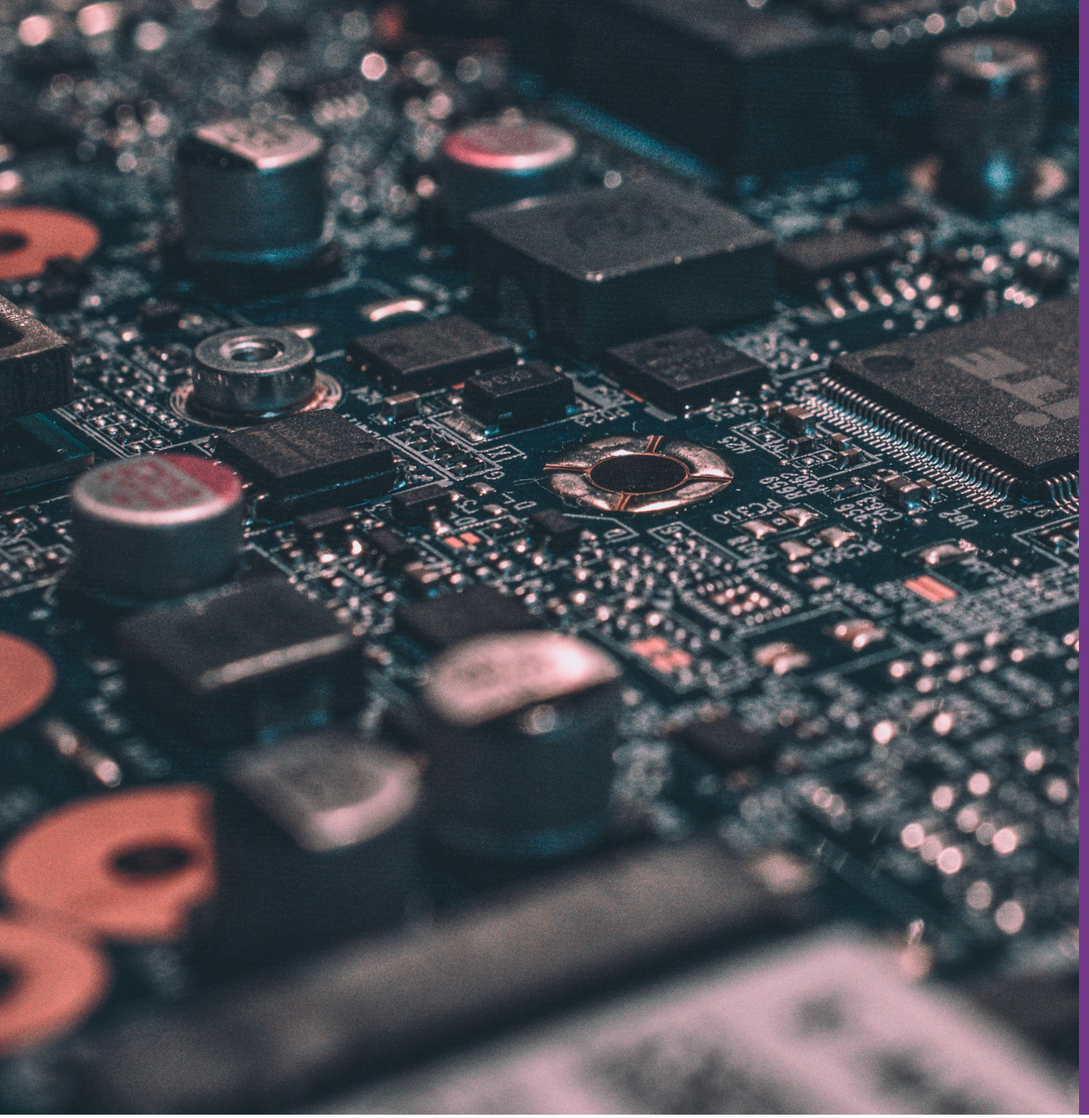


EBOOK

Buyer's Guide for Hardware Security Modules

Choosing the Right HSM and HSM Vendor for the Changing Security Landscape

ENTRUST

SECURING A WORLD IN MOTION

ENTRUST
SECURING A WORLD IN MOTION

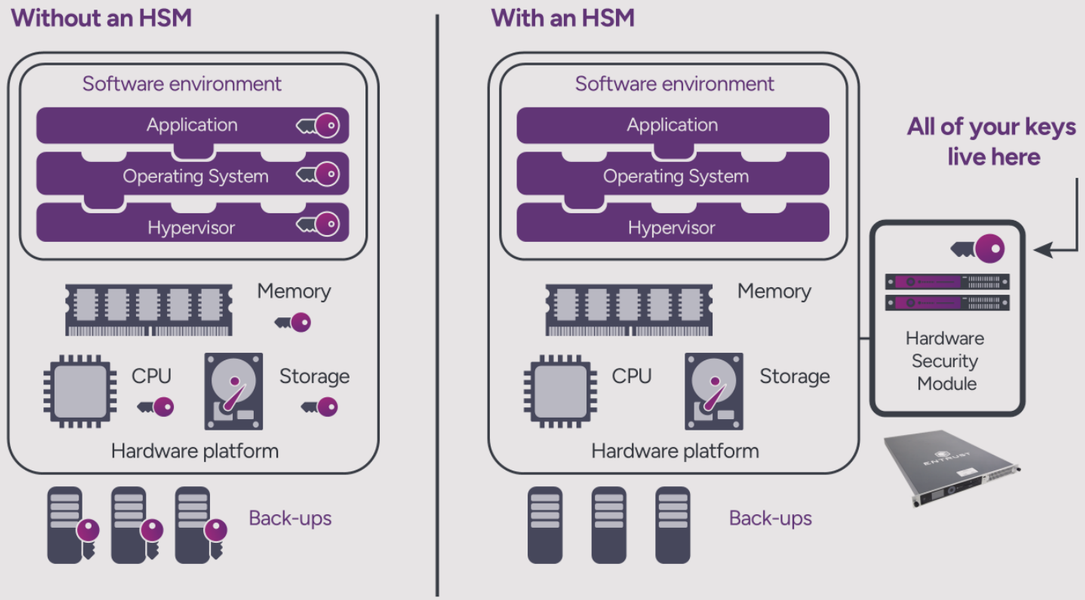
Table of Contents

Introduction

Organizations have relied on hardware security modules (HSMs) for almost three decades to safeguard their sensitive cryptographic keys. Academics and information security experts recognize that cryptographic keys are an organization's crown jewels, protecting its encrypted data. The alternative to HSMs, storing those high-value cryptographic keys in a data center server, was weak security. With a bit of know-how and the right tools, those keys could easily be located and stolen.

