guidelines. For instance, the VMware hardening guide has recently been renamed the VMware Security Hardening Guide - and is now also the basis for the latest guidance of National Institute of Standards and Technology (NIST) 800-53 for vSphere and NSX configuration and security management.



**COSTLY COMPLIANCE
REQUIREMENTS CAN BE
VIRTUALLY ELIMINATED
WITH A CONTINUOUS
COMPLIANCE SOLUTION**

Entrust CloudControl

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. Entrust CloudControl provides organizations with a solution that mandates frequent, ongoing testing, automation remediation, and reporting of IT systems – helping to significantly reduce compliance-related costs and considerably minimize the attack surface of virtualized and cloud platforms.

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

Risk reduction

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

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

Process improvement

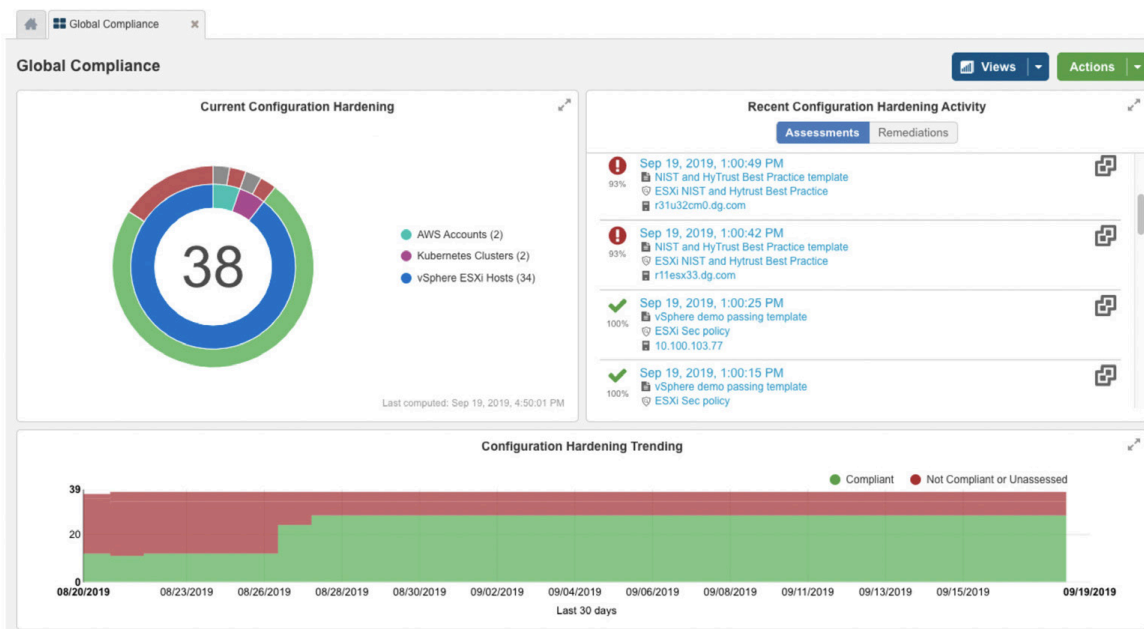
- Increase effectiveness and visibility of compliance initiatives
- Decrease time and increase reliability of task completion
- Increase leadership confidence in compliance activities

Figure 1. Public sector organizations can streamline compliance efforts and increase ROI (return on investment) by automating critical security processes and procedures.

Security configuration management - simplified

Using Entrust CloudControl can significantly improve an organization's ability to identify, remediate, and report on configuration and security management drift. These capabilities increase visibility and decrease the risk of misconfigurations that can lead to unintended downtime or security exposure. Automation also improves personnel utilization and process optimization, which reduces operational costs while significantly increasing return on investment (ROI).

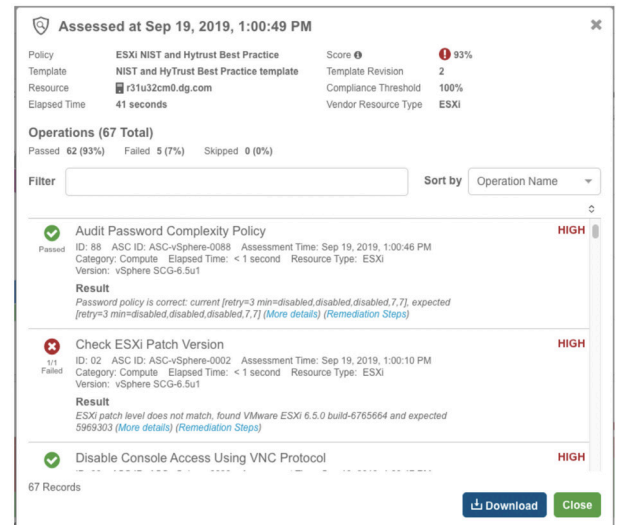
Entrust CloudControl provides a solution that adheres to industry best practices and compliance frameworks such as NIST 800-53, CIS Benchmark, Payment Card Industry Data Security Standard (PCI-DSS), DISA STIGs, Health Insurance Portability and Accountability Act (HIPAA), and customized requirements. CloudControl also provides frequent and 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 Entrust 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 Entrust CloudControl

- Unified Visibility: Search, tag, inventory, and manage your vSphere infrastructure to understand your overall compliance posture.
- Security Configuration Hardening: Ensure 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, Payment Card Industry Data Security Standard (PCI-DSS), and DISA STIGs, or create a custom template to meet your needs.
- Continuous Compliance: Continuously assess your infrastructure for configuration and automatically remediate on a scheduled basis.



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 Entrust 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 ensure a significant return on investment (ROI).

For more information

888.690.2424

+1 952 933 1223

sales@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust is dedicated to securing a world in motion by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com



Entrust and the Hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer. © 2021 Entrust Corporation. All rights reserved. HS22Q2-dps-scaling-security-configuration-assessment-remediation-cloudcontrol-sb

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact