Security Is Top Of Mind:

Create a safer world enabling organizations to digitally transform

Microsoft Security is now a $10B business with 3,500 employees
and a Leader in 5 Gartner Magic Quadrant and 7 Forrester Wave reports.

Quadrupling our cybersecurity investment to $20 billion over the next five years.
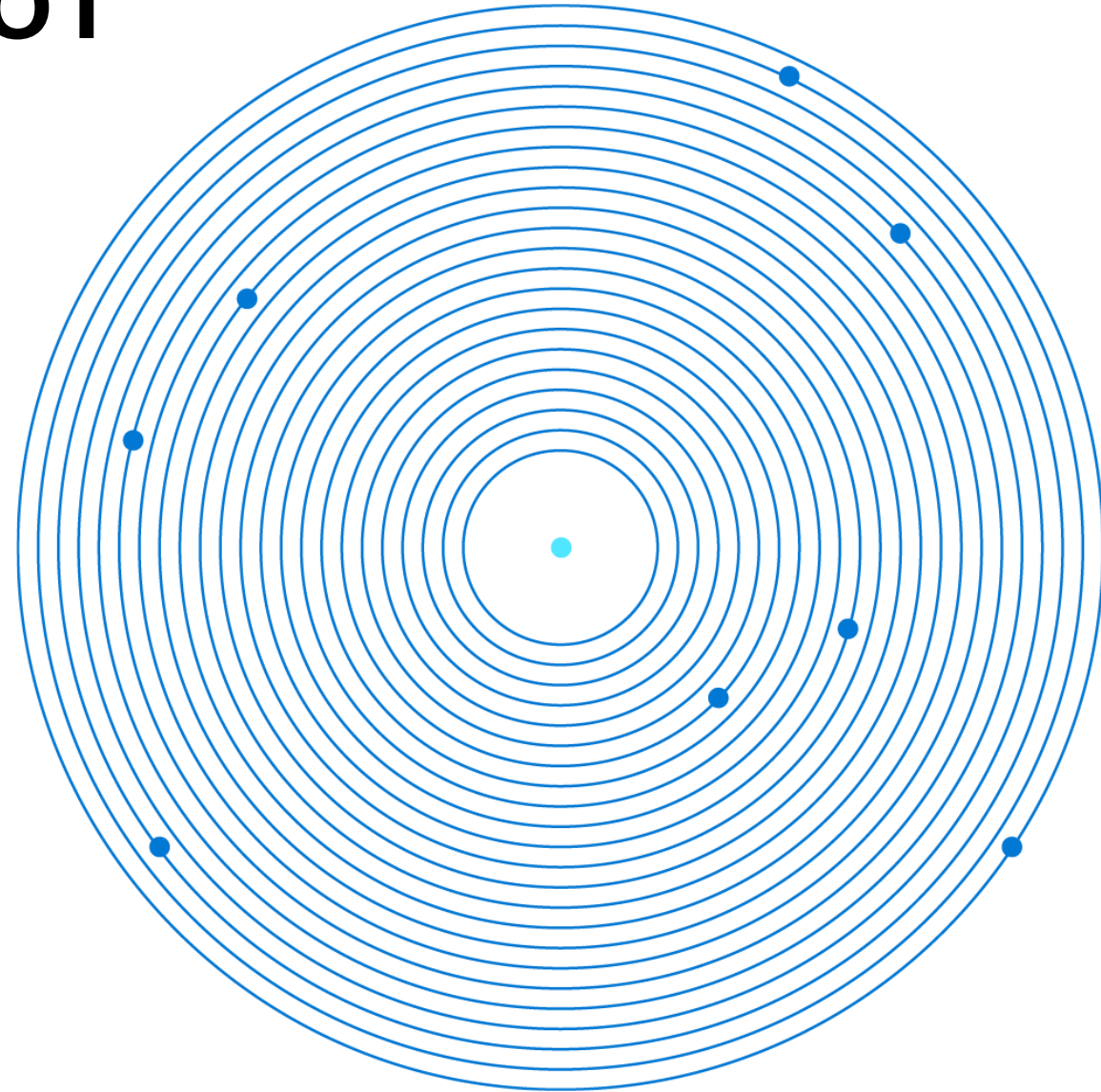
We're at the end, almost...