The reality is that stolen keys have become a preferred target for threat actors. It allows them to persist on the network sometimes beyond when the initial exploit is patched. Recent exploits leverage the theft of keys, such as SAML signing keys (like the golden SAML attack in SolarWinds) and machine keys (like the recent SharePoint Tool Shell attack).

Storing Keys in Software Vs. an HSM



History and Function of TPMs

Trusted Platform Modules (TPMs) originated in the late 1990s with the Trusted Computing Group (TCG), an industry consortium that developed the initial specifications.

A TPM is a specialized microchip integrated onto a computer's motherboard. It provides hardware-based security functions at the device level, such as securely storing cryptographic keys, protecting user and platform data, and ensuring the integrity of the boot process. By validating the boot chain, a TPM helps ensure the device has not been tampered with before it is even fully started.

While both HSM and TPM devices are designed to protect cryptographic keys and sensitive data, HSMs have become a standard component of most organizations' data security strategies as cybersecurity has evolved.

Attribute	TPM (Trusted Platform Module)	HSM (Hardware Security Module)
Purpose	Secures a single device (endpoint security)	Secures the entire network/ enterprise systems
Form Factor	An embedded chip within the device's motherboard	External/dedicated physical appliance
Security Level	Basic, suitable for device-level protection	High, tamper-resistant, FIPS-certified
Performance	Low (boot checks, basic encryption)	High (bulk cryptography, key management)
Use Cases	Full-disk encryption, device boot integrity	PKI, financial transactions, digital signatures
Scalability	Limited to individual devices	Enterprise-wide deployment and scaling

But Why HSMs and Not Trusted Platform Modules?

While both HSMs and TPMs are hardware-based security solutions, they serve different purposes and offer varying levels of security.

TPM is an embedded chip that aims to secure the specific device by ensuring system integrity during boot-up and providing basic key storage (e.g., for full-disk encryption). It is ideal for endpoint security.

On the other hand, an HSM is a dedicated, often external, physical device designed for high-performance cryptographic operations and comprehensive key management across multiple systems or an entire network. HSMs offer a higher level of security due to their tamper-resistant and responsive design, robust physical security measures, and adherence to stringent security standards like FIPS 140-2/3 and Common Criteria. They offer greater performance, scalability, and more sophisticated key lifecycle management capabilities. They are better suited for enterprise-level applications requiring strong security, such as financial transactions, digital signatures, secure manufacturing, and public key infrastructure (PKI).

Threat Landscape

The threat landscape is continuously evolving. Stolen signing or machine keys can allow adversaries to impersonate trusted systems, move laterally, and remain undetected long after an initial exploit is patched. Meanwhile, global cybercrime costs are expected to reach $12.2 trillion annually by 2031, according to the Cybersecurity Ventures Cybercrime Report.

In this environment, a “one-size-fits-all” approach to hardware security no longer works. Buyers should consider HSMs that not only meet current compliance standards like FIPS 140-2 and 140-3 but also offer future-proofing capabilities, such as support for Post-Quantum Cryptographic (PQC) algorithms and cryptographic agility.

But how do you choose the right one?

> Global Cybercrime Costs to Reach $12.2 Trillion Annually by 2031.
>
> **CYBERSECURITY VENTURES, OFFICIAL CYBERCRIME REPORT 2025**

Choosing the Right HSM

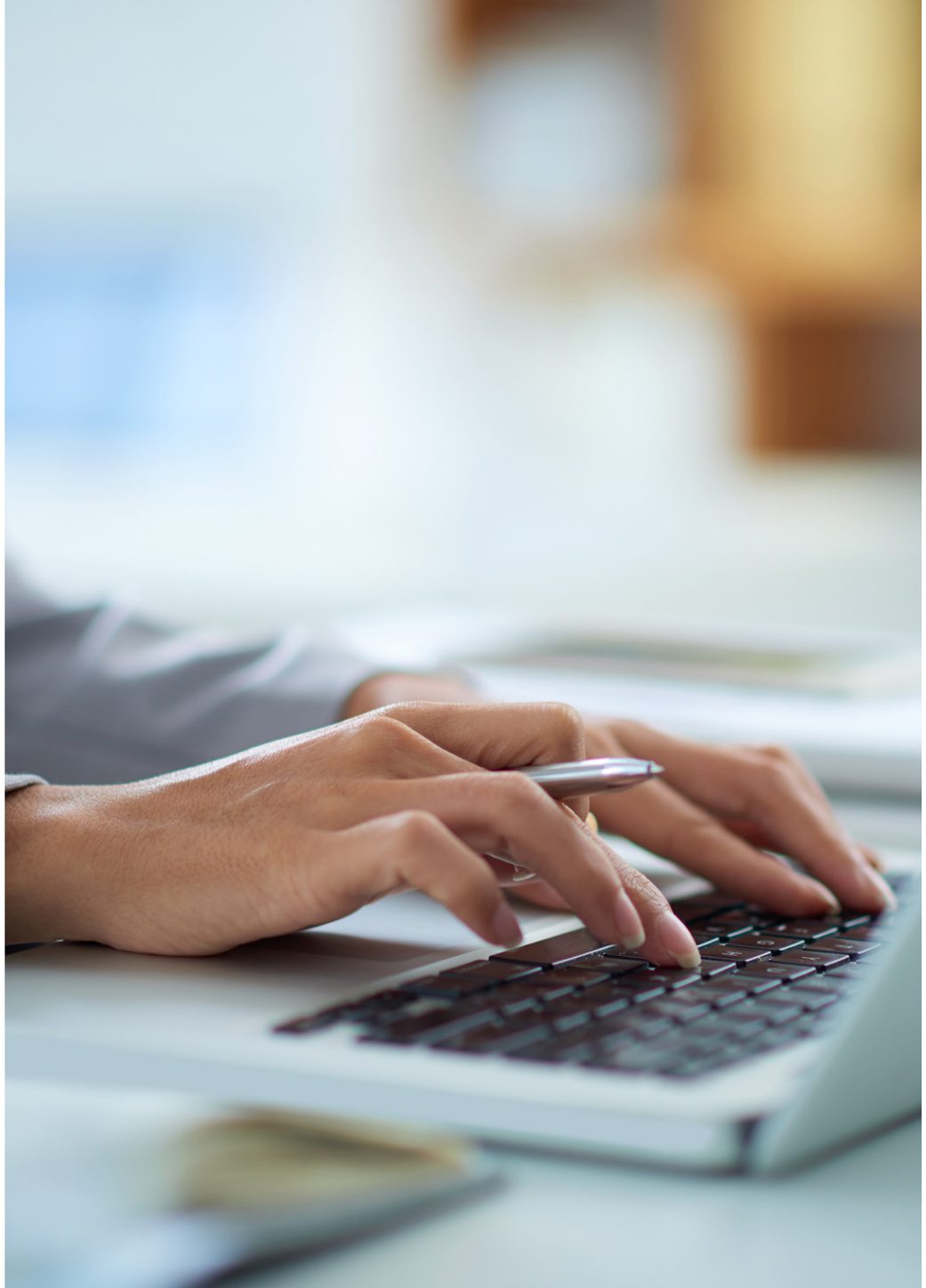
So, you've identified you have a business problem to solve; now you must adhere to industry or government security mandates, or perhaps you have been recently audited and have been advised to enhance your key management and protection procedures.

