Microsoft Azure

Azure IoT Academy

Transforming your business

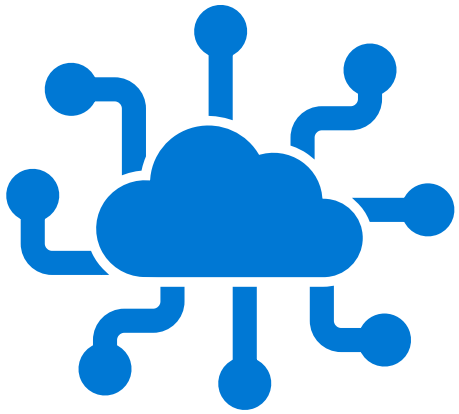
Month 3, Day 2

Rebekah Midkiff
Technical Specialist
Microsoft

Alan Blythe
Sr. Technical Specialist
Microsoft

Eric Johnston
Sr. Technical Specialist
Microsoft

IoT Academy Expectations



- *We have a very large audience, so please keep yourself on mute except when called.*
- *Please raise your hand and wait for acknowledgement before unmuting to ask a question.*
- *Use Teams reactions to ease interactions of a large audience*
- *We want this to be interactive so please don't hesitate to let us know if you have a question (comment in chat or raise hand).*
- *If you're stuck on a hands-on lab, we request that you notify us in chat and raise your hand so we can move you to a breakout meeting for assistance.*

IoT Academy Journey

Month 3

- Defender
- IoT Security
- Azure Sentinel
- Azure Pricing & Cost Management
- Partner Showcase
- Awards Ceremony

Month Three, Day 1 Review

- Microsoft Defender
  - Operational Technology (OT) Security vs IT Security
    - OT risk = business risk
  - PCAP – network recording of traffic that is being presented too it. It's the recording of all the packets that are being presented too it. It's a VCR for packets
  - Reviewed alerts, grouped by severity
  - Risk assessment report
  - Data mining report
  - Reviewed event timeline
  - Reviewed trends and statistics
    - Created dashboard
    - Reviewed alerts

Day Two Agenda (All times are in ET)

- 10:05am – 10:20am Introduction/Expectations Kickoff - Team
- 10:20am- 12:00pm Presentation
- 12:00pm – 12:15pm Coffee Break (Flexible timing)
- 12:15pm – 1:00pm Presentation/Certificate Demo

Day Three Agenda (All times are in ET)

- 10:10am – 11:00am Partner Showcase - CloudRail
- 11:00am- 11:30pm Break
- 11:30pm – 12:30pm Partner Showcase – PTC
- 12:30pm – 12:45pm Break
- 12:45pm – 1:00pm IoT Close – Awards Ceremony

Why a Security focused primer?

- FBI reports $4.2 billion in losses in 2021
- Loss of consumer trust
- Loss of trade secrets
- Risk of litigation, negligence
- Increasing regulation

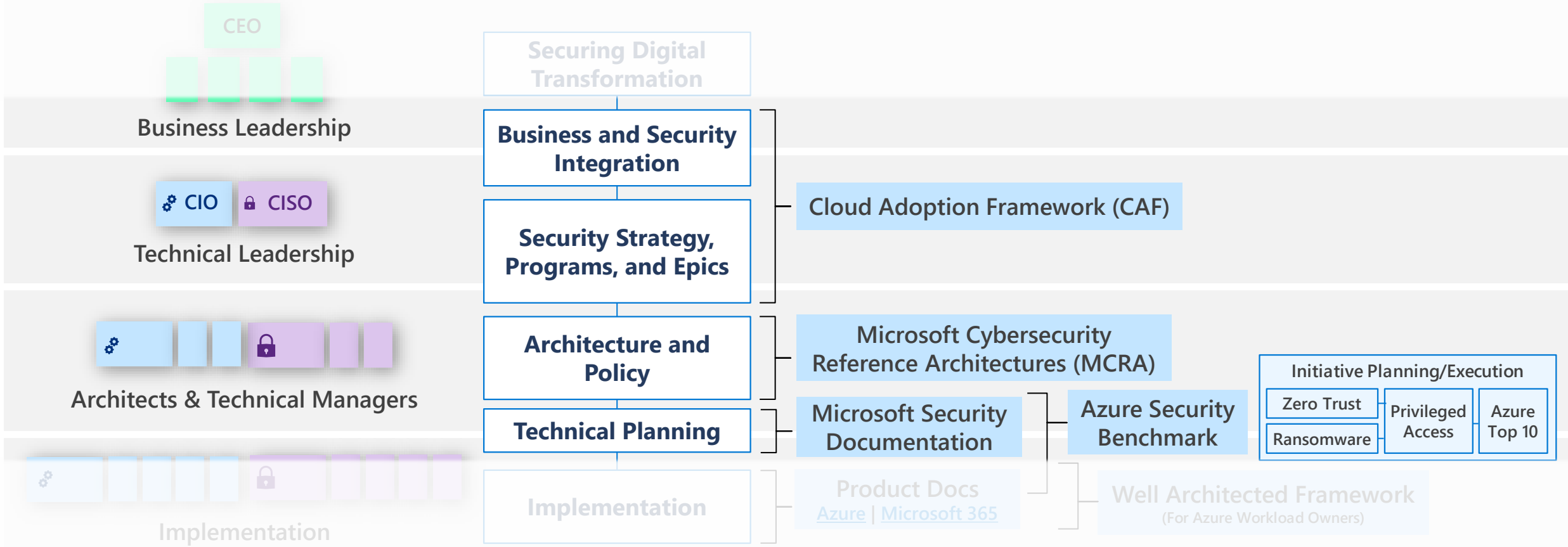
Agenda

- Why is Zero Trust important
- Principles and components of Zero Trust
- How to implement the Zero Trust model
- Microsoft resources to enable your Zero Trust journey

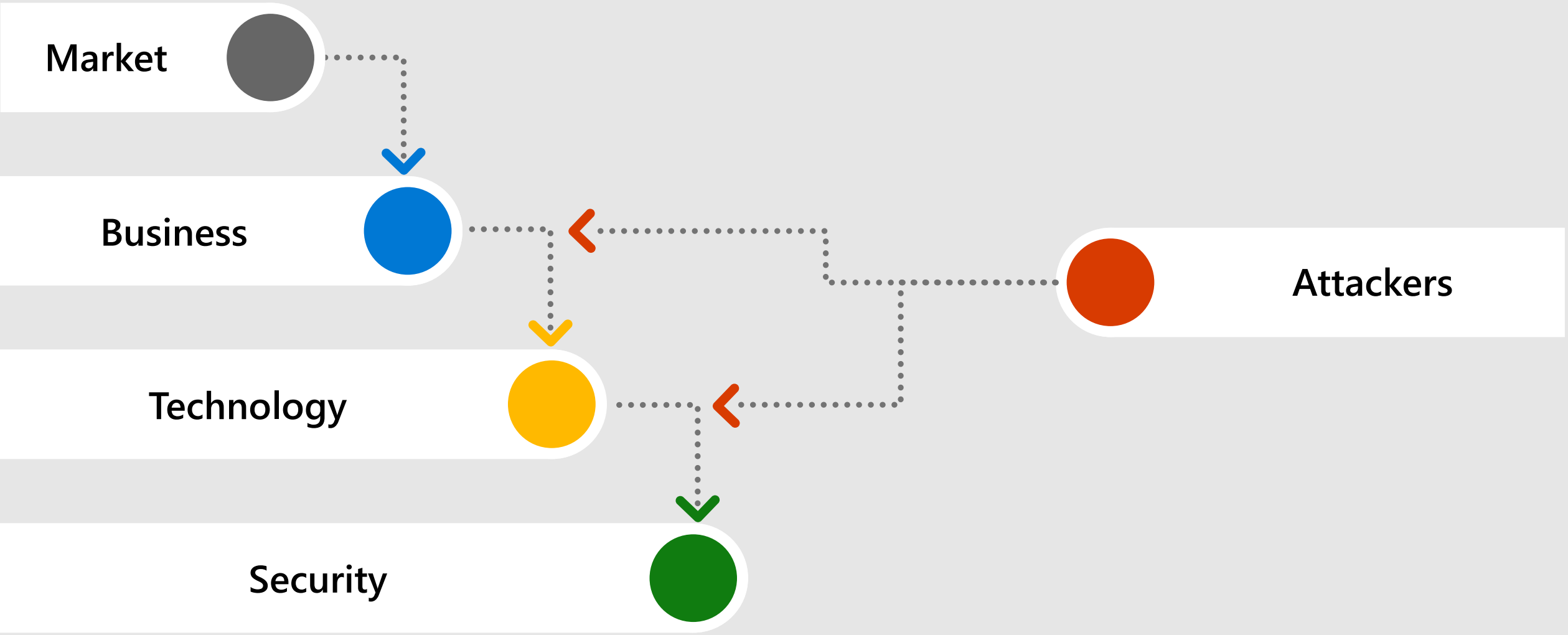
Security Guidance

May 2021 - https://aka.ms/MCRA

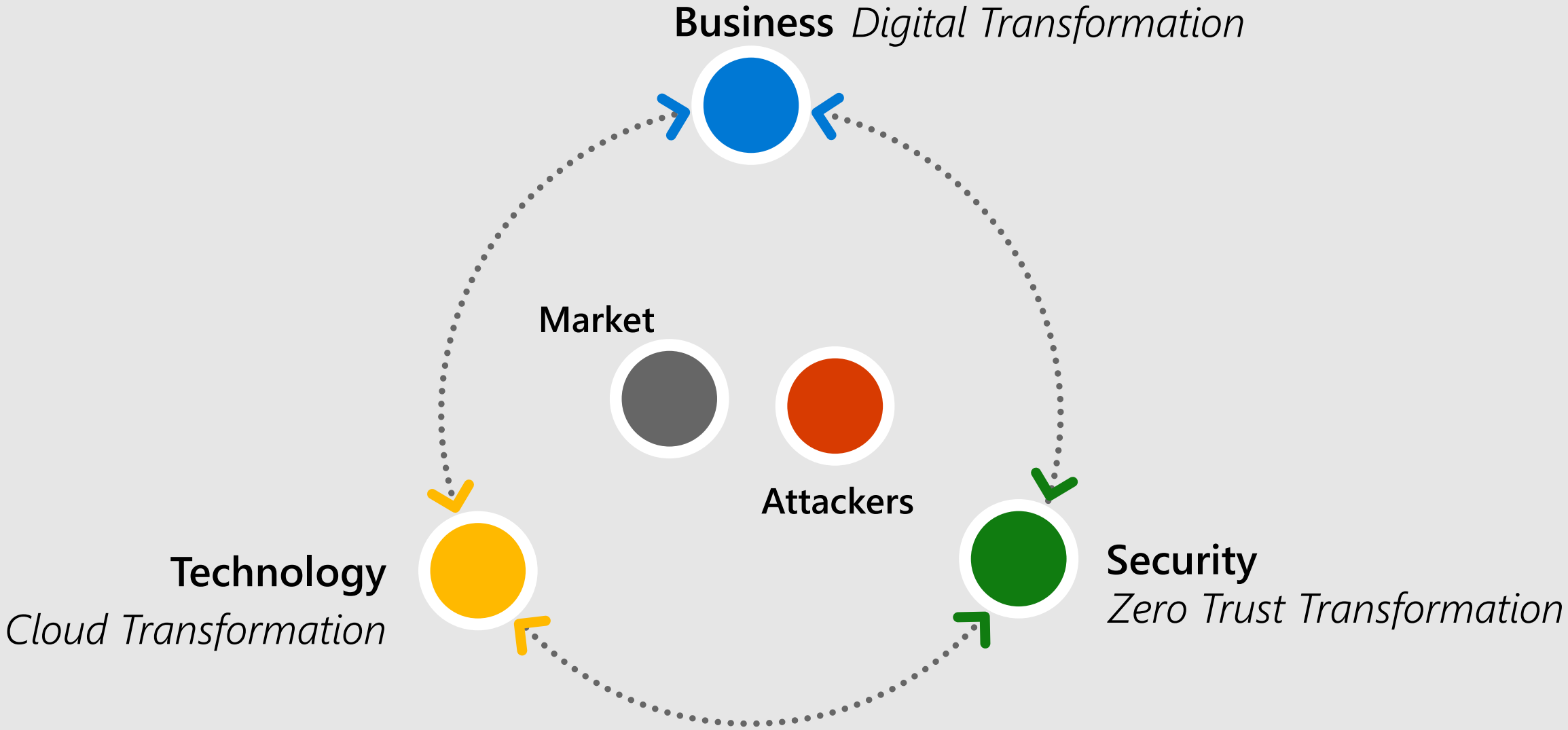
Microsoft



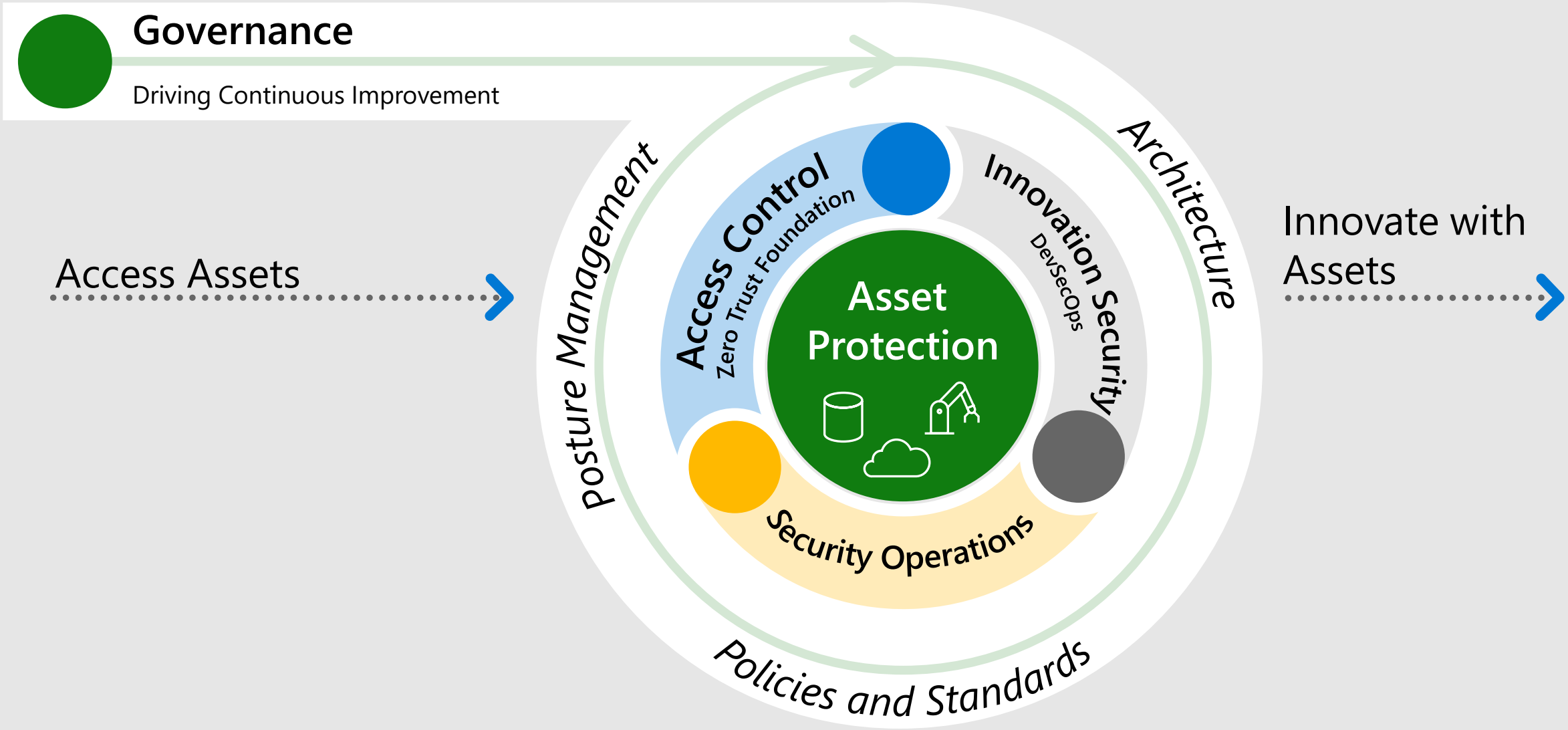
The world is transforming rapidly

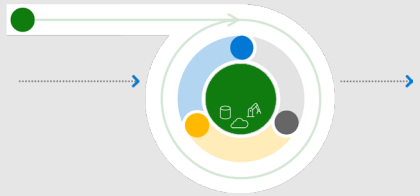


Working together



Security Shifts to Continuous Improvement





Build Modern Security

Common Modernization Initiatives

Ransomware Recovery Readiness

Ensure backups are validated, secure, and immutable to enable rapid recovery

- Zero Trust Foundations
- Modern Security Operations
- Infrastructure and Development
- OT and IoT Security
- Data, Compliance, and Governance

“Zero Trust” has been around for a while

Historically slow mainstream adoption for both network & identity models:

Network – Expensive and challenging to implement
Google’s BeyondCorp success is rarely replicated

Identity – Natural resistance to big changes
Security has a deep history/affinity with networking

Increasing consensus and convergence (though still some variations)

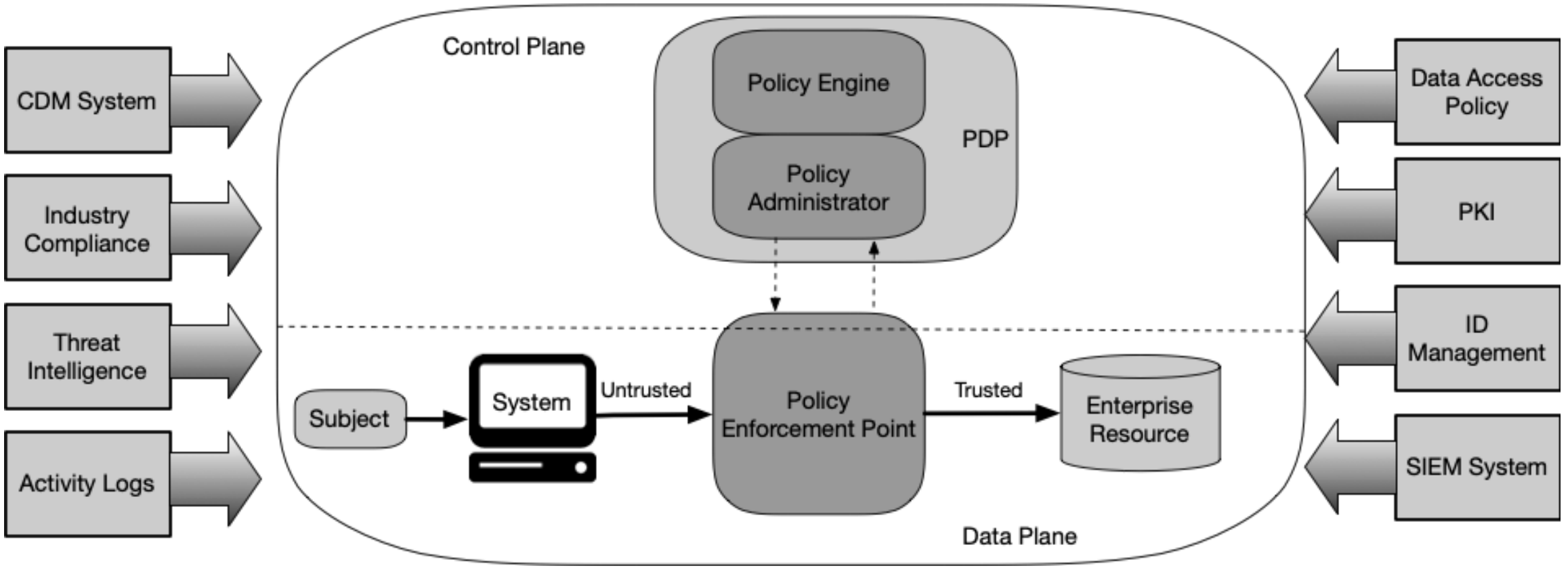
Principles of Zero Trust

Instead of assuming everything behind the corporate firewall is safe, Zero Trust assumes *an open environment where trust must be validated*.