Microsoft Defender for IoT HOL

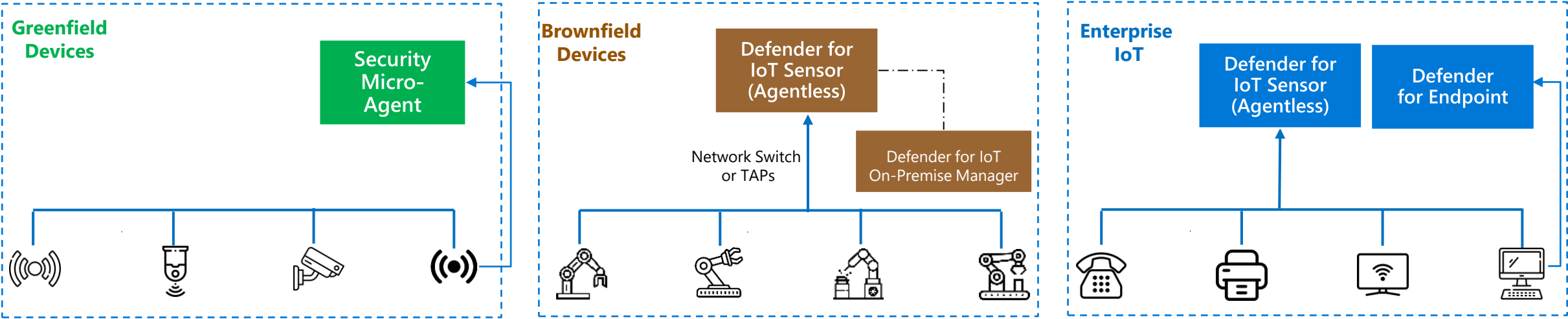**Survey│Recap│micro-agent update**
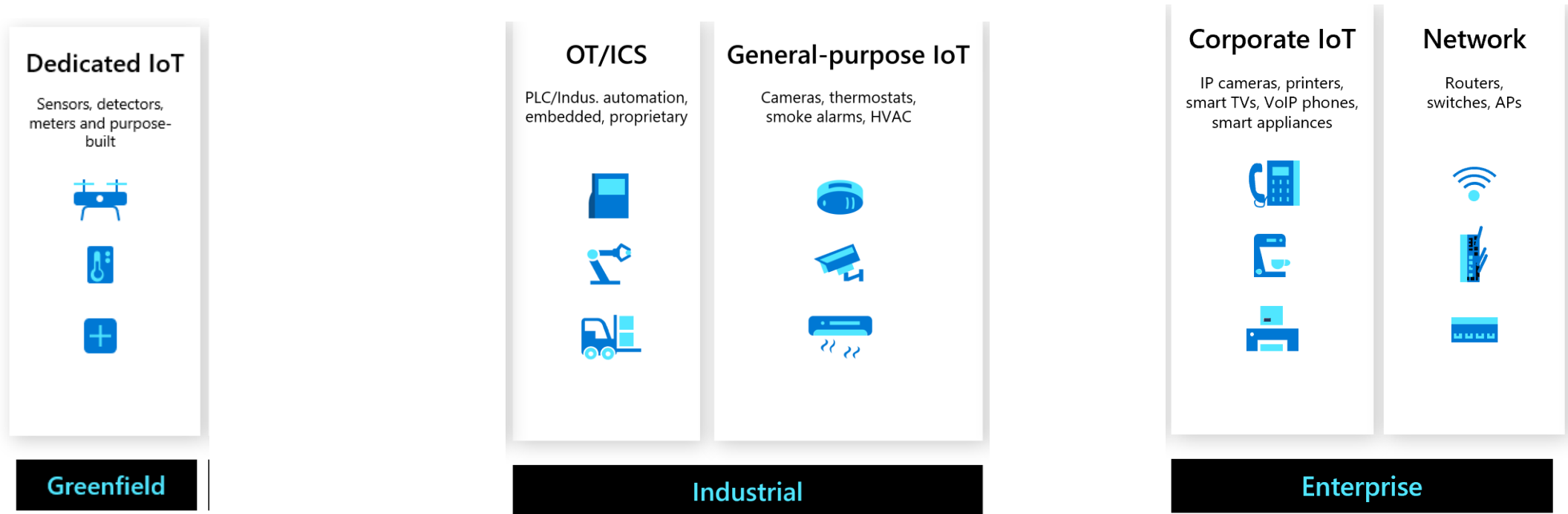
Graziano Galante

