ENTRUST

New Strategies for Multi-Cloud Data Protection

FEATURING RESEARCH FROM FORRESTER

Best Practices: Cloud Data Encryption

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

Enterprise adoption of multiple cloud platforms continues in earnest whether it's aimed at improving collaboration, reducing datacenter 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 in order to be effective and meet compliance mandates. Forrester's new recent research articulates a number of important best practices, 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 keys regularly to ensure alignment with compliance requirements and auditor expectations

These security measures are critical to protecting your cloud data and workloads, and it's vital to get them right from the outset. Following the Forrester report find out how Entrust can help you meet your cloud data protection goals while reducing your administrative and compliance burden. Entrust.com/HSM

IN THIS DOCUMENT

Best Practices: Cloud Data Encryption

Cloud Data Encryption Is A Key Enabler Of Cloud Migrations

by Andras Cser

November 11, 2020 | Updated: November 12, 2020

Why Read This Report

As firms and software vendors migrate their workloads and their sensitive data to the cloud, cloud data encryption (CDE) is becoming a critical priority for them. This document assesses various architectural options of encryption key management (pros, cons, and best practices for each) and highlights application CDE integration best practices as well.

Key Takeaways

You Can't Move To The Cloud Without Cloud Data Encryption
To reduce the threat surface and likelihood of breaches as well as to satisfy auditors' requests for repeatable data protection in the cloud, most firms believe that they can't even begin migrating their workloads and data to the cloud without proper data encryption.

Separate Encryption Keys From The Data
Keeping data together with encryption keys increases the likelihood of an attacker finding the keys, decrypting them, and exfiltrating sensitive data to the outside. Keeping encryption keys in hardware security modules is a key step toward securing the keys, ensuring separation between the data and the keys.

Never Lose Sight Of Data Manipulation Support
As data flows between applications and environments, various apps and infrastructure components (proxies, etc.) do search, sort, filter, and extract transform load (ETL) operations on the data. CDE should always support these data manipulation steps to be accepted by business and developer stakeholders.

Best Practices: Cloud Data Encryption

Cloud Data Encryption Is A Key Enabler Of Cloud Migrations

by Andras Cser
with Merritt Maxim, Benjamin Corey, and Peggy Dostie
November 11, 2020 | Updated: November 12, 2020

Table Of Contents

Related Research Documents

Best Practices: Cloud Governance

Hybrid Cloud Security Best Practices

Now Tech: Payment Tokenization, Q1 2019

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Cloud Migration Mandates Cloud Encryption

Cloud encryption and data protection used to be a nice to have. With breaches stemming from overprivileged storage instances containing unencrypted, sensitive data, the importance of encryption has been increasing. Using IaaS and SaaS mandates that you: 1) understand where your sensitive data elements are and 2) can protect them. To enable cloud migrations, firms have to encrypt data in cloud workloads because:

- **Migrating workloads to the cloud without data protection is challenging.** Although companies recognize that not all data is sensitive or personally identifiable (PII), they don't have a reliable, automated way of separating sensitive and nonsensitive data, and they still feel they need to encrypt *all* structured and unstructured data that moves to the cloud. Firms report that because of cloud data breaches in the past, they are hesitant to migrate unprotected, cleartext data to the cloud.

- **Compliance and audit requirements are getting stronger.** Most companies are subject to PCI DSS (which requires that all payment card data should be encrypted) and numerous other, vertical- or country-specific compliance mandates (GDPR, HIPAA, FERC/NERC, CCPA, GLBA, FIPS, PIPEDA, NYDFS, etc.), all of which require some form of data encryption. Previously, firms could mitigate these requirements by storing data in air-gapped, on-prem systems — something that is outright impossible in the cloud.

- **Multicloud IT deployments disperse data into multiple locations.** Interviewees reported that their data is in too many places: IaaS (AWS, Azure, Google Cloud Platform), SaaS (Salesforce, SAP), as well as other public and private clouds. Encryption and visibility of data across these platforms is highly problematic and requires careful planning of migrations and ongoing cloud encryption operations that require heavy administrative support. A German manufacturer said that in order to avoid vendor lock-in in the cloud, they mandate that workloads be distributed across multiple platforms, but since each platform has its own encryption key management system, it increases administrative costs.

