



Microsoft Defender for IoT



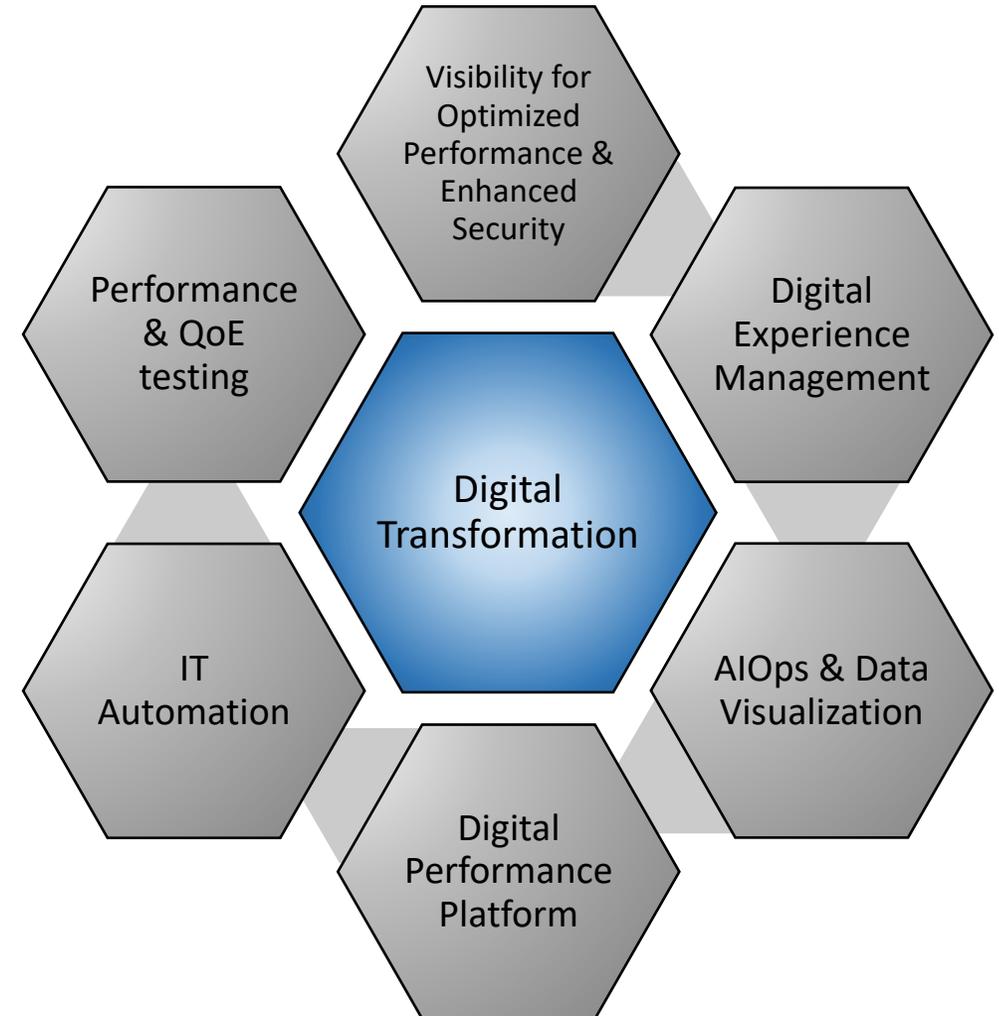


Our Vision & Mission

Performance Partner

We support our Customers' Digital Transformation Journey by delivering on the promise of **optimized performance & enhanced security of digital services**

We deliver leveraging on our strong expertise in the areas of:





How Gartner defines Operational Technology (OT) security

“The practices and technologies used to protect people, assets and information involved in the monitoring and/or control of physical devices, processes and events.”

Manufacturing, energy & water utilities, smart buildings, chemicals, pharmaceuticals, oil & gas, transportation & logistics, mining, life sciences, retail, ...

