MACRONIX

ArmorFlash™ and ArmorBoot

A Hardware Root of Trust Path to EU Cyber Resilience Act Compliance



October, 2026

CONTENTS

02 Executive Summary

03 Background and Regulatory Urgency: EU CRA Timeline

04 Threats to Connected Devices and the Need for Hardware Defenses

06 Key Technologies in Macronix Secure Flash Products

09 Product Applications and Deployment

10 Product Portfolio and CRA Compliance Crosswalk

12 Conclusion: A Path to Zero Trust Architecture



Executive Summary

With the EU Cyber Resilience Act (CRA) now in force, digital product manufacturers worldwide face pressure to build security into their underlying architectures. Macronix brings cybersecurity defenses down to the nonvolatile memory (NVM) layer through a chip-level hardware root of trust. The solution provides encryption-based protection for automotive, industrial and AI data-center applications, while helping OEMs address demanding CRA requirements without changing their existing syttem-on-a-chip (SoC) architecture.

- **Asset protection and zero trust architecture :**
  Active metal shielding delivers physical protection, while AES-GCM provides logical encryption. Together, these features establish protection at both the physical and logical layers.
- **A tamper-resistant digital passport :**
  A unique identifier (UID) and a two-level L1/L2 certificate chain support component provenance and supply chain security.
- Lifecycle resilience :
  ArmorFlash memory offers up to 20 years of data retention and 100,000 program/erase cycles, with support for secure recovery and readiness for post-quantum cryptography (PQC).

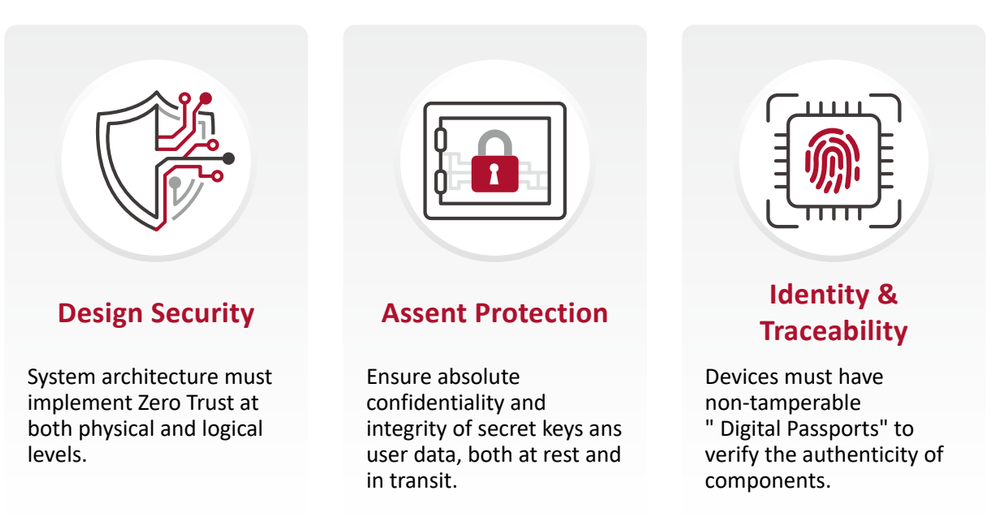


Figure 1. The EU Cyber Resilience Act sets stringent security requirements for connected devices, requiring resilience against cyberattacks from the lowest layers of the system.

Background and Regulatory Urgency : EU CRA Timeline

The CRA marks a shift away from relying on software patches after vulnerabilities are discovered. Hardware development and validation typically take 18 to 24 months, so manufacturers need to incorporate hardware-based security in storage components during design to meet the mandatory 2027 compliance deadline.

Year	Regulatory Requirement or Milestone
2024	The EU Cyber Resilience Act (CRA) enters into force and the transition period begins.
2026	Vulnerability reporting and notification of significant security incidents become mandatory.
2027	Full compliance becomes mandatory; products must undergo conformity assessment and bear the CE marking to be sold.

