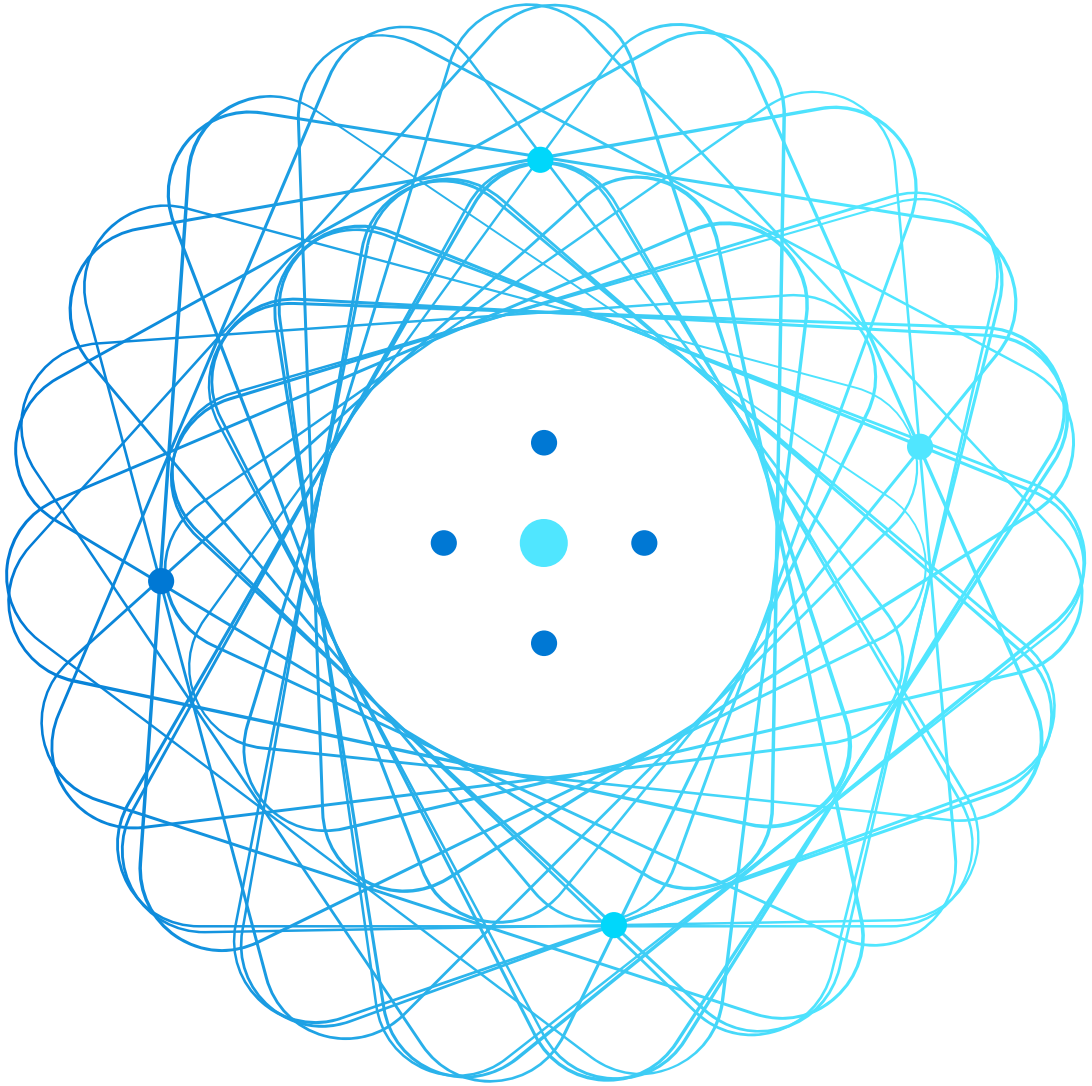
Microsoft Azure

AZ-220T01
Module 10: Azure Security Center and IoT security considerations



Lesson 1: Learning objectives

Module 10 – Learning objectives

- Describe security concerns and best practices for an IoT solution
- Describe the Azure IoT Security Architecture and Threat Modeling
- Describe the features and support provided by Azure Defender for IoT
- Configure Security Agents and Security Module Twins
- Aggregate Azure Defender for IoT Events

Lesson 2: Security fundamentals for IoT solutions

Security recommendations

General:

Stay up to date!