Global **P**artner **S**olution IoT - EMEA
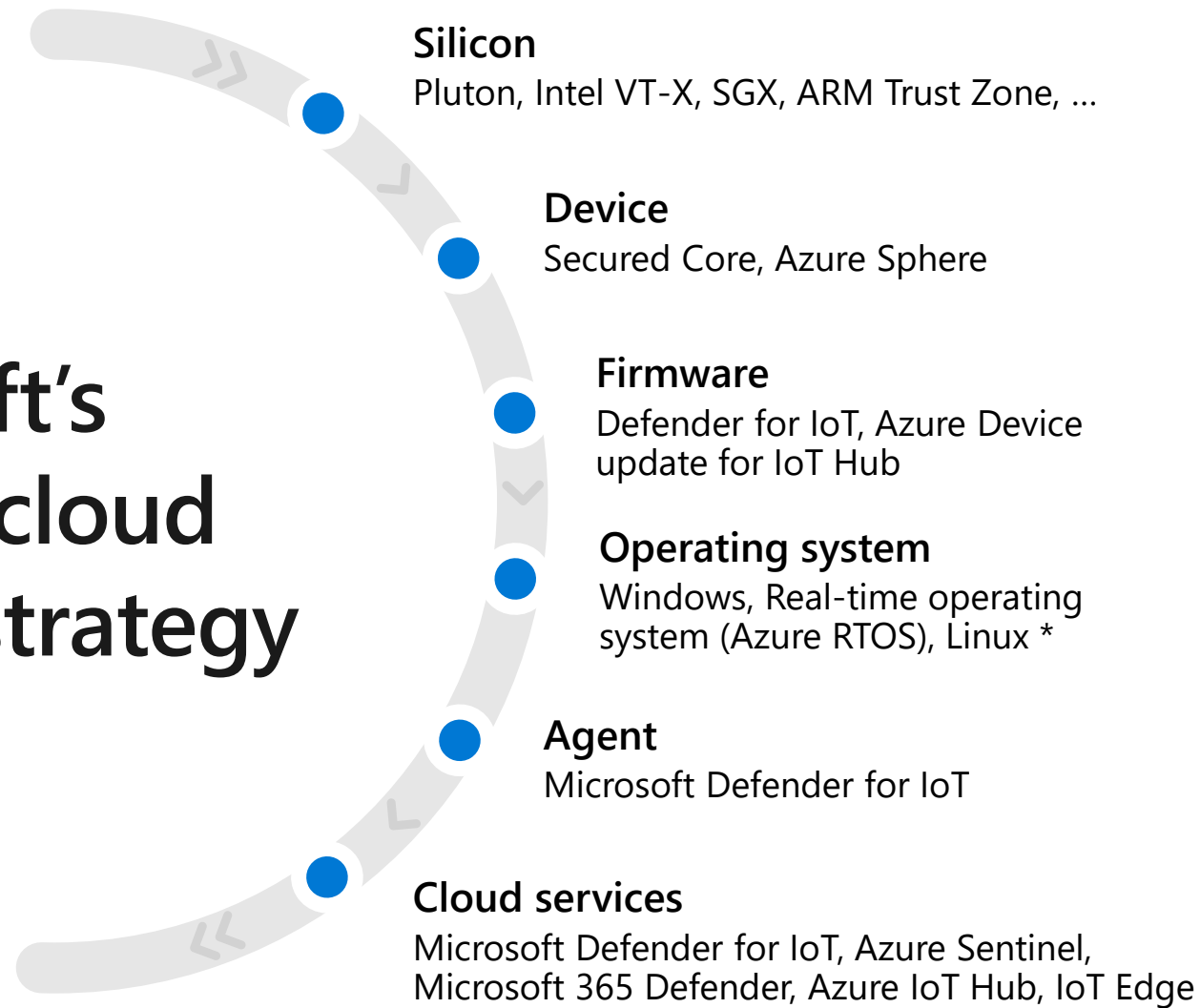
Survey

IoT/OT Security — what we have seen today

Introducing the Microsoft Defender for IoT micro agent

Built-in endpoint security for your IoT devices

Microsoft's chip-to-cloud IoT/OT strategy

Silicon
Pluton, Intel VT-X, SGX, ARM Trust Zone, ...

