

# An experts guide to Securing your IoT environment



Paul Rouse  
Senior Security Consultant, Kocho

Paul Roberts  
Technical Specialist – IoT Security, Microsoft

Mitesh Desai  
Director Of Technology, Kocho

## Microsoft Security Mission:

Create a safer world enabling organisations to digitally transform

- Quadrupling cybersecurity investment to \$20 billion over the next five years.
- Microsoft Security is now a \$10B business with 3,500 employees and a Leader in 5 Gartner Magic Quadrant and 7 Forrester Wave reports.
- Recent security acquisitions include CyberX, ReFirm Labs, RiskIQ, and CloudKnox.



# How do we define IoT?

→ Many things to many people

# IT – Information Technology



Laptops



Desktops



Servers

# Next Gen IoT – Internet of Things



Autonomous Cleaning Robots



Smart Prosthetics



Smart Traffic Management Solutions

# Enterprise/Corporate IoT



Multi Function Printers



VoIP Phones / IP Cameras



Smart TV's / Smart Speakers



# OT – Operational Technology



Petroleum Refinery



Industrial Control Systems (ICS)

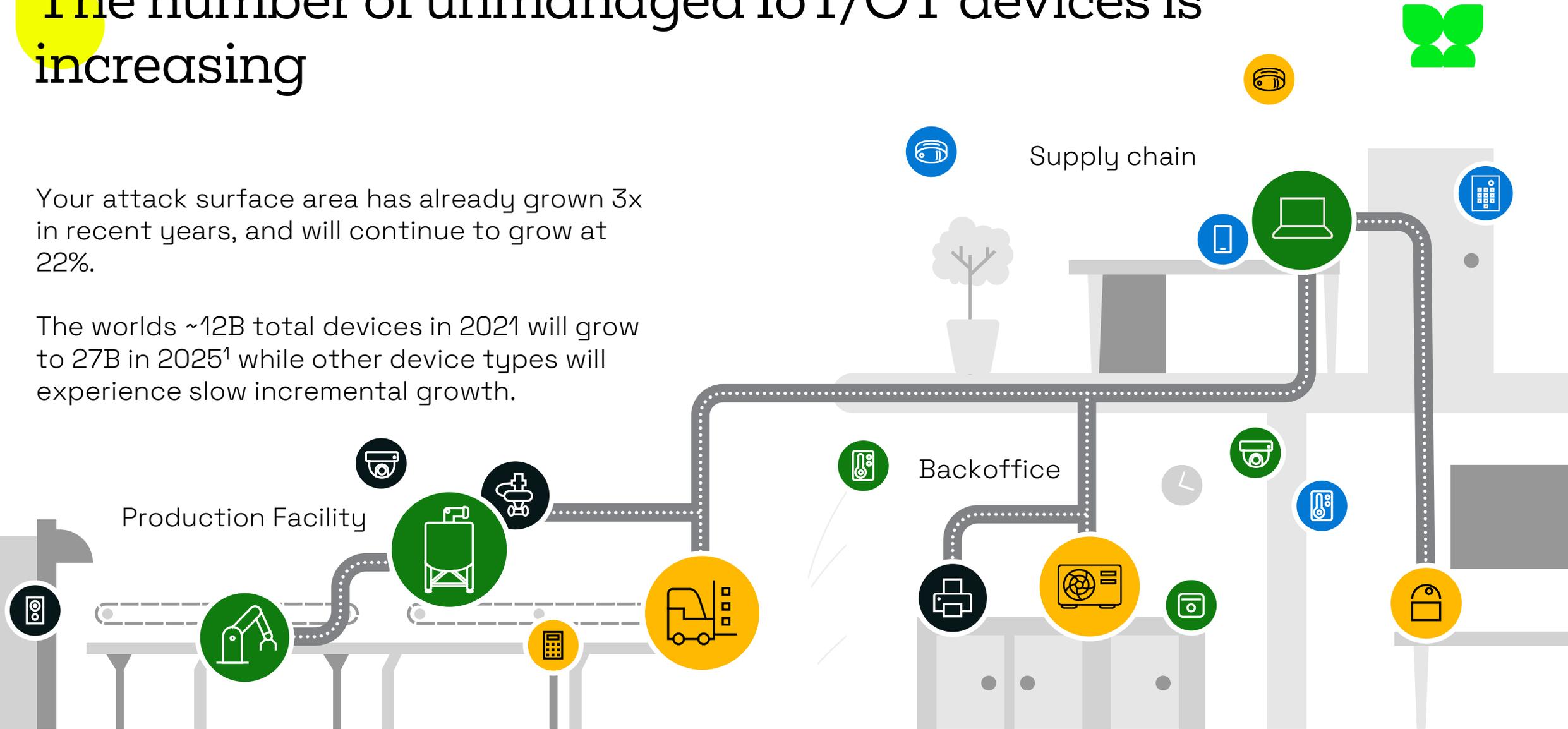


Automated Manufacturing

# The number of unmanaged IoT/OT devices is increasing

Your attack surface area has already grown 3x in recent years, and will continue to grow at 22%.

The world's ~12B total devices in 2021 will grow to 27B in 2025<sup>1</sup> while other device types will experience slow incremental growth.



1. <https://iot-analytics.com/number-connected-iot-devices/>



# Real world attack examples



**ZDNet** SEARCH VIDEO

MUST READ: Firmware attacks are on the rise and you aren't worrying about them enough

## NASA hacked because of unauthorized Raspberry Pi connected to its network

NASA described the hackers as an "advanced persistent threat," a term generally used for nation-state hackers.