Keep authentication keys safe

Use device SDKs when possible

Identity and Access Management:

Define access control for the hub

Define access control for back-end services

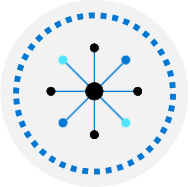
Data protection:

Secure device authentication

Secure device communication

Secure service communication

Security recommendations



Networking:

Protect physical access to your devices

Build secure hardware

Monitoring:

Monitor unauthorized access to your devices

Monitor your IoT solution from the cloud (overall health)

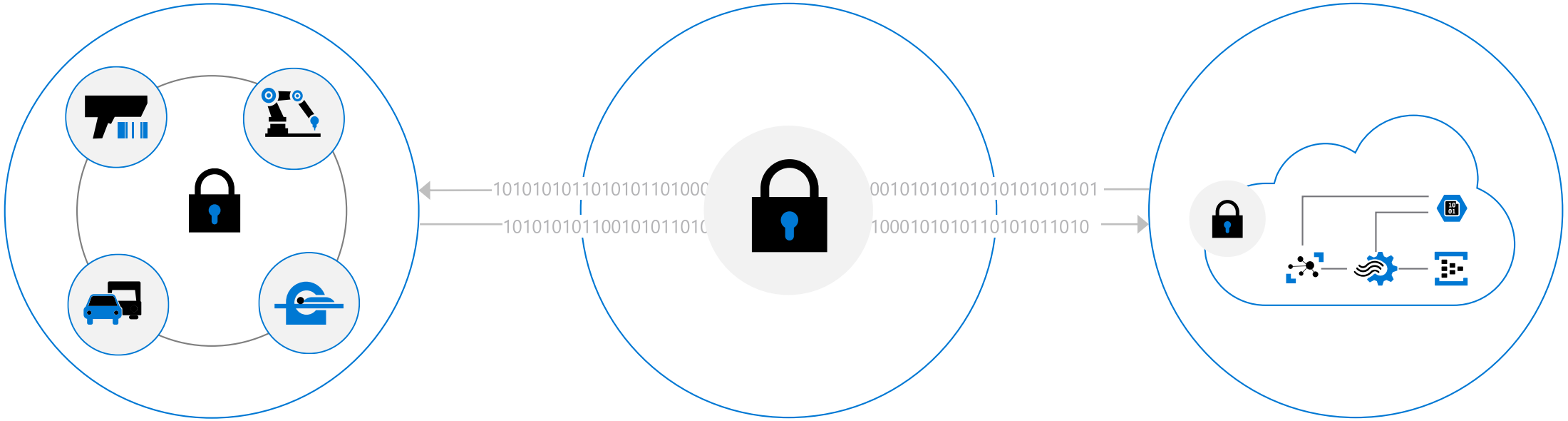
Set up diagnostics

Security in IoT must be end-to-end

Securely connect million of devices…

…over a secure internet connection…

…to Microsoft Azure – Built with security from the ground up



Device Security

Device SDKs in multiple languages
Any OS | Any HSM including Azure Sphere

Connection Security

X.509/TLS-Based Handshake and Encryption

Cloud Security

IoT Hub | Windows IoT | Azure Sphere Services
Azure Trust Center | Azure Compliance Offerings

