HARDWARE SECURITY MODULE: ORIGINAL EQUIPMENT MANUFACTURERS

COMPETITIVE RANKING

ABiresearch.
THE TECH INTELLIGENCE EXPERTS℠

HARDWARE SECURITY MODULE: ORIGINAL EQUIPMENT MANUFACTURERS

This study assesses and compares six manufacturers of Hardware Security Modules (HSM). ABI Research selected the most prominent players offering the National Institute of Standards and Technology's (NIST) Federal Information Processing Standards (FIPS) 140-2 (Level 3) compliant HSMs, at a minimum. This report sets out the market positioning of each profiled company—leaders, mainstream, and followers—and provides strategic recommendations accordingly.

ABI Research assessed Utimaco as the top market leader. Utimaco scored first in the general ranking and was an implementation leader. This is mostly due to a combination of a comprehensive portfolio of hardware and software based on a scalable platform, and diverse application offering. Thales ranked second on the general ranking and was among both the innovation and implementation leaders, outperforming Utimaco with service feature sets. Futurex ranked third in the general ranking due to its well-developed service product and consistent offering of applications and features on both hardware and service, and also classed as an implementation leader. Securosys, while not in the overall leader category, ranked first in the innovation category, outperforming the other vendors in this assessment due to a very extensive offering into new applications.

ABI Research developed this Competitive Assessment (CA) to offer a comparative assessment and ranking of the following HSM manufacturers: Entrust, Kryptus, Securosys, Futurex, Thales, and Utimaco.

OVERALL COMPETITIVE RANKINGS

LEADERS

utimaco®	1	80.6
THALES	2	77.0
FUTUREX	3	75.2

MAINSTREAM

ENTRUST	4	69.4
securosys	5	69.0
KRYPTUS shaping trusted bonds	6	62.4

OVERALL RANKING MATRIX

INNOVATION *VERSUS* IMPLEMENTATION VENDORS
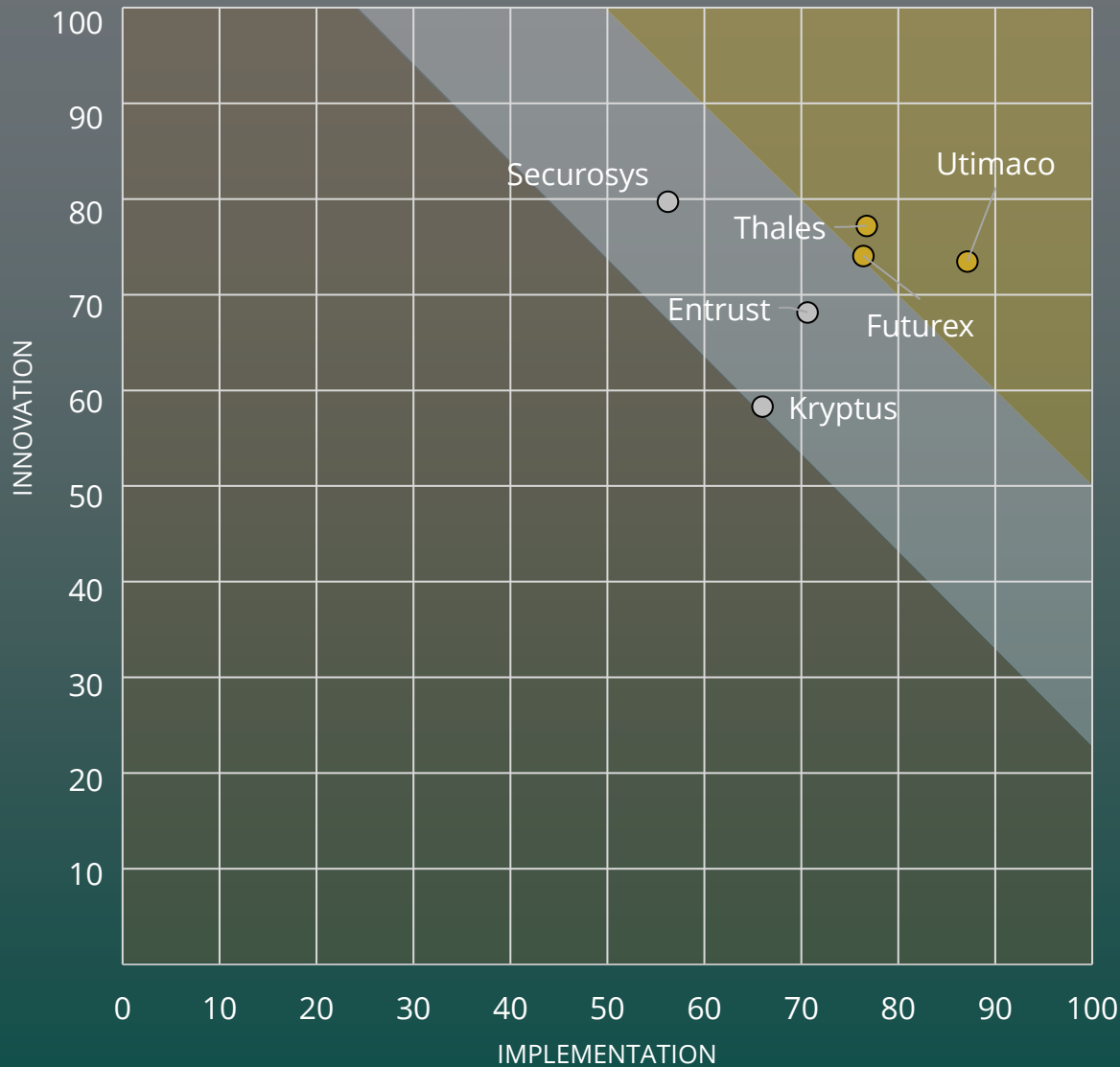
LEADERS

MAINSTREAM

FOLLOWERS

Securosys

Utimaco

Thales

Entrust

Futurex

Kryptus

INNOVATION

IMPLEMENTATION

ABiresearch

4

MARKET TENDS

The main trends in HSM market offerings are:

- **Increased choice of deployment models**: The availability of hybrid (on-premises and cloud) and multi-cloud (both public and private), as well as self-managed or fully-managed service offerings is driven by increased demand for HSM capabilities in a growing number of enterprises undergoing digital transformation strategies, in particular as they migrate to the cloud. Hybrid deployments (where an on-premises node is connected to the cloud cluster) is a huge growth market. A greater number of vendors are entering the market, and notably service providers, are offering scalable and cost-effective services to an expanded user base.

- **Greater choice of features for more customer flexibility**: Demand for flexibility in terms of use cases, management, and deployment are driving vendors to increasingly differentiate and innovate in a market that has traditionally been relatively monolithic. Greater competition, especially in terms of service offerings, means that manufacturers are pitted against third party service providers and need to offer rich feature sets, modular options, ease of management, and greater choice of functions. This is given rise to holistic services where the type of HSM (GP, payment) is less important than the applications it can enable, and to a certain extent, converged HSM appliances for those customers preferring on-premises deployments.

- **New end markets and application**: Demand has been growing beyond the traditional financial, enterprise, and government industries with HSM capabilities sought to enable cryptographic, as well as identity and access management efforts in the IoT and 5G networks. Beyond that, blockchain applications continues to interest and appeal, despite high fluctuations in market demand (hype to downscale). Beyond that, there is increased focus on enabling crypto-agility, notably with the advent of the post-quantum cryptography (PQC) standards awaited this year from the US NIST.

CRITERIA AND METHODOLOGY

VENDOR MATRIX

Methodology: After individual scores are established for innovation and implementation, an overall company score is established using the Root Mean Square (RMS) method:

$$Score = \sqrt{\frac{innovation^2 + implementation^2}{2}}$$

The resulting overall scores are then ranked and used for percentile comparisons.

The RMS method, in comparison with a straight summation or average of individual innovation and implementation values, rewards companies for standout performances.

For example, using this method, a company with an innovation score of nine and an implementation score of one would score considerably higher than a company with a score of five in both areas, despite the mean score being the same. ABI Research believes that this is appropriate as the goal of these matrices is to highlight those companies that stand out from the others.

RANKING CRITERIA

Leader: A company that receives a score of **75 or above** for their overall ranking

Mainstream: A company that receives scores **between 60 and 75** for their overall ranking

Follower: A company that receives a score of **60 or below** for their overall ranking

Innovation Leader: A company that receives a score of **75 or above** for their innovation ranking.

Implementation Leader: A company that receives a score of **75 or above** for their implementation ranking.

INNOVATION CRITERIA

Customer Flexibility: Companies that offer a great choice of features in software, deployments, backup, capacity, monitoring, multitenancy, management, mobility, scalability, availability, access control, and authentication are the ones that excel in the customer flexibility criterion.

As-a-Service Options: Considering the demand for cloud and managed service models for HSM, companies that offer a broad range of deployment models beyond the sale of on-premises appliances including options for both public and private cloud achieve maximum scores in this criterion.