**DARKReading** SIGN UP FOR OUR NEWSLETTERS

## Verkada Breach Demonstrates Danger of Overprivileged Users

In re-evaluating supply chains, companies should classify vendors with super admin privileges to devices or backdoors as a significant threat.



**ZDNet** SEARCH VIDEO

## Hackers are attacking smart building access systems

More than 2,300 building access systems can be hijacked due to a severe vulnerability left without a fix.




**ZDNet** SEARCH VIDEO

## Triton hackers return with new, covert industrial attack



Traces of a hacking group behind the destructive Triton malware have been found at a new infrastructure facility following an infamous attack in the Middle East.

**Bloomberg**

## Hackers Breached Colonial Pipeline Using Compromised Password



The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant.

**ZDNet** SEARCH VIDEO

## Microsoft: Russian state hackers are using IoT devices to breach enterprise networks

Microsoft said it detected Strontium (APT28) targeting VoIP phones, printers, and video decoders.

One of Russia's elite state-sponsored hacking groups is going after IoT devices as a way to breach corporate networks, from where they pivot to other more high-value targets.

Attacks have been observed in the wild said the Microsoft Threat Intelligence Center, one of the OS maker's cyber-security divisions.

The OS maker attributed the attacks to a group it calls Strontium, but is also commonly known as APT28 or Fancy Bear.

[SEE ALSO](#)  
10 dangerous app vulnerabilities to watch out for (free PDF)

# Top IoT/OT challenges for CIOs and CISOs



## IoT adoption and risk

68%

organizations say IoT/OT is critical to supporting business innovation and other strategic goals<sup>1</sup>

60%

view IoT/OT security as one of the least secured aspects of their IT/OT infrastructure<sup>1</sup>

31%

of organizations slowing, limiting, or have stopped the adoption of IoT/OT projects due to security concerns<sup>1</sup>

## Technology gaps

71%

of lack a complete inventory of its IoT/OT devices<sup>1</sup>

70%

have low or average confidence that IoT devices are secure (i.e.: vulnerabilities mitigated, securely configured)<sup>1</sup>

61%

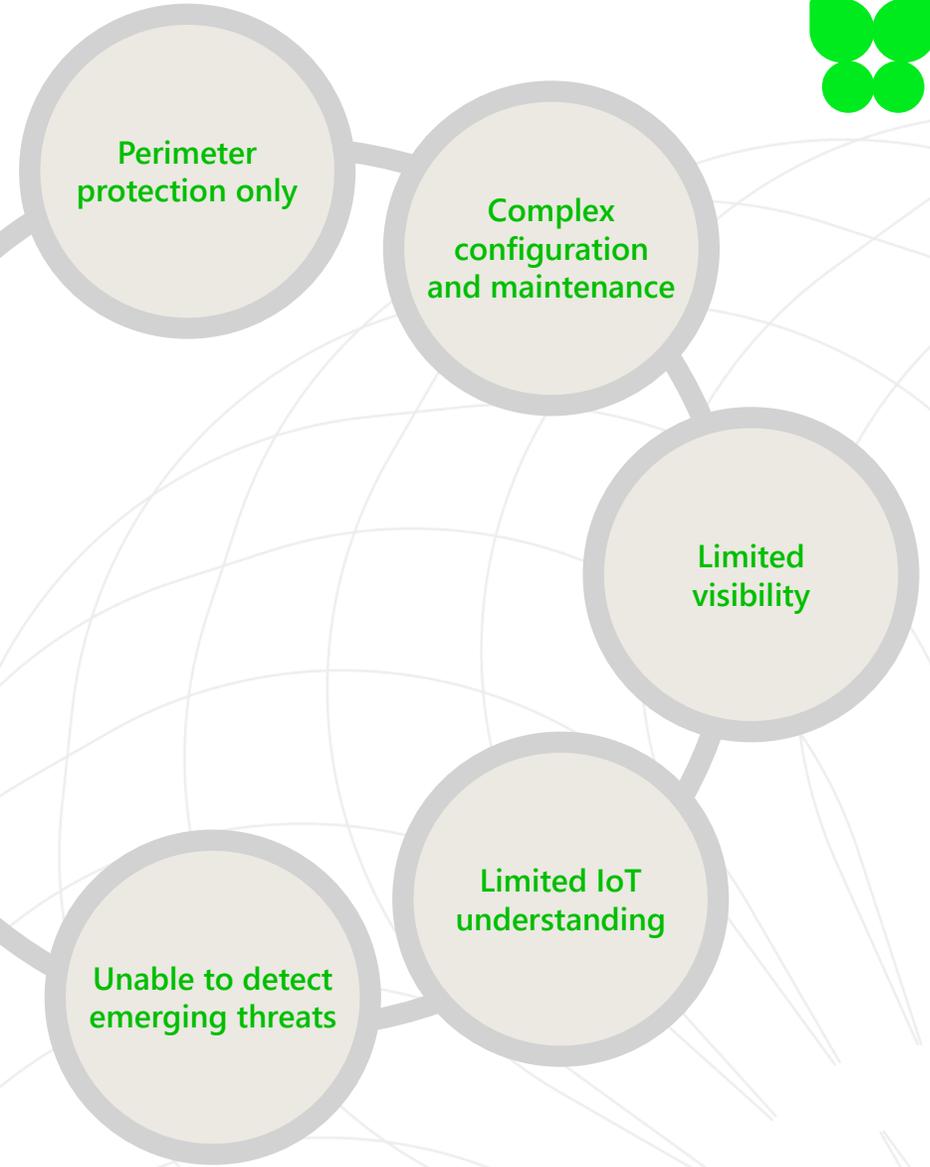
have low or average confidence in the ability to identify whether IoT devices are compromised<sup>1</sup>

