www.nanolocksecurity.com

@NanoLockSec

NanoLock Security

nanolock

Flash-to-Cloud Powerful Defense for Connected Edge Devices

With threats looming from network hacking and physical access attacks, billions of IoT and connected edge devices face the persistent risk of cyber-attacks and the challenge of protecting, securing and cost-effectively managing these devices is daunting. By leveraging a flash-based line of defense that has no impact on performance, NanoLock Security guarantees lifetime protection - from fabrication and the supply chain, through operations and firmware updates, to the device's end-of-life.

Powerful IoT Edge Protection

The NanoLock Security solution is embedded directly into the standard flash memories provided by the industry's leading flash memory providers, securing a hardware root-of-trust for connected edge devices. The solution enforces the security perimeter by preventing any modification or manipulation of critical code, while allowing only authenticated commands and validated firmware updates. NanoLock makes sure the connected edge devices are still protected and delivers real-time trusted alerts, even when the processor or the network is breached. This powerful protection blocks ransomware attacks on firmware, boot images, system parameters and critical applications in a broad array of connected edge devices.

Revolutionized Cost Structure: Shifting from CAPEX to OPEX

NanoLock Security enables tremendous savings in cyber spending and provides a unique Pay-Per-Controlled-Device cost structure that shifts security investments from a capital expense to an operational expense, or CAPEX to OPEX. NanoLock's solution therefore eases upfront security expenses and generates monetization opportunities for organizations that are managing connected device networks. With NanoLock, telecoms, OEMs, device manufacturers, industrial companies and system integrators alike can have ironclad cyber-physical protection in application domains, such as connected and autonomous vehicles, security cameras, routers, smart meters, critical infrastructure components, and more.

Last Protection Standing

Hermetic Protection

NanoLock safeguards against network, cloud or on-premise attacks, even if the hacker has physical access to the device.

+ **HW Root of Trust**. Embedded in the flash memories of leading vendors and agnostic to processor and OS, NanoLock's solution continuously shields connected edge devices, even if the processor is hacked. With Nanolock, connected edge devices are immune to persistent, large scale cyber-attacks.
+ **Lightweight.** With zero power and computational resources, memory constraints or latency, NanoLock's solution is ideal for IoT and connected edge devices.
+ **Trusted notifications and alerts.** Utilizing the trustworthy flash, NanoLock ensures real-time, reliable notifications and stops faulty or misleading information from hacked devices.

A Secured Tunnel for OTA Updates

NanoLock's solution secures connected edge devices during vulnerable firmware over-the-air (OTA) updates.

+ **Flash-to-cloud protection** creates a secured tunnel that assures safe and trusted delivery of authorized updates, applications and critical parameters.
+ **Successful updates**, even if the processor is hacked.
+ **True reporting.** No false update notifications.

Tight Network Control

Gain control over the entire connected edge device network with NanoLock's MoT (Management of Things) platform

+ **FOTA monitoring and updates**. Management tools for updating and tracking edge device software updates and new versions.
+ **Accurate status and reports.** Real-time attack detection and alerts as well as detailed status reporting.
+ **Big Data analysis** to identify critical patterns and anomalies.