MULTI-CLOUD SECURITY SOLUTIONS

New multi-faceted, integrated platform helps organizations meet the demands for securely managing multi-cloud deployments and decentralizing risks while centralizing visibility for compliance.

Overview

Entrust is the go-to expert for multi-cloud deployments. We help organizations navigate the increasing complexities of securely managing the deployment of, and access to, virtual machines (VMs) and containers across multi-cloud deployments – all while meeting compliance requirements.

As a trusted adviser, leveraging expertise in data protection and encryption, certificate solutions, and identity, Entrust is delivering an enterprise-grade platform combining cryptographic asset management for VMs, containers, keys, secrets, and certificates – on-premises and in the cloud. The platform provides encryption, integrity protection, environment hardening, and robust compliance management to prevent policy violations and inadvertent misconfigurations – which can lead to malicious attacks or unplanned outages. The Entrust platform ensures organizations have a robust cloud security posture that can be established and maintained.

The Challenge

As organizations migrate more operations from on-premises to hybrid and multi-cloud environments, it becomes even more challenging to maintain consistent security procedures and compliance across a larger and more complex cloud footprint. Problems often encountered include managing the security of VMs and containers across their lifecycle and ensuring deployment and access is in line with policy. Preventing misconfigurations that could lead to malicious attacks is critical as multi-cloud deployments scale. This means ensuring consistent security policies are applied across the board by administrative teams tasked with deploying and maintaining large-scale, dynamic virtual machine and container environments.

Learn more at entrust.com

Establishing and maintaining a robust and consistent security posture across diverse cloud deployments is vital for proper security auditing and compliance with growing government and industry cybersecurity regulations.

The Solution

Entrust offers a multi-cloud security platform that provides a unified approach to compliance management for building and deploying virtual machines, software as a service applications, and containerized environments. By establishing consistent security policy and preventing misconfigurations, the platform facilitates compliance. Enabling visibility and knowledge of the cryptographic assets allows the organization to bring them under control. And protecting the data ensures workloads do what they are supposed to do. Together, the unified multi-cloud security platform delivers:

VM and container cryptographic key management, policy management, and compliance management to prevent policy violations and misconfigurations that can lead to malicious attacks.

Cloud security posture management (CSPM) to discover and identify assets, monitor and assess compliance and risks, and provide a granular alert and remediation capability while maintaining established levels of security hygiene.

Role-based access control (RBAC) allied with certificate and secrets management to ensure that users and containers have necessary credentials for communicating with other services, authenticating themselves using passwords, API keys, or certificates.

VM and container image signing and encryption to ensure protection throughout the lifecycle.

Entrust Multi-Cloud Security Platform

The Entrust Difference

Entrust brings together the foundational elements necessary for a comprehensive multi-cloud security strategy into a multi-faceted, integrated platform. Combining what has to date been independent point solutions including CSPM, encryption, cryptographic key, and certificate management, Entrust delivers what no other vendor has been able to offer – a single platform providing comprehensive visibility of the environment and consistent configuration and policy enforcement. The new offerings include an extensive set of cloud-enabling features to support containers and Kubernetes, bring your own key (BYOK) capabilities, web services, secrets management, and multi-cloud key management.

The Entrust platform empowers customers to evolve their infrastructure with solutions that avoid vendor lock-in. One example is the unique Security World key management architecture that delivers trusted cryptographic services with scalability, failover, and load balancing from the data center to the multi-cloud environment.

The platform evolves traditional on-premises product offerings including PKI, identity, data protection, encryption, and cryptographic key management, to an as a service model that lets customers use what they need, when they need it. The Entrust solution enables greater flexibility and a transfer from capital to operational expenditures. With new data centers across the globe, Entrust ensures customers have localized access to services with optimal performance and geo-fencing capabilities.

Protecting multi-cloud deployments includes not only securing assets and workloads across multiple cloud services, but also identifying, authenticating, and controlling access of the users and machines that interact with these distributed systems.

Offerings from other vendors might focus on encryption and key management or cloud security posture management, but these solutions cannot enable the wide security coverage that Entrust provides through its combination of data protection, certificate, and identity solutions.

Benefits

- Provide unified policy, visibility, and administrative guardrails establishing a baseline that can constantly monitor deployments
- Discover and identify workloads, monitor, and assess compliance and risks – while providing granular alert and remediation capability
- Leverage built-in compliance templates for hardening virtual machine and containerized environments
- Ensure users and containers have the necessary credentials to communicate with other services, authenticating themselves using password, API keys, or certificates
- Offer identity orchestration to bridge the gap between different systems and enable identity services from diverse vendors to be seamlessly monitored, managed, and secured to avoid vendor lock-in
- Simplify authentication, authorization, and risk policy decisions
- Protect the integrity of deployed VMs and containers by signing and encrypting their images
- Secure distributed workforces and provide secure access to applications from anywhere
- Deliver automation with real-time compliance and security
- Securing complex VM and container deployments on-premises and in hybrid and multi-cloud environments

Learn more at entrust.com

Entrust Multi-Cloud Security Platform

Entrust Products Supporting the Platform

KeyControl simplifies management of encrypted workloads across multi-cloud environments by automating the lifecycle of encryption keys, including key storage, distribution, rotation, and revocation. KeyControl also offers bring your own key (BYOK) capability to generate, manage, and use your own encryption keys across cloud service providers, including AWS, Google Cloud Platform, and Microsoft Azure.

DataControl delivers data encryption, multi-cloud key management, and workload security while enabling compliance with data privacy regulations.

CloudControl provides a unified framework for security and compliance across the hybrid and multi-cloud environment, including centralized authentication, authorization, and audit control to reduce both risk and operational overhead.

nShield HSMs and **nShield as a Service** provide a secure solution for generating encryption and signing keys, creating digital signatures, encrypting data, and securely executing sensitive applications within a protected FIPS 140-2 or FIPS 140-3 certified environment.

Entrust Multi-Cloud Security Solutions Integrate With Leading Technology Providers

vmware   Google   Microsoft   IBM

aws   NetApp   ORACLE   mongoDB

Red Hat   Quantum   NUTANIX   rubrik

COHESITY   BLOOMBASE

Entrust Identity Enterprise and **Identity as a Service** deliver cloud-based identity and access management with multi-factor authentication, credential-based passwordless access, and single sign-on.

Entrust PKI establishes and maintains a trustworthy networking environment by providing key and certificate management services (on-premises or managed as a service) that enable encryption and digital signature capabilities across a wide set of applications.

Certificate Hub enables customers to find, control, and automate the management of the device and use digital certificates that help ensure only authorized access to multi-cloud services.

Professional Services helps customers with the skills and expertise to develop the solution that is right for their specific needs. Custom cryptographic solutions include Internet of Things, enterprise code signing, HSM application integration, cryptography as a service, and encryption applications, among others.

nShield Security World offers a common key management framework across all nShield HSM products that provides strong, granular controls over the access and usage of keys and policies.

nShield Option Packs extend the capabilities of nShield HSM deployments with easy to set up software to support web services, containers, timestamping, cloud integrations, and database security.

Learn more at entrust.com

Entrust Multi-Cloud Security Platform

Key Features

- Single platform delivering compliance management for VMs, containers, keys, secrets, and certificates in on-prem, hybrid, and cloud environments

- Enforce a robust cloud security posture across all deployments

- Enable a broad security coverage for risk mitigation

- Ensure compliance with data security and privacy regulations

Learn more at entrust.com

ENTRUST