1. The State of IoT/OT Cybersecurity in Enterprise Organizations, Ponemon Institute, October 2021



# Challenges with existing solutions

-  Firewalls
-  NAC
-  Vulnerability scanners
-  Agents



# Microsoft Defender for IoT

→ A unified solution for IOT and OT Security

# Architectural principles



**Cloud**

Across the enterprise  
Unified IoT/OT solution  
Continuous monitoring  
and learning



**Corporate**

Easy deployment  
and maintenance  
Agentless  
Integrated IoT/OT approach



## **Discover**

Complete coverage and visibility  
focused on IoT/OT devices



## **Assess**

Risk analysis for any device  
and segment across all networks



## **Detect**

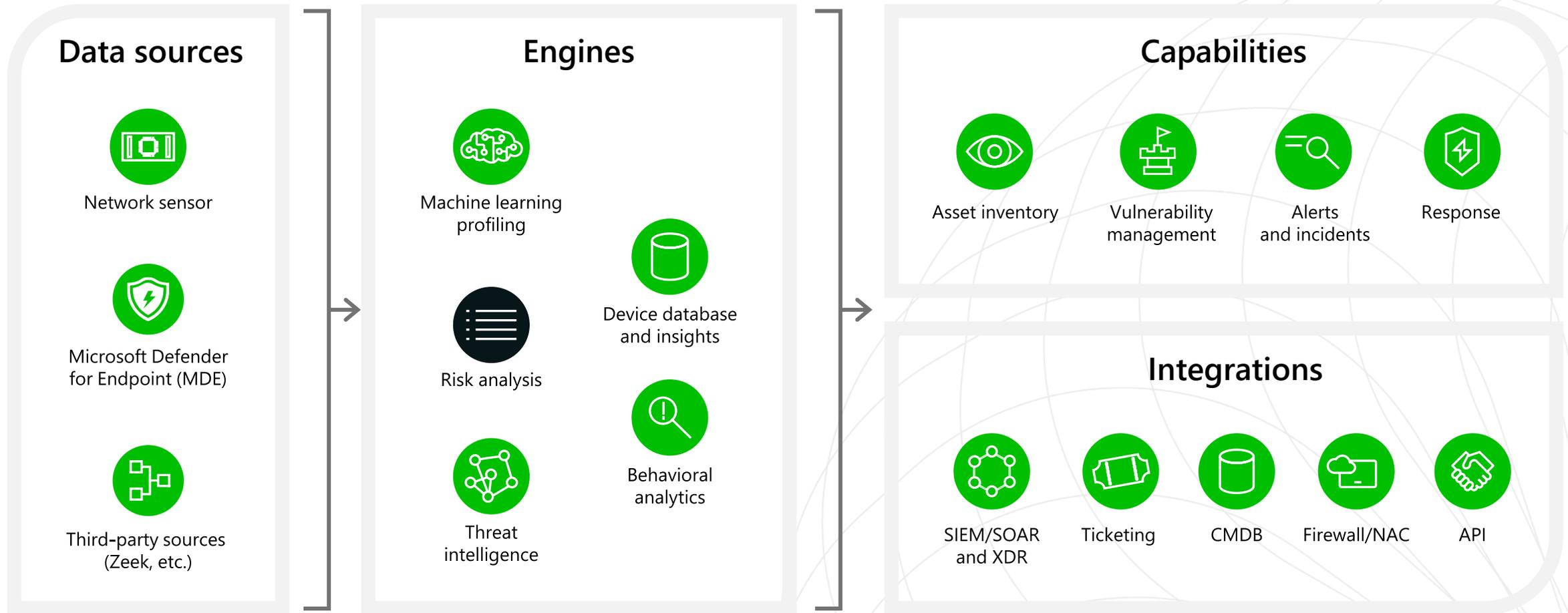
Behavioral analytics and TI built  
to adapt to attacker's speed



## **Respond**

Rapidly identify multi-stage attacks  
across IT/IoT/OT and mitigate with  
automated playbooks

