eBook

Busting Top Cloud Encryption Myths

And Why You Need External Key Management

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

Introduction

Cloud adoption is essential for modern organizations, driving digital transformation efforts and enabling scalability and innovation. However, as with so many technological advancements, the shift to cloud infrastructure has introduced a slew of security challenges, particularly surrounding data protection. Most notably, organizations assume that relying solely on the encryption provided by the Cloud Service Provider (CSP) is sufficient, but this approach presents significant risks, especially in complex, multi-cloud environments.

In this eBook, we'll address the key myths surrounding cloud encryption and the necessity of external key management. We'll debunk the idea that CSP-provided encryption is universally sufficient, highlighting the risks of insider access, lack of separation of duties, and the complexities of multi-cloud deployments.

We'll also tackle the myth that external key management (EKM) hinders cloud adoption by demonstrating how it actually streamlines operations, enhances security, and provides agility. Then, we'll clarify that external key management is not just for regulated industries but is, in fact, a crucial security best practice for all organizations seeking to protect sensitive data in the cloud. Finally, we'll address the dangerous misconception that an organization's data can be "not sensitive enough" to warrant external key management.

Ultimately, this eBook advocates for external key management as a solution that provides enhanced control, strengthens security posture, ensures compliance, and enables secure and efficient cloud adoption.

Myth #1

Encryption Provided by my CSP is Sufficient in All Cases

While it is true that CSPs typically offer controls like cloud-native encryption, which are an essential layer of protection, assuming that they are sufficient in all cases is putting organizations at risk, especially those with data across multiple clouds.

Most modern organizations have this kind of cloud environment—according to the 2025 Thales Data Threat Report, 64% of enterprises **report 26 or more SaaS vendor solutions within their environment**. CSPs do typically encrypt data at rest and during transit, but retain control over the encryption keys, which presents potential risks for several reasons:

- **Insider and Malicious Access:** CSPs typically have access to customer data for maintenance, security, or compliance reasons. If a malicious actor gains access to the CSP's system with valid credentials, they could potentially access the encryption keys and decrypt sensitive data.
- **Lack of Separation of Duties:** CSPs not only store and manage data, but they also control encryption keys. This creates a conflict of interest because the entity handling the encryption and decryption of data should, ideally, be separate from the entity storing that data. When the CSP has control over both, the customer's data security is dependent on the CSP's trustworthiness and internal controls.
- **Legal Risks:** Under laws like the U.S CLOUD Act, regulatory bodies can compel CSPs to provide access to customer data, even without customer consent. As such, CSPs may be required to decrypt data without the customer's involvement, undermining the customer's control over data.
- **Challenges in Multi-Cloud Environments:** For organizations using multiple cloud providers, each provider may have its own encryption processes, key management strategies, and storage policies. This complexity increases the potential for errors or inefficiencies in key management, leading to exposure or non-compliance with security policies. Moreover, relying solely on CSP-held keys creates a single plane of failure that magnifies insider and external attack surfaces.

External key management, however, helps address the limitations of cloud-native encryption and can significantly enhance security. By separating the control of encryption keys from the CSP, organizations can take greater control of their data security and reduce exposure to various risks.

Separation of Duties

With external key management, encryption keys are stored and managed outside the CSP's control, typically either in an on-premises system or through a third-party key management service. This means that even if the CSP is compromised, the encryption keys remain secure and inaccessible. What's more, regulations like GDPR and PCI-DSS mandate proof of key separation and owner-controlled custody.

Enhanced Compliance and Control

Many industries are subject to strict regulatory requirements that demand robust control over encryption keys and data protection. External key management grants organizations greater control over encryption keys, helping to ensure compliance. This is especially important for industries handling highly sensitive or proprietary data, for which CSP-provided encryption often falls short of compliance standards.

Protection Against Insider Threats

External key management keeps encryption keys safe from potential insider threats working at CSPs. These solutions are particularly secure, offering granular access controls, continuous monitoring, and auditing to ensure only authorized personnel can access encryption keys.

Multi-Cloud Portability

Managing encryption keys externally allows organizations to easily move data across cloud environments without being locked into a single vendor's encryption infrastructure. This flexibility means organizations can avoid vendor lock-in and apply consistent security policies across different cloud platforms.

Data Sovereignty and Privacy

As global data privacy regulations become stricter, organizations must ensure their data protection practices align with them. External key management allows businesses to store keys in jurisdictions that align with their regulatory and compliance requirements, providing control over data residency and preventing potential conflicts with CSP legal obligations.

