nanolock

Food & Beverage Industry
CASE STUDY

A world-leading dairy processing manufacturer implements NanoLock OT Defender to protect its multi-vendor Programmable Logic Controllers (PLCs).

NanoLock Security integrates measures for secure access control in new and legacy PLCs, along with real-time auditing to mitigate third-party threats and prevent production disruptions.

Company profile:	**Global dairy processing manufacturer**
Annual revenue:	**US$2B**
Employees:	**Over 1,000**
Number of facilities:	**50+ locations across the globe**

The company is a global dairy processing manufacturer with over $2 billion in sales volume. It operates across 50+ facilities worldwide and employs over 1,000 personnel. The company specializes in the mass production of dairy products and relies heavily on programmable logic controllers (PLCs) from multiple vendors to ensure efficient operations across its plants.

The Challenge

The company encountered several security vulnerability challenges in their existing facilities and in preparation for the opening of a new plant. Their challenge lay in managing multiple Programmable Logic Controller (PLC) vendors across plants, stemming from the use of various external technicians and over 1,000 employees who had access. The current security systems and management tools being used by the company fail to address the challenges of securing legacy and multi-vendor PLC environments, as well as make it difficult to manage authorization and ensure accountability for modifications made to the PLCs.

With numerous third-party contractors involved and a significant workforce interacting with PLCs, the company prioritized implementing strict access controls, traceability tools, and role-based access management to prevent unauthorized modifications. The company required a single solution to mitigate risks and gain centralized management of users and devices in a scalable and vendor-agnostic manner, and sought a proactive approach to enforcing PLC security, rather than relying solely on detection-based solutions.

The Solution

NanoLock OT Defender was selected for its device-level, zero-trust prevention approach and compatibility with both new and legacy PLCs from multiple vendors. NanoLock OT Defender enabled the company to enforce strict access controls, prevent unauthorized and unauthenticated access, and gain visibility into configuration changes across all its PLCs.

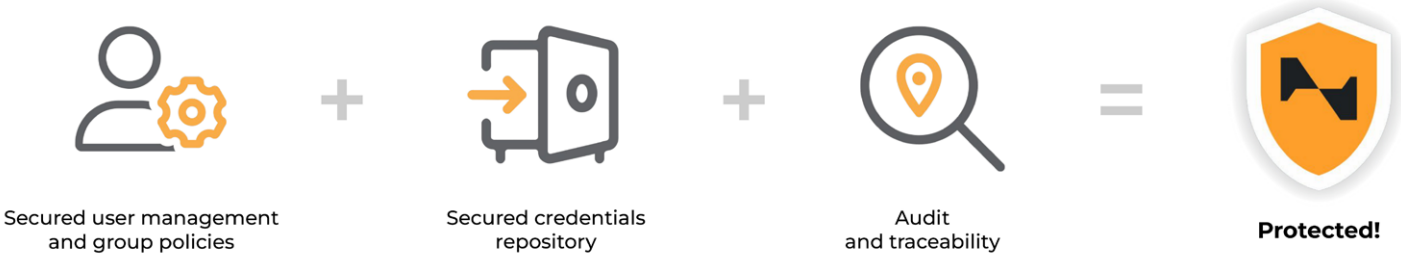
The solution's audit trails, traceability tools, and role-based access management capabilities aligned with the company's critical security needs and the security team's requirements for centralized management and visibility. While another solution was considered in the past, further examination revealed that NanoLock OT Defender differed significantly from the previously considered solution's capabilities and was considered a complementary solution rather than a direct replacement for them.

Results and Benefits

By implementing NanoLock OT Defender, the manufacturer achieved the following benefits:

- Maintained security and safety by authorizing and authenticating access to all PLCs, both new and legacy, regardless of vendor or age
- Eliminated risks associated with managing third-party automation contractors
- Enhanced visibility through centralized management, user traceability, audit trails, and role-based access control
- Achieved seamless integration with existing systems and quick deployment, minimizing disruption
- Centralized management of all PLC vendors in a single interface , displaying all PLC types on one screen

With NanoLock OT Defender, the company successfully integrated prevention and safety measures into its operational processes, securing access to all its PLCs and mitigating risks from insider threats, third-party contractors, and technician errors.



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