Partner Ecosystem: This criterion evaluates the types of partnerships companies have secured for the integration and interoperability of HMS with technologies (and providers of such technologies) such as Transport Layer Security (TLS)/Secure Socket Layer (SSL), code and digital signing, encryption key and Public Key Infrastructure (PKI) management, identity and access management, authentication, encryption, tokenization, firewalls, payments, web apps and servicers, containers, and cloud services and Internet of Things (IoT), among others.

Go-to-Market: The criterion assesses the scope and reach of go-to-market strategies such as sales (internal sales team, channel partners, regions service), as well as participation in associations and alliances, including programs for technology integration and sales channels, also for standards and best practice development and general information sharing in cybersecurity.

New Applications: This criterion considers the state of development and readiness of HSMs for use in new applications, notably in post-quantum cryptography ((PQC) public key encryption and digital signatures), in the IoT (key injection for root of trust, communication security such as Long-Range Wide Area Network (LoRaWAN), for example), in blockchain (consensus logic, Bitcoin Improvement Proposals, etc.), and in 5G (e.g., Secure Mobile Subscriber Authentication and Key Agreement).

ABiresearch.

IMPLEMENTATION CRITERIA

Form Factor: Number of different types of appliances (network attached, Peripheral Component Interconnect (PCI) express cards, small form factor or USB), application (general purpose, payment, and converged), and services that the company offers for its HSMs.

Security Algorithms: The different types and breadth of algorithms that the HSM appliance and service offers (asymmetric, symmetric, key authentication, hash, named curves, and Random Number Generation (RNG)).

Certification and Compliance: Types of certifications and compliance to various nationally and internationally recognized standards of the HSM appliances and the respective data centers from which the HSM services are hosted for payment (PCI PTS HSM) and General Purpose ((GP) FIPS 140-2, CC EAL4+) applications.

Application: The applications enabled by the HSM offerings for GP (key/credential generation, storage, management, PKI, signing, encryption, smart card issuance, DNSSEC, timestamping, root certificate, etc.), payment and related transaction operations (for magnetic strip and EMV-based cards, PIN ATM, Point of Sale (PoS), 3-D Secure, CVV, etc.), and converged (tokenization, credentialing, etc.).

Architecture: This criterion evaluates the HSMs overall architecture including availability and feature choice related to operating systems (Windows, Linux, etc.), virtual environments (VMware, Hyper-V, etc.), API (management and crypto), SDK (including HSM emulators, client libraries), and physical security (baffles, tamper proofing, SCA, etc.).

ABiresearch.

INNOVATION RANKINGS

TOP INNOVATORS

Securosys and Thales are the innovation leaders in this competitive assessment, ranking first and second, respectively. Futurex and Utimaco come in at a close third and fourth position.

Securosys is the surprise winner in this innovation category, contending and beating the market HSM leaders in this space. While other vendors have focused on new deployment models and flexible features, Securosys has focused on innovating within the HSM technology itself and focusing on new use cases for HSM usage. With a laser focus on technology improvement, Securosys is certainly providing a breath of fresh air.

Thales offers an uncontested broad range of customer options for the flexible deployment of its HSM solutions; in fact, there is little that the firm does not offer for its hardware appliances. It's strong partner network and participation in technology alliances and associations means it is in the cusp of industry developments and integration efforts, a much-valued asset in an increasingly connected world.

| 1 | securosys | 79.7 |
| 2 | THALES | 77.2 |

FULL INNOVATION RANKING

	Rank	Score
securosys	1	79.7
THALES	2	77.2
FUTUREX	3	74.1

	Rank	Score
utimaco®	4	73.5
ENTRUST	5	68.2
KRYPTUS shaping trusted bonds	6	58.3

TOP INNOVATOR
ABiresearch

IMPLEMENTATION RANKINGS

TOP IMPLEMENTERS

Utimaco is the implementor leader, reaching a score above 75 in this criterion, with Thales and Futurex in second and third place, respectively.

Utimaco offered the most complete and diverse range of HSM solutions, serving all types of applications, at all price points, and in various form factors. The strength of this diversity of these offerings is possible due to the way in which it has abstracted its hardware layer from the software and firmware stacks that is has developed to layer on top. This means it provides the most flexibility and scalability of any HSM platform on the market today.

Futurex is the most developed in terms of payment offerings, with a comprehensive hardware and cloud offering that is difficult to match. It has built on this foundation a well-rounded GP portfolio targeting enterprise which exploits the converged platform format to its successful advantage.

Thales is an undeniable market leader in the HSM space. It's clout, reach, and expertise in the security industry makes it a stalwart with a market leading HSM product. It features in third, however, because it is a step behind in terms of its cloud-based options for payment applications in particular, although it is fast catching up.

1	utimaco®	87.1
2	THALES	76.7
3	FUTUREX	76.4

TOP IMPLEMENTER
ABiresearch

FULL IMPLEMENTATION RANKING

TOP IMPLEMENTER
ABiresearch

utimaco®	1	87.1
THALES	2	76.7
FUTUREX	3	76.4

ENTRUST	4	70.6
KRYPTUS shaping trusted bonds	5	66.0
securosys	6	56.3

INDIVIDUAL COMPANY ASSESSMENTS
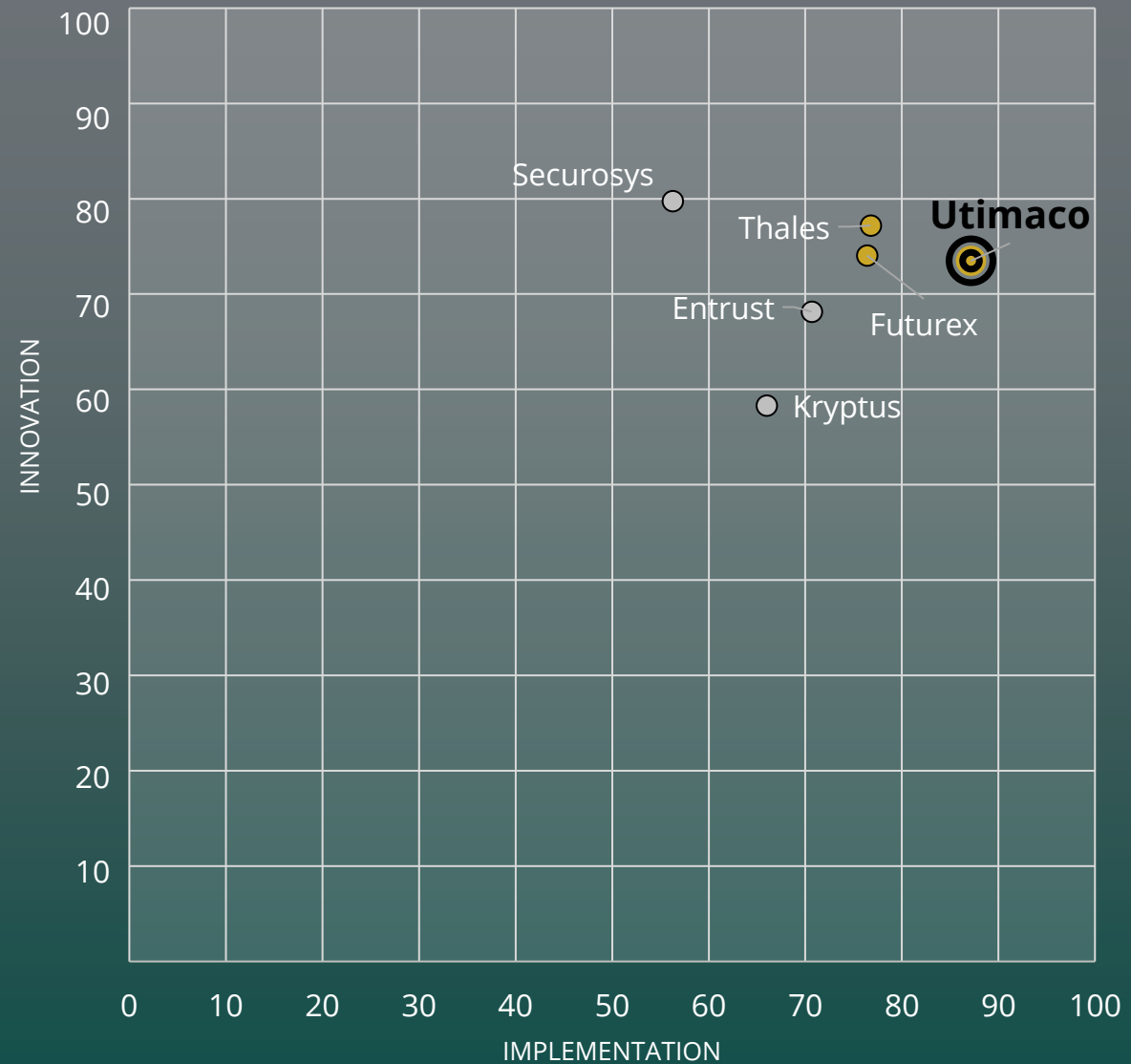
INNOVATION

utimaco®

**INNOVATION
SCORE: 73.5**

Utimaco is a global platform provider of trusted cybersecurity and compliance solutions and services with headquarters in Germany and the US. The firm offers HSMs, solutions for key management, data protection, identity management, signing, and timestamping, as well as compliance solutions for telecommunication providers in the field of regulation.

