The Indegy and Aruba ClearPass solution provides visibility, security and access control to both the IT and OT devices within industrial networks. These devices include traditional Windows-based systems, Macs and mobile devices, as well as OT devices like industrial controllers (PLCs, RTUs, DCS controllers). The agentless solution is simple to deploy and connects directly to the enterprise’s existing IT security operations infrastructure.

The Challenge

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

The Solution

The joint Indegy-Aruba ClearPass solution offers complete visibility, security and access control for the network and all industrial devices. This enables security professionals to effectively detect and mitigate threats to the safety, reliability and continuity of both the IT and OT converged environment.

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
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. The 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 is not always clear which assets should be upgraded or patched, or which spare parts are needed.

Detecting Threats to Operational Environments

As more and more industrial networks are connected to corporate environments and cloud solutions, their risk exposure profile increases. Since OT environments are very different from IT environments, and use different proprietary protocols, IT security solutions like Firewalls and Intrusion Detection Solutions (IDS) are inadequate for detecting threats. NAC systems and other IT visibility tools are not effective across the OT environment since agents cannot be used on OT devices and IT scanning tools can cause OT to become unstable. In addition, the critical control devices lack event logs, so tracing back which events took place is nearly impossible.
Validating Configurations and Managing Changes

The configuration settings of controllers directly impact the industrial processes that they manage. Any unauthorized change to the configuration, or to the 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 very difficult to ensure that the work being done is authorized and that it is possible to restore a controller to a previously known good configuration after an incident.

The Indegy-Aruba ClearPass joint solution enables industrial organizations to ensure the security of industrial environments.

The Joint Solution

Indegy, a leader in OT security can provide full visibility of the industrial network. By combining Indegy’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 both the IT and OT environment. Customers who rely on ClearPass to provide visibility and control for their IT environments can now get visibility on their OT networks with the same granularity, policies, and workflow that they have established. Fast and effective incident detection, incident response and threat mitigation can be achieved across the entire organization.

Like this solution brief?
Visit us at Indegy.com for more content like this.

Follow us: