# 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 that just a few years ago.

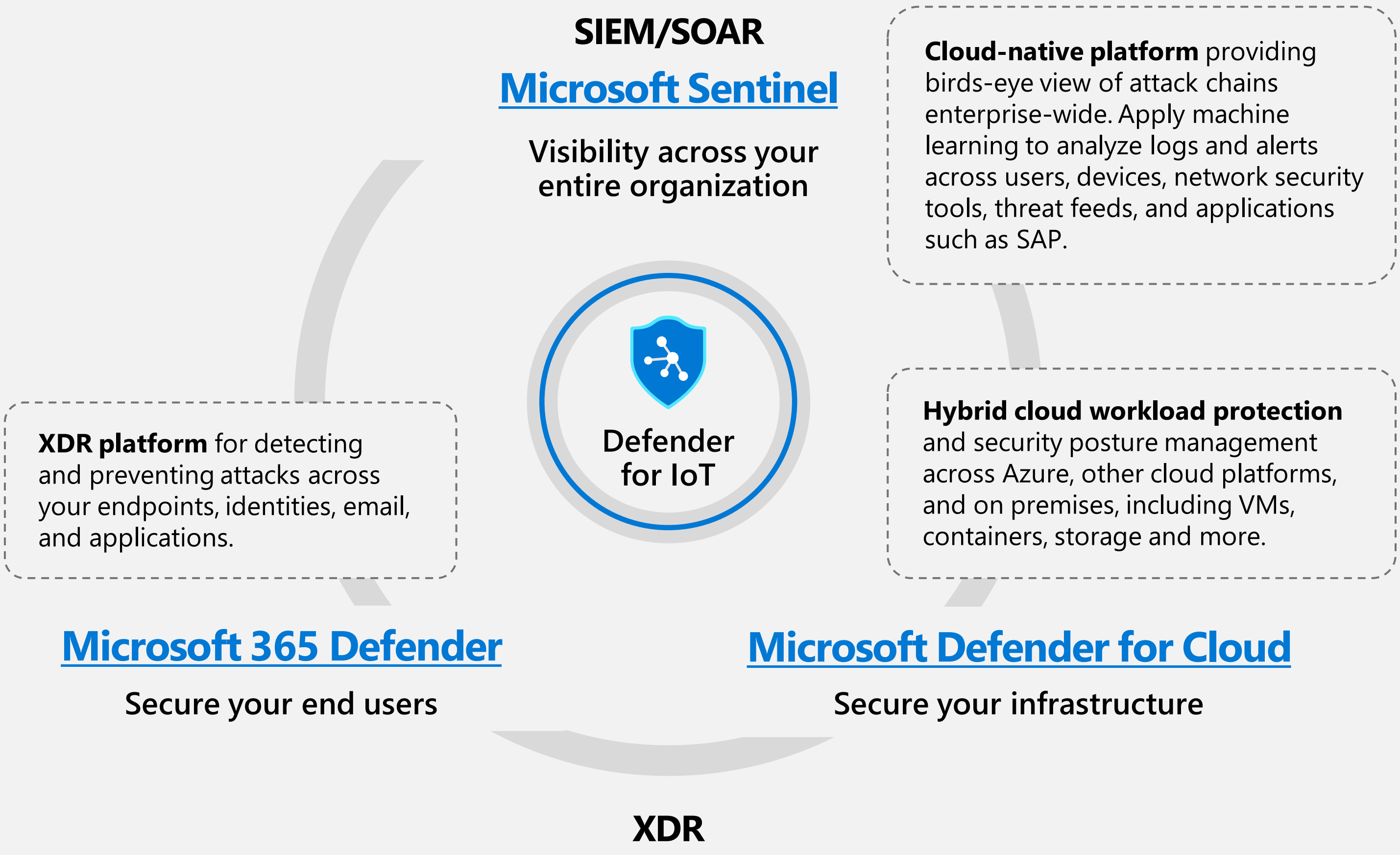
These devices are often unmanaged, unpatched, misconfigured, and unmonitored—making them ideal access points for attackers looking to compromise organizations of all kinds.

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



**SIEM/SOAR**

**Microsoft Sentinel**

Visibility across your entire organization

**Cloud-native platform** providing birds-eye view of attack chains enterprise-wide. Apply machine learning to analyze logs and alerts across users, devices, network security tools, threat feeds, and applications such as SAP.

Defender for IoT

**XDR platform** for detecting and preventing attacks across your endpoints, identities, email, and applications.

**Hybrid cloud workload protection** and security posture management across Azure, other cloud platforms, and on premises, including VMs, containers, storage and more.