Utimaco ranks fourth in the innovation category, with a score of 73.5, preceded by Securosys, Thales, and Futurex. Utimaco provides a high level of customer flexibility for both on-premises and service offerings of its HSM products. Utimaco's strength lies in the way that it's HSMs can be easily configured through the offer of numerous software and firmware stacks, both for general purpose and payment applications. This flexible approach for loading applications enables clients to mix as well as change applications throughout the lifetime of their HSM use. This flexibility allows for a natural extension into cloud deployments.

u.trust 360 is Utimaco's centralized monitoring and management platforms for all its HSM offerings. It provides centralized administration, monitoring, and provisioning of hundreds of HSMs across multiple data centers, network segments, and locations through one single pane of glass. Based on customizable user groups it provides real-time status updates and compliance reporting, as well as centralized alerts and enables consistent security policy enforcement, provides transparency, and maintains the health of the HSM infrastructure.

A key evolution of that is the u.trust Anchor product family which is the world's first converged crypto platform, enabling Payment and General-Purpose uses cases on one central HSM platform.

u.trust Anchor CSAR (Cloud Services Architecture) as part of this new product line allows the deployment of a shared crypto-services platform on which various additional applications can be added and customized (i.e., payment, blockchain, PQC, etc.). Based on a fully containerized model, each partition is sealed within a container with dedicated configurations and policies set for each container. This is a step beyond simply offering multi-tenancy for one firmware implementation and reflects the next generation of converged HSM platforms.

In terms of service deployment models, Utimaco is on par with other vendors in the assessment. Offering both fully and self-managed service options, including hybrid deployment models (combining on-premises and cloud). The firm further offers service options for deploying Utimaco HSMs in public cloud infrastructures, as well as in select data centers and colocation infrastructure providers with which it has partnerships.

ABi research. 19

INNOVATION

utimaco®

**INNOVATION
SCORE: 73.5**

Utimaco's partner ecosystem is broad and varied. A long-standing player in the cybersecurity and compliance industry, the firm has built partnerships with many different stakeholders for technology integration, including direct competitors. On par with Thales, both firms are only superseded by Entrust's partner ecosystem in this regard.

Utimaco's go-to-market strategy is well developed, with a global sales reach served by both an internal sales team and channel partners, and dedicated programs to drive those channels. Beyond that, Utimaco is an active participant in various associations and industry alliances for technology integration and development, as well as government-based security information sharing initiatives.

With regards to new applications, Utimaco offers options for a whole host of new use cases, including IoT use cases and crypto-agility capabilities (e.g., for PQC). Beyond that, the firm offers strong support for various blockchain applications including specific elliptic curves, BIP32/44, signing algorithms for consensus and verification, as well as Distributed Ledger Technology (DLT_ platform support.

IMPLEMENTATION

utimaco®

TOP
IMPLEMENTER
ABiresearch.

**IMPLEMENTATION
SCORE: 87.1**

Utimaco ranked first in the implementation category, with a score of 87.1. In large part, this is because it offered the most complete and diverse range of HSM solutions, serving all types of applications, at all price points (from entry-level to top of the line), and in various form factors.

- For network attached appliances, there is the SecurityServer Local Area Network (LAN) and Cryptosec LAN for GP, PaymentServer LAN and Cryptosec-Banking for Payment, and PaymentServer Hybrid and Cryptosec-Banking for converged applications.

- For PCI-express (PICe) cards, Utimaco offers SecurityServicer as well as the CryptoSec-Dekaton, all available in different product ranges (low to high).

- Further, there is the Payment Server SFF, a small form factor offering.

- In terms of services, Utimaco offers three HSM-as-a-Service options: its own cloud offerings CryptoServer Cloud and MyHSM (Payment HSM-as-a-Service), as well as Interxion KeyGuardian for public cloud implementations.

The diversity of these offerings is possible because Utimaco has worked from the basis of building a uniform underlying hardware platform upon which various (and multiple) firmware stacks and software options can be added, and which include cloud ready Application Program Interfaces (APIs). Through this, Utimaco is able to offer converged HSM solutions which can be used for singular or for multiple applications (payment and general purpose) and be both PCI-HSM and FIPS 140-3 compliant (or none at all if not required). No other vendor currently offers this level of diversity, and Utimaco is unique in this regard.

Utimaco therefore offers one of the widest range of general-purpose and payment applications in the market, which can be served by any combination of firmware and software options, in the various deployment models (on-premises, cloud, and hybrid). In terms of available security algorithms, Utimaco offers the whole gamut of cryptographic capabilities in encryption (symmetric, asymmetric) key authentication, hashes, named curves, and RNG (including regional and legacy options). Importantly, within its crypto API offering is the possibility for clients to load their own proprietary algorithms.

From an architecture perspective, Utimaco does well, with varied choice in Operating System (OS) and virtual environment deployments as well as a comprehensive selection of SDKs, HSM emulators and simulators, custom firmware, and crypto APIs on offer. It is only in terms of APIs for management that Utimaco falls short in comparison to other vendor offerings.

IMPLEMENTATION

utimaco ®

TOP IMPLEMENTER
ABiresearch.

IMPLEMENTATION
SCORE: 87.1

From a certification and compliance perspective, Utimaco is one of the two vendors, alongside Thales, to offer FIPS 140-2 Level 4 HSM appliance (on-premises only) as well as PCI PTS HSM v3 (although Kryptus also offers the latter, and Futurex is in the process of obtaining the certification).

CONCLUDING REMARKS

Utimaco is the overall leader of this competitive assessment, with an overall score of 80.6. Since the acquisition of the Atalla HSM and Enterprise Secure Key Manager product lines from Micro Focus International in 2018, Utimaco has successfully integrated these products with its long-standing General Purpose HSM portfolio. The firm's leadership is attributable to the fact that it created a vision for a converged HSM platform offering for all applications and has largely been able to deliver on that promise. This abstraction of the underlying hardware platform from the applications means that Utimaco has been able to focus on the operational side of HSMs and how the resulting applications can be customized, deployed, and managed in line with changing customer needs. This is acutely true today in a post-COIVD-19 pandemic world where digital transformation has significantly accelerated and innovation in customizable hybrid offerings are becoming an important part of HSM market expansion.

HARDWARE SECURITY MODULE: ORIGINAL EQUIPMENT MANUFACTURERS

THALES

LEADER
ABiresearch.

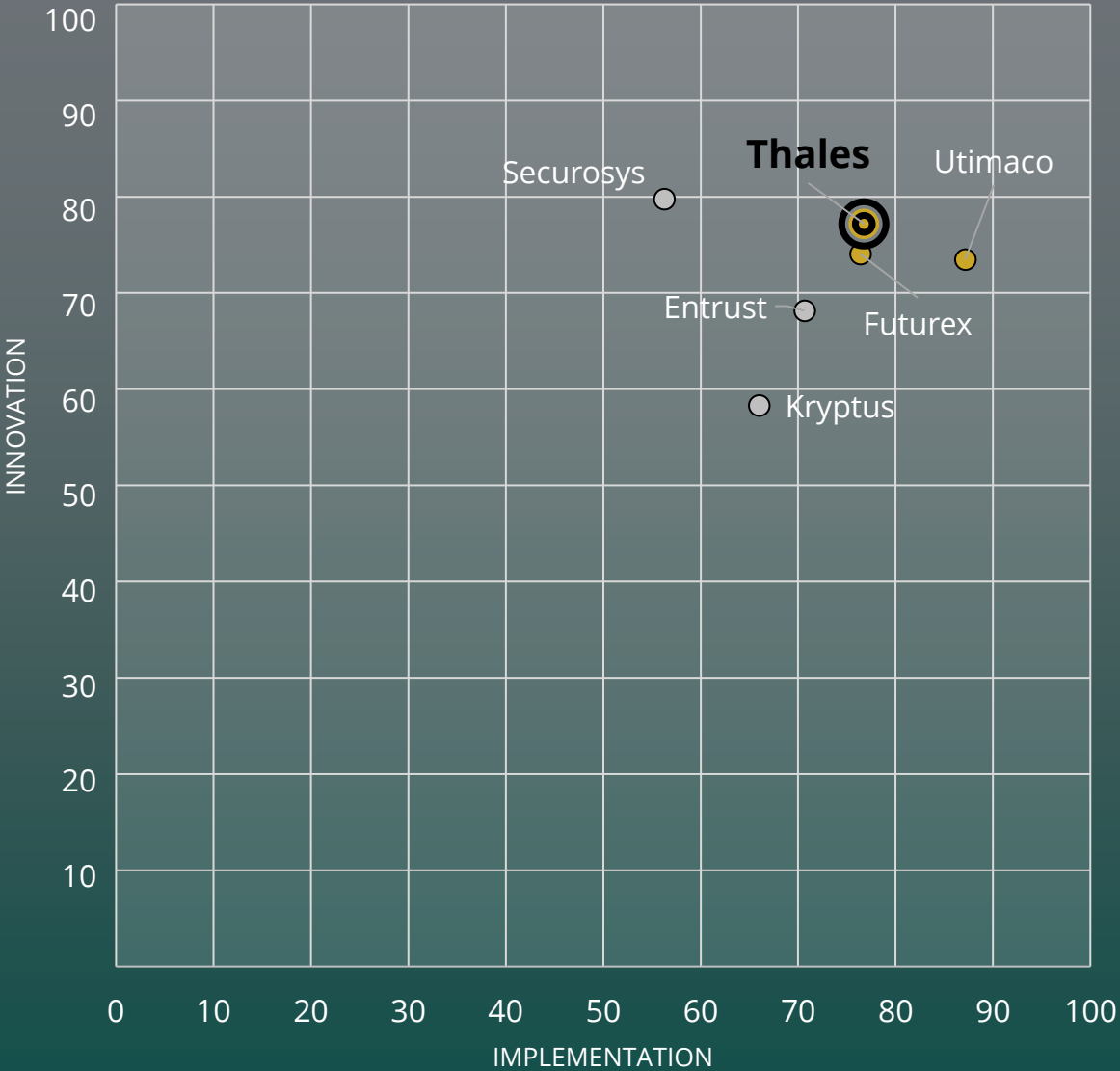TOP INNOVATOR
ABiresearch.

