LiquidSecurity® 2

Hardware Security Modules for a Secure, Cloud-Based World

Amer Haider

Vice President, Security, Marvell

Sept 2022 *(Embargoed until Sept 14, 2022 6AM EST)*

MARVELL™

Overview

Company founded **1995**	FY22 revenue **$4.46B**
Employees **7,200+**	Patents worldwide **10,000+**

Global fabless semiconductor supplier

MARVELL

Nasdaq-100

Market-Leading Cloud-Optimized Silicon

Storage
#1 in HDD, SSD and
Fibre Channel controllers

Processors
#1 in 4G/5G baseband and
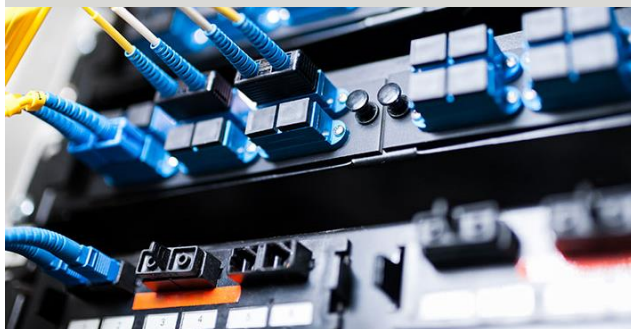data processor units (DPUs)

Electro-optics
#1 in PAM4 DSPs, linear TIAs, drivers
and coherent DSPs

Networking
#2 in Ethernet switches, copper PHYs
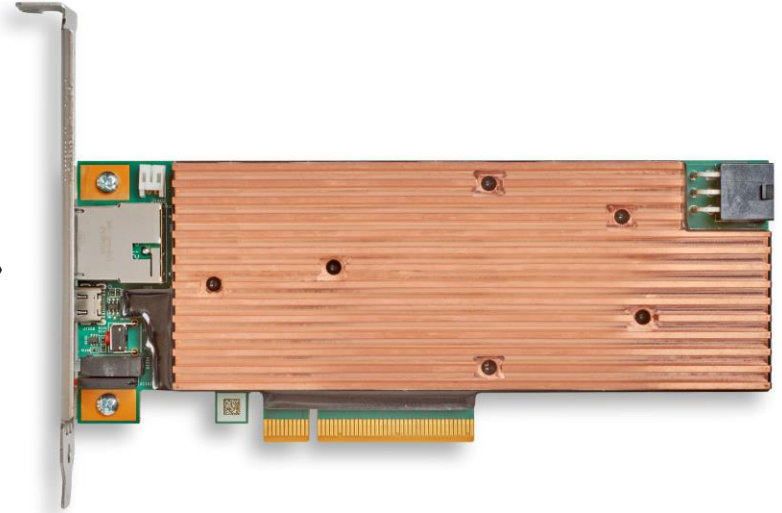and Automotive Ethernet

Security
#1 in processors and cloud hardware
security modules (HSM)

Announcing LiquidSecurity 2

Most advanced unified architecture to meet your security and compliance needs

The world will be a safer place if every encryption key is protected in hardware

Privacy, security, and compliance risks

- GDPR, HIPAA, CPRA and other regulations impose penalties for inadvertent data disclosure.

- All businesses handling user data are now moving to encrypt *all* their user data at rest.

- The average cost of a breach in 2022 is $4.35 million with many cases far higher[1].

1. IBM

The New York Times

T-Mobile Reaches $500 Million Settlement in Huge 2021 Data Breach

The company, which said the hacking had affected 76.6 million people, agreed to pay $350 million to settle claims and spend $150 million to bolster security.