IoT security best practices for the IoT developer role

Follow secure software development methodology

Choose open-source software with care

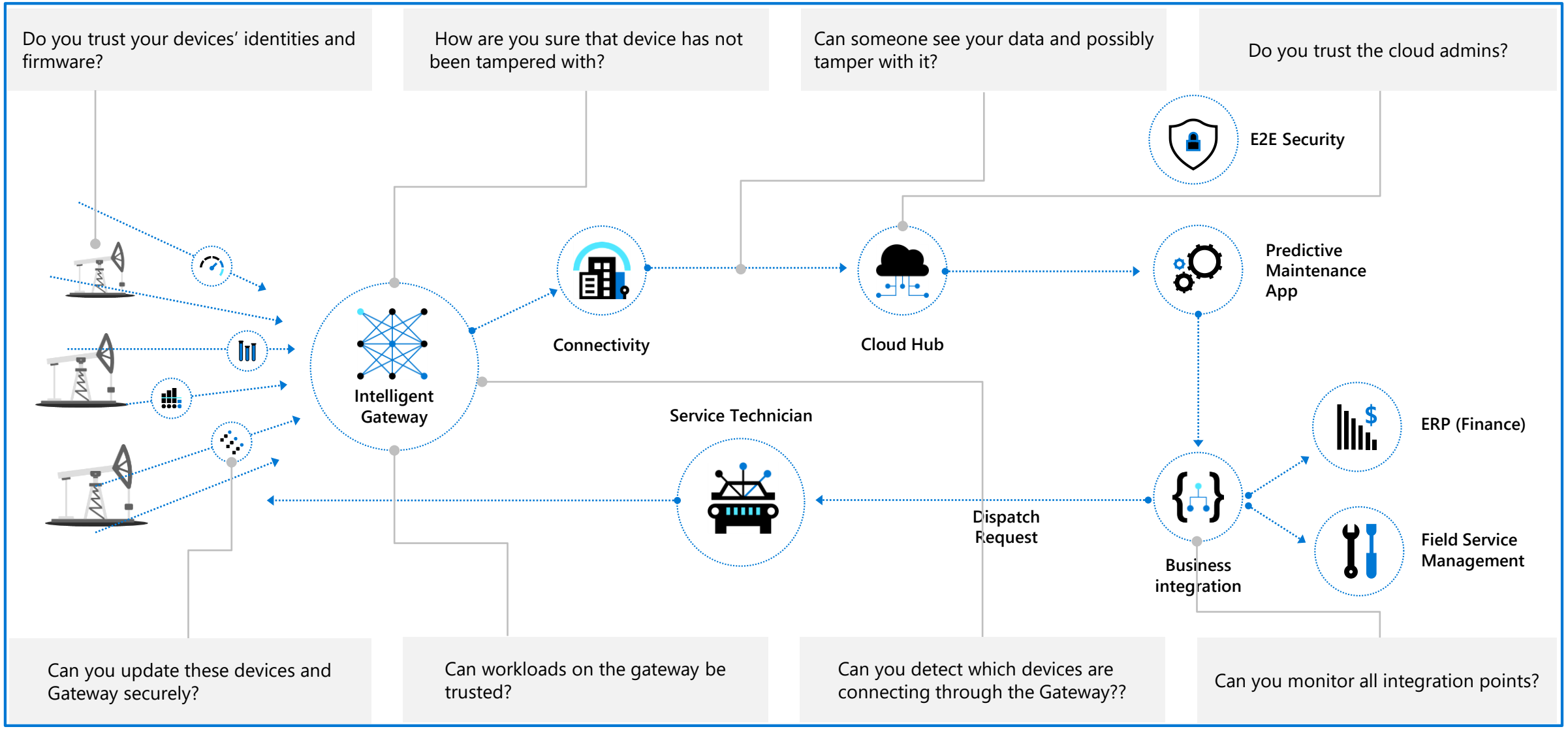
Integrate with care

IoT security architecture and threat modeling

From a security architecture and threat modeling viewpoint, it's typical for dedicated security staff and/or architects to own that responsibility…

But developers need to be able to participate in the conversations!