You are likely using an application such as a database or privileged access management tool that uses cryptographic keys for encryption or digital signing, and you've realized those keys need to be robustly protected. Your audit might have also identified the need to limit access to those keys to mitigate against insider threats and/or poor security hygiene. In such a scenario, organizations are faced with one question:

How to choose the right HSM that meets their needs and caters to the evolving threat landscape?

This guide assists organizations in selecting the best HSMs to meet their business and security needs. It provides a few recommendations by outlining a list of potential criteria to consider, irrespective of what organizations intend to use the HSM for.

In terms of scope, this guide will focus solely on general-purpose HSMs, not traditional payment HSMs used for card processing. Here are a few ways to identify the type of general-purpose HSM that is right for your organization and the factors you should consider before making a purchase decision.



Key Considerations When Selecting a Hardware Security Module

1. Technical Considerations

When looking to buy an HSM, the decision involves critically evaluating a range of factors to ensure optimal security, performance, and operational efficiency. These considerations range from the fundamental choice between on-premises, hybrid, or cloud-based deployment to the practicalities of form factor and the necessary performance metrics like speed for cryptographic operations.

Further, you should evaluate load balancing for high availability and scalability and backup capabilities to ensure business continuity, analyze compatibility through business applications, application programming interfaces (APIs), and account for ongoing serviceability, software updates, and scalability to meet future demands – like most critical IT infrastructure, HSMs are not a one-and-done solution. They need to be regularly maintained, with scheduled software and firmware updates.

Physical, Cloud, Or Hybrid

One of the first considerations when choosing an HSM is to decide whether you want to deploy physical on-premises HSMs or go down the cloud or as-a-service route. On-premises provides you maximum ownership, control, and possession of the keys and is often preferred by organizations that have high assurance requirements and may be reluctant to share high-value assets like cryptographic keys with a cloud provider.

If you are considering a cloud-based option, here are some of the themes relating to keys being managed in the cloud:

Ownership - aka Responsibility

- Specifically denotes to whom the keys belong
- In the comon cloud security responsibility model, information and data is always the responsibility the cloud consumer
- Keys that are instrinsically linked to the data they protect usually have the same characteristic

Control - aka Management

- Specifically denotes who can carry out the various key management lifecycle tasks
- Having control means being able to carry out key lifecycle tasks and often automating them but also includes precluding others from this capability

Possession or holding

- Specifically denotes who owns the infrastructure or geographioc location where the keys physically reside

There is a range of options available from the public cloud service providers. A native cloud-based HSM or key management solution is one option.

While there are many advantages of adopting a cloud-based service, one of the downsides of using the cloud service providers is that their HSM services are generally opaque; you don't have a line of sight of your keys or awareness of who else might be exposed to them inadvertently. To offset this concern, some cloud service providers offer dedicated HSMs, which give customers greater control of their keys – but still not the level of control you achieve when deploying on-premises HSMs. The cloud service providers also support methods such as Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK), which offer a method to use your own HSMs with the cloud provider. For brevity, we won't cover these methods in detail in this guide.

The following infographic captures some of the considerations when deciding whether to adopton-premises or cloud.

ON-PREMISES **Physical HSM**	**vs.**	**CLOUD** **HSM as a Service**
• CAPEX investment • On-site team required for deployment and configuration • Remote administration for remote maintenance and software updates	**COST**	• No installation or CAPEX required for additional hardware • Support generally included, all-inclusive maintenance option may be available • Predictable costs over time
• Requires delivery, installation, and setup • Scaling up requires additional equipment and installation	**EASE**	• Scalable with unified management across HSM estate • Subscription-based service
• Physical hardware requires rack space, power, cooling, etc.	**SPACE**	• Zero rack space required for the same level of hardened security • Hosted in data centers globally
• Staff training • Recurring overhead of highly skilled resource for monitoring and maintenance	**RESOURCES**	• Typically maintained and managed by trained, security-screened personnel

Hybrid

Some organizations utilize the cloud to extend their HSM footprint beyond their on-premises deployments. It can provide organizations with the flexibility and scale to cope with business needs.

