Kocho
BECOME GREATER

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.

Kocho
BECOME GREATER

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

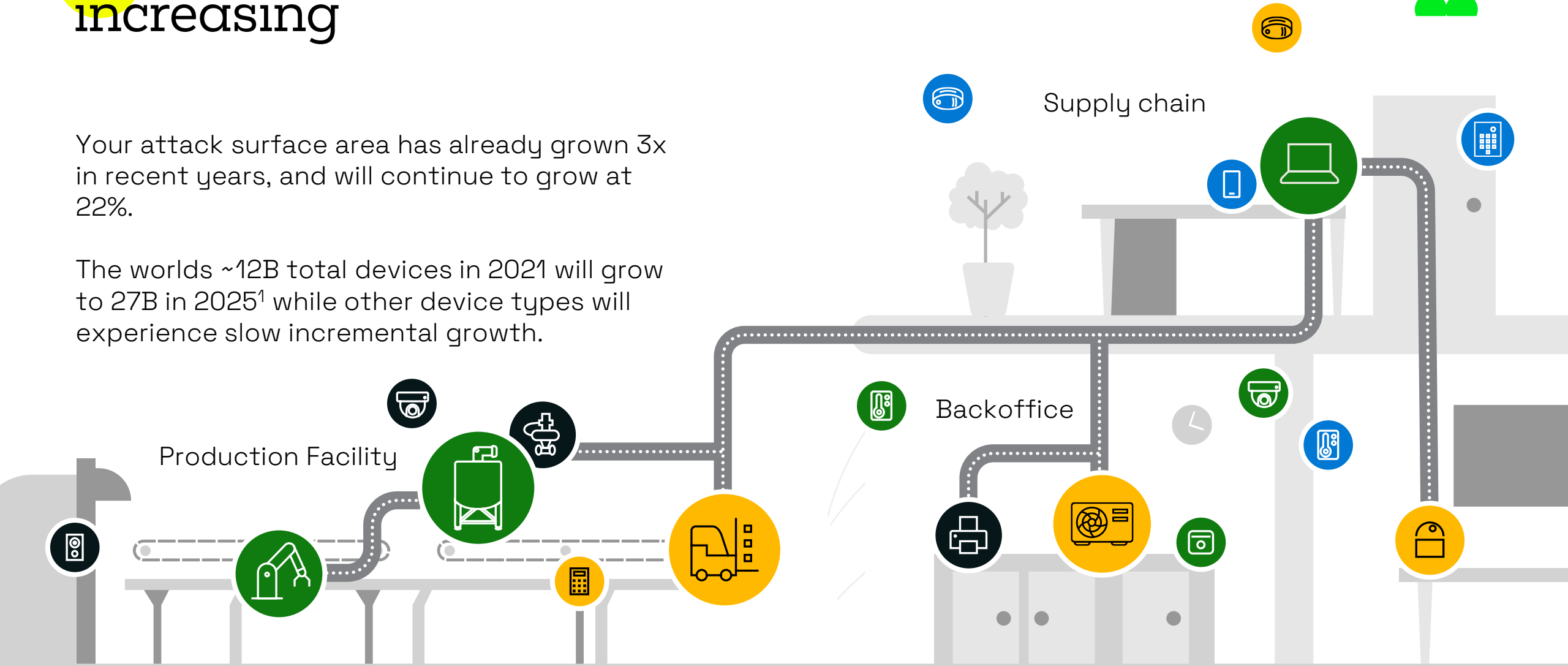
Industrial Control Systems (ICS)

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 worlds ~12B total devices in 2021 will grow to 27B in 2025[1] while other device types will experience slow incremental growth.



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

Real world attack examples

ZDNet

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 hack

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

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

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

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.

SEE ALS

10 dangerous app vulnerabilities to watch out for (free PDF)

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.

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[1]

60% view IoT/OT security as one of the least secured aspects of their IT/OT infrastructure[1]

31% of organizations slowing, limiting, or have stopped the adoption of IoT/OT projects due to security concerns[1]

Technology gaps

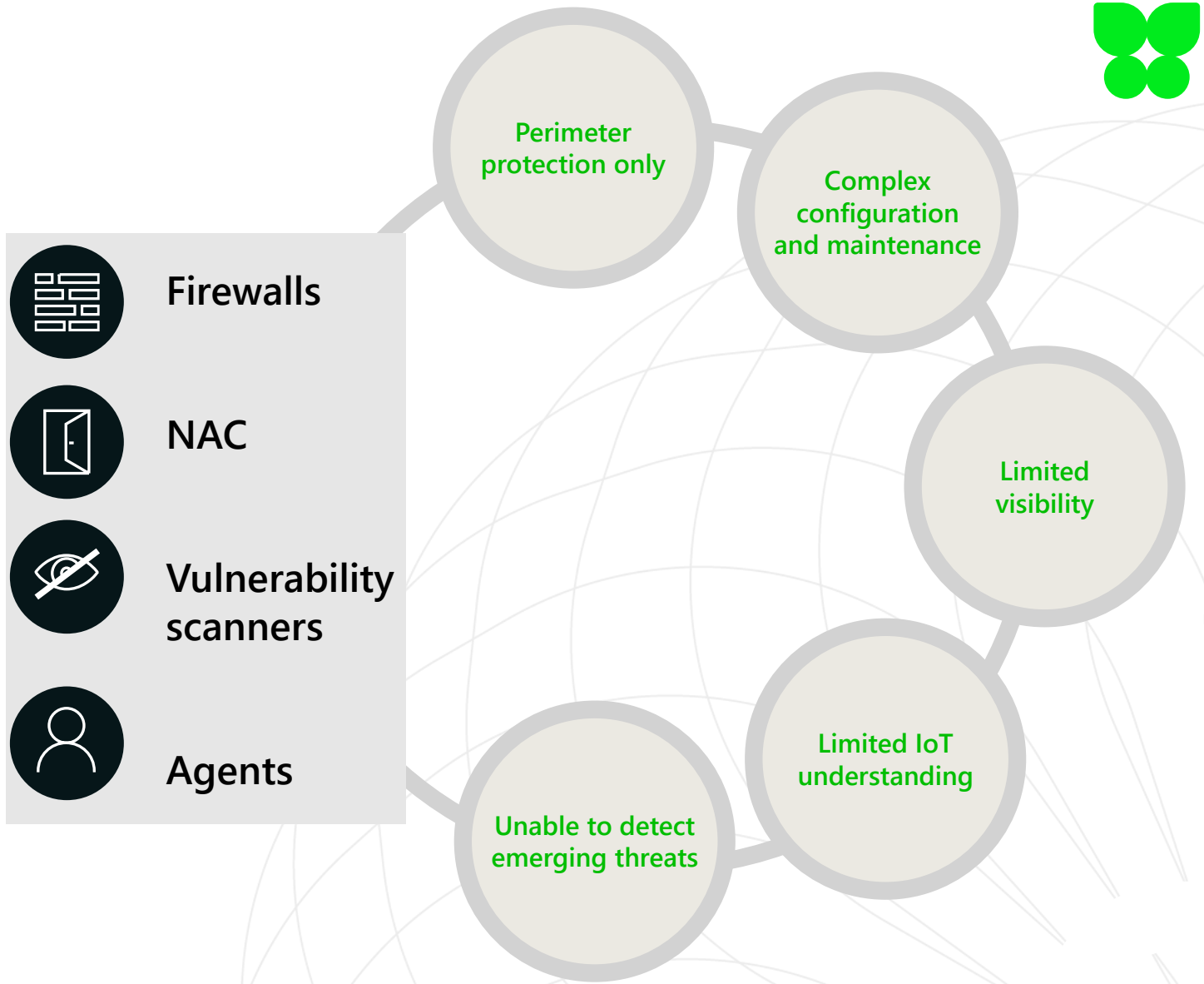
71% of lack a complete inventory of its IoT/OT devices[1]