# Solution high-level architecture

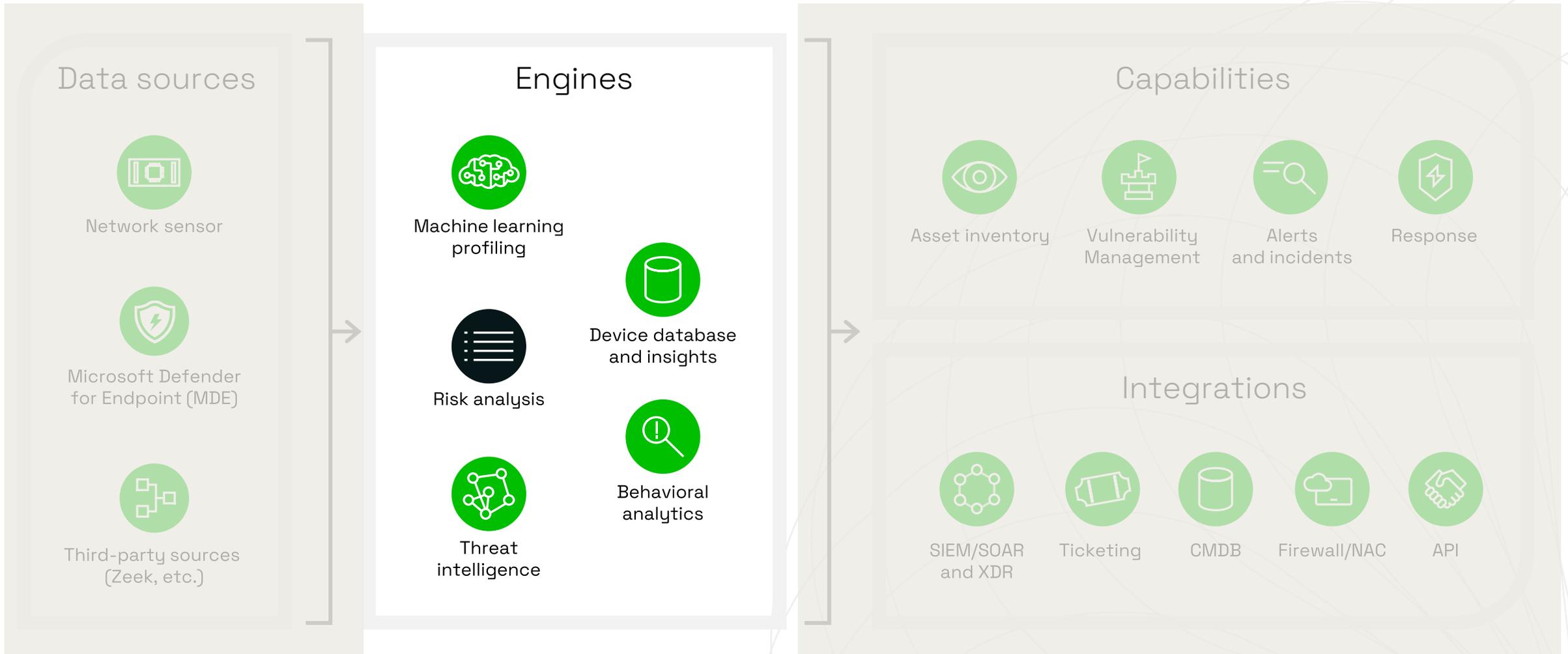


# Solution high-level architecture: Agentless Data sources

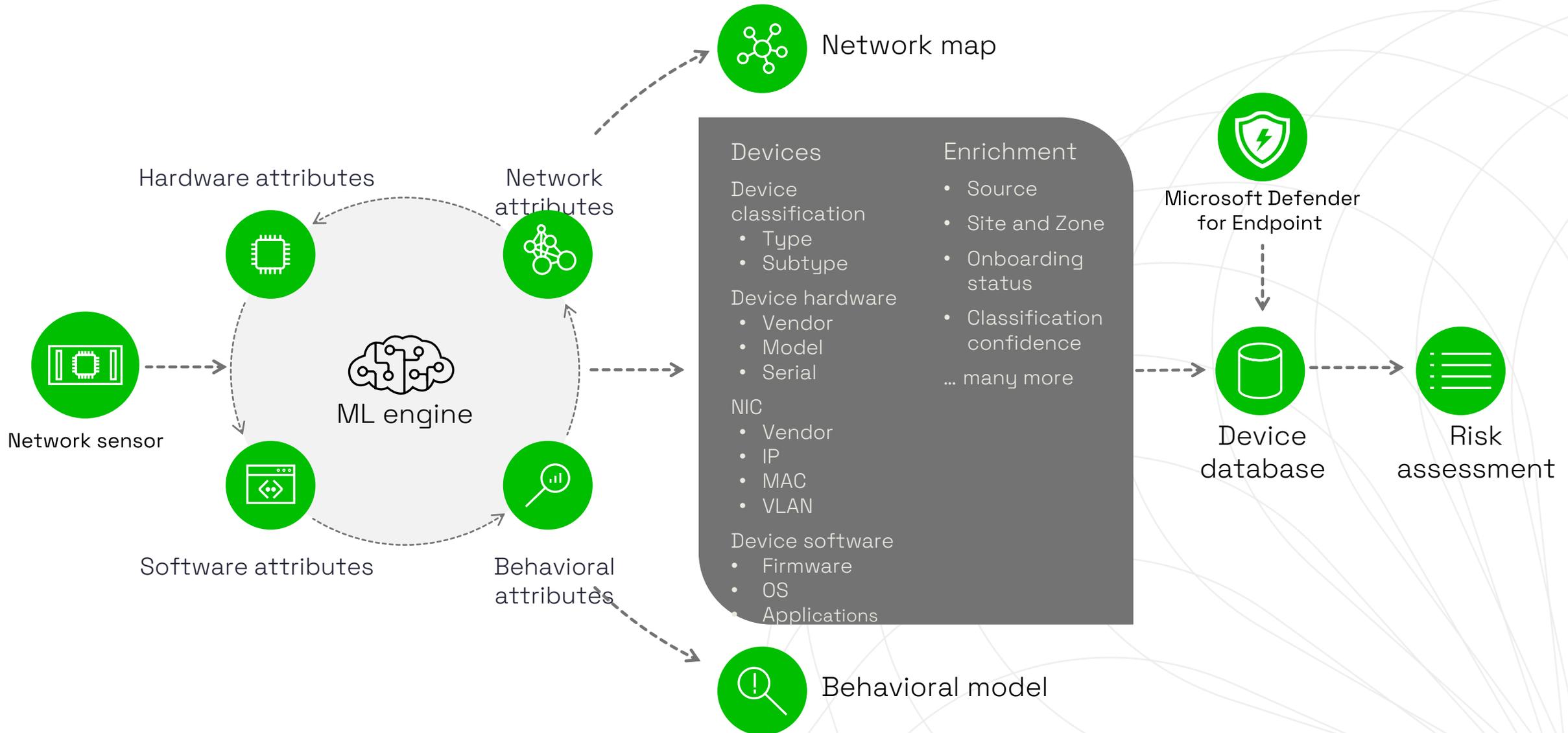




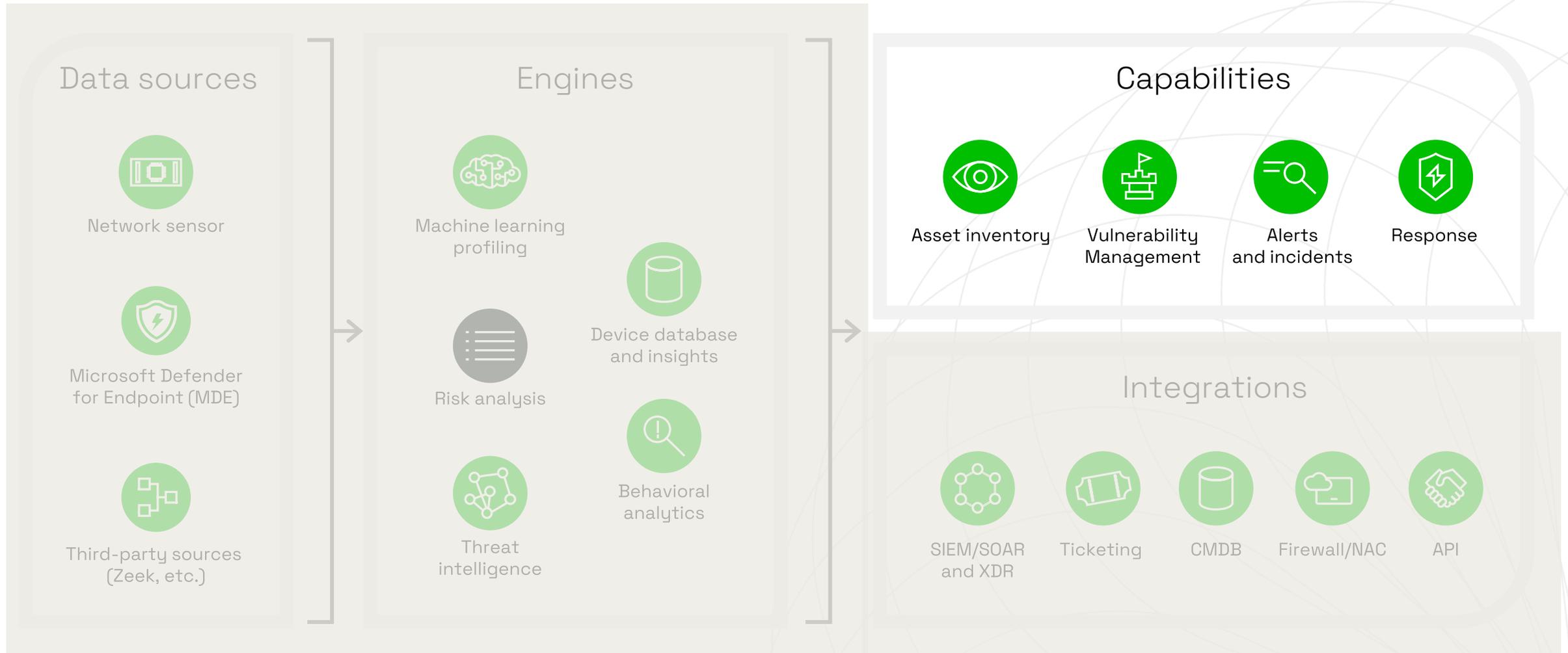
# Solution high-level architecture: Engines



# ML-powered detection for IoT devices



# Solution high-level architecture: Capabilities



# A unified security solution for IoT and OT



Defender for IoT | Device Inventory

Showing subscription 'Rome ILDC - IoT - Integration (Client)'

Search (Ctrl+F)

Refresh | Edit columns | Export

Getting started

Device Inventory

Alerts

Recommendations

Pricing

Sites and sensors

4696 Total devices

13 Important devices

0 New devices

Devices by class

unclassified (2871) | ot (762) | endpoint (697) | iot (345) | 1 more

Device type == 12 selected X

Device class == 1 selected X

Add filter | Reset filters

Showing 345 of 345 devices

Group by | No grouping

Site	IPv4 address	Device name	Device type	Device subtype	Vendor	Device model	MAC address	VLAN