TOP IMPLEMENTER
ABiresearch.

OVERALL: 77.0 | INNOVATION: 77.2 | IMPLEMENTATION: 76.7 | RANK: 2

INNOVATION

THALES

TOP INNOVATOR
ABiresearch

INNOVATION
SCORE: 77.2

Thales is a global market leader in data protection, specializing in encryption, advanced key management, tokenization, and authentication and access management solutions.

The firm scored second in the innovation category, with a score of 77.2, only second to Securosys in the assessment. Thales offers a broad range of customer options for the flexible deployment of its HSM solutions. In terms of backup options, capacity, policies management, monitoring/logging, availability, scalability, access control, and management and configuration, there is little that the firm does not offer.

Thales approach to converged hardware platforms is to enable customers the flexibility to choose both general purpose and/or payment capabilities on either platform. This includes functionality modules in the general-purpose appliances and custom functions through software extensions where general purpose commands can be added as customizations to supplement core payments functionality.

In terms of services, Thales has a full suite of deployment options available for customers, whether on public or private cloud implementations. The services (as well as the HSM appliances) can be fully or self-managed by clients, and hybrid deployments are extensive and seamless compared to the competition.

One of Thales' greatest strengths is its partner ecosystem, which surpasses that of the other vendors in this assessment. As a large multinational, the firm already has global clout, but it cultivates those partnerships and is a dynamic participant in the technology industry across the board, not just in mainstay technologies, but also in emerging ones, including IoT, blockchain, 5G and quantum. This translates to a strong scoring in the Go To Market criteria.

Thales is actively involved in numerous security technology alliances and associations (e.g. concerning Common Criteria, Crypto Modules, eIDAS, FIPS 140-3, PCI, Oasis PKCS11, KMIP, CSA, Linux, etc. among other technology and standard development efforts).

The Thales Accelerate Partner Network provides the framework for partners to integrate with Thales technologies. The Network delivers focused training, profitable discount structures and support. The partner ecosystem includes value added resellers, technology vendors, embedded solutions (OEM) partners, managed service providers (MSPs), and distributors with an overlay of strategic alliance partner, allowing Thales to increase scale and provide greater reach to potential customers.

INNOVATION

THALES

TOP INNOVATOR
ABiresearch.

INNOVATION
SCORE: 77.2

Part of the Network is the Thales's Technology (Integration) Partner Program, which provides technical, marketing, and business development support to partners who want to enhance their services and technologies by validating and documenting integration with Thales products supporting interoperability efforts. Technology Partners receive recognition for successful integration with Thales products, as well as benefits such as access to tools and technical information that support their business development and marketing efforts.

All this underlies the extensive internal sales and channel partners that Thales has built up over the years, with a highly organized and expansive internal team focused on various aspects of the sales process and supporting both direct and indirect sales. Combined with Thales global network of channel partners, Thales has the most extensive sales reach of any vendor in this assessment and is a formidable force to compete against.

With regards to new applications, Thales scored well, offering HSM solutions across the board, from IoT, blockchain, crypto-agility, post-quantum cryptography and 5G. The latter is where the firm really stands out, with a high-profile partnership announcement in December 2021 with Ericsson, where the Luna HSM is being integrated into Ericsson's 5G Core offering to telco. Serving the role of an Authentication Security Module, the solution is set to enable communications service providers to store crypto keys and algorithms to protect subscriber data management solutions.

IMPLEMENTATION

THALES

TOP IMPLEMENTER
ABiresearch

IMPLEMENTATION SCORE: 76.7

Thales scored second in the implementation category, with a score of 76.7, behind Utimaco. Thales offers a varied choice of form factors and performance options for its HSM solutions. There are two series each of GP HSMs (Luna HSM) for both network appliance and PCIe card varieties. The S series uses multi-factor authentication, and the A series password authentication. Each series (for each form factor) has 3 models that differentiate in performance, key capacity, and the number of partitions. The firm also offers the Luna USB HSM as a small form factor. In terms of service offerings, Thales proposes the Thales Data Protection on Demand (DPoD) Luna Cloud HSM.

All Luna HSMs, including Luna Cloud HSM, work in a similar fashion, sharing a common integration point to all client applications – the Luna Universal Client. This means customers have the flexibility to move their keys between the various HSM form factors.

With regards to payment HSMs, Thales has three models under the payShield 10K brand, as well as a service offering DPoD payShield P2PE Services (Technology or Private Preview, available for deployment and which will launch later this year). However, the payShield cloud service on DPoD currently only provides Point to Point encryption, decryption, key management, and key distribution services and not the full breadth of payment capabilities offered by the hardware appliance. However, there are more expansive services available through CSPs and coming soon directly from Thales. The Thales approach is partner based, leveraging a broad ecosystem to offer extensive payment services through partners. Thales plans to extend these partner based applications offerings in Thales own cloud services. Further, Thales does not offer market dedicated converged hardware platforms that combine payment and GP capabilities, but the capabilities are available to enable customers the flexibility to choose to deploy general purpose and/or payment functionality on either range of solutions.

In terms of certification and compliance, Thales is at the fore, offering the latest for the various corresponding applications: PCI PTS HSM v3, FIPS 140-2 (Level 3 and 4), CC EAL 4+, QSCD for eIDAS, and numerous country specific standards (including secret classifications). It is also one of the few that is in the process of certifying for FIPS 140-3. Further, on the security algorithms offerings, Thales has one of the most complete range of options available on the market.

With regards to architecture, Thales provides a broad range of options for its GP HSM in terms of OS, virtual environment, APIs (for management and crypto), SDKs and physical security. For many of these same options for the payment HSMs, Thales offers them through partner solutions, such as Microsoft Azure Payment HSM, Oper8 payG8 services, First Tech HSM Off Premises (HoP) service, DataMesh payment solutions, among many other cloud service providers' platforms.

IMPLEMENTATION

THALES

TOP IMPLEMENTER
ABIresearch

IMPLEMENTATION SCORE: 76.7

Thales has been conducting a proof-of-concept of its own hosted payShield multi-cloud service with key customers over the past few months and will be taking the service live later in H1 2022 – this covers all functionality supported by their on-prem HSMs.

Thales enables customers to trial the actual solution, rather than simply emulating or simulating the experience. It also offers HSM availability via eLABS and Thales cloud service, as well as via partner services.

CONCLUDING REMARKS

Thales ranks second in the competitive assessment, with an overall score of 76.7. The firm scored consistently well across all the criteria defined in the assessment, in both categories, which is a testament to the dedication it takes to offer a high-level comprehensive HSM offering on all fronts. Thales is undoubtedly a stalwart in the digital security industry, with long-standing experience in the HSM market. With the acquisition of Gemalto, it gained a fuller and more complete HSM offering across GP and payment applications. Thales excels in cloud-based solutions, such as Luna Cloud HSM services on the DPoD cloud marketplace, and is actively expanding its payment services into offering a fully-fledged own cloud service based on the success it has had with its many partner solutions.