- **Assume breach** – Assume that attackers will succeed (partially or fully) and design accordingly
- **Verify explicitly** – Validate trust of users, devices, applications, and more using data/telemetry
- **Use least privileged access** – to limit the impact of any given compromise

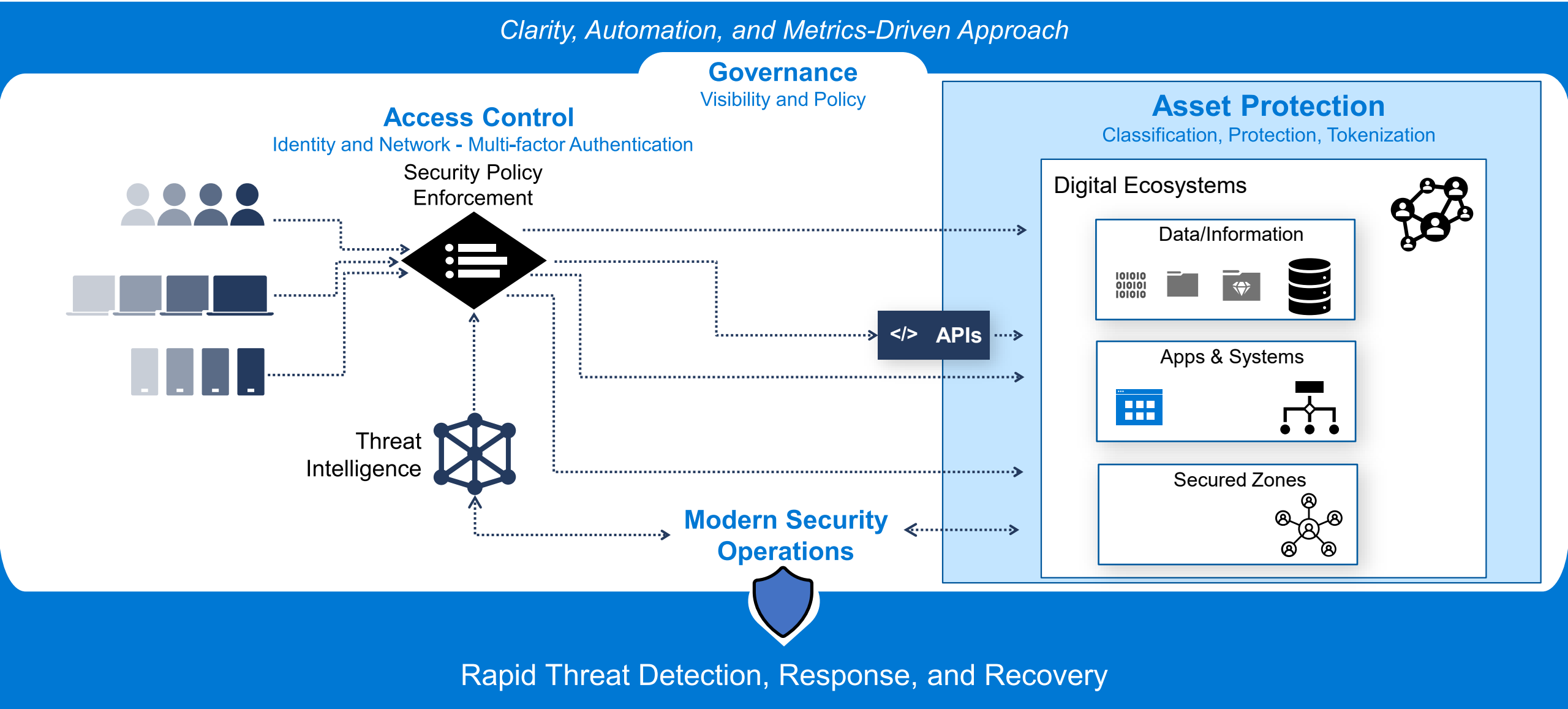
Microsoft is actively working with NIST, The Open Group, CISA, and many others across industry to harmonize definitions, model, and architectures for Zero Trust

NIST Zero Trust Architecture

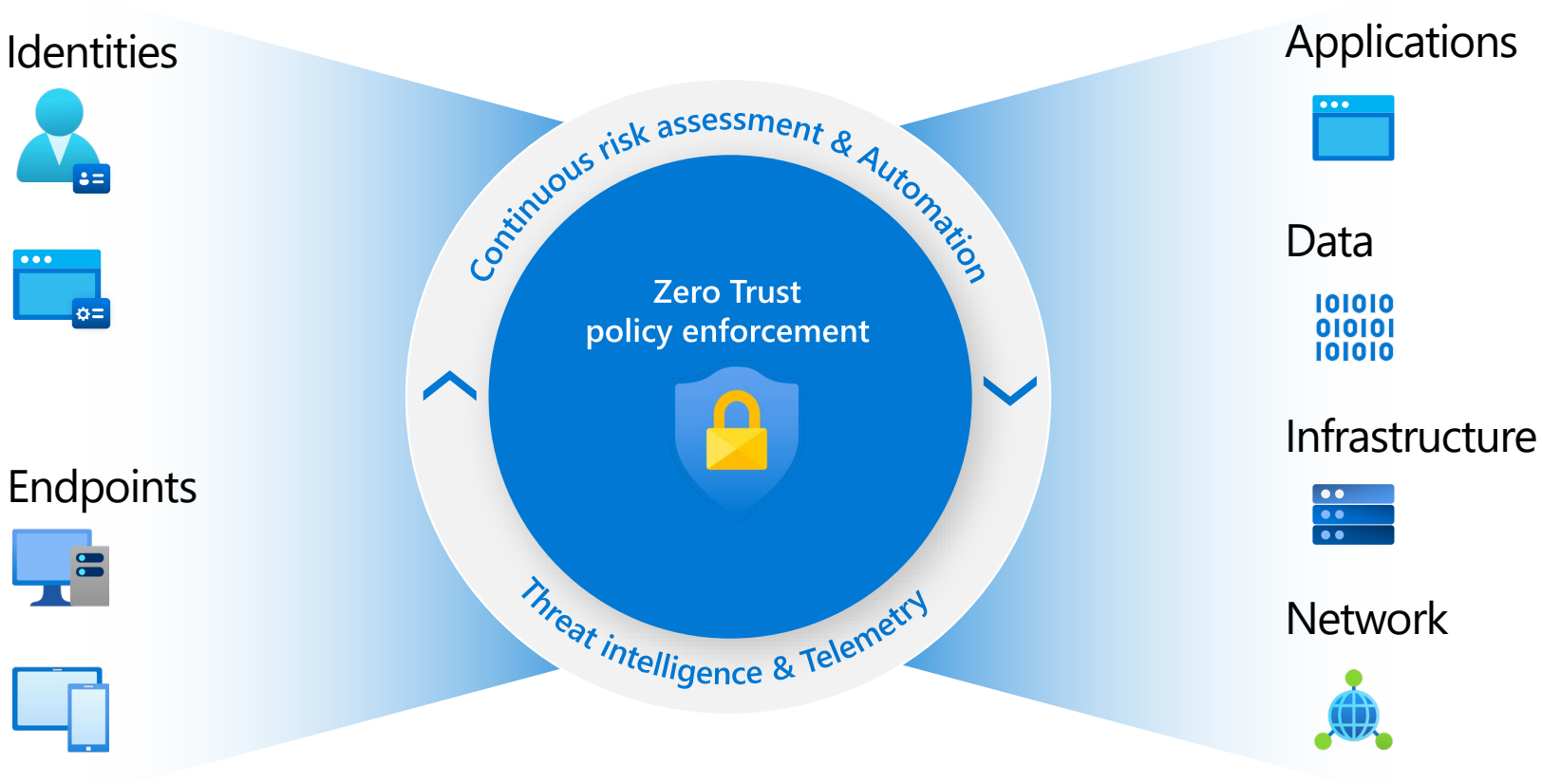


Zero Trust Components

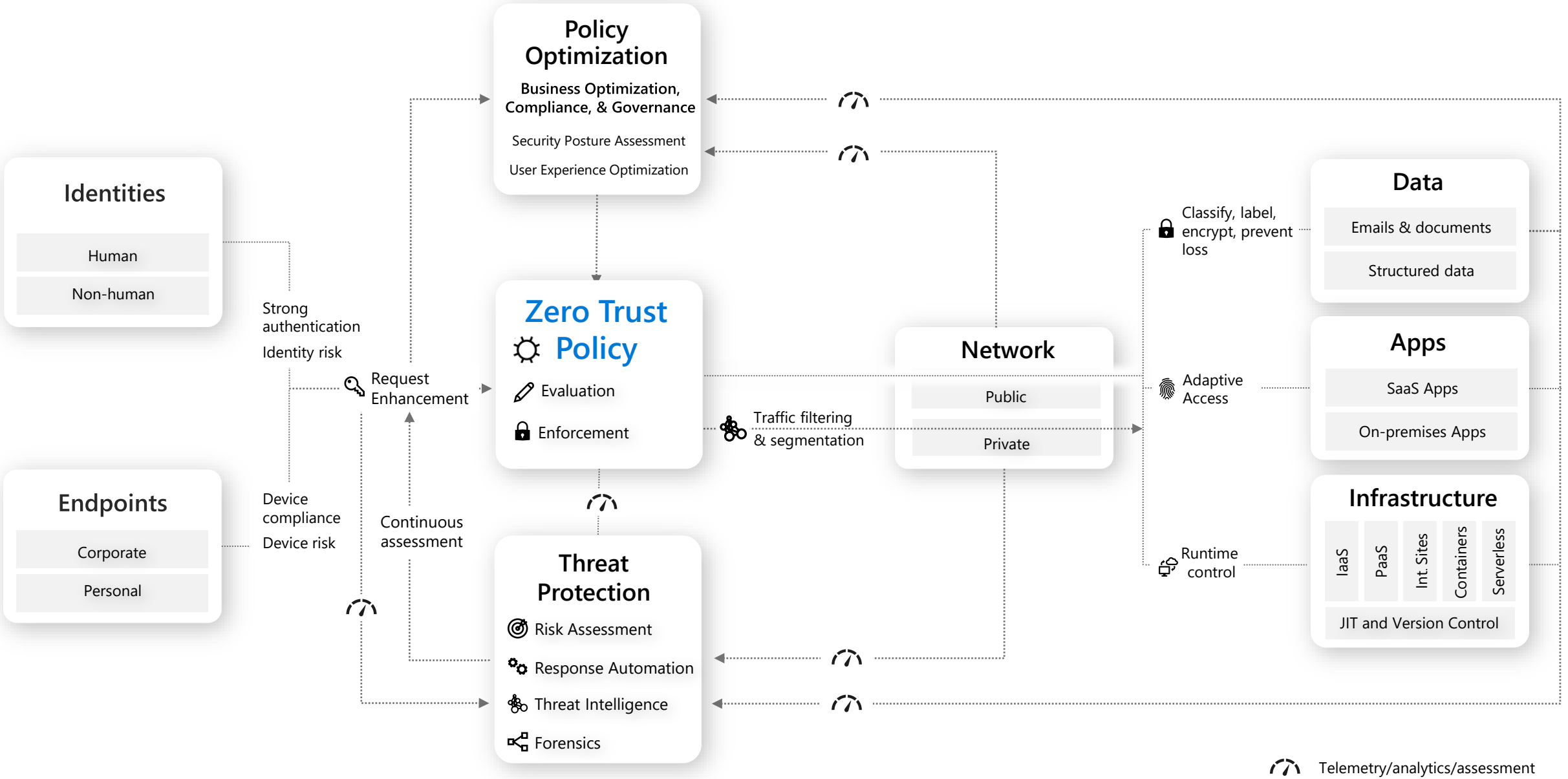
Enable flexible business workflows for the digitized world



