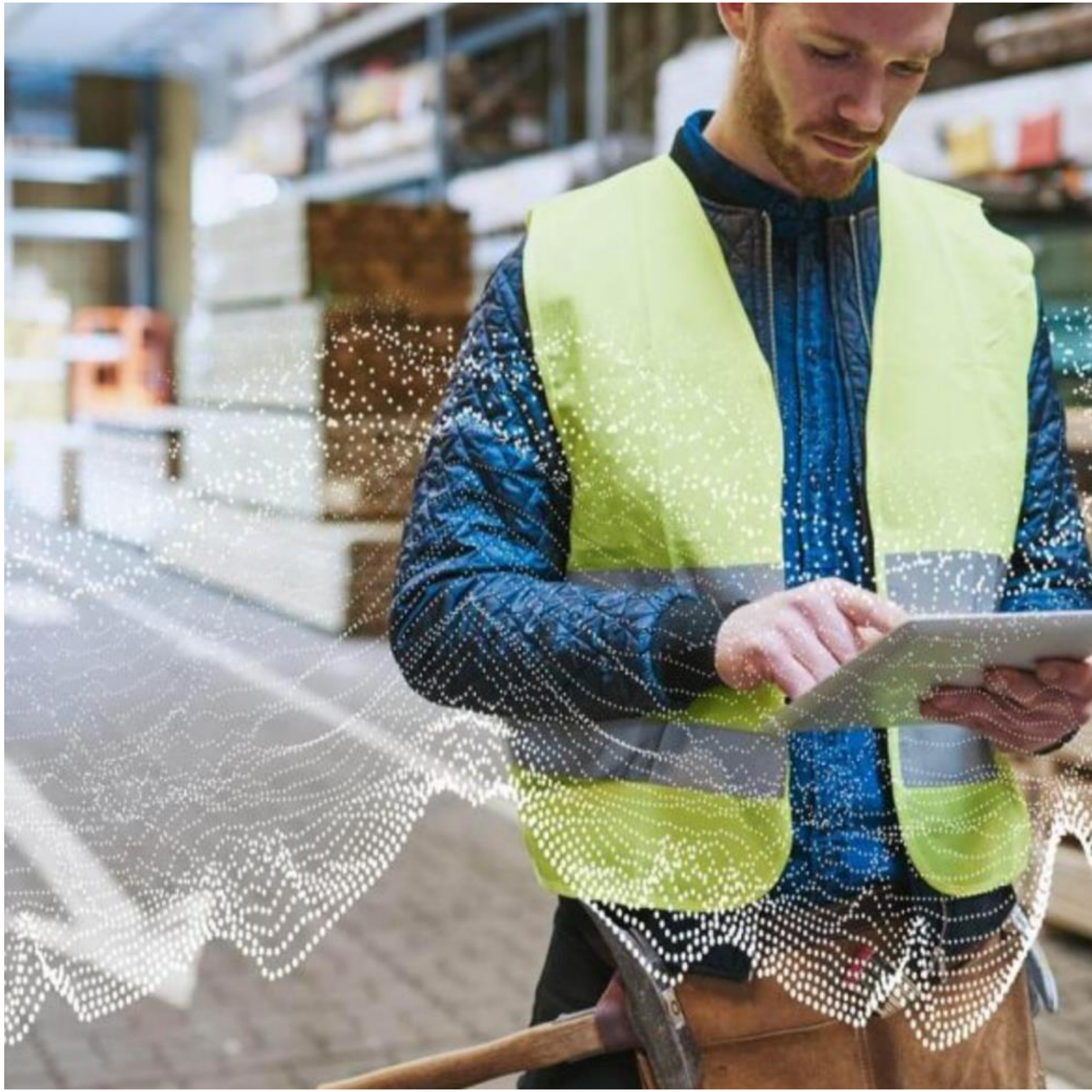
Microsoft Azure

Defender for IoT Overview



Differences between IT & OT security

IT Security

OT Security

Differences between IT & OT security

IT Security	OT Security
Data confidentiality & privacy	Safety & availability
Standard protocols & devices	Specialized protocols, devices & legacy OS platforms
High levels of connectivity	Traditionally air-gapped (apparently)
Multiple layers of controls & telemetry	Little or no visibility into IoT/OT risk

IoT/OT risk = business risk

Financial

Destructive malware shuts down factories worldwide, causing billion of dollars in losses (WannaCry, NotPetya, LockerGoga, Ekans, …).