Threat model



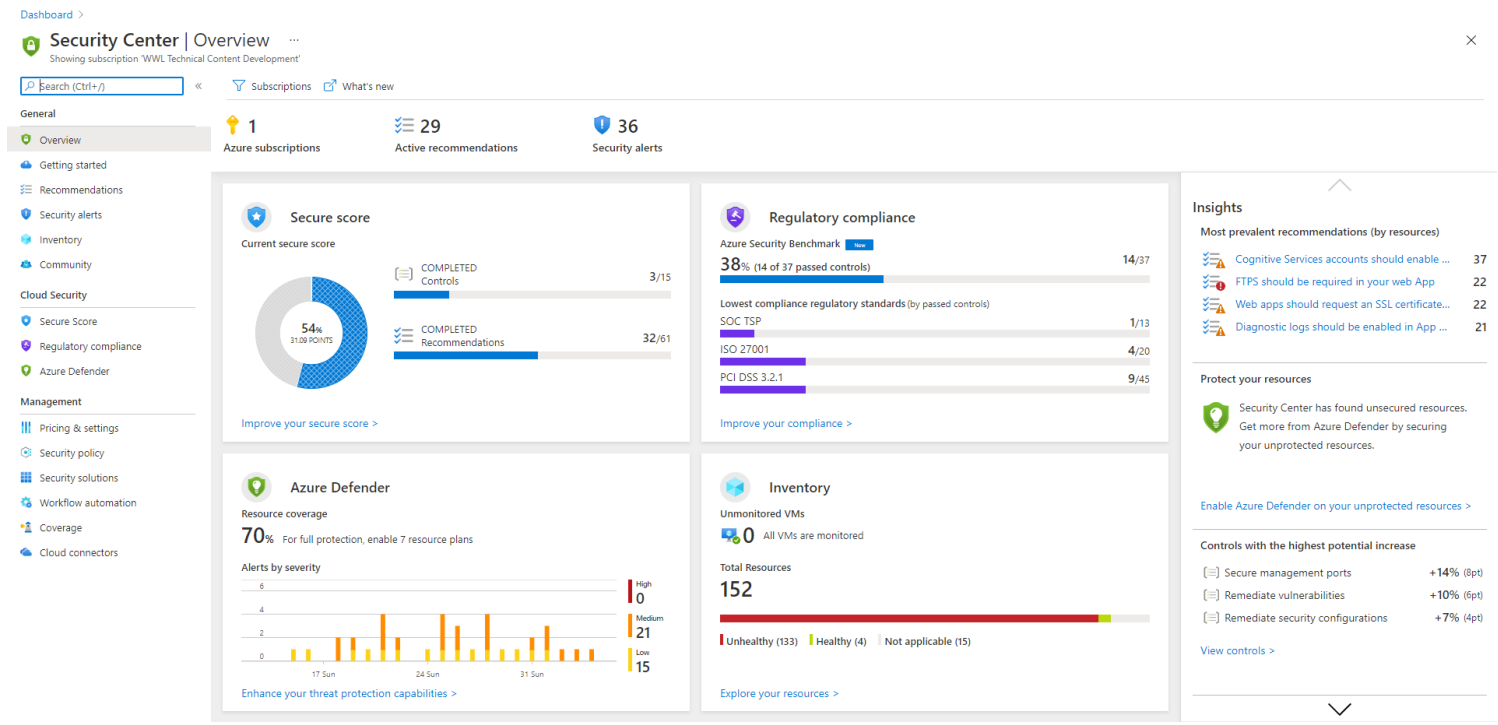
Lesson 3: Introduction to Azure Defender for IoT

Introduction to Azure Security Center

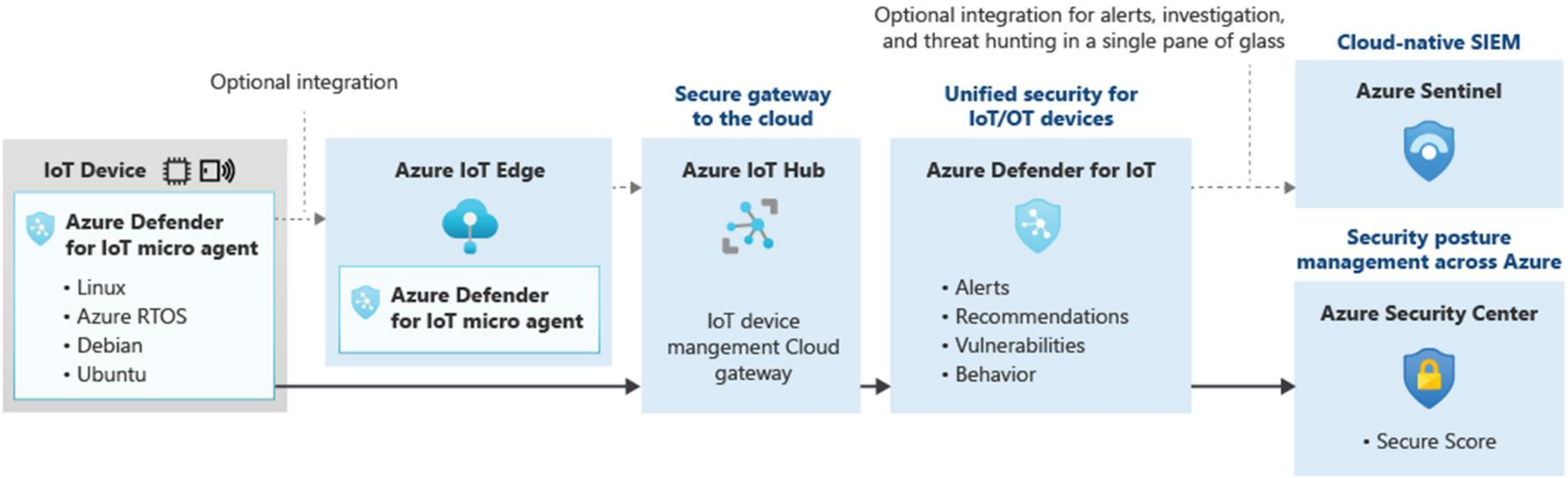
Visibility into security posture and state of the Azure IoT Solution

