txOne networks | Keep the Operation Running

Security Compliance for Machine Builders

The new security regulations in the EU will change the competitive landscape of machine builders. TXOne Networks aims to help you stay ahead in this dynamic world, with our industry-proven OT cybersecurity expertise.

What to know about Regulation (EU) 2023/1230?

The European Parliament and Council of the European Union have introduced Regulation (EU) 2023/1230, effective as of July 19, 2023. This regulation updates the Machinery Directive from 2006, expanding its product scope and modifying conformity assessment procedures. Products must now comply with specific security requirements outlined in the regulation, with full compliance required by January 14, 2027.

What is the relationship between Regulation (EU) 2023/1230 and the CRA for machine builders?

The European Union has introduced the Cyber Resilience Act (CRA), setting new cybersecurity standards for all digitalized products, including IoT devices and mechanical equipment. This act not only complements the existing Regulation (EU) 2023/1230 by covering "products with digital elements," but also establishes mandatory cybersecurity requirements for the lifecycle of both hardware and software. Additionally, the CRA ensures that products, especially those with a CE label, meet fundamental cybersecurity standards and are supported with at least five years of security updates, enhancing their long-term usability.

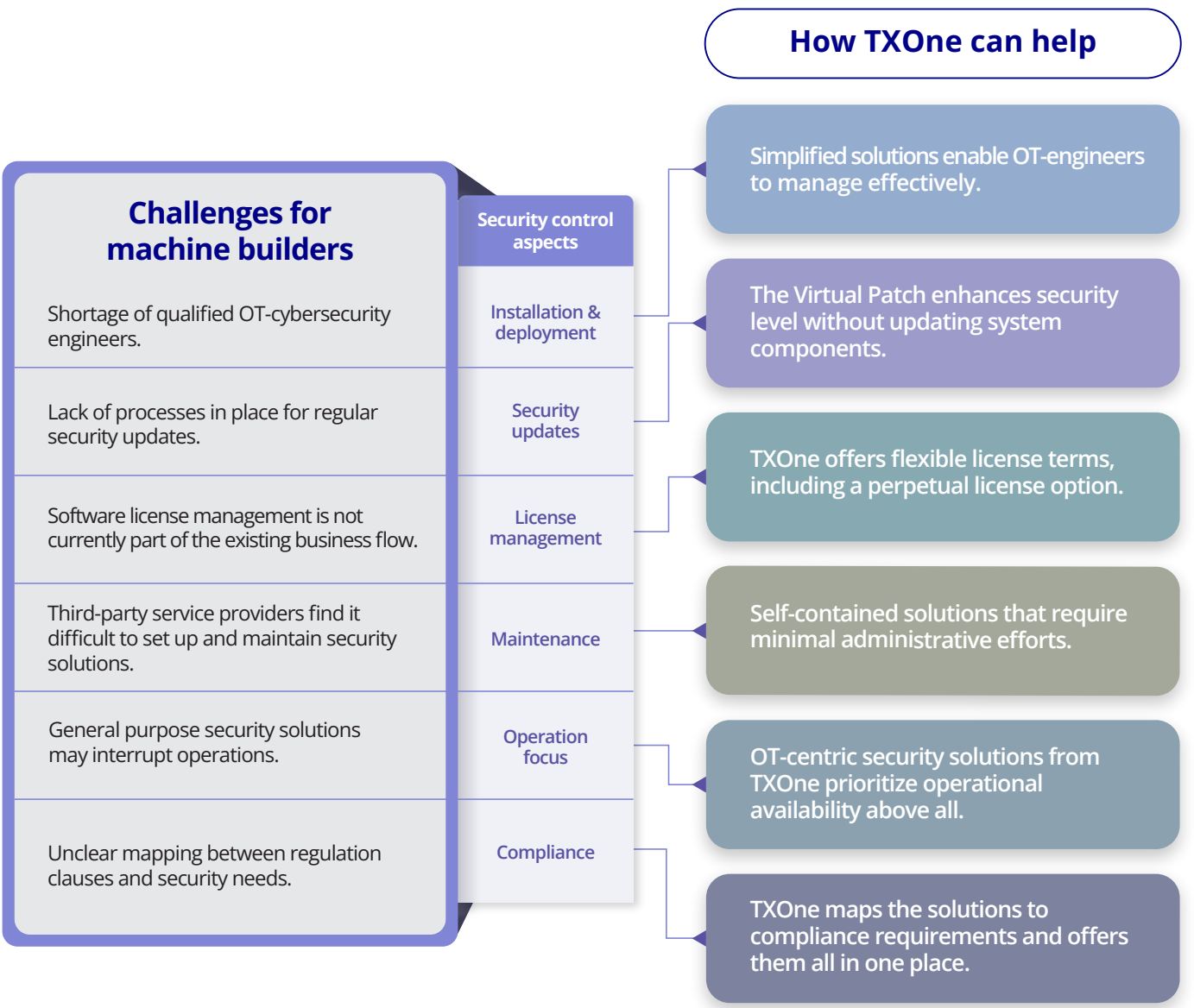
New security requirements highlights

The internal and external communications of the machine do not lead to a hazardous situation.

The hardware and software inside the machine should be adequately protected against accidental or intentional corruption.

The machine shall collect evidence of legitimate or illegitimate interventions.

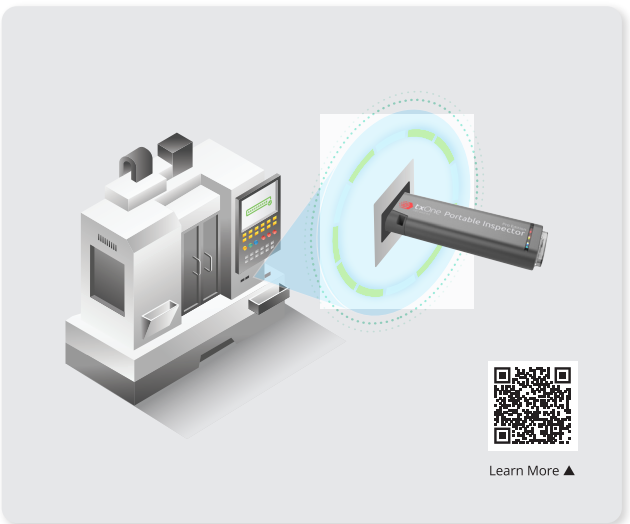
Overcome the challenges with TXOne Networks



TXOne solution portfolio for machine builders

Element: Security inspection for a machine

Before handing over the machine, machine builders can run a malware scan and generate a comprehensive security report confirming its health status and including a list of all the software installed.



Stellar: Battle against malware and keep business continuity

From small to large machines operated by Windows operation systems, the most efficient way to protect it is with this endpoint anti-malware software. It comes in two modes: protection mode scans everything around the machine, while lockdown mode creates a trusted application list to block all unauthorized applications.

Edge: Secure the network against accidental or intentional security incidents

Network security appliances are widely used. For any machine managed remotely, an OT-centric firewall ensures a secured connection. IPS (Intrusion Prevention System) appliances can block malicious packets and insecure network commands. A small form factor can be embedded as part of the machine, while the larger ones can protect multiple machines simultaneously.

Learn More ▲