The vulnerability management obligations taking effect in 2026 also call for robust secure logs [JS1.1] and traceability. ArmorFlash's built-in authentication and tracking features can provide a legally valid digital passport for each device, helping manufacturers streamline audits and incident response when vulnerabilities arise.

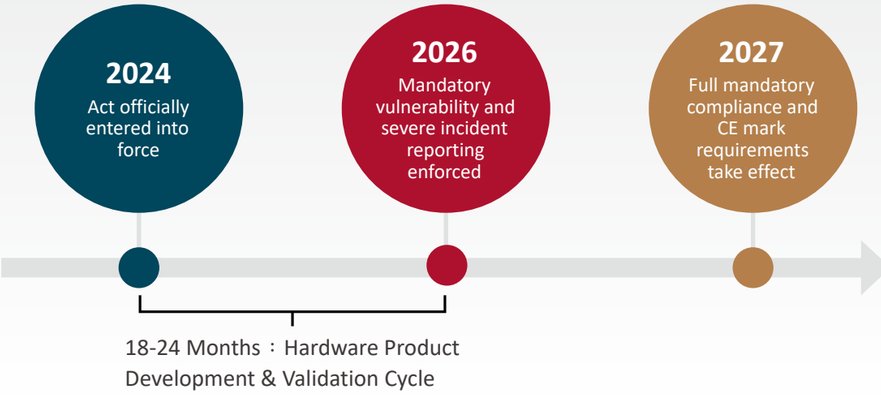


Figure 2. The EU Cyber Resilience Act milestones conclude with full mandatory compliance in 2027.

Threats to Connected Devices and the Need for Hardware Defenses

In today's threat environment, attackers often target standard SPI interfaces. ArmorFlash and ArmorBoot address the following attack vectors at the hardware level.

- **Bus sniffing :**
  Conventional Flash interfaces transmit commands in plaintext. ArmorFlash, therefore, uses highly secure data access (HSDA) to encrypt commands, addresses, and data, so intercepted traffic appears as ciphertext.
- **Replay attacks :**
  Because an attacker repeats a valid command to gain control, Macronix uses three types of counters to make each secure session unique over time.
- **Rollback attacks :**
  If an attacker maliciously downgrades firmware to a version with known vulnerabilities, hardware's root of trust and monotonic counters enforce forward-only firmware version progression and block unauthorized downgrades.
- **Physical tampering :**
  Voltage glitches, abnormal temperatures and clock interference are examples of physical attacks, so the hardware's built-in environmental sensors can trigger a protective lockout or system reset when they detect anomalies.

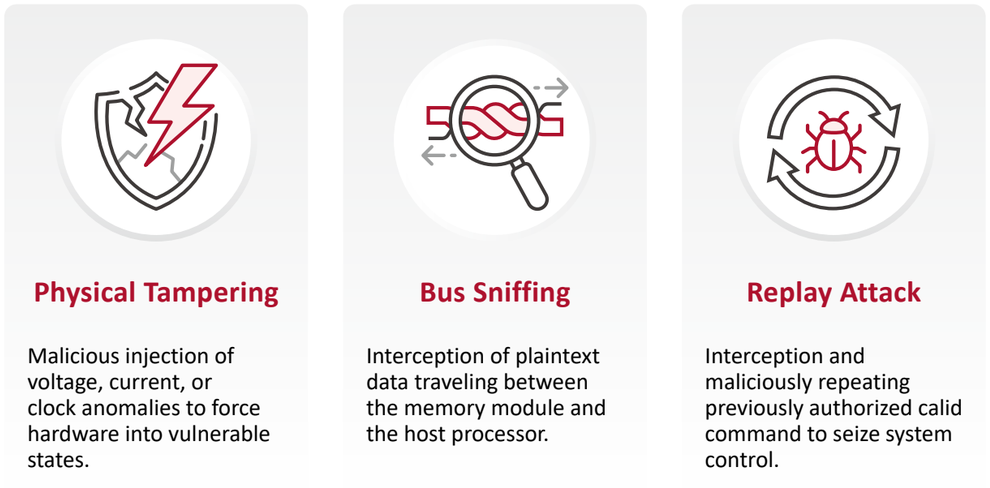


Figure 3. Several threats to connected devices are addressed by CRA security design requirements.

