tenable®

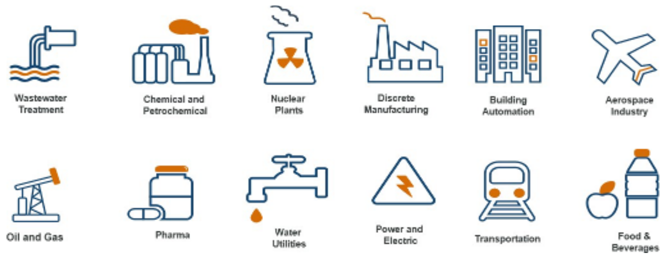
DATA SHEET

TENABLE.OT™

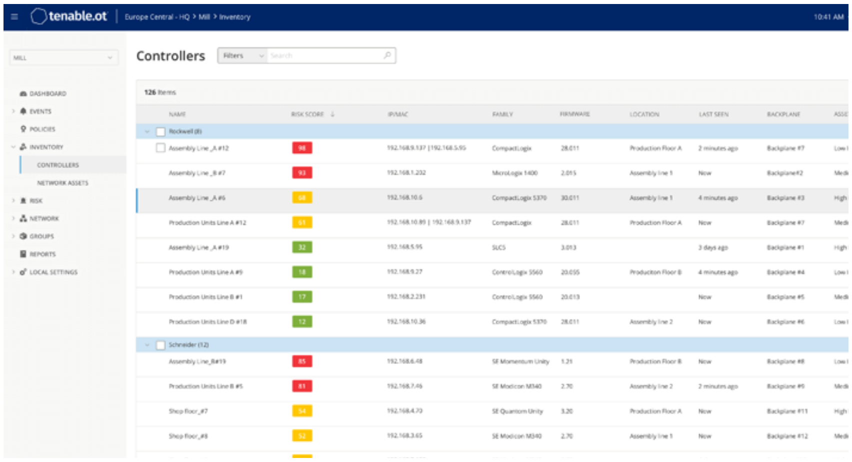
PRODUCT OVERVIEW

At the heart of every industrial facility is a network of industrial control systems which is comprised of purpose-built controllers. Sometimes known as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs), these controllers are dedicated industrial devices that serve as the bedrock of all industrial processes. Today's sophisticated Operations Technology (OT) environments have a large attack surface with numerous attack vectors. Without complete visibility, security and control across the converged IT and OT, the likelihood of getting attacked is not a matter of 'if'; it's a matter of 'when'.

Tenable.ot™ protects industrial networks from cyber threats, malicious insiders, and human error. From complete visibility across the entire attack surface to threat detection and asset tracking, vulnerability management, and configuration control, our Industrial Control System (ICS) security capabilities maximize the safety and reliability of OT environments. The solution delivers deep situational awareness across all sites and their respective IT and OT environments.



Programmable Logic Controllers (PLCs) are core to the operations of critical infrastructure. Critical Infrastructure continues to expand to new businesses and disciplines.



Controllers

126 Items

NAME	RISK SCORE	IP/MAC	FAMILY	FIRMWARE	LOCATION	LAST SEEN	BACKPLANE	ASS
Rockwell (8)								
Assembly Line _A #12	98	192.168.9.137 |192.168.5.95	CompactLogix	28.011	Production Floor A	2 minutes ago	Backplane #7	Low
Assembly Line _B #7	93	192.168.1.202	MicroLogix 1400	2.015	Assembly line 1	Now	Backplane#2	Medi
Assembly Line _A #6	68	192.168.10.6	CompactLogix 5370	30.011	Assembly line 1	4 minutes ago	Backplane #3	High
Production Units Line A #12	61	192.168.10.89 | 192.168.9.137	CompactLogix	28.011	Production Floor A	Now	Backplane #7	Medi
Assembly Line _A #19	32	192.168.5.95	SLC5	3.013		3 days ago	Backplane #1	High
Production Units Line A #9	18	192.168.9.27	ControlLogix 5560	20.055	Producton Floor B	4 minutes ago	Backplane #4	Low
Production Units Line B #1	17	192.168.2.231	ControlLogix 5560	20.013		Now	Backplane #5	Medi
Production Units Line D #18	12	192.168.10.36	CompactLogix 5370	28.011	Assembly line 2	Now	Backplane #6	Low
Schneider (12)								
Assembly Line_B#19	85	192.168.6.48	SE Momentum Unity	1.21	Production Floor B	Now	Backplane #8	Low
Production Units Line B #5	81	192.168.7.46	SE Modicon M340	2.70	Assembly line 2	2 minutes ago	Backplane #9	Medi
Shop floor_#7	54	192.168.4.70	SE Quantom Unity	3.20	Production Floor A	Now	Backplane #11	High
Shop floor_#8	52	192.168.3.65	SE Modicon M340	2.70	Assembly line 1	Now	Backplane #12	Medi