Bringing you the best of both worlds:

Seamlessly integrates on-premises and cloud HSMs to support a hybrid deployment model with the ability to port keys, which are important to ensure scalability and high availability.

With multi-cloud, single cloud, or hybrid model, you have a dedicated FIPS 140-3 Level 3 certified HSM giving you complete secure control of your keys and data.

Interoperate with multiple cloud service providers, moving keys to another CSP, or repatriate keys and data while maintaining full control.

Form Factor

Form factor refers to the shape, size, and configuration of an HSM, dictating how it integrates with your existing infrastructure. Selecting the right form factor is critical as it affects how the HSM is deployed, its compatibility with your existing infrastructure, and its suitability for the intended application.

There are three main HSM form factors to consider:

1. Peripheral Component Interconnect Express (PCIe)

Typically used to embed in a spare slot in a server motherboard, they generally are available in half-height and full-height configurations. Organizations often choose this form factor for applications that require dedicated, high-performance cryptographic services delivered locally – such as blockchain consensus nodes, certificate authorities, or high-volume transaction systems.

Because PCIe HSMs operate within the host server, they offer low-latency cryptographic operations and direct integration with on-premises applications, making them ideal when performance, security control, and proximity to the workload are priorities. They are often specified by the number of lanes, e.g., x1, x4, x8, which can be considered data pathways that allow communication between the CPU or chipset and PCIe device. As a general rule of thumb, the number of lanes is typically not a critical selection criterion.

2. Network-Attached Appliance – Typically, an Ethernet-connected 1U appliance that can be rack-mounted. In contrast to the dedicated service offered by PCIe HSMs, these can provide cryptographic services to applications distributed across the network to multiple application hosts or containers, providing a shared resource for securing many instances of an application.

3. USB Device – USB-connected HSMs also provide high assurance, key protection, and cryptographic services, but in a small form factor. They're perfect for desktop usage by a developer or for storing in a vault for infrequently used keys, such as CA root keys.

Performance and Speed

After choosing their preferred form factor, many first-time HSM buyers make the common mistake of selecting a model based solely on the highest transaction rates – assuming that faster is always better.

Before making that decision, it's important to pause and evaluate whether transaction speed is truly critical for your use case. Ask yourself: Do I really need high throughput? In many scenarios, a lower-performing HSM can meet your needs perfectly well, offering sufficient performance without unnecessary cost or complexity.

Let's consider use cases where high transactions are often needed:

- **Online transactions where high throughput is required** – E-commerce payment gateways, for example, where HSMs are used to encrypt and sign millions of payments per hour, ensuring fast and secure processing during peak times.
- **Remote signing solutions** – Cloud-based document signing solutions require HSMs with high transaction rates to swiftly sign documents uploaded by multiple users simultaneously, preventing delays in critical business workflows.
- **Key injection in a high**-volume manufacturing plant – Smart device manufacturing units use HSMs with high transaction rates to quickly inject unique keys into thousands of devices daily, ensuring efficient production line throughput.

Use cases when lower transaction rates are sufficient include:

- **Root Certificate Authority (Root CA)** – A Root CA uses an HSM with lower transaction rates. Typically, the HSM is used during the root key ceremony and then locked in a safe.
- **Code signing in a software development team** – An enterprise software development team uses an HSM with low transaction rates for code signing, as the volume of signing operations is limited to occasional patches or builds, prioritizing code integrity over speed.

Performance - Transactions Per Second

Transactions per second (TPS) or operations per second (OPS) relate to speed and performance. They tell you how many cryptographic operations, such as signing, encrypting, decrypting, and key generation, the HSM can perform in a second.

TPS varies significantly based on the type of cryptographic operation you perform. For example, key generation is typically slower than signing or encryption – generating a key involves thinking up a large random number, so it takes time. Look for benchmarks that specify algorithms (e.g., RSA, ECC, AES, and SHA), key size, and operation type (e.g., signing, encryption, decryption, key generation, and hashing). Most of these well-established algorithms are now table stakes.

Most reputable HSM vendors will support these as standard. That said, some of the so-called classical asymmetric algorithms that have been used extensively over the past decades are being deprecated in the not-too-distant future. You've probably already heard of post-quantum cryptography. More on this later in this guide. Alongside your specific use, here are a few general considerations when deciding what you need in terms of performance:

- Vendor performance metrics quoted are not always comparable and may be under ideal conditions. Consider your specific workload, server, chipset, OS, and typical transaction sizes. These can influence the performance of your overall solution.
- Make sure that the HSM supports all the types of cryptographic algorithms and keys your applications need (e.g., RSA, ECC, AES, HMAC, specific elliptic curves) and post-quantum algorithms (e.g., ML-DSA, ML-KEM, SLH-DSA, LMS), of course.

- Often, a trial or Proof of Concept approach will allow you to de-risk the selection of HSM and allow you to select the right HSM for the job. Some vendors offer HSM simulators as an initial evaluation tool. While they can seem useful for initial evaluation purposes, they clearly will not help with evaluating real-life environmental factors. Transaction rates, network latency, etc., will not be representative.
- Check whether the HSM leverages hardware acceleration for the algorithms your organization uses most frequently. This is where HSMs gain their performance advantage over software-based solutions.
- Be confident to adopt a flexible HSM architecture that's able to implement and properly accelerate new algorithms for future needs (e.g., PQC algorithms).

Underlying Framework/Architecture

When it comes to the underlying framework or architecture for configuring, deploying, and managing HSMs, vendors often have their own philosophy and distinct approach. Some popular vendors have adopted the “keys in the box” approach, preferring to store keys inside the physical memory space of the HSM. While the approach initially seems appealing and easy to grasp, it can present limitations regarding storage capacity and resilience.

By contrast, Security World, the Entrust nShield HSM architecture, provides a unified administrator and user experience and guarantees interoperability, whether the customer deploys one or hundreds of devices. Using Security World, the cryptographic keys are abstracted and securely stored as key tokens outside the physical boundary of the HSM device.

