Microsoft Defender for IoT for Manufacturing

The needs of the manufacturing industry are constantly evolving, requiring a new security solution that can identify, analyze and react to the ever-changing threat attacks.

Digital transformation and the IoT/OT security challenge

As organizations increasingly rely on intelligent devices to optimize efficiency, experts predict CISOs will soon be responsible for securing an attack surface 3x larger than just a few years ago.

These devices are often unmanaged, unpatched, misconfigured, and unmonitored—making them ideal access points for attackers looking to compromise organizations of all kinds.

The business risks include production downtime, theft of sensitive IP, and even safety and environmental incidents.

Microsoft Defender for IoT is an agentless solution for unified asset discovery and security monitoring across all types of unmanaged devices, including:

- **Enterprise IoT (EIoT) devices** such as VoIP phones, conferencing systems, printers, and building automation systems
- **Operational Technology (OT) devices** used in critical industries like manufacturing, energy utilities, and oil & gas (PLCs, DCUs, HMIs, engineering workstations, historians, etc., including legacy Windows systems)

Benefits for manufacturing

Gain visibility into OT devices and beyond

Achieve a holistic view of the IoT/OT device inventory and manage security from a single interface

Stay up to date on vulnerabilities and risks

Feel at ease with constant visibility of IoT/OT device activity and real-time discovery of vulnerabilities

Respond to incidents with confidence

Receive prioritized recommendations for remediation and contextual guidance on the attackers and their TTPs

Continuous visibility into IoT/OT assets, vulnerabilities, and threats

Defender for IoT is a network detection and response (NDR) solution purpose-built for discovering and securing IoT/OT devices. Leveraging IoT/OT-aware behavioral analytics and threat intelligence, it goes beyond signature-based solutions to catch modern threats like zero-day malware and living-off-the-land tactics missed by static indicators of compromise (IOCs).

Key use cases include:

- **IoT/OT asset discovery:** What devices do we have, how are they communicating, and how can we use this information to accelerate network segmentation initiatives for Zero Trust?
- **IoT/OT vulnerability management:** What is our IoT/OT security score? What are key risks to our most important, "crown jewel" assets—and how do we prioritize patching and mitigation?
- **Continuous threat monitoring, threat hunting and incident response:** How do we know if we have any IoT/OT threats in our network? How do we strengthen Zero Trust by instantly detecting unauthorized or compromised IoT/OT devices?
- **Operational efficiency:** How do we rapidly troubleshoot inefficiencies and reduce downtime from misconfigured or malfunctioning IoT/OT equipment?
- **Unified IT/OT security and governance:** How do we integrate with existing SOC workflows and tools (Microsoft Sentinel and Microsoft Defender 365, plus Splunk, IBM QRadar, ServiceNow, etc.) to rapidly respond to and mitigate threats?

Real-world IoT and OT attack examples

IoT

VoIP phones and office printers used to gain access to corporate networks

Microsoft discovered an IoT campaign in which attackers exploited vulnerabilities such as default admin credentials and missing patches on a phone and printer. After establishing initial beachheads on compromised devices, the attackers scanned the network for other insecure devices. They enumerated administrative groups in search of privileged accounts for access to high value data. As they moved between devices, they dropped a shell script to establish persistence. Analysis of network traffic showed the devices were also communicating with the same C2 server as the DROVORUB campaign targeting Linux devices.

Malware exploits vulnerabilities in smart building access systems

Researchers uncovered a malware campaign that exploits critical vulnerabilities in smart building access systems, for which the manufacturer has never released a patch. These smart building systems control the doors that employees and visitors can access based on their access codes or smart cards. Attackers are actively targeting thousands of devices every day in over 100 countries, with most attacks observed in the U.S. These attacks can lead to "siegeware" which prevents employees from entering or leaving a building.

Attackers heavily targeting VPN vulnerabilities

Cyber adversaries are actively targeting VPN vulnerabilities more than other attack avenues to break into enterprise networks. These devices are ideal access points because they can be compromised from the internet and provide immediate access to corporate networks.