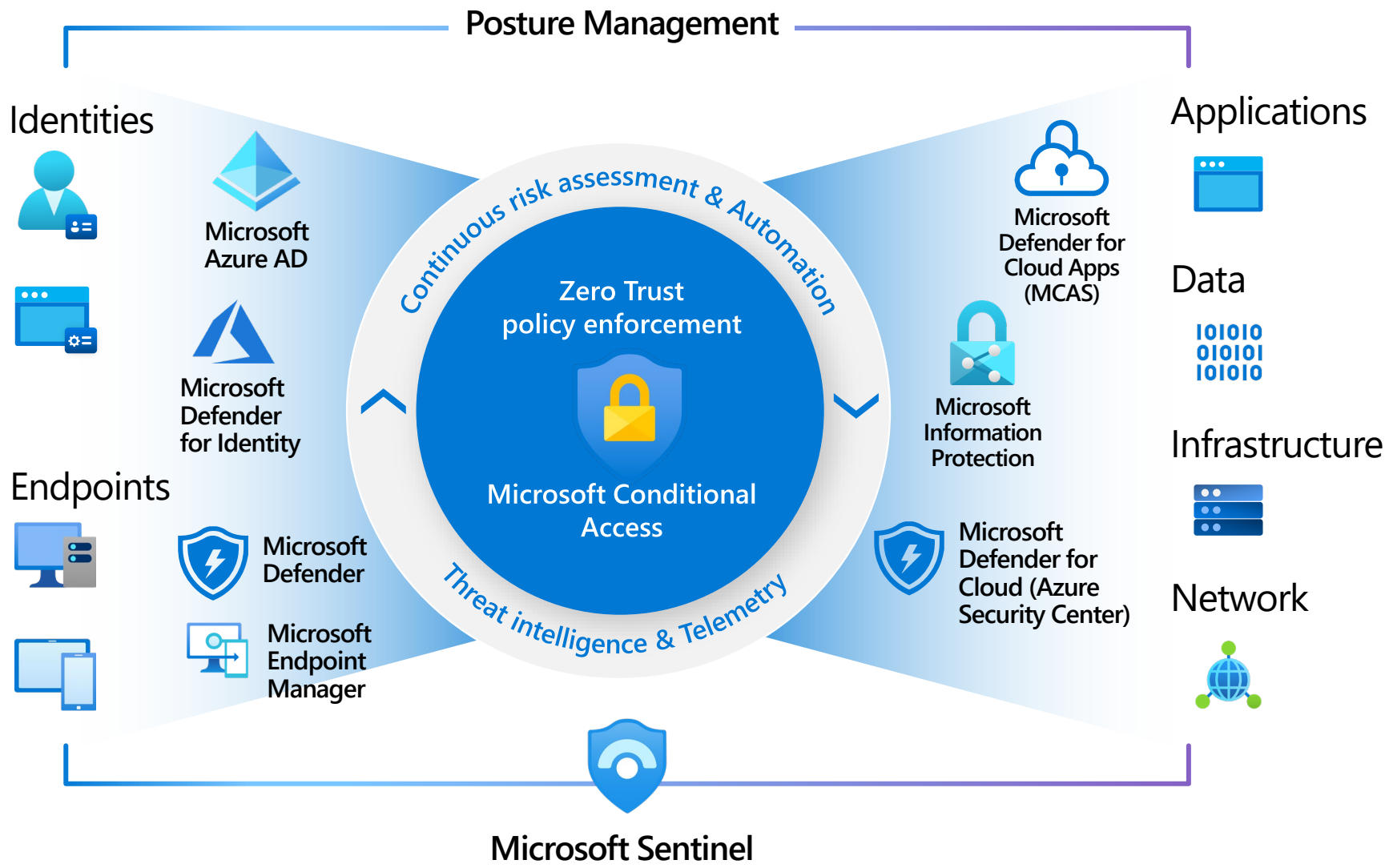
Zero Trust Approach from Microsoft



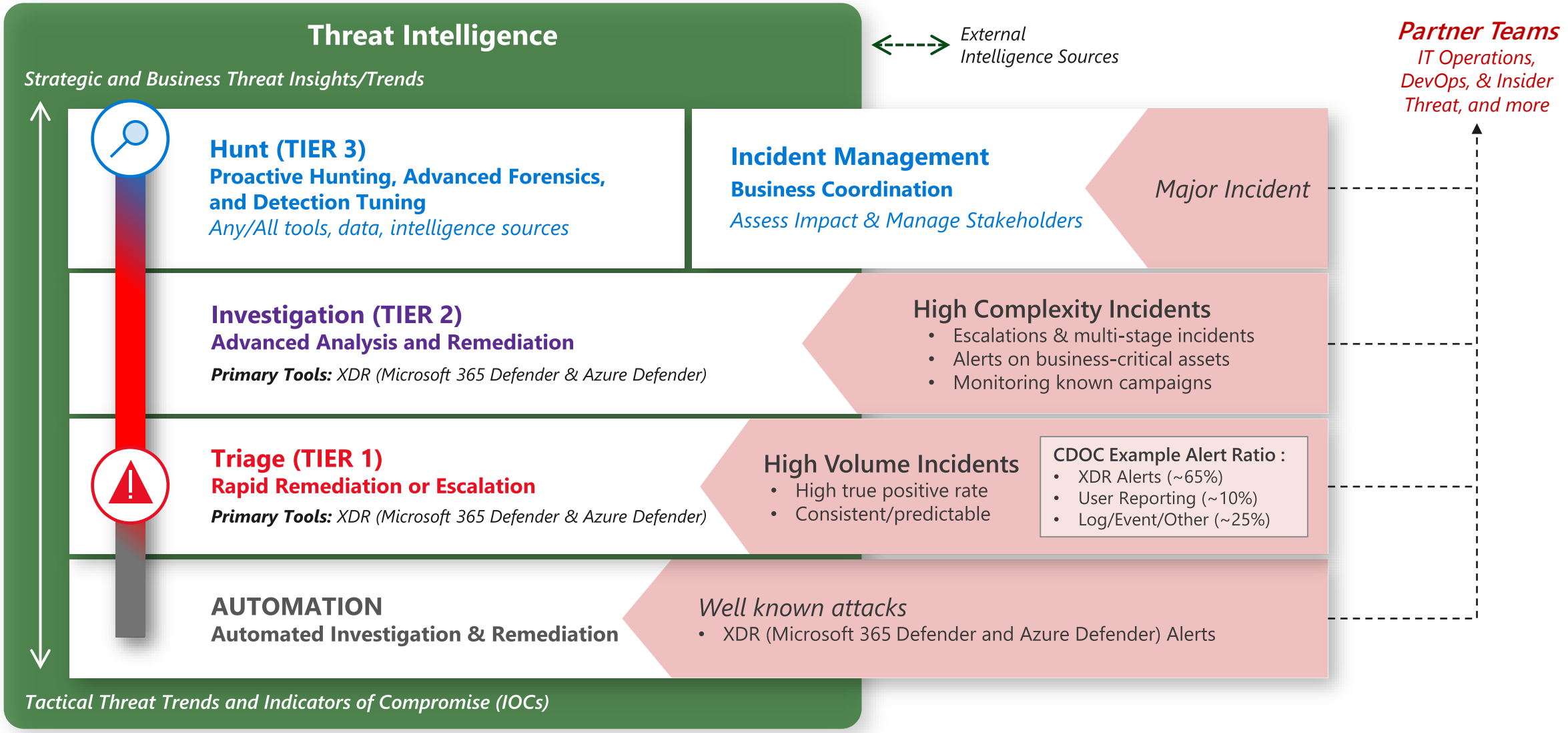
Zero Trust architecture



Microsoft Zero Trust Capabilities



Security Operations Model – Functions and Tools



Defend across attack chains

Insider and external threats

Microsoft

May 2021 – https://aka.ms/MCRA

Defender for Office 365

Phishing mail

Open attachment

Click a URL

Browse a website

Defender for IoT (& OT)

IoT Device Exploitation

Disrupt OT Environment

Defender for Endpoint

Exploitation and Installation

Command and Control

Azure Defender

Azure AD Identity Protection

Brute force account or use stolen account credentials

Defender for Identity

User account is compromised

Attacker attempts lateral movement

Attacker collects reconnaissance & configuration data

Domain compromised

Privileged account compromised

Microsoft Cloud App Security

Attacker accesses sensitive data

Exfiltration of data

EXTERNAL THREATS

INSIDER RISKS

Azure Sentinel

Leading indicators

History of violations

Distracted and careless

Disgruntled or disenchanted

Subject to stressors

Insider risk management

Insider has access to sensitive data

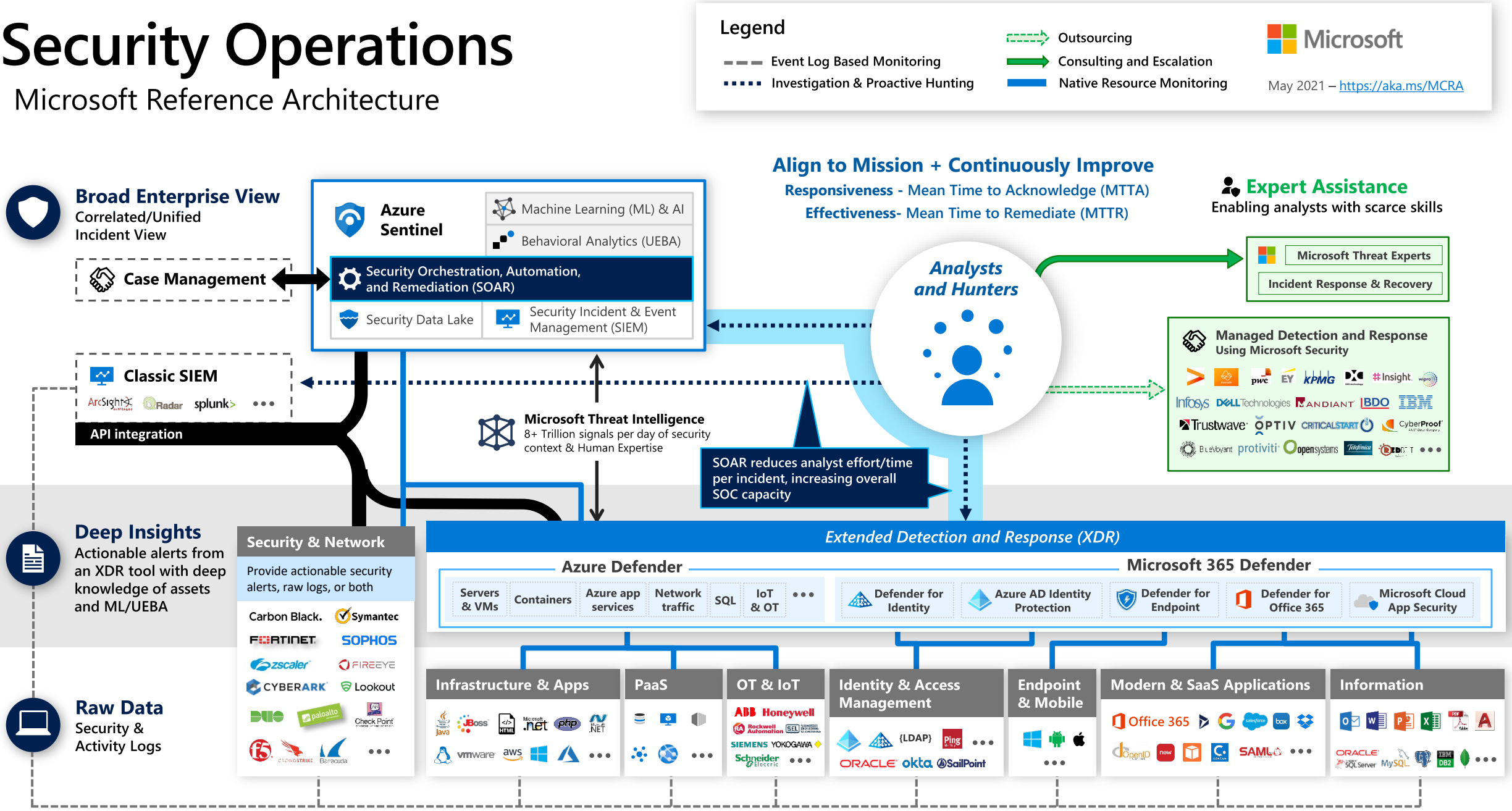
Anomalous activity detected

Data leakage

Potential sabotage

Security Operations

Microsoft Reference Architecture



Key Zero Trust Resources

to help you on your Zero Trust journey

Zero Trust Resources

aka.ms/zerotrust

Maturity Model

aka.ms/ztmodel

Business Plan

aka.ms/ZTbizplan

Deployment Guidance

aka.ms/ztguide

- Zero Trust: Security Through a Clearer Lens session (Recording | Slides)
- CISO Workshop Slides/Videos
- Microsoft's IT Learnings from (ongoing) Zero Trust journey

Resources

CAF Docs

aka.ms/cafsecure

CAF Intro video

aka.ms/cafsecure-videos

MCRA Docs

aka.ms/mcra

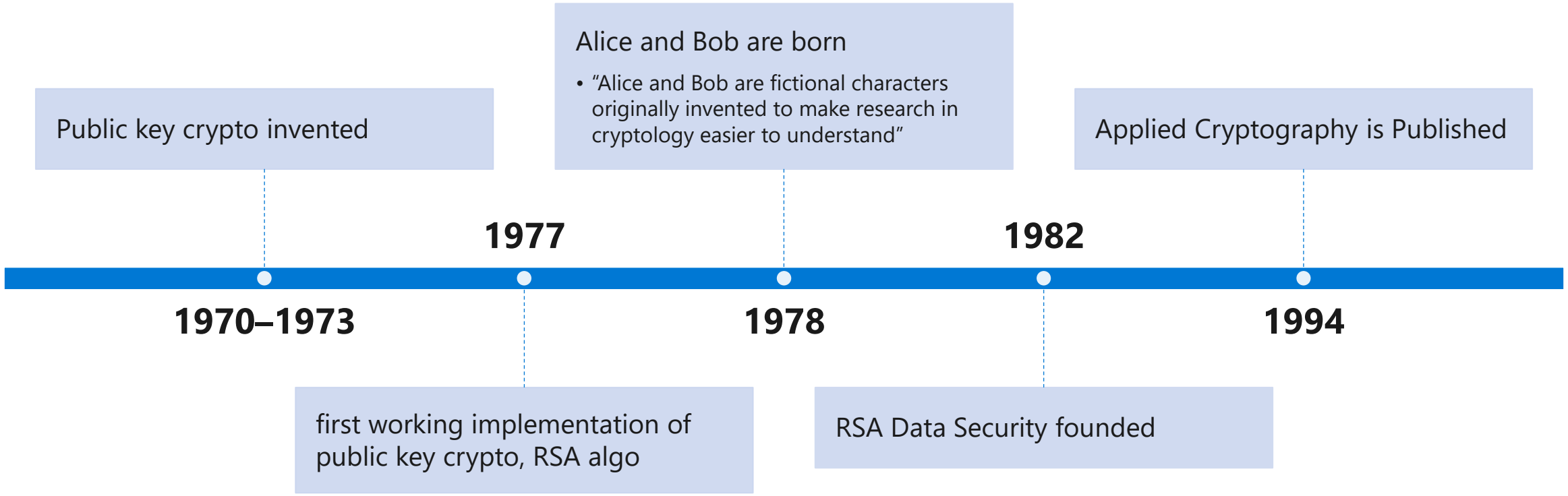
MCRA Intro video

aka.ms/mcra-videos

Build security into your processes

- Product Security Requirements
- Architectural Design Decisions
- Security checkpoints for all major features or improvements
- 3rd Party independent review

A brief history



http://cryptocouple.com

Some Terminology

- **Integrity**: ensures a message has not been modified in transit
- **Non-repudiation**: ensure a message originated from a known sender, can't be denied who sent, digital signatures
- **Authentication (AuthN)**: verify the identity of a user, process, or device
- **Authorization (AuthZ)**: The right or a permission that is granted to a system entity to access a system resource
- **Encryption**: The cryptographic transformation of data to produce ciphertext
- **Cipertext**: Data in its encrypted form
- **Hash**: The output of a hash function (e.g., hash(data) = digest). Also known as a message digest, digest, hash digest, or hash value.

https://csrc.nist.gov/glossary

Hashing vs Encryption

https://www.linkedin.com/learning/learning-cryptography-and-network-security-2

Uses of Hashing

 Integrity	File hashing Message hashing
 Non-repudiation	Digital signatures
 Authentication	Password comparison, storing a representation of a password, not reversible

Hashing overview

Strict rules underlie how an algorithm works

Input data of any length, the same length output is always produced

The same input will always produce the same output

The output can not be reversed back to the original data

Does not compress data, creates a unique representation of the data

Some algos, two different inputs can produce the same output. This is known as a “hash collision”

Sometimes referred to as a “message digest”

Common Hash Algorithms

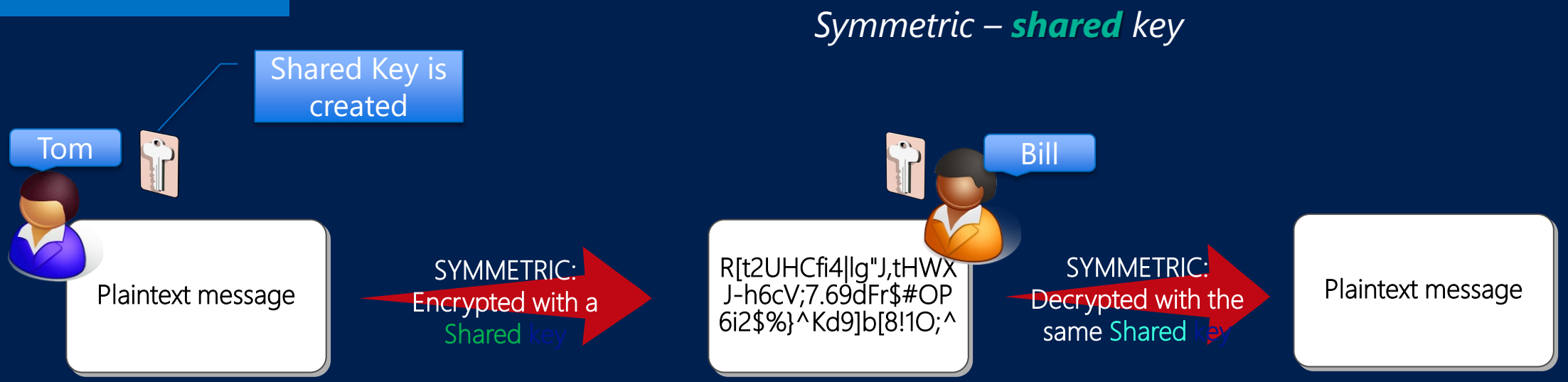
- CRC: Cyclic redundancy checks (unkeyed)
- MD5 (unkeyed)
  - md5(message) → string
- SHA-256 (unkeyed)
  - sha256(message) → string
- HMAC (keyed)
  - hmac(message, key) → string

https://en.wikipedia.org/wiki/List_of_hash_functions

Symmetric Cryptography

Symmetric Encryption

- With symmetric cryptography, the same key is used to encrypt and decrypt
- Fast, less computation required compared to assymetric
- Problem of Key Exchange
- **Hack all** vs hack one



Symmetric Algorithms – Examples

- **DES (Data Encryption Standard)**
  56 Bit Key length, US standard
- **3DES (“triple DES”)**
  Triple encryption with a 56 Bit DES key, results in only 112 Bit safety instead of the calculated 168 Bit
- **IDEA (International Data Encryption Algorithm)**
  128 Bit key length, developed in Switzerland (ETH, Zurich)
- **CAST**
  40-128 Bit key length. Developed by Northern Telecom (Nortel), USA, high performance
- **RC2, RC4, RC5 and RC6**
  Developed by Ron Rivest
- **AES, Blowfish, Twofish, CAST-5, Safer…**

AES

- Advanced Encryption Standard (AES) or Rijndael
- In the 1990's a "DES Cracker" machine was built that could recover a DES key in a few hours
- If a machine was built to recover a DES key in one second, it would take that system 149 trillion years to crack a 128-bit AES Key
- AES is the U.S. official standard for sensitive but unclassified data encryption, effective as of May 26, 2002
- Block symmetric encryption algorithm
- Key sizes of 128, 192, 256 bits (variable)

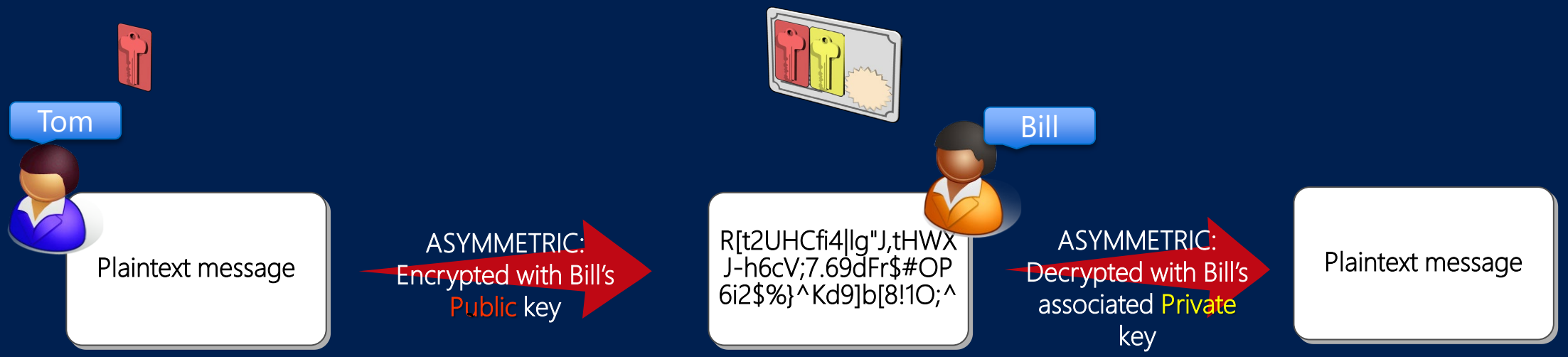
Asymmetric Cryptography - Overview

- If you asymmetrically encrypt something with a key, only the corresponding private key from the key pair can decrypt the information:
  - Public Key: Can and should be distributed
  - Private Key: Must remain secret
- Also called „Public Key Encryption“
- Personal Key Storage
  - Keyring (OpenPGP), Personal Security Environment (PSE) (S/MIME)
    - Collection of public and private keys