Integrating security into the storage component can remove a bus exposure point associated with an external secure element (SE), while reducing overall bill-of-materials cost and board space.

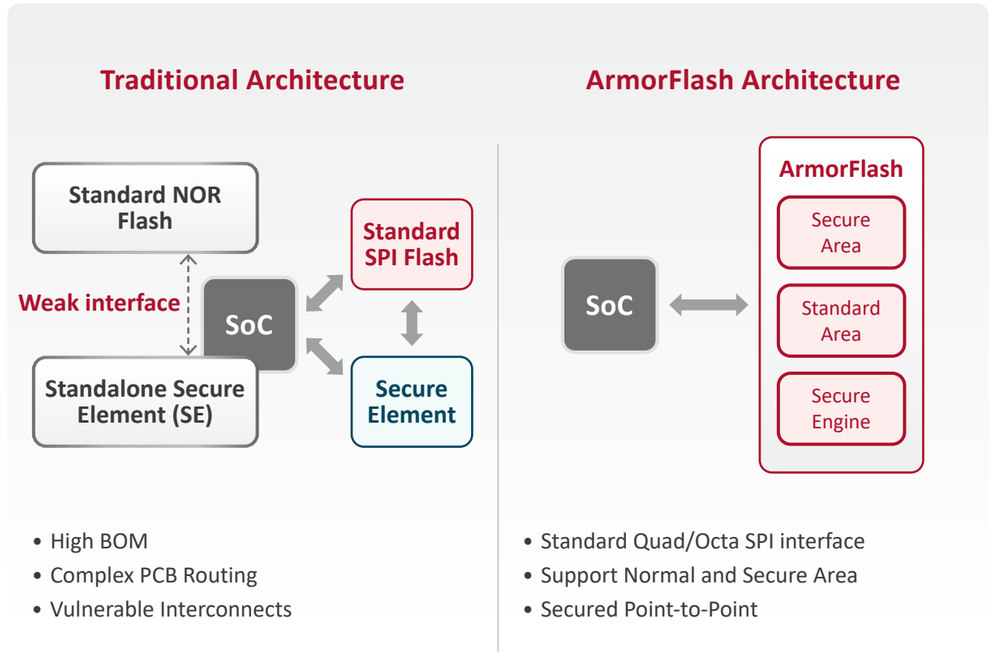


Figure 4. Macronix ArmorFlash provides a high-throughput hardware root of trust.

Key Technologies in Macronix Secure Flash Products

Highly Secure Data Access and AES-GCM Encryption

The ArmorBoot MX78 uses AES-GCM authenticated encryption in accordance with NIST SP 800-38D. Its core HSDA mechanism encrypts data as well as host request commands, access addresses, and parameters before they enter the bus. Even if an attacker physically probes the interface, the ciphertext does not reveal system operation or memory layout.

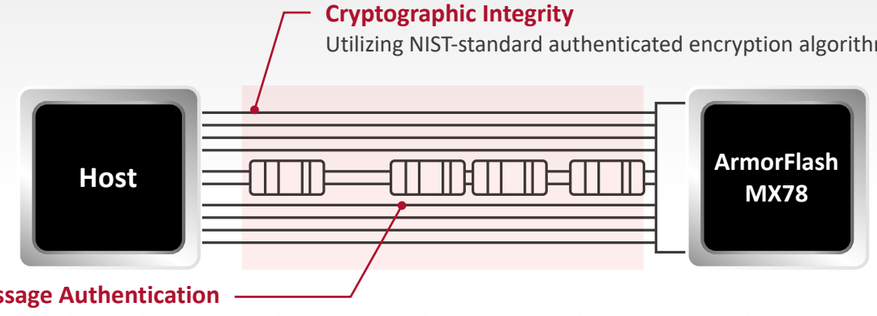


Figure 5. Host requests, addresses and parameters are converted to ciphertext before reaching the communication interface, preventing an attacker probing the interface from reconstructing the commands.

