Solution Brief

ENTRUST

SECURING A WORLD IN MOTION

Why native virtualization platform security falls short

One of the overwhelming advantages of virtualization technology is the ability to create a virtual data center in minutes rather than months, while minimizing the costs of owning the actual hardware infrastructure itself. Being able to share the same hardware infrastructure across multiple disparate virtual data centers (multi-tenancy) provides the operational agility many government departments and agencies need, while significantly cutting costs associated with physical data center deployments.

A major challenge for multi-tenant environments on virtual platforms is the

Successfully maintaining security and compliance in multi-tenancy environments

E□ective isolation of each virtual deployment requires organizations to prevent unauthorized communications between one tenant's virtual machines (VMs) and networks with another tenant's resources. Isolation also prevents one tenant's privileged administrators from exposing their own workloads to others (accidentally or intentionally) or gaining unauthorized access to another tenant's data. Further, the logging of all virtual administrative activity per tenant – both approved and denied – is required as a "check and balance" to ensure proof of ongoing security and compliance.

Entrust CloudControl empowers organizations to:

- Strengthen the native security of VMware NSX and ESXi virtualization platforms through its support of VMware Cloud Foundation (VCF)
- Implement two-factor authentication (2FA) technology to prevent privileged-account brute forcing and identity spoofing
- Enforce least privilege access and separation of duties on virtual machines and resources
- Label virtual resources and create rules to define fine-grain access controls to enforce administrative boundaries
- Automate temporary access requests using Root Password Vaulting
- Generate detailed access logs and reports to support compliance initiatives
- Define administrator access to virtual resources to support multi-tenant environments
- Prevent unauthorized movement of VMs from a designated host or onto a host that does not have an acceptable security policy
- Enforce data policy based on software labels or physical hardware using tags and trusted platform modules (TPMs)

Entrust Workload Security Solutions

Entrust CloudControl solves multi-tenancy challenges by enforcing access control policies for virtualized servers and desktop infrastructure (VDI), e□ectively segmenting virtual deployments and securely isolating each tenant's critical applications and data. Using Entrust, organizations can increase agility, accelerate deployment times, and decrease infrastructure costs – without risking unauthorized access to another tenant's virtual infrastructure. Supporting VMware Cloud Foundation, the centralized solution enables organizations to achieve authentication, authorization, and audit control for UI and API access to critical infrastructure resources in the ecosystem including ESXi hosts, vCenters, NSX-T Managers, vSAN, and SDDC and associated workload and management domains.

Entrust capabilities to strengthen multi-tenant deployments include:

Privileged Administrator Access Policy Implementation, Management, and Enforcement

Using a five-element role-based access control (RBAC) model to define granular administrative access control, Entrust can enforce access based on:

1) the virtual resource requested;
2) group membership;
3) administrative role;
4) the label classification;
5) the rules that govern access to a resource.

System Integrity Monitoring and Log Analysis

Entrust enhances the native logging capabilities of the VMware® platform to provide granular, system-level logging of all administrative actions and events that have taken place in the virtual infrastructure.

Operational Workload Security, Hardening, and Compliance

Entrust provides automated workload security assessment of VM configuration, remediation, and hardening of VMs against attack using predefined best-practice configuration templates. Regular assessments maintain configurations in accordance

Restricting Workload Access Using Workload Geo-Fencing

For workload and data geo-fencing, Entrust permits the decryption of workloads only when launched specifically on trusted hardware or when validated against predefined software rule sets and constraints. Workload geo-fencing 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 mission-sensitive workloads on unauthorized hosts.

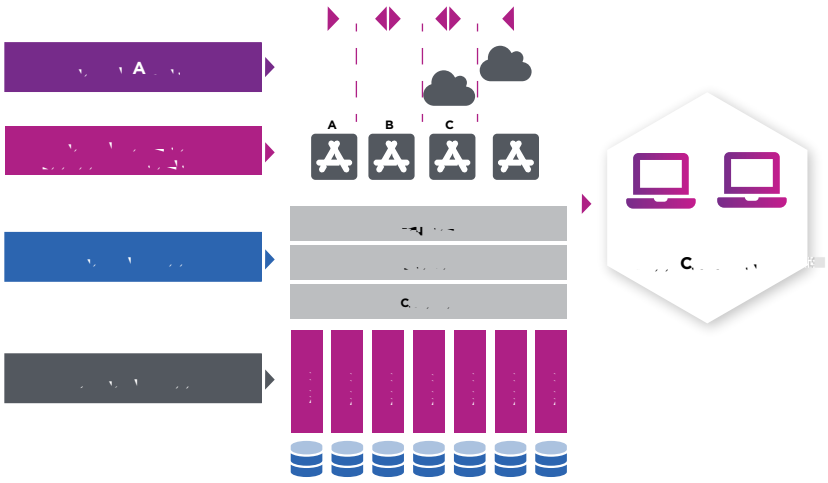

Figure 1. Entrust CloudControl helps organizations to e□ectively isolate virtual data center deployments to operate securely in multi-tenant environments

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

Learn more at
entrust.com