Solution Brief

Strengthening Public Sector Security and Compliance

Mitigating risk and achieving security compliance in the cloud

ENTRUST

SECURING A WORLD IN MOTION

Proving IT compliance in the cloud

Public sector systems provide services that support the military, critical infrastructure, emergency response, civilian state and local government operations, and more. The public sector lives under the constant threat of IT infrastructure attacks from malware, bad actors, and Advanced Persistent Threats (APTs). For many government entities, the process of measuring, maintaining, and validating their IT security efficacy under compliance frameworks such as FISMA, FedRAMP, and DISA STIG has evolved into a costly, resource-intensive, 24/7 requirement.

With the addition 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 the utilization of these platforms a risky proposition when used for high-value, mission-critical deployments. Departments and agencies must mitigate these risks by implementing third-party, automated solutions that bridge these gaps and meet the standards required for success in the public sector.

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

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, FedRAMP, DISA STIG, CJIS, PCI DSS, and HIPAA
- Routinely assesses whether the workload security within the virtualized and cloud environment continues to be effective over time due to operational changes
- Audit quality logs that enable complete audit trails tied to privileged users' approved and denied activities
- Fine-grained, role-based, and resource-based authorization, enforcing separation of duties, least privilege, and need-to-know access
- Strong, multi-factor authentication to protect access to the virtualization platform

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

Using manual resources to support dynamic, highly elastic, virtualized and cloud environments is an impossible task. Therefore, 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 mandate frequent, ongoing testing, automated remediation, and 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 a number of 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 by organizations to achieve compliance. The most common public sector regulatory mandates are listed below:

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 2. Public sector organizations must meet a number of stringent IT compliance requirements

Using third-party 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 resource and process optimization, which reduces operational costs while significantly increasing public sector ROI.

Entrust Cloud Security Policy Framework (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. By using Entrust CloudControl, automating the security of virtualization and cloud environments ensures critical government programs are not affected by unauthorized access to sensitive data – or inadvertent changes that could render the infrastructure vulnerable to attack. Entrust CloudControl is supported by a portfolio of best-of-breed, integrated workload security solutions that include:

Strong authentication: Enforces two-factor authentication on all critical or destructive actions, preventing accidental or malicious activity from compromising the network.

Centralized auditing and reporting: Audit-quality logging to prove adherence to compliance.

Unstructured data security: Discovery, classification, and protection of high-value, uncontrolled data.

Military-grade data encryption at rest: Sensitive workloads remain encrypted with integrated key management, wherever the workloads are located.

Workload configuration hardening: Predefined templates enable auto-remediation of workload configuration to quickly mitigate risk.

Software tagging and hardware-based geo-fencing: Set logical restrictions to ensure sensitive workloads and clones operate only within predefined boundaries.

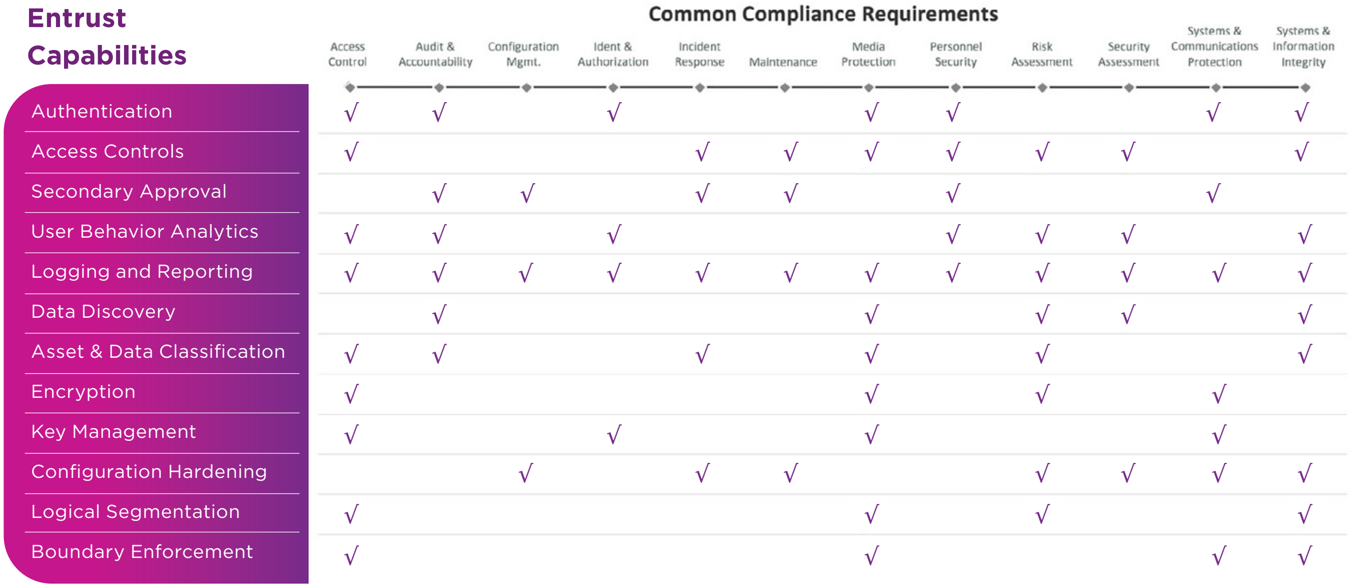
Password vaulting and separation of duties: Increases privileged user accountability.

Continuous monitoring: Monitor compliance deviations that impact security policy, access controls, and enforcement.

Secure multi-tenancy: Enables secure, logical data and workload deployment, allowing for multi-mission workloads on the same platform – without foreign cross-data contamination.

The Common Compliance Capabilities Matrix below provides a mapping of the most common compliance requirements to the capabilities found in Entrust's Cloud Security Policy Framework (CloudControl).

Common Compliance Capabilities Matrix



	Common Compliance Requirements											
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 3. The features of Entrust CloudControl help organizations meet a number of the most common compliance requirements such as NIST 800-53, FedRAMP, DISA STIG, PCI DSS, HIPAA, and GDPR.

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

Summary

IT and compliance automation helps public sector organizations 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 and security practitioners can effectively bridge the capability gaps found in cloud platforms to significantly reduce capital expenditure on legacy datacenter infrastructure, streamline resources, prove security and compliance, and ensure a significant return on investment.

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

Learn more

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

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