Single pane of glass to manage IoT and hybrid cloud security infrastructure

Receive actionable, prioritized alerts to respond to any potential compromises of your Azure IoT solution



Introduction to Azure Defender for IoT



Azure Defender for IoT deployment options

Agentless solution – provides passive monitoring of IoT device communication on a network

Agent-based solution – provides Built-in and Enhanced modes for monitoring IoT devices. IoT Hub integrates the Agent-based solution option

Configure built-in IoT Hub integration

Standard Tier IoT Hubs

Geolocation and IP address handling:

Default: IP addresses for incoming and outgoing connections from IoT Devices, IoT Edges, and IoT Hubs are collected

Log Analytics creation:

Automatic for back-end data storage to support the solution

5 GB for 31 days included for no extra charge

Customize your IoT security solution:

Can be extended beyond IoT Hub to bring in other resources

Leverages existing Security Center functionality

Built-in alerts

The built-in assessments include a large number of alert options… they include…

Built-in alerts for IoT devices, such as:

- Attempted firewall disabling
- Attempted port forwarding
- Attempted local sign-ins

Built-in alerts for IoT Hub, such as:

- x.509 device certificate thumbprint mismatch
- Expired or invalid SAS token
- Attempt to change diagnostic settings without permission

Customizable security alerts

"You know your IoT devices best…"

Examples - custom alerts will relate to your scenario:

How many direct method calls is too many?

How many rejected messages is too many?

Custom messages can be sent through a custom message SDK

Lesson 4: Enhance Protection with Azure Defender for IoT Security agents

Your security agent options

Characteristics	C-based security agent	C#-based security agent
Supported Windows platforms?	No	Yes (WMI pre-requisite)
Supported Linux platforms?	Yes, x64 and x86	Yes, x64 only
Linux prerequisites	libunwind8, libcurl3, uuid-runtime, auditd, audispd-plugins	libunwind8, libcurl3, uuid-runtime, auditd, audispd-plugins, sudo, netstat, iptables
Disk footprint	10.5 MB	90 MB