**Microsoft 365 Defender**

Secure your end users

**Microsoft Defender for Cloud**

Secure your infrastructure

**XDR**

*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

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 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 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.

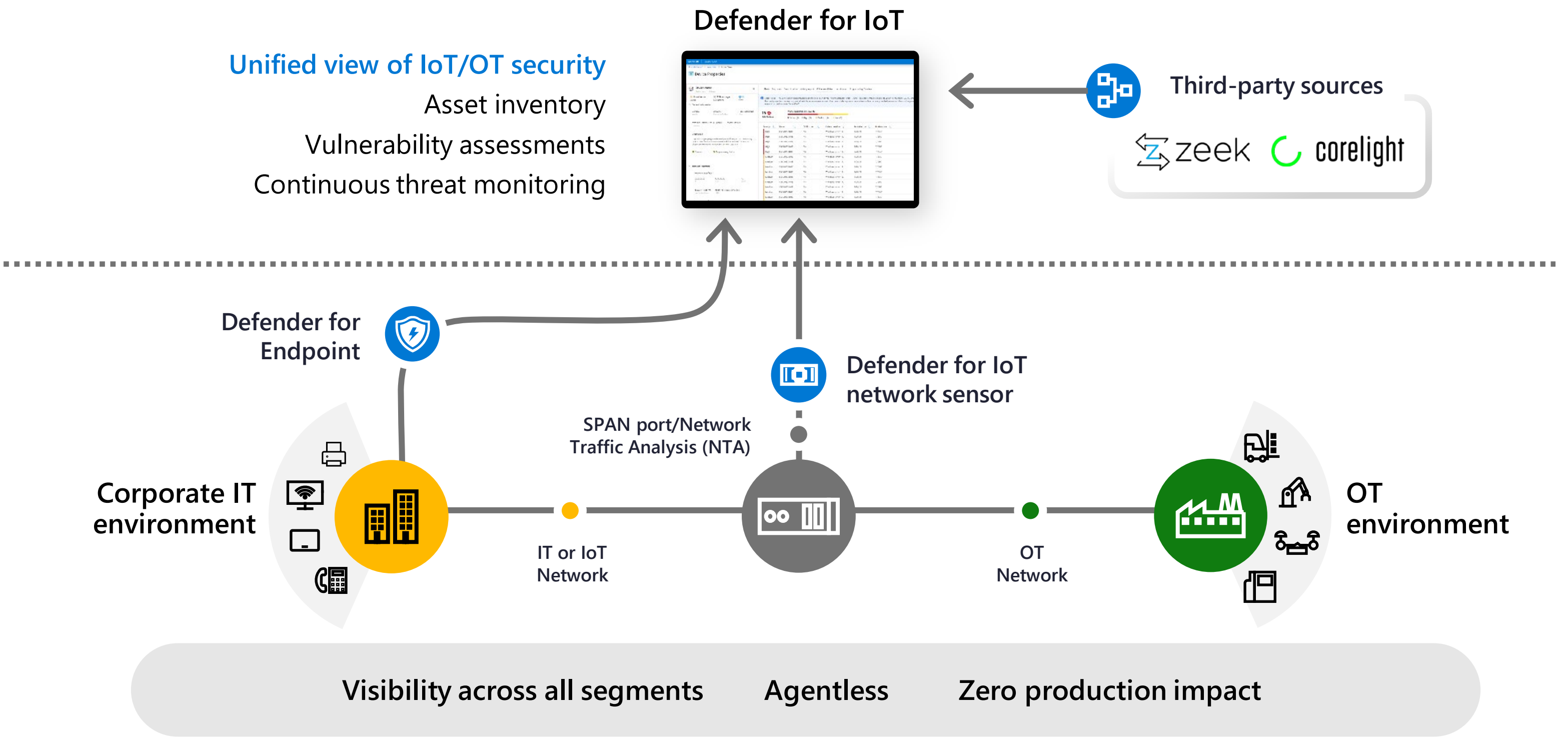
### Attack on global food processor shuts down all US plants

