aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba and Microsoft Azure Defender for IoT

Extending Network Visibility and Security to Operational Technology (OT) Devices and Industrial Control Systems

PARTNER SOLUTION OVERVIEW

Industrial and manufacturing customers typically have large deployments of Operational Technology (OT) sensors, actuators, programmable logic controllers, and human machine interfaces that run factories and plants. Historically, OT systems were air gapped from the rest of the enterprise in hopes that the moat would protect them from attack. That approach proved ineffective in the face of modern cyber threats, like the Stuxnet virus, that can cross air gaps.

As a result, customers need to pivot away from air gaps to active OT monitoring with the objective of providing uniform visibility and security policies across OT control buses, programmable logic controllers, SCADA remote terminal units, and other devices. OT systems use unique physical layers (PHY) and protocols, so specialized tools are needed to monitor them and share data with Aruba ClearPass Policy Manager.

BREACHING THE MOAT

Inserting eyes and ears into an OT network requires tight alignment with the operating modes of OT infrastructure. In addition to understanding the PHYs and protocols, the monitoring system needs to have a library of devices types, know correct and abnormal operating modes, and do no harm in both normal operating and failure modes. Aruba has teamed with Microsoft Azure Defender for IoT to help bridge the IT and OT security divide. Defender for IoT combines deep knowledge of industrial control systems, machine learning-based threat analytics, and a bi-directional link to ClearPass Policy Manager. The joint solution identifies OT devices, finds vulnerabilities, detects threats, and responds appropriately. ClearPass Policy Manager uses device profiling, role-based access control, and real-time policy enforcement to identify, on-board, and control devices. Defender for IoT enhances these services by discovering OT devices, flagging risks and abnormalities, and enforcing security postures.

KEY BENEFITS

- Visibility into what OT devices are on your network
- Quarantine and block OT devices based on zero-day threats
- Remediate systems with outdated or non-compliant software
- Automatically enforce access policies
- Certified Interoperability

The joint solution allows IT administrators to centrally manage connected devices and enforce policies governing what those devices can do: OT retains control of their devices, IT obtains uniform visibility and security policies across the entire enterprise, and the end user avoids costly downtime, safety incidents, and loss of intellectual property.

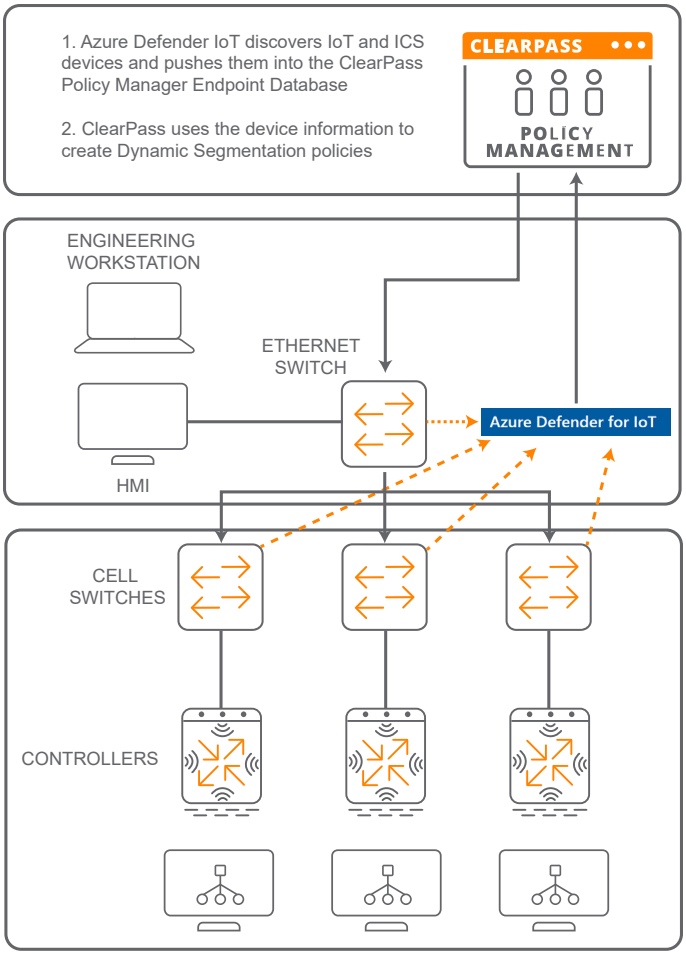
HOW IT WORKS

When an OT device connects to the network it is discovered by Defender for IoT, which synchronizes with ClearPass Policy Manager to give a comprehensive view of all IT and OT devices. The supplied context can be used by Aruba to dynamically segment OT communications and ensure they only communicate with their intended devices and applications.

These features enable OT managers to:

- Gain insight into network devices across IT and OT networks
- Utilize contextual data to deploy seamless edge security
- Ensure that only compliant devices are allowed on the network

Microsoft



CERTIFIED INTEROPERABILITY

Aruba and Defender for IoT have taken the guesswork out of deployments by certifying the interoperability of Defender for IoT with Aruba infrastructure. Set-up is simple: just follow the three-step configuration process within the Defender for IoT GUI and create the ClearPass API Client. Once completed, Defender for IoT will immediately populate the ClearPass endpoint database with OT endpoint data and custom attributes which can then be used to create dynamic segmentation policies in a Zero Trust environment. The joint integration is executed and administered through the Defender for IoT dashboard for at-a-glance network diagnostics.

SUMMARY

Aruba and Defender for IoT help industrial and manufacturing organizations achieve uniform visibility and security policies that span both IT and OT infrastructure.

For more information on ClearPass, please visit: https://www.arubanetworks.com/products/security/network-access-control/.

For information regarding Azure Defender for IoT, please visit: https://azure.microsoft.com/en-us/services/azure-defender-for-iot/

Member of
Microsoft Intelligent Security Association

Microsoft

www.microsoft.com Phone Number: 1-425-882-8080 1, Microsoft Way, Redmond Washington 98052-6399

aruba
a Hewlett Packard Enterprise company

PSO_ArubaandMicrosoftAzureDefenderforIoT_RVK_080521 a00116811enw

Contact us at www.arubanetworks.com/contact