OT

Oil pipeline carrying over 3 million barrels a day shut down

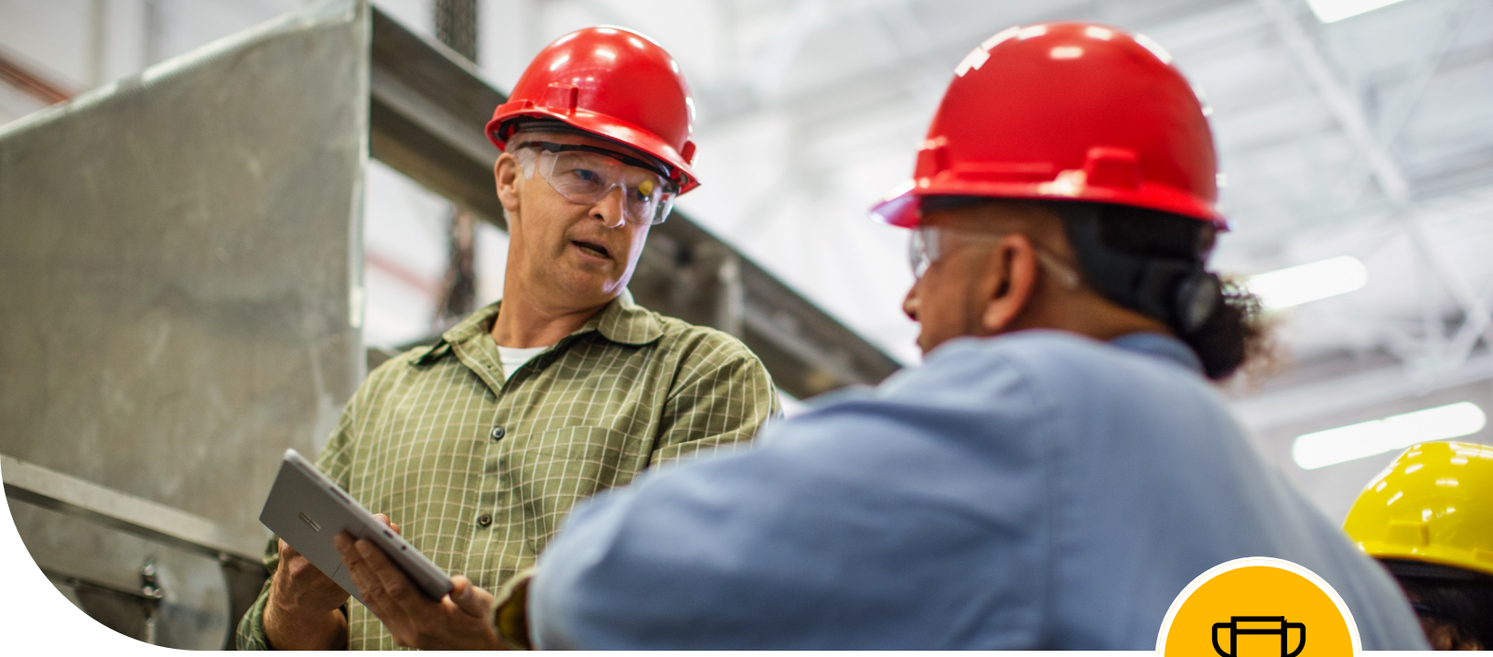
This attack by the DarkSide cybercriminal organization shut down production when the company disconnected it's OT systems to ensure safety of industrial operations. The incident demonstrates how IT and OT networks are now so interconnected that an attack on either one will disrupt the other, causing numerous cascading effects.

TRITON attack on safety controllers in a petrochemical facility

Attackers initially compromised the IT network and then stole RDP credentials to pivot to the OT network through the firewall separating IT from OT. Then they installed custom malware on an engineering workstation followed by a specially-crafted backdoor in safety controllers, intending to cause a major safety and environmental incident. The attack failed due to bugs in the attackers' malware, but they managed to shut down the facility for two weeks, causing an estimated revenue loss of more than $5M.

Attack on global food processor shuts down all US plants

The attack by REvil, a Russian-speaking gang, stopped all US production and resulted in a ransom payout of $11 million. The attack started in Australia, with the initial intrusion vector suspected to be via remote access protocols such as RDP and TeamViewer and/or stolen credentials. At least 40 food companies have been targeted by ransomware gangs over the last year.



Microsoft Security: a Leader in six Gartner Magic Quadrants[1] including the Magic Quadrant for IoT Platforms and SIEM.

Microsoft Security is also recognized as a leader for real-world detection in the 2022 MITRE Engenuity ATT&CK® Evaluations[2], a dedicated test for ICS.

Why Microsoft Defender for IoT

We know what it takes.

The key thing to remember about Defender for IoT is that you get one solution for security across all IoT and OT use cases. More importantly, it integrates with your entire security information and event management (SIEM) and extended detection and response (XDR) platforms, and interoperates with other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

- Gain full visibility into assets and risks 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 Microsoft Azure-connected, or in hybrid environments

[1] GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[2] MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. With the creation and stewardship of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.