Enterprise...	100.106.35.8	fe4936400732c...	Miscellaneous	Embedded dev...	Universal Glob...	N/A	32:F9:A9:05:44...	N/A
Enterprise...	100.106.35.148	a65a6b9a0803...	Miscellaneous	Embedded dev...	Universal Glob...	N/A	BD:C2:BA:25:46...	N/A
Enterprise...	100.106.35.64	5a73becde58a...	Miscellaneous	Embedded dev...	Universal Glob...	N/A	84:90:C5:07:A2...	N/A
Enterprise...	172.23.13.127	2CD63C5G0E...	Media and Surve	Camera	Hikvision	DS-2CD63C5G...	12:84:54:8C:F5...	N/A
Enterprise...	100.106.35.83	a948aebb37e0...	Miscellaneous	Embedded dev...	Universal Glob...	N/A	3D:4C1D:C2:13...	N/A
Enterprise...	10.10.3.134	7f624e983c0c2...	Miscellaneous	Embedded dev...	Universal Glob...	N/A	08:11:A2:8D:A2...	N/A
Enterprise...	10.166.113.53	TSW-73-7F459...	Audio and Video	Smart Display	Crestron	TSW-730	E2:73:AC:F4:90...	N/A
Enterprise...	100.106.35.131	490560a88aac...	Miscellaneous	Embedded dev...	Universal Glob...	N/A	4F:0E:EA:E2:BF:00	N/A
Enterprise...	10.166.113.62	2350b2356eba...	Communication	N/A	ViaVideo Com...	N/A	99:CB:C6:B7:EF...	N/A
Enterprise...	10.91.168.18	ACXX500-DSCD	Smart Facility	Fire Alarm	First Alert	AC10-500	A2:F5:BC:FB:CD...	N/A