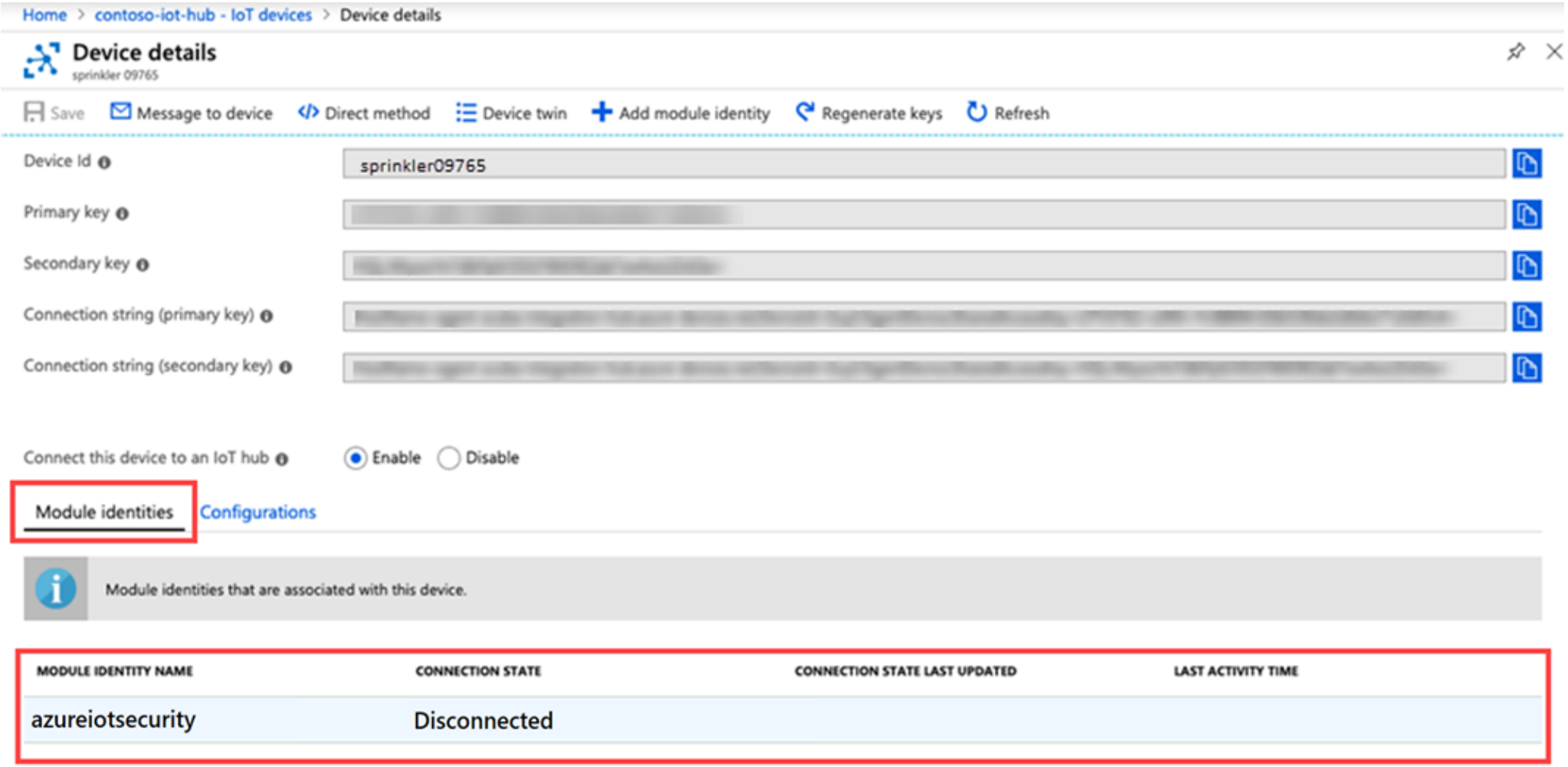
The above lets you figure out which agent to use in any given situation…

Security agent deployment and testing

Deployment details depend on the device, but all have the same basic pattern…

1. Create an azureiotsecurity module definition on the device registration; The agent presents as a device module to IoT Hub and uses a module twin for configuration
2. Download the appropriate script from GitHub
3. Review it
4. Execute it
5. Run the simulated attack script to test your end-to-end solution

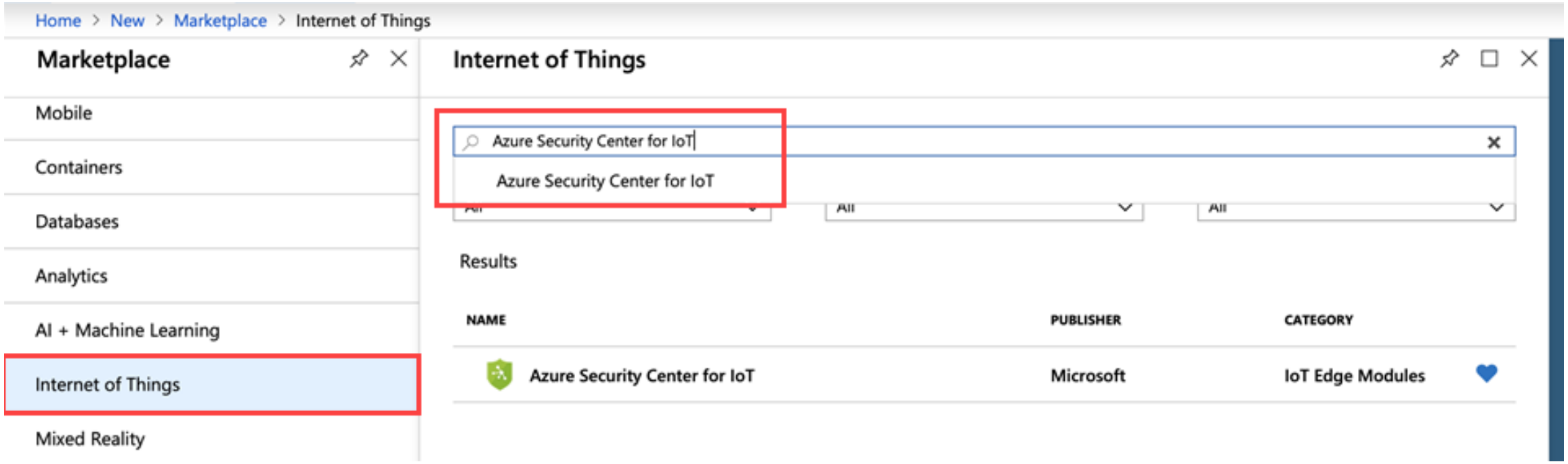
Module configuration on a non-edge device