Device Identity and the Two-Level L1/L2 Certificate Chain

Each chip is provisioned during manufacturing with an immutable UID. L1/L2 certificate verification that allows a device to establish its authenticity through supply-chain-level digital signatures. This helps prevent counterfeit components from joining the system and provides a hardware foundation for the identity and traceability required by the CRA.

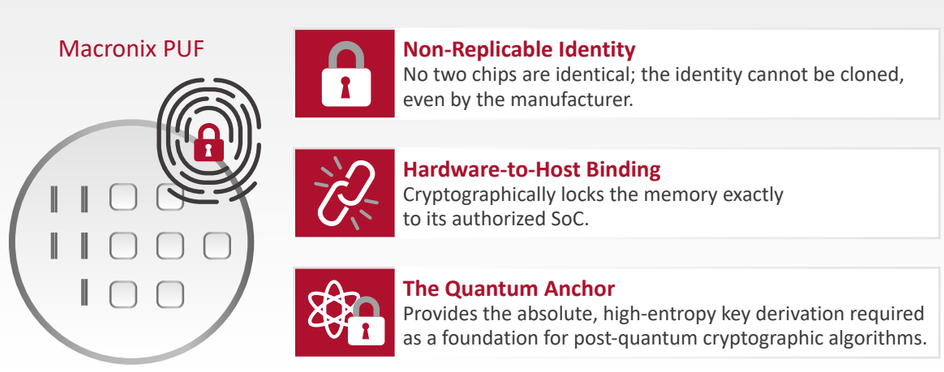


Figure 6. The Macronix PUF enables a unique fingerprint for each chip.

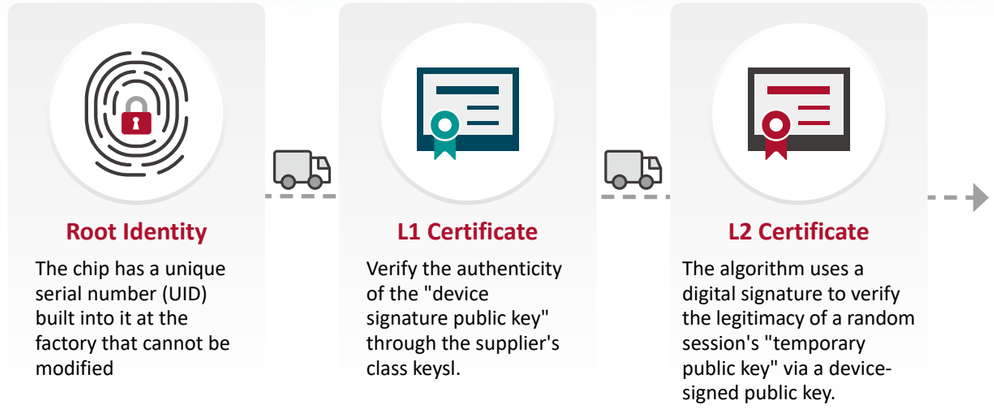


Figure 7. Strong identity verification is provided by a digital passport based on an L1/L2 certificate chain.

Three Types of Monotonic Counters

Macronix uses three types of counters to defend against replay attacks :

- **Global persistent counter (GP_MC) :**
  Records the total number of secure sessions over the chip's lifetime as a master tally.
- **Session volatile counter (SV_MC):**
  Increments with each key use and forms part of the AES-GCM initialization vector (IV).
- **User counters:**
  Allow system integrators to track the device lifecycle persistently and strengthen operational resilience.