TSW-73-7F459CCC  
HMI

Unauthorized Status

5 months ago Last Seen

0 Alert

General Information

Vendor: Crestron | Model: TSW-730 | OS: Windows

Location: Enterprise1-IoT-NEW\_1 | default

Network Interfaces

IP: 10.166.113.53 | MAC: E2-73-AC-F4-90-7E

View full details



Discover, classify, contextualize all your IoT and OT devices so you can secure the devices accessing your network and resources.

# Integrated Asset Inventory in Microsoft 365 Defender



→ View your complete IT/IoT inventory along side the rest of your IT devices (workstations, servers and mobile) within a single unified view.

The screenshot displays the Microsoft 365 security console interface. The left-hand navigation pane includes sections for general security (Home, Incidents & alerts, Hunting, Action center, Threat analytics, Secure score, Learning hub), Endpoints (Search, Device inventory, Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration & baselines), and Email & collaboration (Investigations, Explorer). The main content area is titled "Device inventory" and has tabs for "Endpoints", "Network devices", and "IoT devices". The "IoT devices" tab is active, showing a table of devices with columns for IP, Device type, Vendor, Model, and Device name. The table lists various audio and video devices from Shure and Crestron, as well as a printer from Xerox.

IP	Device type	Vendor	Model	Device name
[REDACTED]	Audio and Video	Shure	P300	[REDACTED]
[REDACTED]	Audio and Video	Crestron	TSW-730	[REDACTED]
[REDACTED]	Audio and Video	Crestron	MPC-M5 Cntrl Eng	[REDACTED]
[REDACTED]	Audio and Video	Crestron	TSW-730	[REDACTED]
[REDACTED]	Printer	Xerox	AltaLink C8055	[REDACTED]
[REDACTED]	Audio and Video	Crestron	MPC-M5 Cntrl Eng	[REDACTED]
[REDACTED]	Audio and Video	Crestron	TSW-730	[REDACTED]
[REDACTED]	Audio and Video	Crestron	TSW-730	[REDACTED]
[REDACTED]	Audio and Video	Crestron	MPC-M5 Cntrl Eng	[REDACTED]
[REDACTED]	Audio and Video	Crestron	TSW-730	[REDACTED]
[REDACTED]	Audio and Video	Crestron	TSW-730	[REDACTED]
[REDACTED]	Audio and Video	Crestron	TSW-730	[REDACTED]

# Integrated Vulnerability Management in Microsoft 365 Defender



The screenshot displays the Microsoft 365 security dashboard. The left sidebar contains navigation options: Home, Incidents & alerts, Hunting, Action center, Threat analytics, Secure score, Learning hub, Endpoints, Search, Device inventory, Vulnerability management, Dashboard, Recommendations, Remediation, Software inventory, Weaknesses, Event timeline, Partners and APIs, and Evaluation & tutorials. The main content area is titled "Security recommendations" and shows a table of recommendations filtered by "Status: Active +1" and "OS platform: Linux +1". The table has columns for Security recommendation, OS platform, Weaknesses, Related component, and Threats. A green arrow points from the text on the right to the "Threats" column in the table.

Security recommendation	OS platform	Weaknesses	Related component	Threats
Update Openbsd Openssh	Other	31	Openbsd Openssh	🔒 🚫
Onboard devices to Microsoft Defender for Endpoint	Other	1	Security controls (Onboard Devices)	🔒 🚫
Update Ubuntu Telnet for Linux	Linux	1	Ubuntu Telnet for Linux	🔒 🚫
Update Ubuntu Libfuse2 for Linux	Linux	1	Ubuntu Libfuse2 for Linux	🔒 🚫
Update Ubuntu Bash for Linux	Linux	1	Ubuntu Bash for Linux	🔒 🚫
Update Ubuntu Libxml2 for Linux	Linux	8	Ubuntu Libxml2 for Linux	🔒 🚫
Update Ubuntu Libc-bin for Linux	Linux	13	Ubuntu Libc-bin for Linux	🔒 🚫
Update Ubuntu Libc6 for Linux	Linux	13	Ubuntu Libc6 for Linux	🔒 🚫
Update Ubuntu Locales for Linux	Linux	13	Ubuntu Locales for Linux	🔒 🚫
Update Ubuntu Gdisk for Linux	Linux	2	Ubuntu Gdisk for Linux	🔒 🚫
Update Ubuntu Tcpcdump for Linux	Linux	2	Ubuntu Tcpcdump for Linux	🔒 🚫
Update Ubuntu Libsqlite3-0 for Linux	Linux	3	Ubuntu Libsqlite3-0 for Linux	🔒 🚫



Identify and prioritise vulnerabilities and misconfigurations and use integrated workflows to bring devices into a more secure state.

# Integrated Incidents in Microsoft 365 Defender



→ View prioritised incidents that are inclusive of involved IT/IoT devices all in a single dashboard to reduce confusion, clutter, investigation times and alert fatigue.