- **Customer-owned key management is unresolved with old, cloudwashed COTS apps.** Firms often work with independent software vendors (ISVs) who move their tried-and-true, but legacy, on-prem commercial off-the-shelf (COTS) applications to the cloud. Forrester estimates that in 70% to 80% of the cases ISVs purely migrate the on-prem app to an IaaS platform (in which the ISV provides management services for their app) without refactoring or rewriting (we call this "cloudwashing"). In such instances, data protection, customer-managed keys (CMK), or bring your own encryption/keys (BYOE/BYOK) is especially problematic since the old, on-prem app has no concept of BYOE/BYOK.[1]

IaaS Key Management And Hardware Security Modules Provide CDE

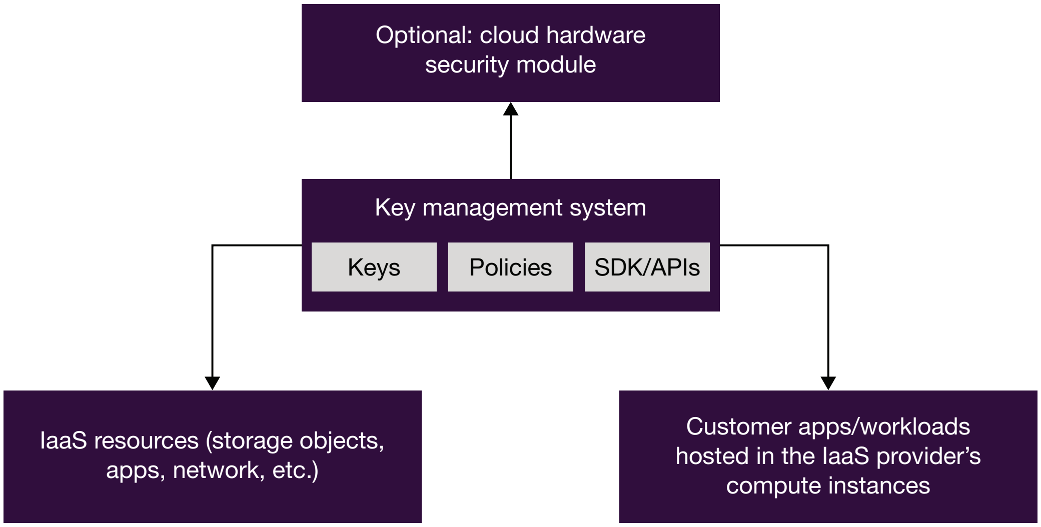
Cloud data encryption provides a mechanism to address these data security issues when moving workloads into the cloud. While CDE processes and solutions come in many shapes and sizes, we can identify several archetypical design patterns.

USE THE NATIVE CLOUD ENCRYPTION METHOD PROVIDED BY THE CLOUD PLATFORM

This pattern involves using AWS's Key Management System (AWS KMS), Azure Key Vault, Google Cloud Key Management, and other similar IaaS-provided key management IaaS platform features. These CDE methods offer an integrated, usually FIPS 140 Level 2 encryption key management service with the ability to create and manage your own keys (see Figure 1).