A key token is a securely encrypted key that cannot be used without access to the matched HSM and de-tokenization key. This removes the risk associated with a single point of failure and ensures you don’t run out of physical storage space for your keys.

As an HSM buyer, ultimately, you need to do your research and find out which framework or architecture works best with your requirements.

Performance – In-Field Upgrades

It can be difficult when first buying HSMs to know if you have purchased a model that will perform well in your deployment scenario. Some vendors, including Entrust, offer performance upgrades that can be enabled in the field via a licensing certificate. This means you can deploy a lower-performance HSM in the first instance and then upgrade the performance at a later date without time-consuming and costly hardware replacements.

High Availability/Redundancy and Backups

If you plan for unscheduled downtime, service disruption, and data breaches before they happen, you can mitigate risks and build resilience into your security systems. HSMs are usually deployed in pairs for high availability.

Keeping your crypto operations running: failovers, load balancing, and more

- Check what happens if one HSM breaks down. Understand the impact on your operations and how easy it would be to replace the HSM without loss of service, etc.
- Ensure the HSM provides automatic failover mechanisms.
- Evaluate whether the device includes or integrates well with load-balancing mechanisms to distribute cryptographic operations evenly across all active HSMs. This maximizes throughput and prevents single points of contention.
- Verify if the HSM system enables load balancing across multiple HSMs for scalability in enterprise or cloud environments.
- Look for HSMs that can efficiently handle multiple concurrent connections or threads. This is critical for applications with high concurrency demands.

Back up, restore, and recover

- Evaluate how backup and restore processes are carried out.
  - How much effort is it for the organization to implement these processes?
  - Is additional hardware or cost required to perform backups?
  - Can backup be automated without service downtime and be part of the existing organization procedures?
- Some HSMs allow backup to encrypted files stored on network drives or cloud storage. Ensure these backups are strongly encrypted and the encryption keys are managed securely.
- For disaster recovery, check if the HSM supports clustering across geographically dispersed data centers. This protects against regional outages. Data synchronization between geographically separate HSMs is a critical aspect here.

Monitoring, maintenance, and responsibility models

Big problems usually start as small problems: warning notifications, missed updates, approaching capacity limits, and declining performance. Make sure you know how to monitor and manage HSMs and crypto operations, and who's responsible for the day-to-day operations and disaster recoveries.

- Check if the HSM provides robust monitoring of its health, status, and performance, including logging of high-value key usage.
- How are software and firmware updates handled in a high availability (HA) environment? Can they be applied without interrupting service or requiring downtime for the entire cluster? Check for this, as it is crucial for maintaining security, operation, and availability, and addressing vulnerabilities.
- For cloud-managed HSMs, understanding the shared responsibility model is critical. While the cloud provider manages the underlying infrastructure and HSM redundancy, you are responsible for key lifecycle management, access controls, and often the actual triggering of Disaster Recovery (DR) procedures.

APIs

Application Programming Interfaces are crucial for HSMs as they dictate how effectively other applications can communicate with the HSM to leverage its capabilities. Ensure the HSM supports the APIs you will be using.

The main APIs used in conjunction with HSMs are:

- **PKCS#11**, often referred to as P#11, is a widely adopted industry standard API for cryptographic operations. Hence, prioritize HSMs that support such standards. This ensures broad interoperability across platforms and applications.
- **Microsoft CAPI/CNG** for Windows-based ecosystems.
- **Java JCA/JCE** (for Java applications).
- **OpenSSL** for open-source environments.
- **RESTful/Web services** for modern, cloud-based, or microservices architectures, which can simplify the integration of an HSM with your web-based infrastructure.
- **Key Management Interoperability Protocol (KMIP)**. HSMs are often used as the root of trust for KMIP servers, making HSMs and their key management capabilities available through the KMIP API.

Additionally, some vendors offer their own native API. For example, Entrust nShield HSMs offer the nCore native API for providing access to advanced HSM features for specialized use cases.

Operating System Support

When selecting an HSM, ensure it is compatible with your preferred operating system. Network-attached HSMs typically require software to be installed on client machines. Hence, you need your HSM to be compatible with the server OS. Similarly, when you deploy a PCIe or USB form factor HSM, it needs to be compatible with the server hosting the HSM.

Software Development Kit (SDK)

Some HSM vendors offer an SDK feature to allow developers to create custom cryptographic applications that interact directly with the HSM. Entrust provides this through its nCore SDK, which gives customers access to low-level APIs and tools for developing applications that perform specialized cryptographic operations beyond standard interfaces such as PKCS#11, JCE, or Microsoft CNG.

This level of extensibility allows organizations to tailor cryptographic functionality to unique operational or regulatory needs – for example, integrating proprietary algorithms, automating certificate management, or embedding security controls directly into business applications.

Secure Execution Environments

Some HSMs also support what's known as secure execution or confidential computing, which allows sensitive business logic or application code to run within the tamper-resistant boundary of the HSM, alongside the associated key material. Entrust's CodeSafe technology enables this capability, protecting not just cryptographic keys but also the code that uses them.

Applications running inside this secure environment can encrypt, decrypt, and process data entirely within the HSM, benefiting from hardware-enforced policies and protection against external compromise. This model – sometimes referred to as "black box computing" – is ideal for highly sensitive workloads such as transaction validation, signing operations, or identity verification systems.

Scalability

Prepare for the expected and unexpected. HSMs are often referred to as "general purpose", indicating that they are intended for many use cases across industries: PKI, code signing, key and secrets management, tokenization, database encryption, etc.

The Entrust Approach: CodeSafe SDK

CodeSafe, the nShield HSM SDK, has been a pioneering part of our product line for two decades. With CodeSafe, running custom code within the HSM doesn't impact the FIPS certification of the HSM.

Some HSM vendors require modification to their base HSM firmware, thereby branching off a certified firmware to something custom and outside of the certification process.

Learn More

Use Cases: Now and Later

When choosing an HSM and an HSM vendor, consider what use cases you need them for, and what use cases you might need them for later.

