

THALES

CYBERSECURITY

The Evolving Role of HSMs

Key Market Forces
Driving Change

cpl.thalesgroup.com

Executive Summary

Cryptography is the foundation of digital trust, securing everything from customer transactions and sensitive data to digital identities and critical business applications. As organizations face increasing regulatory requirements, accelerated cloud adoption, AI-driven innovation, and the transition to post-quantum cryptography (PQC), managing cryptographic risk has become a strategic business priority.

Hardware Security Modules (HSMs) provide the trusted foundation for protecting cryptographic keys and securing the most sensitive operations across the enterprise. Today's HSMs must deliver more than strong security. They need to support crypto agility, quantum readiness, scalable deployment, and consistent governance across hybrid and multi-cloud environments. This makes HSMs a core component of trust infrastructure that enables resilience, compliance, and future-ready digital transformation.

Why This Matters Now

Cryptographic requirements are growing, while simultaneously, the landscape is changing rapidly. Organizations must prepare for the transition to post-quantum cryptography (PQC), meet growing regulatory requirements, support hybrid and multi-cloud environments, and secure AI-driven workloads to support innovation. These trends are increasing the demands on cryptographic infrastructure.

As a result, HSM selection has become a strategic infrastructure decision rather than simply a security purchase. Buyers should evaluate not only current capabilities, but also architecture, deployment options, ecosystem integration, governance, and the vendor's roadmap for future cryptographic requirements.

Choosing the right HSM is ultimately about more than protecting keys: it's about building a trusted foundation that can adapt as security, compliance, and business needs evolve.

Table of Contents

Executive Summary	2
Why This Matters Now	2
Industry Perspective	4
1. Post-Quantum Cryptography Is Raising the Stakes	4
2. Crypto Agility Has Become a Business Requirement	5
3. AI, Cloud, and Digital Transformation Are Expanding Cryptographic Demand	6
4. Compliance Expectations Continue to Rise	7
Upholding The Next Generation of Digital Trust	8
Final Takeaways	8
About Thales	9





Industry Perspective

Industry analysts are increasingly viewing HSMs as strategic infrastructure rather than standalone security devices. Several market forces are driving this shift.

01



Post-Quantum Cryptography Is Raising the Stakes

The transition to post-quantum cryptography (PQC) is one of the most significant changes to enterprise security in decades. Analysts from organizations including Gartner, IDC, Forrester, and NIST consistently emphasize that organizations should begin preparing now. Not because quantum computers can break today's encryption, but because cryptographic migrations take many years to complete.

The "harvest now, decrypt later" threat further accelerates the need for planning. Sensitive data stolen today may remain encrypted until future quantum computers become capable

of decrypting it. Organizations protecting intellectual property, financial records, healthcare data, government information, and long-lived digital assets cannot afford to wait until quantum computing becomes commercially viable.

HSMs are central to this transition. They provide the hardware root of trust required to securely generate, protect, and manage both traditional and post-quantum cryptographic keys while supporting controlled migration between algorithms.

Post-quantum migration is already in motion: 59% of organizations are prototyping and evaluating PQC algorithms
([Thales Data Threat Report, 2026](#))



Crypto Agility Has Become a Business Requirement

Industry analysts increasingly identify crypto agility as a defining capability for modern cryptographic infrastructure.

Rather than viewing cryptography as a static technology, organizations must now assume that algorithms, standards, regulations, and threats will continue to evolve. Enterprises need the ability to introduce new algorithms, rotate keys, update policies, and transition applications without disrupting operations.

Crypto agility reduces operational risk during technology transitions and allows organizations to respond more quickly to regulatory changes, emerging vulnerabilities, and future cryptographic standards.

HSMs that support flexible policy management, standards-based integration, and roadmap-driven algorithm updates are becoming essential components of enterprise resilience.

“Quantum safe by design requires the entire HSM internal stack and operating model to be designed around PQC capability, trust, and agility, not just added PQC algorithms. Most HSM vendors understand these architectural implications, but few have commercially-ready solutions that are quantum safe by design.”

[ABI Research: HSM Market Data Overview 2026](#)



AI, Cloud, and Digital Transformation Are Expanding Cryptographic Demand

Digital transformation is fundamentally changing how organizations use cryptography. As enterprises embrace AI, cloud-native applications, automation, APIs, software supply chains, and connected devices, the number of identities, workloads, and transactions requiring cryptographic protection continues to grow at an unprecedented pace.