CYBERSECURITY NEWS

Florida Orthopaedic Institute Reaches $4M Settlement Over Data Breach

A 2020 data breach at Florida Orthopaedic Institute impacted 640,000 individuals and resulted in data being encrypted.
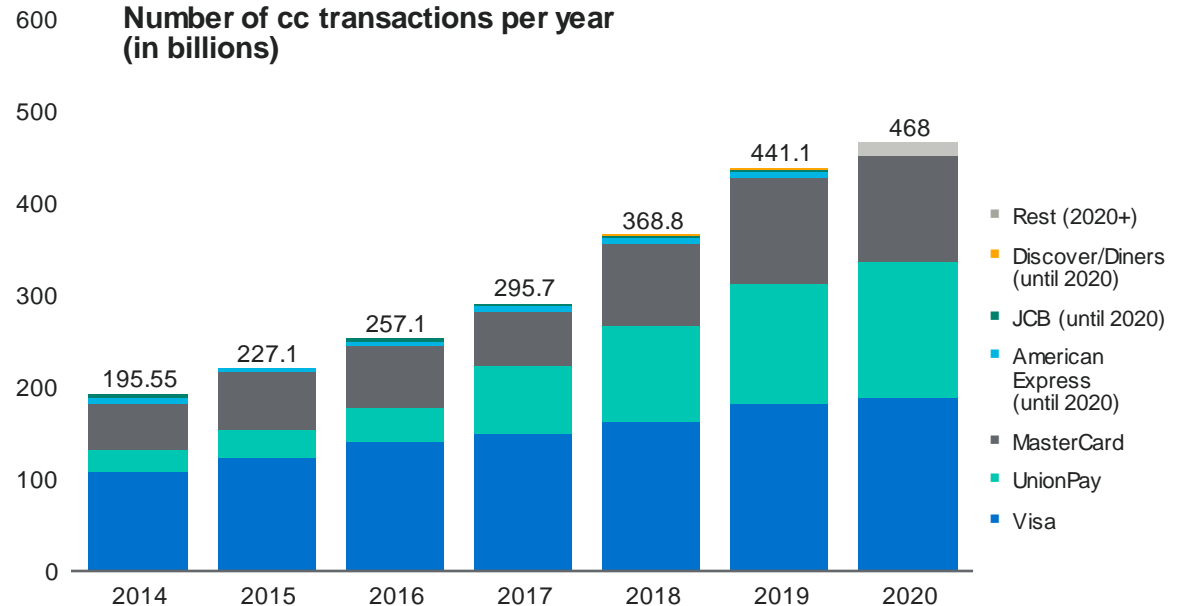
CNET Your guide to a better future

Money

Capital One $190 Million Data Breach Settlement: Are You Eligible for a Payment?

Affected customers could collect up to $25,000, according to a preliminary settlement.
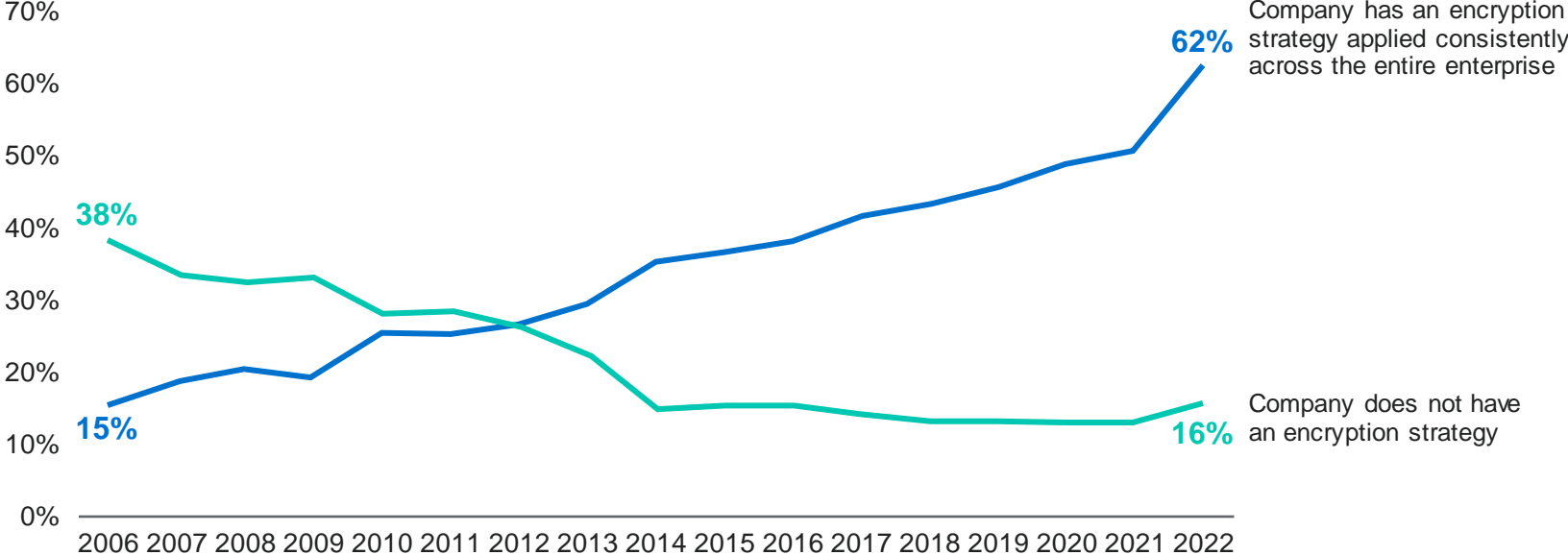
Encryption is at the heart of global commerce

