# Securing Manufacturing Without Risking Productivity

Manufacturing environments are often complicated ecosystems of interconnected operational technologies (OT) and IT devices — OT to automate production, and IT to manage the OT systems. Due to digitization, IT devices can make up half of the modern manufacturing environment.

Tenable OT Security, formerly known as Tenable.ot, helps you understand the asset makeup of your entire factory floor, providing holistic coverage and security across your IT and OT environments. With technology purposely designed to be safely used on OT devices, Tenable OT Security allows you to maintain productivity while securing your systems.

## Cybersecurity Challenges In Manufacturing

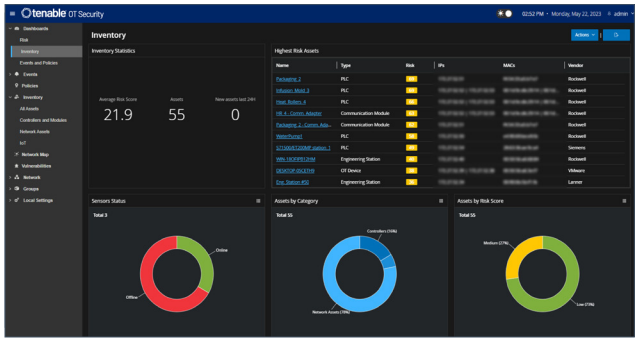
- **An Expanding Attack Surface:** With interconnected devices, sensors and systems, there are more potential vulnerabilities that can be exploited, increasing the risk of cyber attacks.
- **Vulnerabilities in Legacy and Cyber-Physical Systems:** Many manufacturing facilities still rely on legacy systems and equipment that can lack modern security controls. Integrating these systems with new digital technologies can create compatibility issues and expose vulnerabilities that cyber attackers can target.
- **Insider Threats:** Insiders with malicious intent or those who inadvertently compromise security practices can pose a significant risk to manufacturing operations, resulting in unplanned downtime.
- **Evolving Threat Landscape:** As manufacturers adopt digital technologies, they become targets for a wide range of cyber threats, including ransomware, phishing attacks, industrial espionage, and nation-state attacks.


## Requirements to Secure IT/OT on the Factory Floor

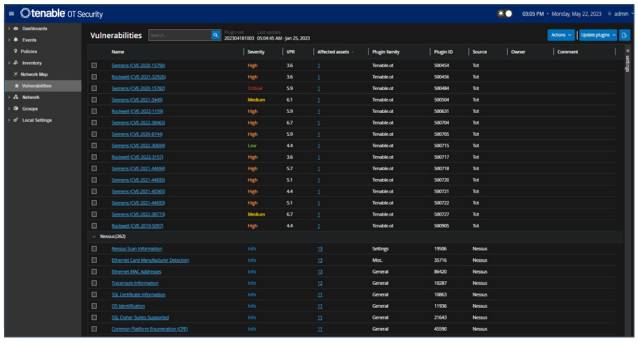
- ☐ **Asset Inventory:** Visibility of IT and OT devices and their model, family, type, firmware version, OS version, hardware version and serial number is crucial for maintaining a proper inventory of the ever-growing attack surface across your manufacturing environment.
- ☐ **Vulnerability Management:** An effective cybersecurity program requires proactive approaches such as vulnerability management, helping you identify weaknesses in both modern and legacy systems across manufacturing environments that can be exploited through unauthorized access.
- ☐ **Threat Detection:** Intrusion-detection capabilities in a manufacturing environment are essential for early threat warning, insider threat discovery and malware detection, and can aid in reducing the likelihood of unplanned downtime.
- ☐ **Configuration Management:** As the threat landscape continues to evolve, it is vital to monitor for changes in device configurations. Human error or possible malicious activity can cause critical configurations to change, resulting in unplanned downtime and potentially compromising the safety and productivity of the manufacturing ecosystem.

# Tenable OT Security for Manufacturing Operations

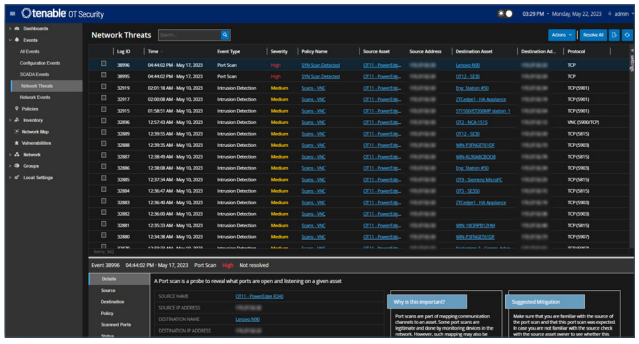
Tenable OT Security is designed to address the unique needs of organizations running OT, such as manufacturers — from understanding and maintaining inventory of systems on the shop floor, to enabling vulnerability and threat detection of cybersecurity incidents in real time — all while maintaining productivity.



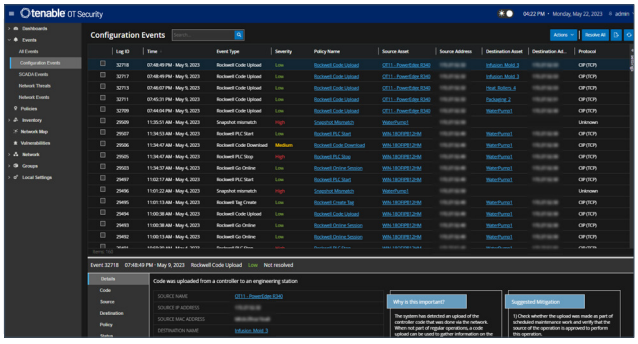

**In-Depth Asset Visibility:** By delivering unmatched visibility of IT and OT devices across your global sites and their assets — from Windows servers to PLC backplanes — Tenable OT Security provides you with a centralized view to monitor, manage and secure your entire infrastructure, including potential entry points attackers may exploit.




**Risk-Based Vulnerability Management:** Tenable OT Security's risk-based vulnerability assessment identifies security "soft spots." By using a combination of the Asset Criticality Rating (ACR) and the Vulnerability Priority Rating (VPR) you can prioritize mitigation and remediation efforts of the vulnerabilities with the most risk.




**Threat and Anomaly Detection**: Tenable OT Security's multi-detection engine identifies policy violations and anomalous behaviors, and tracks signatures for potential high-risk events. Alerts include detailed information for a comprehensive audit trail, enabling faster incident response and thorough forensic investigations.




**Device Configuration Monitoring**: Tenable OT Security captures a complete snapshot of device configuration, firmware version, software updates, ladder logic, diagnostic buffer and tag structure, and alerts you when changes have been made to these configurations, letting you roll back devices to their last known good state.

## About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

**For More Information:** Please visit our Tenable OT Security page
**Contact Us:** Please email us at sales@tenable.com or visit tenable.com/contact