70% have low or average confidence that IoT devices are secure (i.e.: vulnerabilities mitigated, securely configured)[1]

61% have low or average confidence in the ability to identify whether IoT devices are compromised[1]

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

Challenges with existing solutions



Kocho
BECOME GREATER

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

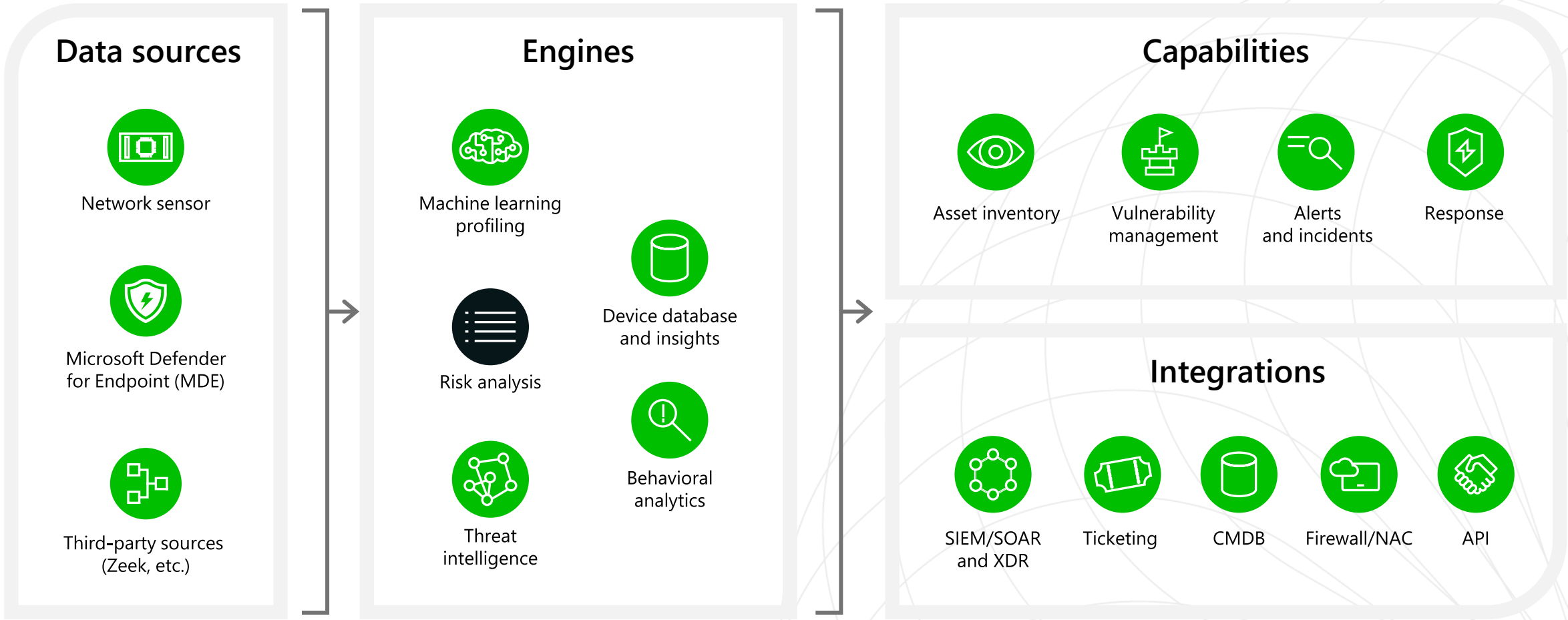
Detect

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

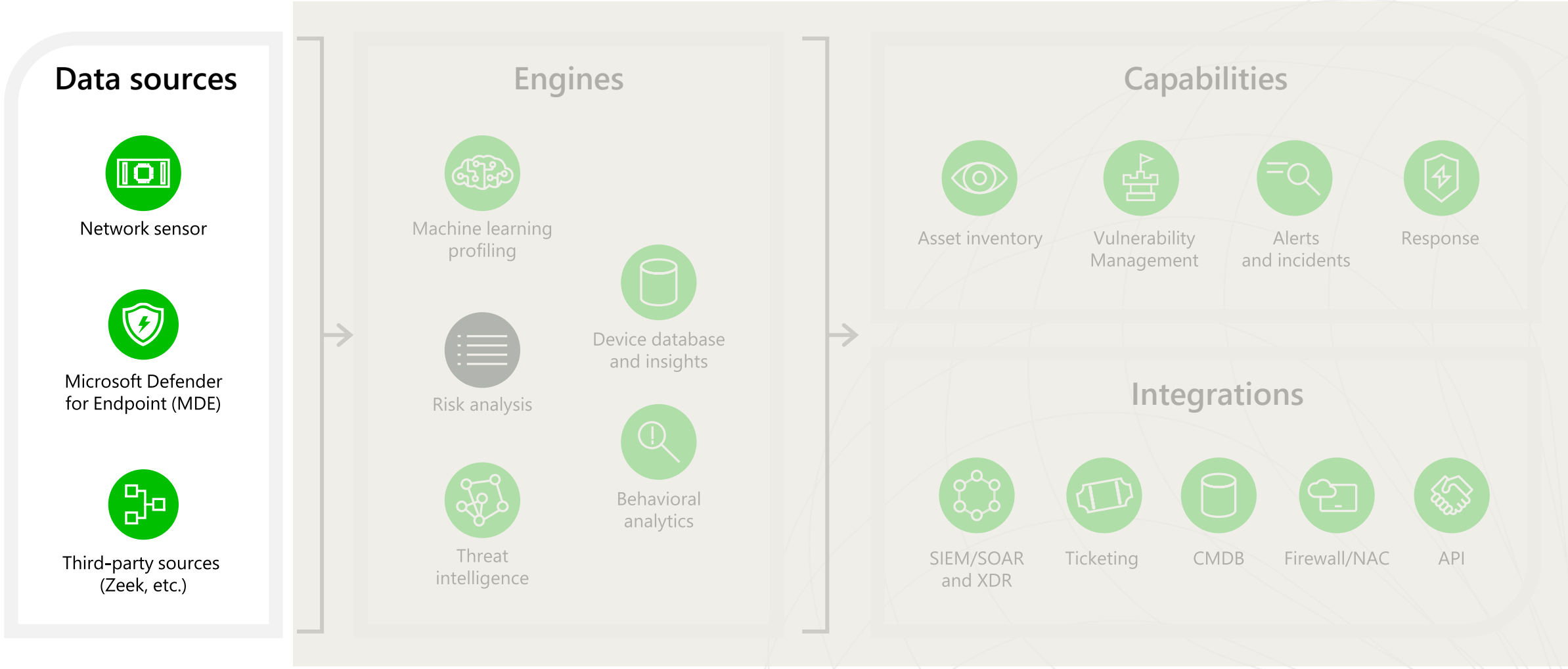
Respond

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

Solution high-level architecture



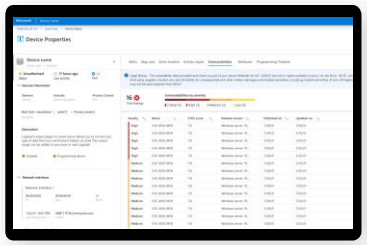
Solution high-level architecture: Agentless Data sources



