Industrial Control Systems (ICS) are vulnerable to attacks, putting production lines and services at risk, potentially resulting in disruptions, compromised safety, financial loss, business shutdown, and even loss of lives. Existing solutions such as IDS, IPS, and PAM either provide post-incident detection – without preventing the damage, or rely on network connections. They do not protect from insiders, and lead to alert fatigue.

Shift from post-incident detection to proactive prevention

The 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 ensures that every access, change request, or update attempt through a Programmable Logic Controller (PLC) is always authenticated and authorized, regardless of its origin. It protects all new and legacy PLCs, from all vendors, without impacting performance, functionality or user experience.

Employees or 3rd party ICS maintenance providers may not fully comprehend or adhere to the security policies in place. NanoLock flips this security paradigm at the source, preventing your people from becoming a security liability.

Key benefits

- Prevents production downtime
- Zero impact on performance and functionality
- Compliance with the strictest regulations
- A single interface that supports all vendors
- Maintains safety

Protecting the entire OT terrain

- Connected Devices & Networks
- Offline Devices & Environments
- Devices on Air-gapped Networks

Insiders pose the greatest (overlooked) threat

- **INSIDERS**
  - Technicians, engineers, employees
- **HUMAN ERRORS**
- **SUPPLY CHAIN**
  - External partners
- **OUTSIDERS**
How it works

1. With a single installation and setup, PLC protection is activated. The NanoLock Enforcer agent is added to authorized engineering workstations to manage user authentication, grant/deny access to PLC, and report activity to the NanoLock Management Server (MoT).

2. Only authorized users created and managed by the Nanolock MoT server can change the 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, HMI access, and security policies 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
- Provides full visibility and traceability with audit trails into PLC-change related activities that have the potential to influence processes
- Manages access privileges in a distributed employee environment
- 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

“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

“The CIO shall establish mechanisms and processes to reduce and manage cybersecurity risks relating to connections between a field controller and any network or device... Preventing unauthorised data transmission and write functions.”

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

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