OT ASSET DISCOVERY With Azure Defender for IoT

Passive monitoring with optional active technology — “Hybrid” approach provides comprehensive asset discovery & ongoing management

Industrial and critical infrastructure organizations know that threats from adversaries continue to become more sophisticated. However, they struggle to even keep accurate inventory of the assets that they need to protect, let alone actually implement strategies to keep those assets protected.

Azure Defender for IoT combines passive monitoring and optional selective probing (or “active scanning”) techniques to provide the most accurate and detailed inventory of assets in industrial and critical infrastructure organizations.

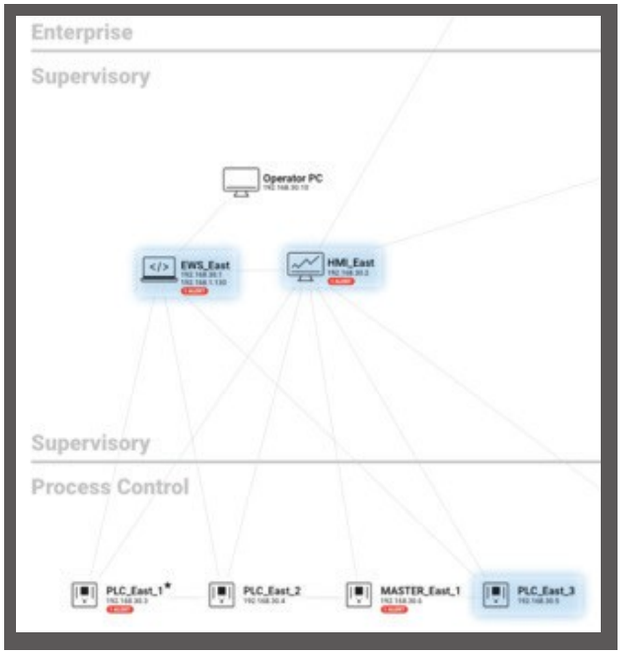


Figure 1: Topology map showing communication behavior between ICS devices, as provided by passive monitoring.

Figure 2: Device profile obtained by clicking on one of the devices in the network topology map.

HIGHLIGHTS

- Continuous passive monitoring to establish baseline inventory
- Optional selective probing for comprehensive “point in time” view using safe, vendor-approved device queries
- Hybrid “best of both worlds” approach
- Proven expertise: Asset inventory performed on thousands of production ICS networks worldwide, across diverse industrial sectors

Passive Monitoring

Historically, industrial and critical infrastructure organizations have been reluctant to allow security devices to connect to their production networks. Our passive monitoring technology has been widely deployed because it is non-invasive and has zero impact on production networks. It works by collecting a copy of the traffic from the SPAN port of a network switch or via a network tap, using proprietary Network Traffic Analysis (NTA) to provide valuable and comprehensive information about your asset inventory.

Passive monitoring captures detailed information about ICS assets such as the IP and MAC address, serial number, product name, product code, manufacturer, device type, and OS or firmware version.