Microsoft 365 security

## Incidents

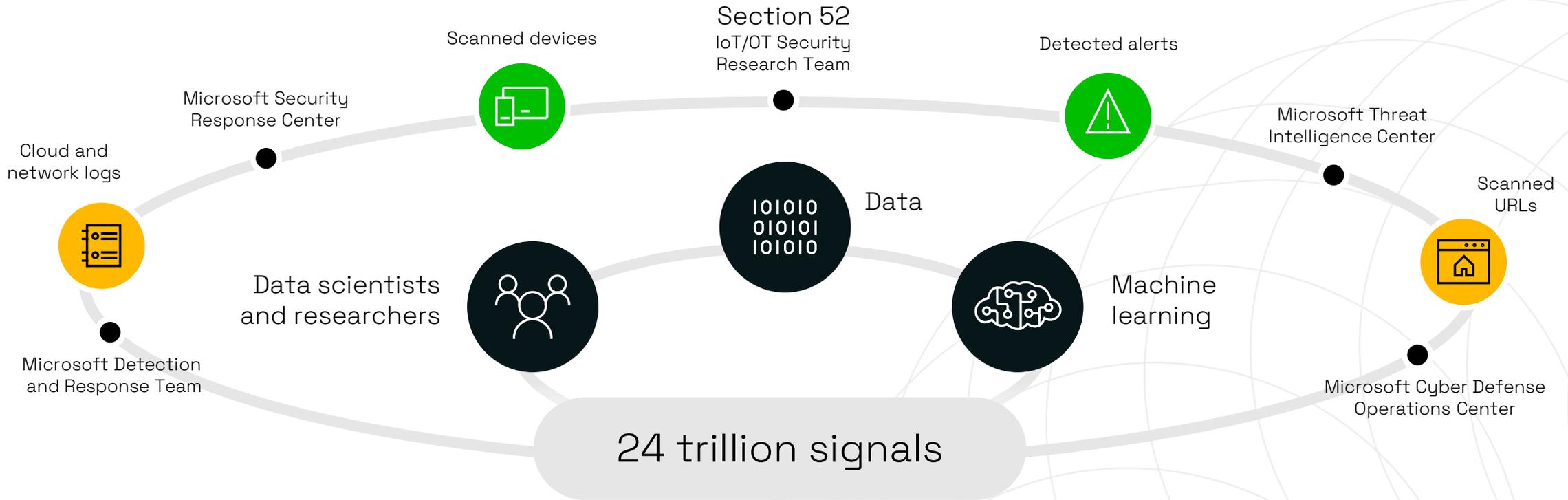
Create a notification rule

Most recent incidents and alerts

1-30 < > 30 days Choose columns 30 items per page Filters

✓	Incident name	Tags	Severity	Investigation state	Categories	Ir
>	Multi-stage incident involving Initial access & Command and control on ...		Medium	3 investigation states	Initial access, Execution, Persis...	
>	[Redacted]		Low	N/A	Malware	
>	[Redacted]		Medium	N/A	Execution	
>	[Redacted]		Medium	N/A	Execution, Defense evasion, D...	
>	[Redacted]		Low	N/A	Malware	
>	[Redacted]		Low	N/A	Malware	
>	[Redacted]		Low	N/A	Malware	
>	[Redacted]		Medium	N/A	Execution	
>	[Redacted]		High	5 investigation states	Initial access, Execution, Persis...	
>	[Redacted]		Low	N/A	Malware	
>	[Redacted]		Low	N/A	Malware	

# World class threat expertise for IoT/OT



Section 52 and broader research teams leverage world's richest threat intellect feed

Discover IoT/OT vulnerabilities, monitoring campaigns and creating unique detections

Results: #1 in detection visibility coverage in MITRE ATT&CK® for ICS evaluation

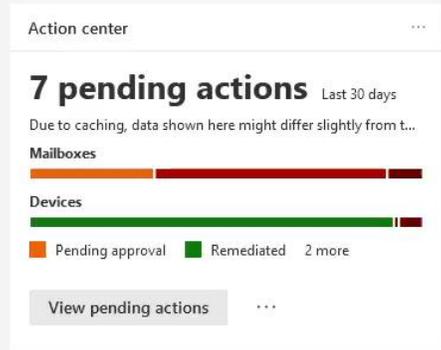
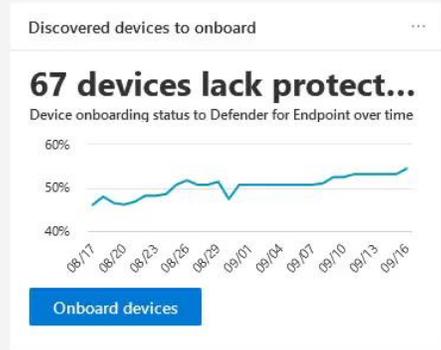


Demo

- Home
- Incidents & alerts
- Hunting
- Actions & submissions
- Threat analytics
- Learning hub
- Trials
- Assets
- Devices
- Identities
- Endpoints
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management
- Email & collaboration
- Investigations
- Explorer
- Review
- Campaigns

