

December 1, 2025



Marvell Extends Collaboration with Microsoft, Expanding Azure Global Cloud Security Services in Europe

Expands Use Cases for Marvell-powered, Cloud-based Security Services in the Region, Adding to Existing Offerings in Asia and North America

SANTA CLARA, Calif.--(BUSINESS WIRE)-- [Marvell Technology, Inc.](#) (NASDAQ: MRVL), a leader in data infrastructure semiconductor solutions, today announced that Microsoft expanded the use cases for its cloud-based security offerings powered by Marvell® LiquidSecurity® hardware security modules (HSMs) for customers in Europe, adding to existing cloud-based security offerings in Asia and North America. The announcement follows two new European certifications awarded to Marvell for LiquidSecurity earlier this year.

With LiquidSecurity, Microsoft Azure can deliver cloud-based services for certifying cross-border contracts, verifying identification documents and handling other transactions—reducing time, cost and operational overhead across a wide range of use cases.

“We congratulate Marvell on achieving eIDAS and CC EAL4+ certification of its LiquidSecurity HSMs, which power our Azure Key Vault, Azure Key Vault Managed HSM and Cloud HSM services,” said Soumya Subramanian, vice president of Cloud Security Engineering at Microsoft Azure. “Through our collaboration with Marvell, we are able to offer Azure’s customers working in the electronic identity and passport space the most secure and compliant key management services available in public, sovereign or government clouds today.”

“Marvell has been the pioneer in cloud-based HSMs and remains the industry leader,” said Michela Menting, senior research director at ABI Research. “Common Criteria EAL4+ and eIDAS certifications represent the latest steps by Marvell in forging a more diverse and larger market for HSM services.”

“It’s been a tremendous experience to work with Microsoft, which shares our vision of improving security through custom silicon and cloud technologies,” said Will Chu, executive vice president and general manager of Custom Cloud Solutions at Marvell. “We look forward to further exploring how cloud-based security can transform our daily activities.”

Marvell obtained certifications for LiquidSecurity under eIDAS (electronic IDentification, Authentication and trust Services) and Common Criteria EAL4+, two security frameworks aimed at improving online trust and security. Established by the European Parliament and the Council of the European Union, eIDAS outlines the requirements for replacing traditional contract mechanisms with digital authentication systems between or with participating EU countries. Common Criteria EAL4+ unifies the three major international security evaluation standards.

Iron-clad Security, Lower Power and Less Hardware

A critical element of global commerce, HSMs perform the authentication and encryption processes behind secure key protection and management for data at rest and in motion, public key infrastructure (PKI), 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. Marvell LiquidSecurity HSMs, by contrast, are PCIe-based devices powered by Marvell OCTEON® DPUs and designed for use in dense, multi-tenant cloud environments.

A single LiquidSecurity 2 HSM adapter can manage up to 1 million encryption keys and process more than 1 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. In addition, 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.

Marvell LiquidSecurity HSMs can also be uniquely customized to meet the performance, power, space and software requirements of individual customers.

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 30 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 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.

View source version on businesswire.com:

<https://www.businesswire.com/news/home/20251201423905/en/>

Media Contact:
George Millington
pr@marvell.com

Source: Marvell Technology, Inc.