thalescpl.com

THALES

Hybrid Cloud Data Security and Control

A hybrid cloud strategy enables organizations to leverage the agility, cost savings and scalability of the public cloud services while retaining private cloud or other on-premises infrastructure for regulatory compliance, cost savings, or I/O performance.

While the security of most cloud platforms is strong, deploying effective security controls for data flowing between multiple clouds or hybrid systems can be challenging with proprietary tools and APIs. This leads to profound gaps around visibility, control, and consistency.

If your organization is seeking the best strategy for a hybrid or multi-cloud world, ask yourselves a few questions:

- Do you have any control and visibility over your cloud data?
- Can you prevent the cloud administrators from gaining access to your sensitive data?
- How do your protect your data in case of a breach or subpoena?
- Can you independently audit and prove compliance to regulatory mandates?
- How do you manage your cryptographic keys across multiple vendors and environments?

Regardless of the cloud service model or provider, the security of your organization's data in the cloud is YOUR responsibility.

- Are you aware of the pitfalls of isolated data encryption deployments?
- Does the use of multiple cloud providers require an agnostic approach to security?
- Do you have the flexibility to port your applications and data from one cloud service to another, or between on-premises and multiple cloud providers?

With cloud providers offering diverse services and models, answering these questions and ensuring that your data is secure is ultimately your organization's responsibility.

Hybrid Cloud Drivers and Challenges

Recent Thales research illustrates the many drivers to multi- and hybrid-cloud architectures. The architectures present a range of benefits and challenges.

Our research shows that 84% of organizations are adopting a multicloud strategy due to reasons such as application suitability for specific clouds, to mitigate lock-in to a single cloud provider, different teams' selections (with the corresponding risk of shadow IT), and, of course, to enable pricing leverage. The challenges of multicloud then become clear: different workflows and management tools, lack of unified security monitoring across providers, and the challenges of sharing data across cloud providers.

Turning to hybrid cloud, drivers include improved security, simplification and standardization, improved IT agility, and the potential to save expenses while leveraging fully amortized on-premises IT resources. Regardless of cloud providers and models, the primary hybrid cloud challenges are around both security and control.

Multicloud and hybrid cloud drivers and challenges present opportunities to approach cloud security with thought and foresight.

Security is both the top driver as well as the inhibitor for hybrid cloud adoption.

Cloud security approaches

To truly leverage the power of cloud, you need the ability to independently audit and prove that both your data and the encryption keys are always secured and under your control and visibility.

Ask a few questions to see if the security that comes with your cloud service is sufficient for your organization:

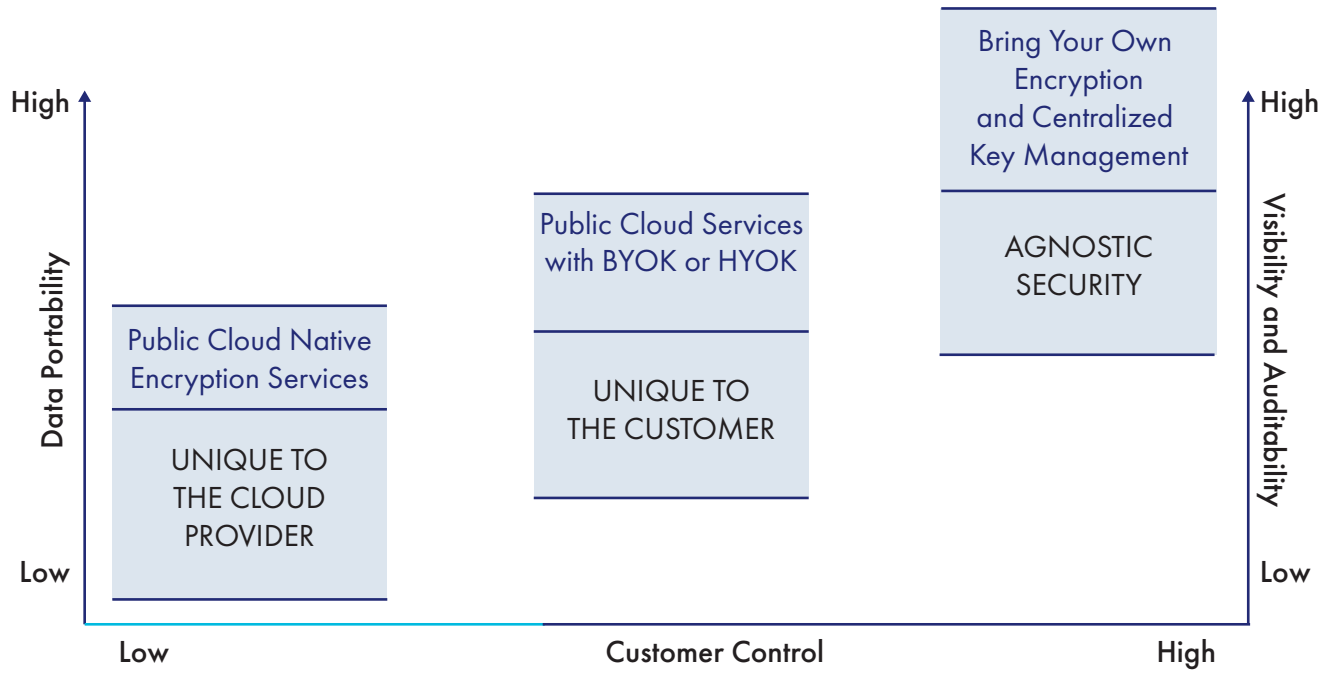
- Does the cloud provider provide encryption? If so, do you have the necessary controls and visibility to protect the encryption keys and perform audits?
- If the provider does not offer encryption, can you bring your own encryption and key management to the cloud?