Deploy a security module on your IoT Edge device

On an IoT Edge, deployments are done through modules, as previously discussed…

In the Marketplace, there is a legacy IoT Edge Module for Azure Security Center for IoT that can be viewed



Security agent authentication

Authentication methods:

SecurityModule mode – authenticated using a shared key configured in the module

Device mode – authenticated using the device's identity, shared key or certificate

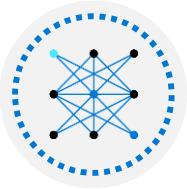
Authentication method initially set during deployment

Can be changed in the appropriate configuration file after deployment

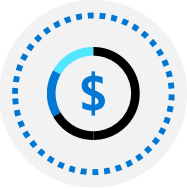
Built-in agent-based alerts

Agents add even more alerts to the solution… a small fraction:

Unexpected binary command line



Apparent bot behavior



Crypto-coin mining

Security configuration file unexpectedly accessed (e.g. .htaccess)

Local user added to a new group

Recommendations from Azure Defender for IoT

Device *configuration* recommendations, such as locking down an open firewall

Device *operational* recommendations, such as correcting conflicting settings in the security module twin configuration

IoT Hub *configuration* recommendations, such as correcting duplicate credentials across devices

Baseline

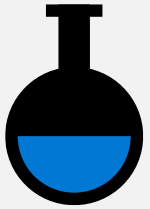
Baseline – allow running custom configuration checks on a device and comparing the result to a desired result

Stored in an XML file on the device being evaluated

Module twin gives location of the file and a SHA256 hash of the file

File format documentation is mostly by examples in GitHub

Lesson 5: Module Labs



Module 10 Labs

Lab 18: Azure Defender for IoT:

You will enable Azure Defender for IoT Hub

You will manually create a security module twin

You will add a security agent for C# that you will deploy on your simulated device

Lesson 6: Module 10 review questions

Module review: Question 10.1

A company is implementing a threat modeling process to help improve the security of their IoT solution.

Which of the following answer choices lists the three primary areas of consideration within the threat modeling process?

Answer A:
Device security features, cloud security features, data security features.

Answer B:
Security and privacy features, features whose failures are security relevant, features that touch a trust boundary.

Answer C:
Hardware features, software features, cloud service features.

Module review: Question 10.2

When working to develop a secure IoT solution, which of the following tasks is typically assigned to the IoT developer role?

Answer A:
Make hardware tamper proof.

Answer B:
Protect against malicious activity.

Answer C:
Follow secure software development methodology.

Module review: Question 10.3

Which of the following choices is a feature of Azure Defender for IoT?

Answer A:
Azure Defender for IoT is enabled by default when an IoT Hub resource is created.

Answer B:
Azure Defender for IoT requires Device agents.

Answer C:
Azure Defender for IoT includes a DPS enrollment pipeline.

Module review: Question 10.4

A developer has started an investigation of Azure security tools.

What is Azure Security Center intended to help with?

Answer A:
Securing the devices and securing device communications as they transmit over the wire.

Answer B:
Securing the network and the services.

Answer C:
Developing the threat models.

Module review: Question 10.5

A developer has deployed the Enhanced mode of Azure Defender for IoT, and they are now ready to implement security agents.

Which of the following statements describe how security agents are used?

Answer A:

Security agents handle raw event collection from the device operating system.

Answer B:

Security agents are part of the IoT Edge device attestation mechanism for DPS.

Answer C:

Security agents require maximum available resources.

Module review: Question 10.6

A developer wants to deploy Azure Defender for IoT.

Which of the following choices describe the differences between the Built-in and Enhanced deployment options?

Answer A:
Real-time monitoring is only available with the Enhanced option.

Answer B:
Built-in mode uses device agents on your devices to aggregate and analyze raw security events from your devices.

Answer C:
Enhanced mode uses device agents on your devices to aggregate and analyze raw security events from your devices.