- **Pros: price, preintegration, key import.** Cloud native KMS is relatively inexpensive compared to other methods. It's very easy to integrate with IaaS-provided databases, data and object storage, and network security constructs of the IaaS environment. They support an optional managed, cloud hardware security module-based KMS that serves as a back end to store and protect customer-supplied keys. Customers can create their own or import keys from other sources. Key tagging, inventory, expiration, and deletion are also supported.
- **Cons: lack of key separation from encrypted data; some IaaS pieces are unsupported.** Our interviewees report that the greatest challenge with IaaS KMS is that keys are not entirely separate from apps and data they encrypt and protect: In a breach, an adversary could gain unauthorized access to the keys stored in the IaaS KMS then decrypt and exfiltrate all customer data. Further downsides include: 1) no interoperability with a different IaaS platform's key management system and encryption methods, 2) no uniform coverage of all IaaS apps across all geographies, 3) limited support for encryption algorithms and preexisting customer key import, and 4) versatile but very complex access policy enforcement to keys. Automatic key rotation support is still spotty.
- **Best practices: separate key storage for each environment, identity controls for keys.** When using IaaS-provided CDE, ensure that it covers all geographies and IaaS-provided applications and has the ability to import all your key types. Make sure you have a separate key vault for each environment (dev, user acceptance testing, integration, staging, and production). Make sure you define and then manage access roles for admins (using solutions such as those from IBM, One Identity, Oracle, and SailPoint) and apps to use keys by creating a strong roles-based access control scheme in the management console of your cloud service provider, thus ensuring separation of duties (SoD) when it comes to handling keys and encrypted data. If possible, also extend the KMS to cover other clouds you have.

FIGURE 1 High-Level Architecture For Using An IaaS-Provided, Native Cloud Key Management System


Optional: cloud hardware security module
Key management system
Keys
Policies
SDK/APIs
IaaS resources (storage objects, apps, network, etc.)
Customer apps/workloads hosted in the IaaS provider's compute instances

USE ON-PREM OR CLOUD-BASED HARDWARE SECURITY MODULES (HSMS)

In this scenario, companies store keys separately from cloud workloads in dedicated hardware (or in some rare instances, software) security modules, usually in a physical location and network separate from the IaaS providers. HSMs are purpose-built, tamper-evident and -resistant appliances that protect against unauthorized access to keys, data bus snooping, and physical attacks. IaaS providers also offer hosted, cloud HSMs based either on their own HSM technology or a third-party vendor's HSM solution (such as Entrust/nCipher, Thales, and Utimaco) (see Figure 2).

- **Pros: keys separate from workloads, high availability, tamper resistance.** When stored in an on-prem or non-IaaS HSM, keys are physically separate from where the encrypted data lives. HSMs are very mature technology, with high availability, scalability, serviceability, and crypto (encryption and decryption) performance built in. These HSMs have a broad range of supported legacy and modern infrastructure and apps and are offered in a range of form factors. With an on-prem HSM, the firm has full control over its data encryption keys and can avoid IaaS platform lock-in much more easily than with IaaS-vendor supplied KMS solutions. HSMs also provide flexible and versatile key rotation services.

- **Cons: you need to ensure physical security, network latency, immaturity for the cloud.** When you have an HSM on-prem, you must ensure physical security of your data centers, and control access to it. HSMs have to be protected like crown jewels: Access to them and their contents should be based on least privilege and Zero Trust principles to reliably defend against a major breach. Since HSMs are priced per unit (each with its performance specifications), they may be costly especially if keys are not used heavily, just stored. There is always network latency when on-prem HSMs manage keys and provide encryption in IaaS- and SaaS-hosted applications. In many instances, in the minds HSM vendors, cloud encryption integration for IaaS services and components is just an afterthought as support for PKCS#11 in the cloud is immature. In rare instances, IaaS infrastructure components may not be fully supported by your HSM, or IaaS resources may not fully support your HSM's capabilities. There are pros and cons of cloud platform-provided CDE and on-prem/cloud based HSMs (see Figure 3).

- **Best practices: SDK/API support, centralized single-pane-of-glass key management.** With HSMs, you have to take into consideration how cloud-hosted applications use encryption features and seek out vendors that support all programming languages used in your apps (including C, C#, C++, Python, Ruby, Java) across the broadest range of standards (KMIP, PKCS family of protocols).[2] Use one, centralized HSM infrastructure to manage keys for all on-prem, IaaS, and SaaS apps, regardless of which cloud provider hosts them.

