

Modern Hardware Security Modules **Address Complexity**

An IDC Technology Spotlight Sponsored by Crypto4A
By: **Robyn Westervelt**, Research Director, Security & Trust

July 2020

Hardware Security Modules are Being Transformed

Emerging cloud adoption requirements, the growing use of mobile devices for authenticating payments and emerging internet of things (IoT) use cases are fueling adoption of hardware security modules (HSMs). These hardened devices are designed to securely store and manage digital keys and perform encryption processing. But they are also often a source of frustration because they are viewed as highly complex devices that require highly skilled personnel to manage.

As more enterprises accelerate digital transformation across hybrid and multi-cloud environments, HSMs are increasingly becoming a wholistic platform supporting a variety of emerging use cases where encryption and public key infrastructure operations are required to protect sensitive information.

FLEXIBLE, SCALABLE AND SUSTAINABLE

- The next generation of HSMs are being transformed into comprehensive platforms flexible enough to support a wide variety of innovative use cases.
- HSMs are emerging to support containerization and may contain powerful application servers with an emphasis on ease-of-use and administration.
- To reduce complexity, HSM manufacturers are adding automation, ensuring integration and interoperability with existing infrastructure and future-proofing for emerging crypto requirements and business use cases.



The Next Generation of HSMs

The use cases for HSMs are diverse and constantly evolving to support new business initiatives. This hardware is used to establish a root of trust to authenticate users and devices to IT infrastructure and services. HSMs contain the certificates and keys required to **support the signing of critical contracts**, to **validate the integrity and authenticity of software code and updates**, to **provide key injection to establish device identity** and to **support emerging cryptocurrency and other blockchain schemas**.



The next generation of HSMs are being transformed into comprehensive platforms flexible enough to support a wide variety of innovative use cases. Market-leading platforms are no longer being constrained by cryptography. Buyers should evaluate platforms for long-term efficacy in the face of emerging crypto algorithms and quantum-safe

encryption. This adaptability enables the HSM to conform to evolving business strategies rather than constricting them. Buyers may no longer have to acquire dedicated hardware for payment processes. Modern HSMs are likely to support both general-purpose and payment functionality. Modern HSMs can support containerization and may contain powerful

application servers with an emphasis on ease-of-use and administration. They can support virtual infrastructure and containerized workloads, and enable HSM manufacturers to support customization and securely provide enhancements and optional functionality and services.

Business Continuity for a Physically Distanced World

The global COVID-19 pandemic has made it difficult for crypto services teams to operate offline root certificate authorities (CAs), because today's solutions require a physical presence. Furthermore, processes required for business continuity with traditional HSMs typically use split keys distributed to important users that act as guardians for these precious assets. The techniques used for these functions are vendor specific and result in vendor lock-in solutions. Automation is a much-needed requirement here. The HSM should be able to provide the functionality of operating offline root CAs and maintaining business continuity using secure messaging over email and end-user computer-based and mobile applications. This would eliminate the need for physical presence, vendor-specific tools and the requirement of key ceremonies.

