OTORIO

Maunfacturing

Secure Your Manufacturing Operations with OTORIO's Tailored Risk Management Solutions

Ensuring Cyber Security Safety in a Dynamic Manufacturing Environment

Manufacturing is the one of the most targeted sector by cyberattacks

The manufacturing industry is undergoing significant changes, with a focus on improving customer engagement and satisfaction through flexible business models. To achieve higher levels of operational efficiency and availability, new technologies are being increasingly used. These technologies ensure on-time delivery of critical raw materials according to customer preferences and enable predictive maintenance analytics. Digital transformation is not limited to production but extends to connecting systems throughout the supply chain, transportation, and end-user consumption.

Although manufacturing plants were previously considered cyber-secure due to being air-gapped, today's increased interconnectivity and data sharing between systems and networks, expands the attack surface for both manufacturers and consumers and increases risk. According to the World Economic Forum (WEF), the manufacturing sector has been the most targeted industry by cyberattacks. A report has shown that 98% of organizations have a connection to a third party that has been breached. As a result, manufacturing security leaders need to adopt an enterprise-wide approach to security risk management across various business domains, such as OT, IT, executive management, risk governance, and compliance. Security leaders need to take into account operational context and its business impact to effectively manage and mitigate risk while involving domain owners in the overall operational security lifecycle.

> "We tested several OT security solutions in one of our operation sites for a minimum of 40 days and found that RAM² from OTORIO was significantly better than the other solutions tested. It gave us a clear global overview of the OT assets and risks which is exactly what we needed."
>
> Director OTS,
> Manufacturing company

Ensuring Operational Resilience

OTORIO's industrial-native OT cyber risk management platform is tailored to the needs of the manufacturing industry, whether it pertains to process or discrete manufacturing. Our solutions are designed and built from the ground up with safety, reliability and resilience of operations as top priority.

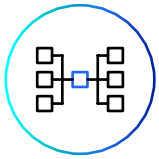
OTORIO's platform merges **cyber and physical systems into one source of truth.** This provides different domain owners with an accurate and common viewpoint of the business-related cyber risks in their operational environment, enabling better security management decision making while maximizing the ROI from operational security controls and processes. Starting with **consolidated and advanced visibility of all operations (IT-OT-IIoT) assets,** the platform **provides operational context,** and impact-driven prioritization of the most critical risks in the plant. Additionally, OTORIO's solution supports common industry security standards and regulations by providing **automated, out-of-the-box asset and site-level compliance assessment.** This assessment is based on a recognized framework and best practices, enabling you to govern policy-based OT security frameworks and comply with industry regulations. The concise compliance and risk assessment reports include clear, **actionable mitigation steps tailored to the unique operational environment,** internal processes and unique manufacturing characteristics. OTORIO's solution leverages existing security controls while reducing noise and alert fatigue in the manufacturing environment.

A unified, actionable framework for operational security practitioners

The platform bridges the gap between the different domains, demonstrating value to the different functions:

CISO's are able to govern operational security with one source of truth and provide risk reports for decision-making regarding investments, insurance and compliance.

Security analysts benefit from proactive automated detection, improved mean time to detect and respond, and better collaboration with operational process engineers.



Operation engineers get a consolidated view of their asset inventory and security posture, along with prescriptive mitigation steps that empower them to proactively reduce cyber risk to ensure safety with maximum production availability (zero downtime).

Improved meantime to detect

Raw asset information
PLCs, RTUs, Sensors

Security systems
EDR, Firewall, NAC, AD, SRA

Industrial solutions
OPC, DCS, Historian

Logs
Windows event logs, Servers, HMI

Network monitoring
IDS, Traffic, Netflow

- **Improved MTTD** (Mean Time To Detect)
- **Improved MTTR** (Mean Time To Response) with automated mitigation steps
- **OT** context-based **prioritization**
- **Risk based** approach by adding impact levels for production precesses and/or assets

Automate and simplify the OT risk management process

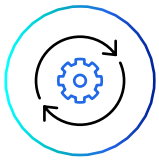
OTORIO's platform empowers manufacturing companies to protect their interconnected systems in the operational environment, while ensuring operational safety using OTORIO's context risk-based prioritization and prescriptive mitigation playbooks, tailored for the manufacturing industry. It delivers centralized comprehensive visibility of manufacturing legacy and modern systems, DCS, control access, etc., and continuously monitors cross-domain data sources and performs out-of-the-box compliance standards, such as NIST 800-82 and IEC 62443.

Enable safe digitalization and modernization

- Protecting interconnected modern equipment and legacy systems, without compromising on the safety of operations.
- Providing centralized risk overview across the different business domains: OT, IT, Executive management, Governance risk and compliance.
- Automated visibility, orchestrating data from existing security controls.
- Reducing noise and alert fatigue.
- Preventing unauthorized access that may result in shutdown of systems, late delivery of essential raw materials and financial loss, or even environmental damage and threat to human life.

Prevent disruption and ensure operational availability

- Assessing network segmentation to ensure that OT manufacturing systems can continue to operate safely if an IT system has been compromised, vice versa.
- Securing the increasing attack surface with improved access control against unauthorized manipulation of manufacturing systems.
- Empowering OT security teams to prevent successful ransomware attacks with prescriptive playbooks for risk mitigation and hardening of assets.
- Impact-driven prioritization of risk mitigation actions.



Improve OT security operations efficiency

- Automating OT Security operations.
- Continuously monitors cross-domain data sources to identify potential breaches.
- Tailored to network architecture and capable of covering systems and vendors with direct impact on the manufacturing supply chain, process, transportation and the output consumed by the customers.
- Automated network segmentation assessment.
- Out-of-the-box compliance audit for ever-changing regulation and standards (e.g., NIST).
- Implementing a risk-based approach to reduce the risk of exploitation of unpatched systems.
- Empowering security practitioners to proactively reduce risk, without compromising safety.

Summary

The manufacturing industry is adopting new technology and agile business models to improve customer engagement and operational resilience. However, this increased interconnectivity and data sharing also increases the risk of cyber attacks, requiring manufacturing security leaders to take an enterprise-wide approach to risk management. OTORIO's industrial-native OT cyber risk management platform is tailored to meet the unique needs of the manufacturing sector, providing consolidated visibility of all operational assets, business impact-driven risk prioritization, and prescriptive mitigation steps. This solution bridges the gap between different domains and functions, enabling manufacturing companies to confidently digitize processes without compromising safety, reliability, or efficiency.

About OTORIO

OTORIO's industrial-native OT security platform enables industrial organizations to achieve an integrated, holistic security strategy. Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. OTORIO's global team brings the extensive mission-critical experience of top nation-state cyber security experts combined with deep operational and industrial domain expertise.

CN 160523