Solution Brief for Public Sector

Automated, 'Zero-Touch' Compliance, Assessment and Remediation

Mitigating risk and achieving security compliance in the cloud

ENTRUST

SECURING A WORLD IN MOTION

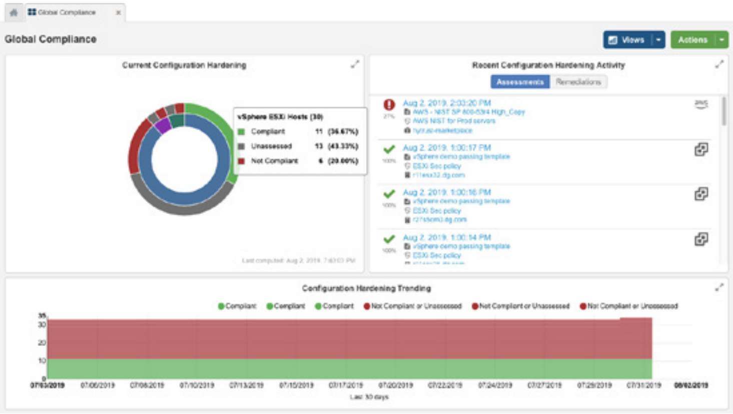
Challenges of IT Compliance in the Enterprise

Public Sector IT infrastructure is under the constant threat of attack from malware, bad actors, and Advanced Persistent Threats (APTs). For many government entities, the process of measuring, maintaining and validating their IT security under the compliance frameworks such as FISMA, NIST 800-53, NIST 800-171, CCRI, FedRAMP, and DISA STIG, has evolved into a costly and resource-intensive requirement. Entrust public sector systems provide services that support the military, critical infrastructure, emergency response, transportation, civilian state and local government operations, and more.

"ORGANIZATIONS CAN REDUCE THEIR COMPLIANCE COSTS BY IMPLEMENTING SOLUTIONS THAT MANDATE FREQUENT, ONGOING TESTING AND REPORTING OF IT SECURITY SYSTEMS."

With increased deployment of virtualization and cloud platforms, many public sector IT and security practitioners are struggling to meet the most basic compliance requirements due to missing or underdeveloped platform technology. Unfortunately, this lack of native security functionality makes these platforms an increased security risk when used for high value, mission-critical deployments. Departments and agencies must mitigate these risks by implementing third party, automated solutions to bridge these gaps and meet the standards required for success in the public sector. As federal programs like Command Cyber Readiness Inspection (CCRI), Continuous Diagnostics and Monitoring (CDM), and Comply-to-Connect (C2C) scrutinize whether those standards are being met daily, it's becoming increasingly important for Federal agencies to deal with compliance drift head on.

Entrust protects, assesses and remediates thousands of systems and users regardless of where they reside – private, hybrid, or in the public cloud. Entrust protects these systems/workloads for the largest financial, health care, and government organizations across the globe. The missions for these organizations are starkly different, but the demand for a scalable and highly configurable solution is critical.



vSphere ESXi Hosts (30)		
Compliant	11	(36.67%)
Unassessed	13	(43.33%)
Not Compliant	6	(20.00%)

27% Aug 2, 2019, 2:03:20 PM
AWS - NIST SP 800-53r4 High_Copy
AWS NIST for Prod servers
fyi.io-marketplace

100% Aug 2, 2019, 1:00:17 PM
vSphere demo passing template
ESXi Sec policy
r11esx32.dg.com

100% Aug 2, 2019, 1:00:16 PM
vSphere demo passing template
ESXi Sec policy
r27esxm3.dg.com

100% Aug 2, 2019, 1:00:14 PM
vSphere demo passing template
ESXi Sec policy

Figure 1. Entrust's global compliance dashboard shows compliance status across a multi-cloud (AWS, Containers, VMware) environment