HARDWARE SECURITY MODULE: ORIGINAL EQUIPMENT MANUFACTURERS

OVERALL: 75.2 | INNOVATION: 74.1 | IMPLEMENTATION: 76.4 | RANK: 3
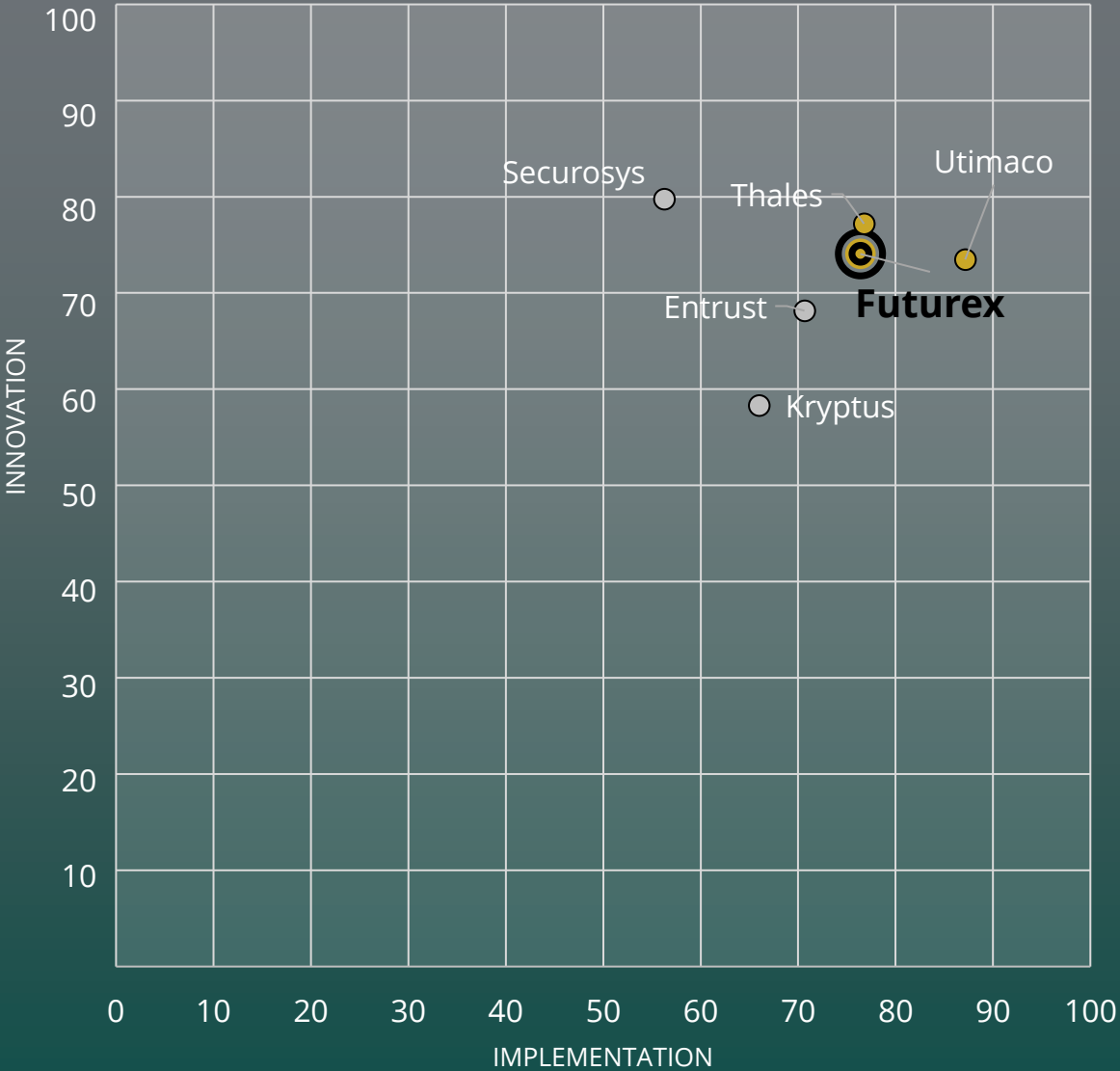
INNOVATION

INNOVATION
SCORE: 74.1

Futurex is a U.S. based company specializing in data security through the offer of HSMs, key management, and secure storage solutions. Futurex ranked third in the innovation category, with a score of 75.2. The firm scored well in the customer flexibility and as-a-service options criteria, higher than the other vendors in this assessment (in both categories). Futurex offers the richest choice of features for its HSM products; only Securosys comes close in this customer flexibility criteria.

The firm is unique in that the same suite of features available for its on-premises product is also available at the service level through its VirtuCrypt Cloud HSM offering, and notably for its payment-based offerings, which is rare on the market. Beyond even Utimaco's service efforts, Futurex is at the forefront of the service proposition for HSM-based applications, having managed the VirtuCrypt for almost a decade. It's HSM appliances have evolved to serve that proposition, enabling Futurex to carve a distinctive place for itself in the HSM market.

As such, Futurex excels at offering a wide and varied range of service propositions, including hybrid deployment options. The firm has worked with both public cloud service providers and partner data centers, as well as offering own VirtuCrypt data centers (about eleven to date across the Americas, Europe, and Asia-Pacific) to propose compelling options for cloud-based HSM usage across the board. This has been especially effective in the payment space, where service propositions have lagged a little behind GP applications, marking Futurex out as an innovator in the space.

Futurex scores well also in the partner ecosystem and in its go-to-market strategy, which is well-developed. Having a strong establishment in North America, Futurex lacks, however, the global reach that companies like Utimaco and Thales, and even Entrust have, especially in European markets. But the firm has nonetheless made some significant inroads in the Asia-Pacific market recently, where cost-effective service propositions are in high demand.

From a new applications perspective, Futurex has forayed into IoT-enablement (key injection for root of trust) and 5G (secure mobile subscriber authentication and key agreement) and is also working on PQC capabilities. However, it is a little less focused on the blockchain front than companies like Securosys, despite a partnership in place with R3 for its Corda Enterprise Platform, which integrates Futurex HSMs.

IMPLEMENTATION

FUTUREX

TOP IMPLEMENTER
ABiresearch.

IMPLEMENTATION
SCORE: 76.4

Futurex ranked third in the implementation category, with a score of 76.4. While the firm still offers different hardware models for GP (Vectera Plus) and payment (Excrypt Plus and Excrypt SSP Enterprise v.2) applications, it's next generation CryptoHub HSM is a fully fledged converged platform. The CryptoHub is offered in various pricing ranges, dependent on the mix of licenses and functionality desired by the end user. Beyond that, Futurex offers the VirtuCrypt Cloud HSM and Key Management Service, the flagship in its product portfolio. The firm is unique in offering all the same security algorithms, certification and compliance, applications, and architecture for its hardware appliances and its cloud offering, which drives its high score in the innovation category.

In terms of security algorithms, Futurex offers a good range of coverage, although not as extensive as some of the market leaders. With regards to certification, Futurex does well, and is in the process of certifying for both PCI PTS HSM v3 and FIPS 140-3. It does not yet have Common Criteria EAL 4 and QSCD for eIDAS in Europe but is in the process of obtaining them.

With regards to applications, Futurex scores the highest, with the only application not on offer from its products being Timestamping. The fact that it offers such a broad range of applications in both payment and GP, and this equally as an on-premises or service offering is Futurex's key strength.

Futurex again scores the highest from an architecture criteria perspective. The firm is particularly strong it is API offerings, for both management and crypto, which puts it ahead of the other vendors in this area. In fact, Futurex was the first to release a web API for payment HSMs, to enable developers to integrate payment applications with both Futurex's on-premises and cloud HSMs.

CONCLUDING REMARKS

Futurex ranks third in this competitive assessment, with an overall score of 75.2. The firm is a leader in the payment space in particular, well-known in North America for its extensive payment HSM offerings. Its expansion into international markets is ongoing, but it will be difficult to surpass the clout of companies such as Thales and Utimaco, especially in Europe where demand (especially from a GP perspective) is largely prescribed by regional regulations and standards.