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

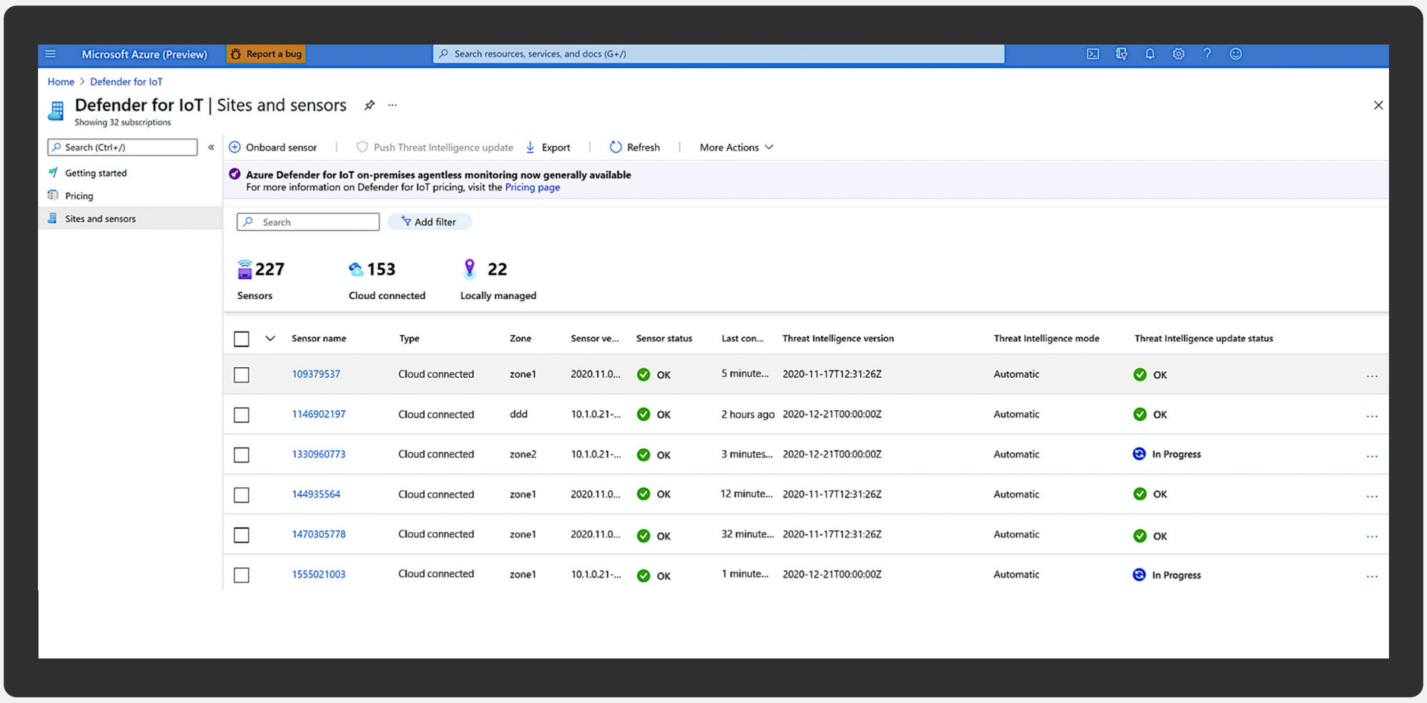
The solution's agentless technology delivers deep visibility into IoT/OT risk within minutes of being connected to the network, with zero impact due to its passive, non-invasive, network traffic analysis (NTA) approach. Network traffic is captured by an on-premises sensor that connects to a SPAN port 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.**


Defender for IoT
Unified view of IoT/OT security
Asset inventory
Vulnerability assessments
Continuous threat monitoring
Third-party sources
zeek
corelight
Defender for Endpoint
Defender for IoT network sensor
SPAN port/Network Traffic Analysis (NTA)
Corporate IT environment
IT or IoT Network
OT Network
OT environment
Visibility across all segments
Agentless
Zero production impact