Entrust CloudControl for Public Sector Compliance

- Automates key security processes in virtualized and cloud environments to increase ROI and reduce the costs associated with maintaining regulatory compliance
- Supports compliance initiatives such as NIST 800-53, NIST 800-171, CCRI, FedRAMP, DISA STIG, CJIS, PCI-DSS, and HIPAA
- Routinely assesses whether the workload security within the virtualized and cloud environment continues to be consistent and enforced over time due to operational changes
- Audit-quality logs that enable complete audit trails tied to approved and denied activities for privileged user activities
- Provides scalable, automated, and zero-touch capabilities to assess and remediate what are generally manual high-touch tasks
- Fine-grained role-based and resource-based access control, enforcing separation of duties, least privilege, and need-to-know access

Automated, continuous compliance for workloads in the cloud

Continuous monitoring has become a best practice methodology in compliance automation due to its effectiveness in reducing levels of risk. It also reduces manpower required to maintain a compliant state. While legacy security controls may meet these stipulations when workloads are first deployed, the manual task of security oversight quickly dissipates as workloads migrate across servers, data centers, and from private to public clouds.

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 risk
- 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 2. Public sector organizations can streamline compliance efforts and reduce ROI by automating critical security processes and procedures.

Using manual methods to support dynamic, highly elastic virtualized and cloud environments is an impossible task. Implementing solutions that provide continuous monitoring and automation of IT processes to support compliance efforts has significant benefits. The public sector can reduce compliance-related costs and minimize the attack surface of virtualized and cloud platforms considerably by implementing solutions that enforce frequent, ongoing testing, automated remediation, and compliance reporting of IT systems.

Compliance automation optimizes resources and increases ROI

Depending on their assigned mission, public sector IT systems in the United States must adhere to several different compliance requirements. Each mandate prescribes a foundational, layered defense-in-depth approach that balances IT security controls with policies and procedures which must be met to attain compliance. The most common public sector regulatory mandates are:

Common compliance instruction

Governing bodies/legislation	
CJIS	— Criminal Justice Information Systems
CNSSI 1015 / 1253	— Committee on National Security Systems Instruction
DODI 8500.01 / 8510.01	— Department of Defense Instruction
FedRAMP	— Federal Risk and Authorization Management Program
FIPS	— Federal Information Processing Standards
HIPAA	— Health Insurance Portability and Accountability
ICD-503	— U.S. Intelligence Community Directive 503
NIST 800-53 / 800-171	— National Institute of Standards and Technology
PCI DSS	— Payment Card Industry Data Security Standard

Figure 3. Public sector organizations must meet several stringent IT compliance requirements.

Using solutions such as Entrust can significantly improve an organization's ability to respond to, identify, remediate, and report on compliance deviations that increase visibility and decrease risk. Another added benefit of automation is improved personnel utilization and process optimization, which reduces operational costs, while significantly increasing public sector ROI (Return on Investment).

Encryption and Key Management

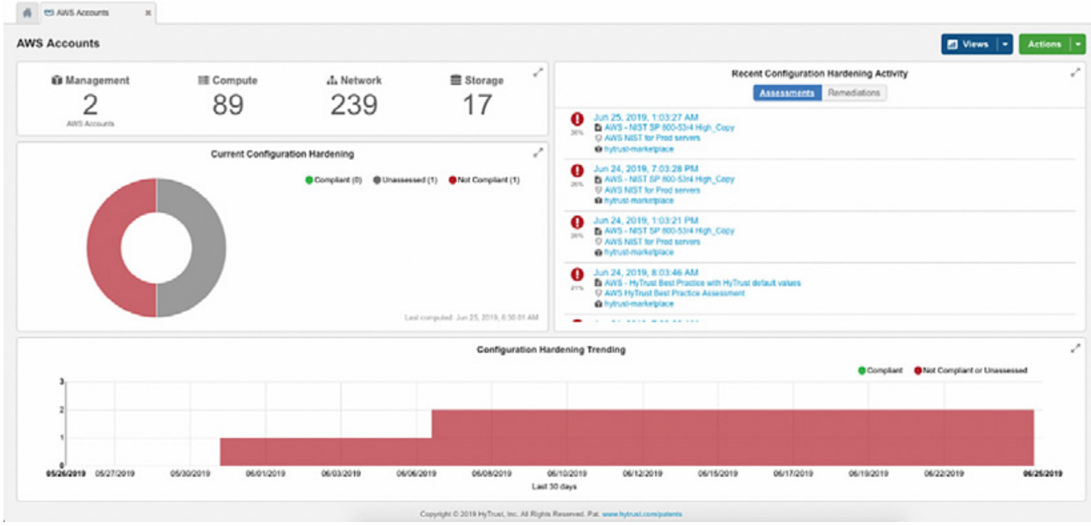
In addition to automating compliance and remediation, encryption of data-at-rest (DAR) is a key component of most federally mandated regulations. This includes FISMA, NIST 800-53, NIST 800-171, and the Presidential Executive Order. Beyond the risk of non-compliance, encryption is the simplest security strategy to protect sensitive data like personally identifiable information and mission-critical secrets. Encrypting sensitive data protects your organization from external threats and provides granular access controls that minimize threats from privileged users.