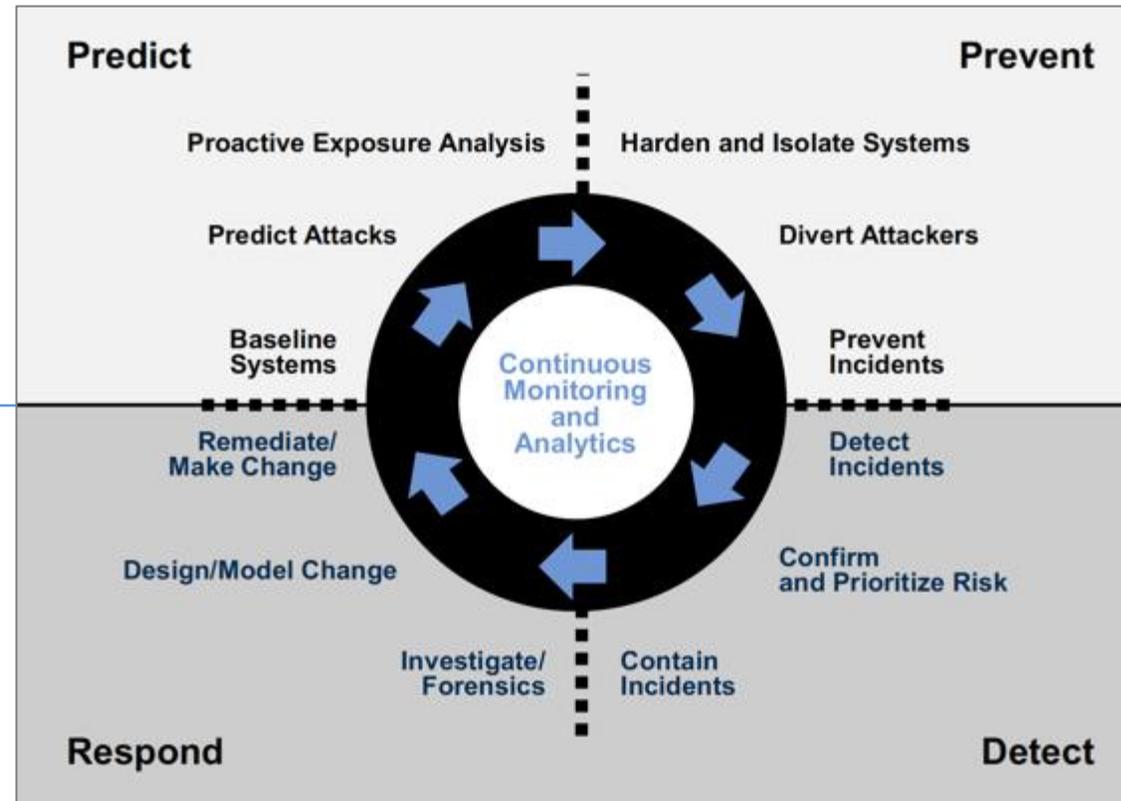




“Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities.” GARTNER

- ✓ Automated threat modeling (attack vectors)
- ✓ Risk-based prioritization of mitigation activities
 - ✓ Baselining