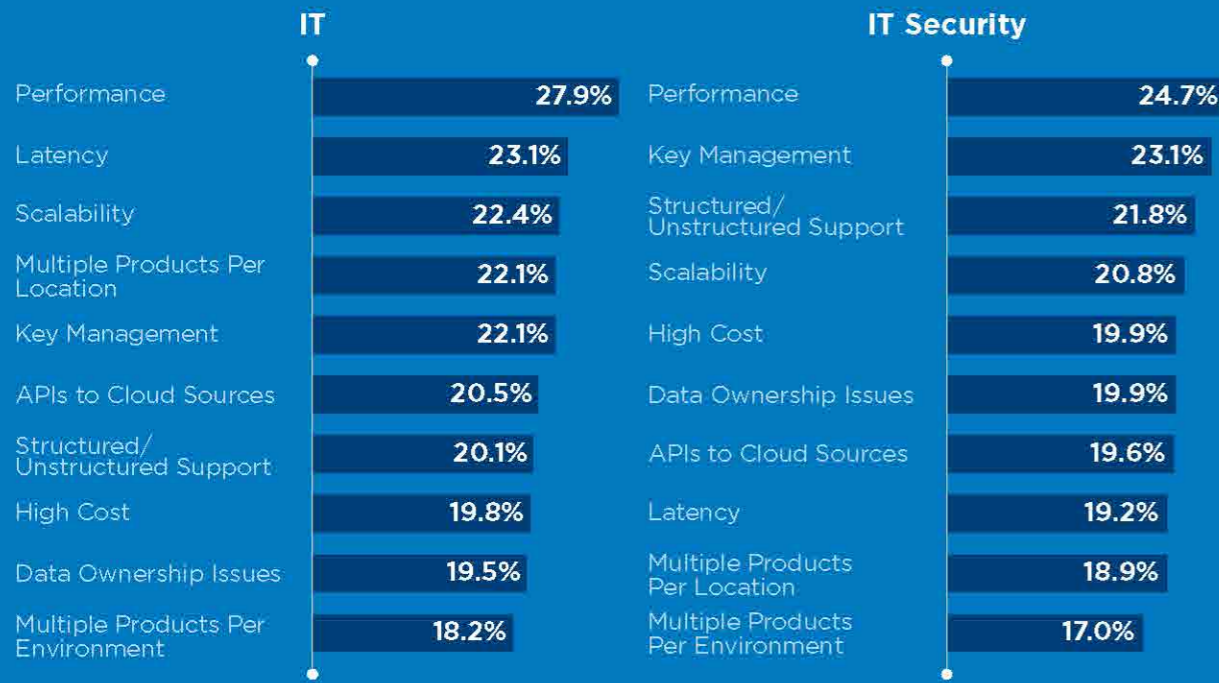
Growing Enterprise Complexity Requires HSM Manufacturers to Innovate

Organizations of all sizes are collecting massive amounts of data about their customer base, and the use of data scientists and the computing power of cloud resources to support big data and analytics projects have prompted IT security professionals to address rapidly growing security and privacy concerns. The computing-intensive processes associated with encryption and the scalability necessary to track millions of internet of things devices flooding the market require organizations to maintain HSMs to meet compliance obligations and manage encryption keys.

TOP ENCRYPTION CHALLENGES

IT and IT Security teams differ on the challenges of implementing and managing encryption. IT teams are generally concerned about application performance, scalability and network latency. Security teams face the challenge of managing multiple key management solutions protecting structured and unstructured data.

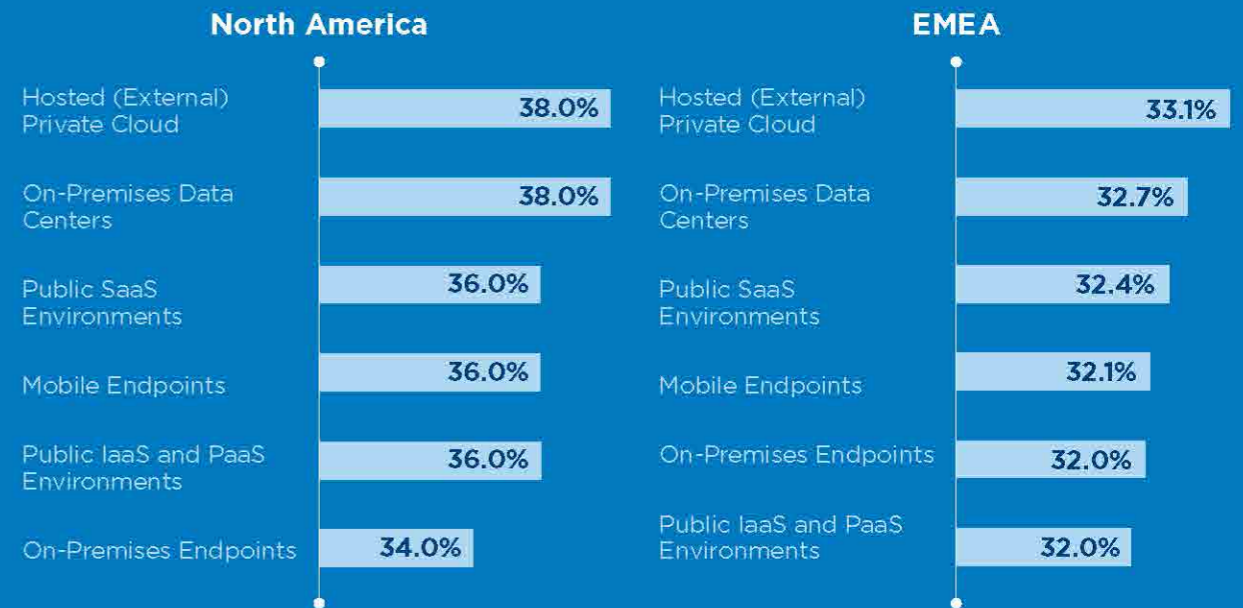
Q. What are your current "data encryption" challenges?