However, Futurex has a uniquely strong offering in terms of its cloud HSM service, for GP and payment applications equally. An outlier in terms of its overall company background when compared to the broad security portfolios offered by Utimaco, Thales, and Entrust, Futurex has carved itself a successful niche in the HSM market. This is further strengthened by its new converged CryptoHub HSM, which will unify the hardware layer and enable Futurex to focus on enhancing the operational side of HSM management for end users. Overall, Futurex certainly deserves its place as a top vendor in the HSM space.
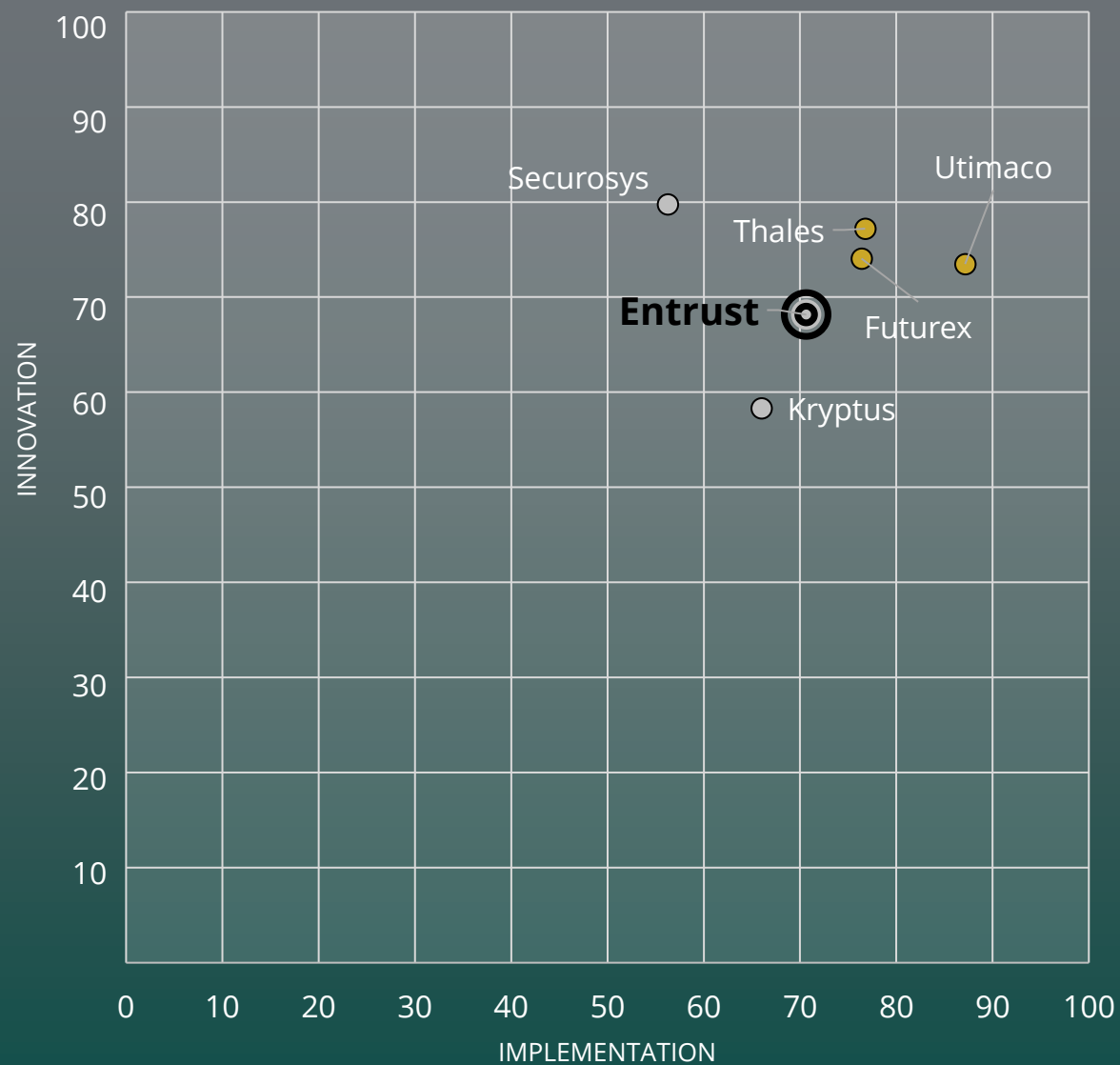
ABI RESEARCH COMPETITIVE RANKING

HARDWARE SECURITY MODULE: ORIGINAL EQUIPMENT MANUFACTURERS

ENTRUST

OVERALL: 69.4 | INNOVATION: 68.2 | IMPLEMENTATION: 70.6 | RANK: 4

OVERALL: 69.4 | INNOVATION: 68.2 | IMPLEMENTATION: 70.6 | RANK: 4

ENTRUST INNOVATION *VERSUS* IMPLEMENTATION FOCUS

INNOVATION

ENTRUST

INNOVATION
SCORE: 68.2

Entrust is a firm specialized in identities, payments, and data protection solutions with global standing. Entrust scored 68.2 in the innovation category. Entrust entered the HSM market in 2019, when it purchased nCipher from Thales, and with it acquired both talent and experience. The acquisition of 1996-founded nCipher allowed Entrust to strengthen its trusted identity and secure issuance technology solutions. A heavyweight in the smartcard and certificate/PKI space, the addition of an HSM line of products was a natural next step for the firm. It has quickly established itself as a strong market player in the global HSM space.

In terms of customer flexibility, Entrust scores highly with a wide range of available features and options for its product offering, only third behind Futurex and Securosys in this regard. The main limitations are around the availability of expanded payment functionalities as Entrust does not support niche legacy payments processing, although some digital payment applications are enabled on its GP products. Further, the firm does not offer a fully managed on-prem service to clients, as do some of the other vendors.

Where Entrust falls behind the leaders is primarily on its service proposition in terms of geographic availability. The Entrust nShield as a Service is still a relatively new offering, launched initially in the UK and US in 2019. But it is quickly catching up and the firm recently announced new expansion into Europe in December 2021 and is live in APAC as of February 2022.

Entrust nShield as a Service does work with the main cloud service providers including Microsoft Azure, AWS and Google Cloud, offering BYOK capabilities. Entrust have deployed nSaaS using commercial digital infrastructure companies to ensure adjacency and guarantee interconnectivity with Public Cloud Providers. Entrust is further focused on expanding its service proposition from private data centers.

In terms of partner ecosystem, Entrust is the strongest vendor in this assessment, in large part due to its reputation and expertise in the IAM, PKI and certification/key management space. A leader at the software and services end of these applications means that it has a partner ecosystem that is tightly aligned with the HSM market, a key strength for the application side of things. In part, this is what allows Entrust to offer numerous digital payment services, despite only offering a GP HSM.

With regards to its go to market strategy, Entrust has a far reaching, global network of channel partners and a well-established internal sales team that is already well attuned to the end-markets for GP HSM solutions. Entrust offers two main programs, the nFinity HSM Technology Program and the nFinity HSM Channel Program for technology integration and sales respectively.

From a new applications perspective, Entrust is squarely in the mainstream, offering key injection for IoT root of trust, some basic 5G and blockchain options, and has available crypto-agile features, notably for PQC.

IMPLEMENTATION

ENTRUST

IMPLEMENTATION
SCORE: 70.6

Entrust scored 70.6 in the implementation category. The firm offers its flagship nShield Connect XC in three performance ranges as hardware appliances, as well as a converged offering, the nShield SoIo XC, also in the three performance declinations. It further offers a small form factor HSM, the nShield Edge, as well as its own cloud offering, nShield as a Service.

While Entrust does not offer a dedicated payment HSM, it does offer a range of payment applications on its GP and converged platforms, if not the full gamut enabled by an actual payment HSM that is PCI PTS HSM certified. Entrust can provide a number of functionalities linked to the issuance, credentialling and key management market, as well as tokenization and digital payments.

From a security algorithm perspective, Entrust is no laggard and scores highly on breadth and scope. Similarly from a certification and compliance perspective, and it does offer a payment related certifications under PCI P2PE.

In terms of architecture, Entrust scores highly in terms of options for build, especially on the crypto API side, which is in line with its broad coverage in terms of security algorithms. There is also a good choice in terms of operating system and virtual environments, which makes for an attractive product offering suitable for various implementations.

CONCLUDING REMARKS

Entrust comes in fourth in the assessment, scoring a total of 69.4. The firm places itself well within the mainstream of the HSM market. The main elements holding Entrust back are its lack of payment HSM appliance which would be a good fit with its broader offerings in the smartcard and issuance space, as well as its newer service proposition. However, the lack of payments HSM is just one missing use case and further, nSaaS is fully available to workloads running in the public cloud and Entrust has integrations with cloud enabled applications. . Nonetheless Entrust is a strong contender in the HSM market and has ample opportunity to push the envelope in terms of cloud-based service development. This is where it can most successfully showcase its expertise in PKI, identity and key management and drive new business. .

