SOLUTION OVERVIEW

Tenable.ot for Check Point

Protecting OT Assets and Critical Infrastructure

Business Challenge

Operational technology (OT) systems and industrial control security (ICS) networks lack visibility and security controls.

With the rise of external and internal threats that target OT infrastructure, you need an approach that provides real-time visibility and security while addressing unique technical and operational requirements of these networks.

Tenable.ot provides detailed information on each discovered asset, such as IP address, device type, vendor and model and is delivered to Check Point's NGFW. If your OT alerts are separated from IT security, it creates blind spots and additional challenges for identification, remediation and risk reduction across your complete IT/OT environment.

Solution

Check Point and Tenable have partnered to provide customers with a seamless offering to increase visibility into ICS and critical infrastructure, as well as protect them from cyber threats.

Tenable.ot's advanced, OT-specific asset discovery and tracking capabilities integrate with Check Point's next generation firewalls (NGFWs) and dynamically populate with assets based on tags. This allows Tenable.ot to provide continuous updates on the assets it identifies in your ICS network to help firewall administrators improve overall cybersecurity posture.

Tenable.ot provides detailed information on each discovered asset, such as IP address, device type, vendor and model and is delivered to Check Point's NGFW. Administrators can take advantage of this integration to extend policies across IT and OT environments.

Features

The Tenable integration for Check Point firewalls helps you:

- Get detailed visibility across IT and OT devices, their attributes and risk level
- Get an in-depth view of external and internal threats targeting OT environments that firewall protections can address
- Take advantage of automated asset discovery, classification and tracking for more efficient and effective firewall management
- Auto-generate policies for every device based on its attributes
- Apply virtual patching using Check Point Gateway

Technology Components

- Tenable.ot™
- Check Point Security Gateway
- Check Point Security Management

Key Benefits

- Get an in-depth view of external and internal threats targeting OT environments that can be addressed via firewall rules
- Take advantage of automated asset discovery, classification and tracking to facilitate better policy creation and firewall management
- Full inventory of all deployed industrial assets including state and configuration to enable change control tracking within your IT framework
- Address regulatory compliance and change management requirements
- Single pane of glass view

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**.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. is a leading provider of cybersecurity solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry-leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device-held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects more than 100,000 organizations of all sizes. Learn more at **checkpoint.com**

Securing Access to Critical ICS Assets

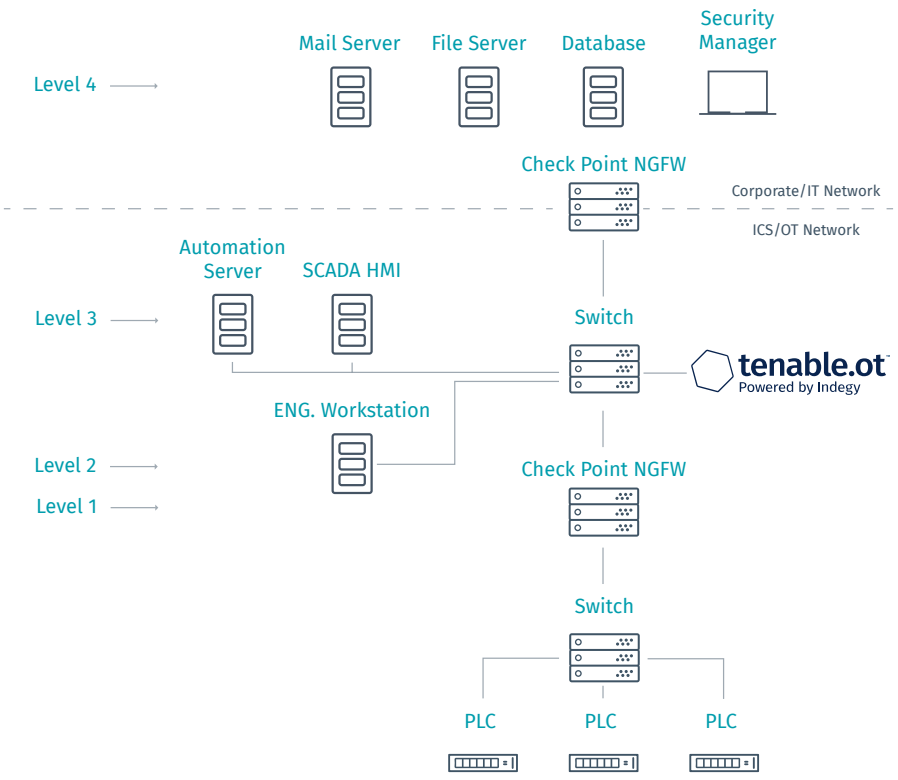
Administrators can now easily make changes to policies and gain complete access control over ICS networks.

With the joint solution, you can configure policies that apply to specific OT assets, taking their various characteristics into account. For example, when you need to access your ICS network to update engineering stations, the NGFW administrator can set a policy that applies to these devices only without relying on manual mapping based on IP addresses that can change over time.

Safeguard Converging OT and IT Environments

With the integration of Tenable.ot and Check Point's NGFWs, your administrators can configure rules that address individual OT assets and groups by their type or vendor.

There is no need for prior knowledge of the network or address specifics. For example, an administrator can set a rule to allow only necessary communications to facilitate data gathering by a manufacturing-efficiency system to other devices in the OT network.



For support please go to: **support@tenable.com**