

August 6, 2024



Microsoft Integrates Marvell NIST FIPS 140-3 Level-3 Compliant LiquidSecurity HSMs into Azure Key Vault and Managed HSM Services

SANTA CLARA, Calif., Aug. 6, 2024 /PRNewswire/ -- [Marvell Technology, Inc.](#) (NASDAQ: MRVL), a leader in data infrastructure semiconductor solutions, today announced that Microsoft—which extensively uses the Marvell® LiquidSecurity® family of HSMs to perform encryption, key management, and other security functions within Azure—will update its fleet of LiquidSecurity HSMs to the FIPS 140-3, Level-3 standard to further enhance its internal security posture and the portfolio of security services offered to its customers.

Marvell LiquidSecurity 1 and LiquidSecurity 2 hardware security modules (HSMs) achieved FIPS 140-3 Level-3 certification from the National Institute of Standards and Technology (NIST) in June. Stringent FIPS 140-3 certification is required by many financial institutions and government organizations and, to date, has largely been available only with traditional HSMs for on-premise use.

"We congratulate Marvell on achieving NIST FIPS 140-3, Level-3 certification of its LiquidSecurity HSMs which power our Azure Key Vault and Azure Key Vault Managed HSM services, and on which we continue to innovate new offerings," said Soumya Subramanian, VP of Cloud Security Engineering at Microsoft Azure. "Through our collaboration with Marvell, we are able to offer Azure's customers the most secure and compliant key management services available in Public, Sovereign or Government clouds today."

FIPS 140 (Federal Information Processing Standard) is a set of security requirements established by NIST (National Institute of Standards and Technology) and managed by both the United States and Canada as part of the CMVP (Cryptographic Module Validation Program). They specify the security requirements that will be satisfied by a cryptographic module, providing four increasingly stringent levels intended to cover a wide range of potential applications and environments. Many government organizations and financial institutions are mandated to use NIST FIPS-certified HSMs for encryption and key management. Because of the rigorous testing required to meet this certification, the use of HSMs has grown across all markets and use cases have proliferated.

FIPS 140-3 introduces several new security enhancements over FIPS 140-2. This new NIST FIPS 140-3 certification will eventually replace FIPS 140-2 certification as the latter will be moved to Historical List by September 21, 2026.

Transforming Encryption Through Optimized Processors

LiquidSecurity devices were created to eliminate the friction associated with achieving better security. A critical element of global commerce, HSMs perform the authentication and

encryption processes behind secure key protection and management, credit card purchases, ATM withdrawals, sign-in services and other high-volume transactions. HSMs have historically been packaged as 1U and 2U server appliances running standard microprocessors. These appliances are managed directly by HSM users and deployed on their premises.

LiquidSecurity HSMs, by contrast, are PCIe-based devices powered by OCTEON® DPUs and designed for use in dense multi-tenant cloud environments. Six of the ten largest cloud service providers use LiquidSecurity in their operations. A single LiquidSecurity2 card can manage 100,000 pairs of encryption keys and process more than one million operations per second. As a result, cloud service providers can deliver HSM services while consuming a fraction of the power, rack space and hardware required by traditional HSMs. Meanwhile, HSM users can switch from the complexity of managing hardware to the ease of subscribing to HSM services. The cloud-based model for HSMs also reduces barriers to employing HSM and encryption services for secure medical records and other transactions.

Revenue from cloud-based HSMs is expected to grow from under 15% today to over 40% by 2028, according to ABI Research.

"Marvell is uniquely positioned to take advantage of cloud-based HSM demand in the market, and remains an industry leader in the space," said Michela Menting, senior analyst at ABI Research. "FIPS 140-3 represents the latest milestone toward a more diverse and larger market for HSM services."

"Marvell has been leading the effort to transform HSMs into cloud-based devices since 2015," said Will Chu, senior vice president and general manager of Custom Compute and Storage at Marvell. "Microsoft has shared in this vision of modernizing the HSM market and we are thrilled to continue working side by side with Microsoft to help Azure customers benefit from the latest security standards for the most demanding applications deployed at cloud scale."

About Marvell

To deliver the data infrastructure technology that connects the world, we're building solutions on the most powerful foundation: our partnerships with our customers. Trusted by the world's leading technology companies for over 25 years, we move, store, process and secure the world's data with semiconductor solutions designed for our customers' current needs and future ambitions. Through a process of deep collaboration and transparency, we're ultimately changing the way tomorrow's enterprise, cloud, automotive, and carrier architectures transform—for the better.

Marvell and the M logo are trademarks of Marvell or its affiliates. Please visit www.marvell.com for a complete list of Marvell trademarks. Other names and brands may be claimed as the property of others.

This press release contains forward-looking statements within the meaning of the federal securities laws that involve risks and uncertainties. Forward-looking statements include, without limitation, any statement that may predict, forecast, indicate or imply future events, results or achievements. Actual events, results or achievements may differ materially from those contemplated in this press release. Forward-looking statements are only predictions and are subject to risks, uncertainties and assumptions that are difficult to predict, including those described in the "Risk Factors" section of our Annual Reports on Form 10-K, Quarterly

Reports on Form 10-Q and other documents filed by us from time to time with the SEC. Forward-looking statements speak only as of the date they are made. Readers are cautioned not to put undue reliance on forward-looking statements, and no person assumes any obligation to update or revise any such forward-looking statements, whether as a result of new information, future events or otherwise.

For further information, contact:

Kim Markle

pr@marvell.com



View original content to download multimedia:<https://www.prnewswire.com/news-releases/microsoft-integrates-marvell-nist-fips-140-3-level-3-compliant-liquidsecurity-hsms-into-azure-key-vault-and-managed-hsm-services-302215209.html>

SOURCE Marvell