## 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.



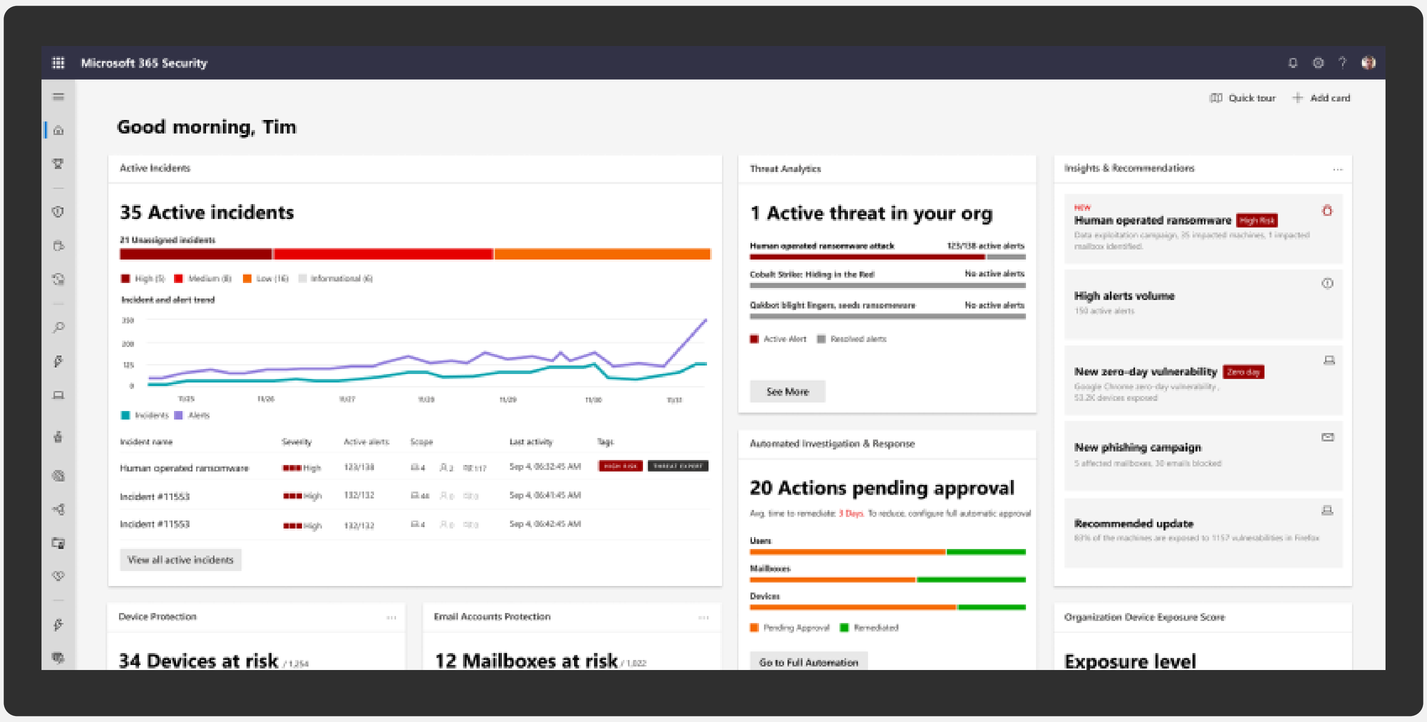
Defender for IoT | Sites and sensors

Showing 32 subscriptions

**Azure Defender for IoT on-premises agentless monitoring now generally available**
For more information on Defender for IoT pricing, visit the Pricing page

227 Sensors | 153 Cloud connected | 22 Locally managed

| ☐ | Sensor name | Type | Zone | Sensor ve... | Sensor status | Last con... | Threat Intelligence version | Threat Intelligence mode | Threat Intelligence update status | |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 109379537 | Cloud connected | zone1 | 2020.11.0... | ✓ OK | 5 minute... | 2020-11-17T12:31:26Z | Automatic | ✓ OK | ... |
| ☐ | 1146902197 | Cloud connected | ddd | 10.1.0.21-... | ✓ OK | 2 hours ago | 2020-12-21T00:00:00Z | Automatic | ✓ OK | ... |
| ☐ | 1330960773 | Cloud connected | zone2 | 10.1.0.21-... | ✓ OK | 3 minutes... | 2020-12-21T00:00:00Z | Automatic | In Progress | ... |
| ☐ | 144935564 | Cloud connected | zone1 | 2020.11.0... | ✓ OK | 12 minute... | 2020-11-17T12:31:26Z | Automatic | ✓ OK | ... |
| ☐ | 1470305778 | Cloud connected | zone1 | 2020.11.0... | ✓ OK | 32 minute... | 2020-11-17T12:31:26Z | Automatic | ✓ OK | ... |
| ☐ | 1555021003 | Cloud connected | zone1 | 10.1.0.21-... | ✓ OK | 1 minute... | 2020-12-21T00:00:00Z | Automatic | In Progress | ... |



Microsoft 365 Security

Quick tour | Add card

Good morning, Tim

Active Incidents

35 Active incidents

21 Unassigned incidents

🟥 High (5) 🟥 Medium (8) 🟧 Low (16) ⬜ Informational (6)

Incident and alert trend

| Incident name | Severity | Active alerts | Scope | Last activity | Tags |
|---|---|---|---|---|---|
| Human operated ransomware | High | 123/138 | 4 2 117 | Sep 4, 06:32:45 AM | HIGH RISK THREAT EXPERT |
| Incident #11553 | High | 132/132 | 44 0 0 | Sep 4, 06:41:45 AM | |
| Incident #11553 | High | 132/132 | 4 0 0 | Sep 4, 06:42:45 AM | |

View all active incidents

Threat Analytics

1 Active threat in your org

| | |
|---|---|
| Human operated ransomware attack | 123/138 active alerts |
| Cobalt Strike: Hiding in the Red | No active alerts |
| Qakbot blight lingers, seeds ransomware | No active alerts |

🟥 Active Alert ⬜ Resolved alerts

See More

Insights & Recommendations

NEW
Human operated ransomware High Risk
Data exploitation campaign, 35 impacted machines, 1 impacted mailbox identified.