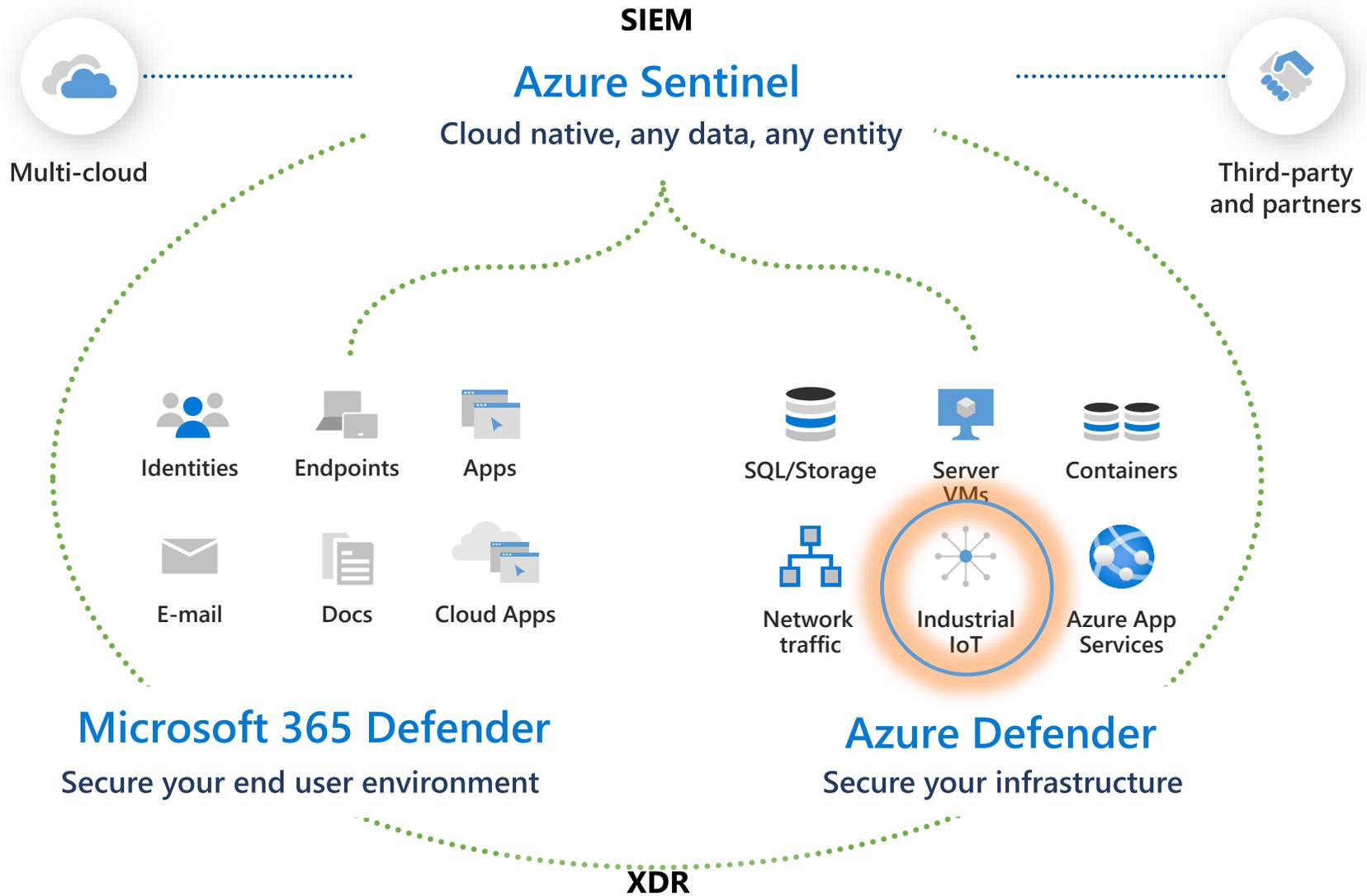
- ✓ Deep forensics, investigation & threat hunting capabilities
 - ✓ Full-fidelity PCAPs
- ✓ SIEM integration & REST API



- ✓ Non-invasive asset discovery
- ✓ Hardening recommendations for network & endpoint vulnerabilities
- ✓ Integration with firewalls & unidirectional gateways

- ✓ Continuous monitoring
- ✓ Patented M2M anomaly detection
- ✓ Detection of unauthorized changes to ladder logic and firmware

Stay ahead of attackers with a unified SecOps experience





IoT/OT Asset Discovery

What devices do we have & how are they communicating?



Operational Efficiency

How do we identify the root cause of malfunctioning or misconfigured equipment?



Risk & Vulnerability Management

What are risks & mitigations impacting our crown jewel assets?



Unified IT/OT Security Monitoring & Governance

How do we break down IT/OT silos?

How do we leverage existing workflows & tools to centralize IT/OT security in our SOC?

How do we demonstrate to auditors that we have a safety- and security-first environment?



