thalestct.com

THALES

Own and Manage Your Encryption Keys

Customer-owned encryption: The only way to truly safeguard data stored and managed in cloud environments

White Paper

Executive Summary

For agency leaders and IT administrators responsible for data security—from the most basic statistics to highly sensitive documents—understanding the role of encryption and the management of encryption keys is vital to keeping confidential data just that—confidential. And, for organizations that entrust their data to cloud storage, it is essential that they understand the options available for safeguarding this protected data—even if it's being managed in the cloud by a third-party vendor. This white paper discusses the importance of data encryption, the vulnerabilities of third-party encryption, the necessity of encryption key ownership, and how all of it affects the security of your organization's data stored in the cloud.

Do You Have an Encryption Strategy for Data Stored in the Cloud?

To keep data safe from prying eyes, as well as comply with regulatory compliance mandates, you need to encrypt the data. Encryption codes the data in such a way that you need an encryption key to "crack the code" and gain access to it but the data encryption story doesn't end there. To truly keep data safe from unauthorized access, you need an encryption strategy that considers every facet of the encryption process: from the coding of the data to the creation and management (deployment, use, and disposal) of the encryption keys.

While Federal agencies are rapidly adopting cloud solutions, many agencies still hesitate to bring compliance-regulated or mission-sensitive data to the cloud. Handing off your most sensitive data to a third-party goes against the most deep-rooted security best practices. Who has access to your data? Who is protecting the cryptographic keys used to secure your data? Where is your data stored? Will you only use one cloud provider? These are all questions agency leaders should be asking themselves when they are looking to deploy either a complete or hybrid cloud solution.

In order to learn more about why encryption alone is not enough to secure your data in the cloud, you need to investigate the data encryption process by answering the who-what-when-where-why, and how of data encryption. And, while the technical specifications of the actual encryption method are not to be ignored, this paper specifically addresses the issues of ownership and access to encryption and encryption keys as they relate to safeguarding data stored in the cloud.

The "*Who-What-When-Where-Why and How*" of Data Encryption

Encryption is the cornerstone of data center security.
Recognized universally by analysts and experts as an underlying control for cloud data, encryption sets a high water mark for demonstrating regulatory compliance. Combined with strong key management that is controlled by the organization itself, encryption is a core mechanism for protecting data in the cloud.

For agency leaders and IT administrators, understanding the encryption process as it relates to the ownership of and access to an organization's data is crucial to securing it in the cloud. There are five basic questions that will help you evaluate whether or not you have provided your organization's cloud-stored data with the best protection possible.

1. **Who is encrypting the data that you currently are storing/ planning to store in the cloud?** In theory, your agency's encrypted cloud data cannot be accessed by any entity that does not hold the encryption key. That being said, it is imperative that you know who owns the encryption and the encryption keys to your agency's data.
2. **What protection is offered by your encryption scenario?** By identifying any points of vulnerability in your encryption scenario, you can find out if you are providing the utmost protection for data stored in the cloud and take steps to add extra security measures or change to a more secure encryption scenario.
3. **When and Where does your data become encrypted?** The answers to these questions provide significant insight into the safety of an organization's data stored in the cloud—from the most routine transactions to its most valued assets.
4. **Why is the encryption scenario so important?** The circumstances that encompass the encryption scenario are directly related to how safe your data actually is
5. **How does owning your encryption and your encryption keys make a difference in the security of your data?** Separating encryption ownership from the duties of cloud service provider (CSP) management offers you unmatched control of, and access to, the data you store in the cloud.

The Question of Accountability in a Breach-Prone World
While your data can be successfully managed in the cloud by a reputable third-party, the sole entity responsible for the data is YOU— from the moment you take possession of it and whether it is categorized as data-in-transit or data-at-rest. No exceptions.

Ownership and management of data are two very different things. If the data is stolen—you are responsible. If the data is lost—you are responsible. If the data is manipulated—you are responsible. So, while it's possible to outsource data encryption and management services as offered by three of the data encryption scenarios, keep in mind that you can't outsource ownership of that data. And, with this level of accountability, why would you trust the process of securing your data to anyone but yourself?

Understanding the Levels of Protection in the Three Data Encryption Scenarios

There are three encryption scenarios for data stored in the cloud. They are:

1. Server-Owned Encryption and Keys
2. Server-Owned Encryption with Customer-Managed Keys
3. Customer-Owned Encryption and Keys

To understand the level of protection offered by each of the three encryption scenarios for cloud storage, you need to be very precise about the security of the data—whether it's data in transit or data at rest. What you learn could mean the difference between thinking that your cloud data is secure and knowing that your cloud data is secure. Consider the following scenarios.