- Ask if the HSM supports the expected growth in workloads. Check the specifications for key generation, signing, and encryption speeds.
- Evaluate the number of keys the HSM can store. A scalable HSM should be able to support thousands to millions of keys, depending on the application.
- Check whether key storage can be expanded through upgrades in software or additional hardware modules.
- Select an HSM with a modular architecture that allows increasing capacity without having to replace the complete system.
- Check if the HSM supports seamless integration with additional units for redundancy or increased performance.

Multi-Tenancy and Partitioning: Increasing HSM Utility Without Sacrificing Security

Make sure that the HSM supports multiple secure partitions/domains to handle different applications/tenants. This is useful for scalability in multi-application environments.

Entrust HSMs deliver robust key isolation within these secure partitions, enabling organizations to host diverse workloads with confidence. Full multi-tenancy capabilities will allow securely segregated tenants to share HSM resources under centralized governance.

When evaluating vendors, be sure to prioritize HSMs that:

- Integrate easily with existing and future systems across on-premises, cloud, and hybrid environments.
- Offer cloud-native deployment options that scale with infrastructure and provide proven disaster-recovery (DR) capabilities through trusted service providers.
- Support centralized management with decentralized partition ownership, allowing IT administrators to manage policies and configuration, while individual teams maintain control of their own cryptographic partitions.
- Allow in-field software, firmware, and hardware logic upgrades with Field Programmable Gate Array (FPGA) technology that enables new cryptographic logic to be soft-loaded, ensuring crypto-agility without impacting neighboring tenants or system availability.
- Scale efficiently in both performance and cost as usage and applications expand.

Check out some of Entrust nShield HSM's technological capabilities.

Key Considerations When Selecting a Hardware Security Module

2. Future Readiness

Post-quantum cryptography

Cryptography is at a critical point in time. There are more data security risks than ever, and more data security regulations than ever, attempting to prevent and mitigate the damage from data security risks. And that's with cryptographic processes built on fundamental principles defined decades ago. The advent of quantum computers, which will be able to crack current encryption algorithms in the coming decade, changes everything.

The solution is post-quantum cryptography. And HSMs are proving to be key enablers for PQC by providing a secure, tamper-resistant environment for generating, storing, and managing larger and more complex keys and operations inherent in PQC algorithms. They facilitate crypto-agility, allowing organizations to simultaneously support both current and quantum-resistant cryptographic algorithms (hybrid mode) during the transition, and offer hardware acceleration to mitigate the increased computational demands of PQC.

The National Institute of Standards and Technology (NIST) recently approved new quantum-resistant algorithms that are being implemented, but not all HSMs offer the same implementations. Further, future threats require cryptographic agility (or crypto-agility), the ability to adapt to new threats and switch between cryptographic algorithms, and make updates without disrupting systems.

A few benefits of cryptographic agility include:

- **Future-proofing security:** Crypto-agility allows organizations to adapt to new cryptographic algorithms and standards, ensuring long-term protection against emerging threats, including those posed by quantum computers.
- **Improved resilience:** Organizations can swiftly replace compromised or outdated algorithms with new ones without disrupting critical systems, thus maintaining a continuous security posture.
- **Compliance and regulatory adherence:** Cryptographic agility helps organizations meet evolving compliance requirements and industry regulations that may require adopting new and stronger cryptographic methods.
- **Reduced risk of data breaches:** By enabling the rapid deployment of quantum-resistant algorithms, crypto-agility minimizes the window of vulnerability to attacks that could potentially compromise currently encrypted data.

Crypto-agility finds applications across industries and sectors. Here are a few use cases:

- **Financial services:** Rapidly switching to new algorithms for payment processing to comply with emerging regulations or counteract newly discovered vulnerabilities.
- **Government/defense:** Ensuring long-term security of classified data by being able to update encryption methods as quantum computing advances.
- **Healthcare:** Protecting sensitive patient data with the flexibility to adapt to new cryptographic standards mandated by healthcare regulations.
- **Internet of Things (IoT):** Enabling secure communication for a vast array of devices by allowing firmware updates to incorporate new cryptographic primitives as needed.

Field programmable gate arrays are types of integrated circuits that can be reprogrammed to adapt to new needs and use cases, as opposed to integrated circuits and chips that are built for specific processes. In an HSM, that means a limit to what cryptographic algorithms and processes the device can provide.

If you want true future-readiness in an HSM, you want to ensure it uses field programmable gate arrays so it can be reprogrammed for new algorithms and threats.

Choosing an HSM from the perspective of future readiness requires analyzing features that ensure long-term scalability, security, and adaptability to evolving threats, technologies, and regulations. Here are a few factors to consider:

- Check whether the HSM supports or has a roadmap for PQC algorithms, such as lattice-based cryptography and NIST PQC standards.
- See if the software and firmware need to be updated to incorporate new quantum-resistant algorithms without hardware replacement.
- Make sure the HSM meets the latest standards, such as FIPS 140-3 or Common Criteria EAL4+. The HSM should also support compliance with established regulations like eIDAS and PCI DSS. Further, the HSM should support emerging protocols like TLS 1.3 or emerging standards for blockchain and IoT.
- Check if the HSM can scale to support high TPS rates, such as 15,000 TPS or more, for enterprise use.
- Look for HSM-as-a-Service options so that you can scale cost-effectively and without having to manage physical hardware.
- See if the HSM is compatible with modern applications, such as IoT, blockchain, and cryptocurrency wallets.