Asymmetric Encryption

Asymmetric – a key pair of mathematically-related private and public keys

Messages encrypted with Bill's public key can only be decrypted using Bill's private key

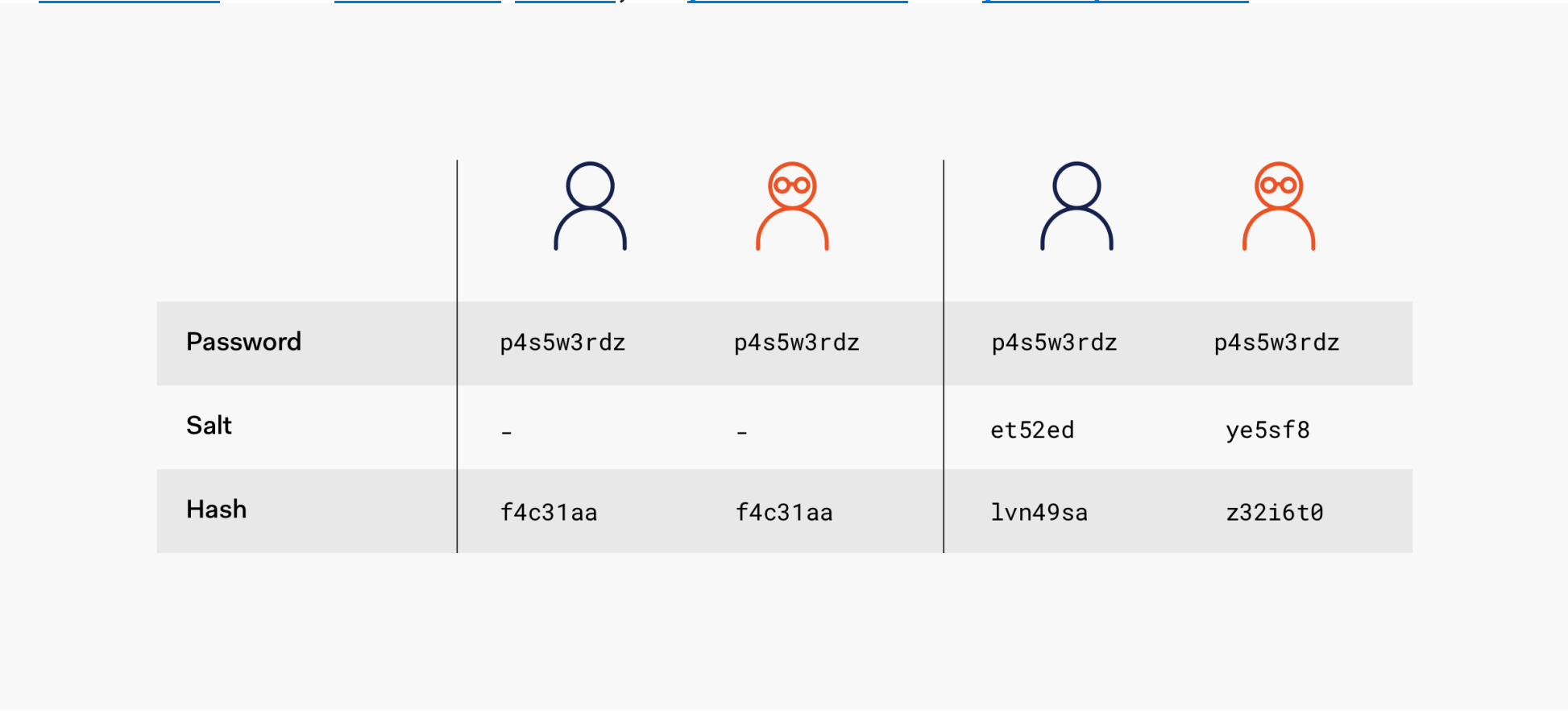


Asymmetric Algorithms – Diffie-Hellman

- First implementation of an asymmetric algorithm
- Allows users to exchange keys over a non-secure medium
- Does *not* provide data encryption or digital signatures
- Security based on calculating discrete logarithms in a finite field
- Vulnerable to man-in-the-middle attacks – lack of authentication
- Can be counter measured with digital signatures

Salt

- a **salt** is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase



Password	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

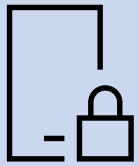
https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

Nonce

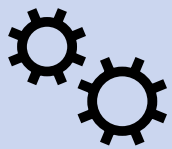
- a **nonce** (*number once*) is an arbitrary number that can be used just once in a cryptographic communication.[1] It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.

https://en.wikipedia.org/wiki/Cryptographic_nonce

OWASP



Open Web Application Security Project



A nonprofit foundation that works to improve the security of software

Provides

- Tools and Resources
- Community and Networking
- Education & Training

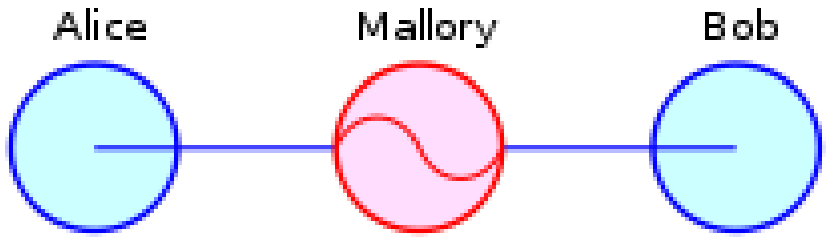
Juice Shop (OWASP) – Learn to hack

- Covers the top 10 Web vulnerabilities
- “Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!”

https://owasp.org/www-project-juice-shop/
https://owasp.org/www-project-top-ten

Man in the Middle Attack

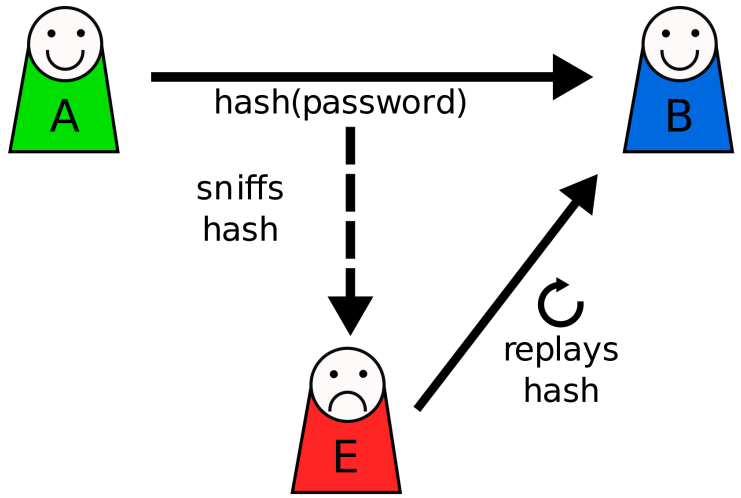
- Alice trusts Bob
- Alice trusts Mallory with a secure document to send to Bob
- Mallory modifies the document and sends it to Bob
- Mallory has changed the document that Bob believes is original



https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Replay Attack

- Alice trusts Bob
- Eve improperly learns off Alice's password hash
- Eve replays the hash from Alice
- Eve impersonates Alice



https://en.wikipedia.org/wiki/Replay_attack

Some mitigations for these attacks

- PKI
- OpenID Connect
- JWS – JSON Web Signatures
- Nonces

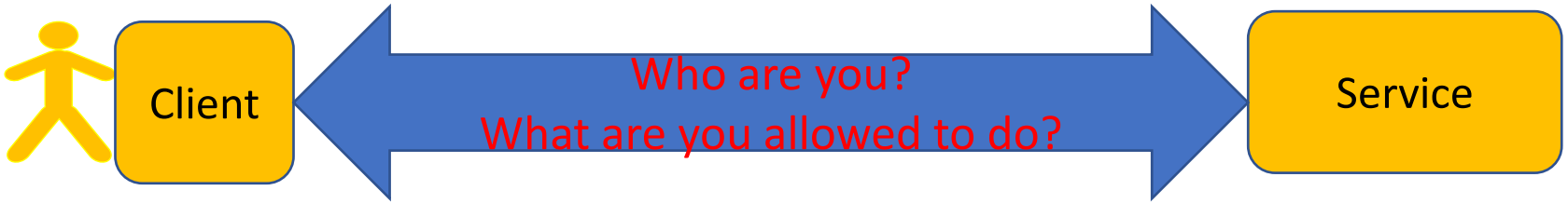
Microsoft

Modern authentication and authorization

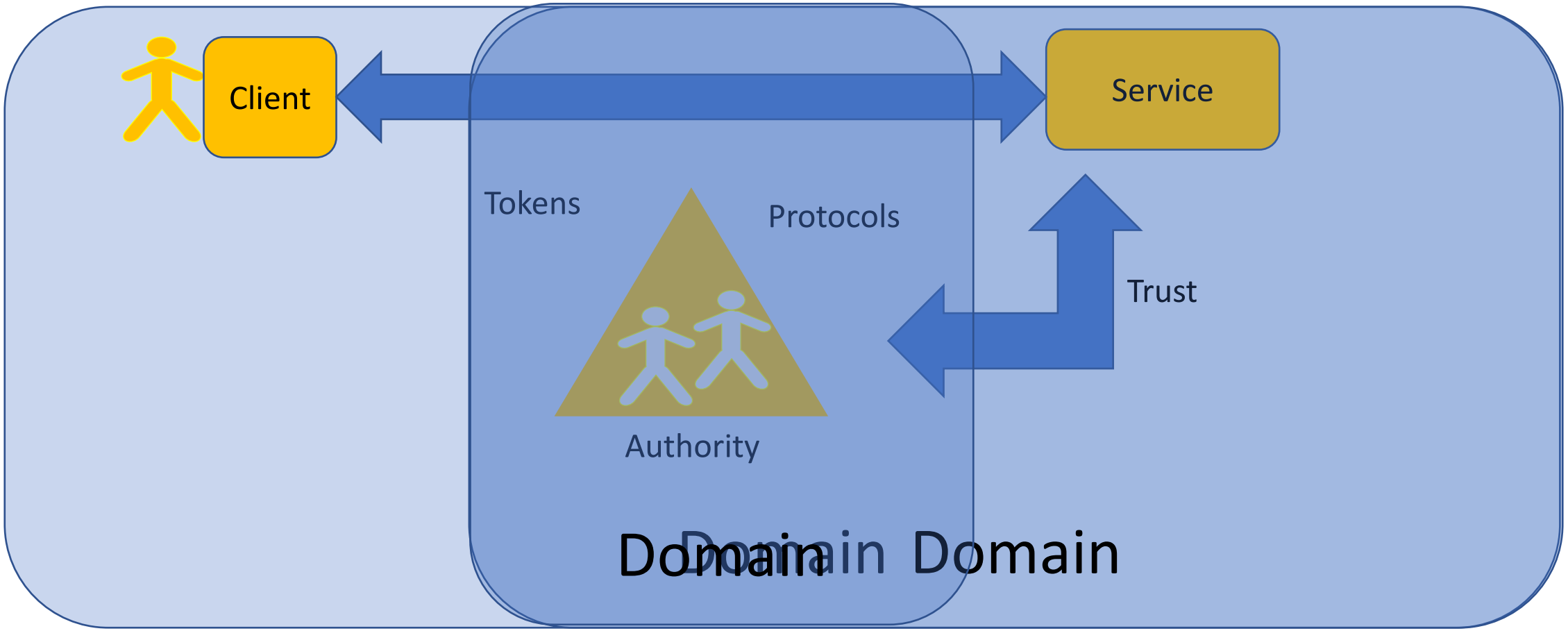
Why do we need a new way of authenticating users and managing access to resources?

Microsoft Services

Basic Issue



Canonical Solution



Microsoft

Modern authentication and authorization

What are the standard protocols supporting these requirements?

Microsoft Services

Microsoft

OAuth 2.0 and OpenID Connect

OAuth 2.0 Introduction

Microsoft Services

Introduction to OAuth 2.0

- Example #1: You want Snapfish to print your holidays photos stored on OneDrive
- Example #2: You play an online game and want to share achievements on Facebook
- Example #3: You want Mint to summarize your financial data from various banks

Things to consider:

- Do you trust these applications enough to give your password?
- Is the application storing your credentials safely?
- How do you know the application will not misuse your credentials
- How do you know the application will not do something you didn't authorize

Introduction to OAuth 2.0

- OAuth 2.0 is an open protocol that allows secure **authorization** in a simple and standard method from web, mobile, and desktop applications.

- OAuth 2.0 is not an authentication protocol.

- OAuth 2.0 is based on the presence of a trust setup between the service that's providing a Resource and the Authorization server. The Resource provider will be registered with the Authorization server.

OAuth 2.0 Concepts and Terminology

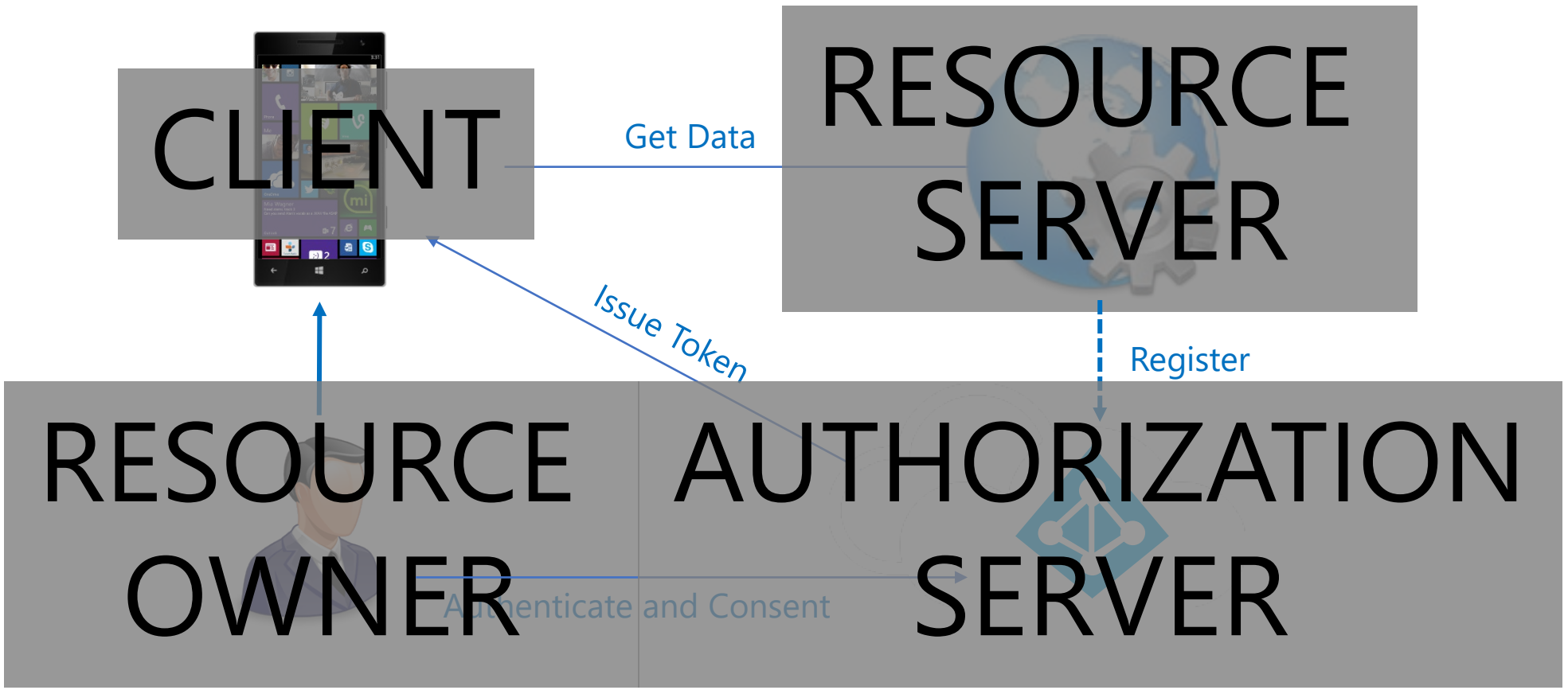
- Client
  - Application that needs to use the resource
  - Various types –
    - browser-Web-App, Native, Daemons, etc.
  - Often end-user facing
  - E.g. Snapfish "Print shop" application

- Resource Owner
  - Owner of the requested resource
  - Typically the user of the application
  - E.g. "Owner of the OneDrive account/photos"

- Resource Server
  - Hosts the resource
  - Typically an API provider
    - E.g., Microsoft Graph API
  - Trusts tokens from an Authorization Server
  - E.g. OneDrive "Photo library"

- Authorization Server
  - Issues access tokens to clients
  - Authenticates resource owners
  - Gets access consent from the resource owner
  - Could be "Photo library provider"

OAuth 2.0 Concepts and Terminology



OAuth 2.0 Concepts and Terminology

- Client/Service Registration
  - Tells Auth Server it is OK to issue tokens for this client to this resource server
  - May include limits on what the client can do
  - Client and service identities in Authorization Server namespace
- Endpoints
  - 'Well-known' locations at Authorization Server and in client
    - Authorization Endpoint
    - Token Endpoint
    - Client Redirect Endpoint
- Tokens
  - JSON Web Tokens (JWT)
  - Access Tokens v. Refresh Tokens
  - "Bearer" tokens most common
  - Scope
- Flows
  - Standard patterns for obtaining tokens
  - Describe how to interact w. above endpoints
  - Covers various devices + services scenarios

