Building a better working world

Microsoft

EY IoT Security Monitoring supported by Microsoft Azure Defender for IoT

Broad security monitoring solution for industries

Your digital world. Realized.

Operational technology (OT)/internet of things (IoT) security challenges require real-time monitoring and response capabilities to overcome cyber threats

- Did you know according to the EY Global Information Security Survey 2020, only 26% of organizations reported that their most significant breaches in the past year were discovered by their security operations center (SOC)?
- Successful cyber-attacks not only affect the organization's productivity, but also impact the brand value of the organization adversely
- Reputation losses have long-lasting effects – loss of brand value and drops in revenues
- Shop floor personnel lack cybersecurity knowledge and expertise on managing the complexity of OT/IoT devices
- Traditional IT capabilities to identify and mitigate security events do not match security requirements of OT/IoT devices
- Production environments lack security information and event management (SIEM) solutions to monitor OT/IoT systems, e.g. supervisory control and data acquisition (SCADA)

Benefits of EY IoT Security Monitoring supported by Microsoft Azure Defender for IoT

- Perform continuous, agentless vulnerability and threat detection with IoT/OT behavioral analytics
- Detect human failure affecting the security of your OT/IoT environment and increase awareness by proper response
- Gain broad visibility into assets and risk across your entire IoT/OT environment
- Avail flexible deployment options including on-premises, Microsoft Azure-connected or hybrid
- Deploy on-premises solution as a physical or virtual sensor that passively ingests network traffic (multiple sensors can aggregate their data to an on-premises management console)
- Integrate OT/IoT devices into a secure hub for tailored security management and secure communication in production area
- Seamlessly integrate OT/IoT devices into your cloud SIEM and leverage pre-defined monitoring and response rulesets
- Provide scalability for single sites in up to 100+ global organizations
- Create your own personalized alarms for your critical communication
- Benefit from non-standard industrial protocols support

EY IoT Security Monitoring supported by Microsoft Azure Defender for IoT for monitoring the security of your OT environment

EY IoT Security Monitoring supported by Microsoft Azure Defender for IoT is a professional asset discovery and security monitoring solution for OT/IoT environments. This solution helps accelerate IoT/OT innovation with broad security across all your IoT/OT devices. For end-user organizations, this solution offers agentless, rapidly deployable network-layer security that works with diverse industrial equipment and interoperates with Microsoft Azure Sentinel and other SOC tools. For IoT device builders, the solution offers lightweight agents to embed device-layer security into new IoT/OT initiatives. Further, clients can choose to deploy the solution on-premises or in Microsoft Azure-connected environments.

Target audience:

- Chief information officer (CIO)
- Chief information security officer (CISO) or client equivalent
- Internal audit security teams
- OT/IT security operation centers
- Control and automation engineers
- Manufacturing IT
- Chief development officer (CDO) or chief financial officer (CFO) or head of manufacturing

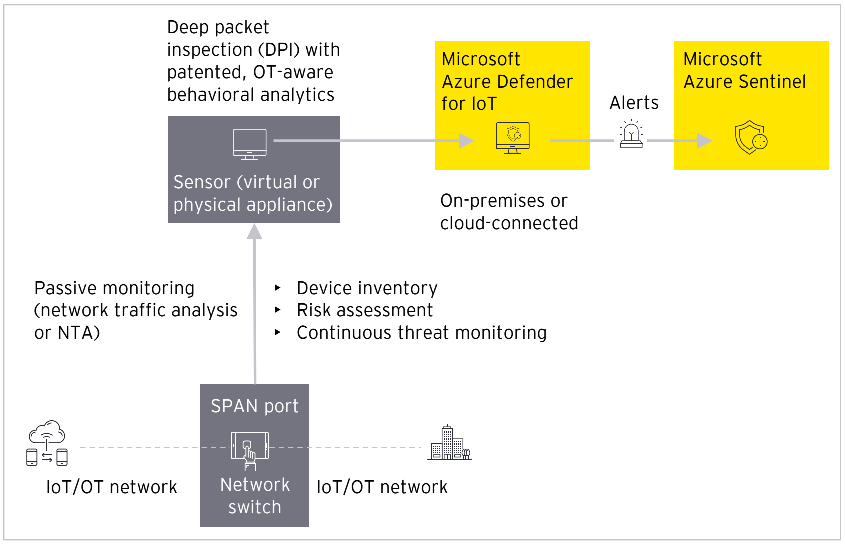
Target sectors:

