Safety Focus:
Food & Beverage Manufacturing

Protecting sensitive industrial control systems (ICS) from outsider and insider attacks, as well as human errors

Customer: Food and beverage (F&B) manufacturing enterprise

Requirements: Keeping production lines and entire operations safe, intact, and running

NanoLock OT Defender: Zero-trust, device-level, prevention-based operational technology (OT) cybersecurity solution for ICS, with zero impact on performance, functionality, and user experience

In F&B production lines, impeccable precision is mission-critical. An unauthorized or an accidental change in determinants e.g., temperature, humidity, and timing can lead to wasted batches, safety incidents, shutdowns, and lost revenue.

Outsiders, supply chain actors, insiders, and human errors all pose risks to Programmable Logic Controllers (PLCs) – regardless of vendor, and whether PLCs are new or legacy, connected or disconnected. Existing solutions are external-facing (ignoring insider threats and errors). And they are either network or detection based, entering the picture when PLCs have already been tampered with or even blocked.

F&B safety necessitates ZERO tolerance for unplanned changes

JBS (Brazil/US) faced ransomware in 2021. Shutdown in several plants. Paid $11M **to restore access to the PLCs.**

Wall Street Journal on JBS Attack

Cyberattack on food giant Dole temporarily shuts down North America production.

CNN on Dole Attack

Just one incident can eat through an entire operation as well as global food supply chains. With so much at stake, F&B manufacturers are under growing regulatory pressure to bring their cybersecurity practices up to speed.

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

"The Federal Government states that prioritizing resources to 'prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk' is essential."

National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture, November 10, 2022

"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... 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

The Nanolock OT Defender Solution

Addressing the root of it all - that trust cannot be assumed and must be evaluated on an ongoing basis.

The NanoLock OT Defender is a zero-trust, device-level, prevention-based OT cybersecurity solution that ensures every access, change request, or update attempt through all PLCs across the plant is always authenticated and authorized - with no impact on performance or functionality.

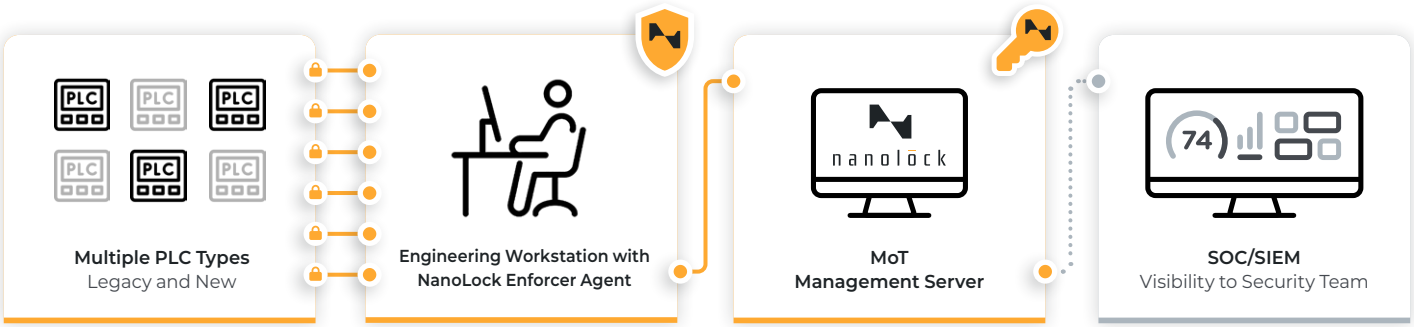
Ensures control of distributed ecosystems via:

- Preventing unauthorized access to all PLCs from different vendors, new or legacy; connected, disconnected or air-gapped
- Full visibility and traceability with audit trails into PLC-change related activities that have the potential to influence processes
- Management of access privileges
- Complies with the strictest regulations
- Installation in less than a day and easily integrates with existing SOC|SIEM or monitoring & reporting systems

70% of hacked food and beverage companies go out of business within a year of an attack, according to “Risky Business: Cyberattacks on the Food Supply,” by Capstone Logistics

How NanoLock protects F&B manufacturers from known and unknown attacks and human errors

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 each PLC, and report activity to the NanoLock Management Server - Management of Things (MoT). Only authorized users created and managed by the MoT server can change the PLC configuration based on permissions, multi-factor authentication, and predefined policies. 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. 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.



Complies With: ISA NIST enisa NERC CIP

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

nanolock