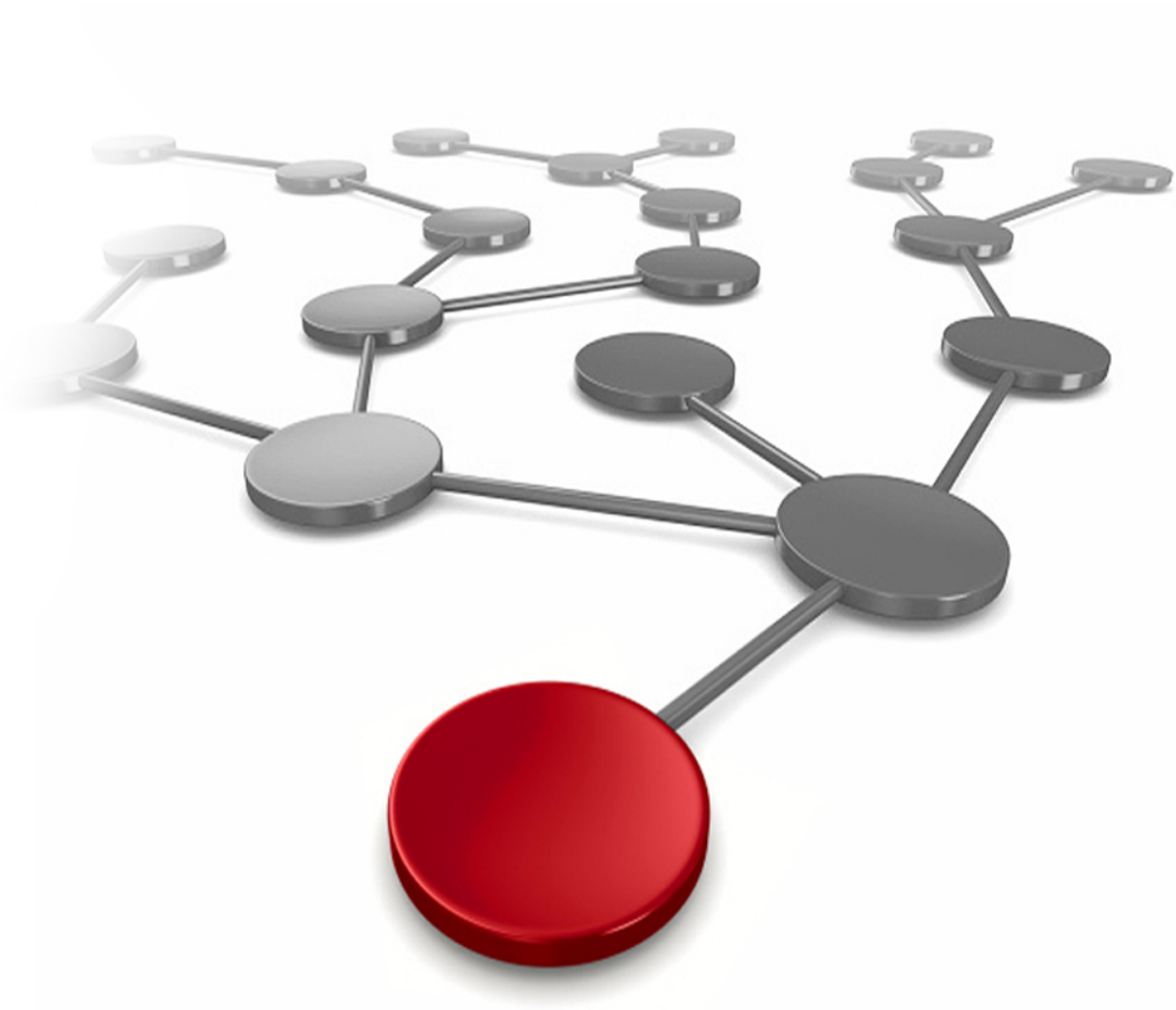
Redbooks
ibm.com/redbooks

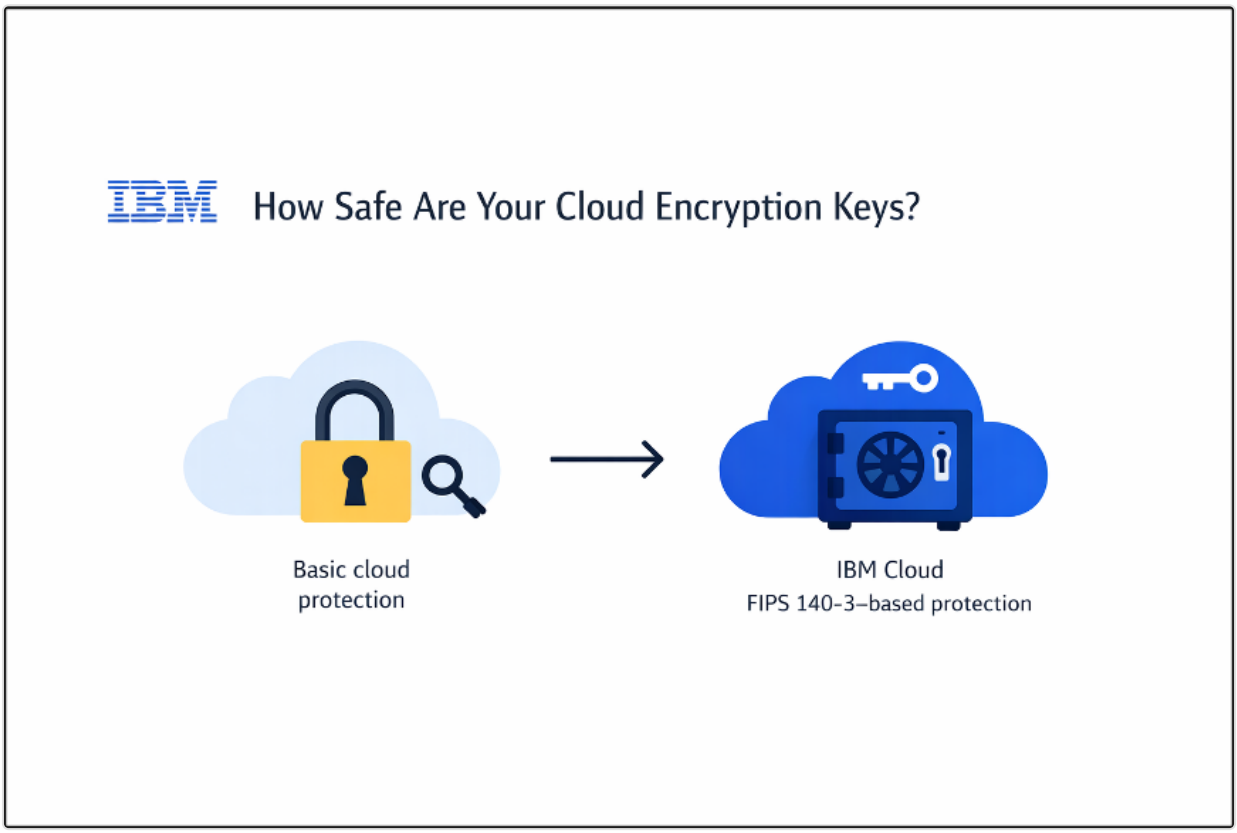
How Safe Are Your Cloud Encryption Keys?

Lokesh Bhatt
Dinesh G V



IBM

How Safe Are Your Cloud Encryption Keys?



How Safe Are Your Cloud Encryption Keys?

Introduction

This publication begins with a simple, everyday question – where do you keep the keys to the things that truly matter to you?

Most people don't keep:

- their house keys on the dining table,
- their car keys under the doormat,
- their locker keys taped to the locker.

Instead, we instinctively choose different levels of protection:

- A drawer for something ordinary
- A locker for valuables
- A bank vault for assets that cannot be compromised

The more valuable the asset, the stronger the protection we expect for the keys protecting it. The same principle applies in the digital world.

Today, organizations store their most valuable assets in the cloud:

- customer data
- financial records
- healthcare information
- intellectual property
- AI models
- business-critical applications

And just like physical valuables, all of these are ultimately protected by one thing: **cryptographic keys**.

Authors

Lokesh Bhatt is a senior technology leader with deep expertise in Hybrid Cloud, AI Infrastructure, and mission-critical enterprise platforms. With an overall experience of 20 years, he has led complex modernization programs, architected large-scale SAP and PowerVS deployments, and advised CXOs on cloud transformation strategies. Lokesh is recognized for bridging business vision with engineering execution, driving measurable outcomes across performance, resilience, and cost optimization. He frequently collaborates with global product teams, contributes to cloud architecture best practices, and is passionate about democratizing AI-enabled infrastructure for enterprises.

Dinesh G V is a technical leader building enterprise-scale applications with deep expertise in IBM Cloud and cloud-native architectures. Dinesh leads development of observability solutions and integrations, driving reliability, performance, and operational insights for enterprise workloads. Dinesh has been recognized for technical leadership, innovation, and mentoring high-performing teams, with multiple patents and industry recognitions.

Are My Encryption Keys Secure in the Cloud? Why Should I Worry About Them?

When organizations move to the Cloud, encryption is often considered the primary line of defense. But encryption is only as strong as the protection around the encryption keys themselves.

If someone gains access to the keys:

- encrypted storage can be decrypted
- backups can be read
- databases can be exposed
- sensitive workloads can be compromised

In many ways, encryption keys become the *master keys - the cryptographic roots of trust that secure all protected data* - for an organization's digital kingdom.

This raises an important question: **"Who protects those keys in the cloud?"**

Can I Trust My Cloud Provider to Guard My Keys?