Device
Secured Core, Azure Sphere

Firmware
Defender for IoT, Azure Device update for IoT Hub

Operating system
Windows, Real-time operating system (Azure RTOS), Linux *

Agent
Microsoft Defender for IoT

Cloud services
Microsoft Defender for IoT, Azure Sentinel, Microsoft 365 Defender, Azure IoT Hub, IoT Edge

* Supports major Linux distributions

Device lifecycle security vision

Firmware Analysis

Sign & Certify

Build more secure devices

Credentials Scanning

Configuration Hardening

Firmware scanning – based on Refirm Labs

Hardening & Prevention
Attestation, application control, disk encryption

Update & patch
Azure Device Update

Harden, monitor & respond

Monitor & Alert
Inventory
Security posture
Vulnerabilities
Threat detection

Respond
Sentinel
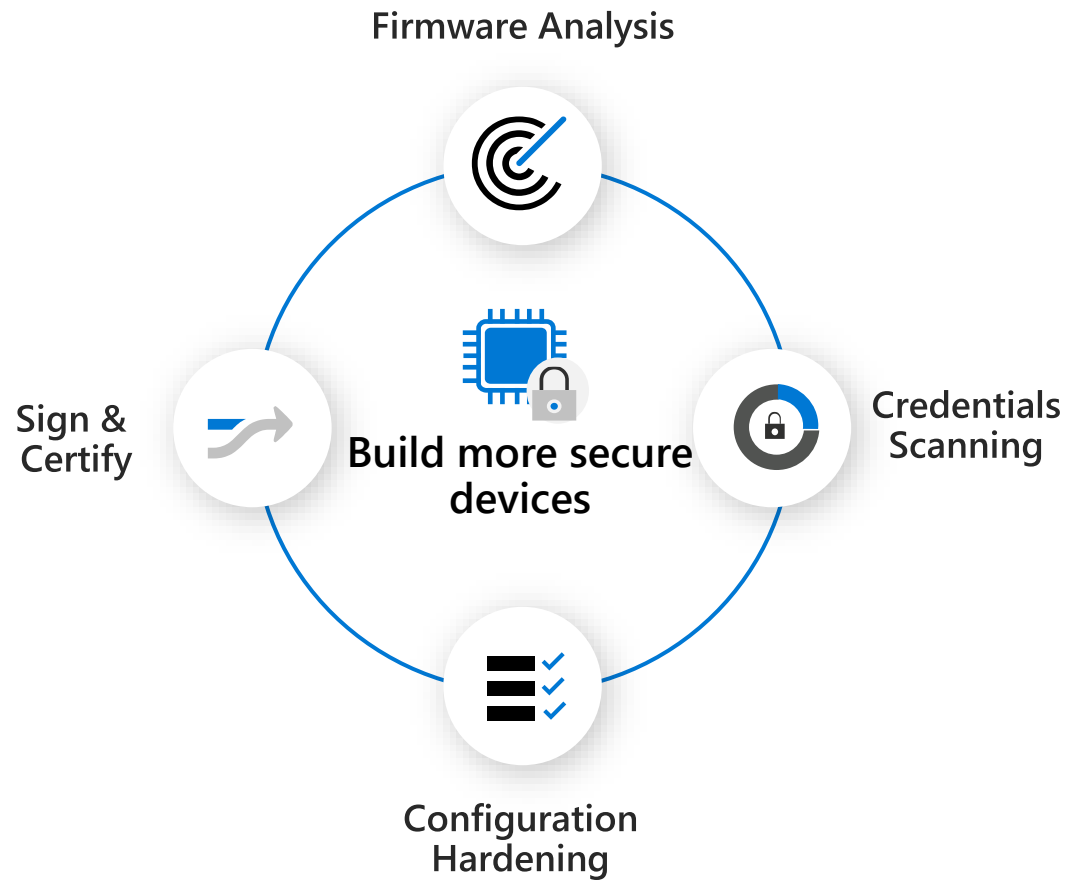
Meets the needs of your IoT devices, with minimal impact

The Microsoft Defender for IoT micro agent is easy to deploy and has minimal performance impact on the endpoint.