- Over 1 billion credit card transactions per day[1].

- 2.8 billion credit cards in use (and that's credit only)[2].

- Total debit / credit purchases to rise from $8 trillion to $12.9 trillion by 2025 in U.S. alone.[3]

Number of cc transactions per year (in billions)

Chart data — Number of cc transactions per year (in billions):
- 2014: 195.55
- 2015: 227.1
- 2016: 257.1
- 2017: 295.7
- 2018: 368.8
- 2019: 441.1
- 2020: 468

Legend:
- Rest (2020+)
- Discover/Diners (until 2020)
- JCB (until 2020)
- American Express (until 2020)
- MasterCard
- UnionPay
- Visa

1.Statista 2. Shift Processing 3. Motley Fool

Encryption also gaining enterprise momentum

**Trends in encryption strategy.
Country samples are consolidated.**

Company has an encryption strategy applied consistently across the entire enterprise

62%

38%

15%

Company does not have an encryption strategy

16%

2022 Global Encryption Trends

7

What is an **HSM**?

- **Hardware security modules (HSMs)** are specialized devices for key management, encryption and authorization.

- Private keys are stored and operated in tamper-resistant FIPS certified hardware

- Certification of FIPS-140 standard managed by NIST.

- **The problem?** Traditional HSM costs tens of thousands of dollars, deployed mostly on-prem, and require handling and care.[1]
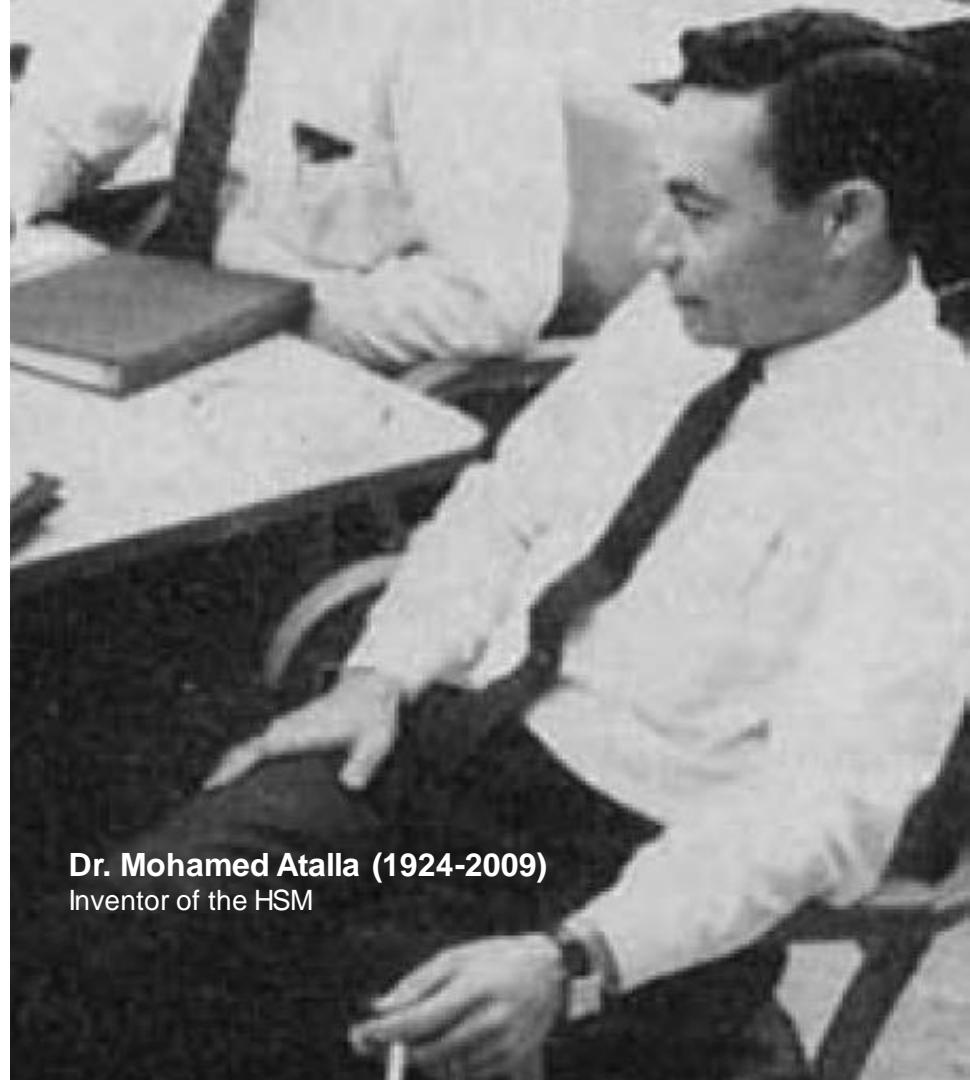
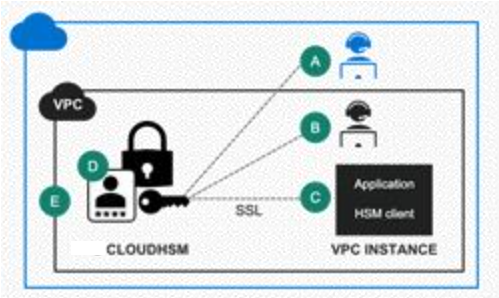**Dr. Mohamed Atalla (1924-2009)**
Inventor of the HSM

1. ABI Research

Cloudification expands users and use cases
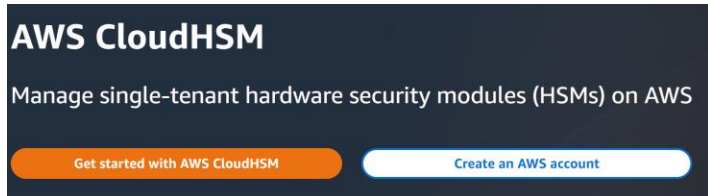
On-Prem appliances	Public Clouds and SaaS	Hybrid Clouds

Broad adoption underway

https://docs.aws.amazon.com/cloudhsm/latest/userguide/cloudhsm-user-guide.pdf

What is Azure Key Vault Managed HSM?

https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

https://www.oracle.com/security/cloud-security/key-management

https://www.alibabacloud.com/product/cloudhsm

LiquidSecurity 1

HSM on PCIe adapters

- Transformed the category in 2015 with optimized processing.
- 100,000 keys, 32 partitions.
- Best performance per dollar and per watt.
- Public cloud, private cloud, or enterprise.
- Technology managed by CSP; access policies managed by customer.