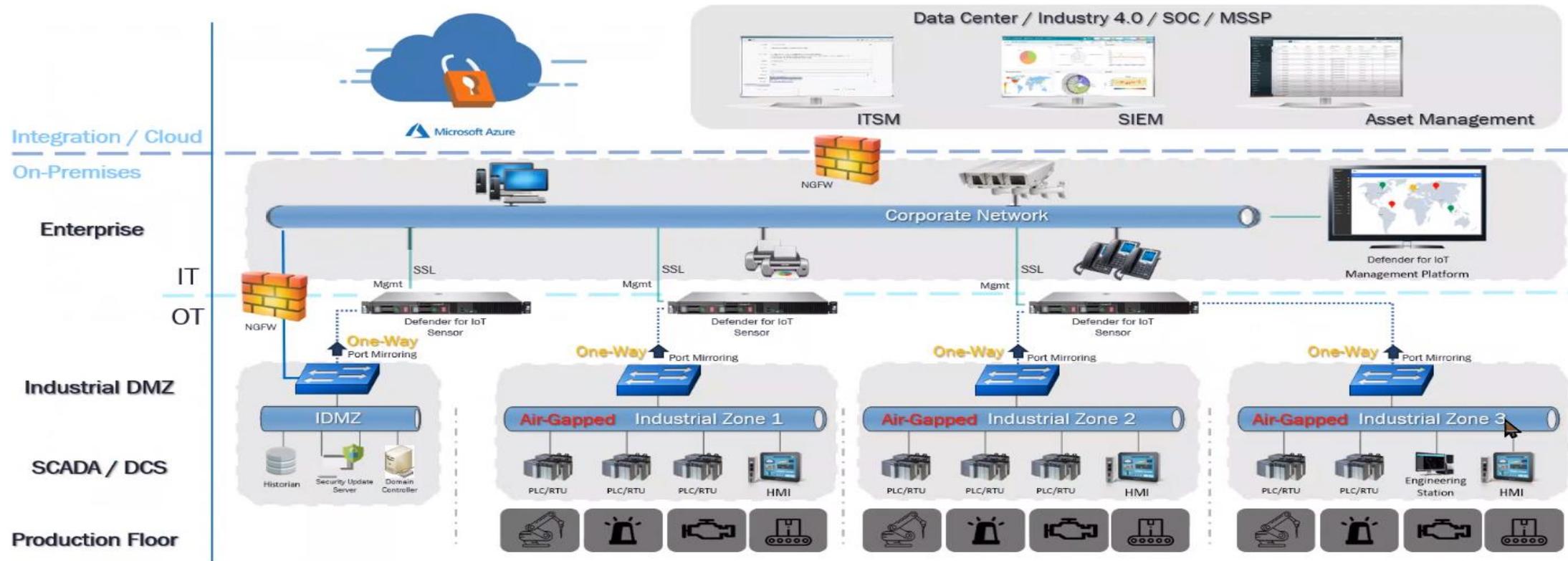
Continuous IoT/OT Threat Monitoring, Incident Response & Threat Intelligence

How do we detect & respond to IoT/OT threats in our network?



