X-PHY®

Building a Community Based Root of Trust with Hardware Driven Memory Security

From Passive Storage to Proactive Defense

Jaime Coreano
Vice President of Sales, USA

FMS
the **Future** *of* **Memory** *and* **Storage**

The Problem – Software Trust is Fragile

Software Security Vulnerability

Software defenses (passwords, MFA, IAM) are easily bypassable.

Unverified Runtime Behavior

TPM/Secure Boot only protects at startup — runtime behavior is unverified.

Hackers Target Storage

Storage is treated as a passive resource, making it the prime target for attackers.

Static Trust

Breaches propagate because compromised endpoints remain trusted.

Takeaway: Traditional cybersecurity solutions are insufficient for today's threat landscape.

What could be the fix: A hardware-rooted identity system built into every SSD, functioning like a USB security key but managed securely via the portal.

Rethinking Security from the Ground Up

Traditional Trust Models

Traditional trust models rely on static credentials. Once access is granted, trust is assumed

X-PHY's Approach

In contrast, X-PHY embeds continuous verification in M.2 SSD firmware, rechecking trust at every access.

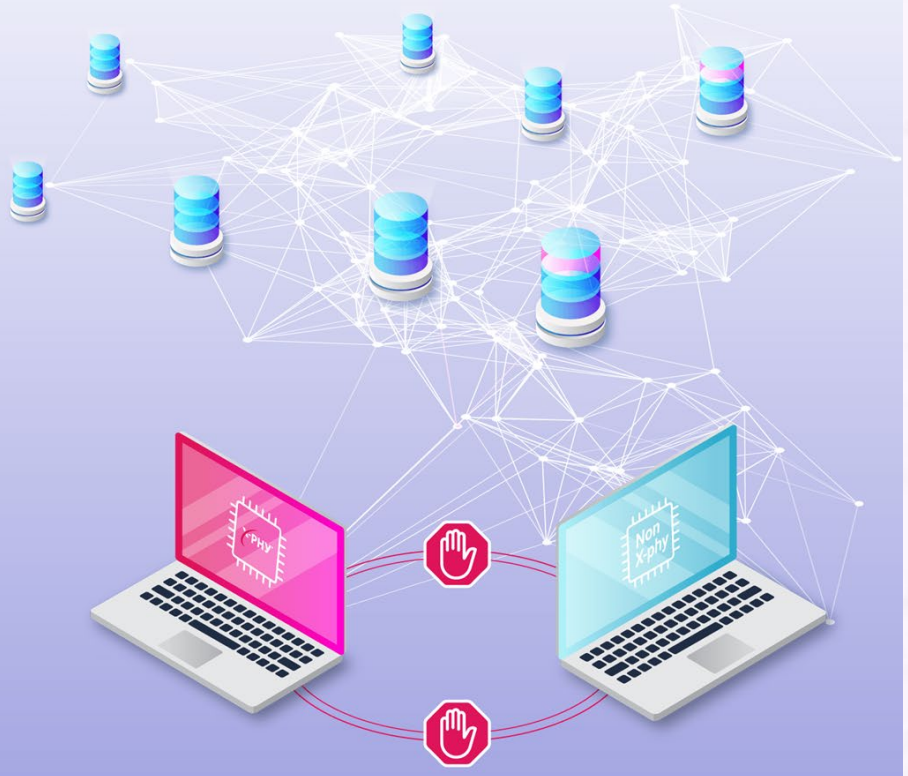
FMS the Future of Memory and Storage

Why Hardware-Driven Security?

X-PHY Solution

- Real-time, hardware-rooted attestation — beyond traditional user-only verification (IAM).
- Continuous trust validation on data access — not just at system boot (TPM).

Feature	IAM	TPM	X-PHY
Validation Frequency	Login	Boot	**Per Access**
Device + Role Identity	✗	Partial	✓
Automatic Threat Isolation	✗	✗	✓
Built-in to Memory	✗	✗	✓



Data Transmission Blocked
X-PHY device to non-X-PHY device

Introducing X-PHY- The Community-Based Root of Trust (CBRoT)

X-PHY Verification

Only X-PHY enabled devices linked to the X-PHY portal can access and interact across all systems.