Broad coverage from diverse data sources

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

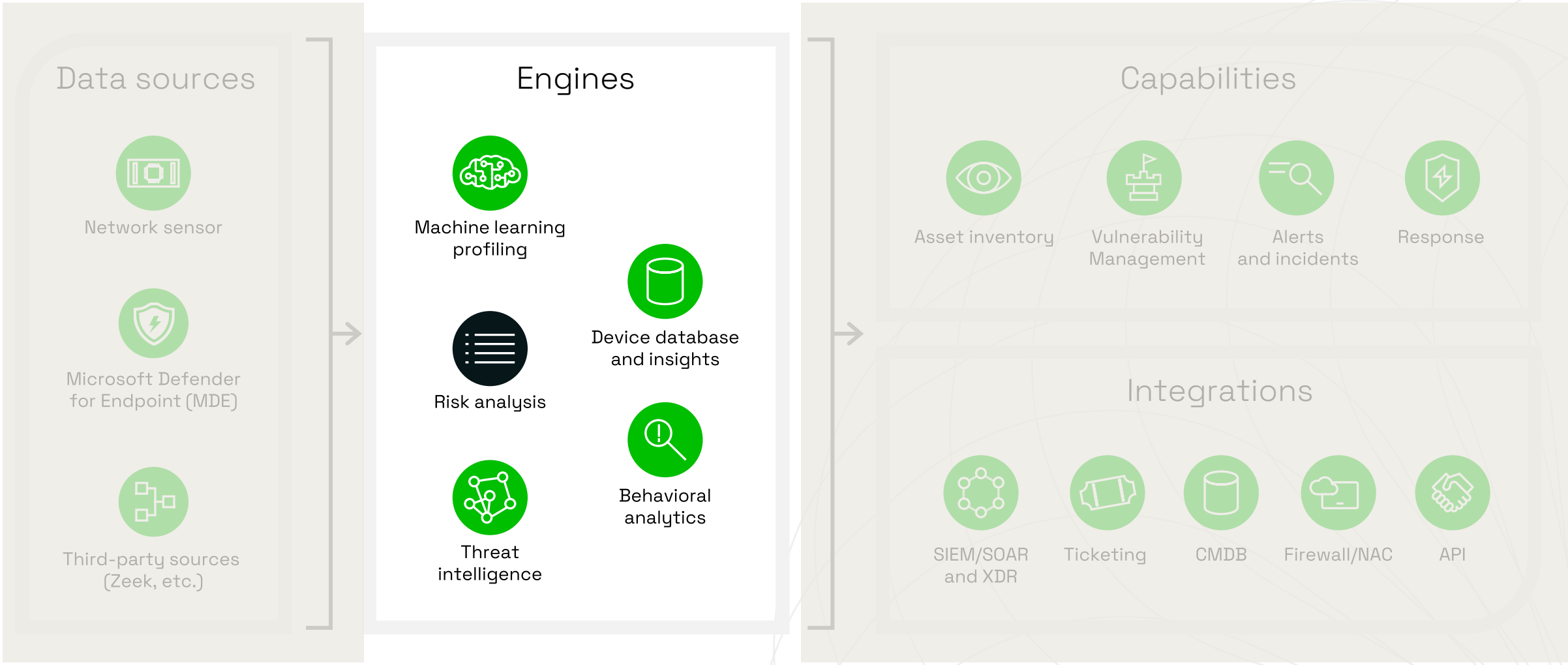
Visibility across all segments

Passive

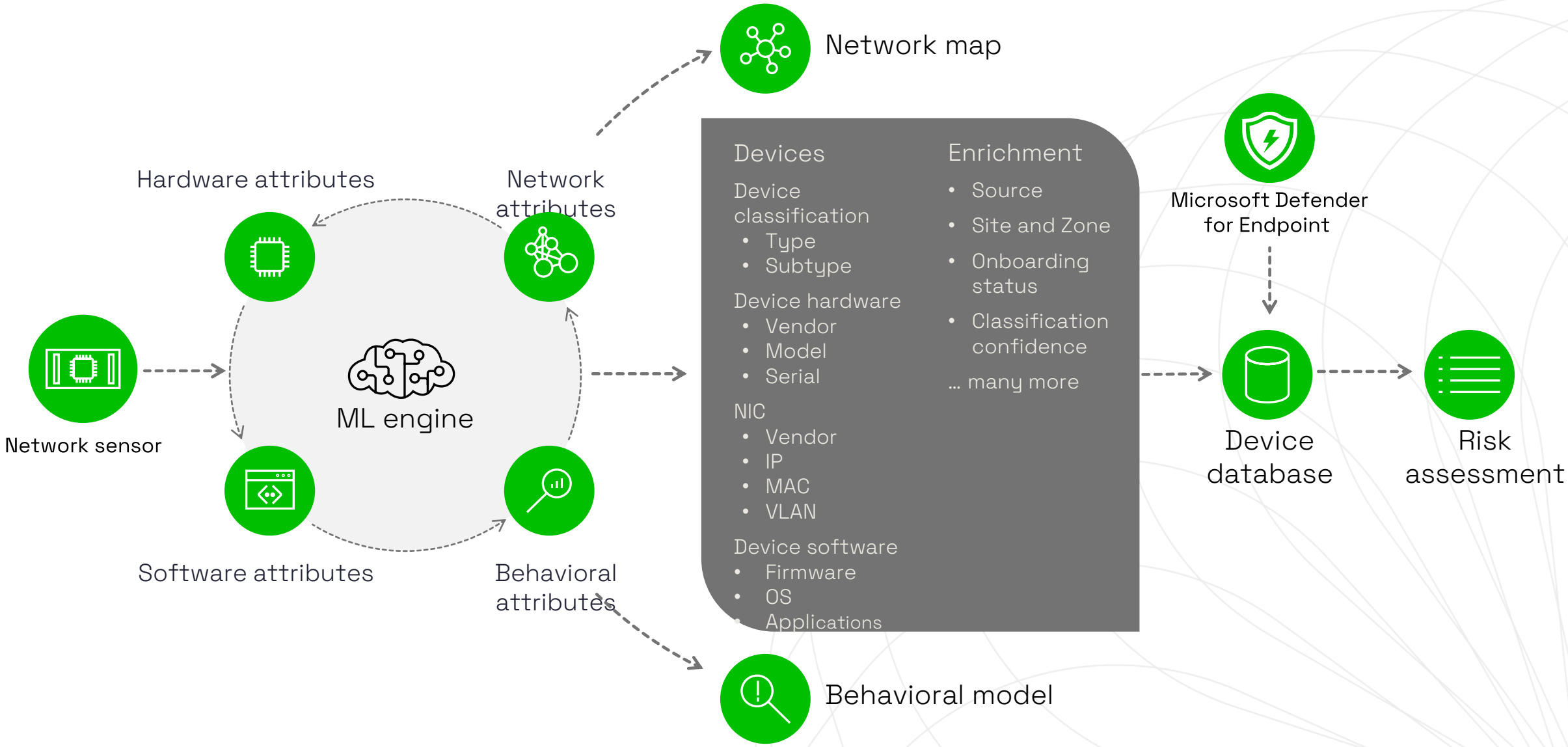
Agentless

Immediate value

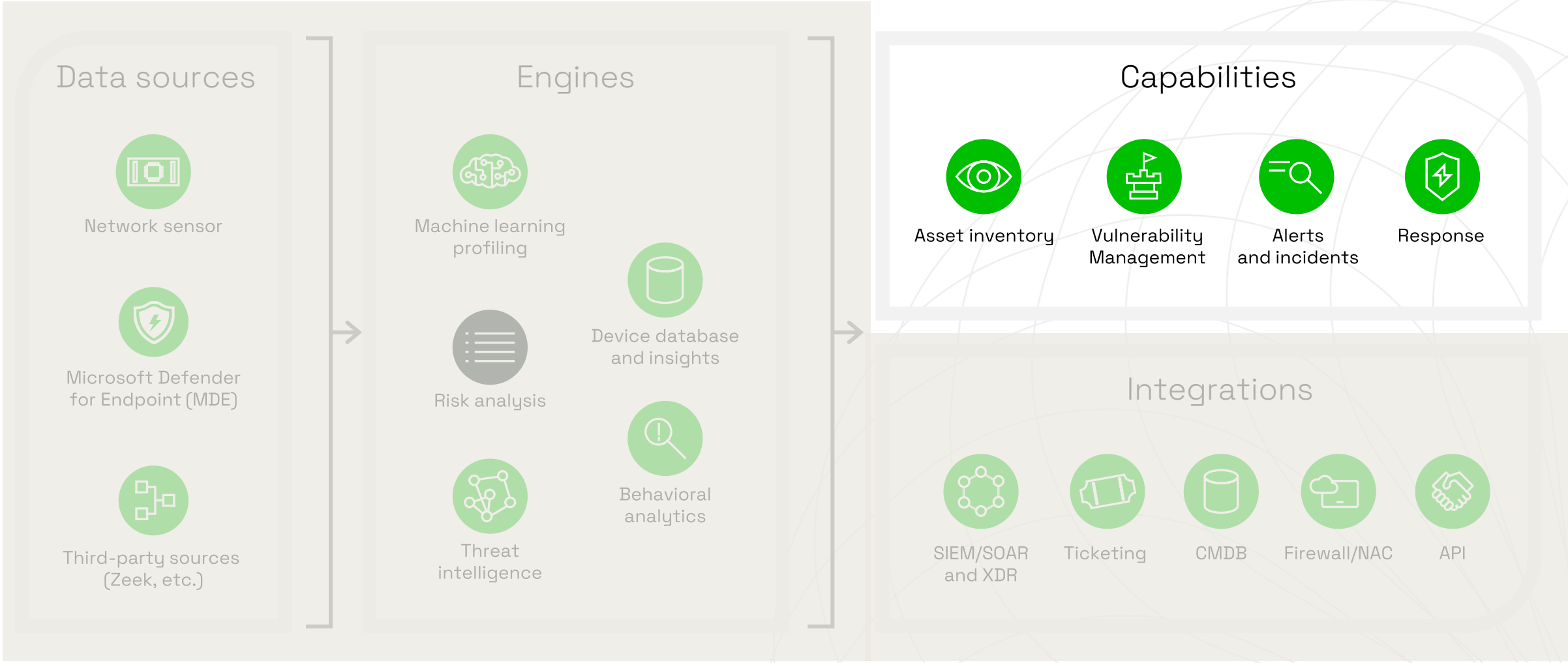
Solution high-level architecture: Engines