Entrust DataControl is a multi-cloud-ready virtual appliance offering powerful data-at-rest encryption at the VM level and complete workload lifecycle management – from boot to sanctioned decommissioning. Entrust DataControl includes its own key management server (KMS), which is FIPS 140-2 compliant. The advantages of Entrust DataControl include zero downtime encryption and rekey, access controls for separation of duties among admins, and deduplication-friendly encryption for maximum storage benefit.

"USING ENTRUST CLOUDCONTROL, PUBLIC SECTOR ORGANIZATIONS CAN NOW BROADEN THE MISSION SCOPE OF VIRTUALIZED AND CLOUD PLATFORMS, KNOWING THAT THEIR INFRASTRUCTURE AND DATA IS SECURE."

Entrust CloudControl

To help public sector organizations improve the security and compliance posture of their cloud-centric environments, Entrust offers an innovative framework designed to protect workloads, wherever they reside. Entrust CloudControl automates the compliance assessment, encryption, and remediation tasks across a true multi-cloud (AWS, Azure, and VMware) environment. This ensures that critical government programs are not affected by unauthorized access to sensitive data – or inadvertent changes that could render the infrastructure vulnerable to attack. This assessment and remediation is done with the idea of “Zero Touch” compliance, which allows for a policy to be set to run automatically to assess, remediate, and report on the compliance posture of the environment.



Jun 25, 2019, 1:03:27 AM
AWS - NIST SP 800-53r4 High_Copy
AWS NIST for Prod servers
hytrust-marketplace

Jun 24, 2019, 7:03:28 PM
AWS - NIST SP 800-53r4 High_Copy
AWS NIST for Prod servers
hytrust-marketplace

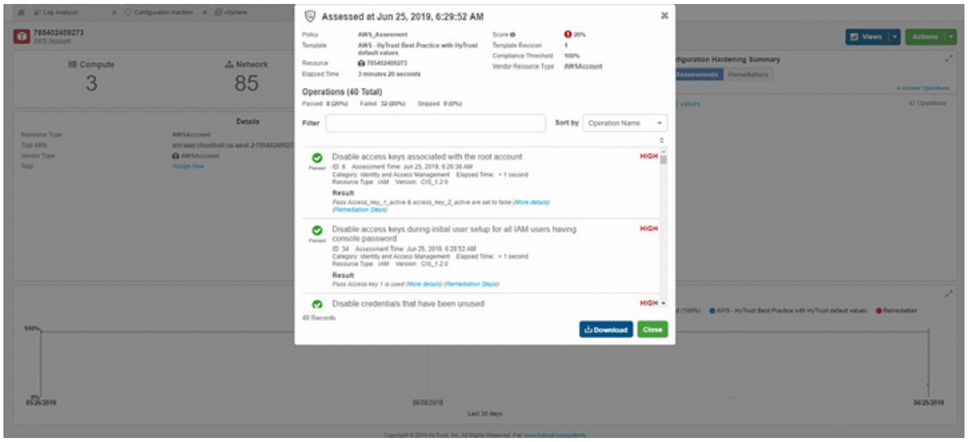
Jun 24, 2019, 1:03:21 PM
AWS - NIST SP 800-53r4 High_Copy
AWS NIST for Prod servers
hytrust-marketplace

Jun 24, 2019, 8:03:46 AM
AWS - HyTrust Best Practice with HyTrust default values
AWS HyTrust Best Practice Assessment
hytrust-marketplace

Copyright © 2019 HyTrust, Inc. All Rights Reserved. Pat. www.hytrust.com/patents

Figure 4. Quickly view configuration hardening activity across one or more AWS account and understand where improvements can be made.