FIGURE 2 Customer-Provided, On-Prem HSM Use High-Level Architecture

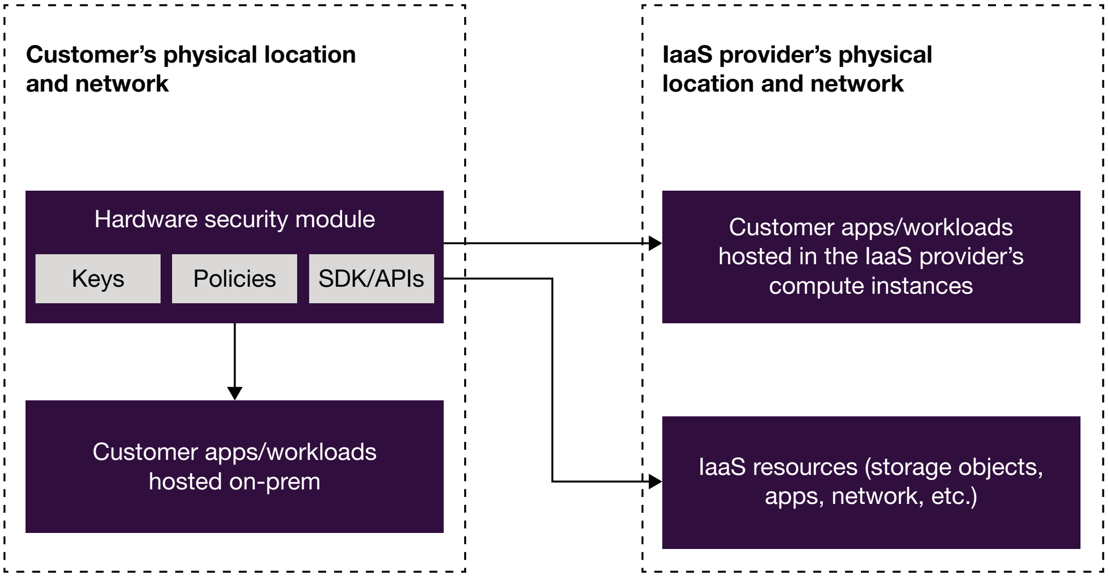

Customer's physical location and network
Hardware security module
Keys
Policies
SDK/APIs
Customer apps/workloads hosted on-prem
IaaS provider's physical location and network
Customer apps/workloads hosted in the IaaS provider's compute instances
IaaS resources (storage objects, apps, network, etc.)

FIGURE 3 Pros And Cons Behind Cloud Platform-Provided CDE And On-Prem/Cloud-Based HSMs

	Cloud platform provided CDE	On-prem/cloud-based HSMs
Pros	Price, preintegration, key import	Keys separate from workloads, high availability, tamper resistance
Cons	Lack of key separation from encrypted data, some IaaS pieces are unsupported	Hard to ensure physical security, network latency

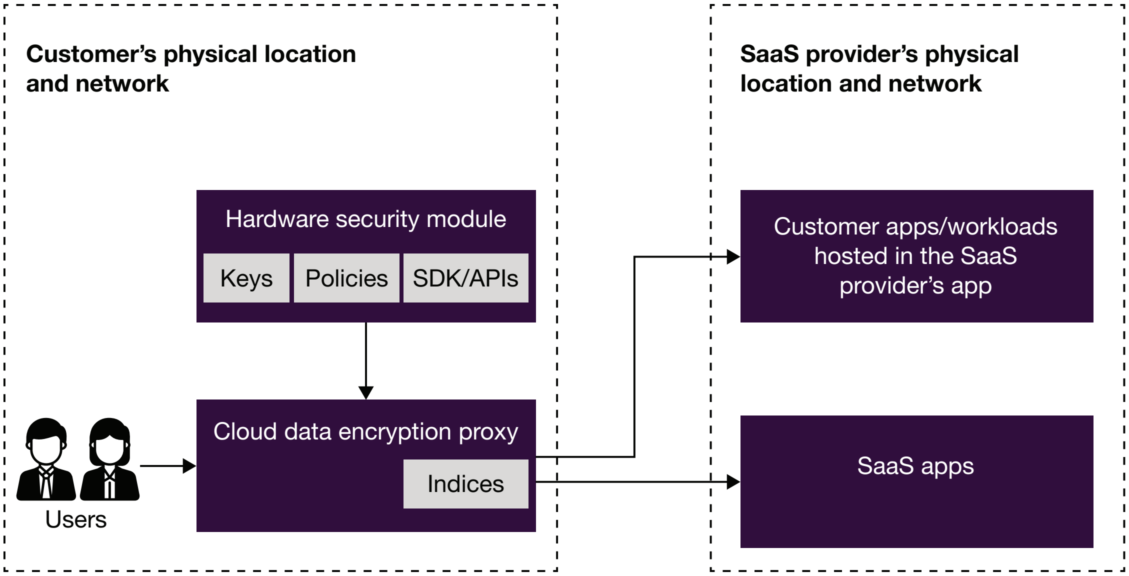
CDE Integration With Your Applications: Keep User Friction Low