IP Theft

Manufacturers are 8x more likely to be attacked for theft of IP like proprietary formulas and designs than other verticals (DBIR).

Safety

Safety controllers in petrochemical facility compromised with purpose-built back door in TRITON attack.

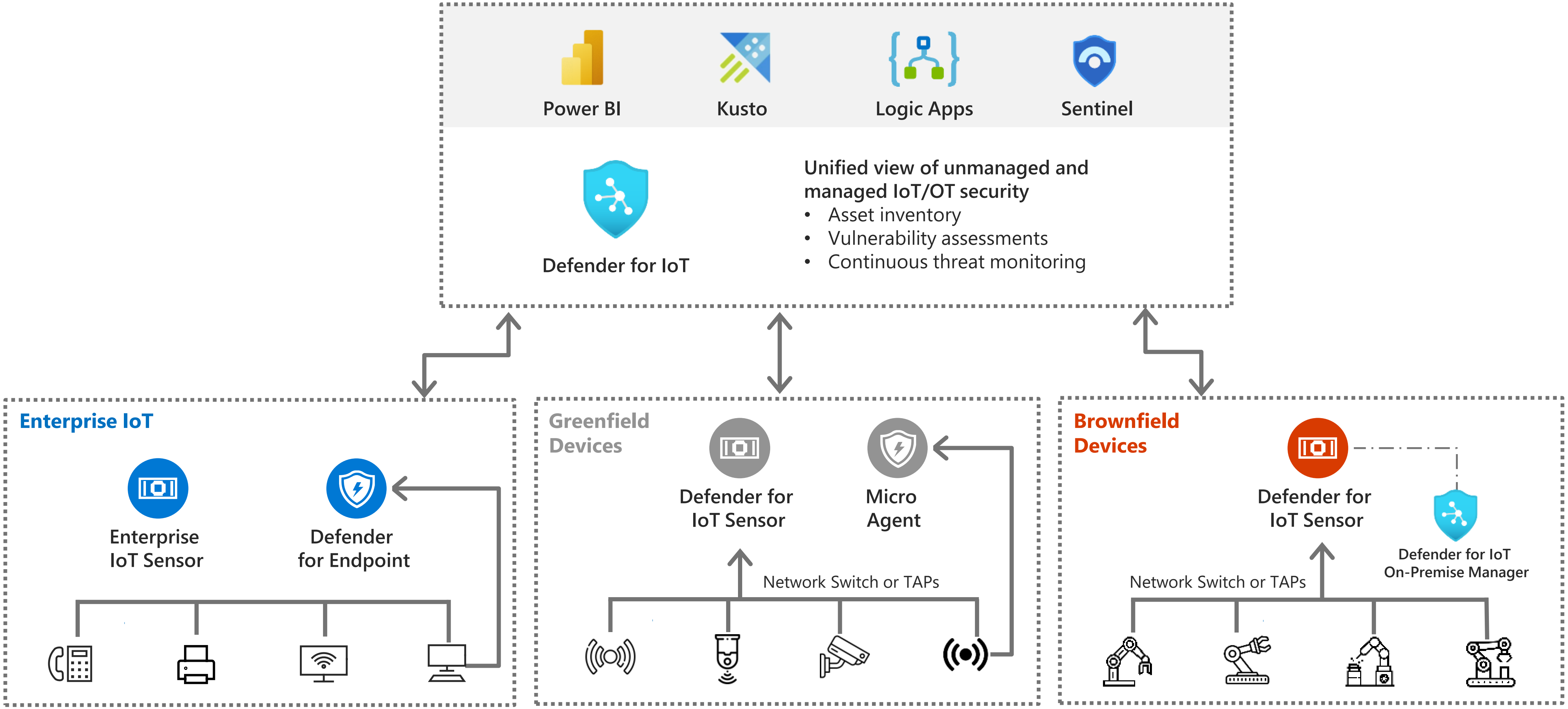
Why IoT/OT cybersecurity is now a board-level concern

Digital transformation & IT/OT connectivity have significantly expanded the attack surface