HARDWARE SECURITY MODULE:
# ORIGINAL EQUIPMENT MANUFACTURERS

securosys

TOP INNOVATOR
ABiresearch

OVERALL: 69.0 | INNOVATION: 79.6 | IMPLEMENTATION: 56.3 | RANK: 5

OVERALL: 69.0 | INNOVATION: 79.6 | IMPLEMENTATION: 56.3 | RANK: 5

SECUROSYS
INNOVATION
VERSUS
IMPLEMENTATION
FOCUS

HARDWARE SECURITY MODULE: ORIGINAL EQUIPMENT MANUFACTURERS

ABiresearch 38

INNOVATION

securosys

TOP INNOVATOR

ABiresearch.
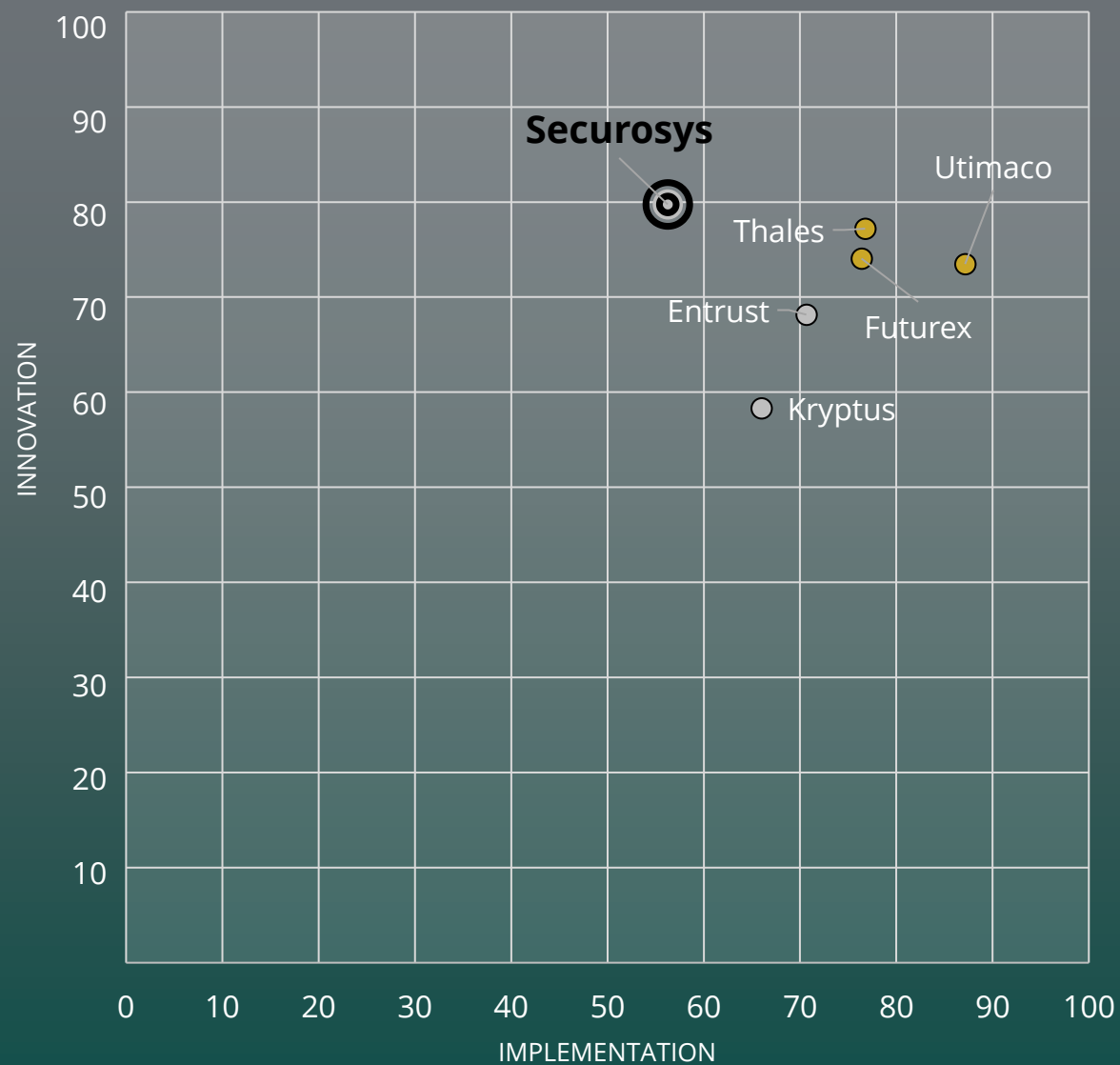
INNOVATION
SCORE: 79.7

Securosys is a Swiss-based technology company specializing in securing data and communications, with a niche market focus around blockchain and crypto asset solutions, the Swiss banking system (SIC) and stock market (SIX), and PKI.

Securosys came first in the innovation category, scoring 79.7. The firm has the most diverse and broad range of options and features allowing for maximum customer flexibility for its HSM product offerings (both on-premises and cloud-based). Securosys leverages a Trusted Execution Environment (the Imunes TEE) to allow any type of code (custom or other) to run securely within the appliance. This is what enables the secure configurability, update/upgrade, and management of the HSM and the applications it can run. Securosys Primus HSMs are designed for containerized deployment of applications, with software options available as CI/CD containers. The Decanus Terminal allows for the management of the HSMs, which can manage up to 64 Primus HSMs in different locations worldwide or just one partition on the Primus HSM, not unlike Utimaco's u.trust 360 management platform.

Securosys has a well-developed service offering, with a global presence. The firm scored second only to Futurex in the as-a-Service options criteria. The CloudsHSM runs on the Primus HSM hardware and is operated from various active and backup data centers in Switzerland and Germany, with services available globally (with dedicated Securosys staff available). Various service packages are on offer: shared or dedicated HSMs with varying levels of performance, capacity, and support. From a public cloud perspective, Securosys has ensured that its HSM technology works to address how enterprises interact with public and enterprise cloud services (including key management, secure data storage, etc.). While its footprint is not as expansive as some of the leaders in this assessment, there is still plenty of opportunity for Securosys to grow.

With regards to go-to-market, Securosys has a small but established internal sales team that is in full expansion and has built up a decent channel partnership in most regions. The firm has sales and partner training programs, and even hosts a yearly user and developer conference.

From a partner ecosystem perspective, Securosys is squarely in the mainstream. As a relative start-up in the space (founded only in 2014), it has a strong technology partner network, in all the key areas pertaining to HSM functionalities (PKI and key management), security, and cloud, but importantly also in blockchain, where it is particularly well engaged. In part this is due to its own developer conference, but also its active engagement in fintech and blockchain conferences, which brings visibility to the firm's innovative technology.

INNOVATION

securosys

TOP INNOVATOR
ABiresearch

INNOVATION
SCORE: 79.7

From a new applications perspective, Securosys scored highest in this criteria. The firm drives a robust and highly active R&D effort, notably around key management and blockchain. With regards to the latter, Securosys has official support for Corda, Hyperledger, ETH2.0, and many other blockchain protocols. Its HSMs are further primed for PQC usage with a crypto-agile platform that is field-upgradeable when those algorithms are standardized. Securosys recently patented a new technology for private (signature) keys. Dubbed Smart Key Attributes (SKA), the technology allows for the addition of rules to individual keys preset by a client so that they can only be used based on the predefined rules. This unique innovation means SKA could potentially minimize the amount of issuance/revocation required and could be used in a wide variety of applications, including for identity management, banking and fintech, and authorization of blockchain transactions, among others.

IMPLEMENTATION

securosys

IMPLEMENTATION
SCORE: 56.3

Securosys came fifth in the implementation category, scoring 56.3. Securosys flagship product is the Primus HSM (X-Series, X/E-Series, and E-Series). As a newer entrant on the HSM scene, and with a focus on GP HSMs, the firm has a more restrained portfolio than the leaders. It does not offer a payment or converged HSM, nor does it have any PCIe or small form factor variant for its Primus HSM. However, it does have various performance models at different pricing ranges, and it's CloudsHSM is also similarly varied.

In terms of traditional (both current and legacy) security algorithms covered, Securosys has them all covered, and they are equally available on-premises and for the cloud service. Where it really shines is the numerous blockchain algorithms that it also covers (e.g., ETH 2.0/BLS, Key Derivation), a stark contrast to most of the other vendors in this assessment. From a compliance perspective, Securosys lacks only PCI-related certification (PTS HSM, PIN, and P2PE), but has both FIPS 140-2 Level 3, CC EAL 4+, and QCSD for eIDAS, as well as the relevant data security compliance requirements for CloudsHSM.

Securosys does not offer any payment-specific applications to date, it can provide digital payment functionalities, including tokenization for PCI DSS compliance, credential issuing, generation, and management, as well as P2PE. Further, it has complete offering from a GP perspective.

Securosys offers a good choice of APIs for crypto and management regarding the HSM architecture, and also offers REST API and Microsoft Double Key Encryption capabilities. Further, the Primus HSM is an agnostic network appliance, so the API is guest-dependent on the virtual environment.