# Home

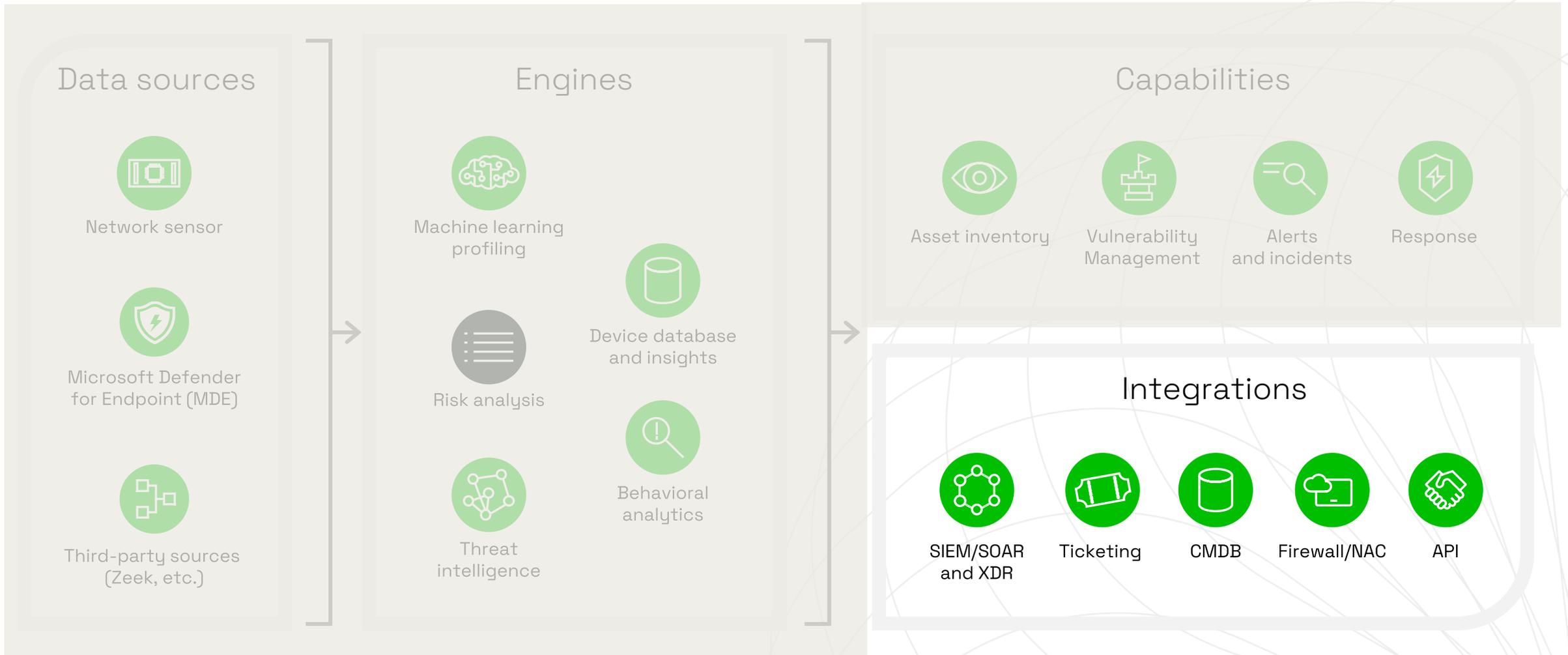
Guided tour What's new? Community + Add cards



Active incidents

Discovered devices

# Solution high-level architecture: Integrations



# IoT/OT threat monitoring solution for Sentinel



Cloud-native SIEM/SOAR, deeply integrated with Defender for IoT

Deep contextual telemetry obtained from Defender for IoT

- Alerts
- Asset details
- Network connection details

Threat intelligence via Section 52 research team OT-specific content

- Analytics rules
- Dashboards (workbooks)
- SOAR playbooks

The screenshot displays the Microsoft Azure Sentinel investigation interface. At the top, the navigation bar shows 'Microsoft Azure' and 'Investigation' with a search bar. Below this, the breadcrumb trail reads 'Home > Azure Sentinel workspaces > Azure Sentinel incidents > Investigation'. The main header includes 'PLC Programming' (Incidents), 'Medium' (Severity), 'New' (Status), 'Unassigned' (Owner), and a timestamp '11/4/2019, 6:35:22 AM' (Last incident update time). The central area features a network diagram with a central node 'x' connected to 'PLC Programming' (shield icon), 'Engineering Workstation' (laptop icon), and two IP addresses: '10.2.1.24' and '10.2.1.25' (laptop icons). A callout box for the PLC node lists 'Related alerts (3)', '10 least prevalent processes (12)', and 'Host logins in incident timeframe (4)'. The right sidebar shows details for 'PLC (BRISTOL BABCOOK INC.)', including Device Name, IP (192.168.1.1), MAC (00:10:41:5a:21:11), Vendor (BRISTOL BABCOOK INC), Firmware versions, Protocols (Emerson OpenBSI), Model (1756-L234ER-QB123-LOGIX5327), Last Seen (17:00 01.06.2020), and Device type (PLC). A 'DeviceLink' is provided at the bottom of the sidebar.

# Why Microsoft?

- Unified solution for enterprise IoT and OT
- Flexible sensor options: MDE, network sensor, 3<sup>rd</sup> party
- Agentless protection with zero performance impact, rapidly deployed (typically <1 day per site)
- Continuous asset discovery, vulnerability management, and threat monitoring
- World's largest IoT/OT security research organization - Section 52
- Integrated with Microsoft SIEM/XDR and third-party SOC solutions

# Next Steps & Resources

Arrange a Vision Call to discuss....

- Proof of concepts
- MCAP workshops
- Security Posture Assessments
- Your requirements

Learn more

- Product page: [Microsoft Defender for IoT \(MDIoT\)](#)
- Blog: [Announcing Enterprise IoT support for MDIoT](#)
- Blog: [Microsoft Defender for IoT integration with Microsoft Sentinel](#)
- Test Results: [#1 in MITRE ATT&CK for ICS evaluation](#)
- Video - [Product demonstration \(OT focused\)](#)
- Training - [Product training series \(OT focused\)](#)





# Thank you

—————> Any questions?