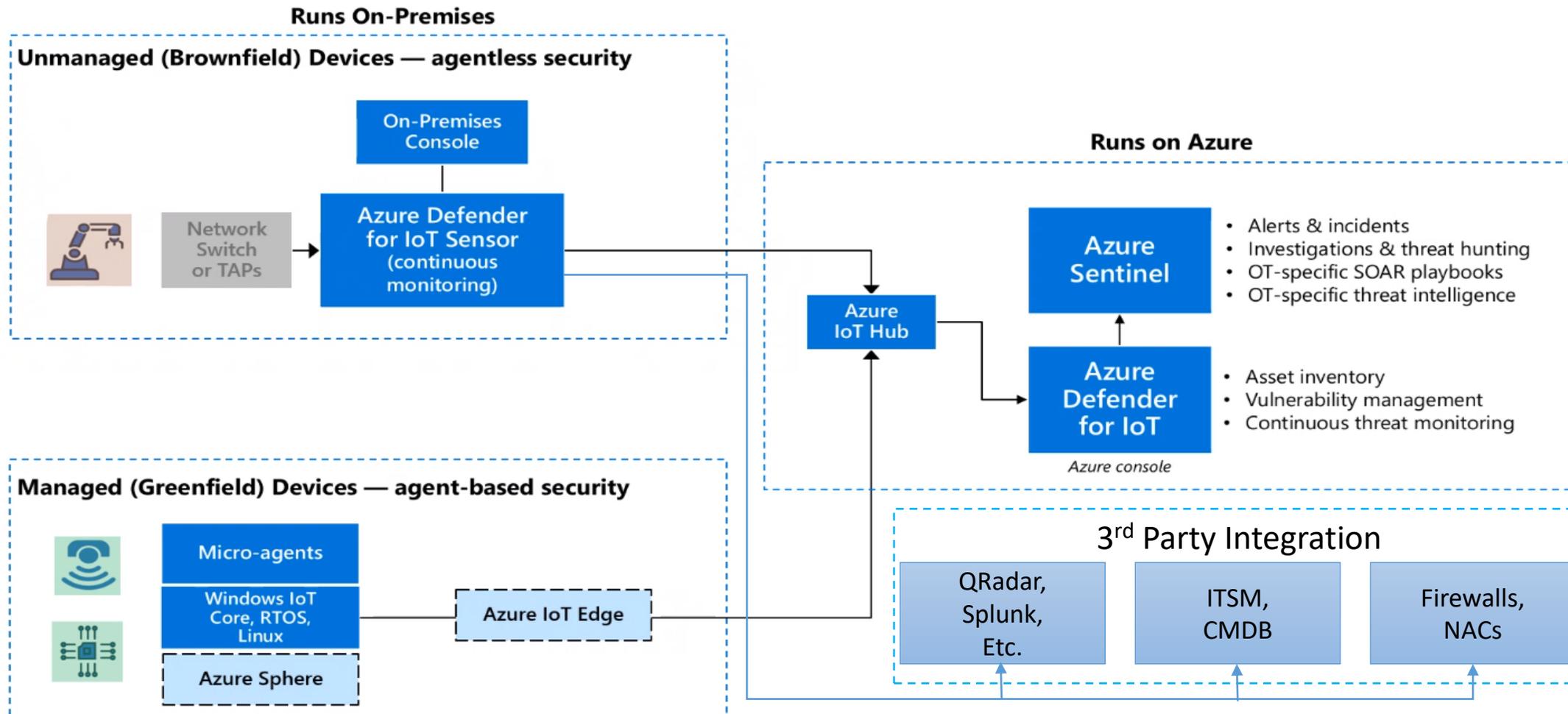


Multi-Layer, Multi-Tenant Architecture

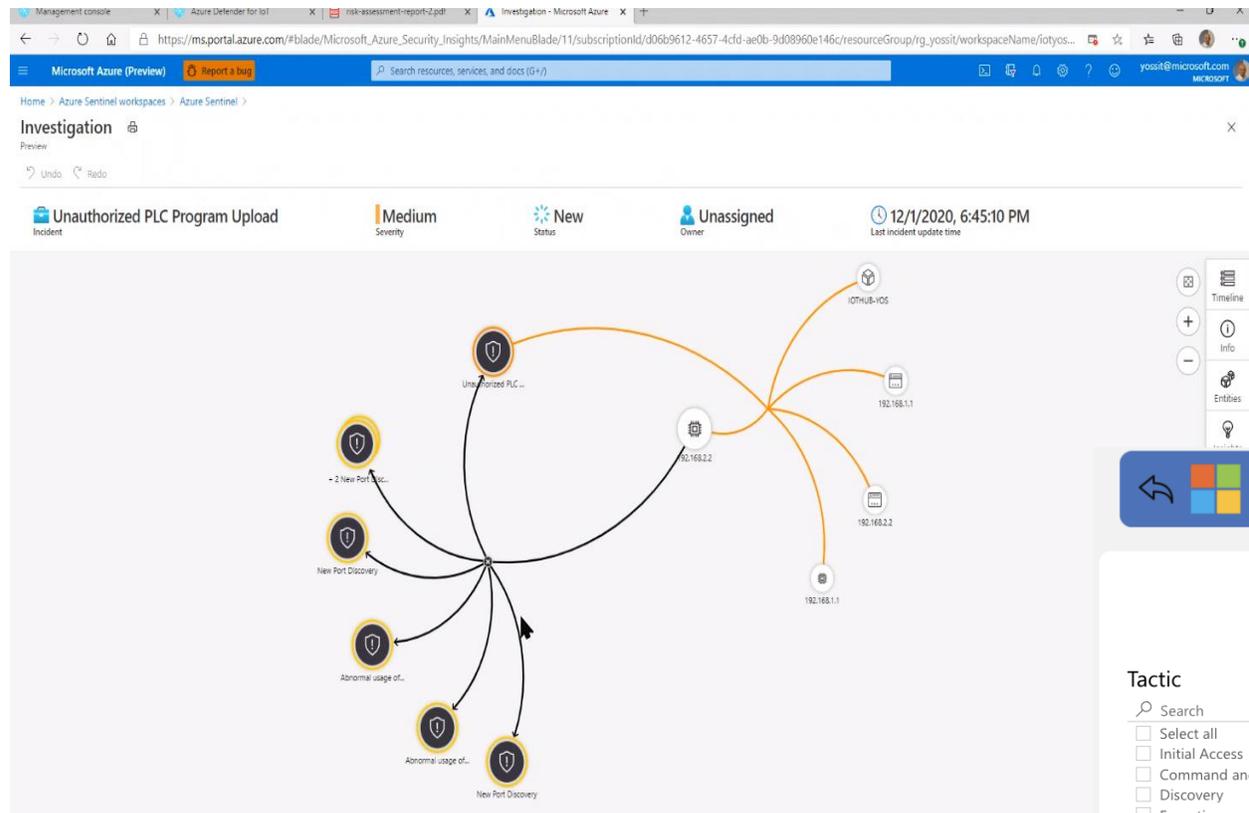




Azure IoT/OT Security — Unified, End-to-End Protection For Both Greenfield & Brownfield Environments



SIEM Integration and Audit - Compliance reporting



Advanced Dashboard

MITRE

Filters
Graph

Tactic	Technique	Technique Name	Technique Description
<input type="checkbox"/> Select all <input type="checkbox"/> Initial Access <input type="checkbox"/> Command and Control <input type="checkbox"/> Discovery <input type="checkbox"/> Execution <input type="checkbox"/> Impact <input type="checkbox"/> Impair Process Control <input type="checkbox"/> Inhibit Response Function <input type="checkbox"/> Persistence	<input type="checkbox"/> Select all <input type="checkbox"/> T806 <input type="checkbox"/> T807 <input type="checkbox"/> T808 <input type="checkbox"/> T814 <input type="checkbox"/> T822 <input type="checkbox"/> T828 <input type="checkbox"/> T830 <input type="checkbox"/> T833 <input type="checkbox"/> T841 <input type="checkbox"/> T857 <input type="checkbox"/> T859 <input type="checkbox"/> T869	<input type="checkbox"/> Select all <input type="checkbox"/> Brute Force I/O <input type="checkbox"/> Command-Line Interface <input type="checkbox"/> Control Device Identification <input type="checkbox"/> Denial of Service <input type="checkbox"/> External Remote Services <input type="checkbox"/> Internet Accessible Device <input type="checkbox"/> Loss of Productivity and Revenue <input type="checkbox"/> Man in the Middle <input type="checkbox"/> Modify Control Logic <input type="checkbox"/> Network Service Scanning <input type="checkbox"/> Service Stop <input type="checkbox"/> Standard Application