txOne networks

Customer Story

Protecting Critical Infrastructure: How Valmet Enhances Industrial Control System Security with TXOne Networks

Faced with strict cybersecurity demands and complex industrial environments, Valmet needed robust protection that wouldn't compromise uptime. Choosing TXOne Networks allowed Valmet to seamlessly embed OT-native cybersecurity into their automation solutions – boosting customer confidence, simplifying regulatory compliance, and setting new standards for industrial control system security.

The Situation

Valmet is a Finland-based global leader in industrial automation and machinery, serving critical sectors like pulp and paper production, power generation, and process industries. The company employs approximately 19,000 professionals worldwide and maintains a strong presence in Germany, where many of its customers operate essential national infrastructure. Valmet's automation technology – including its flagship distributed control system, Valmet DNAe – forms the operational backbone of major industrial plants, from paper mills to power plants, ensuring stable and continuous production processes.

In recent years, cybersecurity emerged as a defining challenge. Valmet's customers, especially those classified as critical infrastructure operators, faced increasingly stringent cybersecurity regulations such as the EU's NIS2 directive. These regulations require vendors like Valmet to deliver automation systems with built-in, advanced cybersecurity capabilities.

Valmet

"With TXOne, we can deliver OT-native cybersecurity tailored to the specific requirements of industrial environments."

Teemu Kiviniemi
Solution Manager
OT Cybersecurity
at Valmet

"Our customers operate machines critical for entire countries – like power plants. They trust us to ensure these systems are secure," explains Teemu Kiviniemi, Solution Manager, OT Cybersecurity at Valmet, and continues: "With TXOne, we can provide OT-native cybersecurity that can handle the unique constraints of industrial environments."

Industrial control systems, unlike IT systems, can't simply be updated or rebooted without careful planning. Some of Valmet's customers run older equipment that can't receive patches regularly, leaving potential security gaps open. Because of this, Kiviniemi describes patch management as the biggest single problem in OT cybersecurity. If security measures are insufficient or inappropriate – such as IT solutions forcing unexpected reboots – it could cause catastrophic downtime. "Imagine a security solution that restarts at the wrong time: a power plant might shut down, causing widespread outages and big parts of Germany would be without energy," Kiviniemi emphasizes.

Valmet needed a solution specifically designed for the industrial environment – one that would reliably protect legacy systems and offer continuous, automatic protection without risking operational interruptions.

The Transition

Recognising these critical requirements, Valmet began evaluating potential cybersecurity partners. Previously relying on traditional IT-based security products, the team quickly recognised that these tools were no longer adequate for industrial settings. "There's a clear difference between IT and OT security. Typically IT tools used in OT just detect threats, but we needed something designed specifically for operational technology that actively prevents attacks in real-time," Kiviniemi says.

The right partner emerged when TXOne Networks reached out directly to Valmet. From the initial conversation, Valmet saw TXOne as different from competitors. TXOne offered solutions developed explicitly for OT environments, addressing precisely the constraints and risks Valmet faced. After initial discussions, Valmet decided to thoroughly evaluate TXOne's full product portfolio.

Testing was rigorous and comprehensive, lasting nearly two years. Valmet and TXOne's engineering teams collaborated closely to integrate the cybersecurity technology into Valmet's automation systems. Challenges inevitably arose during implementation – some technical adjustments and refinements were necessary – but TXOne's team responded quickly and proactively. "We encountered typical integration issues, but TXOne supported us every step of the way, making necessary adjustments promptly," Kiviniemi explains. "We treat TXOne's products as if they were our own; if something doesn't work immediately, we fix it together."

Valmet ultimately integrated a range of TXOne solutions, including the Stellar endpoint protection suite, EdgeIPS network-level defenses, and tools offering virtual patching capabilities. This last capability was particularly crucial: virtual patching allowed Valmet to shield systems from vulnerabilities at the network level until the next scheduled maintenance outage. This meant that even if a customer couldn't patch immediately, their systems remained secure.

Equally important, Valmet made sure cybersecurity became seamlessly embedded into their existing service infrastructure. They trained their global network of service engineers in deploying and managing TXOne's cybersecurity technology. According to Kiviniemi, Valmet does not need a separate cybersecurity team: "The same engineers who maintain and install the control systems can manage cybersecurity. It's all integrated, transparent, and easy."

The Result

Today, many Valmet automation solutions come equipped with built-in, OT-native cybersecurity powered by TXOne Networks. The impact has been significant: customers no longer worry about unprotected vulnerabilities or operational interruptions from IT-style security updates. Continuous cybersecurity protection is now simply part of the standard Valmet offering.

Operational continuity – a top priority for critical infrastructure operators – is ensured through solutions that guard legacy systems against threats even during prolonged patching delays. "If a vulnerability emerges, our customers know their system remains safe until the next scheduled maintenance. That's peace of mind," says Kiviniemi.

This strategic move has substantially strengthened Valmet's market position. Customers have responded enthusiastically, increasingly viewing Valmet not just as a machinery provider, but as a trusted cybersecurity partner. Regulatory compliance, especially regarding NIS2 and similar directives, has become easier, since customers now receive automation systems already compliant with stringent cybersecurity requirements. This compliance is integral rather than an add-on, significantly reducing complexity and enhancing overall protection.

The integration of TXOne's technology has opened new avenues for Valmet. The company now offers dedicated cybersecurity services, from risk assessments and remote monitoring to comprehensive incident response. These services have created new business opportunities, demonstrating Valmet's proactive stance in industrial cybersecurity.

Valmet's approach represents a pivotal step forward in how automation providers handle cybersecurity. The proactive integration of TXOne's solutions into Valmet's automation portfolio has raised the standard across the industry. "Cybersecurity is a team sport," Kiviniemi concludes. "With TXOne, we've shown that securing critical infrastructure can be done proactively, comprehensively, and seamlessly – without compromising operational performance."

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.