Customers
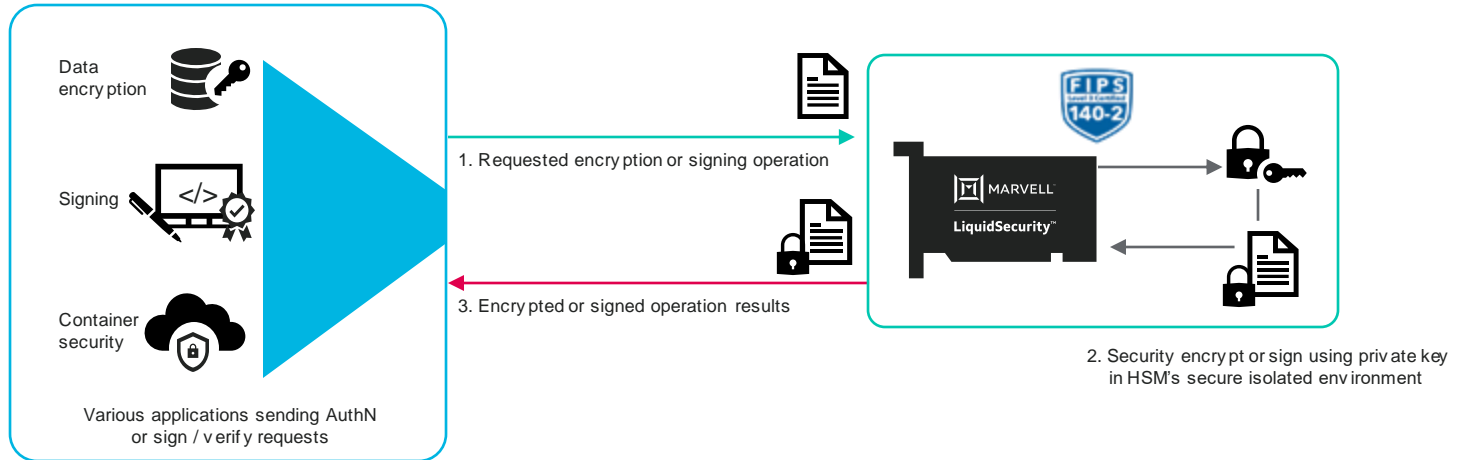
6 of 10 largest CSPs

Top five social media; Top-ranked SaaS provider

Leading OEMs and ISVs

Protecting encryption keys as a service

- Pay-as-you-go or embedded into SaaS services
- Developers can start using HSMs within minutes to hours and scale quickly
- Available now through hyperscaler CSPs

Data encryption

Signing

Container security

Various applications sending AuthN or sign / verify requests

1. Requested encryption or signing operation

3. Encrypted or signed operation results

2. Security encrypt or sign using private key in HSM's secure isolated environment

FIPS 140-2

MARVELL
LiquidSecurity™

Securing consumer data on mobile

- Today, apps and smartphones rely on cloud storage for back-ups

- Marvell's **LiquidSecurity HSM** secures the encryption operation and stores encryption keys in FIPS boundary