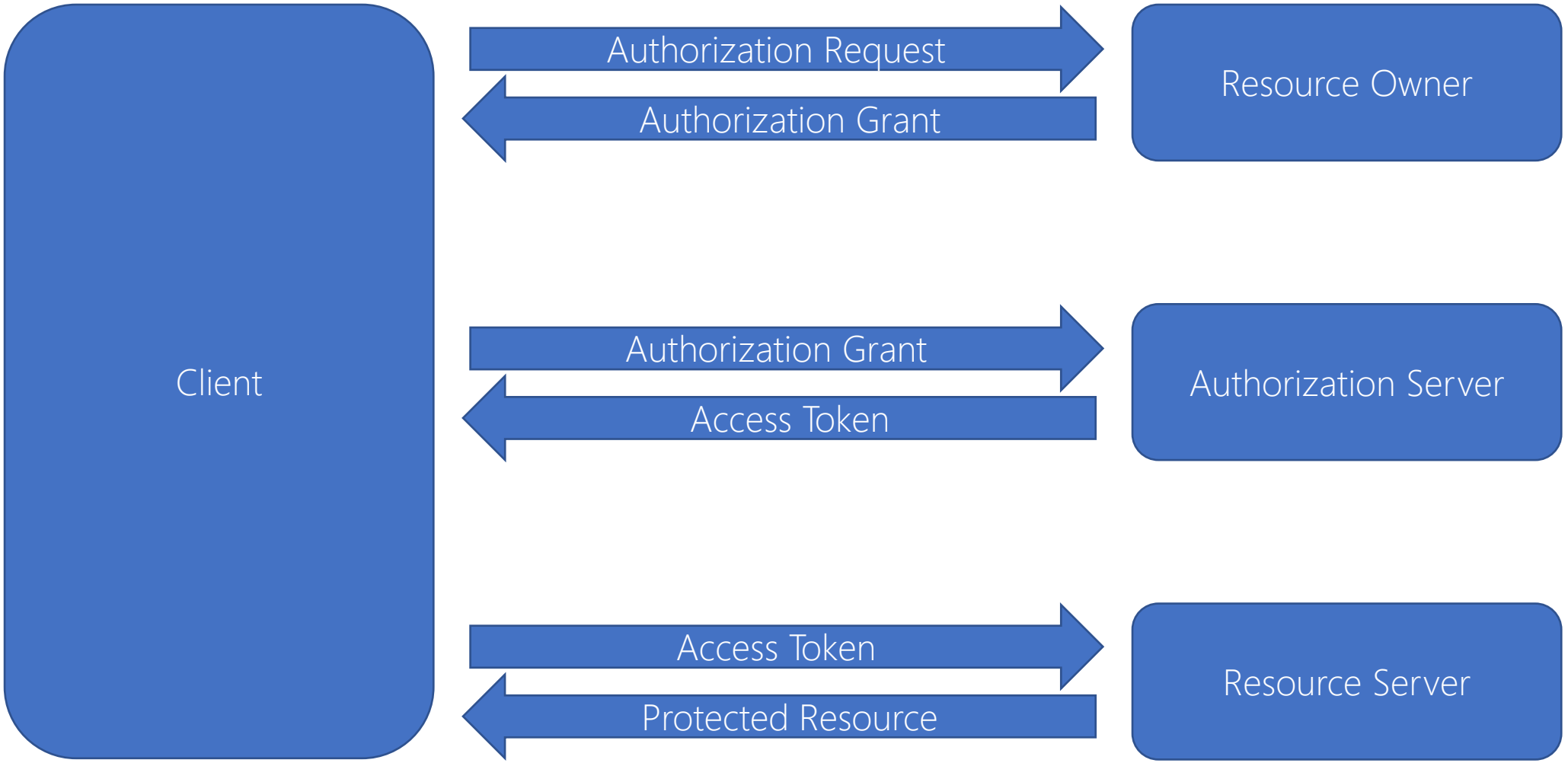
Microsoft

OAuth 2.0 and OpenID Connect

OAuth 2.0 Grants & Flows

Microsoft Services

Protocol Flow



Why different flows?

- Client security – confidential vs public
- Can user enter consent in real time?
- Is HTTP redirection possible?
- Potential for token exposure

OAuth 2.0 Flows

Flow name	Typical scenario
Authorization code grant	Client: fully browser capable UI (Web app or native app with webview) accessing REST resources.
Implicit flow	Client: restricted browser capable UI (JS SPA calling Web API. Cross-domain restriction prevents browser redirection). Potential for token theft. No refresh token.
Client credential	Client: service which also owns the resources. Usually a non-UI daemon. Client manages own credentials (e.g. X509 cert).
Resource owner pwd	Client: native UI apps unable to support browser controls. Credentials supplied by owner to client.

Microsoft

OAuth 2.0 and OpenID Connect

OpenID Connect

Microsoft Services

OpenID Connect

- OAuth 2.0 does not tell the client who the user is
- OIDC: add user identity request to OAuth2 request
- Becomes pure authentication protocol if access token is NOT requested
- Replaces as WS-Fed as authentication protocol

```
GET https://login.windows.net/meraridom.com/oauth2/authorize?
response_type=id_token%20token&client_id=c5f7b3…
```

- Optional parameters: **`prompt=login`** and **`amr_values=mfa`**

OpenID Connect

OAuth 2.0 is purely for authorization, not authentication

- Person granting access might not be the real user (resource owner)
- Does not have a notion of an "identity“
- Access Token contains scopes, which define the scope for the token, often the rights granted.

OpenID Connect builds on OAuth 2.0 and adds authentication information

- OIDC extends the OAuth Spec and adds claims.
- OIDC ID Token: JWT with at least a “sub” claim to identify the end user (“subject”)
- UserInfo Endpoint: returns more claims about the end user (JSON/JWT)

Microsoft

Developing Applications

Authentication Requirements for Applications

Microsoft Services

Scenarios and code samples

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-code-samples

In this article:

- Web Browser to Web Application
- Single-Page Application (SPA)
- Native Application to Web API
- Server or Daemon Application to Web API
- Calling Azure AD Graph API
- Authorization
- Legacy Walkthroughs

Microsoft

Modern authentication and authorization

How does MS support these requirements and how to develop with it?

Microsoft Services

Authentication Options

… to Cloud Applications:

- Standalone ADFS[1]
- Standalone AAD tenant
- Azure AD tenant with password hash sync[2]
- Azure AD tenant with federation (e.g. ADFS)[1]
- Azure AD tenant with Pass-Though Authentication[2]

… to On-Premises Applications:

- As above plus Azure AD or Application Proxy

1. SSO possible with ADFS

2. SSO possible with Azure AD Seamless Single Sign-On

Azure AD Modes

- B2E – Business to Employee
  - Membership controlled by one organization
  - Usually one (few) domains
  - Often sync'ed with on-premises store (e.g. Active Directory)
- B2B – Business to Business
  - Possibly existing B2E
  - Supports membership from other orgs
  - Uses federation with the other tenants
  - Enables access to resources managed by this tenant
- B2C – Business to Consumer
  - Separate tenant from B2E
  - Customizable attribute structure
  - Customizable registration, login, logout, pwd reset UI
  - Support for resident and social ids (FB, gmail, MSA)

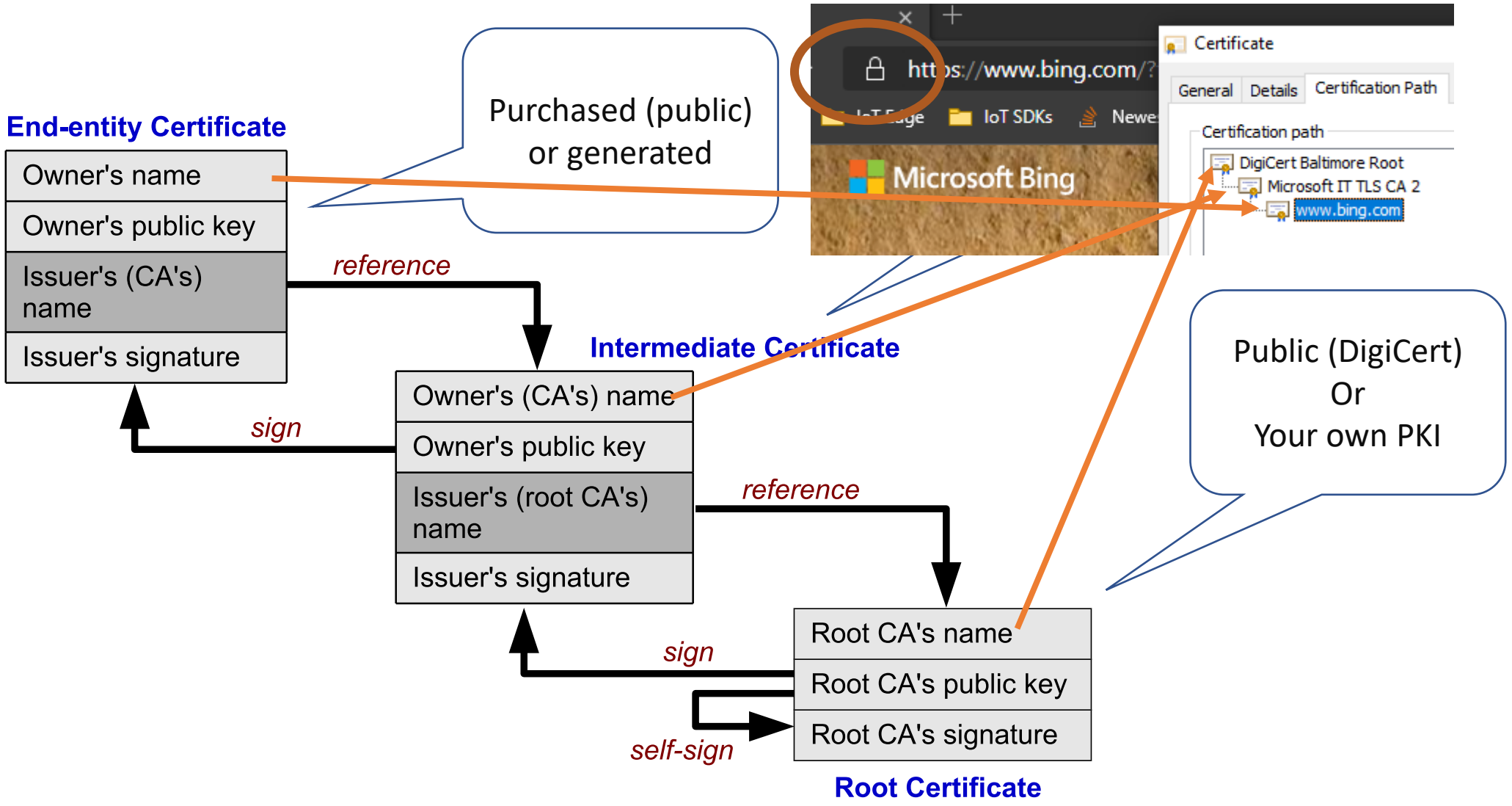
Demystifying IoT Edge Certificates

Steve Busby
Principal Technical Specialist
IoT & Mixed Reality Sales

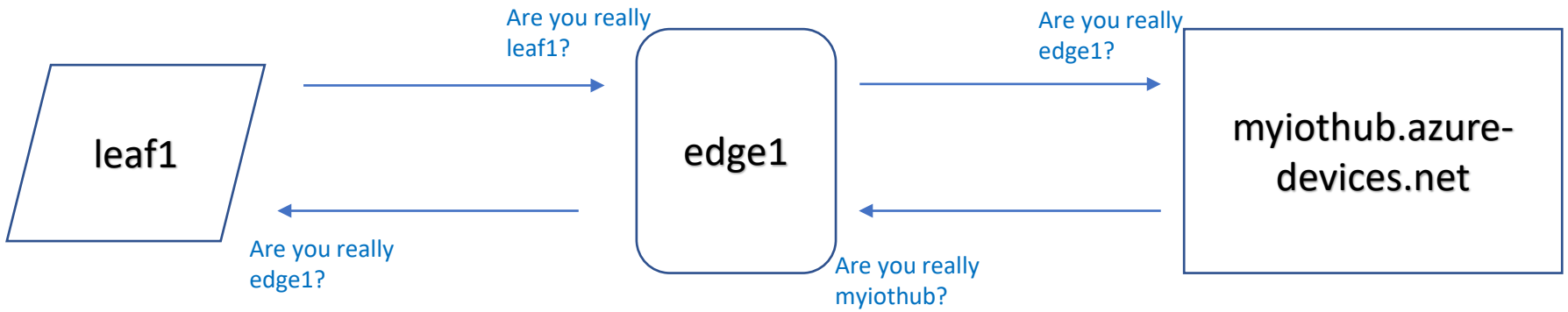
A few notes

- The presentation is a gross oversimplification of PKI and the TLS handshake
  - Only meant to illustrate the certs involved
  - For in-depth information about those things, search “pki explained in simple terms” on YouTube and enjoy!
- Not addressing how to securely store and initially transfer the certs
- Will show tie-backs to our ‘dev/test’ scripts
  - Please use “real” production certs
  - But the concepts are the same