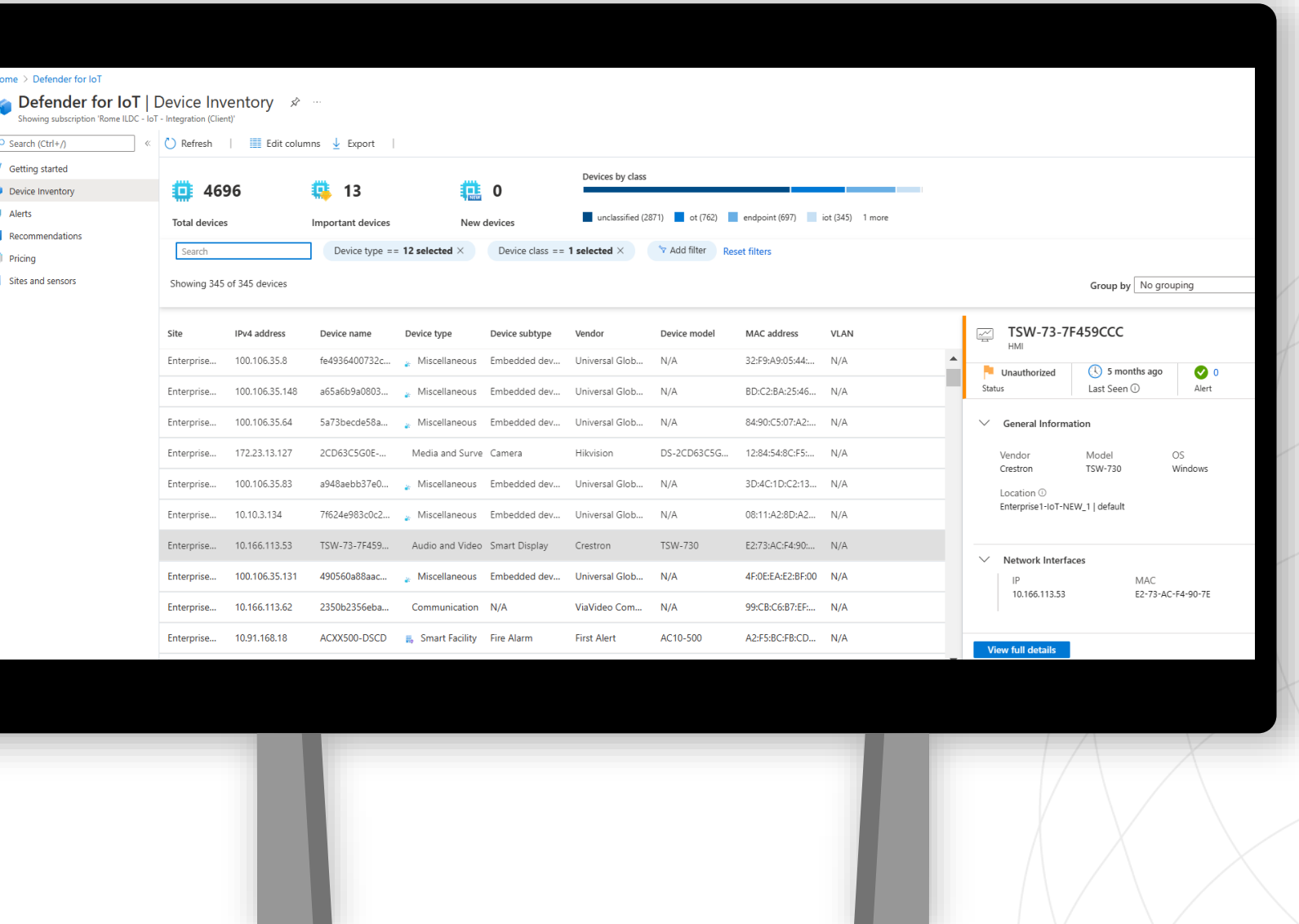
ML-powered detection for IoT devices



Solution high-level architecture: Capabilities



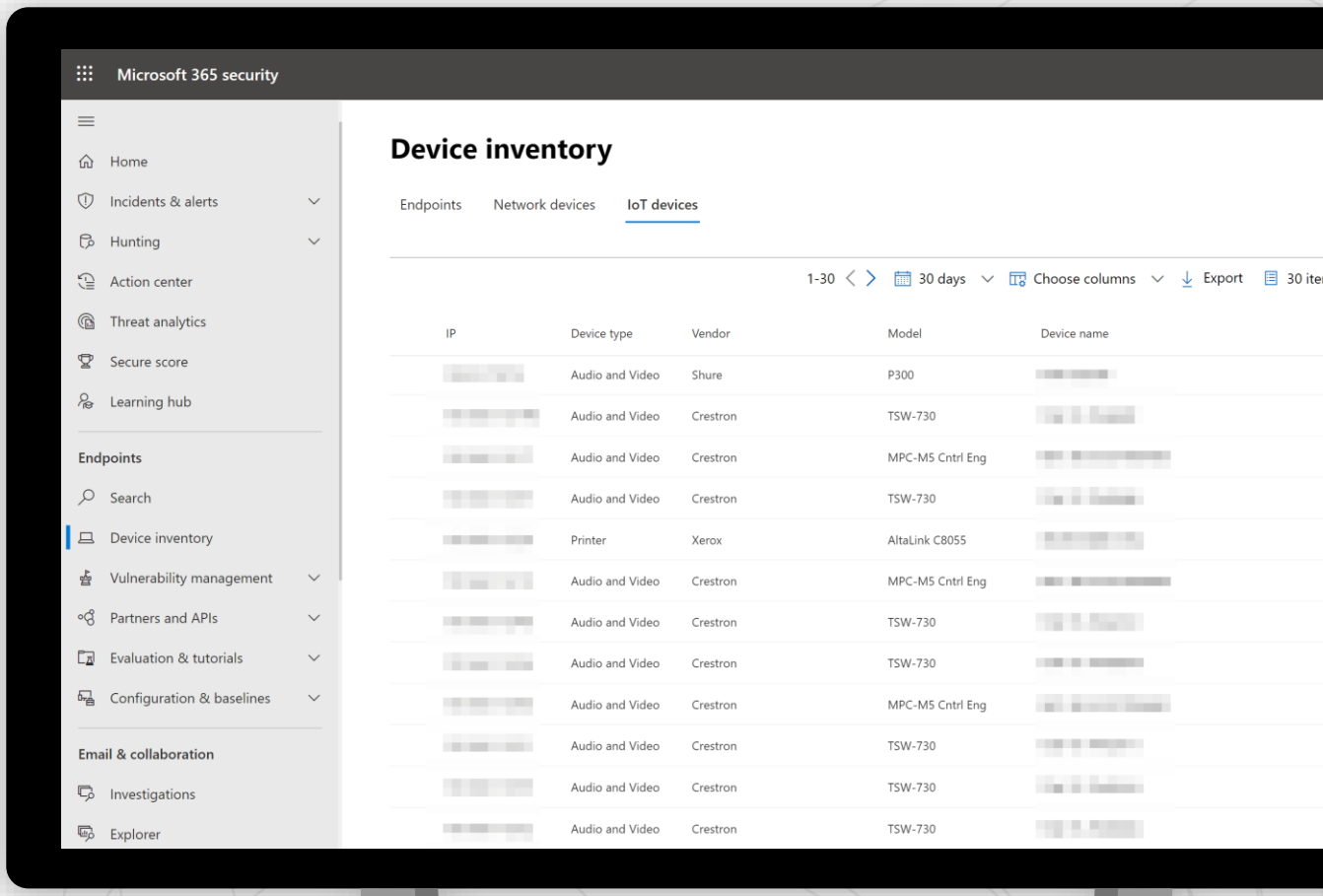
A unified security solution for IoT and OT