ENCRYPTION AT REST BY REGION

The percentage of total data encrypted at rest is higher in North America than EMEA, according to survey respondent estimates. A greater amount of encrypted data at rest resides in private clouds and on-premises data centers, followed by public SaaS environments, the survey found.

Q. On a scale of 1-5 where 1 is not sensitive at all and 5 is extremely sensitive, please rate how sensitive the DATA is to your organization that exists in each of these IT environments; Please estimate the percentage (%) of the TOTAL DATA in each of the environments below that is encrypted (at rest).



Source: Data Security Survey, IDC, January, 2020

A Critical Element of the Payment Industry

HSMs play a significant role in supporting the integrity and confidentiality of sensitive digital transactions. Enterprises rely on these devices for authentication, database encryption and document and software code signing. But HSMs were designed at a time when they were military assets. These were not meant to be used easily or deployed easily. They were meant to be cared for by very few elite IT staff.

These physical devices provide a highly secure environment to store and manage the digital keys used for strong authentication and the processing power for scalable and reliable encryption. HSMs are designed to prevent the theft or manipulation of sensitive data by storing cryptographic keys and digital certificates. This hardware is a critical element of the payment industry as it provides authorization for card-processing systems. HSMs have long been used to support database and application encryption to manage public key encryption and in establishing an encrypted communications channel for websites and web-based services and their users.



HSM Users Demand Flexibility for Growing Use Cases

HSM vendors are adding managed services and addressing longstanding complexities associated with key management, trust ceremonies, Public Key Infrastructure and certificate management. Disruptive players are on the horizon to inject the necessary modernization into these highly required components to support root of trust and encryption for a variety of unique use cases well into the future. HSM manufacturers must reduce complexity and potentially bridge the divide between payment and general-purpose HSMs.

IDC's 2020 Data Security Survey found buyers increasingly frustrated over the growing complexity of their security infrastructure. The survey, which reached 620 IT and IT security respondents across North America and EMEA, found that 45% use a single vendor or a vendor suite of products for their hardware security modules. Meanwhile, 17.4% of survey respondents indicated they require customized HSM software and 22.6% indicated adoption of an HSM as-a-service. Nearly 12% of survey respondents use multiple HSM vendors.

HSM Vendors of Choice by Employee Size					HSM Vendors of Choice by Employee Size	
	Total	Employee Size			Role	
		500 to 999 employees	1,000 to 4,999 employees	5,000 or greater employees	IT	IT Security
None	3.2	2.9	2.9	3.8	3.2	3.2
Custom	17.4	11.5	18.5	18.8	16.6	18.3
Single Vendor	23.9	24	26	20.7	19.2	28.5
Vendor Suite	21.1	25	22.4	17.3	22.1	20.2
SaaS	22.6	26	19.5	25.5	25	20.2
Multiple Vendors	11.8	10.6	10.7	13.9	14	9.6
Total	620	104	308	208	308	312

D1. Please describe the techniques and/or solutions your organization uses to address each of the following functions commonly associated with "data loss protection (DLP)" and data security.

