Solution Brief

Entrust Workload Security Solutions for Public Sector Virtual Infrastructure

Extending and securing mission-critical environments in the cloud

ENTRUST

SECURING A WORLD IN MOTION

Introduction

Government departments and federal agencies today are turning to private cloud, Software-Defined Data Center (SDDC), hybrid cloud, or multi-cloud deployment models to reduce capital expenditures, increase agility, and support data center consolidation. However, the flexibility and agility that can be achieved using cloud platforms have been overshadowed by a profound lack of critical, native security features and functionality. These limitations have slowed public sector adoption rates and reduced the effective mission capability of cloud and hybrid cloud platforms. Without these native security and audit controls, leveraging cloud environments for sensitive missions becomes difficult while trying to meet stringent IT security and governmental compliance requirements.

Entrust strengthens native virtual platform capabilities

Entrust understands the challenges faced by public sector organizations when securing virtual and cloud platforms within the U.S. Federal, state/local, and educational IT infrastructures. Using Entrust solutions, government agencies can seamlessly implement the necessary security controls to mitigate common threats – such as insider attacks and protection against credential-harvesting APTs (Advanced Persistent Threats) – as well as identify, remediate, and report on deviations against internal and external compliance requirements.

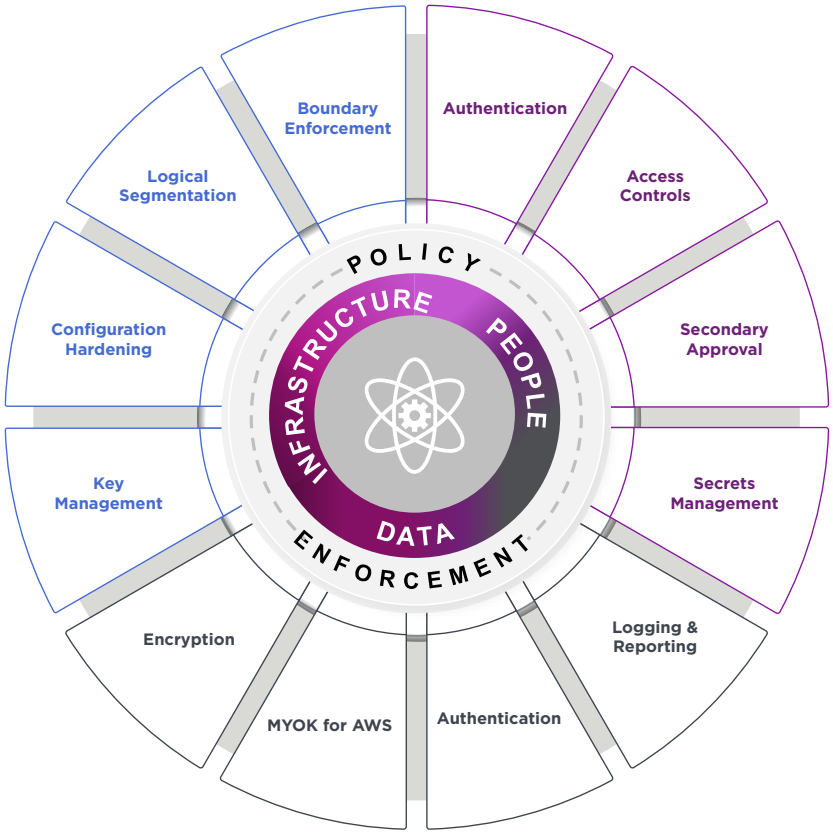

Figure 1. Entrust CloudControl increases security and workload integrity across public and private cloud platforms.

Entrust workload solutions:

- Strengthen the native security of VMware NSX and ESXi virtualization platforms
- Define administrator access to virtual resources to reduce the risk of rogue system administration and insider attack
- Integrate with leading multifactor authentication solutions such as RSA SecureID, Active Directory, RADIUS, TACACS+ and Smart Cards/PKI to mitigate credential compromise
- Enforce least privilege access and separation of duties on virtual machines and resources
- Optimize workload elasticity and virtual desktop density using secure multi-tenancy
- Generate detailed access logs and reports to support governmental compliance initiatives
- Label virtual resources and create rules to define fine-grain access controls to enforce administrative boundaries
- Enforce VM decryption policy based on software labels or physical hardware using Intel TXT® and Trusted Platform Module (TPM)

Using Entrust helps the public sector to:

- Accelerate adoption of virtualization technology in government IT infrastructure to reduce CAPEX and increase deployment flexibility and agility
- Securely implement multi-tenancy deployments to increase mission capability and effectiveness
- Implement military-grade encryption on all VMs – from initial installation through secure decommissioning
- Seamlessly deploy and easily manage enterprise-class key management
- Tightly define where VMs and workloads are allowed to run, protecting against unauthorized replication and access to sensitive workloads
- Meet governmental security, audit, and compliance requirements of National Institute of Standards and Technology (NIST), Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and other compliance frameworks

Entrust CloudControl security policy framework

Entrust CloudCountrol delivers a critical set of capabilities required to proactively secure workloads, wherever they reside in the cloud. The CloudControl framework is supported by a portfolio of Entrust integrated workload security solutions that include advanced access controls, configuration hardening, strong encryption, integrated key management, data discovery and classification, workload placement, data geo-fencing, and granular auditing to meet both internal and external compliance requirements.

Define, detect, and defend sensitive and confidential data

Public sector organizations understand the potential risks posed by unsecured, unstructured data arbitrarily stored by users in unmonitored workloads or archived in periodic backups. Entrust allows organizations to proactively discover sensitive information in data files using predefined and custom search criteria; track and audit data access to identify internal threats; and recover lost critical data should an abnormal event occur.

Granular administrative access control, auditing, and proving compliance

Entrust solves many of the security and audit concerns prevalent in native virtual platforms by enforcing access control policies using a five-element Role-Based Access Control (RBAC) model, allowing organizations to define granular administrative control and enforcement rules that govern access to each virtual resource. Regular assessment and hardening of VM configuration using predefined best practice templates help public sector organizations maintain workload integrity in accordance with VMware Hardening Guides – as well as regulatory guidelines such as NIST 800-53, PCI-DSS, HIPAA, and DISA STIG.

Workload encryption and key management

Entrust provides organizations with a workload lifecycle encryption and integrated key management solution that fully supports enterprise architectures across multiple, disparate, virtualized environments. Using a policy agent that travels with each VM from one virtual platform to another, Entrust can enforce policy and implement strong AES-128/256-bit encryption to mitigate unauthorized workload cloning, decryption, and data access attempts. The key manager supports large-scale enterprise deployments with high-performance and high-resiliency functionality.

Data geo-fencing to prevent unauthorized workload access

For secure workload and data geo-fencing, Entrust permits the decryption of workloads only when launched on predefined, trusted hardware (Intel TXT®) or when validated against predefined software rulesets and constraints. The platform provides government departments and agencies with the ability to tightly define where VMs and workloads are allowed to run, protecting against unauthorized replication and running of sensitive workloads beyond the predefined virtual working environment.

Summary

As public sector organizations begin to take full advantage of virtual cloud environments, they must recognize the potential security risks of native security controls and compliance shortfalls inherent in cloud provider platforms. Entrust CloudControl allows government departments and agencies to make significant strides in their efforts to reduce capital expenditure, maintain the integrity of their virtual infrastructure, and meet the ongoing virtual security and compliance requirements needed for mission success.

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**