CONCLUDING REMARKS

Securosys came fifth overall in this competitive assessment, with a score of 69.0. The firm is a strong contender in the global HSM market, although remains a specialist with a focused offering in the blockchain/fintech and PKI space. Entrust is probably the most relevant direct competitor, and while Entrust has a greater implementation scoring, Securosys is ahead in terms of innovation. As a niche player, Securosys impresses with its efforts in innovating what have been standard attributes in HSM applications. Its SKA technology is a testament to improving on encryption technologies. This technology development focus is Securosys key strength and will drive success in new use case application as the firm continues to grow. Securosys is a visionary company worth keeping tabs on.
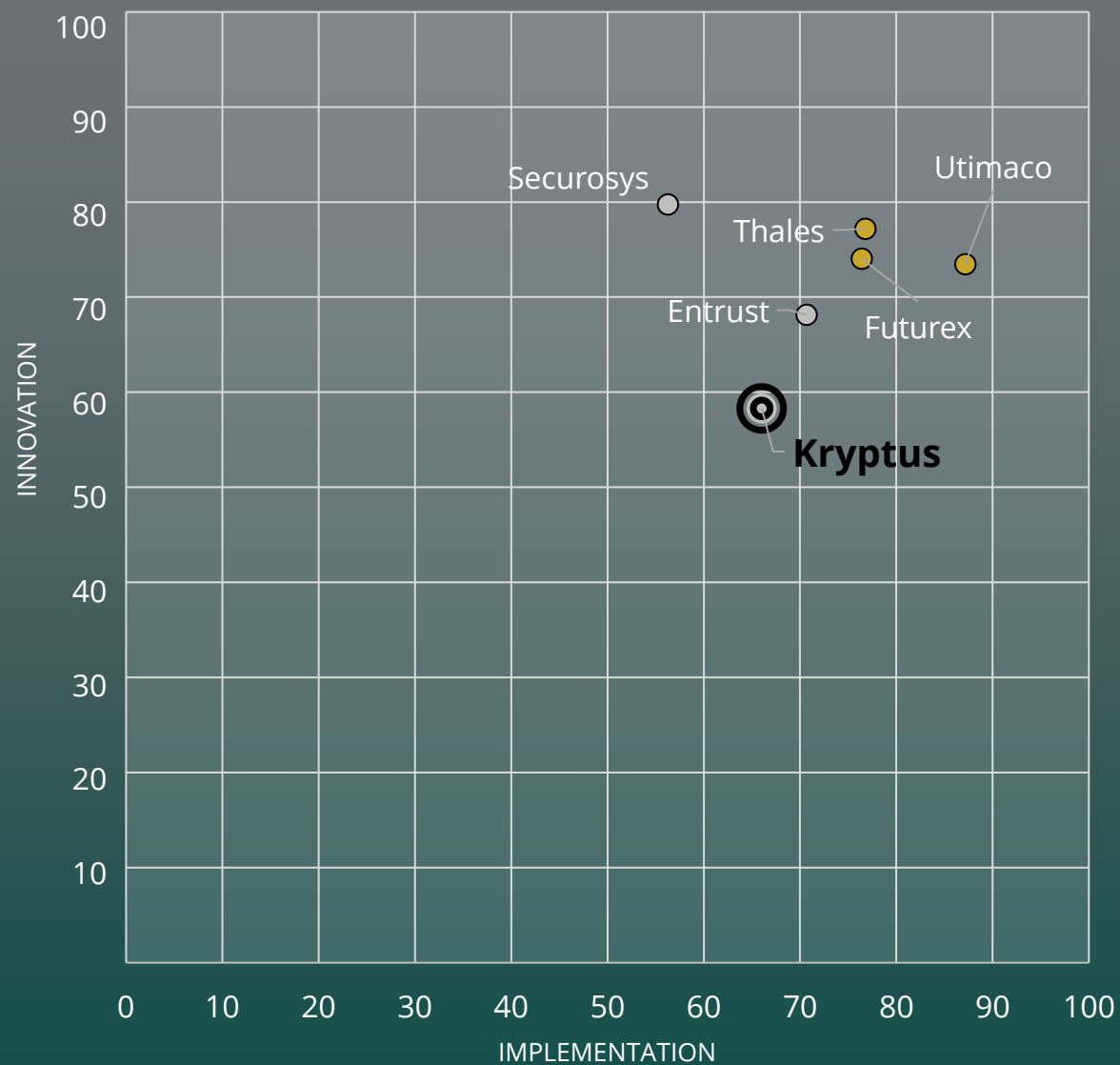
ABI RESEARCH COMPETITIVE RANKING

HARDWARE SECURITY MODULE: ORIGINAL EQUIPMENT MANUFACTURERS

OVERALL: 62.3 | INNOVATION: 58.3 | IMPLEMENTATION: 66.0 | RANK: 6

INNOVATION

KRYPTUS
shaping trusted bonds

INNOVATION
SCORE: 58.3

Kryptus is a Brazil-based startup focused on cryptographic solutions and services for enterprises. The firm scored 56.9 in the innovation category. The firm performed strongly on customer flexibility options, offering a broad choice in both on-premises appliances and their service offering, and, overall, the firm held its own in comparison to the leaders.

In terms of cloud service options, Kryptus offers BYOK capabilities and can assemble clusters between regions (e.g., Brazil and Europe). Further, the firm has the Kryptus Cloud HSM as a private cloud offering, with an existing footprint in Latin America and recent expansion into the Europe, the Middle East, and Africa (EMEA) region.

Kryptus has a good partner ecosystem for a firm of its size, boosted in large part by its strategic partnership with Swiss firm Kudelski Security since 2016, which is also what allowed the firm to expand into EMEA in 2020. It is also engaging in APAC expansion, so while Kryptus does not have the reach of the other vendors in this assessment, it is only at the very start of that process and there is significant opportunity ahead. Further, Kryptus offers close client support post-sales, including customization services to integrate the HSM in user's business environments.

In terms of new applications, the firm has ventured into the blockchain domain in cryptocurrency and in IoT use case deployment but not yet ventured into 5G. It is focused on PQC, with ongoing efforts in ensure its product offerings are crypto-agile.

Beyond that, Kryptus is the only vendor currently to offer embedded KMIP, which allows any application to use HSM functionalities without having to install drivers or libraries,; especially useful for solutions that operate in heterogeneous environments, such as web applications and IoT. The embedded KMIP combined with the virtual HSM and user systems allows the use of private keys without external intermediates (middleware). This makes Kryptus HSM very competitive offering as a cloud solution.

IMPLEMENTATION

KRYPTUS
shaping trusted bonds

IMPLEMENTATION
SCORE: 66.0

Kryptus scored 66.0 in the implementation category. Its flagship product is the kNET HSM, available in three performance models, as well as its KryptusCloud HSM. The appliance is only available as a network attached appliance (no PCIe variant on offer to date).

kNET HSM is by design a GP HSM, but leans towards a converged platform offering, whereby numerous payment functionalities have been implemented.

As such, Kryptus is able to offer most payment applications with its product. The only exceptions are EMV payment tokenization, mobile payment provisioning, and PIN digitization. Further it is PCI PIN, P2PE and PTS HSM v2 and v3 compliant, meaning it can easily satisfy payment requirements from most service providers.

With regards to other certifications, Kryptus is compliant with FIPS 140-2 Level 3 and is going through the process to obtain certification for CC EAL 4+ and QSCD for eIDAS, both important to succeed in the EU market. As an experienced and long-standing security focus working with the Brazilian government, Kryptus is fully compliant with national standards such as Brazil ITI: ICP-Brasil NSH3/NSC3 for Brazil's national PKI.

From a GP application perspective, Kryptus performs highly, offering almost all the same applications as the leaders. From a security algorithm perspective, Kryptus offers a good variety of the most used algorithms, only missing some niche-specific algorithms.

With regards to the architecture criteria, Kryptus scores well, and where it is lacking (notably in virtual environment capabilities), it is in the process of enabling integration. In terms of APIs, it has choice and range, and is currently the only HSM on the market that has KMIP natively within its HSMs.

CONCLUDING REMARKS

Kryptus scores an overall 62.3 in this competitive assessment, coming last but not least, in sixth place. Kryptus is no laggard in the global HSM market; on the contrary, the firm is an emergent startup that has successfully expanded beyond the confines of its domestic market to tackle the international arena. Breakouts like Kryptus in the HSM space are rare, and other similar national firms have not been as successful (e.g., Dinamo, Procenne, and Sansec, to name a few which were not included in this assessment). The firm is on track for a successful expansion, with a converged platform and cloud service that is competitively priced. This is of real interest to cost-sensitive regions (especially in Latin America and the Asia-Pacific), and Kryptus seems primed to deliver to those markets that are yet untapped in the HSM space.

ABI Research is a global technology intelligence firm delivering actionable research and strategic guidance to technology leaders, innovators, and decision makers around the world. Our research focuses on the transformative technologies that are dramatically reshaping industries, economies, and workforces today. ABI Research's global team of analysts publish groundbreaking studies often years ahead of other technology advisory firms, empowering our clients to stay ahead of their markets and their competitors.
+1.516.624.2500 in the Americas, +44.203.326.0140 in Europe, +65.6592.0290 in Asia-Pacific or visit www.abiresearch.com.