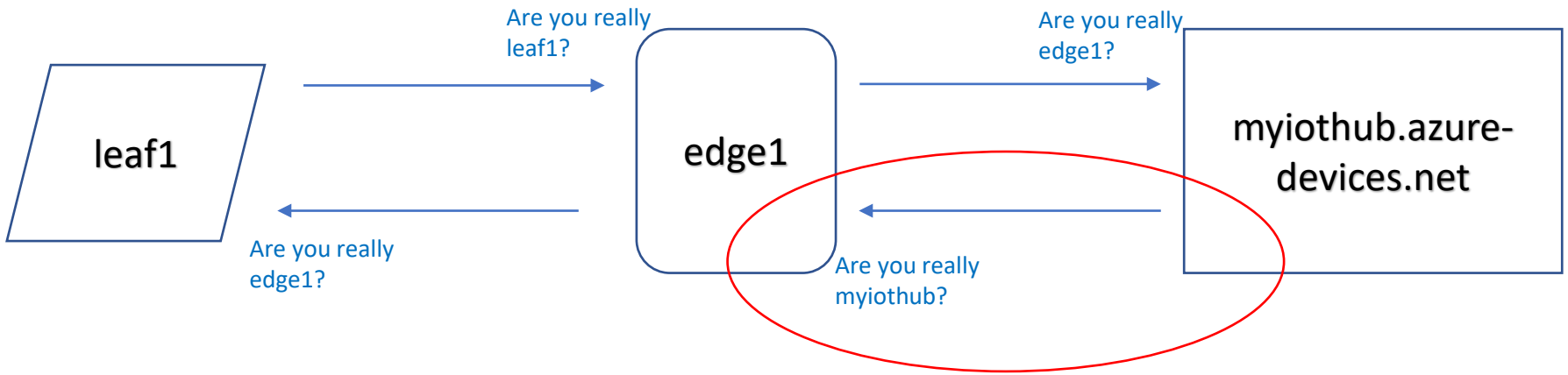
Certificates basics



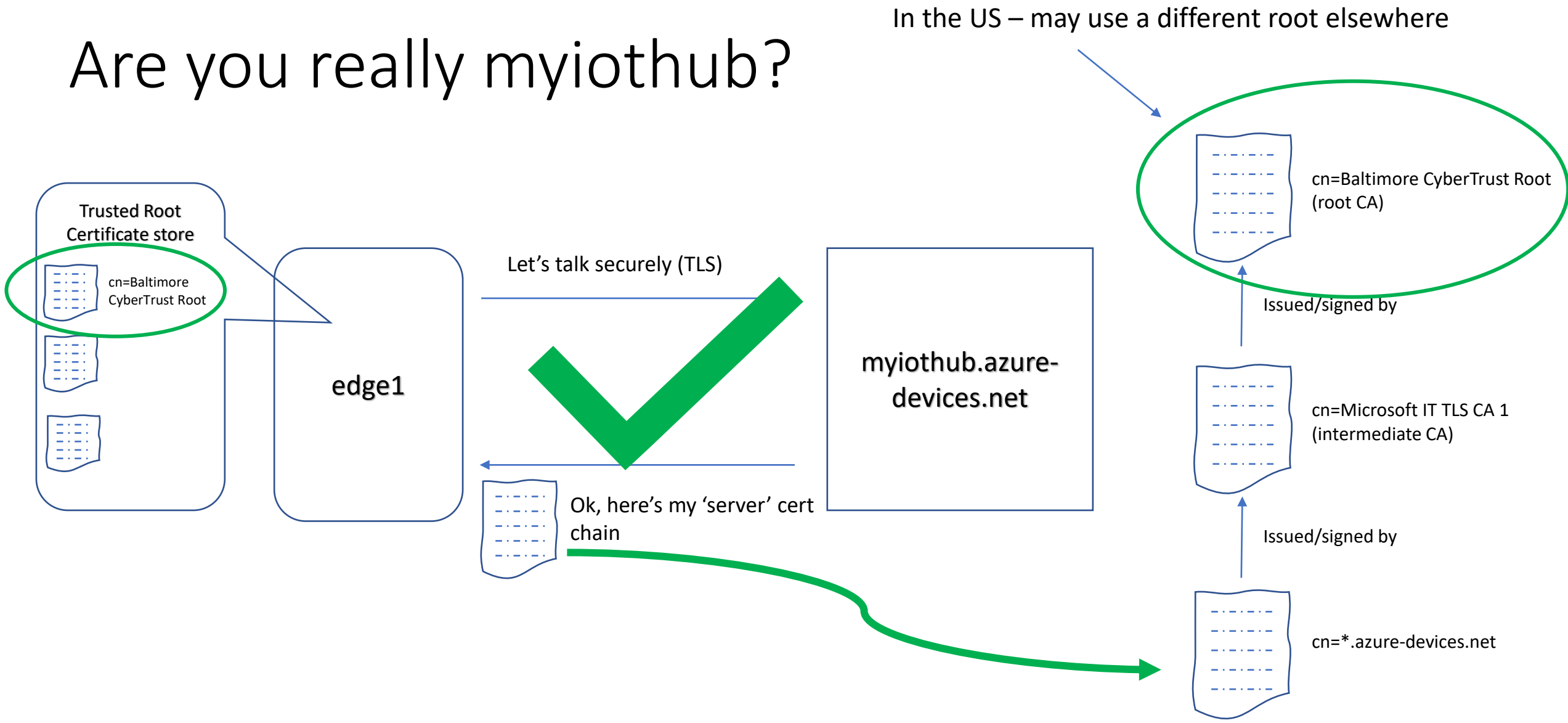
Four IoT Edge cert related scenarios



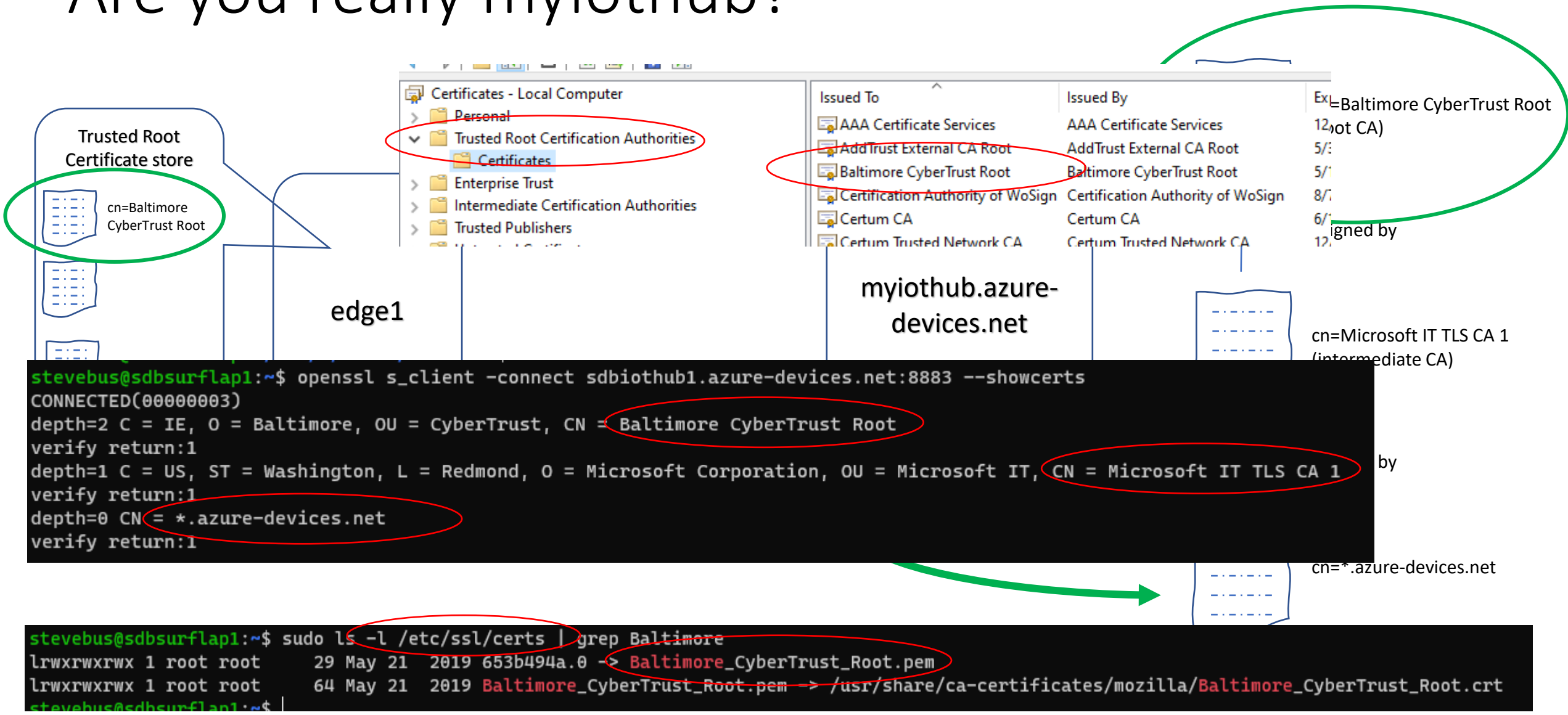
Four IoT Edge cert related scenarios



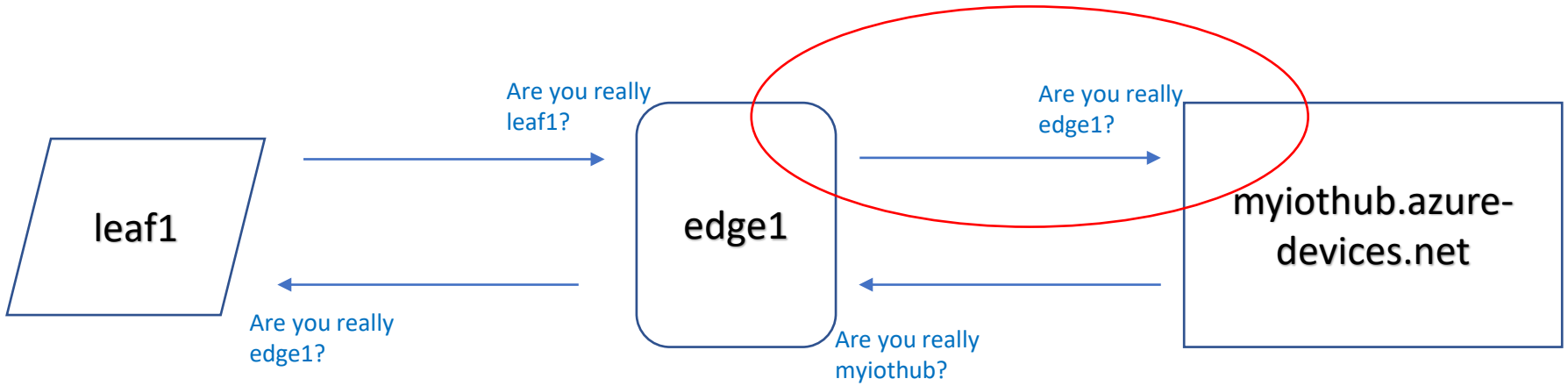
Are you really myiothub?



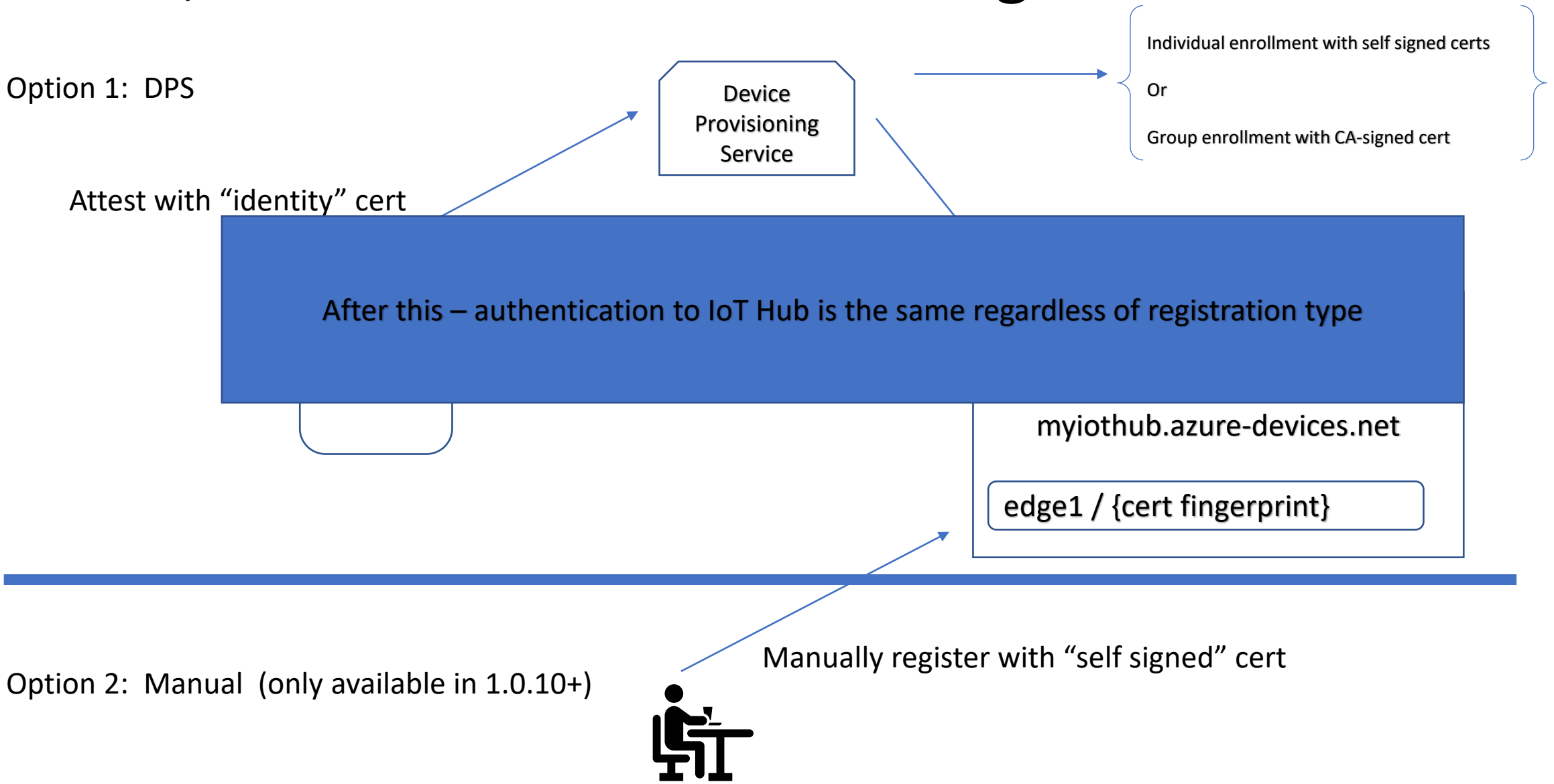
Are you really myiothub?



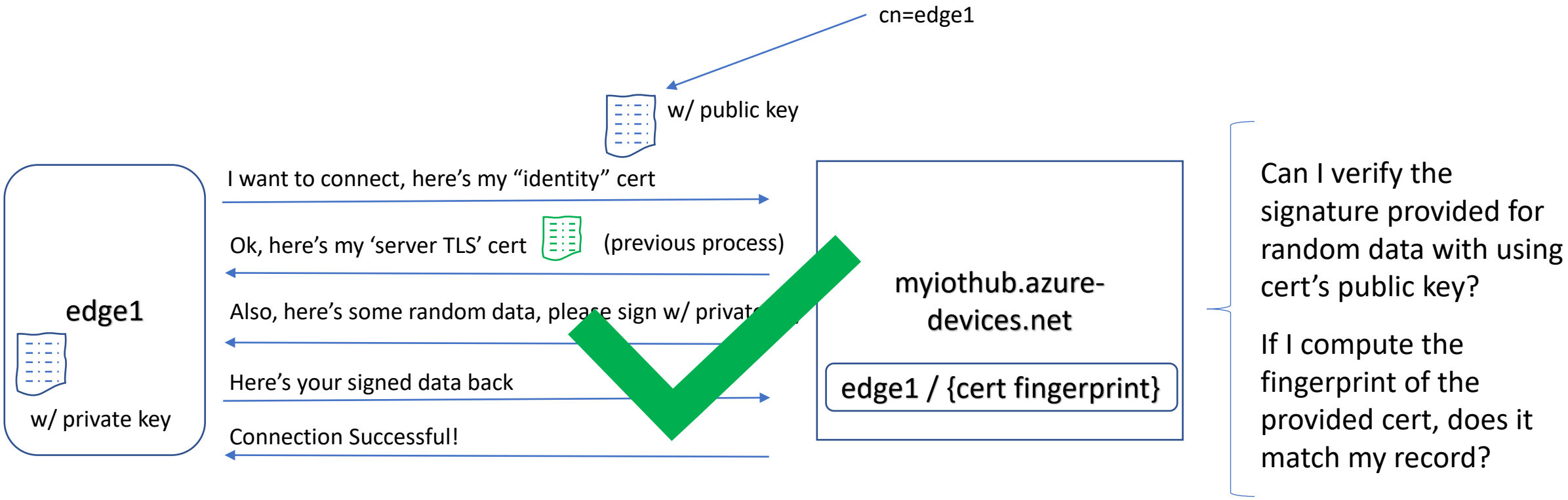
Four IoT Edge cert related scenarios



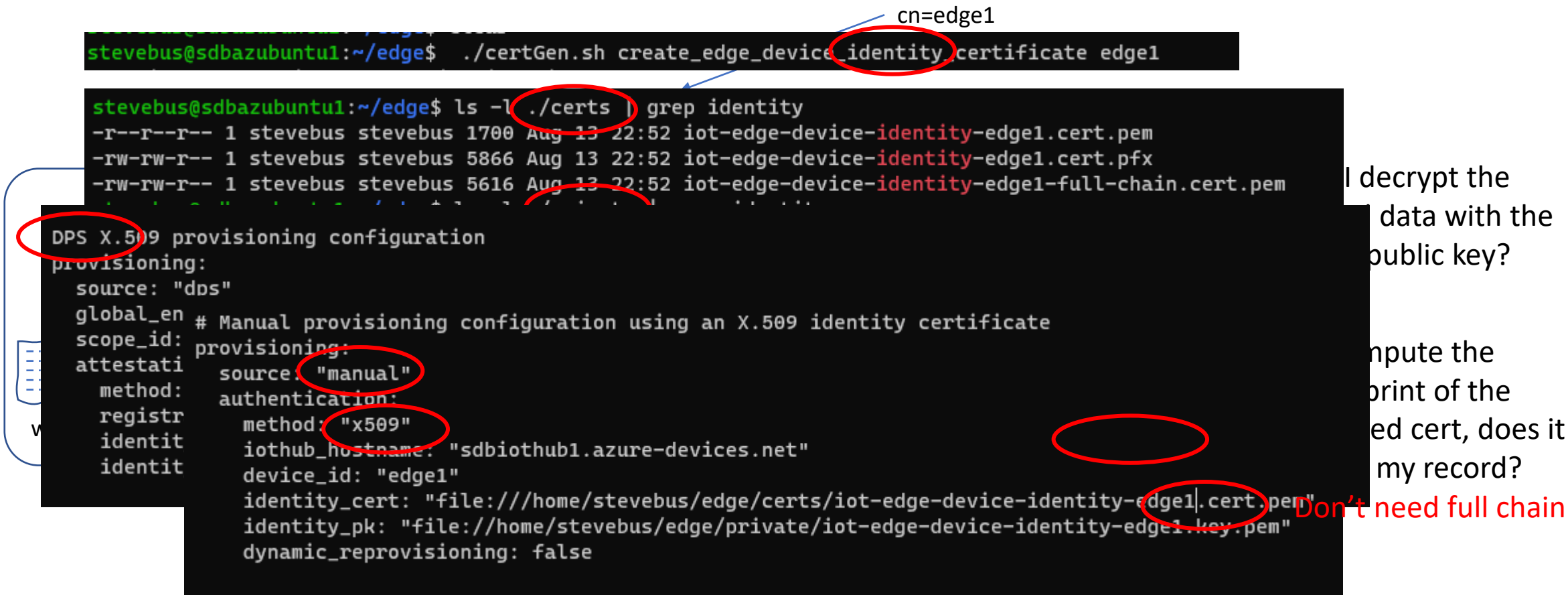
First, we need to talk about registration



Are you really edge1?



Are you really edge1?

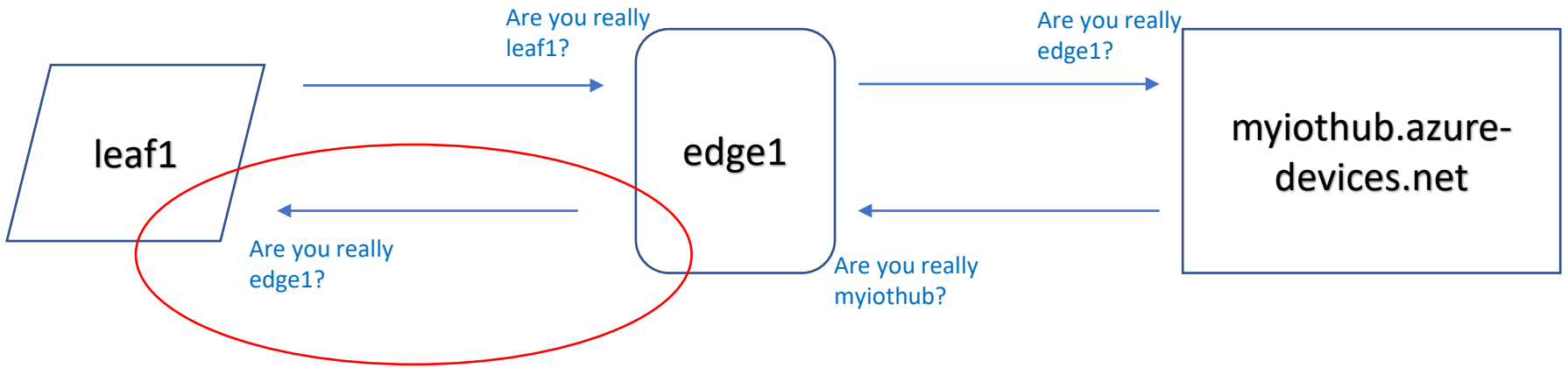


I decrypt the data with the public key?

mpute the print of the ed cert, does it my record?

