nanolock

DEVICE-LEVEL, ZERO-TRUST
OT CYBERSECURITY

OT DEFENDER

Utilities and Energy Businesses – Secure Your Mission-Critical Assets from Insiders, Outsiders, Third-parties, and Human Errors

From contaminated water to explosions, cyber attacks can have life-threatening consequences.

As new technologies are layered on top of legacy infrastructure, and as distribution is digitized, industrial control systems (ICSs) become more vulnerable to attacks. The exponential increase in the number and scope of threats, plus growing geopolitical concerns, theft, and the often overlooked insider threats, are inundating the industry with attacks from all directions.

Existing security approaches are based on post-incident detection rather than proactive prevention. Solutions such as IDS, IPS, and PAM rely on network connections, fail in protecting from insiders, and lead to alert fatigue.

Opt for proactive prevention

NanoLock OT Defender proactively secures the integrity of your Operational Technology (OT) assets whether they are connected to a network, offline or air-gapped. It protects all PLCs from all known vendors, new and legacy, without impacting performance, functionality or user experience.

Key benefits

- Prevents downtimes
- Zero impact on performance and functionality
- Compliance with the strictest regulations
- Single interface - supports all vendors
- Maintains safety

A CISO's nightmare

Hacks are frequent, brazen, and costly yet your employees and 3rd party ICS maintenance providers do not always comprehend or adhere to security policies. NanoLock flips the security paradigm at the source, preventing your people from becoming a security liability.

Protecting the entire OT terrain

Connected Devices & Networks	Offline Devices & Environments	Remote Locations

Insiders pose the greatest (overlooked) threat

INSIDERS
Technicians, engineers, employees

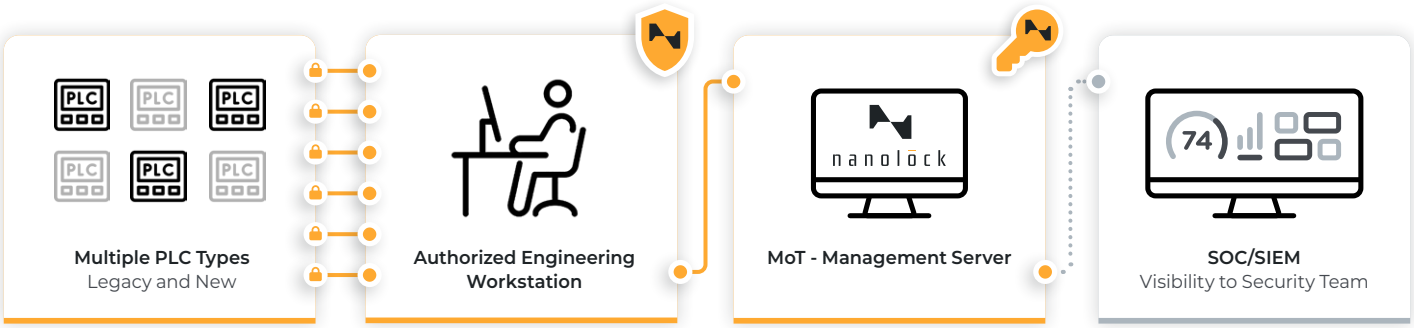
HUMAN ERRORS

SUPPLY CHAIN
External partners

OUTSIDERS

How and why it works

1. PLC protection is activated after the addition of a NanoLock Enforcer agent through a single and simple installation & setup. No changes to the PLC are made.
2. Only authorized users created and managed by the Nanolock MoT server can access, change or update PLC configuration based on permissions, multi-factor authentication, and predefined policies.
3. No other user, whether they have access to the workstation or the Enforcer, can perform any changes, if they are not authenticated and authorized by predefined policies to change a PLC. Devices that require read or HMI access are not impacted.
4. Security policy cannot be overruled by direct access to the PLC even when a device is not connected or is on an air-gapped network.



Differentiating features

- Secures access to all PLCs from different vendors, new or legacy, connected or disconnected to the network
- Manages access privileges in a distributed employee environment
- Full visibility into PLC-change related activities with a potential influence on processes
- Installed in less than a day and easily integrates with existing SOC/SIEM or monitoring and reporting systems

Governments across the world call for zero-trust device-level architecture

"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

"The CIIO shall establish mechanisms and processes to reduce and manage cybersecurity risks relating to connections between a field controller and any network or device."

Cyber Security Agency of Singapore, Cybersecurity Act of 2018; July 2022 Edition; to be enforced within 1 year

Complies With: ISA NIST enisa NERC CIP

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

nanolock