High alerts volume
150 active alerts

New zero-day vulnerability Zero day
Google Chrome zero-day vulnerability, 53.2K devices exposed

New phishing campaign
5 affected mailboxes, 30 emails blocked

Recommended update
83% of the machines are exposed to 1157 vulnerabilities in Firefox

Automated Investigation & Response

20 Actions pending approval

Avg. time to remediate: 3 Days. To reduce, configure full automatic approval

Users

Mailboxes

Devices

🟧 Pending Approval 🟩 Remediated

Go to Full Automation

Device Protection

34 Devices at risk / 1,254

Email Accounts Protection

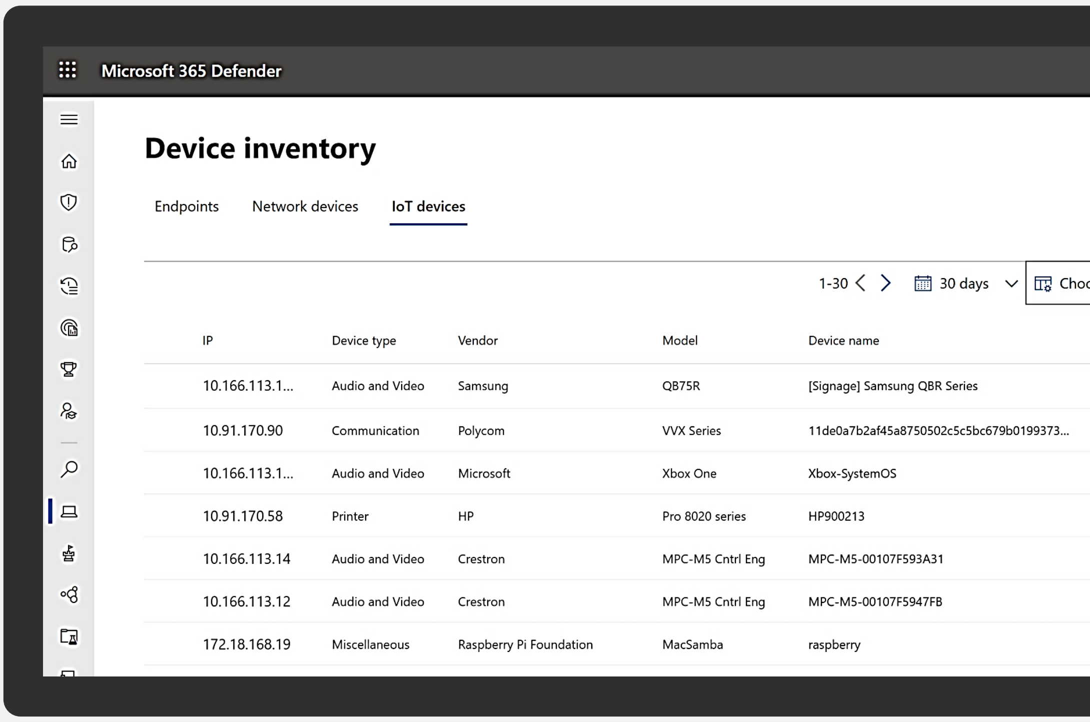
12 Mailboxes at risk / 1,022

Organization Device Exposure Score

Exposure level

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



Microsoft 365 Defender

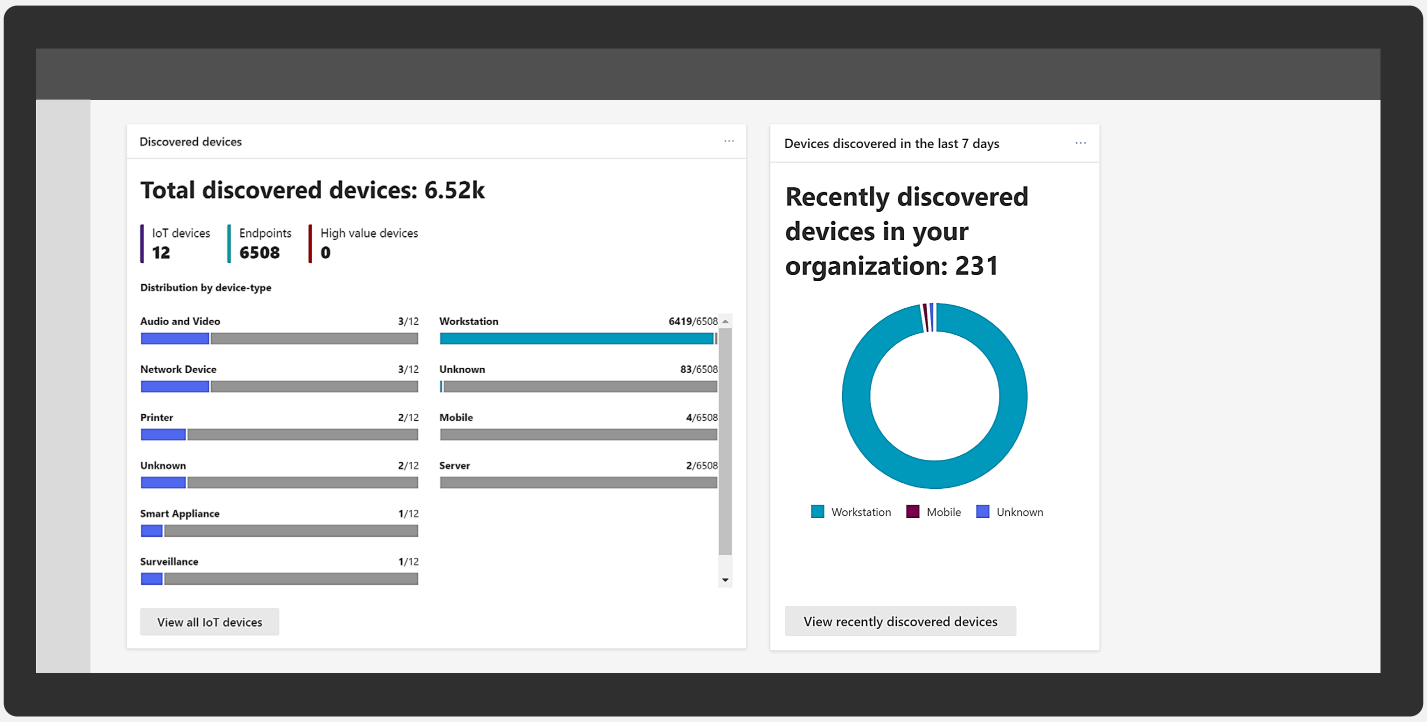
Device inventory

Endpoints | Network devices | IoT devices

1-30 | 30 days | Choo

| IP | Device type | Vendor | Model | Device name |
|---|---|---|---|---|
| 10.166.113.1... | Audio and Video | Samsung | QB75R | [Signage] Samsung QBR Series |