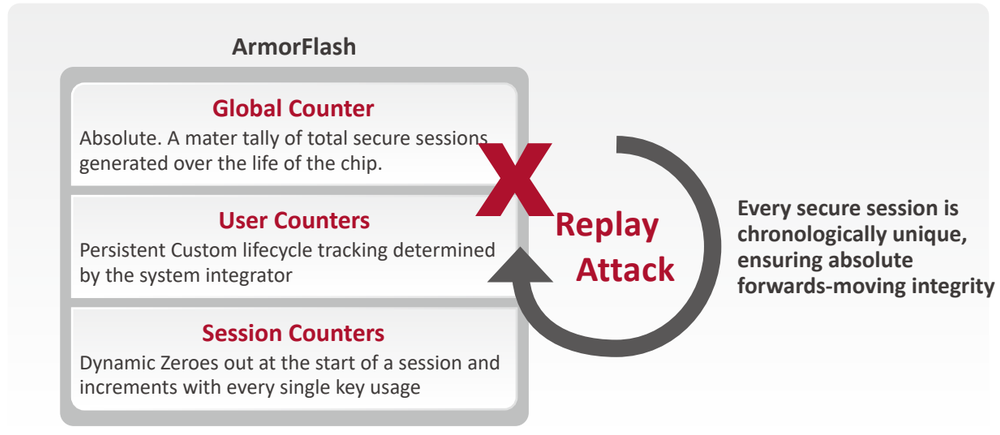
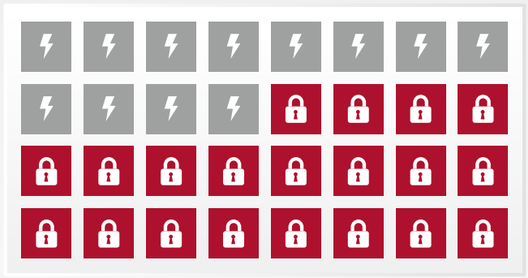


Figure 8. Monotonic counters provide hardware-based protection against replay attacks.

Physical Defenses and Data Zone Lockdown

- **Active metal shielding :**
  Provides physical protection against non-invasive probing and reverse engineering of internal interconnects.
- **Flexible data zones:**
  The 128 Mb version offers 32 independent data zones and supports mixed storage modes. Sensitive data, such as keys and personal information, can be placed in a highly secure mode. The lockdown function can then permanently restrict access to prevent unauthorized modification.



Independent Data Zones

- **128Mb :** support up to 32 independent 4Mb zones.
- **64Mb :** support up to 16 independent 4Mb zones.

Root Key Binding

- Each individual secure zone can be cryptographically bound to its own unique hardware root key, ensuring absolute privilege isolation (Least Privilege principle.

Flexible Configuration

Zones can be dynamically configured seamlessly

- Standard Area: Open read access for general boot code and standard execution
- Secure Area: Authenticated and encrypted read/write for highly confidential keys, user data, and secure logs

Figure 9. Flexible data storage lets users configure security levels for different applications.

Product Applications and Deployment

Feature	ArmorBoot MX76	ArmorFlash MX78
Primary role	Secure boot and firmware resilience	Advanced data encryption and multi-tenant isolation
Key technologies	In-chip verification, automatic secure recovery, replay and rollback protection.	AES-GCM encryption, independent data zones, and HSDA encrypted command transfer.
Technical advantage	Keeps code off the external SPI bus during verification to strengthen boot security.	Supports mixed storage modes and is pin-compatible with standard NOR Flash, simplifying adoption.
Typical applications	Automotive ECU boot protection, industrial PLCs, and embedded systems in critical infrastructure.	ADAS and autonomous driving platforms, AI data centers, and protection of personal data in advanced networking equipment.



