Azure IoT/OT Security — Unified, End-to-End Protection
For Both Greenfield & Brownfield Environments

Runs On-Premises

Unmanaged (Brownfield) Devices — agentless security

On-Premises Console

Network Switch or TAPs

Azure Defender for IoT Sensor (continuous monitoring)

Runs on Azure

Azure IoT Hub

Azure Sentinel
- Alerts & incidents
- Investigations & threat hunting
- OT-specific SOAR playbooks
- OT-specific threat intelligence

Azure Defender for IoT
- Asset inventory
- Vulnerability management
- Continuous threat monitoring

Azure console

Managed (Greenfield) Devices — agent-based security

Micro-agents

Windows IoT Core, RTOS, Linux

Azure Sphere

Azure IoT Edge

3rd Party Integration

QRadar, Splunk, Etc.

ITSM, CMDB

Firewalls, NACs