Cloud providers invest heavily in security. But for sensitive and regulated workloads, customers increasingly ask deeper questions:

- Where are my master keys stored?
- Who can access them?
- Can cloud administrators see them?
- What happens if someone tampers with the hardware?
- How do I verify the provider's security claims?

This is where **Hardware Security Modules (HSMs)** come in.

An HSM is essentially a highly secure vault designed specifically to store and protect cryptographic keys. But not all HSMs provide the same level of protection. Some rely mainly on software protections, while others are designed to actively resist sophisticated physical attacks.

How Can I Trust an HSM? Are There Standards That Help?

That is why the industry relies on security standards such as **FIPS 140-3**.

FIPS 140-3 is the latest NIST standard for cryptographic modules, such as Hardware Security Modules (HSMs), that protect encryption keys in the cloud.

Think of it as a certification standard for the *"vault"* protecting your digital keys.

And just like physical vaults can provide different levels of protection, FIPS 140-3 also defines multiple security levels — ranging from basic software protections to highly hardened, self-defending systems.

How Much Protection Do I Really Need for My Cloud Keys?

FIPS 140-3 has four levels which can be understood using a simple analogy:

FIPS 140-3 Level	Physical Analogy	Cloud / HSM Equivalent
Level 1	Locked drawer	Software-based encryption protections
Level 2	Safe with tamper seals	Tamper-evident hardware with controlled access
Level 3	Bank vault	Hardened HSMs designed to prevent key extraction
Level 4	Smart vault with active countermeasures	HSMs that detect environmental attacks and zeroize sensitive cryptographic material

For many general-purpose workloads, Level 1 or Level 2 protections may be sufficient.

For most enterprise cloud environments today, **Level 3 HSMs** are considered the standard for strong cryptographic protection. They provide hardened hardware security designed to prevent master key extraction even during physical attacks, making them suitable for banking, enterprise SaaS, payment systems, and regulated workloads.

However, organizations operating in highly sensitive environments — such as government, defense, critical infrastructure, confidential AI, and highly regulated industries — may require even stronger assurances. That is where **Level 4** becomes important.

Level 4 systems are designed not just to store keys securely, but to actively defend them. If the system detects physical tampering, voltage manipulation, probing, or environmental attacks, the HSM can automatically destroy sensitive key material before it can be stolen.

In simple terms: **"The vault protects itself."**

How Does IBM Cloud Approach Key Protection?

Most cloud providers today rely primarily on FIPS 140-3 Level 3 HSMs, which already provide strong enterprise-grade security.

IBM Cloud® differentiates itself by investing in highly hardened HSM-based key protection designed for customers that require very high levels of cryptographic assurance.

IBM Cloud's key management offering, **IBM Cloud Key Protect (Dedicated)**, is built around customer-controlled encryption capabilities backed by hardware platforms designed for advanced tamper resistance and strong isolation of cryptographic keys. The underlying hardware platform is designed with capabilities aligned to high-assurance FIPS 140-3 Level 4 requirements and has been submitted to NIST for FIPS 140-3 Level 4 certification.

This approach is designed to provide organizations with:

- stronger protection for their root of trust,
- reduced operational exposure,
- enhanced protection for sensitive workloads,
- and support for demanding regulatory and compliance requirements.

In essence, IBM's approach to cloud key management focuses on combining **customer ownership of encryption keys** with highly hardened HSM protections designed for sensitive and regulated environments.

Review

Let's see if you remove some key ideas.

What makes encryption keys so critical to cloud security? ▼

Encryption keys become the master keys, the cryptographic roots of trust that secure all protected data, for an organization's digital kingdom.

What is an HSM and why does it matter? ▼

An HSM is essentially a highly secure vault designed specifically to store and protect cryptographic keys. But not all HSMs provide the same level of protection. Some rely mainly on software protections, while others are designed to actively resist sophisticated physical attacks.

What does FIPS 140-3 Level 4 mean in practice? ▼

Level 4 systems are designed not just to store keys securely, but to actively defend them. If the system detects physical tampering, voltage manipulation, probing, or environmental attacks, the HSM can automatically destroy sensitive key material before it can be stolen.

How does IBM Cloud approach key protection? ▼

The IBM Cloud key management offering, IBM Cloud Key Protect (Dedicated), is built around customer-controlled encryption capabilities backed by hardware platforms designed for advanced tamper resistance and strong isolation of cryptographic keys. The underlying hardware platform is designed with capabilities aligned to high-assurance FIPS 140-3 Level 4 requirements and has been submitted to NIST for FIPS 140-3 Level 4 certification.

Conclusion

As organizations continue moving critical workloads to the cloud, encryption alone is no longer enough. The real question is: **"Who protects the keys protecting my data?"**

Just as we naturally use stronger physical protections for increasingly valuable assets, cloud security must also evolve from basic encryption to hardened, tamper-resistant, and self-defending key protection systems.

Because in the end, protecting your encryption keys means protecting everything behind them.

References

- FIPS 140-3 — NIST
- IBM Cloud Key Protect

Notices