> “WHILE THE COSTS OF MEETING COMPLIANCE CAN BE DISCONCERTING, THE COST OF NON- COMPLIANCE IS CONSIDERABLY MORE.”



Assessed at Jun 25, 2019, 6:29:52 AM

Policy AWS_Assessment
Template AWS - HyTrust Best Practice with HyTrust default values
Resource 785402409273
Elapsed Time 3 minutes 20 seconds
Score 20%
Template Revision 1
Compliance Threshold 100%
Vendor Resource Type AWSAccount

Operations (40 Total)
Passed 8 (20%) Failed 32 (80%) Skipped 0 (0%)

Filter
Sort by Operation Name

Disable access keys associated with the root account — HIGH — Passed
ID: 6 Assessment Time: Jun 25, 2019, 6:26:38 AM
Category: Identity and Access Management Elapsed Time: < 1 second
Resource Type: IAM Version: CIS_1.2.0
Result
Pass Access_key_1_active & access_key_2_active are set to false (More details) (Remediation Steps)

Disable access keys during initial user setup for all IAM users having console password — HIGH — Passed
ID: 34 Assessment Time: Jun 25, 2019, 6:28:53 AM
Category: Identity and Access Management Elapsed Time: < 1 second
Resource Type: IAM Version: CIS_1.2.0
Result
Pass Access key 1 is used (More details) (Remediation Steps)

Disable credentials that have been unused — HIGH

40 Records

Figure 5. View an assessment report and understand the details behind the report.

The Common Compliance Capabilities Matrix provides a mapping of the most common compliance requirements to the capabilities found in Entrust CloudControl.

Common Compliance Capabilities Matrix

Entrust Capabilities	Access Control	Audit & Accountability	Configuration Mgmt.	Ident & Authorization	Incident Response	Maintenance	Media Protection	Personnel Security	Risk Assessment	Security Assessment	Systems & Communications Protection	Systems & Information Integrity
Authentication	✓	✓		✓			✓	✓			✓	✓
Access Controls	✓				✓	✓	✓	✓	✓	✓		✓
Secondary Approval		✓	✓		✓	✓		✓			✓	
User Behavior Analytics	✓	✓		✓				✓	✓	✓		✓
Logging and Reporting	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Discovery		✓					✓		✓	✓		✓
Asset & Data Classification	✓	✓			✓		✓		✓			✓
Encryption	✓						✓		✓		✓	
Key Management	✓			✓			✓				✓	
Configuration Hardening			✓		✓	✓			✓	✓	✓	✓
Logical Segmentation	✓						✓		✓			✓
Boundary Enforcement	✓						✓				✓	✓

Figure 6. The features of Entrust CloudControl helps organizations meet a number of the most common compliance requirements for: NIST 800-53, FedRAMP. DISA STIG, PCI-DSS, HIPAA, and GDPR.

Summary

IT and compliance automation help public sector organizations optimize their use of virtualized and cloud environments while meeting the necessary operational and regulatory standards that ensure workload and data security. Using Entrust CloudSPF, IT and 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).

Learn more

To learn more about Entrust products and services, visit entrust.com

> "USING ENTRUST CLOUDSPF, IT AND SECURITY PRACTITIONERS CAN EFFECTIVELY BRIDGE THE CAPABILITY GAPS FOUND IN CLOUD PLATFORMS TO SIGNIFICANTLY REDUCE CAPITAL EXPENDITURE ON LEGACY DATA CENTER INFRASTRUCTURE..."

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

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**