



ENTRUST



Entrust CloudControl Enforces Strong Global Security Procedures for a Large Bank's VMware Cloud Deployments

Challenge

A large U.S.-based financial institution with a global footprint needed to establish and maintain consistent security procedures for more than 200,000 virtual machine (VM) instances and 20,000 ESXi hosts across several global data centers.

Beyond the scale of deployments, the bank needed to accelerate the speed of deployments of large VMware private cloud architectures across its globally distributed data centers. This included supporting VMware Cloud Foundation (VCF) architecture.

In addition to the risks of outages and data breaches caused by external bad actors, the bank needed to prevent possible employee misconfigurations of virtual infrastructure and the potential for misuse by privileged administrators.

Further, the bank was aware that there may be regulatory compliance deficiencies in their extensive virtual ecosystem that needed to be identified and resolved.

CUSTOMER PROFILE

One of the largest financial institutions in the world, with a full range of financial products and services, serving retail consumers, small and medium businesses, and large corporations.

Objectives

- Ensure consistent and verifiable security procedures for virtual cloud environments
- Securely accelerate deployments of large VMware private cloud architectures across globally distributed data centers
- Identify and remediate key regulatory compliance deficiencies
- Address executive-level concerns about availability and breaches that could impact their brand reputation, revenue, and stock value

Technology

- Entrust CloudControl for VMware cloud deployments



Entrust CloudControl Financial Institution Case Study

Solution

After a thorough selection process, the bank chose **Entrust CloudControl** to provide its automated workload security policy enforcement and compliance across global deployments.

Entrust helped the bank conduct initial scanning against required regulatory compliance. CloudControl identified thousands of violations that were unknown to the bank's compliance team in a matter of a couple of hours. This set the stage to change internal processes as well as automate many controls to create a higher level of compliance on a continuous basis.

With CloudControl, the bank:

- Ensures that its virtual workloads adhere to required security practices
- Enforces separation of duties and least privilege principles through granular and customizable role-based access controls
- Provides robust configuration hardening to assess and remediate compliance violations
- Receives audit-quality logs to support incident response

- Established secondary approvals to mitigate the risk of admin mistakes and insider threats
- Automatic inspection of the virtual infrastructure for configuration and policy infractions, minimizing manual intervention and validation prior to production deployment

Results

Entrust helped the financial institution enable high availability of critical systems, reducing the risk of outages and supporting a continuously compliant architecture that is used on tens of thousands of virtual machines.

High numbers of regulatory compliance deficiencies were discovered and resolved using the automated CloudControl visibility and remediation feature, ensuring hands-on staff time was significantly reduced while adhering to the required regulatory standards.

Though Entrust was able to deploy the initial CloudControl solution in several weeks, the engagement was so successful that the bank asked Entrust to provide continued support.

With the new CloudControl solution in place, the bank determined that risks posed by unexpected outages and its VM admins have been dramatically reduced.

Learn more about Entrust CloudControl and our cloud security solutions at [Entrust.com](https://www.entrust.com).

Learn more at
[entrust.com](https://www.entrust.com)



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