Technical Brief

Engineering a safer world

NXM Autonomous Security™

"Rogue firmware can cause devices to overheat, putting homeowners' safety at risk." - *Wired*

"Firmware exploit turns smart home products into illicit surveillance networks". - *WSJ*

"Hackers steal infrastructure keys, demand Bitcoin ransom" - *Bloomberg*

"Botnet malware infects millions of devices, crashing websites in distributed attack." - *Reuters*

Security Capabilities Verified DIAMOND

Protect your customers. Enhance your brand.

Fastrack UL IoT Security Rating certification with NXM Autonomous Security software. Add a UL Verification Mark to your product packaging for retail and online promotion. NXM is a UL IoT Security Rating program partner.

psacertified™

Protect, Detect and Recover

NXM Autonomous Security™ transforms IoT security by enabling devices to automatically defend themselves and recover from cyberattacks. NXM's patented software technology monitors and responds to threats and adapts to new ones, enabling device networks to scale without sacrificing security.

Renewable Trust

NXM firmware-enabled devices automatically register themselves upon first boot to a distributed ledger using a self-generated, immutable machine identity unique to each device's processor. NXM's **distributed ledger technology** is used to manage device access and enforce security policies, eliminating attacks that can bring down device networks. A device's identity is rooted in hardware for complete cradle-to-grave security lifecycle management. In response to security events, NXM's firmware puts the device into safe mode, which isolates the compromised device from the network. In order to securely reconnect to the network, the device must refresh its firmware and encryption keys and validate its ID with the distributed ledger.

Intelligent Monitoring

NXM security is always on guard to monitor any changes to the integrity of the device's underlying firmware and check for any unauthorized access. NXM ensures the OEM has digitally signed and authorized firmware before it is loaded onto a device. Any access request or firmware update must be verified through the distributed ledger, which **provides an immutable record of all device activity**. If anomalies such as malware, botnets, or any form of unauthorized access are detected, the device switches into safe mode and issues a security alert to trigger further analysis and response actions.

Secure Communication

All data communication is encrypted chip-to-chip and chip-to-cloud. NXM immutable machine identity enables devices to authenticate each other and generate their own encryption keys in order to establish secure communication channels. NXM enables secure remote maintenance, and many-to-many mesh data sharing, providing the foundation for secure, autonomous device communication that enforces **compliance, data privacy, and network integrity**.

Platform Security Architecture (PSA) Certified

PSA provides a cohesive and scalable security framework supported by the world's leading chip vendors. NXM embodies Arm PSA security-by-design engineering principles that can **reduce product development costs and time to market**. Using NXM's Autonomous Security® software stack helps OEMs fastrack PSA certification. NXM is a founding member of PSA Certified®.

Easy Integration

NXM's firmware SDK enables the OEM application firmware to integrate with PSA and NXM security functions. NXM's software has **no significant impact on processor performance, heat or power consumption**. NXM enhances the security of existing FOTA processes by leveraging the trusted execution environment to verify code integrity.

How does it work?

NXM Autonomous Security™ verifies four key stages in the lifecycle of an IoT device, from provisioning to recovery.

One. Provision Keys

Uses a hardware root of trust to participate in NXM's security consensus ecosystem.

Two. Verify Firmware

Checks that every firmware update is authorized by the OEM.

Four. Refresh & Restore

Safely restores from secure firmware when unauthorized code or activity is detected.

Three. Prove Identity

Verifies device integrity and identity before it connects to the ecosystem.

Top NXM Autonomous Security™ Benefits

Threat	Risk	Prevention	Detection	Response	How We Do It
Rogue Firmware	Can cause battery drain, overheating, and device ignition.	NXM verifies all signed firmware images against the chip's hardware Root of Trust as well as against signatures registered on a distributed ledger.	NXM firmware uses cryptography to monitor and ensure firmware image integrity.	NXM safe mode enables remote reflashing of a device to restore it to a secure or quarantined state on your private network	Firmware Attestation Keys "Safe mode" for Image Refresh Distributed Ledger: Firmware Verification
Botnets	Launches mass attacks against internet sites using your customers devices. Hijacks device resources for illicit applications.	NXM prevents Botnet persistence by verifying signed firmware images against the device's hardware Root of Trust.	NXM's firmware detects the compromised OEM firmware, placing it into safe mode.	NXM safe mode enables remote reflashing of a device to restore it to a secure state, or quarantined state on your network.	Distributed Ledger: Firmware Verification "Safe mode" for Image Refresh Hardware Root of Trust
Cloned Devices	Cloned devices can access customer and sensor data, impersonate OEMs to backdoor (hack) user systems.	NXM verifies the integrity of device firmware before allowing it to connect to your support and administrative networks.	NXM detects when attackers make an unauthorized attempt to access your proprietary networks.	NXM disqualifies cloned devices from accessing your networks, and flags unauthorized firmware images.	Distributed Ledger: Pub/Sub Topics Secure Machine Identity Distributed Ledger: Firmware Verification
Stolen Credentials & API Keys	Enables unauthorized administrative access to cloud infrastructure that supports IoT devices in your product's ecosystem.	NXM creates per-device identity keys that cannot be re-used or cloned across device networks.	NXM detects an unauthorized event involving a stolen or re-used key involving a failed device transaction on NXM's distributed ledger.	NXM provides recourse to compromised devices using safe mode, which restores the security state of the device.	Distributed Ledger: Pub/Sub Topics "Safe Mode" for Image Refresh Secure Machine Identity
Ransomware	Ransomware locks customer ecosystem devices until a ransom is paid.	NXM's per-device identity keys prevent a hack of one device being leveraged into an attack on others. NXM eliminates single point of failure threats.	NXM detects unauthorized firmware when it fails signature verification on both the chip and distributed ledger.	NXM's safe mode refreshes the compromised firmware to a secure state.	"Safe mode" for Image Refresh Secure Machine Identity

Platform Requirements

Processor	OS	Memory	Cloud	PSA
Arm-Cortex M-33/23	RTOS*	1 MB FLASH	AWS / Azure	Yes
Arm-Cortex A **	Yocto	4 Mb RAM	AWS / Azure	Yes
Intel SGX	Coming soon			

* Requires chip-level support for secure memory management and NEON extensions

** MbedOS, Zephyr, FreeRTOS