Source: Data Security Survey, IDC, January, 2020

General-Purpose HSMs vs Payment HSMs

General-purpose HSMs are being used because, unlike payment HSMs, they may be integrated with existing software and applications, typically with a Transport Layer Security (TLS) tunnel where the keys are kept in the hardware. The payment industry is using a mixture of general-purpose and payment HSMs. Banks and mobile payments providers such as Apple Pay have made HSM buyers particularly attracted to general-purpose HSMs to support the increased use of tokenization for digitalized payments. In addition, financial services firms are seeking better ways to secure mobile and person-to-person payments.

HSM manufacturers have long added functionality supporting multiple partitions and today's HSMs also now support multitenancy. Product development teams are refining the next generation of HSMs to function in the DevOps world to appeal to modern, security-minded application development teams in the support of DevSecOps initiatives and PKI, code-signing and DNSSEC operations. This will require support for remote access and increased processing power to support application server functions and software-defined technologies such as containerization.

Key Differentiators of HSM Providers

The general-purpose HSM market is projected to grow rapidly, driven by increased requirements across a variety of industry verticals to support IOT devices and other interconnected systems requiring key injection and support for critical root of trust operations. Payment HSMs will continue to grow based on the need for a secure root of trust environment for performing payment-specific cryptographic operations. Demand is in-line with the growth of digital transactions and the need to maintain compliance with the Payment Card Industry Data Security Standards. These two HSM market segments may be converging as banks, large retailers and mobile payments companies demand hardware that meets their compliance obligations for payment card processing and PIN verification while being flexible enough to support new business initiatives requiring authentication, encryption and key management.

Buyers of HSMs should identify providers that differentiate in the following areas:

Future Proof: Modern HSMs should support crypto agility. They must be easier to implement and manage and be flexible enough to support new technologies, encryption algorithms and key management processes. There is a move by emerging providers to converge certificate management and cryptographic key material in one place. A modern HSM must also support updates and new features and optional add-ons. An HSM that can function in the DevOps world could ease security and compliance challenges. But developers require a solution that is less complex to manage code signing, PKI, DNSSEC and any application that requires the use of an HSM.

Adaptable: Many HSMs have not been designed to truly function in the DevOps world. This has led buyers to adopt secret vaulting solutions. DevSecOps buyers seek a flexible, scalable solution. Safe enough to deploy on the factory floor without a bunker or a secure room. Supporting multiple servers and containerization on the box. The complexity to install an HSM requires trained people. Even with network-attached HSMs, the majority live in air-gapped rooms, behind safes and vaults, and are physically disconnected.

Sustainable: While cost and interoperability with existing key management and encryption solutions rank highly in market surveys, users of hardware security modules interviewed by IDC consistently say that speed of delivery and the availability and knowledge of support personnel keep them loyal customers of a specific HSM manufacturer. Buyers should identify HSM providers that have support personnel who could speak the technical language of encryption and key management specialists and help diagnose problems as quickly as possible. In addition, vendors should provide on-time delivery and make key personnel available to troubleshoot issues.

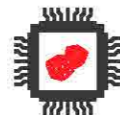
HSM Buyer Trends

HSM buyers want the ability to integrate high-quality solutions that require HSM security to gain operational efficiencies and agility while balancing that with cost. The current perception is that you must have multiple HSMs in a hardened, isolated environment. Key ceremonies and other old constructs are creaky and don't allow DevOps and DevSecOps teams to move rapidly.