In fact, according to the Thales 2025 Data Threat Report, 32% of businesses intend to leverage external key management to attain or accomplish sovereignty initiatives.

Myth #2

External Key Management Will Slow Us Down

Many organizations are reluctant to implement external key management because they believe it will "slow them down," introducing additional complexity, latency, and operational overhead. Common concerns include:

- **Operational Complexity:** Integrating external key management into existing systems can seem daunting, especially for organizations managing diverse environments like on-premises data centers and multiple cloud platforms.
- **Performance Impact:** Some organizations are concerned that externalizing key management could introduce latency, affecting application performance and user experience.
- **Availability and Reliability:** Dependence on an external key management system raises concerns about potential downtime or unavailability, which could disrupt access to encrypted data.

However, the best external key management systems not only address these concerns but can also improve operational efficiency, performance, availability, and reliability. Let's examine how.

Simplifying Operational Complexity

Organizations should be looking for key management solutions that offer centralized key lifecycle management. This means that businesses can manage encryption keys across various environments, including on-premises, cloud, and hybrid infrastructures.

Similarly, these solutions support integration with third-party applications such as Microsoft SQL TDE, Oracle TDE, and KMIP-compliant encryption products, facilitating seamless key management across diverse systems. Key rotation, policy updates, and access controls can all be automated, reducing manual intervention and minimizing errors.

What's more, by centralizing key generation, rotation, archival, and destruction in one platform – and driving it via APIs in the CI/CD pipeline – organizations eliminate manual overhead and actually accelerate release cycles.

Ensuring High Performance

Best in class key management platforms are designed to be highly available and scalable. They support deployment in clustered configurations, allowing for real-time key and policy replication across multiple appliances. This ensures that encryption and decryption processes do not introduce significant latency, maintaining optimal application performance. Moreover, these key management solutions leverage clustered HSMs to deliver sub-millisecond crypto at scale, providing both high assurance and low latency.

Enhancing Availability and Reliability

To ensure availability and reliability, external key management solutions offer features like secure key replication across multiple appliances and automated backups. These capabilities minimize the risk of key unavailability and support disaster recovery efforts.

Meanwhile, features such as automated alerts for key expiration and other critical events help prevent unexpected downtime, ensuring continuous access to encrypted data. Finally, support for a range of deployment options, including virtual and physical appliances, allows organizations to tailor key management infrastructure to their unique availability and reliability requirements.

Myth #3

Our Data Isn't Sensitive Enough to Justify External Key Management

In cybersecurity, nothing is as dangerous as complacency. Organizations often believe that their data isn't sensitive enough to justify robust security measures like external key management, but this is rarely the case.

Many organizations operate under the assumption that only data like financial records or personal health information requires stringent protection. However, seemingly benign data can be used for nefarious means – when combined, even "non-sensitive" metadata or logs can expose attack vectors, meaning that breach costs don't scale linearly with data sensitivity.

For example, internal communications, operational procedures, or customer interactions can reveal proprietary strategies or vulnerabilities. These misjudgments typically stem from poor data classification practices, leading to an underestimation of the potential impact of data breaches.

Although, according to the 2025 Thales Data Threat Report, data classification practices have improved - 87% of respondents reported that they can classify at least half of their data - nearly two-thirds (61%) use five or more tools for data discovery and classification, which can lead to misalignment and conflicting protection policies.

Moreover, data that isn't sensitive today can quickly become so. Changes in regulations, business operations, or threat landscapes can turn benign data into critical data in the blink of an eye. To ensure adequate protection long into the future, organizations should consider all data sensitive.

Myth #4

External Key Management Will Hinder Our Path to Cloud Adoption

Cloud adoption is a priority for most modern organizations. Falling behind competitors in terms of cloud adoption can have wide-reaching impacts on other parts of the business, holding organizations back from innovating, scaling, and improving efficiency. Concerns that external key management could hinder a business's path to cloud adoption are understandable – but unfounded. This misconception arises out of several factors:

- **Perceived Complexity and Integration Challenges:** We touched on this earlier, but some organizations believe that implementing EKM can add complexity to cloud environments.
- **Concerns Over Operational Efficiency:** Similarly, some organizations believe that external key management can slow down cloud operations due to extra steps in key management processes.
- **Regulatory Compliance Misunderstandings:** Some organizations even believe that external key management is incompatible with regulatory compliance due to perceived loss of control, integration concerns, and misunderstanding of EKM capabilities.