Cloud security varies greatly depending on the cloud provider and deployment model you use. Broadly speaking, there are three options as shown below:

1. Bring your own encryption and centralized key management: This allows you to secure your sensitive data the way you like, across your hybrid world, with maximum control, visibility, and portability. It is agnostic to clouds, vendors, and location, giving you the flexibility to unify security for operational simplicity and compliance.

2. Cloud encryption services with Bring Your Own Key: to comply with best practices regarding encryption key management, most mainstream IaaS/PaaS providers offer Bring Your Own Key (BYOK) Application Programming Interfaces (APIs) with some offering Hold Your Own Key (HYOK). In a multicloud environment with unique BYOK API's, you are likely to need additional tools to manage BYOK encryption keys.

3. Utilize native encryption services: these are unique to a cloud service provider and completely managed by them. Depending on your risk profile and sensitivity of data, you may need to complement these services with additional tools for visibility, control and portability.



Bring Your Own Encryption

Thales offers a comprehensive range of encryption and tokenization solutions with the Vormetric Data Security Platform and SafeNet High Speed Encryptor. The Vormetric Platform enables you to centralize control and key management for all of you encryption deployments so that you can achieve consistent security and compliance.

- **Vormetric Transparent Encryption** protects data stored in both on-premises and cloud storage with file-level encryption and access controls.
- **Vormetric Application Encryption** enables you to secure your sensitive data as soon as it is generated or processed in an application running on cloud or on-premise environment.
- **Vormetric Tokenization with Dynamic Data Masking** enables you to reduce the scope of your compliance audits by tokenizing your sensitive data and eliminating the occurrences of clear data from your environment.
- **SafeNet High Speed Encryptor (HSE)** secures your sensitive data on the move, including real-time audio and video streams, from your data center to cloud or other sites.

Centralized key management and protection for operational simplicity

Encryption and tokenization without proper key management and protection can lead to a host of breaches and compliance related issues. Centralized key management allows you to leverage the cloud services without giving up the control of your keys to the cloud providers.

Streamline Data Security Control:

The Vormetric Data Security Platform centralizes enterprise key management with the Vormetric Data Security Manager (DSM). The DSM controls keys and polices for the platform's products, including key management.

Thales cloud security solutions enable you to protect your sensitive data consistently across your entire enterprise - on-premises, hybrid, or multi-cloud environments - with full visibility and control.

The DSM can be deployed in public and private clouds, or deployed as a physical deployment. This enables a flexible architecture that allows you to meet the needs of your organization in a consistent way.

Strong Crypto Key Protection:

- **SafeNet Data Protection On Demand (DPoD)** is a cloud-based platform that provides a wide range of fully managed cloud Hardware Security Module (HSM) services through a simple online marketplace. With zero upfront capital investment and pay-as-you-go pricing, you have the capability to simply click and deploy available services in minutes to meet your organization's business needs.
- **SafeNet Luna HSMs** allows organizations to leverage high assurance, tamper-resistant, FIPS 140-2 validated appliances in their on-premises environment to generate and secure their cryptographic keys and operations. They are also available as dedicated appliances through AWS, Azure and IBM Cloud services.

Bring Your Own Key

Many cloud service providers offer data-at-rest encryption capabilities with the encryption keys managed by the service provider. But for better compliance with both best practices and a range of data protection mandates, many providers also offer Bring Your Own Key (BYOK) services.

With BYOK, customers have the ability to generate and import the encryption keys or key material for their cloud-native encryption services. Thales leverages the cloud provider BYOK APIs to provide different solutions and services for greater control and visibility:

- CipherTrust Cloud Key Manager
- SafeNet Data Protection On Demand
- SafeNet Luna Hardware Security Module

Supported clouds include Microsoft Azure, Microsoft Office 365, Microsoft Azure Stack, Microsoft Azure National Clouds, Amazon Web Services, Salesforce, Google Cloud Platform, and IBM Cloud.

Hold Your Own Key

With HYOK, organizations have 100% confidence that they own and control the encryption key lifecycle while leveraging the Microsoft Azure cloud encryption services.

The integration between Azure Information Protection and SafeNet Luna HSMs enables you to generate and store your encryption keys in your on-premises HSMs as opposed to storing them in the Azure Cloud, and manage them according to your own security policies and compliance-related requirements.

As a result, access to internal and highly sensitive data associated with Microsoft Azure applications and services such as Office 365 always remain under your control, allowing you to achieve maximum security and auditability.

To gain the most from your hybrid cloud solutions, you must ensure that your sensitive data can move securely and quickly between environments.

Thales data protection for the hybrid cloud

Organizations are optimizing their private and public cloud investments by adopting hybrid cloud solutions. To gain the most from this investment, they need to ensure that data can move securely and quickly between environments.

Thales data protection solutions for hybrid clouds allows your architects to ideally mix native cloud encryption solutions and Bring Your Own Encryption solutions, while always controlling the encryption keys and access policies.

As a result, your IT and security teams can gradually streamline their operations, enabling you to have greater visibility and control over your sensitive data no matter where it migrates.

With Thales' market-leading data protection solutions and experts, "encrypt everything" has never been easier.

For more about Thales cloud security offerings visit www.thalesesecurity.com/cloud-security

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com