Optimize for performance
The Azure Defender for IoT micro agent has a very small footprint and low CPU consumption.

Plug and Play
With no specific OS kernel dependencies and support for all major IoT operating systems, it meets your devices where they are.

Flexible deployment
As a standalone agent, Azure Defender for IoT's micro agent supports different distribution models and flexible deployment.
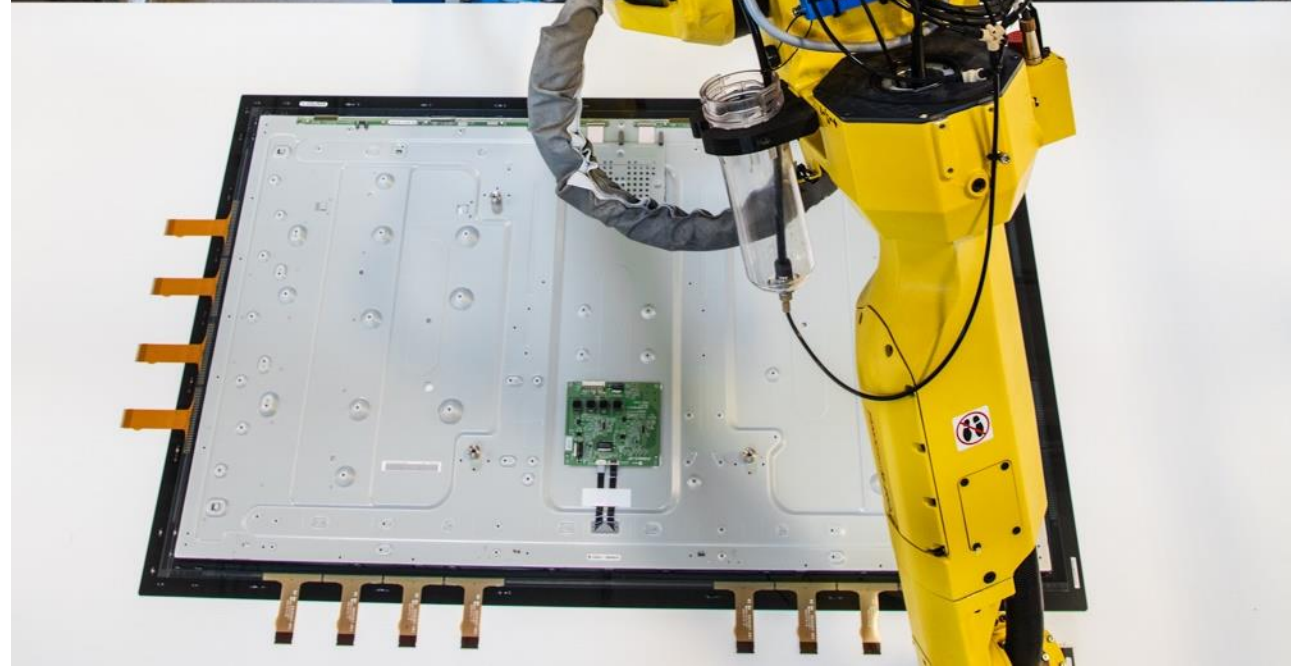
Flexible distribution and deployment models

Choose the deployment method that works best for your environment, devices, and organization.

Source code

- Incorporate the micro agent into firmware during the build phase of your project.

- Customize the source code to include only what you need.

