S1 EP22 – Building HSM-as-a-Service with LiquidSecurity 2

Wednesday, September 14, 2022 · 8:41

Amer Haider, VP of Marvell's Security Solutions Business Unit, and podcast host Chris Banuelos, cover the launch of Marvell's enhanced Hardware Security Module – LiquidSecurity 2, the industry's most advanced solution for performing key management, encryption, and authentication in the cloud for payment, privacy compliance, and other HSM services - powered by the company's OCTEON® family of products. Join us and take a deep dive into the critical role HSMs play in virtually all credit card-based transactions, end markets, and where LS2 will have the largest impact, plus much more. Read the press release: https://bit.ly/3eOd9My

Speakers
Amer Haider
VP Product Management
Security Solutions Business Unit

Host
Christopher Banuelos
Senior Manager of
Global Social Media Marketing

C **Christopher Banuelos 00:04**
Welcome to the Marvell Essential Technology Podcast. I'm your host Chris Banuelos. On today's episode listen into a conversation between me and Amer Haider, vice president of product management, the security solutions business unit, where we discuss Marvell's LiquidSecurity 2 HSM solutions. To stay up to date on future episodes, please be sure to subscribe to the Marvell Essential Technology Podcast. Hey Amer, it's great to have you on today's episode. Wanted to just jump back briefly before we get into our discussion questions. We actually spoke back in July on Episode 18, Securing Private Keys in the Public Cloud. We talked about industry trends related to hardware security modules, as well as how Marvell is shaping the industry when it comes to trends and data privacy and trust. Today, I'm super excited to continue our conversation and focus on the recent launch your team just completed. Can you tell me about that?

A **Amer Haider 01:07**
Hi Chris, really excited to be on today's podcast. We are very happy to announce our brand new LiquidSecurity product family called LiquidSecurity 2 (LS2). This is big news because our last family was announced over four years ago. With the new liquid security family. We set a brand new bar for performance per dollar, performance per watt, and performance density. So what's new with LS2 is we've improved our asymmetric encryption by over 10x. For elliptical curve cryptography, and our bulk encryption is improved over 3x compared to LS1 for AES GCM. We offer 45 partitions, and OS storage of 10x over our LS1 family for over a million cryptographic keys stored in the HSM. So Chris, as you can tell, this is pretty big news for us and the industry.

C **Christopher Banuelos 02:24**
I completely agree, this is huge news for not only you but the industry, what end markets will LiquidSecurity 2 impact and how will this help customers?

A **Amer Haider 02:34**
You know, there's a big trend going on in the HSM market right now, Chris. Well previously, HSM 's were only available on-prem and you had to install and implement and deploy them inside your network. Now, any application developer or enterprise can use HSMs in the cloud. So this cloud transition is is a huge deal for HSM and we are the number one vendor in that space. Hyperscalers use our Liquidsecurity 1 today to build and offer their HSM as a service. With LiquidSecurity 2 we're going to enable our hyperscaler partners and customers to extend and improve their HSM as a service offering for their end customers. We see this is going to expand the total market significantly. Because now application developers either doing enterprise internal applications or building SaaS applications can protect their encryption keys in hardware by just making a couple of API calls. And with the reduction of the costs associated with using HSM or protecting and encryption keys going down significantly, which is our prediction. We'll see more and more use of HSMs for protecting applications. And these are not just applications that are in the cloud, we see users and application developers using HSM in the cloud for their private clouds applications, their public cloud applications and their hybrid cloud applications.

C **Christopher Banuelos 04:18**
So you talk about expanding the market and securing more applications using HSM. Can you tell me more about that?

A **Amer Haider 04:26**
Absolutely. Using HSMs to improve application security can be described by an analogy. Imagine us writing our passwords on a Post-it and putting it on our computer. Right our computer has the password. But if the password or in the case of an HSM, the encryption key is right there in front of you or is easily accessible. The benefit of that password on your computer isn't much. Now what some people do is take that post-it and maybe even put it inside a notebook, but the notebook is still sitting next to your computer. So it is relatively possible, it is easy and maybe possible for someone to get access to that password. Now in the HSM world, or with application security, what many folks will do is take their encryption keys and store them in a database, or somewhere in software. And this leaves a vulnerability, or exposure for losing those keys. And an HSM, those encryption keys are stored inside hardware. So the analogy would be is instead of having the sticky note on in a notebook that's next to your computer, you take that sticky note and put it in a safe. Now that creates an overhead because every time you have to essentially go to your safe punch in the PIN code, and then take the password out and then put it back in. And so that's why HSMs were not widely used to be honest. But now with an HSM as a service offered by the hyperscalers. Any application provider can store their encryption keys for just about $2 an hour in hardware by just making a couple of API calls. So we see this as a great opportunity for expanding application security in the cloud that basically makes our world a safer place.

C **Christopher Banuelos 06:32**
You talked about expansion in the public, private and hybrid environments. And in our last podcast, you shared a very interesting story about the seat belt. Can you provide some background and share the market trends that will drive encryption?

A **Amer Haider 06:48**
Yes, absolutely. Thanks for for mentioning that. Let me give our listeners here a little bit of background on that seatbelt reference you made. So till 1968, seatbelts were a great idea. They still are. But no, they're seldom used because the government didn't mandate them. And while there's a good idea, you could see movies or films or documentaries from that time. And you know, there's kids sitting in the front seat without a seatbelt right. Now, similarly, while storing encryption keys is a great idea and hardware, not everyone does it. One is of course convenience, but it's not mandated. So not everyone is doing it except for some regulated industries like payments and banking. What we see is with privacy, the requirement for storing consumers data encrypted, and in some ways even authenticated using the consumers consent or consumers control over their encryption keys is driving the need for additional security and encryption inside the enterprise. And this will drive the need for protecting encryption keys, and even consumer encryption keys. So the answer is yes, we see significant market trends towards regulation for consumer privacy that will drive encryption and protecting consumer owned encryption keys in the future.

C **Christopher Banuelos 08:27**
Thank you for listening to the Marvell Essential Technology Podcast. As always, please feel free to visit our website to learn more, and we'll see you on the next episode.

Building HSM-as-a-Service with LiquidSecurity 2 - S1 EP22   09/22