The Encryption Scenarios

1. Server-Owned Encryption and Keys

This is an encryption service offered by a third party, usually a CSP, who will encrypt your data for you in the cloud. As the entity performing the encryption, these cloud service providers have access to your unencrypted data because they create, manage, and hold the encryption keys.

Vulnerabilities

- You do not own or control the encryption.
- You do not own or control the use of the encryption key.
- Your encryption key is accessible if cloud service provider transactions, encryption infrastructures, or applications are compromised by internal CSP personnel or external adversaries.
- The CSP can both issue and revoke access to your data if there are paperwork glitches, payment issues, etc.

Because you do not own or manage the encryption keys, unauthorized requests to access your data, including those by the government, will be addressed by the encryption service provider—not YOU. And, if there are unauthorized requests for your data, you will not be able to confirm if your data has been surrendered by the Cloud Service Provider

2. Server-Owned Encryption with Customer-Managed Keys

Also offered by a third party, your data will be encrypted for you in the cloud, but you will be given management access to the encryption keys. As the entity performing the encryption, although with customer-provided keys, third party cloud service providers will still have access to the unencrypted data by default.

Vulnerabilities

- You do not own or control the encryption.
- You do not manage the use of the encryption key to perform the encryption of your data.
- Your encryption key is accessible if Cloud Service Provider transactions, encryption infrastructures, or applications are compromised by internal CSP personnel or external adversaries.
- The CSP can both issue and revoke access to your data if there are paperwork glitches, payment issues, etc.

3. Customer-Owned Encryption and Keys

When you own the encryption keys for your organization's data in the cloud, it CANNOT be accessed by any unauthorized entity that does not hold the encryption key. Data access requests may be made, but you—and ONLY YOU—will be able to answer them. Why?—because you own the data encryption AND the encryption keys.

Advantages of Owning Your Encryption and Your Encryption Keys:

- You address any and all access requests for the surrender of your agencies' encrypted data.
- You manage the encryption key lifecycle and storage.
- You define and control data access permissions for organization personnel, partners, vendors, customers, etc.
- You are the only entity with access to data because you own the data encryption AND the encryption keys.

Three Rules for Encrypting Data Stored in the Cloud

1. Own your encryption so that you can address any and all access requests for the surrender of your company's cloud data.
2. Own and manage the encryption key lifecycle to demonstrate compliance and ensure that your cloud data is always secure.
3. Define and control data access permissions for company personnel, partners, vendors, customers, etc. to prevent unauthorized access to your cloud data.

Not All Encryption Is Created Equal: Server-Side Encryption vs. Client-Side Encryption

The who, what, when, where, why, and how of data encryption matters. There are variations on each scenario, but here's the basic difference between Server-Side Encryption and Client-Side Encryption.

Server-Side Encryption (SSE)	Client-Side Encryption (CSE)
AKA: Service Provider-Managed Encryption	**AKA: Customer-Managed Encryption**
How it works: Encryption is performed by the CSP server as part of the process of saving the data in cloud storage. It uses encryption keys that are accessible, and often times owned by the CSP.	**How it works:** Encryption is performed by the customer's client before uploading the data to cloud storage. It uses encryption keys that are owned and managed by the customer.
Does it meet security requirements? No; when a CSP owns the encryption and the data is encrypted in the cloud it is vulnerable to attack and unauthorized access--even in instances where the customer manages the keys	**Does it meet security requirements?** Yes; when a customer owns the encryption, it is safe from attacks and unauthorized access. Customer-managed keys ensure data ownership and control.

The Migration of Data to the Cloud Requires Due Diligence

To accommodate the migration of data storage to the cloud, Cloud Service Providers have promised—and delivered on—a wide range of benefits to organizations that includes significant cost savings, accelerated innovation, enhanced agility, and more. This is good news for businesses who want to enjoy the many business benefits of cloud storage. But whether your data is stored on premises or in the cloud, business leaders and administrators responsible for the safety of confidential organization/customer/vendor/prospect/ partner data must perform due diligence by knowing the answers to the who-what-when-where-why, and how that data can be accessed in spite of (or because of) the security measures that are in place to safeguard it.

Conclusion

Every agency has an obligation to do everything in its power to make certain that its data is secure—whether it is stored on premises or in the cloud. This close examination of the available encryption scenarios for cloud platforms revealed data access vulnerabilities that aren't a factor when you make the decision to own your encryption and your encryption keys. For federal agencies, the best encryption strategy is the one that provides you with complete control of your sensitive and non-sensitive data so that it cannot be accessed by unauthorized users—including the Cloud Service Provider who offers storage or key management services in either a private or public cloud network. So, whether you are moving data to the cloud for the first time or refining an existing cloud security scenario, the only way to know that your cloud data is truly secure is to own your encryption and your encryption keys. Encryption ownership is the difference between thinking and knowing that your cloud data is secure.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com