DC's 2020 Data Security survey found that buyers of HSMs seek devices from HSM manufacturers with proven quality and reliability. Vendor reputation was a significant driver of new HSM investments. Organizations also seek HSMs that support firmware customization. In addition, buyers continue to want strong tamper detection and auditing capabilities with support for multi-factor authentication. Multiple HSMs and software stacks have long supported the following use cases and approaches:



Code Signing



Entropy Generation



Public Key Infrastructure



Unified Key Management



Elastic Hybrid HSM



Secrets Vault

The projected increase in general-purpose HSMs coincides with growth of application security and IoT data-related projects, advanced analytics and secure data processing at the edge.

Privacy and Trust

Privacy and trust is expected to be a growth driver in the next five years, shifting focus to data discovery, classification and persistent file encryption solutions. HSMs could play a role with database and application connectivity.

Banks and financial services firms continue to require a root of trust with blockchain initiatives for both back-office settlement systems and emerging services. A root of trust will still be required to support emerging use cases in advanced analytics where homomorphic encryption may be applied. HSMs are becoming even more relevant as enterprises invest in promising new technologies designed to ensure data integrity and security. HSMs are increasingly providing an additional layer of protection over distributed ledger applications and cryptocurrency wallets.



HSM Manufacturer Crypto4A

Crypto4A is an emerging HSM manufacturer with management and engineering teams that are deeply rooted in the HSM market. The company has entered the HSM market with an enterprise-grade, FIPS 140-2 Level 3 device containing a comprehensive set of capabilities. The company sought to offer more from a single appliance while reducing complexity and improving ease of use. The QxEDGE™ HSM-as-a-Platform addresses the level of integration required by software development teams, security and operations teams to manage the security of their applications.

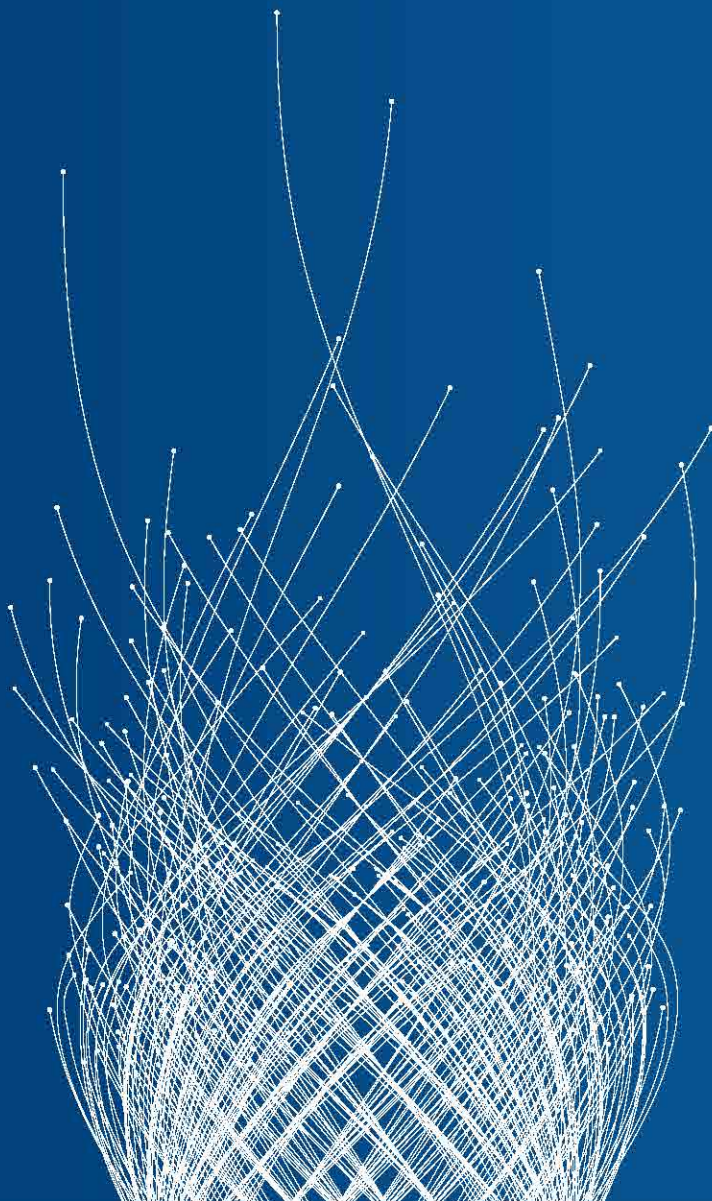
The QxEDGE™ HSM-as-a-Platform can be securely updated using quantum-safe algorithms. Crypto4A addressed crypto agility, leveraging quantum-safe hash-based signature (HBS) algorithms and key encapsulation mechanisms (KEMs) to ensure quantum-safe platform updates and communications for secure auto scaling, High Availability (HA) and Disaster Recovery (DR).