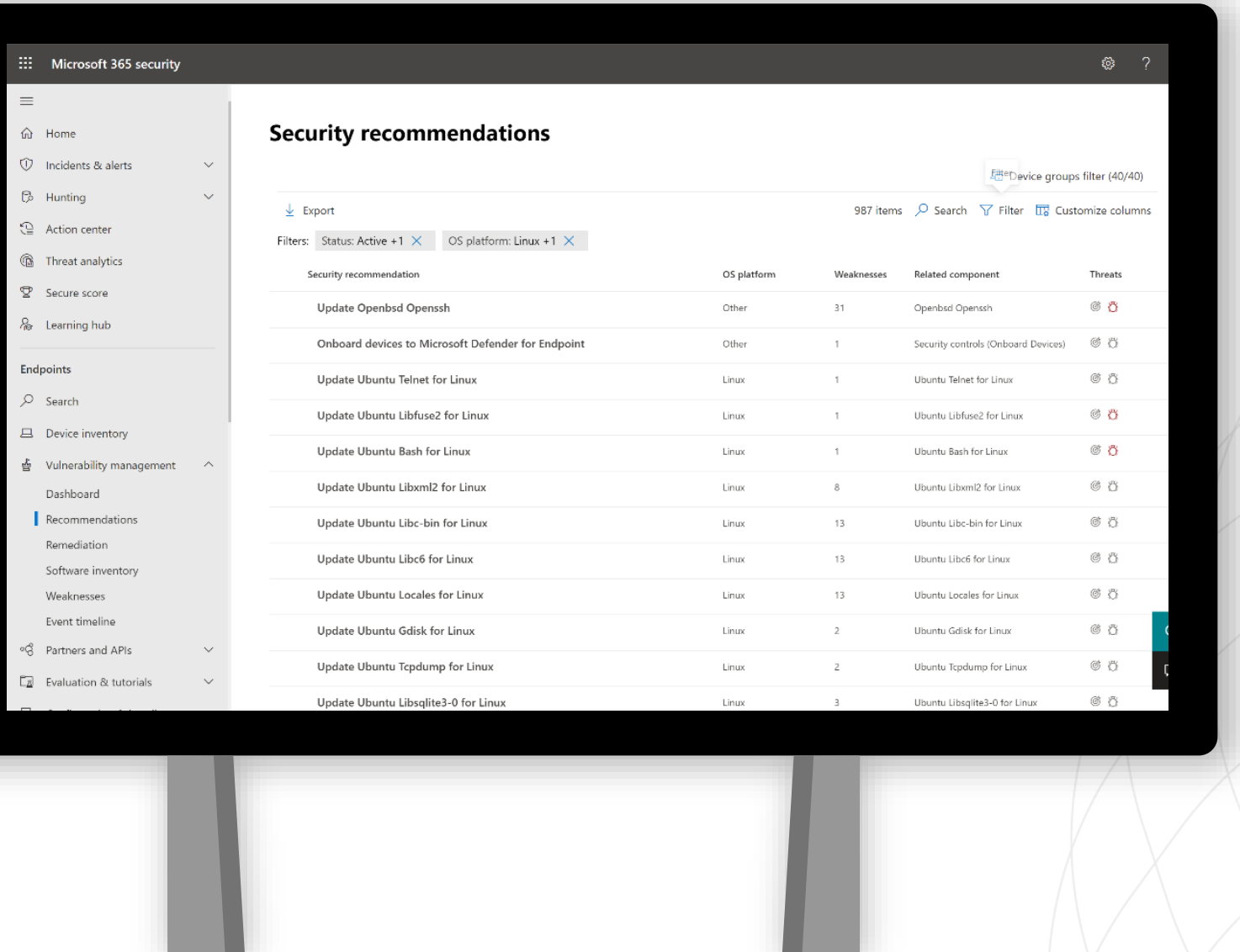
→ Discover, classify, contextualize all your IoT and OT devices so you can secure the devices accessing your network and resources.

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.



