Microsoft Defender for IoT:
Agentless IoT and OT security, integrated with Microsoft SIEM and XDR

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 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)

Seamless sharing of IoT/OT asset and threat data across platforms

Microsoft Defender for IoT is an agentless IoT/OT security monitoring solution that shares rich telemetry with our SIEM/SOAR and XDR solutions to enable rapid detection and response across both IT and OT networks. It also integrates out-of-the-box with third-party SOC tools such as Splunk, IBM QRadar, and ServiceNow.
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 I have, how are they communicating, and how can I 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 & 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 Defender 365, plus Splunk, IBM QRadar, ServiceNow, etc.) to rapidly respond and mitigate threats?

Real-world IoT and OT attack examples

**VolP 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 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.

**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 its 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 2 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.
Fast and frictionless deployment

The solution’s agentless technology delivers deep visibility into IoT/OT risk within minutes of being connected to the network, with zero impact due to its passive, non-invasive, network traffic analysis (NTA) approach. Network traffic is captured by an on-premises sensor that connects to a SPAN port or TAP. Existing Microsoft Defender for Endpoint instances can also be used as sensors to discover enterprise IoT devices located on the same segment and capture IoT-related events. This immediately enriches Microsoft 365 Defender workflows and attack timelines, without any additional deployment.

The solution can be deployed fully on-premises, connected to Azure, or in hybrid environments.

Centralized management for globally-distributed sites

Network sensors can be centrally provisioned and managed from the Azure portal, reducing complexity and manual effort. Sensors can be configured to receive continuous threat intelligence updates incorporating vulnerability and IoC data specifically tailored for IoT and OT devices.
View incidents and vulnerabilities involving IoT devices in a single XDR dashboard.

View enterprise IoT asset inventory in a single unified view that also includes desktops, servers, and network devices.

Discovered devices.
OT asset discovery and network topology mapping

Analyze diverse industrial protocols to visualize OT network topology and communication paths. Accelerate network segmentation initiatives. Identify equipment details such as manufacturer, device type, serial number, firmware level, and backplane layouts. Quickly identify the root cause of operational issues such as misconfigured devices and networks.

OT vulnerability management

Proactively address vulnerabilities such as unpatched devices, unauthorized Internet connections, and subnet connections. Prioritize fixes based on risk scoring and automated threat modeling. Demonstrate continuous improvement on overall security score.

Threat alert timeline

Rapidly triage real-time alerts, investigate historical traffic, and hunt for threats. Catch modern threats like zero-day malware and living-off-the-land tactics missed by static IOCs. Explore full-fidelity packet captures (PCAPs) for deeper analysis.
Microsoft Security is a Leader in five Gartner Magic Quadrants\(^1\) and eight Forrester Wave™ categories, including The Forrester New Wave™: Extended Detection and Response (XDR), Q4, 2021\(^2\).

About Microsoft Defender for IoT

We know what it takes.

Defender for IoT offers agentless, IoT/OT-aware network detection and response (NDR) that is rapidly deployed and provides unified security across diverse IoT and industrial devices. It shares data seamlessly with Microsoft’s SIEM and XDR platforms—Microsoft Sentinel and Microsoft 365 Defender—and interoperates with other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

Gain full visibility into assets and risk 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 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 designations. 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.

\(^2\) The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester’s call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

© Microsoft Corporation. All rights reserved. This material is provided for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESSED OR IMPLIED.