| 10.91.170.90 | Communication | Polycom | VVX Series | 11de0a7b2af45a8750502c5c5bc679b0199373... |
| 10.166.113.1... | Audio and Video | Microsoft | Xbox One | Xbox-SystemOS |
| 10.91.170.58 | Printer | HP | Pro 8020 series | HP900213 |
| 10.166.113.14 | Audio and Video | Crestron | MPC-M5 Cntrl Eng | MPC-M5-00107F593A31 |
| 10.166.113.12 | Audio and Video | Crestron | MPC-M5 Cntrl Eng | MPC-M5-00107F5947FB |
| 172.18.168.19 | Miscellaneous | Raspberry Pi Foundation | MacSamba | raspberry |

Discovered devices



Discovered devices

Total discovered devices: 6.52k

| IoT devices | Endpoints | High value devices |
|---|---|---|
| 12 | 6508 | 0 |

Distribution by device-type

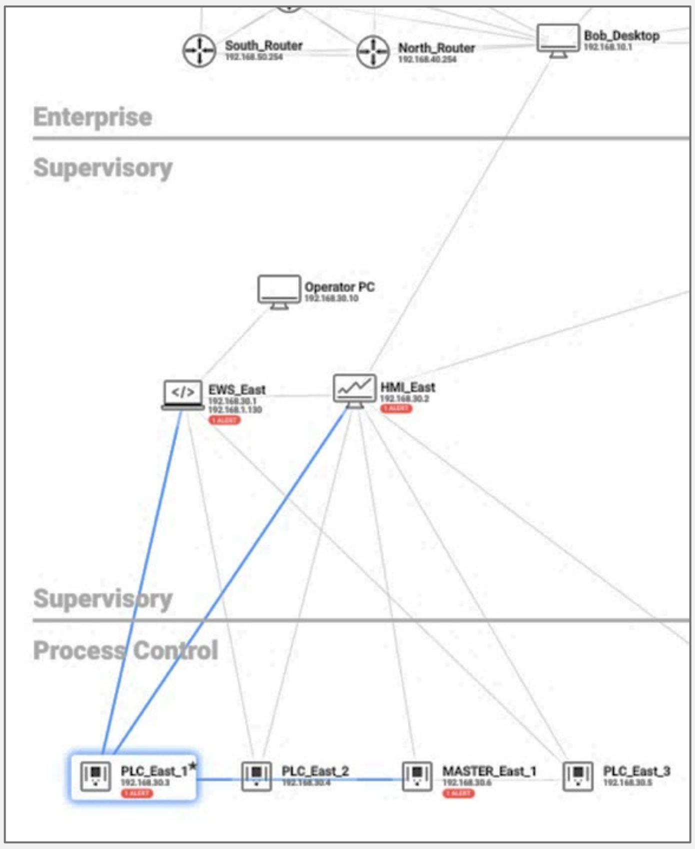
| Device type | Count |
|---|---|
| Audio and Video | 3/12 |
| Network Device | 3/12 |
| Printer | 2/12 |
| Unknown | 2/12 |
| Smart Appliance | 1/12 |
| Surveillance | 1/12 |
| Workstation | 6419/6508 |
| Unknown | 83/6508 |
| Mobile | 4/6508 |
| Server | 2/6508 |