Adversaries are motivated, sophisticated & increasingly destructive

Enterprise SOCs today have virtually no visibility into their IoT/OT risk

IoT/OT security reference architecture



Power BI

Kusto

Logic Apps

Sentinel

Defender for IoT

Unified view of unmanaged and managed IoT/OT security

- Asset inventory
- Vulnerability assessments
- Continuous threat monitoring

Enterprise IoT

Enterprise IoT Sensor

Defender for Endpoint

Greenfield Devices

Defender for IoT Sensor

Micro Agent

Network Switch or TAPs

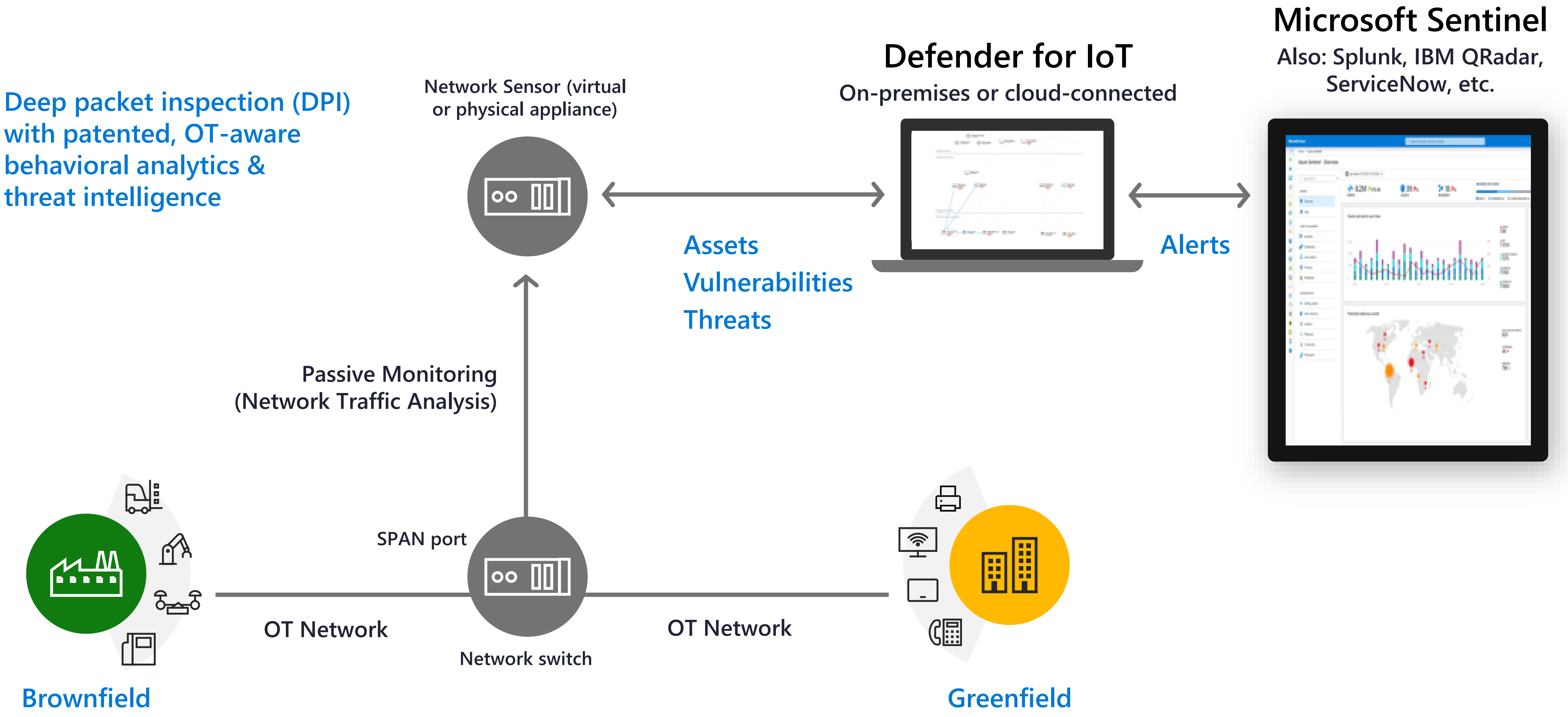
Brownfield Devices

Defender for IoT Sensor

Defender for IoT On-Premise Manager

Network Switch or TAPs

IoT/OT-aware network detection & response (NDR)



Deep packet inspection (DPI) with patented, OT-aware behavioral analytics & threat intelligence

Network Sensor (virtual or physical appliance)

Defender for IoT

On-premises or cloud-connected

Microsoft Sentinel

Also: Splunk, IBM QRadar, ServiceNow, etc.