KEY BENEFITS

- **Gain Full Visibility**
  across converged IT/OT operations. Eliminate blind spots which can harbor lateral threats that can traverse IT and OT.

- **Detect Network and Device Threats**
  that impact industrial and critical operations by leveraging multiple detection methodologies. Proactively threat hunt by using "Attack Vector" technology.

- **Identify and Track IT and OT Assets**
  Gain deep situational awareness into the operation and state of each and every device.

- **Reduce Risk**
  by identifying and triaging vulnerabilities and potential threats before they become exploits and impact industrial operations.

- **Track Configuration**
  changes with full audit trail capabilities. Determine whom, what and why changes were made as well as the result of those changes.

KEY CAPABILITIES

Converged Visibility

Tenable.ot provides complete enterprise visibility by integrating with the rest of the Tenable product portfolio as well as leading IT security tools, such as SIEM, SOAR, next generation firewalls, diode based firewalls and more. The platform also shares information with CMDB, asset inventory platforms, change management tools and more. Our RESTful API is designed to facilitate extraction of data even to proprietary tools, giving a more coherent view of the IT & OT environments in a single pane of glass.

Threat Detection

Tenable.ot detects and alerts about threats coming from external and internal sources - whether human or malware based. Leveraging multi-detection methodologies Tenable.ot identifies anomalous network behavior, enforces network security policies and tracks local changes on devices. Additionally, Tenable.ot can perform device based threat detection which can identify security issues on dormant devices that do not communicate over the network and before attack proliferation. This enables organizations to detect and mitigate risky events in OT environments. Context- aware alerts include extended information and a comprehensive audit trail for fast incident response and forensic investigations.

Asset Tracking

Tenable.ot's automated asset discovery and visualization capabilities provide a comprehensive up-to-date inventory of all network assets, including Workstations, Servers, HMIs, Historians, PLCs, RTUs, IEDs and network devices. Active device scanning capabilities enable the discovery of devices in the network's "blind" zone and local-only data. The inventory contains unparalleled asset information depth – tracking firmware and OS versions, internal configuration, running software and users, as well as serial numbers and backplane configuration for both IT and OT based equipment.

Vulnerability Management

Drawing on our comprehensive and detailed asset tracking capabilities, Tenable.ot generates risk levels for every asset in your ICS network. These reports include risk scoring and detailed insights, along with mitigation suggestions. Our vulnerability assessment is based on various parameters such as firmware versions, relevant CVEs, proprietary research, default passwords, open ports, hotfixes installed and more. This enables authorized personnel to quickly identify new vulnerabilities and efficiently mitigate risk factors in the network.

Configuration Control

Tenable.ot tracks and logs all configuration changes executed by a user or by malware, whether over the network or directly on the device. It provides a full history of changes made to device configurations over time, including granularity of specific ladder logic segments, diagnostic buffers, tag tables and more. This enables users to establish a backup snapshot with the "last known good state" for faster recovery and demonstrate compliance with industry regulations.

LEVERAGE TENABLE'S "ECOSYSTEM OF TRUST"

Leverage your existing security investments. Tenable.ot fully integrates with Tenable.sc and Tenable.io for full visibility, security and control across your converged operations. Tenable.ot works in conjunction with Tenable.ad to identify Active Directory misconfigurations and threats which can result in ransomware attacks in OT environments. Tenable.ot also has full integration with IT security technologies you already use such as IT service management, next-generation firewalls (NGFW) and security information and event management (SIEM) vendors.

With integration and collaboration across the Tenable product line as well as leading IT and OT security systems, you'll gain full situational awareness needed to secure operations from today's IT and OT threats.

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 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 more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact