The adoption of multi-cloud drives the need for better data protection and management of encryption keys and policy controls

Jim DeLorenzo
August 24, 2021

Enterprise adoption of multiple cloud platforms continues in earnest, whether it's aimed at improving collaboration, reducing data center footprint, increasing customer response times, or any number of other business goals. As organizations advance their multi-cloud strategies, they are tasked with applying consistent security configurations across workloads and applications. They must also implement data protection that addresses today's threat vectors and aligns with stringent compliance and audit requirements.

Encrypting cloud data is essential to protecting sensitive information and workloads – but it needs to be done correctly to be effective and meet compliance mandates. A recent report from Forrester, Best Practices: Cloud Data Encryption, articulates several important recommendations, notably:

- Use hardware security modules (HSMs) to store encryption keys separately from cloud workloads
- Use a centralized HSM infrastructure to manage the encryption keys used across cloud environments
- Rotate your keys regularly to ensure alignment with compliance requirements and auditor expectations

These security measures are critical to protecting your [illegible] vital to get them right from the outset.

Multi-cloud computing is here to stay – and so are the complexities associated with

protecting your data and workloads.

Administrative challenges of managing cloud environments

While cloud service providers continue to enhance their built-in security capabilities, the teams tasked with managing cloud environments face a constant battle to fine-tune their configurations and permissions. As exemplified by numerous data breaches over the past few years, misconfigured cloud storage settings are a common, yet often unidentified, trouble spot.

Each cloud platform is unique and, even if you manage to get a handle on who has access to which data and workloads, keeping up with providers' updates and new controls requires constant vigilance. And as the shortage of skilled security professional persists – including those with expertise working across multiple cloud platforms – these challenges aren't going away.

Demonstrating compliance

Identifying and implementing the right security controls is one challenge, while demonstrating compliance with data privacy regulations and industry mandates is another. Security teams cite specific concerns about being able to verify controls and how to report compliance in an auditor-approved format.

As compliance and audit requirements continue to get more stringent, nearly every enterprise is now subject to at least one mandate that calls for the use of data encryption. And as the Forrester report discusses, data encryption is a must-have for cloud workloads. This necessary security measure comes with its own administrative upkeep that can be difficult to handle without the right tools in place.

Cloud data encryption: Getting it right

Workloads go through many lifecycles, from staging to deployment to backup, and eventually have to be securely decommissioned. Each stage poses different risks of potential data theft or other misuse. Managing workload encryption from each cloud's management platform is complex and further increases the risk of inconsistent policies and mistakes.

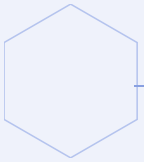
Additionally, an encryption strategy that aligns with compliance mandates requires robust key management. Unfortunately, key management is not universal across cloud platforms so the security team must contend with key storage, distribution, rotation, and revocation in multiple environments.

What's more, when encryption keys are not completely separated from the workloads and data they protect, the potential exists for a security incident that compromises both, leaving data exposed to a breach. Best practices call for the use of certified HSMs to protect your encryption keys.

Entrust can help

Entrust offers a robust set of security solutions to help you protect workloads and data across your multi-cloud infrastructure, including enhanced protection of your encryption keys that supports compliance with data privacy mandates.

ENTRUST CORPORATE



JIM DELORENZO / VIEW ALL JIM'S POSTS

SOLUTIONS MARKETING MANAGER, DATA PROTECTION SOLUTIONS

Jim DeLorenzo is a senior solutions marketing manager for Entrust, where he helps customers understand how Entrust Data Protection Solutions can help address enterprises' unique security and compliance challenges. Jim does this through customer presentations, blogs, articles, whitepapers and other content. Jim has more than 10 years of experience with both startups and established enterprises in the security space, focusing on data protection, endpoint security and penetration testing solutions. He holds a master's degree in marketing and an undergraduate degree in finance.

Product Resources

Entrust Store

Resources

Library

Training

Legal and Compliance

Covid 19 Updates

Social

Twitter

Facebook

Instagram

LinkedIn

YouTube

English 中文 Português Français Deutsch Русский 한국어 Español Italiano 日本語