However, the reverse is true - external key management streamlines cloud adoption, offering:

Scalability and Integration

As organizations adopt multi-cloud strategies, managing encryption keys across various CSPs and on-premises systems can become a serious challenge. EKM solutions provide centralized platforms to manage keys across these diverse environments, eliminating the inefficiencies and vulnerabilities associated with using disparate key management tools provided by individual CSPs. They can also scale to manage vast numbers of cryptographic keys, ensuring that security doesn't become a bottleneck as the cloud environment grows.

Similarly, EKM solutions can integrate with cloud services and DevOps workflows, ensuring that key management aligns with agile development practices. This integration simplifies the encryption and decryption process within cloud applications, making it easier to adopt new cloud-based tools and services.

Control and Security

Moving data into the cloud inherently means losing an element of control, especially when compared to storing all data on-premises. This is particularly true when organizations entrust key management to CSPs. EKM ensures that businesses maintain control over their encryption keys, and this control is essential for ensuring regulatory compliance and granting only authorized parties access to sensitive data.

Agility and Expansion

The inherent dynamism of cloud environments means that organizations must constantly adapt to new services and technologies. EKM grants them the necessary agility to adapt to these changes by offering a flexible and scalable platform that can easily integrate with new cloud services. This means that organizations can expand their cloud footprint without being constrained by the limitations of CP-provided key management solutions.

Moreover, by simplifying key management and providing a consistent security framework, external key management can actually facilitate further cloud adoption. This gives organizations the confidence to migrate more applications and data to the cloud, knowing that their sensitive information is secure.

Myth #5

External Key Management is Only for Regulated Industries

Many organizations believe that external key management is only necessary for regulated industries like finance, healthcare, and government, primarily due to its long-standing association with compliance. EKM is prominently featured in regulations like PCI DSS, HIPAA, and GDPR, each mandating strict controls over encryption keys. But this is a misnomer—EKM is for organizations of all shapes and sizes.

Today, every sector handles sensitive or business-critical information. Think of the expanded applicability of NIS2; from e-commerce to media, protecting assets is a business imperative, and all organizations should want to own their data by controlling the keys, not just to comply with regulations, but as a fundamental security practice.

What's more, whether regulations apply to you or not, following regulatory guidelines is just good practice: according to the Thales Data Threat Report, in 2025, 78% of enterprises that failed audits had a breach history, versus just 21% of those that passed compliance.

The takeaway here is that EKM is more than just a regulatory checkbox – it's a strategic enabler. It supports industry-agnostic best practices like zero trust, customer trust, supply chain security, and innovation at scale to ensure your business stays safe and profitable.

Myth #6

External Key Management is Too Expensive

While external key management might seem like an unwanted additional expense, it is, in fact, a cost-effective investment when weighed against the enormous potential costs associated with data breaches, compliance penalties, and vendor lock-in.

For example, IBM's Cost of a Data Breach Report 2024 puts the average cost of a data breach at $4.88m, and GDPR fines can reach up to 20 million euros or 4% of a company's global annual turnover, whichever is higher, for the most severe violations.

Modern EK solutions offer flexible, often subscription-based, pricing and deliver rapid ROI by significantly lowering audit expenses through automated compliance and dramatically reducing the potential costs of data breaches. Centralized, secure key management minimizes breach risks, eradicates vendor lock-in, and ultimately provides substantial financial benefits – just as it did for this European financial institution.

Explore Thales Key Management Solutions

Thales offers a suite of key management solutions designed to enhance and simplify key management in complex cloud and enterprise environments, supporting a wide range of use cases. Built on FIPS 140-2 compliant virtual or hardware appliances, Thales' solutions provide robust security for sensitive data and centralize the management of encryption keys for both internally developed and third-party applications. This centralized control empowers you to strengthen your data security and maintain complete command over your encryption keys. What's more, Thales' key management products use standard interfaces to connect seamlessly with your applications, enabling easy access to comprehensive key management functions.

Next steps:

- **Find out more about Thales' key management solutions here**
- **Watch our webinar "Cloud Security: Are You Control or Just in the Cloud?"**
- **Read our blog "Your Data, Your Responsibility: Securing Your Organization's Future in the Cloud"**

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com