Assets

Vulnerabilities

Threats

Alerts

Passive Monitoring (Network Traffic Analysis)

SPAN port

OT Network

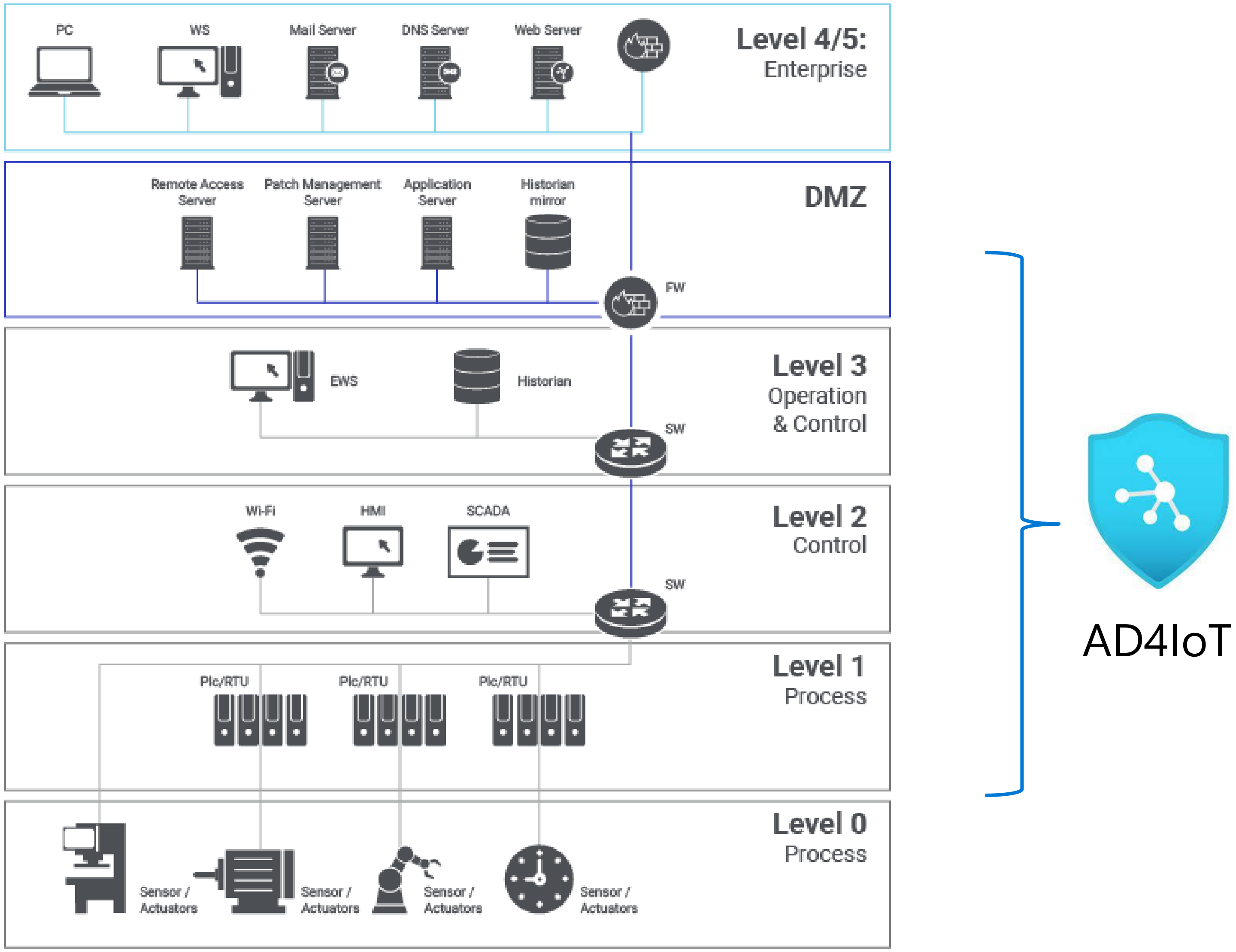
Network switch

OT Network

Brownfield

Greenfield

Purdue Model / ISA 95



Agentless security for unmanaged IoT/OT devices

IoT/OT Asset Discovery

What devices do we have & how are they communicating?

