NXM

Autonomous SECURITY

FULLY AUTOMATED
CYBER INTRUSION
PROTECTION

DATA ORCHESTRATION
AT THE EDGE
MONETIZATION

BLOCKCHAIN
ON A CHIP
PRIVACY
DATA INTEGRITY

Autonomous Security

Recipient of the Frost & Sullivan 2019 North American Visionary Innovation Leadership Award in IoT Security

NXM Autonomous Security enables IoT devices to defend themselves against hackers without the need for human intervention. NXM is a software-based platform that leverages the advanced security features of today's chips to enable brand manufacturers to more easily create trustworthy products that provide unparalleled security, privacy protection and data integrity features. NXM has been engineered to addresses a wide spectrum of IoT needs, from automated IoT onboarding to unprecedented data versatility at the device level that can unlock new recurring revenue opportunities and dramatically reduce the cost of developing artificial intelligence systems and data-driven business solutions.

Identity

NXM transforms ordinary connected devices into autonomous, self-governing machines capable of managing their own security. The first step in this process begins with Identity. To be considered autonomous, a device must possess a self-generated unique ID that works over any communication network. NXM's patented software enables a processor to create and permanently store its own unique identity in protected memory and on NXM's immutable DistributedLedger. Immutable machine identity is the cornerstone upon which all autonomous device networks operate.

Transparency

There is strength in numbers. That's why every NXM-enabled device registers its ID on a private blockchain that acts as a single source of trust for verification purposes. Only devices with IDs on the ledger are considered trustworthy. Machine identity is used for all data communication and NXM cloud storage applications, eliminating the need for vulnerable passwords or security certificates.NXM Distributed Ledger acts as a key exchange system in which enables authorized stakeholders to freely communicate and cooperate with each other.

Automation

Each device acts as an intelligent node in a fully distributed, peer-to-peer network of self-governing devices that autonomously maintain and update their encryption keys based on whoever holds the root of trust. Data communication is fully encrypted from the chip to one or more authorized stakeholders without the need to rely on the security of intermediate communication networks. Device and system integrity are automatically monitored using consensus and proven blockchain processes to enforce behaviour and remedy potential breaches. Rogue IoT devices can be detected and quarantined outside of enterprise firewalls, then restored to health using NXM's unique agile crypto capabilities.

Agility

NXM employs agile cryptography that enables devices to automatically change their cryptography at any time. Devices can have their security keys, algorithms or entire frameworks upgraded remotely in the field at any time. The device is able to remedy potential breaches by immediately generating new encryption keys, permanently blocking past key holders from communicating with the device.

Evolution

NXM's agile crypto technology is capable of guarding devices from rapidly evolving cybersecurity threats, including quantum computers. NXM Quake is a breakthrough quantum-safe encryption solution designed to protect high value computing assets, from sensors to high-end servers, against the threat of quantum attacks. NXM Quake requires no changes to existing security protocols or enterprise processes and is designed to run on any embedded hardware or system.

5G

NXM has been designed to support Software Defined Networks (SDN), edge processing, network slicing and other 5G technologies. Future NXM Multi-Access Edge Computing (MEC)support will be able to take advantage of machine learning on the device, leveraging next generation Neural Processing Unit (NPU) chips and cloudlet apps that enable distributing computing at the edge.

Certified

NXM's Autonomous Security architecture has been independently certified by Underwriters Laboratories (UL) to be Arm®Platform Security Architecture (PSA) compliant for scalability and consistency across large-scale IoT deployments.

Security by Design

NXM Autonomous Security embodies the principles of security by design, offering a new way to deploy and manage IoT device networks at scale that goes beyond conventional centralized, client-server and cloud-based models. Fully distributed, peer-to-peer and automated, NXM is compatible with Arm® PSA, Intel SGX and similar solutions from leading chip makers.