- Power and utilities
- Manufacturing
- Oil and gas
- Pharma
- Transportations and logistics
- Mining
- Smart buildings

Key functionality

The EY IoT Security Monitoring supported by Microsoft Azure Defender for IoT solution usually consists of two main components: (a) probes (sensors) in the form of physical or virtual devices that are placed inside the OT network and the (b) central console.

The probes are connected to the switched port analyzer (SPAN)/mirror ports of network switches in places that are to be monitored. The place of obtaining information depends on which network traffic will be monitored. Information about the acquired network traffic is aggregated in the central console where this data is correlated, visualized and archived.


Deep packet inspection (DPI) with patented, OT-aware behavioral analytics
Sensor (virtual or physical appliance)
Microsoft Azure Defender for IoT
Alerts
Microsoft Azure Sentinel
On-premises or cloud-connected
Passive monitoring (network traffic analysis or NTA)
Device inventory
Risk assessment
Continuous threat monitoring
SPAN port
Network switch
IoT/OT network
IoT/OT network

Customer success stories: EY IoT Security Monitoring supported by Microsoft Azure Defender for IoT in action

The client was one of the largest pharmaceutical companies in the world. The ever-increasing cybersecurity risk and emerging new threats in the manufacturing process control space pushed the client to consider implementing a new security strategy. The client wanted to effectively and timely identify vulnerabilities, respond to threats, and prepare a recovery plan.

- EY teams helped in the implementation of the solution for the client to monitor the IoT/OT environment and gain full visibility into assets and related risks.
- This helped identify anomalous behaviors in the network and update the asset inventory based on the detected devices.
- The customer approach of EY professionals covered all aspects of OT security transformation – from asset identification and technical architecture design through process redefinition to organization structure, governance and operating model definition – to support the execution of the proposed OT security program.

Client challenges

- The client's biggest challenge was to introduce the solution to the current diverse environment with plants dispersed all over the world.
- A serious obstacle was the lack of internal, global standards for network infrastructure and the need to implement the solution at all facilities at the same time.
- The solution had to comply with all regulations concerning the pharmaceutical sector.

Client benefits

- Monitor more than 60,000 plus assets in over 90 production sites globally
- Detect anomalous behaviors and vulnerabilities within the production, laboratory and warehouse areas
- Support in asset management and update of the OT cyber inventory at production sites
- Identify network misconfiguration and risks within industrial networks

EY and Microsoft

The digital technologies that are impacting your business today – social, mobile, analytics and cloud – are rapidly expanding to create new employee and customer experiences, fundamentally changing how your organization works, interacts and competes. The EY and Microsoft alliance combines EY deep insights and experience in disruptive industry trends, new business models and evolving processes with Microsoft scalable, enterprise cloud platform and digital technologies. EY and Microsoft can help accelerate digital transformation with advanced solutions that support enterprise strategy, transform customer and workforce experiences, create new, data-driven business models, build intelligent, automated operations and bring confidence that these innovative solutions are secure, compliant and trusted. Together, we can help accelerate digital strategy and amplify your business performance to thrive in a digital world.

For more information, visit: ey.com/microsoft.

Contact information

EY contacts:

Piotr Ciepiela
Partner
EY Global Cyber Architecture, Engineering
& Emerging Technologies Leader
Ernst & Young sp. zoo Consulting sp. k.
piotr.ciepiela@pl.ey.com

Microsoft contacts:

Jodi Lustgarten
Microsoft Alliance Director
Microsoft Corporation
jodise@microsoft.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

EYG No. 005559-21Gbl

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as legal, accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com