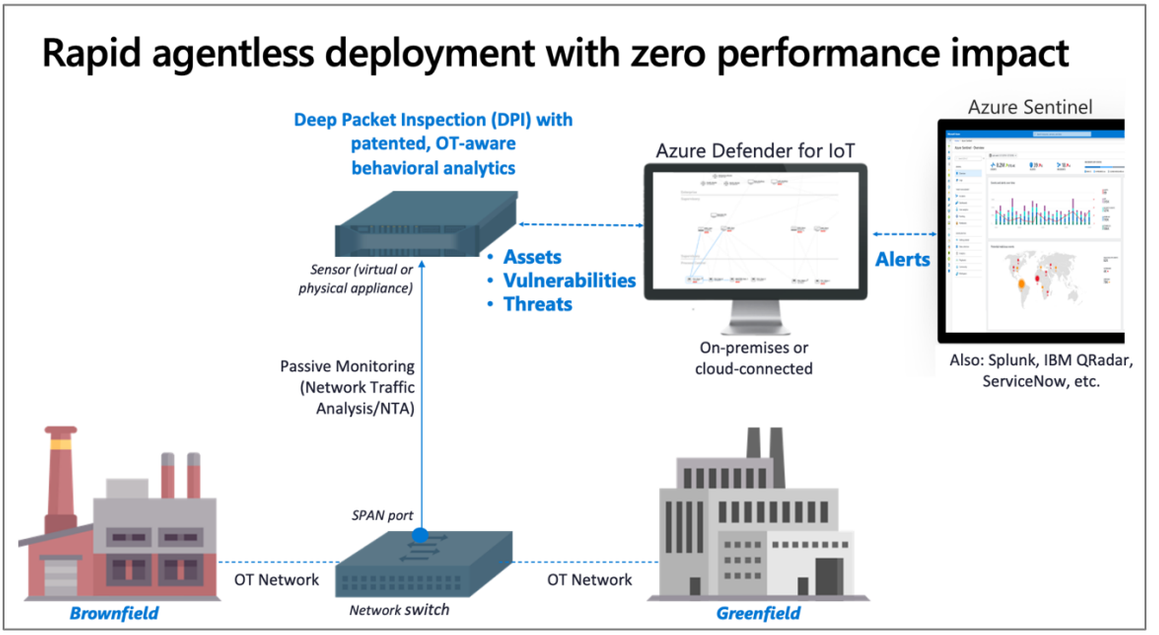
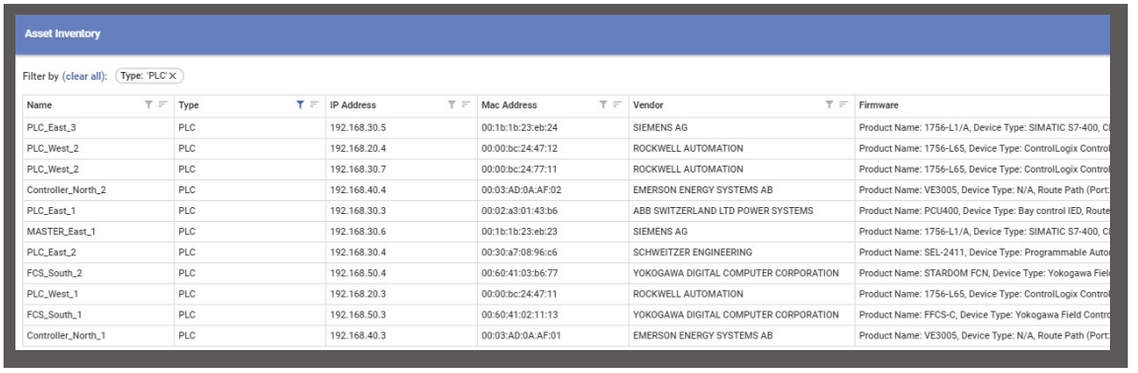


Figure 3: Passive monitoring uses SPAN ports or network taps to analyze traffic with zero impact on production networks. It integrates out-of-the-box with existing SOC workflows and security stacks including Azure Sentinel, Splunk, IBM QRadar, and ServiceNow.

Passive monitoring also provides tabular details of devices, as shown below:



Asset Inventory

Filter by (clear all): Type: 'PLC'

Name	Type	IP Address	Mac Address	Vendor	Firmware
PLC_East_3	PLC	192.168.30.5	00:1b:1b:23:eb:24	SIEMENS AG	Product Name: 1756-L1/A, Device Type: SIMATIC S7-400, C
PLC_West_2	PLC	192.168.20.4	00:00:bc:24:47:12	ROCKWELL AUTOMATION	Product Name: 1756-L65, Device Type: ControlLogix Control
PLC_West_2	PLC	192.168.30.7	00:00:bc:24:77:11	ROCKWELL AUTOMATION	Product Name: 1756-L65, Device Type: ControlLogix Control
Controller_North_2	PLC	192.168.40.4	00:03:AD:0A:AF:02	EMERSON ENERGY SYSTEMS AB	Product Name: VE3005, Device Type: N/A, Route Path (Port:
PLC_East_1	PLC	192.168.30.3	00:02:a3:01:43:b6	ABB SWITZERLAND LTD POWER SYSTEMS	Product Name: PCU400, Device Type: Bay control IED, Route
MASTER_East_1	PLC	192.168.30.6	00:1b:1b:23:eb:23	SIEMENS AG	Product Name: 1756-L1/A, Device Type: SIMATIC S7-400, C
PLC_East_2	PLC	192.168.30.4	00:30:a7:08:96:c6	SCHWEITZER ENGINEERING	Product Name: SEL-2411, Device Type: Programmable Autor
FCS_South_2	PLC	192.168.50.4	00:60:41:03:b6:77	YOKOGAWA DIGITAL COMPUTER CORPORATION	Product Name: STARDOM FCN, Device Type: Yokogawa Fiel
PLC_West_1	PLC	192.168.20.3	00:00:bc:24:47:11	ROCKWELL AUTOMATION	Product Name: 1756-L65, Device Type: ControlLogix Control
FCS_South_1	PLC	192.168.50.3	00:60:41:02:11:13	YOKOGAWA DIGITAL COMPUTER CORPORATION	Product Name: FFCS-C, Device Type: Yokogawa Field Contro
Controller_North_1	PLC	192.168.40.3	00:03:AD:0A:AF:01	EMERSON ENERGY SYSTEMS AB	Product Name: VE3005, Device Type: N/A, Route Path (Port:

Figure 4: Rich device details provided by passive monitoring

Selective Probing ("Active Scanning")

In organizations with highly-segmented environments, it can be resource intensive to connect appliances to each segment of the network for passive monitoring. For more mature organizations, where their policy allows active querying of ICS devices, CyberX offers an optional selective probing approach.