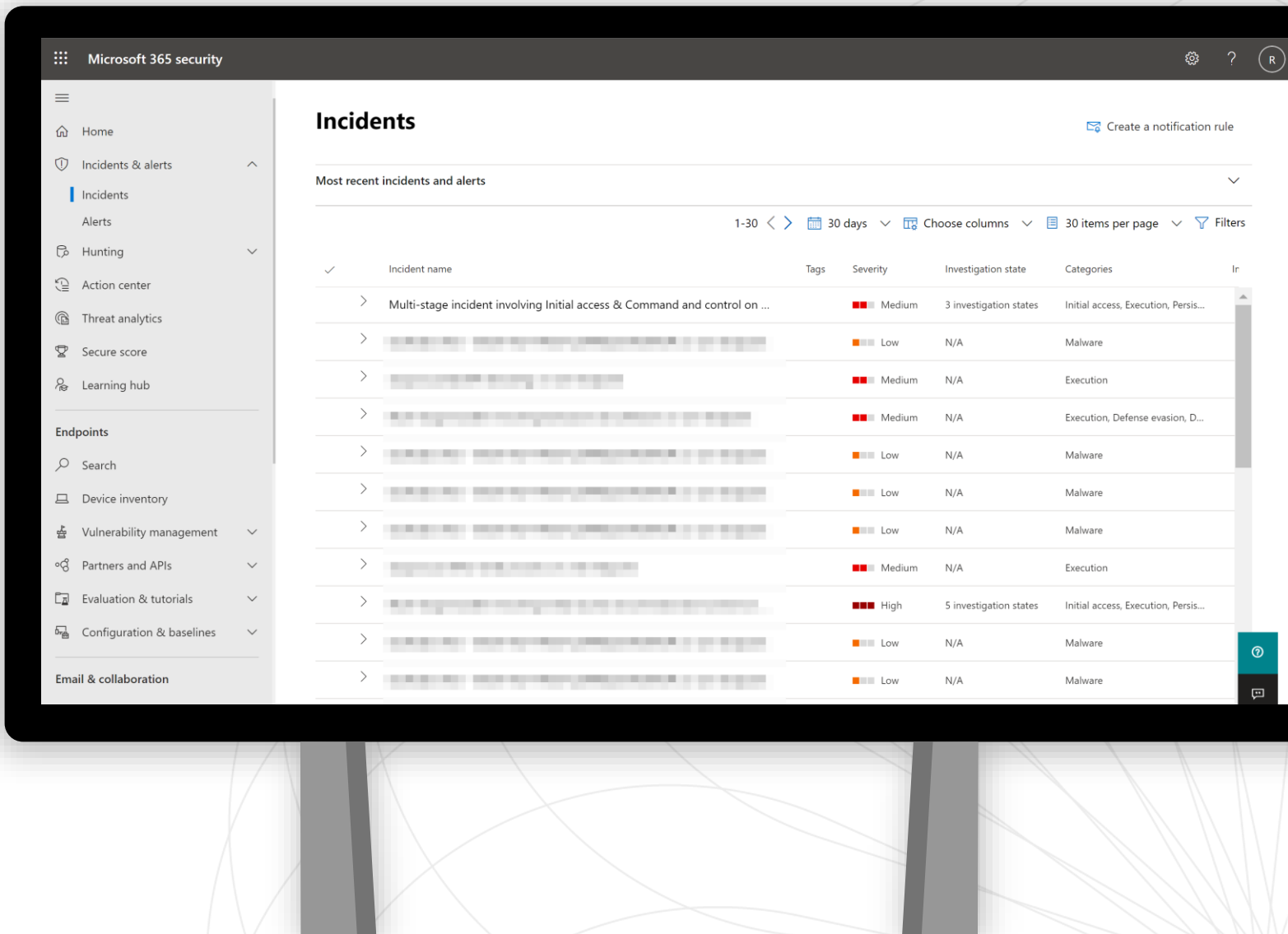
Integrated Vulnerability Management in Microsoft 365 Defender



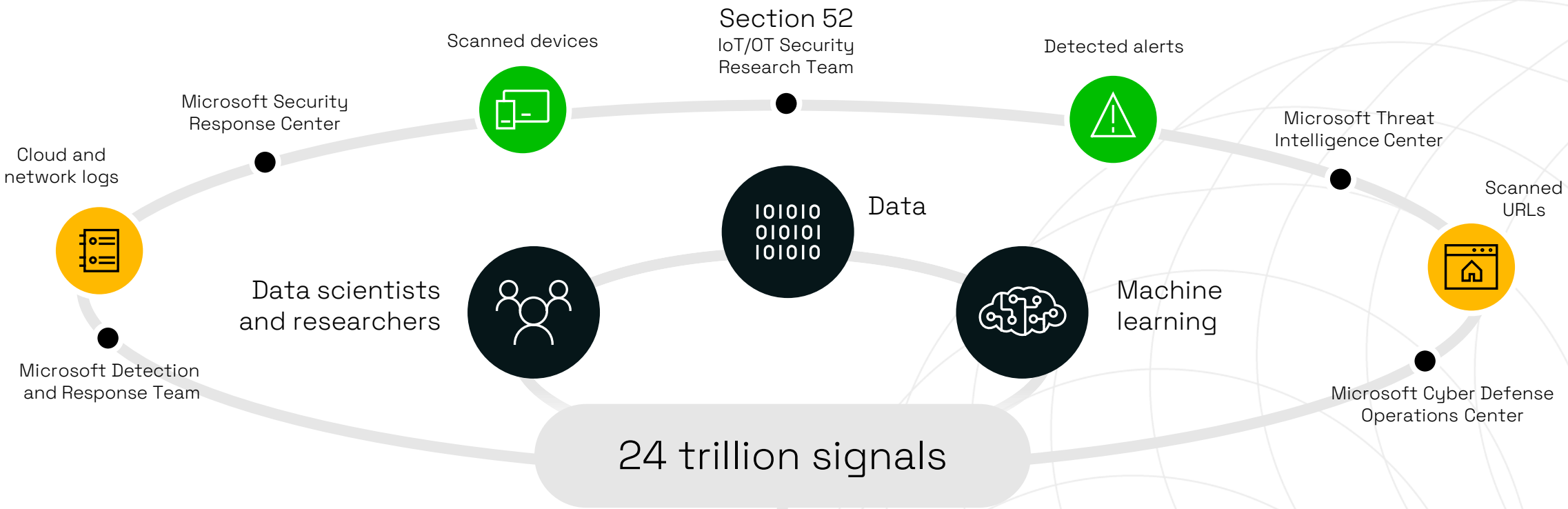
→ Identify and prioritise vulnerabilities and misconfigurations and use integrated workflows to bring devices into a more secure state.

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.



