◯ tenable | Data Sheet

Tenable OT Security

Close OT exposure with the unified security solution for converged OT/IT environments

Product overview

The convergence of operational technology (OT) and IT systems, alongside the rapid adoption of IoT technologies, is transforming industries. This convergence optimizes production processes, drives innovation, and increases efficiencies through real-time data analysis and communication across systems. However, it also expands the attack surface, introducing new vulnerabilities and attack vectors. As OT and IT networks become more interconnected, the potential for cyber threats grows, demanding robust security measures to protect against cyber attacks and ensure the integrity and reliability of critical operations.

Tenable OT Security delivers visibility, security, and control to industrial environments, critical infrastructure, building management systems, and more. It reduces business risk and protects organizations from attacks across today's rapidly converging OT/IT environment. Using a patented hybrid discovery approach to safely gain visibility into OT, IT, and IoT devices and cyber-physical systems, Tenable OT Security delivers a thorough asset inventory with deep situational awareness, all within a single interface. From vulnerability management and threat detection to configuration control and reporting, Tenable OT Security enables organizations to prioritize actions and foster collaboration between their OT and IT security teams to close their exposure.

Where we work

- Discrete manufacturing
- Oil and gas
- Chemical and petrochemical
- Water utilities
- Pharmaceutical

- Power and energy
- Aerospace
- Building automation
- Food and beverage
- Transportation

Key benefits

Know every OT/IT asset in your converged environment

→ **Gain unified visibility** across converged OT/IT environments. Eliminate blind spots and collapse siloes where lateral threats can traverse OT, IoT and IT.

→ **Uncover OT and IT asset vulnerabilities** and triage potential threats before they can become exploits. Prioritize remediation and reduce exposures based on vulnerability severity and impact.

Expose the lethal gaps that put your organization at risk

→ **Supercharge insights** by combining network-only monitoring with advanced detection capabilities to discover policy violations, detect anomalous behaviors, and track high-risk signatures across your attack surface.

→ **Investigate configuration changes** with a comprehensive audit trail to determine who made changes, what was changed, why the change was made, and the resulting outcome.

Close priority exposures with confidence

→ **Eradicate exposures** with cross-asset vulnerability priority ratings, guided remediation, and advanced configuration management.

→ **Take control** of your converged environment and implement strategic defenses to prevent lateral threat movement across OT and IT domains.

Key capabilities

Comprehensive asset visibility

Tenable OT Security automates asset discovery and creates visual asset maps for a unified view of network assets, including workstations, servers, HMIs, historians, PLCs, RTUs, IEDs, and IoT devices. Connector engines specifically target applications that manage IoT devices and ensure complete inventory. Manage your assets by tracking their firmware and OS versions, internal configuration, applications and users, serial numbers, and backplane configuration for both OT and IT-based equipment.

Advanced threat and anomaly detection

Tenable OT Security leverages an advanced multi-detection engine that identifies network anomalies, enforces security policies, and tracks local changes on devices with high-risk events — all with granular precision. With device-based threat detection, organizations can identify issues on dormant devices to detect and mitigate risky events in OT/IT environments. Users have the flexibility to customize and fine-tune detection methodologies to fit the specific needs of their environment. Threat response capabilities are enhanced with context-rich alerts and a comprehensive audit trail for incident response and forensic investigation.

Configuration change tracking

With Tenable OT's Configuration Control, you can track malware and user-executed changes over your network or directly on a device. Tenable provides a timeline of device configuration changes, including specific ladder logic segments, diagnostic buffers and tag tables. Establish a backup snapshot identifying the "last known good state" for faster recovery and compliance with industry regulations.

Risk-based OT/IT vulnerability management

Tenable OT Security utilizes a sophisticated Vulnerability Priority Rating (VPR) scoring model to assess vulnerabilities based on their context and potential impact, allowing for prioritized remediation efforts. Each asset is evaluated with comprehensive data, including firmware versions, proprietary research, and insights into asset relationships, exposures, entitlements, and attack paths. This equips teams with the actionable intelligence needed to make informed decisions and expedite mitigation measures.

Automated asset management

Tenable OT Security simplifies asset management with enhanced visibility and contextualized insights. Hybrid discovery with natural language queries provides non-disruptive inventory management, allowing for rapid identification of assets and their critical exposures. Asset mapping reveals intricate relationships between physically connected and communicating devices to help build robust defense strategies.

Maximize existing security investments

Tenable OT Security is designed to adapt to and work seamlessly within diverse infrastructures, integrating with the rest of the Tenable product portfolio as well as leading IT security tools such as SIEM, SOAR, and next-generation firewalls. Tenable also shares information with configuration management databases, asset inventory platforms, change management tools and more. Our RESTful API is designed to facilitate extraction of data to proprietary tools, giving a more coherent view of the IT and OT environments in a unified view.

About Tenable

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for more than 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us

Please email us at sales@tenable.com or visit tenable.com/contact.

072924