Autonomous Security

NXM Autonomous Security® is a scalable cybersecurity platform that enables device networks to automatically defend themselves and recover from cyber attacks that threaten critical space, air, land and sea assets.

Preventing Fleet-Wide Cyber Attacks

Existing solutions rely on hardcoding secret keys that are shared with Command and Control prior to deployment. This causes numerous stove-piped networks and a lack of network agility. To solve this, NXM's Autonomous Security decentralizes access control and enables connected assets to generate their own keys to support granular and dynamic access with full auditability.

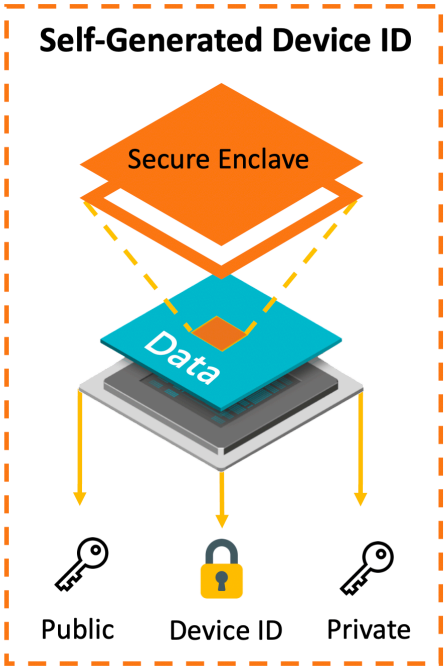
How Do We Do It?

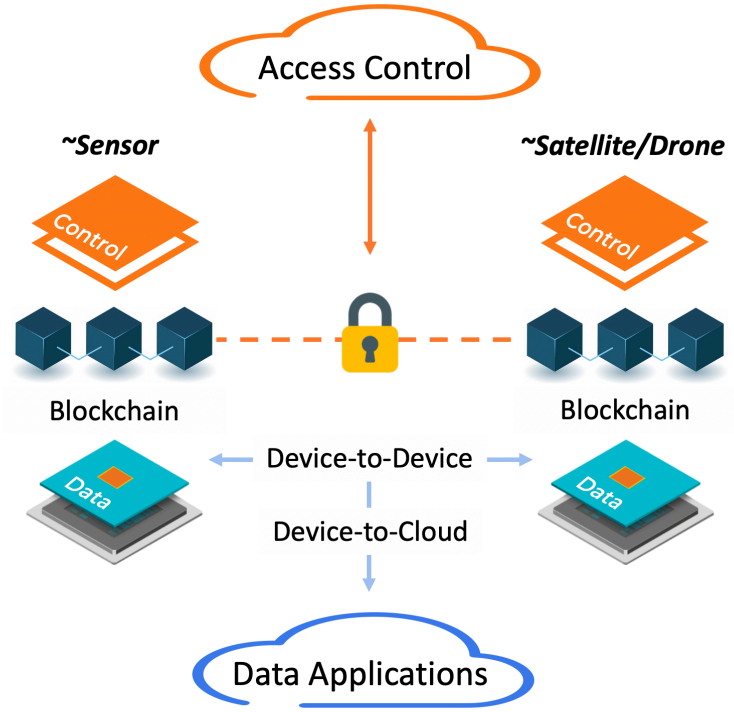
NXM provides a software-based, processor and cloud agnostic solution, that enables devices to generate a globally unique machine identity stored in their secure processing regions and register themselves to a private Command and Control blockchain network.
This creates an immutable machine identity for any connected asset on the network where access control is separated from data applications allowing devices to manage themselves.

Enabling a Secure and Dynamic Data Architecture

NXM enables data applications and connections to scale independently without impacting security.
Connections are not hardcoded and can open and close to allow any connected asset to operate in an agile environment. This extends to many-to-many data sharing applications where all endpoints are authorized via the blockchain and all data is encrypted and authenticated end-to-end.

Control-Data Separation





Left: A secure enclave is an isolated region of a processor that houses the root of trust established at manufacturing. A firmware application inside the secure enclave is used to generate a unique machine identity and key pair that is separate from the root of trust used to register a device to a blockchain.

Right: The connection between a secure enclave and the blockchain provides complete separation of data applications from access control allowing devices to request access to public keys for machine-to-machine communications or sending data to the cloud and allowing devices to recover from cyber intrusions.

Autonomous Cyber Operations

NXM's distributed and decentralized Command and Control (C2) security model enforces finely grained access privileges and administrative control across multiple C2 networks.

NXM's blockchain technology provides a complete audit trail of all device activity and an autonomous way for C2 to establish control over their registered devices.

This also allows C2 networks to integrate under one system without compromising their security and data and creates decentralized authorization for interoperable and standardized communication in a network of networks.

Contact:
gov@nxmlabs.com