World class threat expertise for IoT/OT

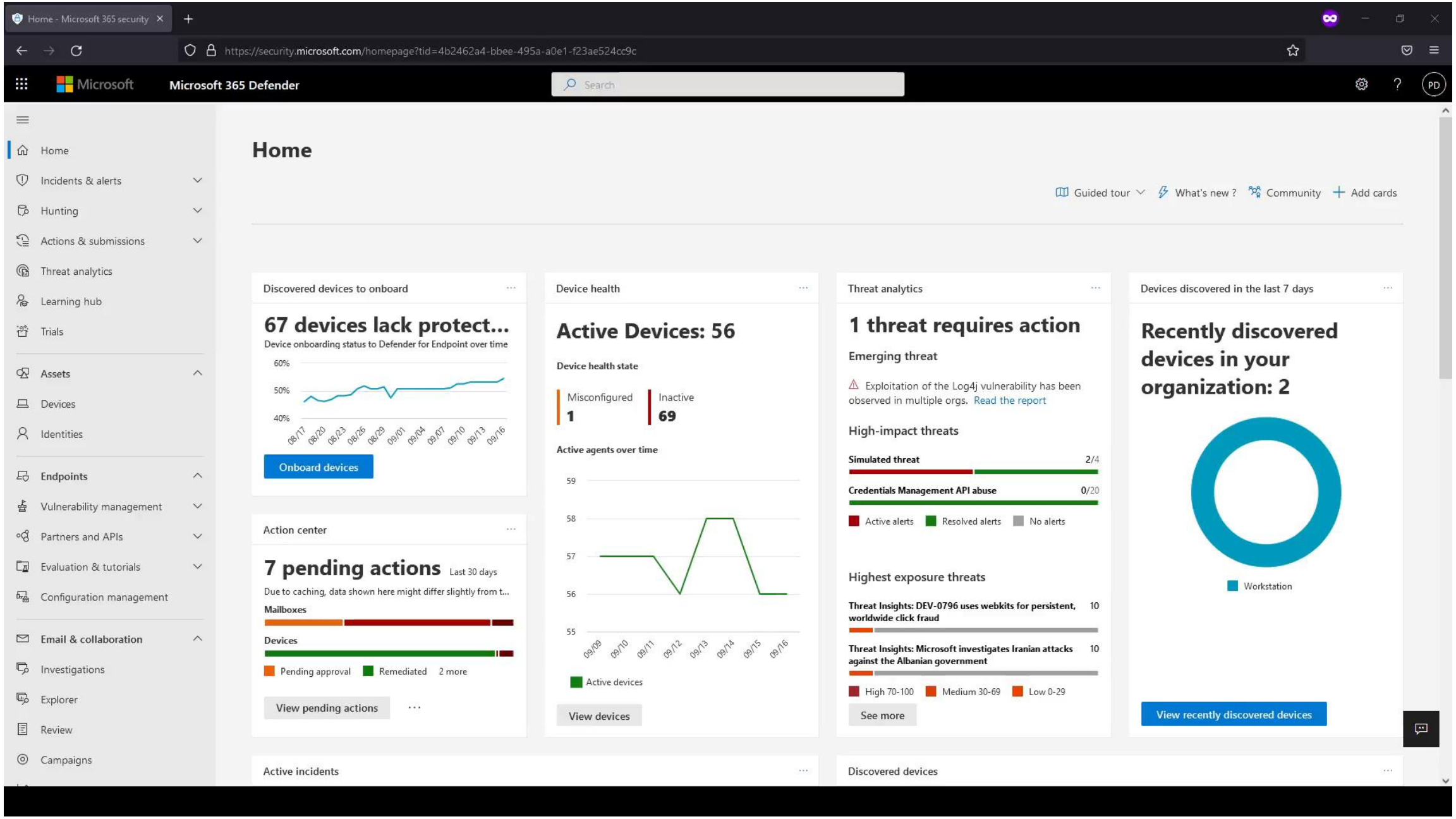


Section 52 and broader research teams leverage worlds richest threat intellect feed

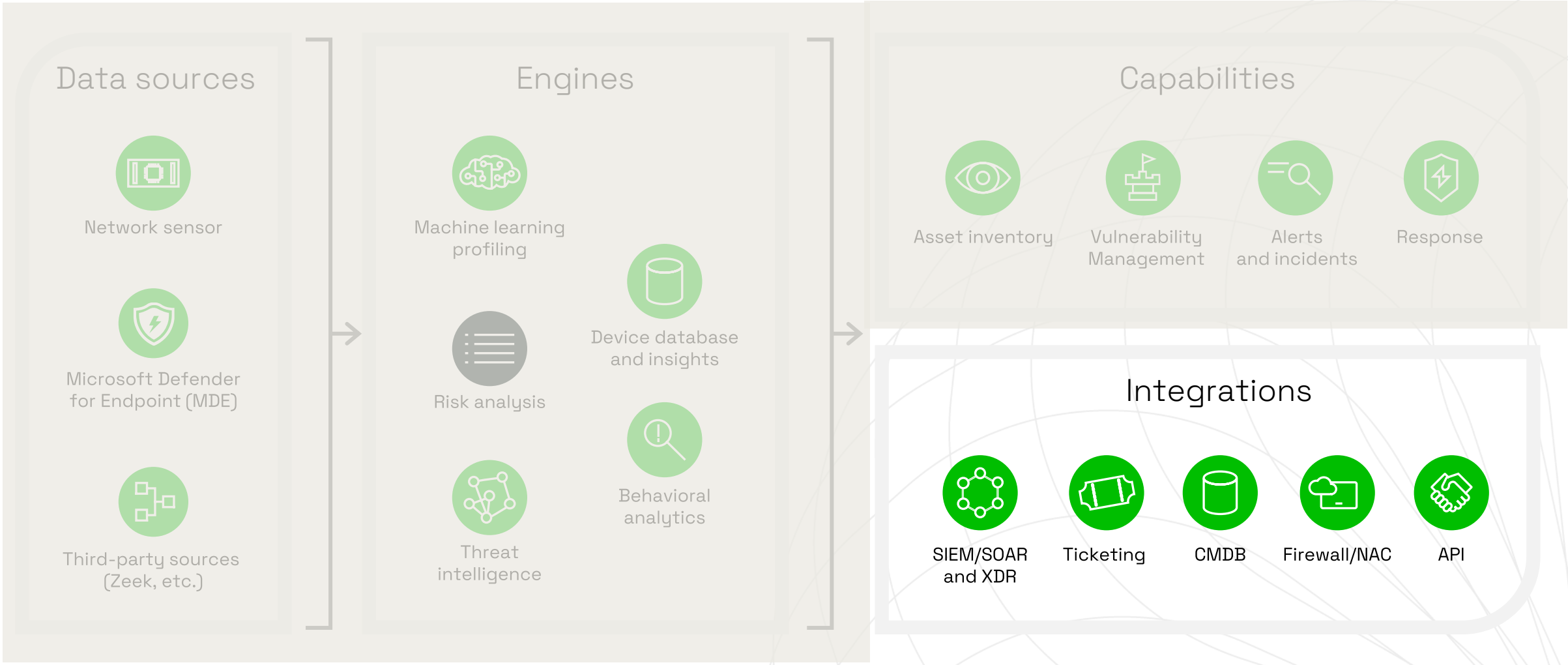
Discover IoT/OT vulnerabilities, monitoring campaigns and creating unique detections

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

Demo


Home - Microsoft 365 security
https://security.microsoft.com/homepage?tid=4b2462a4-bbee-495a-a0e1-f23ae524cc9c
Microsoft
Microsoft 365 Defender
Search
PD
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
Discovered devices to onboard
67 devices lack protect...
Device onboarding status to Defender for Endpoint over time
60%
50%
40%
08/17
08/20
08/23
08/26
08/29
09/01
09/04
09/07
09/10
09/13
09/16
Onboard devices
Action center
7 pending actions
Last 30 days
Due to caching, data shown here might differ slightly from t...
Mailboxes
Devices
Pending approval
Remediated
2 more
View pending actions
Device health
Active Devices: 56
Device health state
Misconfigured
1
Inactive
69
Active agents over time
59
58
57
56
55
09/09
09/10
09/11
09/12
09/13
09/14
09/15
09/16
Active devices
View devices
Threat analytics
1 threat requires action
Emerging threat
Exploitation of the Log4j vulnerability has been observed in multiple orgs. Read the report
High-impact threats
Simulated threat
2/4
Credentials Management API abuse
0/20
Active alerts
Resolved alerts
No alerts
Highest exposure threats
Threat Insights: DEV-0796 uses webkits for persistent, worldwide click fraud
10
Threat Insights: Microsoft investigates Iranian attacks against the Albanian government
10
High 70-100
Medium 30-69
Low 0-29
See more
Devices discovered in the last 7 days
Recently discovered devices in your organization: 2
Workstation
View recently discovered devices
Active incidents
Discovered devices

Solution high-level architecture: Integrations



IoT/OT threat monitoring solution for Sentinel

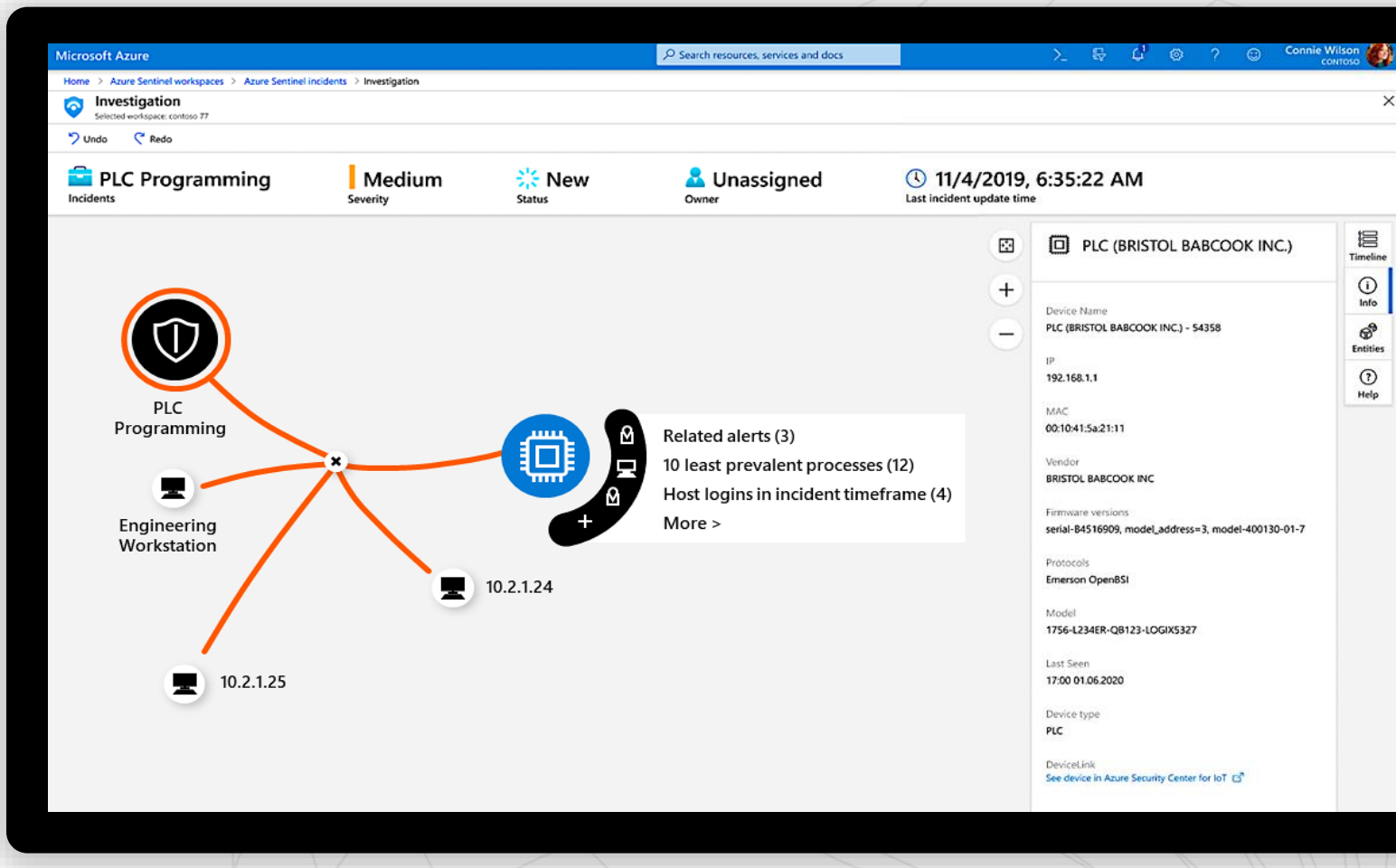
Cloud-native SIEM/SOAR, deeply integrated with Defender for IoT

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



Why Microsoft?

- Unified solution for enterprise IoT and OT
- Flexible sensor options: MDE, network sensor, 3rd 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

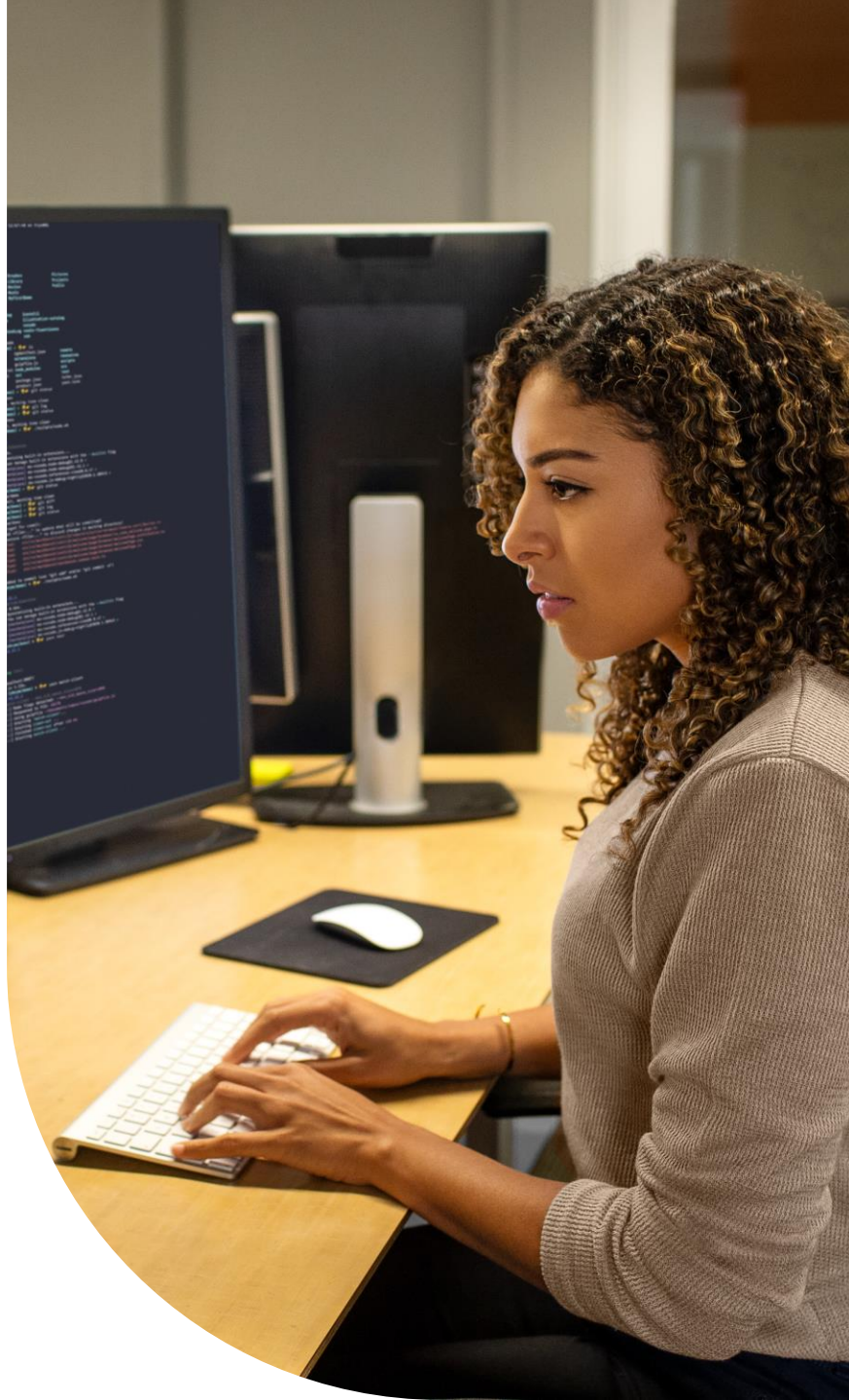
Next Steps & Resources

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)



Kocho

BECOME GREATER

Thank you

→ Any questions?