- Data easily restored or moved to another device.
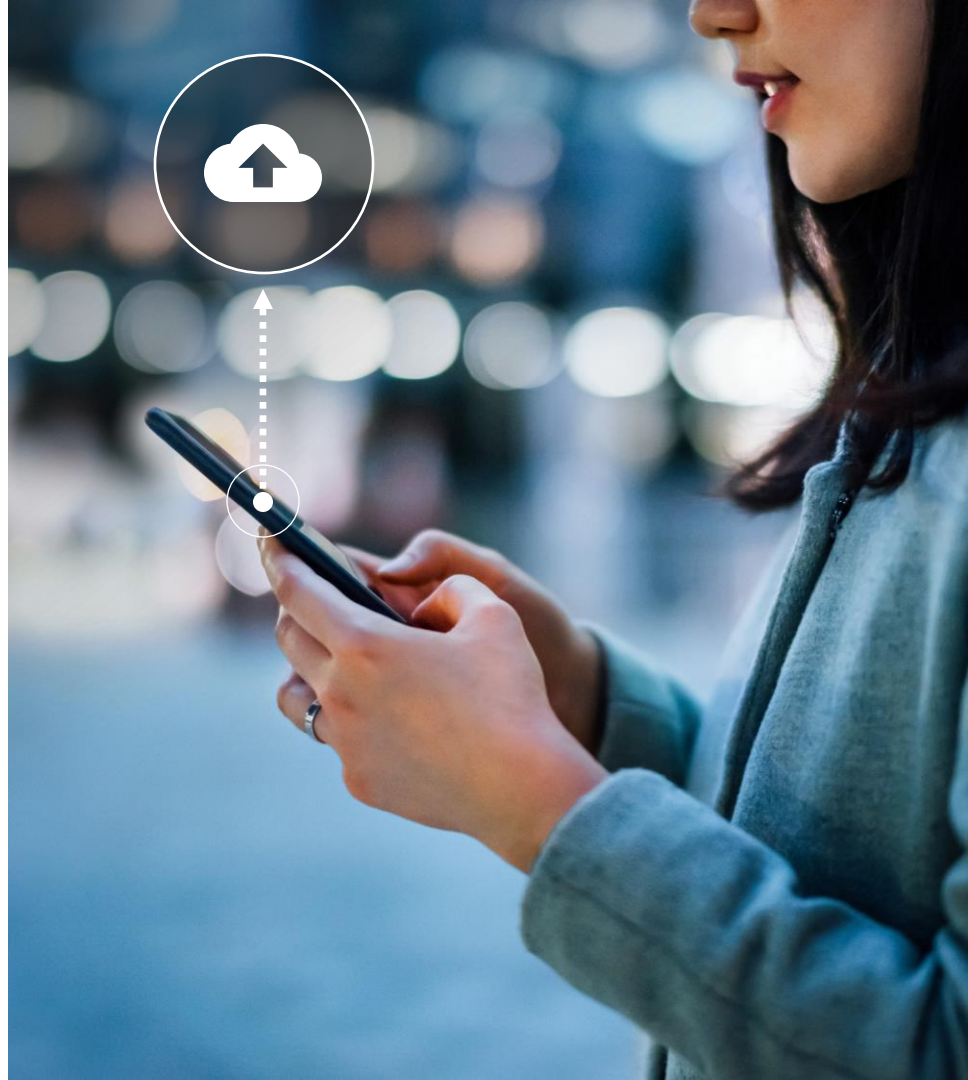
Introducing LS2 Cloud HSM

- **Outstanding performance and TCO:** up to 100,000 ECC operations per second (10x) for secure key management processing.

- **Scalable:** up to 1 million keys and 45 partitions for scaling multi-tenant operations.

- **Comprehensive SDK**, Source code and examples for flexibility and rapid deployment.

- **Flexibility: Multiple models, form factors and capabilities** to meet a full range of customers, applications and markets.

- **Extensive compliance:** FIPS 140-3, CC, eIDAS, PCI PTS HSM 4.0*

Most advanced, unified, compliant, comprehensive, low TCO

LS2 Highlights

Capability	LS1	LS2	Benefits
# Partitions	32	**45**	Scale multitenant deployments with tenant isolation
Key storage	100,000	**1,000,000**	10x Key Store (80% AES, 20% RSA or ECC Keys)
RSA-2K ops/s	35,000	**42,000**	20% more
ECC P-256 ops/s	10,000	**100,000**	12x Most ECC performance yet, designed for ECC
AES GCM ops/s	300,000	**1,000,000**	3.3x better performance
Secure machine	Limited Function	**Scalable**	LS2 arch. SM w/ multiple dedicated cores, run custom code; LS1 CPU limited
Payment HSM	Complete SW, PCI PIN Compliant	**PCI PTS HSM 4.0**	LS2 will be PCI PTS HSM 4.0 certified
Power	25-35W	**35-50 W**	Better Cap-Ex and Op-Ex w/ unified GP + Payments per watt
Form factor	LP PCIe Gen3x8	**LP PCIe Gen4x8**	HHHL, Seamless upgrade for standard servers

