tenable®

Tenable.ot for Aruba

aruba
a Hewlett Packard
Enterprise company

Business Challenge

Unlike IT networks, industrial control systems (ICS) lack visibility, security and control.

OT networks do not have security features embedded and with increased threats targeting industrial environments, they are extremely vulnerable to attacks. Additionally, most of the devices on your network don't require authentication, making it virtually impossible to prevent unauthorized access or changes to critical devices. Moreover, as the Industrial Internet of Things (IIoT) continues to gain adoption in industrial and critical infrastructure environments, new devices are constantly coming online. Without the proper security and access control, they can introduce unacceptable risk into your network.

Solution

Tenable.ot provides full visibility of—and safety across—your industrial network.

By combining Tenable.ot's advanced threat detection, asset and vulnerability management—both at the network and device level, along with Aruba Networks ClearPass Access Control—the joint solution delivers complete visibility, security and control, across your IT and OT environments. This includes traditional Windows-based systems, Macs and mobile devices, as well as OT devices such as industrial controllers (PLCs, RTUs, DCS controllers).

If you rely on ClearPass to provide visibility and control for your IT environments, you can now get visibility on your OT networks with the same granularity, policies and workflow. This enables you to effectively detect and mitigate threats to the safety, reliability and continuity of your IT and OT converged environment.

Technology Components

- Tenable.ot

- Aruba Networks ClearPass

The Challenge

- Lack of a comprehensive view across your entire industrial infrastructure

- Inability to detect and mitigate threats impacting your IT and OT environments

- No situational awareness into who accesses restricted assets or the operations they perform

- No automated OT asset discovery and inventory management

Key Benefits

- End-to-end visibility and security for OT networks

- Automated asset discovery and management

- Continuous validation of asset configurations

- Access control and audit trail based on job role or authority

- Improved incident response and threat mitigation

Key Components

Managing IT and OT Assets in Industrial Networks

Since industrial networks lack access controls, new unmanaged connected devices can potentially introduce threats into these sensitive environments. Lack of automated asset discovery and management is also at the root of many operational incidents resulting from contractors, integrators or employees working on the wrong assets. Such incidents can result in severe operational disruptions. In addition, an unmanaged asset inventory is harder to support and maintain since it's not always clear which assets you should upgrade or patch, or which spare parts you need.

Detecting Threats to Operational Environments

As more and more industrial networks connect to corporate environments and cloud solutions, their risk exposure profile increases. Since OT environments are different from IT environments and use different proprietary protocols, IT security solutions like firewalls and intrusion detection solutions (IDS) are inadequate for threat detection.

NAC systems and other IT visibility tools are not effective across your OT environment because you cannot use agents on OT devices and IT scanning tools can make OT unstable. In addition, critical control devices lack event logs, so event tracing is nearly impossible.

Validating Configurations and Managing Changes

Controller configuration settings directly impact the industrial processes they manage. Any unauthorized change to the configuration logic or firmware can result in severe disruptions and damaged equipment.

Without a backup of past configurations and proper access controls that validate the operator's identity, it is difficult to ensure authorized work and it is not possible to restore a controller to a previously known good configuration after an incident.

The Tenable.ot and Aruba ClearPass solution provides visibility, security and access control to your IT and OT devices within industrial networks thereby reducing your overall cyber exposure and mitigating unacceptable risk.

More Information

For support please contact: **support@tenable.com**