CDE solutions can only do their job if they are integrated with applications. In-house applications may be easier to integrate than COTS applications since you have source code to make any necessary changes in in-house applications. Here are the key best practices when integrating CDE with your apps:

- **Always separate keys from data.** Keys should always be stored and managed separately from the data they encrypt. To enable this, make sure that: 1) you can bring your own keys to manage encryption in the app and 2) there are internal organizational boundaries between employees responsible for key management (IT security) and employees responsible for using the keys in apps and workloads (developers and DevOps). Use key management solutions that have productized support for managing keys in on-prem, private cloud, and public clouds. Most organizations we speak to use at least 2048-bit keys, and 4096-bit keys are becoming more common.
- **Never store keys in the clear.** This is easier said than done. In today's vast array of in-house and COTS applications, app developers and DevOps have been getting away with storing encryption keys in application configuration files. S&R pros should work with app developers to locate, identify, and replace these keys with industry-standard key retrieval and use mechanisms (such as a KMS solution or secret management solution). Scanning source code, combing through CI/CD (Ansible, Jenkins, Terraform, etc.) scripts for key material is often the first step here.
- **Minimize sensitive and PII data before it's transferred to the cloud and encrypted.** You must first scale down the volume of sensitive data because sensitive data must be tokenized or encrypted, and this can be expensive. In structured SaaS applications, such as client relationship management (CRM), it may be sensible to only protect names, dates of birth, and social security numbers, but not what services or products the customer has access to. Minimized sensitive and PII data will also help with speeding up encryption and decryption. Be sure to cover data encryption in transit, at rest, and at use.

- **Seek standards-based KMS solutions that require zero code changes.** You won't have access to the source code of the applications so it's critically important to find KMS solutions that support the apps' key management and CDE needs and which are based on open standards such as the Key Management Interchange Protocol and Public Key Cryptography Standards (PKCS). If the app does not support BYOE/BYOK, then push its vendor to update the app so it does.
- **Decide between proxy-based and API-based approaches for SaaS data encryption.** With most cloud security gateways (CipherCloud, Imperva, Microsoft MCAS) providing some level of proxy-based encryption, you may want to choose proxy-based if the app has no support for data encryption or if you don't want to use the app's native data encryption (such as Salesforce Shield) due to security concerns.[3] Be aware of the performance tax of a proxy-based CDE solution and the fact that you have to monitor all changes in the SaaS app, as changes may break the proxy-based CDE solution. Always ensure that admins who have access to key material will not be able to administer the cloud encryption solution or SaaS applications and that the CDE proxy presents no friction to users (see Figure 4).
- **Always keep data manipulation in mind.** Data manipulation (search, sort, filter, extract, transform and load, etc.) are indispensable and irreplaceable components of any application's business logic. Be sure that your CDE solution supports format preserving encryption (FPE) and provides sufficient instrumentation and speed for data manipulation. Forrester often talks to firms that say their whole cloud migration was nixed because of being unable to cost effectively support data manipulation in and between applications.
- **Rotate keys at least annually.** Keys are everything in data protection, and if a key gets compromised, detecting its unauthorized use can take a long time. To minimize that likelihood, respondents said that their auditors increasingly ask for proof of key rotations in sensitive data-containing workloads. Some key finance apps may even have quarterly key rotation schedules; PCI DSS mandates that the keys must be rotated also when a user who access to key materials leaves the organization or when the key has been used to encrypt a certain number of transactions.