Post-Quantum Algorithms

Algorithm Name	Algorithm Initials	Description	NIST Published Standard
Module-Lattice-Based Key-Encapsulation Mechanism (formerly CRYSTALS-Kyber)	ML-KEM	A key-encapsulation mechanism (KEM) based on structured lattices. It is designated as the primary standard for general encryption due to its efficiency and relatively small key sizes.	FIPS 203
Module-Lattice-Based Digital Signature Algorithm (formerly CRYSTALS-Dilithium)	ML-DSA	ML-DSA can be used to generate and verify digital signatures.	FIPS 204
Stateless Hash-Based Digital Signature Algorithm (formerly SPHINCS+)	SLH-DSA	A stateless hash-based digital signature algorithm.	FIPS 205
FFT (Fast-Fourier Transform) Over NTRU-Lattice-Based Digital Signature Algorithm (formerly FALCON)	FN-DSA	A digital signature algorithm that's also based on lattices. Recommended for applications requiring smaller signatures than ML-DSA.	
Hamming Quasi-Cyclic	HQC	A code-based KEM that was selected in March 2025 to serve as a secondary encryption standard. It offers a cryptographic backup to the lattice-based ML-KEM, providing diversification in case a weakness is found in lattice-based methods.	HQC NIST Presentation
Leighton-Micali Signature system	LMS	A stateful hash-based signature scheme that is secure from quantum computers, but only suitable for applications where the use of the private key can be carefully controlled.	NIST SP 800-208

Key Considerations When Selecting a Hardware Security Module

3. Integrations and Technology Partners

The value of an HSM comes to the fore when it is integrated with third-party applications. The illustration on the next page shows some of the typical use cases where the services of an HSM are required.

When looking for an HSM from the perspective of integrations and technology partners, a few points, such as the device's fit with your organization's tech stack, proven and documented integrations, and cloud service provider (CSP) support, should be kept in mind. Here are a few more factors to consider:

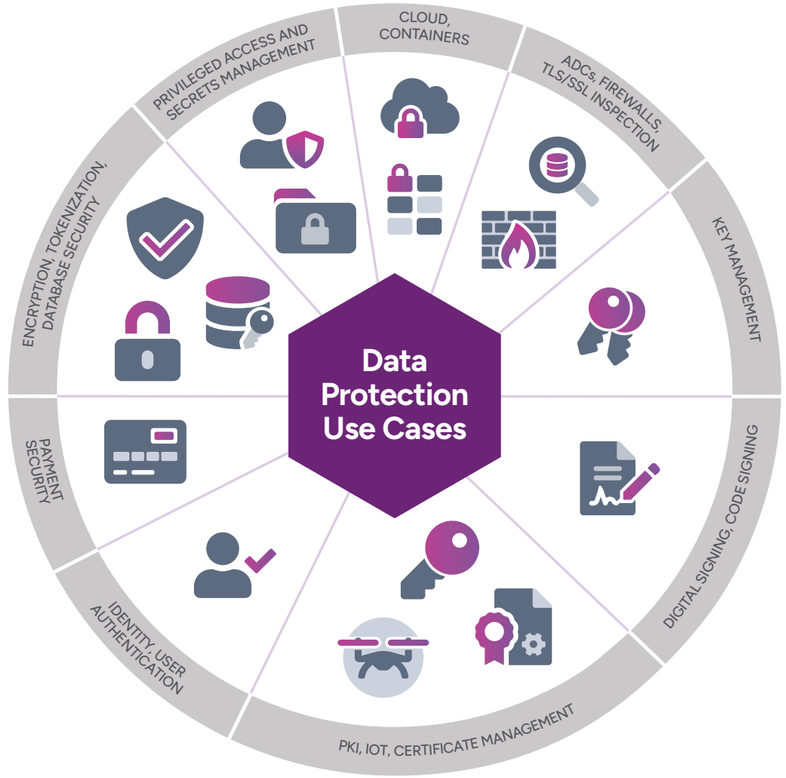
- Check if there are any vendor-specific SDKs or APIs for custom integrations.
- Check the device's support for cloud-based or hybrid deployments and whether it's compatible with prominent cloud providers using BYOK or HYOK.
- Look for integrations with DevOps tools or SIEM solutions for monitoring and automation.
- See if you can test integration with specific platforms or applications during the evaluation phase.

What do HSM vendors offer?

Check whether the HSM vendor has partnerships with major technology companies. These could be major cloud providers like Amazon Web Services (AWS), payment processing companies, and enterprise security firms. Further, see if the vendor has partnered with PKI providers for certificate management.

See if the vendor offers sandboxes, free trials, and proof-of-concept environments.

Research the vendor's track record, reputation, and experience in the HSM market. A reputed and reliable vendor minimizes the risk of unsupported hardware or delayed fixes, which could potentially lead to downtime costs and security challenges.



Learn more about Entrust's nShield HSM integrations and technology partners.

Key Considerations When Selecting a Hardware Security Module

4. Certifications and Compliance

When selecting an HSM, it is essential to check if it has the required certifications to ensure it meets the compliance, security, and performance standards for your specific use case. The two primary certifications directly related to HSMs are NIST Federal Information Processing Standard (FIPS)140-3 and Common Criteria.

FIPS 140 relates specifically to HSMs. The standard was revised in recent years, so you may still see HSMs being offered that are FIPS 140-2 certified. These are currently still valid but will be sunsetted in the coming years.

Organizations use the FIPS 140-3 standard to ensure that the hardware they select meets specific security requirements. The FIPS certification standard defines four increasing, qualitative levels of security:

- **Level 1:** Requires production-grade equipment and externally tested algorithms.
- **Level 2:** Adds requirements for physical tamper-evidence and role-based authentication.
- **Level 3:** Adds requirements for physical tamper-resistance and identity-based authentication. There must also be physical or logical separation between the interfaces by which “critical security parameters” enter and leave the module. Private keys can only enter or leave in an encrypted form. Level 3 also requires the module to detect and react to out-of-range voltage or temperature (environmental failure protection, or EFP) or alternatively undergo environmental failure testing (EFT).
- **Level 4:** This level makes the physical security requirements more stringent, requiring the ability to be tamper-active, erasing the contents of the device if it detects various forms of environmental attack. EFP and protection against fault injection are required, as well as multi-factor authentication.

For most use cases, HSMs certified to FIPS 140-3 Level 3 are more than sufficient. Common Criteria certification is typically used to certify EAL4+ augmented with AVA_VA.5 and ALC_FLR.2 (compliant to Protection Profile EN 419 221-5 Cryptographic Module for Trust Services).

HSM compliance: Trust, security, and legal peace of mind

For financial applications or payment processing, confirm whether the HSM complies with Payment Card Industry Hardware Security Module (PCI HSM) standards.