Selective probing consists of software modules that query Windows and embedded devices like PLCs for specific asset details (such as firmware or Service Pack revision levels) — using safe, vendor-approved commands, scheduled to run as often or as infrequently as desired (typically once per day). The resulting asset information is displayed in our standard console, in the standard asset inventory screens. For example, selective probing provides an immediate snapshot of device details such as OS and firmware revision levels.

Selective probing (active scanning) provides the same textual information about devices that passive scans provide.

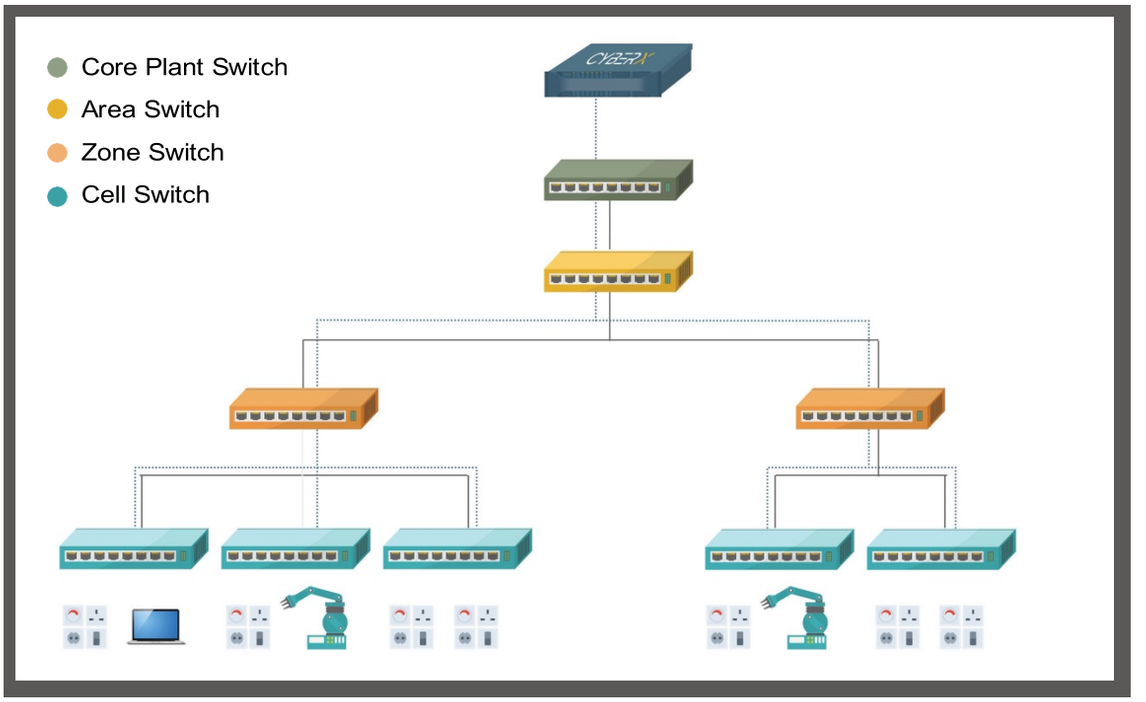


Figure 5: Selective probing queries ICS devices using safe, vendor-approved commands

Hybrid Approach: Best of Both Worlds

Because there are advantages to each approach, more and more organizations are interested in a "hybrid" approach to asset discovery and inventory. A hybrid approach offers the advantage of providing a baseline view of assets using continuous passive monitoring, while providing a comprehensive "point in time" inventory of assets using selective probing, especially for isolated assets on highly segmented networks.

ABOUT AZURE DEFENDER FOR IoT

Azure Defender for IoT offers agentless, network-layer IoT/OT security that is rapidly deployed, works with diverse industrial equipment, and interoperates with Azure Sentinel and other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

Gain full visibility into assets and risk across your entire IoT/OT environment. Continuously monitor for threats and vulnerabilities, with IoT/OT-aware behavioral analytics and threat intelligence. Strengthen IoT/OT zero trust by instantly detecting unauthorized or compromised devices.

Deploy on-premises, in Azure-connected, or in hybrid environments.