Unlike traditional IT environments, modern digital ecosystems rely on cryptography at nearly every layer. It protects sensitive data, verifies the identity of users, devices, applications, and machines, secures software throughout the development lifecycle, enables trusted digital communications, and establishes confidence across increasingly distributed environments.

The rise of AI is further accelerating this demand. AI models, autonomous agents, and data-

intensive workloads require trusted identities, secure access to sensitive data, protected model artifacts, and verifiable software integrity. At the same time, organizations must secure growing volumes of unstructured data while maintaining governance across hybrid and multi-cloud environments.

Industry analysts increasingly view cryptography as foundational infrastructure for digital business rather than a standalone security function. As cryptographic operations continue to multiply, organizations need HSM platforms capable of delivering high performance, centralized key management, consistent policy enforcement, and seamless integration across on-premises, private cloud, public cloud, and SaaS environments.

70% expressed concerns about rapid change in AI ecosystems, making this the top-cited AI security risk ([2026 DTR Financial Services Edition](#))



The result is a shift in HSM requirements. Beyond protecting keys, modern HSMs must provide the scalability, automation, interoperability, and operational resilience needed to support enterprise-wide cryptographic services as organizations continue to expand their digital and AI initiatives.

04



Compliance Expectations Continue to Rise

Growing requirements from financial services, healthcare, government, critical infrastructure, and privacy regulations are increasing demand for hardware-backed trust due to their strong auditability and certified cryptographic controls.

Regulations can be time-consuming, especially since regulators increasingly expect organizations to demonstrate not only that encryption is used, but that cryptographic keys are generated, protected, rotated, and governed according to recognized best practices.

Industry analysts note that organizations investing in modern HSM platforms are often better positioned to satisfy evolving compliance requirements while reducing operational complexity.

Analysts consistently highlight two priorities for enterprise leaders:

- Build crypto agility to adapt quickly to changing algorithms and standards
- Establish a hardware root of trust capable of protecting cryptographic keys across hybrid and multi-cloud environments with clear interoperability.

83% of executives say compliance now consumes budget, talent, and operational bandwidth meant for growth.

[PwC 2025 Compliance Survey](#)



More importantly however, HSM selection must shift to a long-term infrastructure decision that will shape an organization's ability to remain secure, compliant, and resilient in the years ahead.

Upholding The Next Generation of Digital Trust

Analyst guidance increasingly encourages buyers to evaluate HSMs beyond performance specifications or certification checklists.

Modern HSM platforms should provide:

- Strong hardware root of trust
- Post-quantum readiness
- Crypto agility
- Hybrid and multi-cloud deployment flexibility
- High availability and scalability
- Broad standards-based integration
- Lifecycle management and automation

- A clear innovation roadmap aligned with evolving cryptographic standards
- As enterprises prepare for the next decade of cybersecurity, HSMs are evolving from tactical security devices into foundational platforms for the next generation of digital trust. Organizations that invest in scalable, crypto-agile HSM infrastructure today will be better positioned to navigate the transition to post-quantum cryptography while supporting the broader demands of AI, cloud transformation, regulatory compliance, and increasingly complex digital ecosystems.

Final Takeaways

Selecting an HSM is a long-term strategic infrastructure decision, not simply a technology purchase. As cryptographic requirements evolve and organizations prepare for the transition to post-quantum cryptography, the right platform must provide security, scalability, resilience, and the flexibility to adapt over time.

The strongest solutions combine this adaptability with a high-assurance security architecture, continuous software and firmware evolution, interoperability across existing environments, and a clear roadmap for adopting NIST-standardized post-quantum algorithms. This ensures organizations can respond to emerging threats and regulatory requirements while protecting long-term technology investments.

The strongest vendors consistently demonstrate three qualities: trust, innovation, and operational excellence. Beyond meeting today's security and compliance requirements, they offer proven execution, strong ecosystem integration, and a clear roadmap for supporting crypto agility and future cryptographic change.

By evaluating both platform capabilities and vendor maturity, organizations can invest in an HSM solution that protects critical assets today while providing the confidence to navigate tomorrow's security challenges.



About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than **30,000 customers**, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. 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.

Contact Us:

For contact information,
please visit cpl.thalesgroup.com/contact-us

THALES

CYBERSECURITY

[Contact us](#)

For contact information, please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com

