txOne networks

Customer Story

Secure production of sensors :

# Leading sensor manufacturer enhances its OT security with TXOne Networks

**Preventing breakdowns and downtime: This is one of the core tasks of Operational Technology (OT) specialists. Until now, this has been a difficult task, but one that can be accomplished with a modern machine park and sufficient experienced personnel. However, the integration of IT and OT, with machines now networked and often connected to the internet, has transformed this task into a huge challenge. Monitoring the complexity of the connection flows in every OT system has become impossible without technical and organizational tools, especially due to the rise in attacks - both internal and external.**

**An OT security solution was to be introduced at a world-leading global manufacturer of sensors and connected components. Their products are used in industrial communication, display lighting and power supply, among others. The use cases span large industries such as the automotive industry, renewable energies, logistics, and ship automation.**

**From the OT perspective, the machinery is highly diversified due to different manufacturing processes and fields of application, including systems from both market leaders and in-house machines for special sensors. The latter are manufactured in a separate department for special machine construction, which includes simple machines, in-house robots, or production lines.**

## The situation

The central security policy required the company to run an anti-virus scanner on all devices with processors. While the company used a single manufacturer for endpoint security across IT, existing AV solutions in production were outdated and unsupported by the software manufacturer, failing to meet compliance requirements.

Classic SaaS solutions from the providers couldn't fulfill the directive, leading to a search for a new consolidated solution that could be used across the board. One of the primary challenges, and the main reason for choosing an OT-native solution, is the diverse nature of production infrastructures.

Outdated operating systems, latency sensitivity and the focus on availability and reliability are crucial in OT environments.

Initial contact with TXOne Networks was established in April 2022, when the OT security department was being set up to complement the IT security department's central SOC.

To meet the OT-specific challenges, it was clear that a product precisely tailored to the OT environment was needed. The company decided to test the endpoint security solution provided by TXOne Networks.

## Solution approach: OT endpoint security

The solution was extensively tested on several laboratory systems and later on productive infrastructure. Key criteria included support for older operating systems like Windows 2000/Windows XP, as well as newer ones, low resource consumption (CPU/RAM), and simple management of agents via a central console (agent and signature updates, policy handling, etc.).

While the support of the operating systems was already known in advance, TXOne's solution excelled in resource efficiency and administration. Even on resource-limited systems, Endpoint Security ran smoothly without altering system behavior. The centralized and decentralized manageability of agents allowed comfortable operation.

After successfully testing TXOne's endpoint product, the OT security department decided to replace existing security products starting October 2022. The switch was completed by year-end, with the scanner now running on many OT devices.

Sensor production is managed via Microsoft Azure production cloud, where the data is processed using SAP, among other tools. All machines and systems access this and store their production data. Within a few months, the changeover resulted in improved management. Warning messages from the OT are sent via Syslog Forwarding to the SOC, and, if they reach a certain criticality are forwarded to the OT security team. Most events are therefore first analyzed and checked by the IT security experts and only sent to the OT colleagues once they have been filtered. Critical alerts are forwarded to the OT security team, which further investigates via the management interface, sometimes directly in the production halls to examine the affected machines and systems on site. They ensure compliance and security by addressing any issues found, taking the necessary steps to ensure the security of the entire production environment.

## The result

Until now, existing solutions failed to secure production machines or meet compliance due to outdated software and a lack of support from software manufacturers. TXOne provided a simple and clever solution, securing systems and ensuring compliance. The company's OT security specialists gained more insight into their OT on all systems (new and old), understanding more precisely what happens on the individual devices beyond standard production processes. SOC-to-OT security messages are now clearer, with an improved level of detail simplifying criticality assessments. Thus, the OT security team achieved its goal of fully securing a networked production environment.

### About TXOne Networks

TXOne Networks offers cybersecurity solutions that ensure the reliability and safety of industrial control systems and operational technology environments. TXOne Networks works together with both leading manufacturers and critical infrastructure operators to develop practical, operations-friendly approaches to cyber defense. TXOne Networks offers both network-based and endpoint-based products to secure the OT network and mission-critical devices using a real-time, defense-in-depth approach. Learn more at www.txone.com.