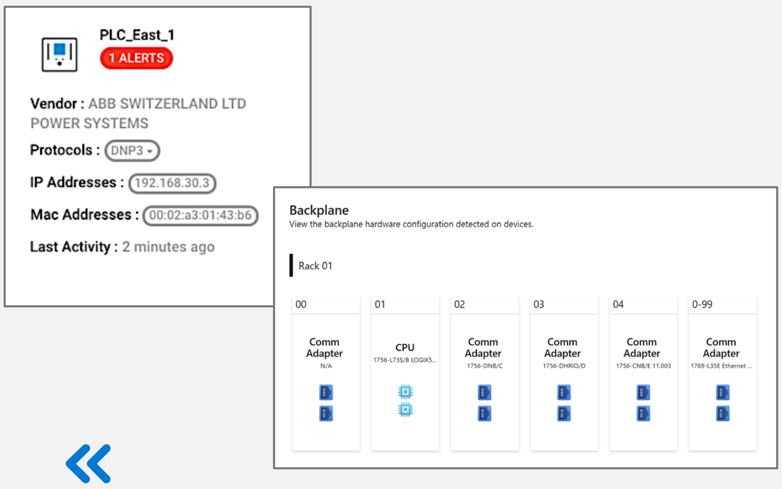
View all IoT devices

Devices discovered in the last 7 days

Recently discovered devices in your organization: 231

View recently discovered devices




PLC_East_1

1 ALERTS

**Vendor :** ABB SWITZERLAND LTD POWER SYSTEMS

**Protocols :** DNP3

**IP Addresses :** 192.168.30.3

**Mac Addresses :** 00:02:a3:01:43:b6

**Last Activity :** 2 minutes ago

Backplane

View the backplane hardware configuration detected on devices.

Rack 01

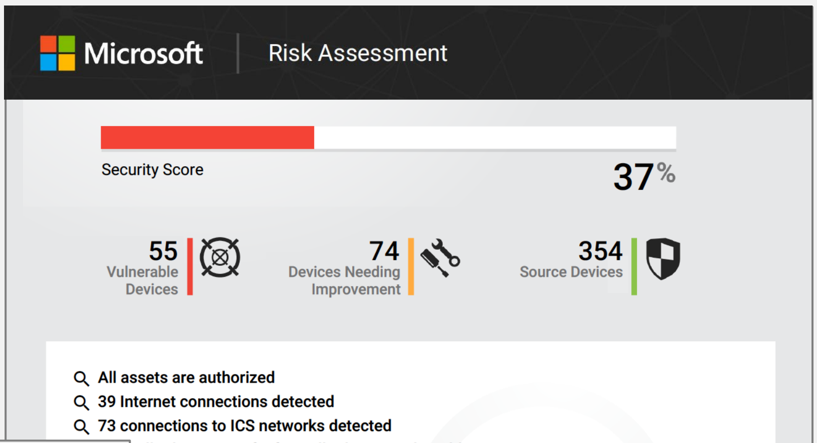
| 00 | 01 | 02 | 03 | 04 | 0-99 |
|---|---|---|---|---|---|
| Comm Adapter<br>N/A | CPU<br>1756-L73S/B LOGIX5... | Comm Adapter<br>1756-DNB/C | Comm Adapter<br>1756-DHRIO/D | Comm Adapter<br>1756-CNB/E 11.003 | Comm Adapter<br>1769-L35E Ethernet ... |

