nanolock

DEVICE-LEVEL, ZERO-TRUST
OT CYBERSECURITY

EDGE DEFENDER FOR MACHINES

Secure machines. **Secure revenues.**

Today's industrial customers expect high-performing, cyber-secure, and regulation-compliant machines. But machines without machine-level security are inherently vulnerable to attacks, which can compromise operational integrity, lead to loss of customer confidence, and erode brand reputation and revenues.

Machine suppliers need a built-in solution to protect from insiders, outsiders, third parties, and human errors – without impacting performance. Until now, existing measures could only partially protect against outside breaches. They could neither prevent insiders and third-party cyber incidents, nor did they protect against human errors. And they placed burdens on machine performance.

NanoLock: All-around security without compromising performance

Embedded in each machine, the zero-trust NanoLock Edge Defender for Machines secures the operational integrity of industrial machines, new and legacy, against outsiders, insiders, supply chain cyber events, and even technician mistakes.

NanoLock protects without impacting performance or functionality, while complying with evolving standards, regulations, and customers requirements. It has a minuscule footprint and minimal system requirements, making it ideal for machines with limited resources.

Provide your customers with the highest level of protection

- Gain a competitive advantage with zero-trust, machine-level protection
- Reduce patching cycles and liability costs
- Protect revenue and asset value
- Secure business reputation

Insiders pose the greatest (overlooked) threat

INSIDERS
Technicians, engineers, employees

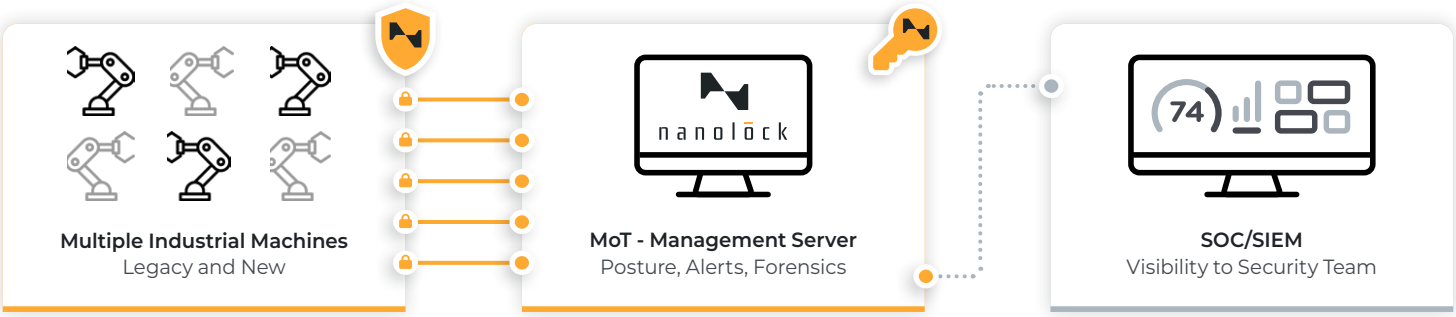
HUMAN ERRORS

SUPPLY CHAIN
External partners

OUTSIDERS

How it works

1. NanoLock Gatekeeper, embedded in each machine, acts as a robust locking mechanism that protects critical code, configuration, and calibration data in the non-volatile memory (NVM) by blocking all unauthorized modification attempts.
2. An alert is issued for each blocked unauthorized change attempt, whether accidental or malicious, internal or external, or utilizing privileged access.
3. The embedded Gatekeeper validates update requests and allows only properly signed authorized updates.
4. In addition to reporting of unauthorized modification attempts, the Gatekeeper communicates the machine's true status, provides detailed attack forensics, and enables a targeted view of the entire network of machines.
5. NanoLock's MoT trusted server continually monitors and manages all NanoLock-protected machines, regardless of vendor, for seamless visibility and management.



Differentiating features

- Embedded in both new and legacy machines with zero impact on performance and functionality.
- Small footprint with near zero power, processing, and memory requirements.
- Prevents outsider, insider and supply chain cyber events, as well as protecting against human errors.
- Local and remote secured updates.
- Reliable security visibility, trusted status and alerts, detailed forensic data.
- Quick integration into SOC/SIEM, IDS, and third-party platforms.
- Saves remediation time and costs.

Governments and standardization bodies worldwide call for zero-trust machine-level architecture

"If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed."

President Biden, Executive Order on Improving the Nation's Cybersecurity, May 2021

"Entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust architecture, software updates, machine configuration, network segmentation, identity and access management or user awareness."

Directive (EU) 2022/2555 of the European Parliament and of the Council, December 2022

Complies With: ISA NIST enisa NERC CIP

For more information:
info@nanolocksec.com | www.nanolocksecurity.com

nanolock