Risk & Vulnerability Management

What are risks & mitigations impacting our crown jewel assets?

Continuous IoT/OT Threat Monitoring, Incident Response & Threat Intelligence

How do we detect & respond to IoT/OT threats in our network?

Operational Efficiency

How do we identify the root cause of malfunctioning or misconfigured equipment?

Unified IT/OT Security Monitoring & Governance

How do we break down IT/OT silos?

How do we leverage existing workflows & tools to centralize IT/OT security in our SOC?

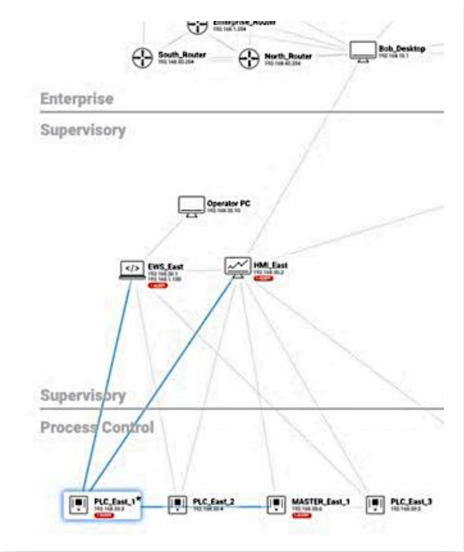
How do we demonstrate to auditors that we have a safety- and security-first environment?

Agentless deployment with zero changes or impact

Leveraging IoT/OT-aware behavioral analytics & threat intelligence

Frictionless. Zero impact.
No rules required.
Deployed in <1 day per site.