FIGURE 4 Proxy-Based Cloud Encryption High-Level Architecture


Customer's physical location and network
Hardware security module
Keys
Policies
SDK/APIs
Cloud data encryption proxy
Indices
Users
SaaS provider's physical location and network
Customer apps/workloads hosted in the SaaS provider's app
SaaS apps

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Supplemental Material

COMPANIES INTERVIEWED FOR THIS REPORT

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

CipherCloud

Equinix

Fortanix

Ionic Security

Kindite

nCipher

StorMagic

Utimaco

Endnotes

[1] BYOE/BYOK is bring your own encryption and/or bring your own keys. BYOE means that the customer can use a pluggable cloud encryption algorithm across multiple components of the IaaS or SaaS platform. BYOK means that the cloud platform offers its own encryption algorithm and the customer can bring (import and manage) their own encryption keys.

[2] Source: Tony Cox, Judith Furlong, and Jeff Bartell, "OASIS Key Management Interoperability Protocol (KMIP) TC," Oasis (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip) and Mohan Atreya, "Introduction to the PKCS Standards," Shippensburg University School of Engineering (https://web.cs.ship.edu/~cdgira/courses/CSC434/Fall2004/docs/course_docs/IntroToPKCSstandards.pdf).

[3] In the case of proxy-based encryption, the proxy is either on-prem or in the cloud performing the encryption and decryption operations on the bidirection data streams between the user and the cloud app.

Security concerns include legacy algorithms or the app provider having access to both the data and the encryption algorithm.

FORRESTER®

forrester.com

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- › Research and tools
- › Analyst engagement
- › Data and analytics
- › Peer collaboration
- › Consulting
- › Events
- › Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

› **Security & Risk**

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

ENTRUST

MULTI-CLOUD DATA PROTECTION STRATEGIES

Multi-cloud computing is here to stay – and so are the complexities associated with protecting your data and workloads.

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.

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 hardware security modules (HSMs) to protect your encryption keys.

Entrust nShield® HSMs

Entrust nShield HSMs are FIPS and Common Criteria certified that act as a root of trust for multi-cloud deployments at enterprises worldwide. The unique nShield Security World architecture provides unmatched scalability, allowing you to use a centralized HSM infrastructure to manage keys for all cloud environments, as well as on-premises.

Entrust nShield Software Option Packs

The Entrust nShield option packs amplify the power of your nShield estate, allowing you to expand your cloud security capabilities. The nShield Web Services Option Pack provides a REST-like API that delivers FIPS-certified cryptographic key and data protection services to your cloud and on-premises applications. The nShield Cloud Integration Option Pack lets you generate keys with your own nShield HSM and export them for use in the cloud (familiarly known as Bring Your Own Key). And the nShield Container Option Pack gives your cloud-based containerized applications access to highly scalable crypto capabilities.

Entrust KeyControl®

Entrust KeyControl allows businesses to easily manage encryption keys at scale. Using FIPS 140-2 compliant encryption, KeyControl simplifies the management of encrypted workloads by automating and simplifying the lifecycle of encryption keys, including key storage, distribution, rotation, and key revocation.

Entrust DataControl®

Entrust DataControl® provides universal data encryption, policy-based key management and workload security for your multi-cloud infrastructure. DataControl secures workloads throughout their lifecycles, across your multi-cloud infrastructure. This provides greater protection of your organization's critical and sensitive information while enabling compliance with data privacy regulations.

To find out more about Entrust nShield HSMs and data protection solutions visit entrust.com/hsm or email HSMinfo@entrust.com.