Product Portfolio and CRA Compliance Crosswalk

Macronix offers an ArmorBoot portfolio from MX75 through MX78 to support resilience throughout a 20-year product lifecycle.

- **MX76 (ArmorBoot) :**
  Strengthens secure boot and system recovery.
- **MX77 (RPMC) :**
  Focuses on replay attack protection.
- **MX75/78 (ArmorFlash) :**
  Provides comprehensive data encryption and physical tamper protection.

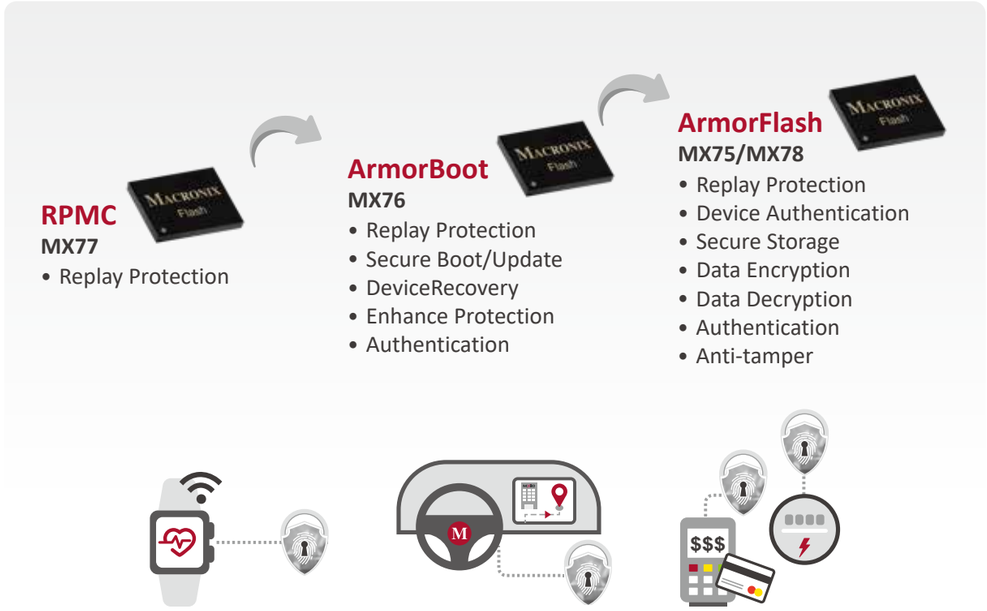


Figure 10. Macronix ArmorFlash product portfolio.

CRA Compliance Crosswalk

CRA Requirement	Macronix Hardware Security Primitive
Secure by design	Chip-level hardware root of trust (RoT).
Asset protection	AES-GCM, HSDA encrypted transfer, and HMAC command integrity checks.
Identity	16-byte UID, L1/L2 certificate chain, and hardware true random number generator (TRNG).
Resilience	Three types of monotonic counters, active metal shielding, and environmental tamper detection sensors.
Lifecycle management	20-year data retention, 100,000 program/erase cycles.

The product family strictly complies with ISO 21434 for road vehicle cybersecurity, ISO 26262 for functional safety, and AEC-Q100 Grade 1 automotive qualification, supporting compliance across global markets.

AEC-Q100
Grage-1

Automotive-Grade Certified
Fully automotive-grade certified. Tested against extreme environmental stresses for vehicle system stability.

100K P/E Cycles

Industry-Leading Endurance
Industry-leading endurance. Validated for one hundred thousand Program/Erase cycles.

20Y Retention

Long-Term Data Integrity
Exceptional physical retention characteristics ensuring data survives untouched for decades in long-lifecycle infrastructure.

FIPS-140-2/3

NIST Cryptographic Standards
Meets the stringent Federal Information Processing Standards defined by NIST for cryptographic modules.

ISO 26262
ASIL-D

Functional Safety Standard
International standard for road vehicle functional safety across the entire product lifecycle.