Layer Protocol	<input type="checkbox"/> Select all <input type="checkbox"/> Adversaries may brute force I/O addresses on a device and attempt to exhaust... <input type="checkbox"/> Adversaries may cause loss of productivity and revenue through disruption an... <input type="checkbox"/> Adversaries may establish command and control capabilities over commonly u... <input type="checkbox"/> Adversaries may gain access into industrial environments directly through syst... <input type="checkbox"/> Adversaries may leverage external remote services as a point of initial access i... <input type="checkbox"/> Adversaries may perform control device identification to determine the make ... <input type="checkbox"/> Adversaries may perform Denial-of-Service (DoS) attacks to disrupt expected ... <input type="checkbox"/> Adversaries may place malicious code in a system, which can cause the system... <input type="checkbox"/> Adversaries may steal the credentials of a specific user or service account usin... <input type="checkbox"/> Adversaries may stop or disable services on a system to render those services ... <input type="checkbox"/> Adversaries may utilize command-line interfaces (CLIs) to interact with system... <input type="checkbox"/> Adversaries with privileged network access may seek to modify network traffic...

Tactics & Techniques

Tactic	Technique	Technique Name	Technique Description
Initial Access	T822	External Remote Services	Adversaries may leverage external remote services as a point of initial access into your network. These services allow users to connect to your network from a remote location. Examples include Remote Desktop Protocol (RDP), Citrix, and other services.

THANK YOU

Performance Partner