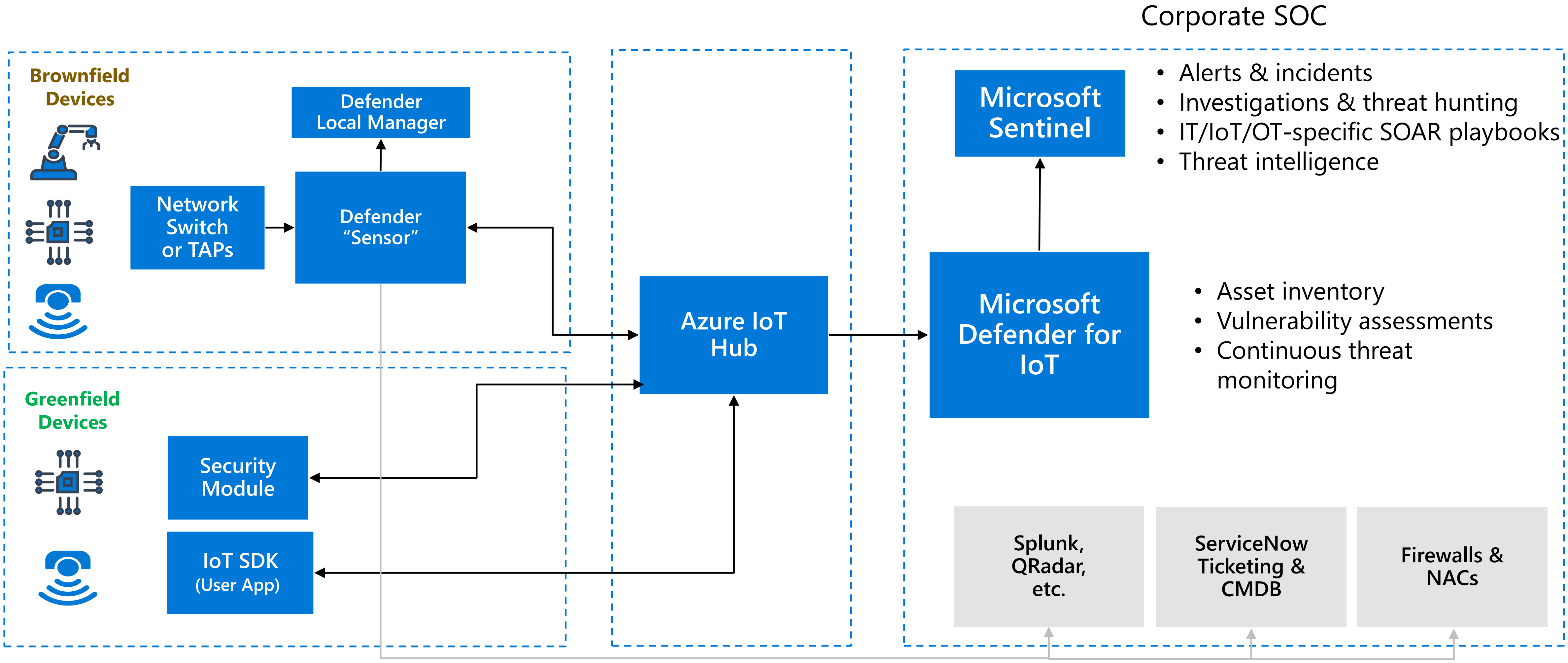
Faster time-to-value



Continuous visibility into
IoT/OT assets, vulnerabilities
& threats

Integrated with Sentinel,
& 3rd-party SOC tools (Splunk,
QRadar, ServiceNow, etc.) for
unified IT/OT monitoring
& governance

