Water Utilities Industry

CASE STUDY

A major water authority in Asia implements NanoLock OT Defender to ensure a sufficient water supply for its country.

Within an hour of deploying NanoLock's solution, the authority secured its devices with zero-trust protection. The authority now plans to extend NanoLock across its water distribution control systems.

Company Snapshot:

Profile:	**Water management and coastal protection**
Operational volume:	**Serves 5+ million people**
Number of employees:	**up to 5,000**

The water authority manages water supply, water catchment, used water, and coastal protection in an integrated way. It ensures a diversified and sustainable water supply, while leading efforts to protect against rising sea levels and flood risks.

The Challenge

Safeguarding Critical Infrastructure from Cyber Threats

NanoLock was approached by the company after the water authority understood that they lacked sufficient protections that the new regulations required. Remote sites, in particular, faced a heightened risk of tampering and manipulation due to the limitations of physical security alone. The implementation of NanoLock's solution aimed to address this pressing issue and provide a robust layer of defense for programmable logic controllers (PLCs).

One of the primary challenges the authority faced was the inability to authenticate the identity of operators while maintaining the functionality of the PLCs. This lack of authentication posed significant security risks, as unauthorized individuals could potentially gain access to sensitive systems and cause disruptions or damage.

Furthermore, the water authority lacked traceability for operations performed by technicians and third-party contractors. Without a proper audit trail, it became difficult to monitor and investigate any suspicious activities or unauthorized changes made to the PLCs. This lack of visibility and accountability created a significant gap in the authority's security posture.

To address these challenges, the water authority sought a solution that could provide robust authentication mechanisms, ensuring that only authorized personnel could access and modify the PLCs. Additionally, they required a system that could track and trace all operations performed on the PLCs, providing a clear audit trail for increased transparency and accountability.

The Solution

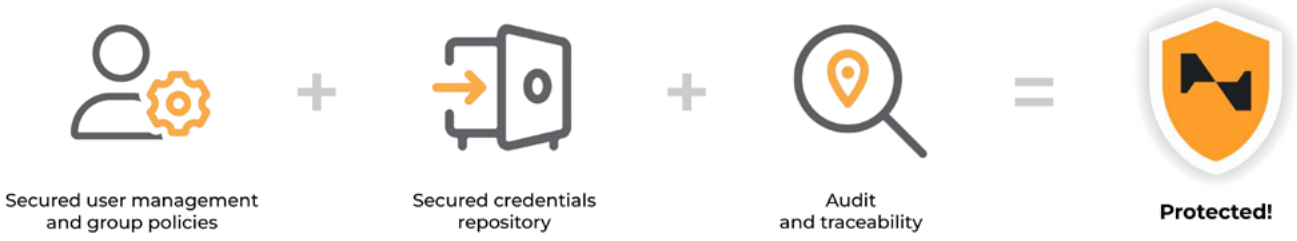
Implementing Multi-Factor Authentication (MFA) for Enhanced PLC Security

NanoLock's solution was chosen for its comprehensive approach to securing PLCs, as well as its ability to address the unique challenges faced in complex OT environments. NanoLock's implementation of Multi-Factor Authentication (MFA) at the PLC level was a key factor in the decision, as it provides a robust layer of security across multi-vendor environments, including legacy devices. This was crucial for the water authority, given its diverse range of PLCs from various vendors. Furthermore, NanoLock's solution seamlessly integrates with existing systems, ensuring a smooth deployment and minimal disruption to operations.

Results And Benefits

- Applying device level protection to new & legacy devices
- Audit trail from the OT floor
- Multi-vendor management system
- Fast & easy to deploy
- Maintaining business continuity

NanoLock OT Defender was initially deployed at a verification lab, mirroring the water authority's real-world deployment scenarios. A key requirement for the authority was compatibility with Schneider Electric PLCs. Being a multi-vendor solution, NanoLock OT Defender met the requirements and integrates with all PLC types.



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

nanolock