Cloud HSM to rise from 18% to >50% in five years

Revenue (millions)

	2022	2027

■ Cloud and Hybrid Cloud   ■ Non-Cloud Architecture
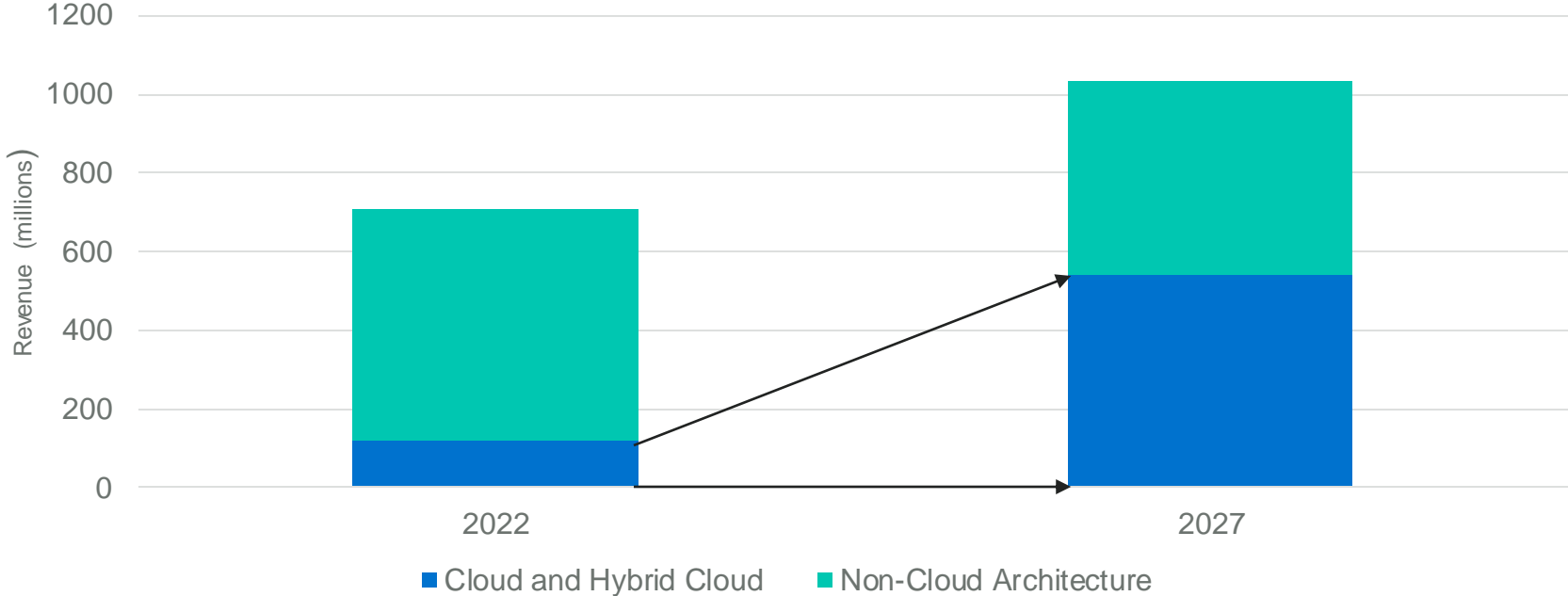
Marvell estimates based on market reports
and industry experts

Summary

| 1 | Marvell cloud-optimized silicon drives best-in-class performance, scalability and cost |

| 2 | Demand for cryptography HSM services are growing world-wide |

| 3 | Transitioning to the cloud greatly expands the users and use cases for HSM services |

| 4 | Unique advantages of LiquidSecurity 2 HSM makes the world a more secure place |