Challenges

Crypto4A is an emerging vendor that must address rapid growth and continued product innovation with limited resources. The company is competing in a mature market with well-established vendors. Like its competitors, Crypto4A must innovate in the face of a global pandemic and uncertain economic conditions. Buyers should assess their risk tolerance and adoption strategy for taking on startup technology. Crypto4A is gaining market traction and its small size makes it agile enough to address technology adoption changes and new adoption requirements.

The HSM Market is Poised for Disruption



IDC believes the HSM market is projected to have strong growth through 2024 as organizations deal with rapid data creation and the need for protecting privacy and security of sensitive data. The HSM market currently consists of payment and general-purpose HSMs, but the market is poised for disruption. The next generation of HSMs are becoming increasingly flexible enough to support a wide variety of innovative use cases. Modern HSMs are likely to support both general-purpose and payment functionality. Modern HSMs can support containerization and may contain powerful application servers with an emphasis on ease-of-use and administration. They can support virtual infrastructure and containerized workloads and are capable of supporting customization to securely provide enhancements and optional functionality and services.

Payment HSMs which are certified with the FIPS standards and the PCI HSM standard are becoming the norm for payment HSMs. Specific payment functions are layered into payment HSMs. A payment HSM will provide you with rich implementations of things like EMV or P2PE features. It does more work and has functions that don't necessarily restrict themselves to cryptography.

General-purpose HSMs offer higher-level APIs enabling integration with a variety of use cases. A general-purpose HSM allows you to create a key but doesn't enable you to restrict it to a specific use. General-purpose HSMs have been able to support a variety of use cases starting with PKI and document signing, protecting tokenized transactions and SSL keys for websites. A big driver for general-purpose HSMs is IoT, with the devices being used for the Injection of Keys and certificates in manufacturing. While robust device authentication, digital signing and data protection for IoT are growing use cases, other areas are emerging, including the need for supporting a root of trust in advanced analytics repositories and now used to secure crypto currency.

Quantum Ready Cybersecurity Foundations for a Trusted Digital World

CRYPTO4A

Crypto4A Technologies, based in Canada, is a world-class team with a track record of creating value in the cyber security industry. Crypto4A provides enterprise, cloud providers, mobile application, and IoT developers with sophisticated hardware-based security to keep the digital keys and their machine identities that run commerce, banking, payments, logistics, and the entire digital economy safe.

Crypto4A's QxEDGE™ - HSM-as-a-Platform allows our customers to create high-quality wholistic solutions that balance best-in-class capabilities, operational efficiency, and agility with cost while ensuring business continuity for your digital transformation in a physically disconnected world.

The QxEDGE™ brings together security applications, a quantum-ready HSM, and the tools and level of integration required by DevSecOps teams to develop, deploy, and manage their security applications at scale in a simple and sustainable way. It has the flexibility to support numerous applications that run in an environment that is familiar to DevSecOps teams by supporting modern cloud native tools and technologies they use every day.

To find out more about how you can ensure a successful digital transformation for your business please visit us at www.crypto4a.com.

IDC Canada

33 Yonge Street, Suite 902
Toronto, Ontario
Canada, M5E 1G4
Twitter @IDCcanada
www.idc.com/ca



The content in this paper was adapted from existing IDC research published on www.idc.com.

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2020 IDC. Reproduction without written permission is completely forbidden.