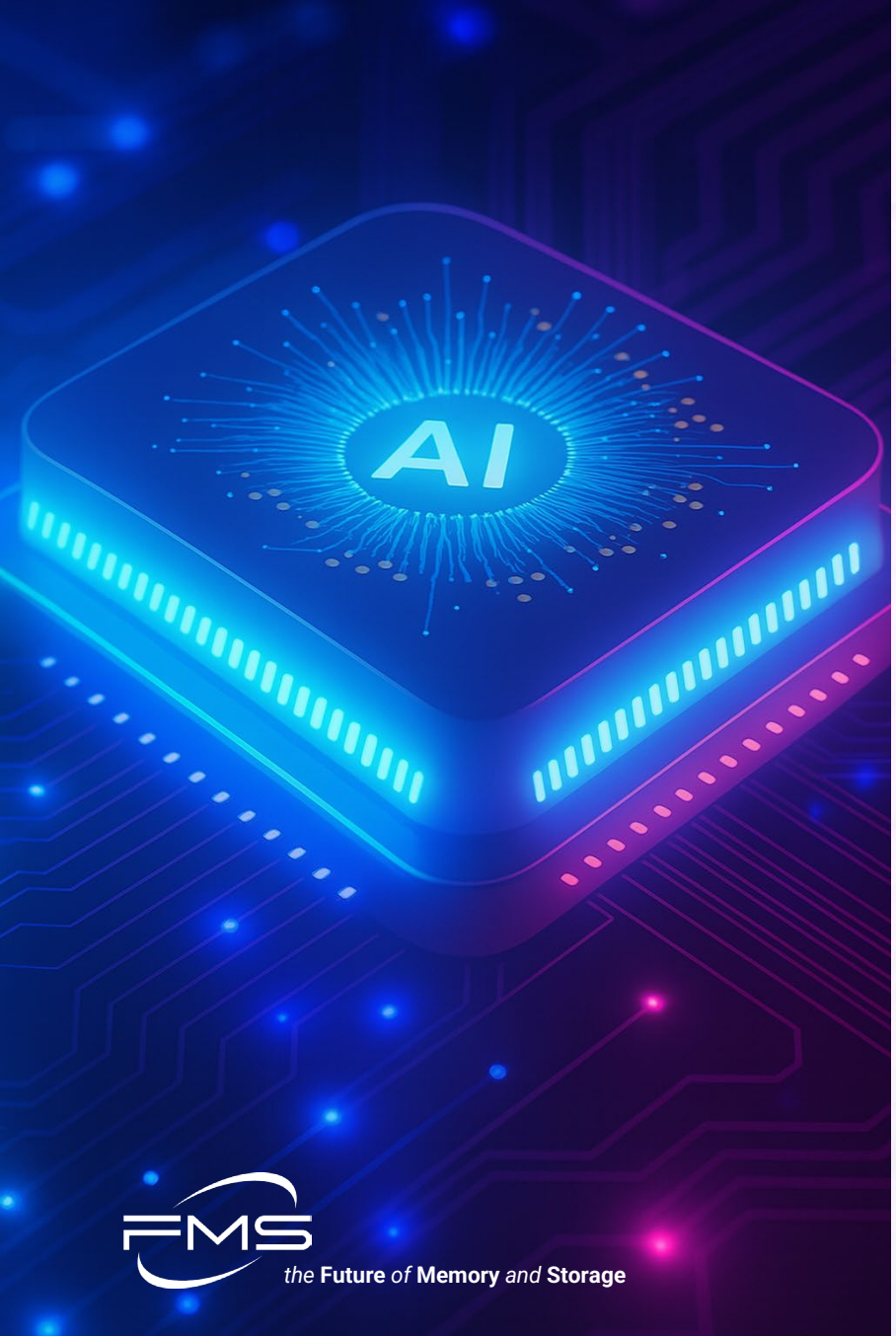
Continuous Revalidation

Trust is not static. Every interaction is revalidated in real time by checking the digital fingerprint and the role.

Zero Assumptions

All endpoint devices are considered untrusted until verified via hardware attestation through the X-PHY Portal.

FMS *the* **Future** *of* **Memory** *and* **Storage**



X-PHY CBRoT Principles

Hardware-Embedded Security
Security embedded directly in the hardware

Unique Digital Fingerprint
Each device has a **unique digital fingerprint** (hardware key)

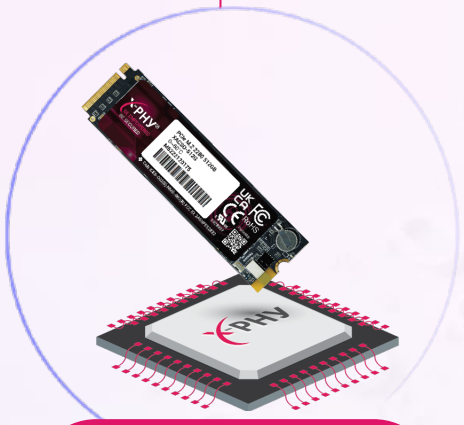
Real-Time Monitoring
Memory enforces **real-time behavioral monitoring**

Proactive Security
Hardware + Firmware-Base AI = Proactive security, not reactive patches

FMS the Future of Memory and Storage

X-PHY CBRoT Ecosystem Overview

Solutions



X-PHY SSD (M.2 form factor)