ISO 21434

Cybersecurity Standard
International standard for road vehicle cybersecurity across the entire product lifecycle.

Figure 11. Automotive and industrial environments demand reliability.

Conclusion :
A Path to Zero Trust Architecture

As OEMs adapt to the EU CRA, ArmorFlash and ArmorBoot offer complementary hardware security capabilities that can be incorporated without redesigning the entire system. Embedding trust in silicon addresses current regulatory needs and provides a security foundation for future autonomous driving and advanced computing applications. A chip-level root of trust offers a practical path toward zero trust architecture.

To learn more about how Macronix secure Flash products can help address EU Cyber Resilience Act (CRA) requirements, contact us through the Macronix website at **www.mxic.com.tw**



Headquarters
Macronix International Co., Ltd.
16, Li-Hsin Road, Science Park, Hsinchu, Taiwan
Sales Direct Line: +886-3-578-1088
Fax: +886-3-563-2888

Taipei
Macronix International Co., Ltd.
19F, 4, Min-Chuan E. Road, Sec. 3, Taipei, Taiwan
Sales Direct Line: +886-2-2509-3380
Fax: +886-2-2509-2200

America
Macronix America, Inc.
680 North McCarthy Blvd. Milpitas, CA 95035, U.S.A.
Tel: +1-408-262-8887
Fax: +1-408-262-8810

Europe
Macronix Europe N.V., Germany Office
Niederlassung Deutschland, Heisenbergbogen 1,
85609 Aschheim-Dornach , Germany
Tel: +49-89-5402-14000
Fax: +49-89-5402-14001

Macronix Europe N.V., Belgium Office
Koningin Astridlaan 49, B6, 1780 Wemmel, Belgium
Tel: +32-2-456-8020
Fax: +32-2-456-8021

Japan
Macronix Asia Limited.
Ichigo Kawasaki Bldg. 5F, 1-2 Higashida-cho, Kawasaki-ku
Kawasaki-shi, Kanagawa Pref. 210-0005, Japan
Tel: +81-44-246-9100
Fax: +81-44-246-9105

China
Macronix (Hong Kong) Co., Limited, SuZhou Office
No. 55, Su Hong Xi Rd, SuZhou Industrial Park,
SuZhou China 215021
Sales Direct Line: +86-512-6288-8345
Fax: +86-512-6258-6799

Macronix (Hong Kong) Co., Limited, ShenZhen Office
Room 1401, Block A Tian An Hi-Tech Plaza Tower
CheGongMiao Futian District Shenzhen 518040 PRC
Sales Direct Line: +86-755-8343-3585
Fax: +86-755-8343-8078

China - Hong Kong
Macronix (Hong Kong) Co., Ltd.
702-703, 7/F, Building 9, Hong Kong Science Park,
5 Science Park West Avenue, Sha Tin, N.T.
Sales Direct Line: +852-3460-5188
Fax: +852-3460-5184

Korea
Macronix Asia Limited.
#906, 396 Seocho-daero, Seocho-gu,
Seoul 135-857, Korea
Tel: +82-2-588-6887
Fax: +82-2-588-6828

Singapore
Macronix Pte. Ltd.
1 Marine Parade Central #11-03 Parkway Centre
Singapore 449408
Tel: +65-6346-5505
Fax: +65-6348-8096

MACRONIX INTERNATIONAL CO., LTD.

www.macronix.com

Copyright© Macronix International Co., Ltd. 2026. All rights reserved, including the trademarks and tradename thereof, such as Macronix, MXIC, MXIC Logo, MX Logo, Integrated Solutions Provider, Nbit, Macronix NBit, HybridNVM, HybridFlash, HybridXFlash, XtraROM, KH Logo, BE-SONOS, KSMC, Kingtech, MXSMIO, OctaBus, ArmorFlash, LybraFlash, FortiX. The names and brands of third party referred thereto (if any) are for identification purposes only.