Don't need full chain

Four IoT Edge cert related scenarios

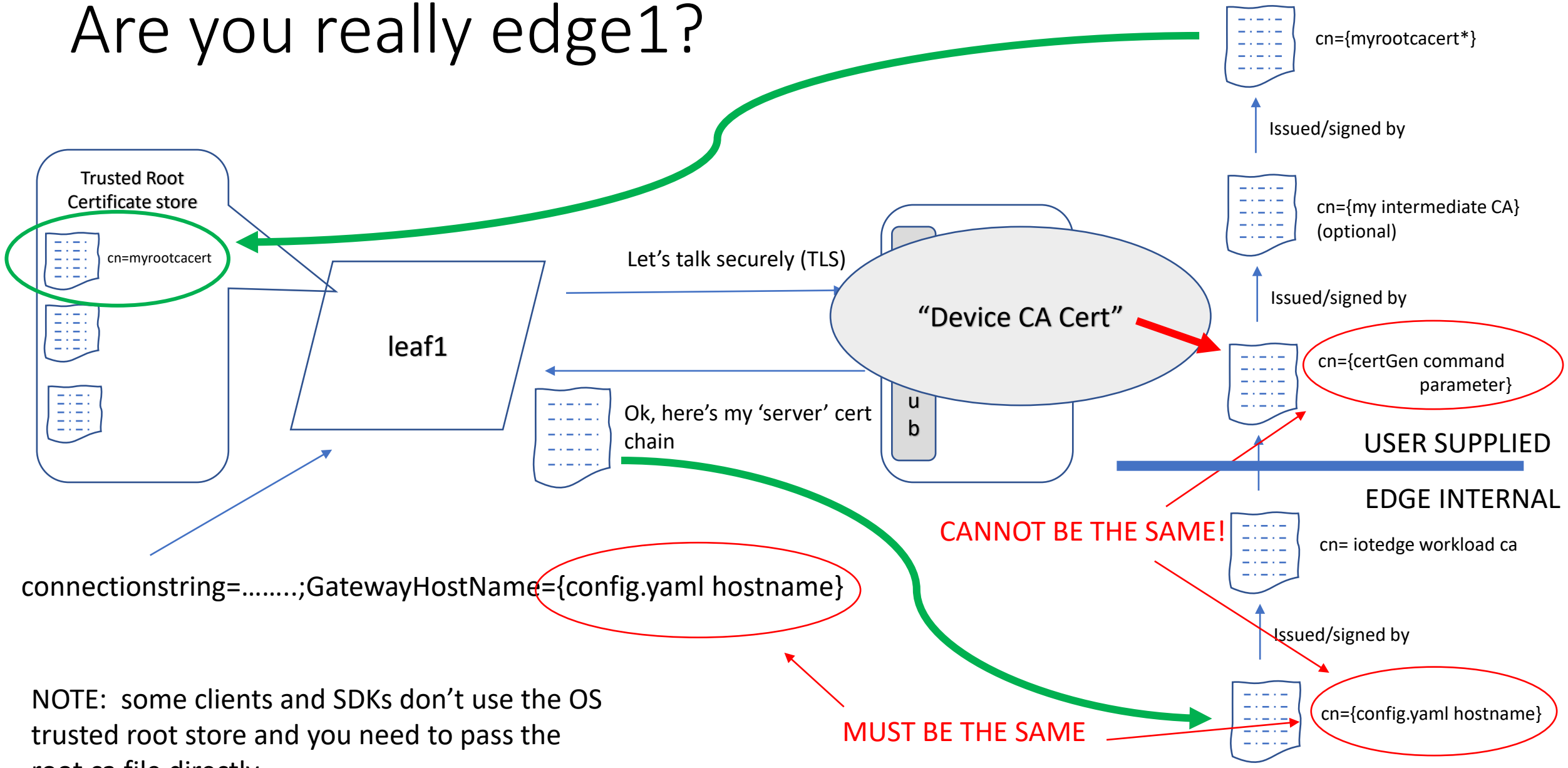


The vast majority of cert “confusion” is in this part of IoT Edge

https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-certs
(written by my very favorite author ☺)

Are you really edge1?

*note: myrootcacert can be a self-signed root cert or real ca



NOTE: some clients and SDKs don't use the OS trusted root store and you need to pass the root ca file directly

Are you ready edge?

*note: myrootcacert can be a self-signed root cert or real ca

```
stevebus@sdbazubuntu1:~/edge$ ./certGen.sh create_root_and_intermediate
```

```
stevebus@sdbazubuntu1:~/edge$ ls -l ./certs | grep root
-r--r--r-- 1 stevebus stevebus 1956 Jul 28 18:19 azure-iot-test-only.root.ca.cert.pem
```

cn={myrootcacert*}

Issued/signed by

cn={my intermediate CA}

Issued/signed by

cn=sdbazubuntu1.ca

USER SUPPLIED

EDGE INTERNAL

cn= iotedge workload ca

Issued/signed by

cn=sdbazubuntu1.eastus.cloudapp.azure.com

Trusted Root Certificate store

cn=myrootcacert

Let's talk securely (TLS)

```
stevebus@sdbazubuntu1:~/edge$ ./certGen.sh create_edge_device_ca_certificate "sdbazubuntu1"
```

```
certificates:
  device_ca_cert: "/home/stevebus/edge/certs/iot-edge-device-ca-sdbazubuntu1-full-chain.cert.pem"
  device_ca_pk: "/home/stevebus/edge/private/iot-edge-device-ca-sdbazubuntu1.key.pem"
  trusted_ca_certs: "/home/stevebus/edge/certs/azure-iot-test-only.root.ca.cert.pem"
```

connectionstring=……..;GatewayHostName={config.yaml hostname}

```
hostname: "sdbazubuntu1.eastus.cloudapp.azure.com"
```

NOTE: some clients and SDKs don't use the trusted root store and you need to pass the root ca file directly

Are you really edge1?

*note: myrootcacert can be a self-signed root cert or real ca

```
stevebus@sdbsurflap1:~$ openssl s_client -connect sdbazubuntu1.eastus.cloudapp.azure.com:8883 --CAfile ./azure-iot-test-only.root.ca.cert.pem
```

```
stevebus@sdbsurflap1:~$ openssl s_client -connect sdbazubuntu1.eastus.cloudapp.azure.com:8883 --CAfile ./azure-iot-test-only.root.ca.cert.pem
depth=4 CN = Azure_IoT_Hub_CA_Cert_Test_Only
verify return:1
depth=3 CN = Azure_IoT_Hub_Intermediate_Cert_Test_Only
verify return:1
depth=2 CN = sdbazubuntu1.ca
verify return:1
depth=1 CN = iotedged workload ca
verify return:1
depth=0 CN = sdbazubuntu1.eastus.cloudapp.azure.com
verify return:1
CONNECTED(00000003)
---
Certificate chain
 0 s:/CN=sdbazubuntu1.eastus.cloudapp.azure.com
   i:/CN=iotedged workload ca
 1 s:/CN=iotedged workload ca
   i:/CN=sdbazubuntu1.ca
 2 s:/CN=sdbazubuntu1.ca
   i:/CN=Azure_IoT_Hub_Intermediate_Cert_Test_Only
 3 s:/CN=Azure_IoT_Hub_Intermediate_Cert_Test_Only
   i:/CN=Azure_IoT_Hub_CA_Cert_Test_Only
---
```

```
Start Time: 1597369326
Timeout   : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: yes
```

cn={myrootcacert*}

Issued/signed by

cn={my intermediate CA}

Issued/signed by

cn=sdbazubuntu1.ca

USER SUPPLIED

EDGE INTERNAL

cn= iotedge workload ca

Issued/signed by

cn=sdbazubuntu1.eastus.cloudapp.azure.com

NOTE: some clients and trusted root store and y root ca file directly

This indicates a working leaf <- edge TLS setup. Anything else is no good

Couple of notes before we move on

- Other certs may be generated from the ‘device ca cert’ internally
  - Not included here because we are only addressing edgeHub TLS-related certs
- For debugging/inspection, the certs are stored in /var/lib/iotedge/hsm/cert
  - For fun, go poking around in there with ‘openssl x509……’ ☺

```
stevebus@sdbazubuntu1:~/edge$ ls -l /var/lib/iotedge/hsm/certs
total 36
-rw------- 1 iotedge iotedge 3790 Apr 21 16:14 device_ca_aliasazxVrrdEVxd7kvKvne1pOEyuSHF8EXSowNDhMzl30jI_.cert.pem
-rw------- 1 iotedge iotedge 9433 Aug 11 20:04 edgeHub637230782262856995serverT2TfowqpQ6_9O5mMQWivUtVXwwc2JCLBWlK5SgUZMkk_.cert.pem
-rw------- 1 iotedge iotedge 1895 Apr 21 16:14 edge_owner_cav0cQJsrFHjxosiOJDer2oKf-O45ZXKVJrO5WFWtFKe0_.cert.pem
-rw------- 1 iotedge iotedge 7762 Jul 28 18:21 iotedged-workload-caGrw6jn-HzmxG8plggnAjPDuGJr0qGW94X1KnqPwU9ng_.cert.pem
-rw------- 1 iotedge iotedge 7417 Jul 28 18:21 iotedge-tlsTLNi220opyZbShBY7-R4NIxntUhft8tKSA59Ln8BbSA_.cert.pem
stevebus@sdbazubuntu1:~/edge$
```

But what about modules?

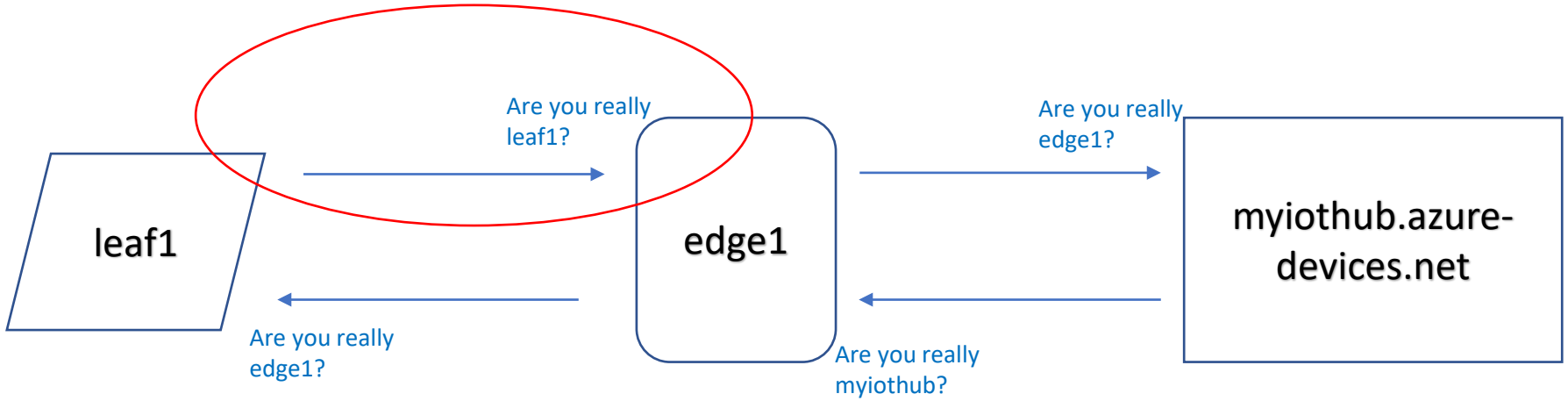
- Modules are ultimately just leaf devices hosted in a container
  - But they do get a few special Edge integration privileges
  - Specifically, they can all the iotedge security manager's 'workload' API
  - One of the things they can get from this API is the "trust bundle"
    - Includes the root certificate used for the device ca cert (and thus edgeHub TLS cert)
- SDK's handle this under the covers
  - ModuleClient.CreateFromEnvironmentAsync()
- Other modules can call the API manually to get the trust bundle

My root CA cert

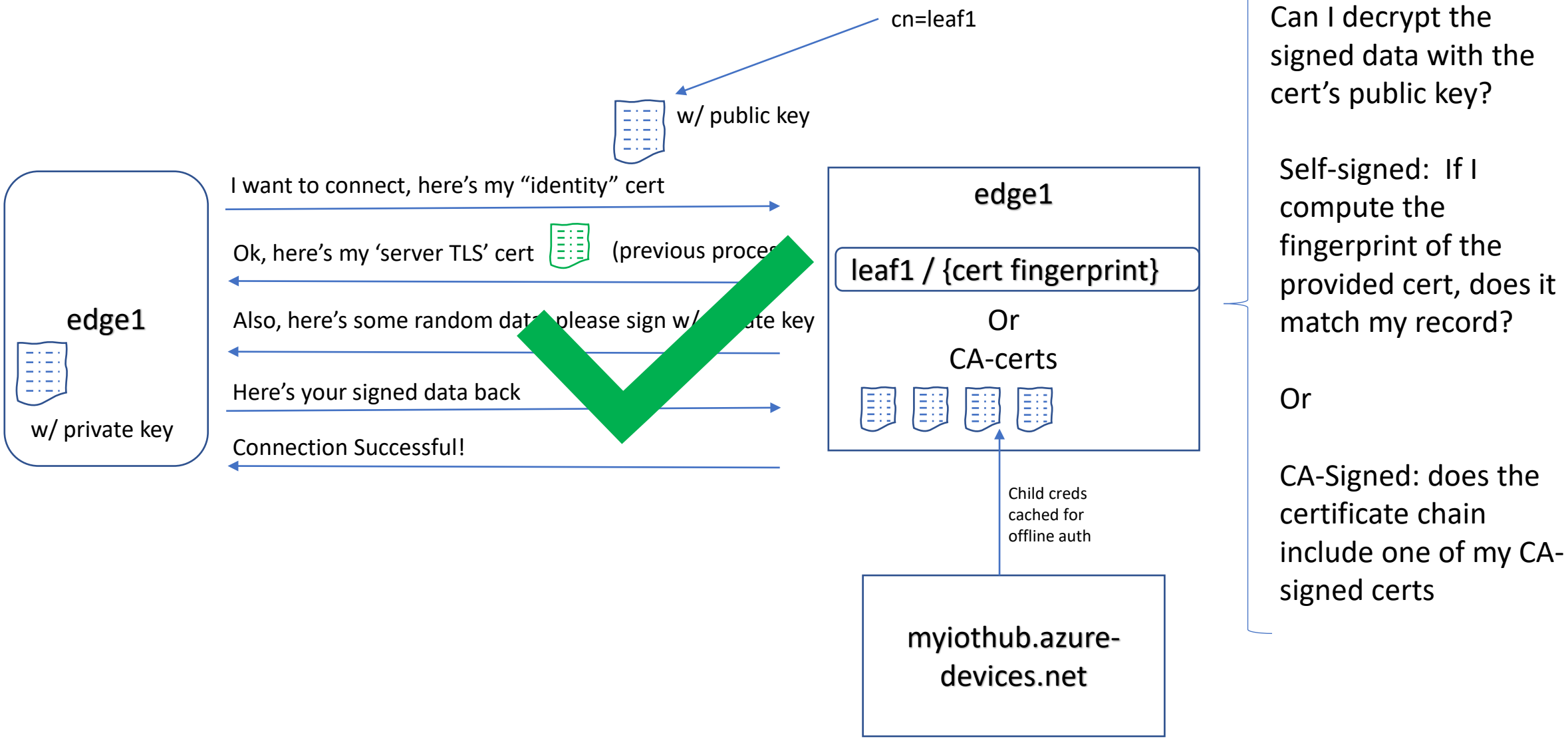
```
stevebus@sdbazubuntu1:~$ docker run -it --name ic --rm -v /var/run/iotedge/workload.sock:/var/run/iotedge/workload.sock --network azure-iot-edge ubuntu bash
root@76ba561b4999:/#
```

```
root@76ba561b4999:/# curl -X GET -s --unix-socket /var/run/iotedge/workload.sock http:///localhost/trust-bundle?api-version=2018-06-28
{"certificate":"-----BEGIN CERTIFICATE-----\nMIIFdzCCA1+gAwIBAgIJAKbf3Uiy0sGRMA0GCSqGSIb3DQEBCwUAMCoxKDAmBgNV\nBAMMH0F6dXJlX0lvVF9IdWJfQ0FfQ2VydF9UZXN0X09ubHkwHhcNMjAwNzI4MTgx\nOTQwWhcNMjEwNzI4MTgxOTQwWjAqMSgw
JgYDVQQDDB9BenVyZV9Jb1RfSHViX0NB\nX0NlcnRfVGVzdF9Pbmx5MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA\nsKNcoyWMx0j68hgSC[illegible]8Bhue6QigXEJK1CUi5m255iL632vtBQ/hrcZ8lvzNcKa\nzV/juk706GZGGifOO+hyWdWBLR9XjP4szNww0MFcnGr
2NyT3XH9DXpa9yD99Pjgm\nL1ugdk5ZE2knDIQgd1C5fwFq+zPOo9AaU01Tb+1MZLHMy+nDbGf1Bgck4pbb6LBc\nw/pWWJzz3IyPempbXpyomuq1pmkjmtj17qUIF9eEikRtxrR6sgZz+cSBNX0jnK6c\nyQHfS0SGsvqjj+pIzTqBfOOQ8Wvo7PZK3bt6gKEbg+Q2t9nCd4U8sk
G7VkyO/kMl\nriZ1QP9o7bU4OHj6eHl2PomqbYinmkWCk/upbtGSALRGCctYxAaiL7dDSh0Rq5Fn\nH6MC+WA2tKLKDXTRM8yckZazyDRG9nt1yLRrky8wz7+PnFP0seuNfnd2PmuG4YMS\nfYNNhxne6qBWb42Pe32WUkz9tBBIoLZDIXFVLhBTrrhmM8HpGq70GugQC9f6dGB8\
niM9B4C7giWjyR1NMpoSjvTUlpm4MN7Lh1V6QSbPLUpv7vzn0GNRFoiERMcLJB7VZ\nhS3FV/r4f6FIJ19JxqSC9OSGiNvXXXUeiwaPq+OfZWBn6ChxhHDLZ7RpT7pAKRij\n3knzPtKVOc/9IShFmNGPXDYnh9Dz2jrodLyNeFSXuVkCAwEAAaOBnzCBnDAdBgNV\nHQ4EFgQUpa
ZTVISqg1hml5LxFirqYhisNxswWgYDVR0jBFMwUYAUpaZTVISqg1hm\nl5LxFirqYhisNxuhLqQsMCoxKDAmBgNVBAMMH0F6dXJlX0lvVF9IdWJfQ0FfQ2Vy\ndF9UZXN0X09ubHmCCQCm391IstLBkTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB\n/wQEAwIBhjANBgkqhkiG9
w0BAQsFAAOCAgEAh9CtEs9Vy4tpLCdhJzysjDSdYNSp\nxd2MEJjqbPHR2tuC0tUspjkTlveg2hJCChyVYGsnkcoO2dE1ffflY7AD3eWF5IQEi\nOI+tX0h3CZxKo/NQ4lWNZboa9c+ATiMm/rO1VNUsmZ5+xUaC2VPwwtUBRSdonW8C\nSm1VYY2tVQrvbxRJco6FXWXufPPmNyy+
45pg76NoFSft3lqU+Ybgv6v4nB0PH2D3\nWOjngMYs59e/0RyRPZleWrYiaqPgFT2hV0kdT+/J1SVcmMUTxpZZW31ndFjXmPpx\nD+uYIxD3kgx+4VH7ek/q0Iet39f+W/Yfy5SoP0HC+am5NAAZIuF4e5Kv0DITGW2B\ntAQm5+UvdsngU+YdLzfKCYMYt7go4kT2giGa+oiHbYz
N1NwpwCkYBBbJX/YtHELz\nwJsOBjVWvNcCVpgQvQMBYKEIj/SkT7tURyRFB2Bivvg7flzU8hoNgpO1LzB5wAbw\ngwiH12Jb6cQ/dHe21LA3VrgR0R5aPLNGcqXxy+Ll9FBoaDYsQfVXBwpPcfKY0pxr\n/YqlW/lr9j6DPYjNs3bHYMUspebw8TJfSnwLHLUBaDqqEhib9o+HCh
CmbdjJFvYw\nPGIRZxj5qsiPI5WGndeOUFkHilIpBTnQoUgTk7RCWx+tn12HzzTlCyjkb2hLUoUA\nXsGnSaA3sfIlRAI=\n-----END CERTIFICATE-----\n"}root@76ba561b4999:/#
```

Four IoT Edge cert related scenarios



Are you really leaf1?