- AI-enabled, real-time behavior monitoring
- Device + Role Identity
- Hardware-level root of trust

X-PHY Portal (Cloud-based)

- Centralized registration & policy control
- API integrations for 3rd parties
- Threat alerts and visibility

Ecosystem Integration

CBRoT (Community Root of Trust)

- Policy-driven, real-time attestation
- Collaborative verification across vendors, partners, endpoints

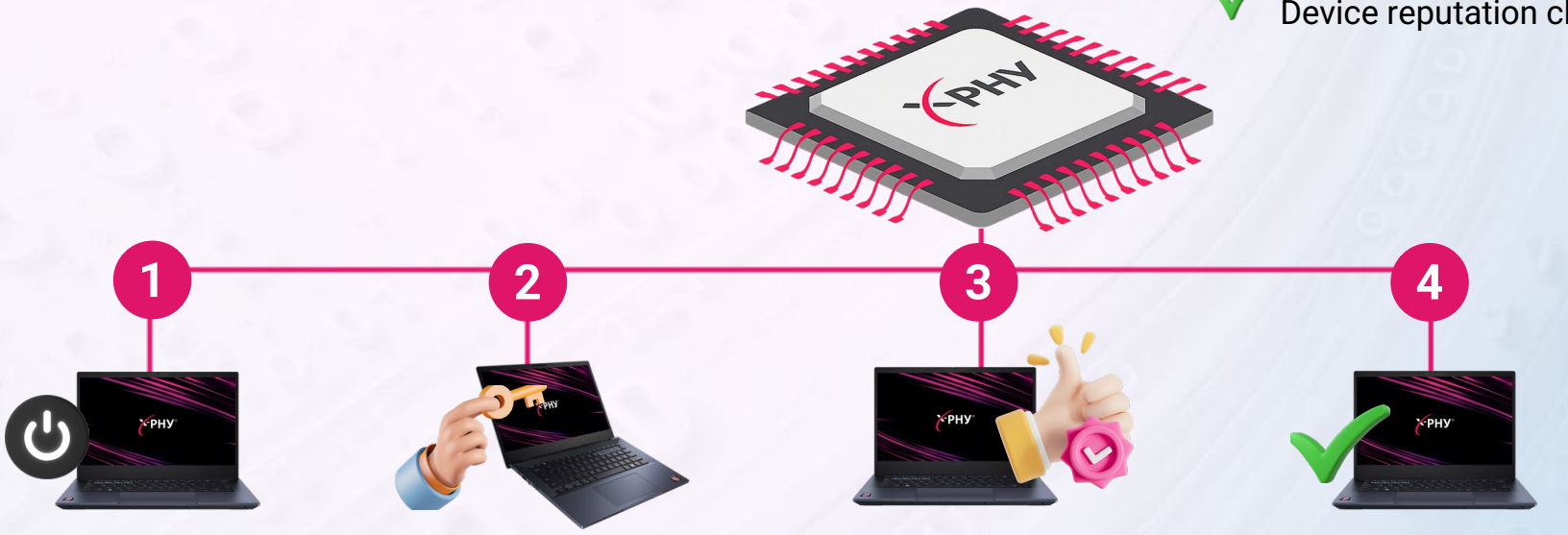
Enterprise Network Stack

- Active Directory / Firewall / SIEM
- 3rd party vendors via API

X-PHY CBRoT 4-Step Process

X-PHY Verification

- Hardware attestation
- Role validation
- Device reputation check



FMS the Future of Memory and Storage

Impact - What Changes?

From Passive to Active Security

- Memory becomes part of the defense layer

From Static to Adaptive Trust

- Revalidation on every access

From Isolated Security Control to Community Governance

- Trust is maintained by updated registries

Results:

- No access from untrusted hardware
- Malicious threats detection in real time

Use Case – Supply Chain:
Enforcing Zero Trust

Threat:

- Shared data is exposed when accessed by non-compliant partner devices.
- Existing API-based access lacks hardware-level trust.

X-PHY in Action:

X-PHY Hardware Token Key within Firmware Level

Blocks unauthorized external access

Replaces API trust with secure portal validation

Use Case – Financial Services:
Enforcing Zero Trust

Threat:

- Endpoints are vulnerable to:
  - Tampering & Insider Threats
  - Unauthorized device access

X-PHY in Action:

Secures endpoints independently of workgroup & domain

Block unknown & unauthorized access

Centralized control via X-PHY Cloud Portal

CONTACT US

UNITED STATES

X-PHY Inc.
Eberle Building,
Suite 300,107 S B St,
San Mateo, CA 94401

X-PHY Inc.
5520 Research Park
Drive, Suite 100
Baltimore, MD 21228

X-PHY®

Be Empowered, Be Secured

+1 669 240 5384
info@x-phy.com
www.x-phy.com