- Accommodate restricted devices with stripped down operations systems
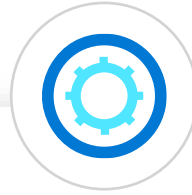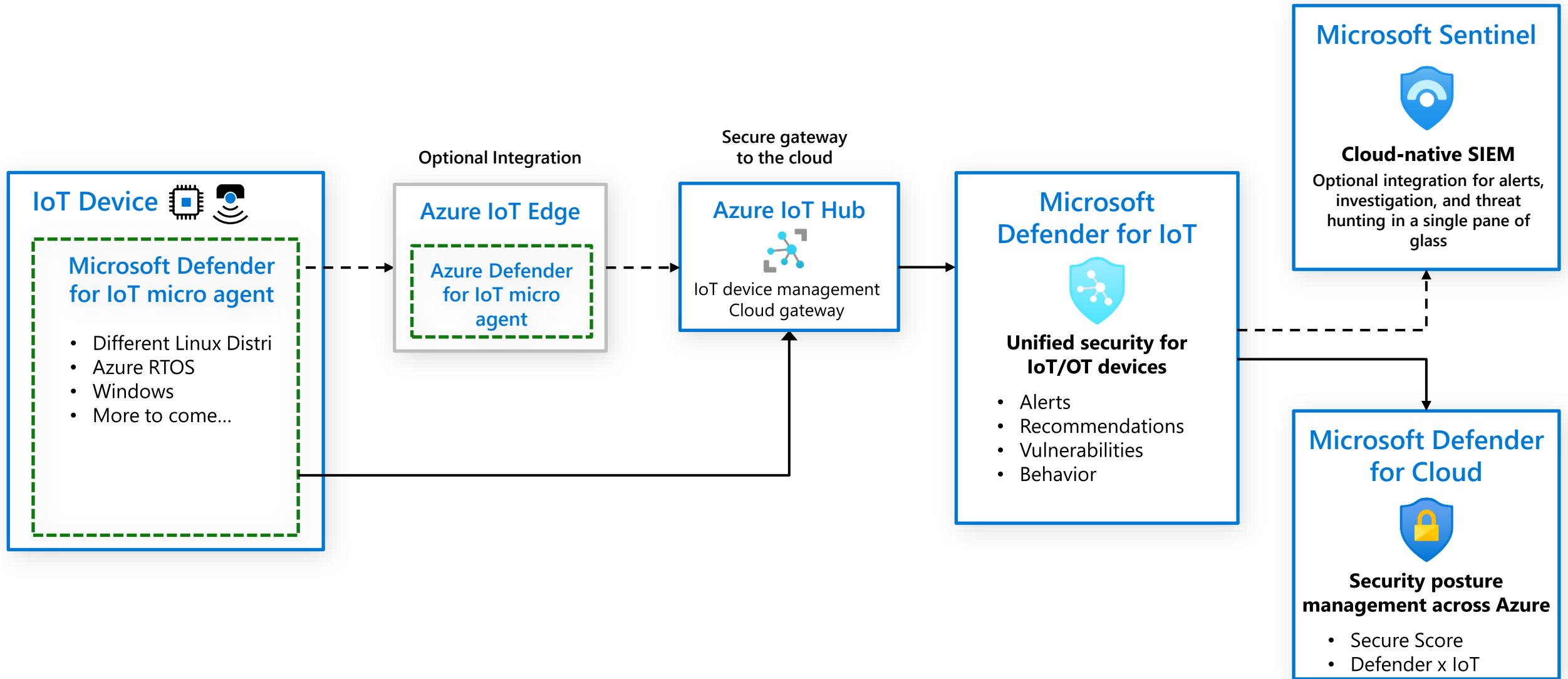
Binary package

- Support post-deployment installation as a binary package

Standalone or integrated with Azure IoT

- Deploy as a standalone agent, or integrate directly into the Azure IoT ecosystem

- Built in to **Azure RTOS**

- Integrated into **Azure IoT Edge**

[Agent Based IoT security with Microsoft Defender for IoT - Microsoft Tech Community](#)

How it works

IoT Device 🔲 📡

Microsoft Defender
for IoT micro agent

- Different Linux Distri
- Azure RTOS
- Windows
- More to come…

Optional Integration

Azure IoT Edge

Azure Defender
for IoT micro
agent

Secure gateway
to the cloud

Azure IoT Hub

IoT device management
Cloud gateway

**Microsoft
Defender for IoT**

**Unified security for
IoT/OT devices**

- Alerts
- Recommendations
- Vulnerabilities
- Behavior

Microsoft Sentinel

Cloud-native SIEM

Optional integration for alerts,
investigation, and threat
hunting in a single pane of
glass

**Microsoft Defender
for Cloud**

**Security posture
management across Azure**

- Secure Score
- Defender x IoT

Firmware scanning – based on Refirm Labs

Thank You