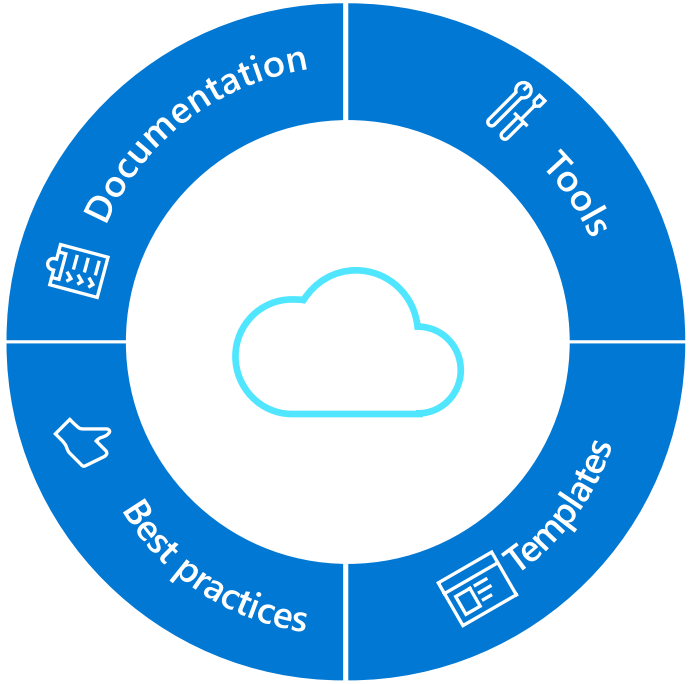
Can I decrypt the signed data with the cert's public key?

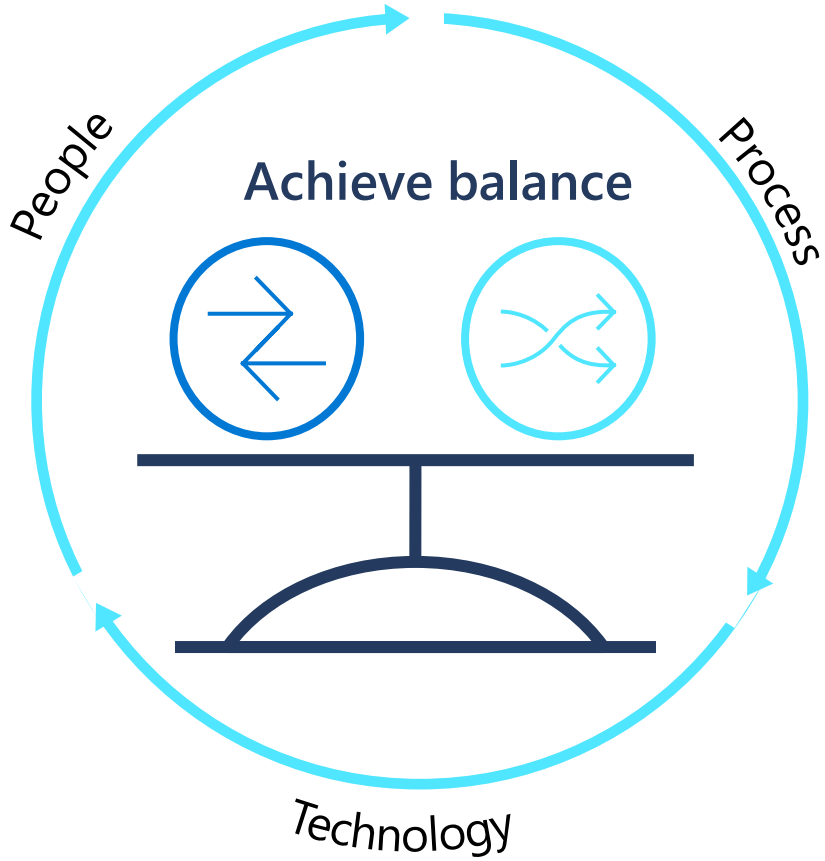
Self-signed: If I compute the fingerprint of the provided cert, does it match my record?

Or

CA-Signed: does the certificate chain include one of my CA-signed certs

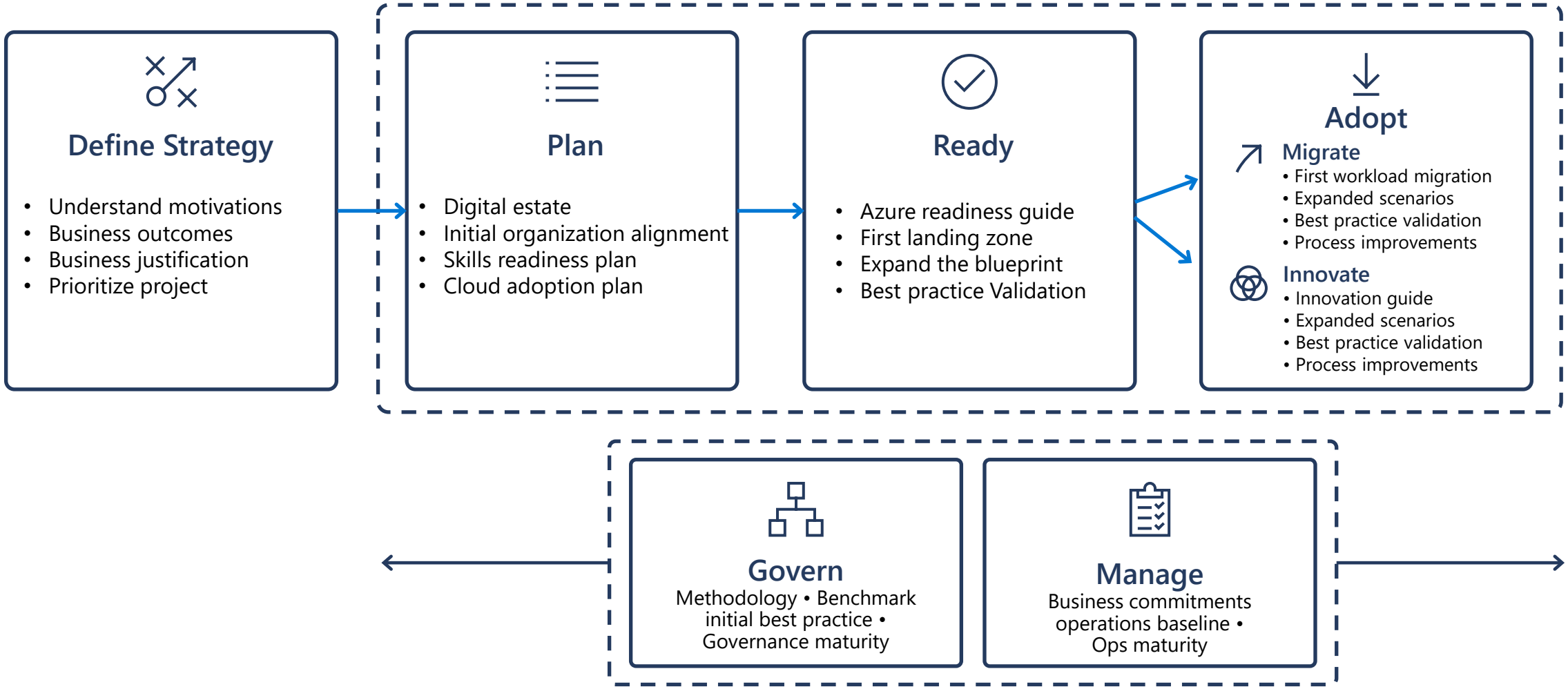
Microsoft Cloud Adoption Framework for Azure



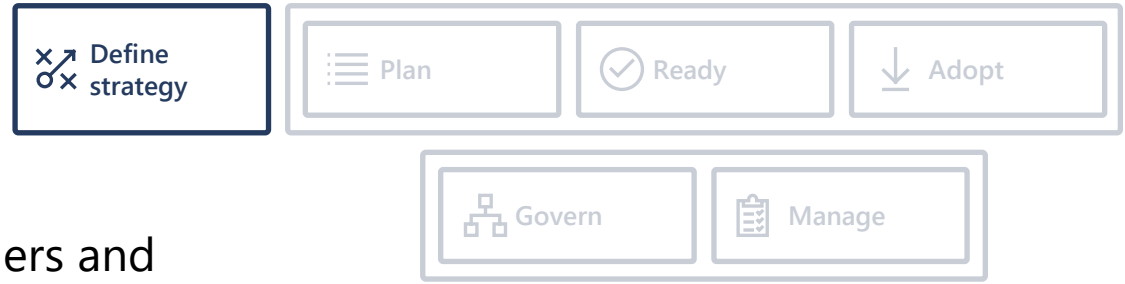


Align **business, people and technology strategy** to achieve business goals with **actionable, efficient, and comprehensive** guidance to deliver fast results with control and stability.

Microsoft Cloud Adoption Framework for Azure



Define strategy



Documenting the cloud strategy will help business stakeholders and technicians understand the benefits the organization is pursuing by adopting the cloud.

Motivations

- Executive mandate
- DC Exit
- Merger and acquisitions
- Cost savings
- Optimization
- Agility
- Tech capabilities
- Market demands
- Geo expansion
- Migration
- Innovation

Business outcomes

- **Fiscal:** revenue, cost, profit
- **Agility:** timer to market, provisioning,
- **Reach:** global access, sovereignty
- **Customer engagement:** cycle time, from request to release
- **Performance:** SLAs, Downtime, operations, reliability

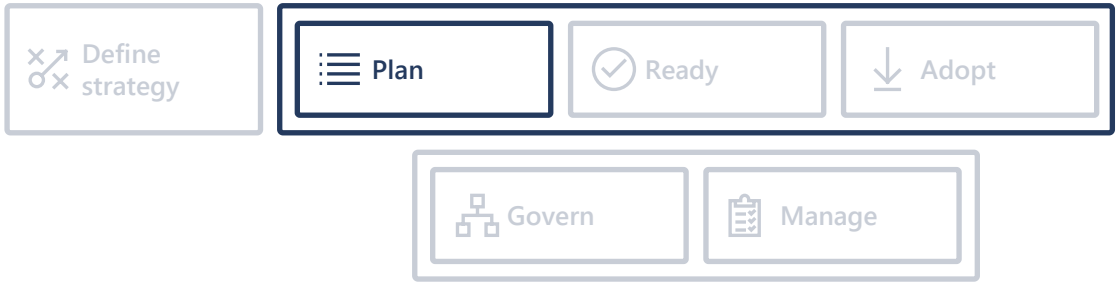
Business justification

- **Business case:** the cloud is not always cheaper, mirroring is not cloud, servers drive cost analysis
- **Financial model:** Capex/ Opex, ROI, gain, cost avoidance/reduction
- **Cloud accounting:** cost center, procurement, profit center, revenue generating, chargeback

First project

- **Business criteria:** workload supported by a BDM
- **Technical criteria:** minimum dependencies and test path, no governance
- **Qualitative analysis:** Current Team analysis

Plan



Cloud adoption plans convert the aspirational goals of the cloud adoption strategy into actions. It will help guide technical efforts, in alignment with the business strategy.

Digital estate

- ❑ **Rationalization:** inventory
- ❑ **Quantitative analysis:** asset optimized and sized properly
- ❑ **Qualitative analysis:** operational process

Initial organization alignment

- ❑ **Cloud Strategy Team**
  - ❑ Business IT: requirements and needs
  - ❑ IT management operations: traditional IT
  - ❑ Governance: executive sponsor, finance, business leadership, legal, security, HR
  - ❑ Cloud platform vendor: account success team
- ❑ **Cost management**
- ❑ **IT-business alignment**
- ❑ **Governance MVP**

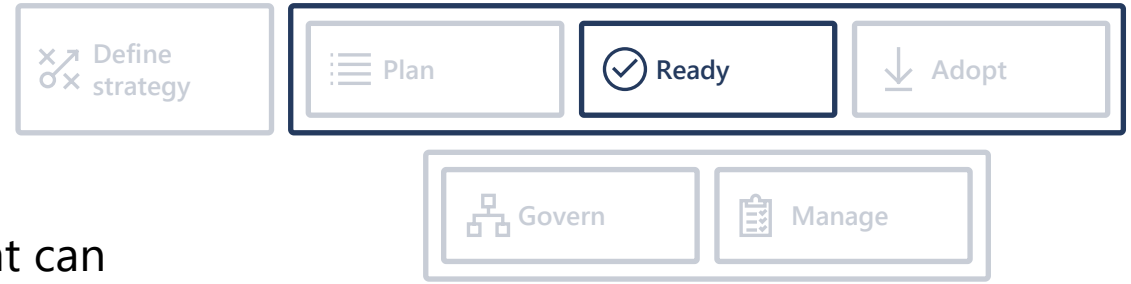
Skill readiness plan

- ❑ **Organizational readiness**
- ❑ **Governance and security alignment**
- ❑ **Initial organization alignment**
- ❑ **Building technical skills:** business/technical, and certifications
- ❑ **Change management guidance**

Cloud adoption plan

- ❑ **5R strategy:** rehost, refactor, rearchitect, rebuild, replace
- ❑ **Infrastructure migration:** VM, server, database focus
- ❑ **Application innovation:** born in the cloud applications, APIs
- ❑ **Data-driven innovation:** Focus on data consolidation and analysis

Ready



Ready establishes a cloud foundation or Adoption Target that can provide hosting for any adoption efforts. This should consist of common denominators across 80–90% of cloud adoption.

Azure readiness guide

- **Resource management:** management groups, subscriptions, resource groups, resources tree hierarchy
- **Naming Standards**
- **Resource tags**

Landing zone infrastructure

- **Network design:** Vnet, hybrid, firewall, hub, front door, endpoints
- **Storage design:** disk, file, blobs, CDN
- **Compute design:** VMs, containers, apps, serverless
- **Data design:** Structured/ unstructured

Landing zone ID

- **Identity and access**
- Role-based access control **RBAC**
- Manage to **least privilege**

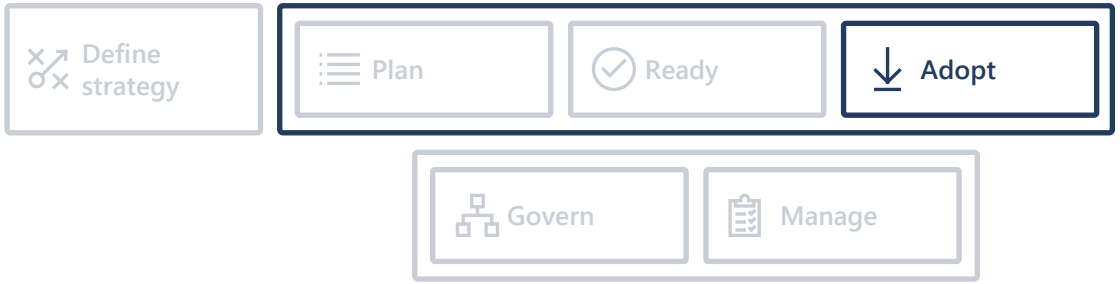
Landing zone cost

- **Costs and billing**
- Analyze **Cloud Costs**
- Monitor with **budgets**
- **Optimize** with recommendations
- **Manage** invoices and payments

Blueprints

- **AI**
- BigData
- Hybrid networks
- **Identity management**
- **IoT**
- **Serverless**
- **SAP**
- VMs
- WebApps
- DevOps

Adopt: Migrate



Cloud adoption will include workloads which do not warrant significant investments in the creation of new business logic. These workloads are candidates for migration to the cloud.

Assess

- **Evaluate** assets and establish a plan
- **Validate pre-requisites:** landing zone, skilling
- **Drivers:** reducing capex, freeing up DC
- **Quantitative factors:** VMs, networking, compatibility
- **Qualitative factors:** process dependencies, critical business events

Migrate: rehost

- **Replicate** (lift and shift) on-prem functionality using cloud native technology
- Leverage **Azure Migration Guide**

Optimize

- **Balance performance and price**
- Deliver the right experience **within budget**
- **Resize VM size, resize storage, resize database**

Secure and manage

- Prepare the migrated asset for ongoing operations: **security, monitoring, configuration**

Adopt: Innovate

Older apps can take advantage of many of the same cloud-native benefits by modernizing the solution or components of the solution. Modern DevOps invites into the process to create shorter feedback loops and better customer experiences.

Infrastructure abstraction

- Cloud native applications built from the ground up **optimized for cloud:**
- Resiliency
- Global scale
- Agility
- Security
- Autoscaling

Innovate: refactor

- