Yubico Expands FIPS 140-2 Product Line with YubiHSM 2 FIPS, the World's Smallest FIPS Validated Hardware Security Module

Complementary to the company's new YubiKey 5 FIPS Series, YubiHSM 2 FIPS enables highly-regulated organisations to achieve a holistic security posture

Yubico, the leading provider of hardware authentication security keys, today announced its latest FIPS 140-2 product offering, and the first of its kind for the company: YubiHSM 2 FIPS. Today's news comes alongside the YubiKey 5 FIPS Series launch, the company's most recent security key line to receive FIPS 140-2 validation.

The YubiHSM 2 launched in 2017, but this marks the first FIPS-validated version of the product. The YubiHSM 2 FIPS is certified at FIPS 140-2, Level 3. With the added availability of YubiHSM 2 FIPS, organisations in highly-regulated industries such as government, financial services, healthcare, and energy now have the opportunity to reap the same security benefits that many other YubiHSM users have. This includes advanced protection for certificate authority (CA) keys, database master keys, code signing, authentication/access tokens, manufacturing processes and component authenticity checks, IoT gateways or proxies, file encryption, cryptocurrency exchanges, and more.

"The YubiHSM 2 FIPS is an exciting addition to our recently updated FIPS-validated product line," said Suresh Thiru, Chief Product Officer, Yubico. "Our high-risk customers are now equipped with a full product suite that helps them not only achieve and maintain compliance, but also advance their security posture across the entire organisation. From protecting servers to users, regardless of their location, Yubico is the partner who strives to do it all."

Primary benefits of the YubiHSM 2 FIPS include:

Secure hardware protection for cryptographic keys — The YubiHSM 2 FIPS enables secure key storage and operations on tamper-resistant hardware, with audit logging. This prevents accidental copying and distribution of keys, and remote theft of cryptographic software keys. Extensive cryptographic capabilities include: hashing, key wrapping, asymmetric signing, decryption, attestation and more.

Innovative design for flexible use and simple deployment — Traditional rack-mounted and card-based HSMs are not practical for many organisations due to their size and deployment complexity. The YubiHSM 2 FIPS offers a portable 'nano' form factor that allows fast and flexible deployment across diverse environments. It fits easily into a USB-A slot, lying almost flush to remain concealed.

Low-cost, high security ROI — The YubiHSM 2 FIPS delivers government-grade high cryptographic security and operations at a price point that is up to 90% cheaper than traditional HSMs. Additionally, low-power usage reduces business energy consumption.

Along with the rest of Yubico's FIPS product lineup, YubiHSM 2 FIPS is manufactured using stringent processes and a secure supply chain for trustworthy components, ensuring strong security and regulatory compliance for the most security-conscious organisations.

For more information on YubiHSM 2 FIPS, please visit the Yubico website. It is also available for purchase on the Yubico store, through Yubico's dedicated sales team, or from any Yubico-approved channel partners and resellers.

Contacts

Louise Roberts and Sonia Morris - Sphere Public Relations
0405 579633 / 0421 672 162
mailto: yubico@spherepr.com.au