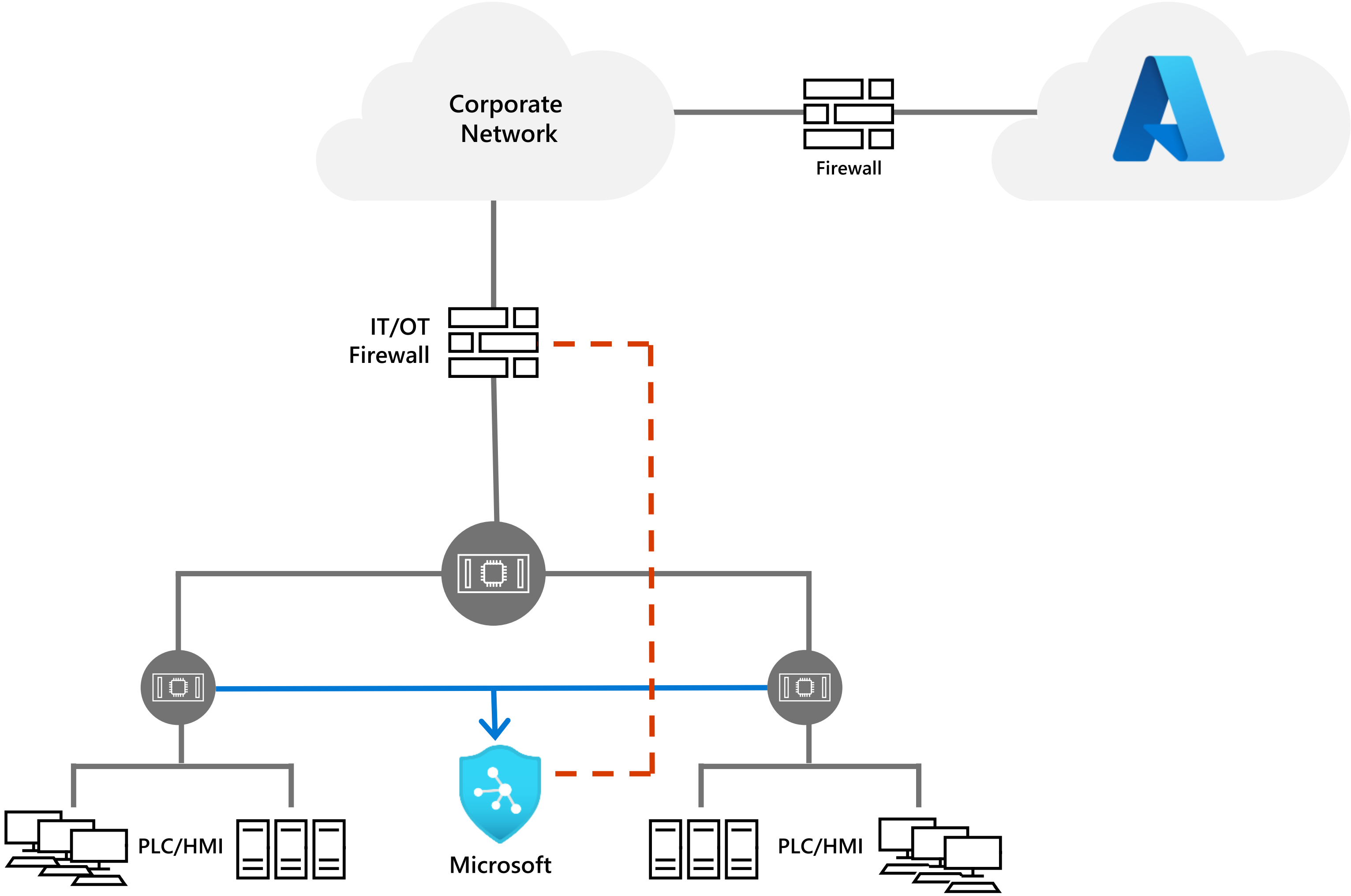
OT Security — Reference Architecture



- Alerts & incidents
- Investigations & threat hunting
- IT/IoT/OT-specific SOAR playbooks
- Threat intelligence

- Asset inventory
- Vulnerability assessments
- Continuous threat monitoring

IoT/OT security reference architecture



World-class threat expertise

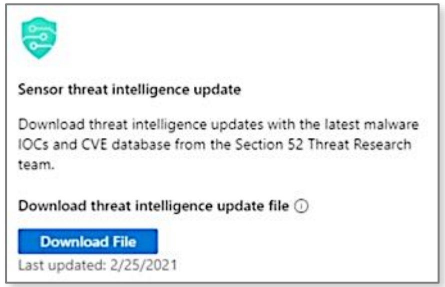
→ Section 52: Former nation-state defenders, IoT/OT security researchers & data scientists

Proprietary vulnerability research
Reverse-engineering malware
Monitoring IoT/OT honeypots
Tracking adversaries & campaigns

→ Continuous threat intelligence updates delivered via the cloud

Latest CVEs
Malware
Malicious DNS & other IOCs

→ Integrated with Microsoft's global threat intelligence feed derived from 24 trillion signals collected daily (STIX/TAXII)



Sensor threat intelligence update

Download threat intelligence updates with the latest malware IOCs and CVE database from the Section 52 Threat Research team.

