OT/ICS/IoT Cybersecurity

April 2021

ADAPTERA
PERFORMANCE PARTNER

Microsoft

Introduction

Digital transformation and IIoT are driving increased connectivity between IT and OT (Operational Technology) networks, increasing the attack surface and the risk of cyberattacks on critical infrastructure.

Growing number of sophisticated cyberattacks (e.g ***WannaCry*** & ***NotPetya*** and ***TRITON***) on industrial and critical infrastructure compromise large scale Cyber-physical systems and impact on industrial scale production. These types of attacks will only get more frequent and potentially more harmful

Why you Need to think on your ICS/OT Cybersecurity

As enterprises implement digitalization for greater efficiency and productivity, boards and management teams are increasingly concerned about the liability and financial risk resulting from the deployment of massive numbers of unmanaged Internet of Things (IoT) and Operational Technology (OT) devices.

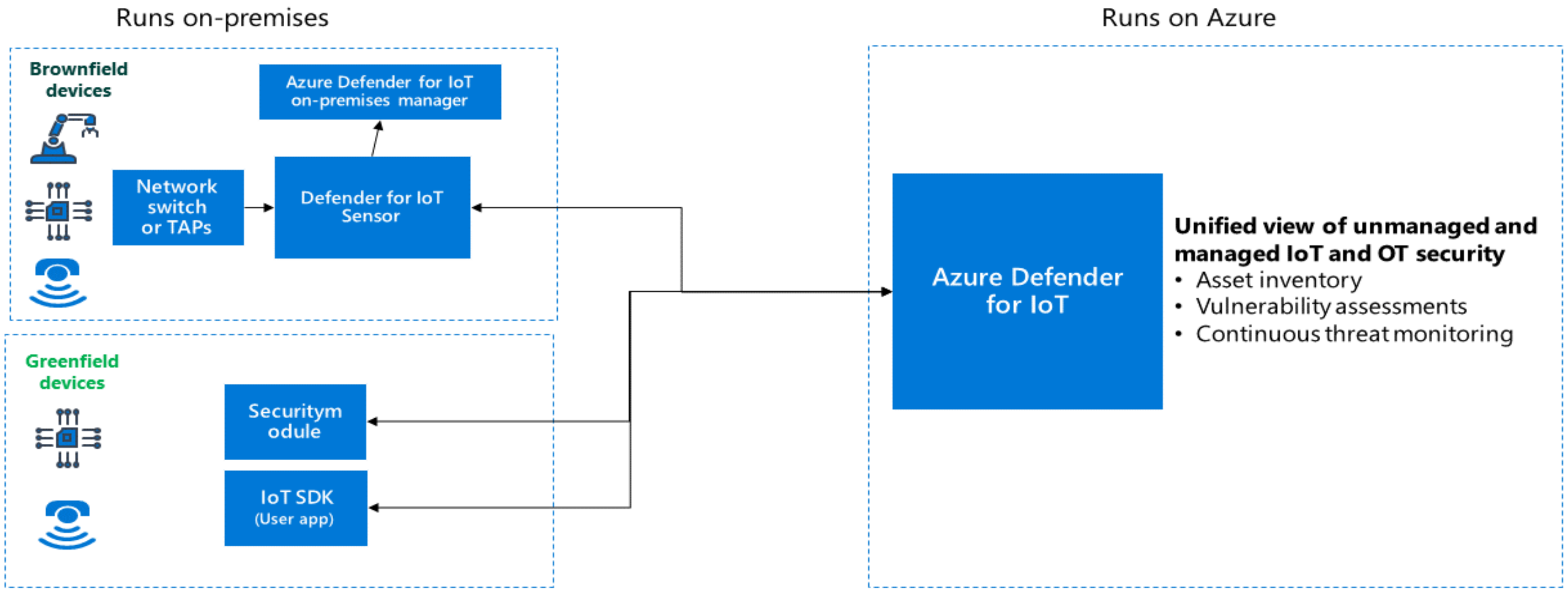
Legacy IoT and OT devices don’t support agents and are often unpatched, misconfigured, and invisible to IT teams – making them soft targets for threat actors looking to pivot deeper into corporate networks.

What is IoT Defender and how it works

- Azure Defender for IoT is a holistic solution that continuously discovers, monitors, and manages IoT and OT threats, risks, and vulnerabilities across all IoT and OT devices (**even legacy devices**)
- Unlike IT security tools, Defender for IoT is an OT-specific security platform: Leverages a deep understanding of industrial protocols (DNP3, ICCP, IEC104, IEC61850, OPC, etc.)
- Provides ICS-aware asset discovery and vulnerability management supporting diverse vendors (Rockwell Automation, Schneider Electric, Siemens, GE, etc.)
- Uses agentless, non-invasive technology with zero impact on your production network and is easily deployed as either a virtual or physical appliance.

Basic architecture of the solution

- **Defender for IoT** connects **both** to the Azure cloud **as well as to on-premises components**.
- Designed for scalability in large and geographically distributed environments with multiple remote locations.



Runs on-premises

Brownfield devices

Azure Defender for IoT on-premises manager

Network switch or TAPs

Defender for IoT Sensor

Greenfield devices

Securitym odule

IoT SDK (User app)

Runs on Azure

Azure Defender for IoT

Unified view of unmanaged and managed IoT and OT security

- Asset inventory
- Vulnerability assessments
- Continuous threat monitoring

ADAPTERA PERFORMANCE PARTNER

Microsoft

ICS / OT Use Cases

- **Unauthorized changes to controllers**: Update to device ladder logic or firmware.
  Can represent attempt to compromise device by inserting malicious code such as a
  RAT. Can also represent insertion of malicious parameters causing the physical process
  — such as spinning turbine — to operate in unsafe manner.
- **Protocol violations:** Unpermitted packet structure or field value that violates vendor’s protocol specification. Can represent a misconfigured application or a malicious attempt to compromise the device – for example, by causing a buffer overflow condition in the target device.
- **PLC Stop:** A command that causes the device to stop functioning, thereby risking the physical process that is being controlled by the PLC.

ICS / OT Use Cases

- **Industrial malware:** Malware that manipulates ICS devices via their native protocols, such as TRITON and Industroyer. Defender for IoT also detects IT malware that has moved laterally into the ICS/SCADA environment, such as Conficker, WannaCry, and NotPetya.
- **Scanning malware**: Reconnaissance tools that collect data about systems and configurations in a pre-attack phase. For example, the Havex Trojan identifies OPC servers by using Windows networking functions to build a list of all servers accessible via Windows networking. OPC is an open communications standard that allows interaction between Windows-based SCADA applications and process control systems.
- **Unauthorized remote access**: Remote access by employees or contractors that can indicate initial compromise of the ICS network.
- **Unauthorized database changes**: Changes to Historians or HMIs that can violate corporate policies and/or compliance regulations.

ADAPTERA’s Added Value on OT Cybersecurity

In July 2020 **ADAPTERA** established a cooperation with CYBERX (now a MICROSOFT company) a leader in Cybersecurity solutions for critical infrastructure OT/ICS/IoT environments in verticals such as Energy, Oil & gas, Water, Industrial plants, Transportation, Telecoms etc.

ADAPTERA has a strong specialization and an extensive expertise in implementing Cybersecurity projects based on advanced technologies of Network Visibility and Performance Monitoring.

Contact **ADAPTERA** for an extensive discussion for the optimal way to increase the Cybersecurity of your OT/ICS/IoT network, based on innovative total visibility solutions.

Thank you!