## 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.


Microsoft | Risk Assessment

Security Score 37%

55 Vulnerable Devices

74 Devices Needing Improvement

354 Source Devices

All assets are authorized

39 Internet connections detected

73 connections to ICS networks detected

vall rules: 0 out of 0 firewall rules are vulnerable

ackup servers detected

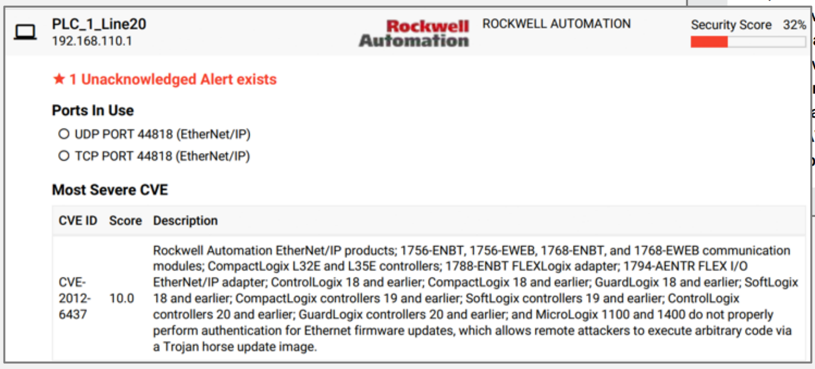
vices accessible remotely

ngineering stations detected

anning device detected

V software detected

attack vectors generated (highest risk)


PLC_1_Line20
192.168.110.1

Rockwell Automation ROCKWELL AUTOMATION

Security Score 32%

★ 1 Unacknowledged Alert exists

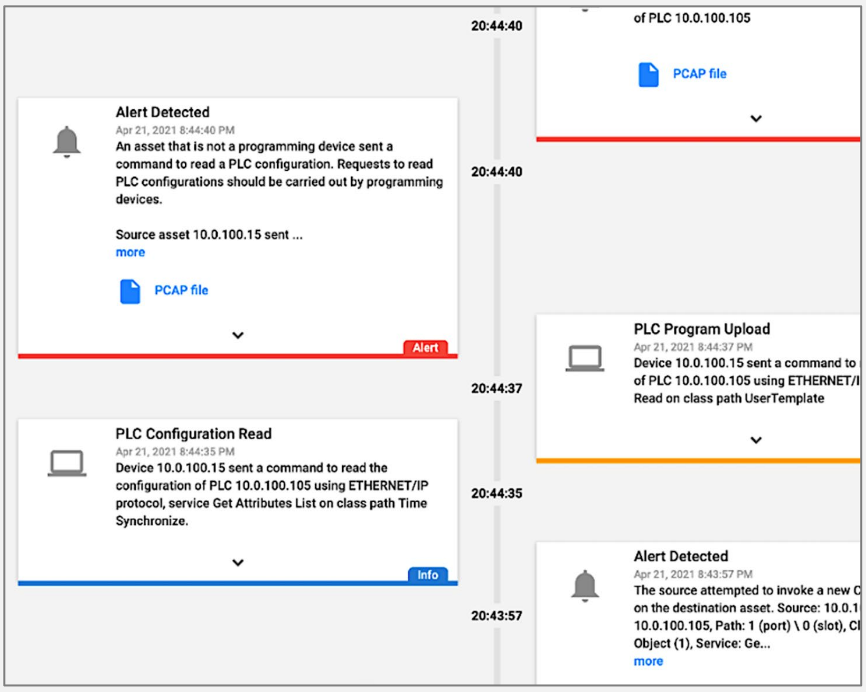
**Ports In Use**

○ UDP PORT 44818 (EtherNet/IP)

○ TCP PORT 44818 (EtherNet/IP)

**Most Severe CVE**

| CVE ID | Score | Description |
|---|---|---|
| CVE-2012-6437 | 10.0 | Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image. |


20:44:40

of PLC 10.0.100.105

PCAP file

Alert Detected
Apr 21, 2021 8:44:40 PM
An asset that is not a programming device sent a command to read a PLC configuration. Requests to read PLC configurations should be carried out by programming devices.

Source asset 10.0.100.15 sent ...
more

PCAP file

Alert

20:44:40

PLC Program Upload
Apr 21, 2021 8:44:37 PM
Device 10.0.100.15 sent a command to
of PLC 10.0.100.105 using ETHERNET/I
Read on class path UserTemplate

20:44:37

PLC Configuration Read
Apr 21, 2021 8:44:35 PM
Device 10.0.100.15 sent a command to read the configuration of PLC 10.0.100.105 using ETHERNET/IP protocol, service Get Attributes List on class path Time Synchronize.

Info

20:44:35

Alert Detected
Apr 21, 2021 8:43:57 PM
The source attempted to invoke a new C
on the destination asset. Source: 10.0.1
10.0.100.105, Path: 1 (port) \ 0 (slot), Cl
Object (1), Service: Ge...
more

20:43:57

## 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 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] 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.