Look for compliance with ISO/IEC 19790. This is the international standard for cryptographic modules, aligning closely with FIPS 140-3.

Key Considerations When Selecting a Hardware Security Module

5. Cost or Value

When looking for an HSM, you are balancing financial investment against the costs of several risks, such as security breaches and non-compliance. Consider the following factors to ensure the HSM provides optimal value for your investment while minimizing risks.

Total cost of ownership

Compare the total cost of ownership (TCO) to the cost of alternative solutions or the cost of a breach. The TCO goes beyond the initial purchase price. It involves direct and indirect costs of purchasing, deploying, operating, maintaining, and finally, retiring the HSM. Understanding the TCO of an HSM is critical for making informed decisions and ensuring the investment meets the organization's long-term security and financial goals.

The TCO of an HSM typically includes:

- **Acquisition costs:** These usually involve the initial purchase price, software licenses, hardware accessories, shipping and delivery, installation and setup, and initial training
- **Operation costs:** They typically involve power consumption, cooling, network infrastructure, staffing, monitoring and logging, and auditing and compliance.
- **Maintenance and support costs:** These costs typically include hardware maintenance agreements, software maintenance and updates, firmware upgrades, and emergency support.
- **Hidden and indirect costs:** Besides these known costs, certain other costs impact the TCO. They include cost due to downtime, integration challenges, scaling costs, cost of training employees, and disposal/decommissioning costs.

Cost now or cost later

- Identify the specific risks your organization faces, such as key compromise, data breaches, downtime, and regulatory fines. Evaluate the likelihood and impact of these risks without an HSM. Compare the cost of the HSM to the potential reputational and financial losses from a security incident.
- Ensure the HSM supports flexibility and scalability. A scalable HSM avoids the risk of expensive upgrades or replacements as your business or organization grows.
- Analyze the HSM's performance metrics against your application requirements. A high-performance HSM reduces delays or downtime, which can be costly in critical applications. Compare this to the HSM's costs.
- Ensure the HSM has robust security features. These reduce the risk of key compromises or physical attacks, which could lead to massive costs.
- Make sure that the HSM integrates seamlessly with your existing systems. An HSM that integrates well saves implementation costs and minimizes the risks of errors.
- Check if the HSM's features and certifications align with your cyber insurance needs, which may reduce premiums and improve coverage. An HSM that lowers insurance premiums or minimizes liabilities in case of a breach adds significant value compared to its cost.

Here are a few key statistics on the costs of non-compliance and data breaches.

$4.4M

The global average cost of a data breach in 2025: a 9% decrease since 2024's highest total ever.

€14.8M

The average cost for organizations that experience non-compliance problems, a 45% increase from 2011.

Key Considerations When Selecting a Hardware Security Module

6. Vendor's Broader Portfolio

Simplifying your IT and data security stack can mitigate risks, streamline management, and eliminate the juggling of multiple vendors and the headaches of dealing with procurement, vendor reviews, and trying to integrate across vendors and technology.

HSMs are foundational to securing other technologies: code signing, PKI, database encryption, key and secrets management, and so much more. Look for vendors that can solve more of your needs than just HSMs. That eliminates the complexity of integrations and streamlines the procurement process. But be aware of becoming captive to your vendors.

Some technology vendors will try to require you to bundle solutions you don't want with those you do want. Sure, it might make integration easier, but it limits your options in the future and requires you to settle for bundled solutions you don't want and might not even use.

The ideal is to find a vendor that can provide many solutions that integrate seamlessly with other technologies, regardless of vendor, and don't prevent you from building your ideal stack across technology providers.

Don’t let your technology vendors limit your possibilities.

When choosing an HSM, it is also essential to look at the vendor’s broader portfolio, such as add-ons and option packs, essential pairings, and key use case offerings. The following are a few factors to consider:

Diversity of HSMs and form factors

- Look for the availability of form factors like network-attached, PCIe cards, USB devices, or portable HSMs.
- Check for support on-premises, cloud, and hybrid environments to match your deployment needs.
- Evaluate if the vendor offers scalability from small-scale to enterprise-grade solutions for high-throughput environments.

HSM add-ons, option packs, and support services

- Check the availability of firmware upgrades or software option packs for specialized tasks.
- See if the HSM vendor supports additional cryptographic algorithms or protocols through add-ons.
- Check the licensing models for add-ons and their impact on the total cost of ownership.
- Evaluate the compatibility of add-ons with existing HSMs to avoid hardware upgrades.
- Does the vendor offer professional services capabilities and global “follow the sun” support? You’ll want to know services are available – for installation, optimization, deployment, and custom development – before you need them.

Essential pairings

- Look for integrations with key management solutions for centralized key lifecycle management across HSMs and cloud environments.
- See if the vendor supports relevant tools to manage HSMs in cloud platforms with features like automated key rotation or policy enforcement.
- Verify whether the vendor offers compatibility with enterprise-grade tools for monitoring, auditing, and compliance.

Use case offerings

- See whether the vendor provides key use case offerings, such as digital signing, PKI, and identity management.
- Check the vendor’s support for secure code signing, document signing, or transaction signing with high-performance key generation and storage.
- Look for robust certificate authority (CA) integration, root key protection, and scalability for issuing and managing digital certificates.
- Check the vendor’s support for identity-based encryption, authentication, and integration with identity platforms.

Ease of management and automation

- See if the vendor offers centralized management consoles for HSMs, add-ons, and pairings.
- Check if the vendor provides automation tools for key lifecycle management, certificate issuance, or digital signature workflows.

Choosing the right HSM is a critical decision that underpins your organization's security posture in an evolving threat landscape. By prioritizing future readiness, robust integration, and clear value, you can ensure a resilient cryptographic foundation.

Entrust nShield HSMs are available in a range of FIPS 140-2 & 140-3 certified form factors and support a wide variety of deployment scenarios – on-prem, cloud-based, or hybrid.

Learn more at Entrust.com

ENTRUST
SECURING A WORLD IN MOTION

ABOUT ENTRUST CORPORATION

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everydaytransactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION