REPORT REPRINT

As HSM market heats up, authentication vendor Yubico joins the party

GARRETT BEKKER

21 NOV 2017

The authentication vendor has introduced its own line of hardware security modules that are intended to fill the white space in the market and deliver advanced features at a lower price point than traditional on-prem HSMs.

THIS REPORT, LICENSED TO YUBICO, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR RE-POSTED, IN WHOLE OR IN PART, BY THE RECIPIENT WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.

©2018 451 Research, LLC | WWW.451RESEARCH.COM

The sleepy hardware security module (HSM) space seems to be heating up a bit, likely driven by the endless tide of data breaches that have driven renewed interest in data encryption. AWS recently launched a homegrown version of its CloudHSM, and Gemalto SafeNet announced its own HSM-as-a-service play earlier this year. Germany-based Utimaco recently announced its entrance into the market for payments HSMs to compete with Gemalto SafeNet and Thales Vormetric.

Not to be left out, popular authentication vendor Yubico has introduced its own line of HSMs that are intended to fill the white space in the HSM market by delivering advanced features at a lower price point than traditional on-premises HSMs. Version two (YubiHSM 2), which Yubico bills as one of the 'world's smallest HSMs,' adds new crypto capabilities, role-based access controls (RBAC), remote management capabilities and tamper-evident logging.

THE 451 TAKE

The HSM market might not be the first thing that comes to mind when considering logical adjacencies for Yubico's multi-factor authentication offerings. However, viewed through the lens of the stolen credential epidemic, the logic of combining the two comes into focus. Yubico can now offer customers the ability to protect credentials at the front end, as well as the back-end servers that may not directly interact with users but still need key protection. Yubico is seeking white space in the market with a 'reasonably priced' option that targets customers that may have the need for a hardware-based security module but don't need all the bells and whistles – and deployment challenges – of full-featured network HSMs. YubiHSM 2 does not currently have FIPS certification; Yubico is betting there will be ample opportunity among customers that don't need FIPS certification, although it will monitor the market as it evolves.

CONTEXT

Yubico was founded in 2007 in Stockholm by the husband and wife combo of Jakob (CTO) and Stina (CEO) Ehrensvard, who subsequently relocated to Palo Alto, California, to be closer to target customers – cloud behemoths with millions of external users. Yubico currently employs just over 100, up from 25 when we last wrote about the company, with new offices in Germany, Japan, Singapore and Australia complementing existing locations in Palo Alto, Stockholm and London. Yubico was initially bootstrapped, and after raising nearly $5m from angel investors, recently raised $30m in a round led by Andreessen Horowitz and New Enterprise Associates to help fund its expansion beyond authentication.

PRODUCTS

Yubico offers a range of USB keys for multi-factor authentication, including the YubiKey 4 Series, the YubiKey NEO and a YubiKey U2F Security Key, all of which support the U2F standard from the FIDO Alliance. The YubiKey 4 Series includes USB key form factors for both standard USB-A and USB-C ports (currently used in some Android devices and newer laptops), as well as the YubiKey 4 Nano, which fits entirely within a USB-A or USB-C port. The NEO line supports both USB and contactless (NFC, MIFARE) connections and, along with the YubiKey 4 series, supports both one-time passwords (OTPs) and smart-card-based PKI authentication.

Since YubiKeys are hardware-based, they offer higher levels of security than software-based authenticators, and eliminate the need for users to type in passwords, PIN codes or OTPs for authentication. To log in, users type their standard username and password, insert their YubiKey, and touch or tap the USB device to be authenticated.

Simply put, HSMs are hardware devices that can store and manage encryption keys in a separate physical device from the underlying computer, and can handle complex tasks like key rotation and key backup. Applications of HSMs include authentication, code signing, document signing, data encryption, PKI, time stamping and random number generation.

YubiHSM is the same form factor as the YubiKey Nano; it can fit completely within a USB-A port on a server and has very low power consumption. Version 1 was essentially a way of storing symmetric secrets in hardware, particularly OTP codes, and was limited to symmetric key operations. YubiHSM 2 is a full-fledged HSM, and adds new asymmetric crypto capabilities, RBAC, remote management and tamper-evident logging.

YubiHSM 2 has a variety of out-of-the-box integrations with most operating systems, and has a variety of tools to make it easier for admins to install on a server or device. YubiHSM 2 is not yet FIPS-compliant, although we expect that Yubico may introduce a FIPS-compliant version for customers in regulated environments. For centralized management, Yubico offers standard interfaces that support PKCS #11 and KSP, and can plug into existing management solutions.

STRATEGY

Yubico has identified a notable price/performance gap in the HSM market between low-end smart-card-based HSMs and high-end network HSMs, with an HSM that delivers roughly 80% of the functionality of traditional HSMs at a fraction of the cost and implementation effort. Pricing for YubiHSM2 will start at about $650 – well below other USB HSMs in the $5,000-8,000 range and network HSMs that typically start at $10,000.

Much of the HSM market has historically been driven by the need to maintain FIPS compliance for highly regulated environments. Yubico's ultimate goal is to address the epidemic of credential theft by replacing software keys with hardware-backed keys wherever possible, including servers, manufacturing and IoT, gateways, routers, and industrial systems that don't require FIPS compliance and for which it would be prohibitively expensive to protect with a $10,000 HSM.

COMPETITION

Unlike most overcrowded sectors of cybersecurity, there are a small number of HSM vendors. The HSM market can be divided into two general segments: general-purpose HSMs and HSMs for payment processing (e-payments, card issuance, interbank clearance, etc.) – both categories are dominated by encryption giants Thales Vormetric and Gemalto.

Gemalto introduced an HSM-as-a-service offering at the RSA Security conference in early 2017. Thales does not currently have an HSM-as-a-service offering, but does offer its HSM as an OEM for cloud providers. Thales also has a key-management-as-a-service offering, as well as the nShield Web Services Crypto API, which enables customer applications that reside in traditional datacenters or the cloud to push commands to their on-premises nShield HSMs via web service calls, without integrating their applications directly with nShield.

As more IT workloads shift to the cloud, AWS has the potential to be a dominant presence in HSMs. AWS has long offered its own CloudHSM service (which was initially based on an OEM relationship with Gemalto SafeNet for the latter's Luna HSM), and launched its own key management service at Amazon re:Invent a few years ago. AWS's most recent iteration is a homegrown version of CloudHSM that is essentially a partition of an HSM and offers an elastic cloud-based pricing model. Microsoft provides an HSM for Azure (KeyVault) based on an OEM relationship with Thales, and we expect Google to introduce an HSM option for Google Cloud Platform or G-Suite customers. SaaS provider Box also has a variety of key management options available to customers.

Micro Focus (via the HPE purchase) and IBM also have an HSM presence, with IBM mainly focused on embedding its HSMs into its own products. Micro Focus has taken a similar strategy with its Atalla line, but with arguably less market presence in general-purpose HSMs. Atalla is a notable force in the market for payments HSMs, as is US-based Futurex.

After its acquisition and subsequent spinoff by Sophos, Germany-based Utimaco has reemerged as an independent entity with a singular focus on HSMs. Its latest update is a PCI-certified HSM that is intended to give Thales Vormetric and Gemalto SafeNet a run for their money in the payments HSM segment.

Other HSM vendors include the likes of Atos SE, AEP, Townsend Security and San Jose-based SPYRUS, as well as recent entrant Cavium. UK-based AEP Networks was acquired in 2011 by Ultra Electronics Holdings, and by most accounts has a diminished presence in the HSM market. Atos has its own HSM, but also OEMs Utimaco's HSM for certain use cases. Other software-based key management vendors include PKWARE, Porticor (acquired by Intuit) and Venafi.

SWOT ANALYSIS

STRENGTHS

Yubico offers a small, lightweight form factor that is considerably less expensive than most USB or network HSMs, and requires less management overhead to install and maintain.

WEAKNESSES

YubiHSM 2 is not currently FIPS-compliant, although we anticipate a FIPS version will be introduced in 2018.

OPPORTUNITIES

There are millions of servers currently using software-based keys, many of which do not justify the cost of a full traditional HSM.

THREATS

Some larger HSM and cloud vendors have introduced HSM and key-management-as-a-service offerings that could siphon some of the demand for a low-cost, self-managed HSM, and we expect more service-based offerings to come.