Download threat intelligence update file ⓘ

Last updated: 2/25/2021

35+ zero-day vulnerabilities reported to CISA by Section 52

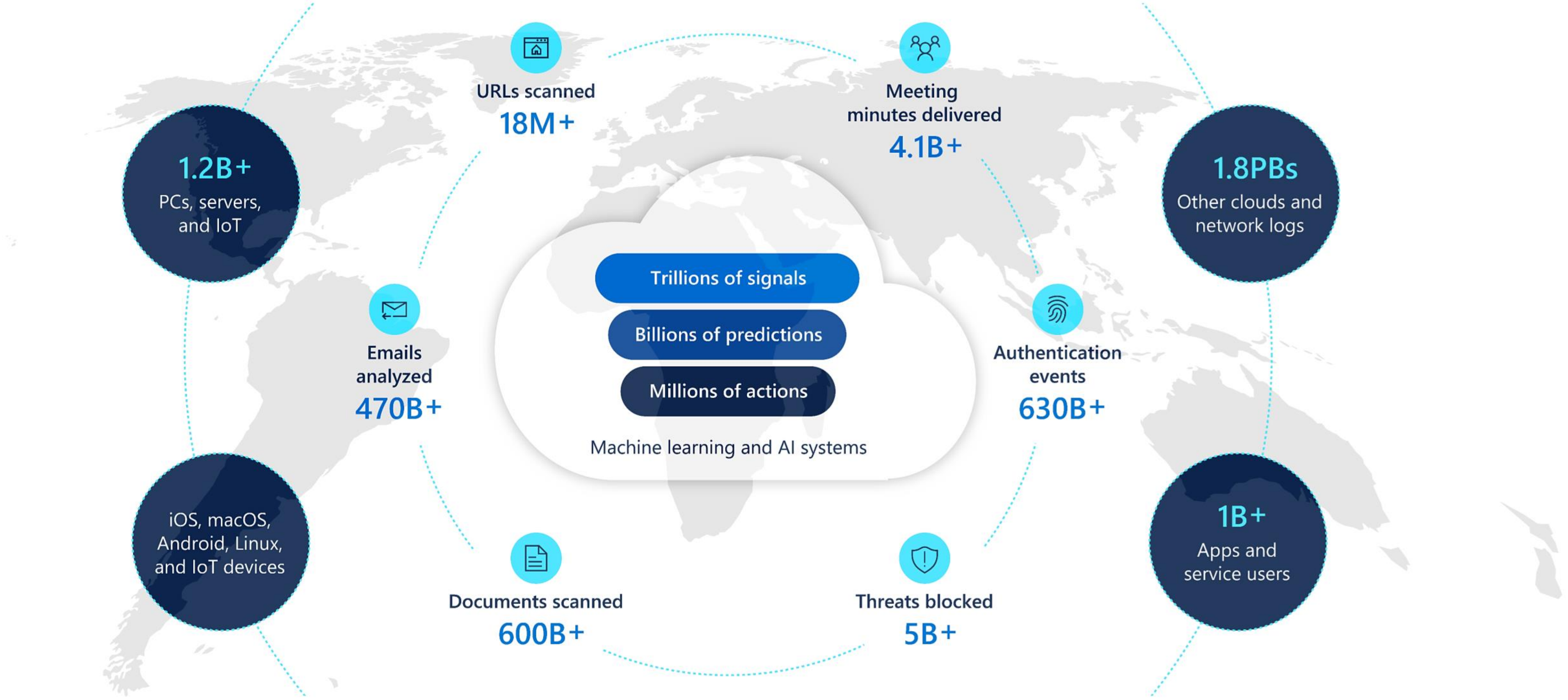
[BadAlloc vulnerabilities in widely-used RTOS/SDKs]
Rockwell Automation Micrologix 1400 PLC Systems
Rockwell Automation CompactLogix 5370
Rockwell Automation MicroLogix 1100 PLC Overflow
Schneider Electric ConneXium Buffer Overflow Vulnerability
Schneider Electric Modicon M340 Buffer Overflow Vulnerability
Siemens Industrial Products
Emerson DeltaV DCS Workstations
GE CIMPLICITY
3S-Smart Software Solutions GmbH CODESYS
AVEVA InTouch
Paradox IP150 Building Security System

IoT/OT campaigns discovered by Section 52

Operation BugDrop: Large-Scale Cyber-Reconnaissance Operation
Gangnam Industrial Style: APT Campaign Targets Supply Chain
RADIATION: DDoS for Hire Using Compromised CCTV Devices

Unique threat insights informed by 24 trillion signals

Continuously analyzed with machine learning — enriched by human expertise



1.2B+
PCs, servers, and IoT

URLs scanned
18M+

Meeting minutes delivered
4.1B+

1.8PBs
Other clouds and network logs

Emails analyzed
470B+

Trillions of signals

Billions of predictions

Millions of actions

Machine learning and AI systems

Authentication events
630B+

iOS, macOS, Android, Linux, and IoT devices

Documents scanned
600B+

Threats blocked
5B+

1B+
Apps and service users

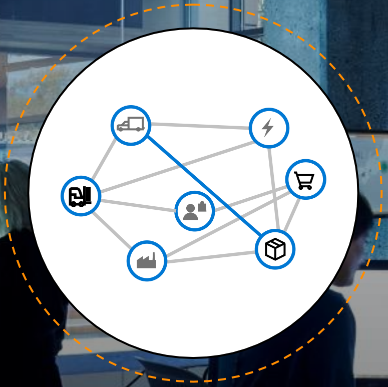
Notable customers across diverse verticals

- Microsoft Azure data centers (BMS)
- 3 of the top 10 global pharmaceutical firms
- $40B Global Manufacturer
- $30B Automotive Manufacturer
- 3 of the top 10 US energy utilities
- Electric & gas utilities across EMEA & Asia
- $15B chemical company
- $23B oil & gas company
- $4B automotive parts manufacturer
- $7B CPG manufacturer
- $40B Japanese systems integrator
- F500 transportation manufacturer
- Largest US water district
- Government agencies including US DoE

Multiple deployment options

100% On-Premises

On-premises sensors
connected to
on-premises SIEM
(Splunk, etc.)



Hybrid

On-premises sensors
managed locally
& connected to
cloud-based SIEM
(e.g., Microsoft Sentinel)

Cloud

On-premises sensors
managed via Azure Security
Center and connected to
Microsoft Sentinel

Thank You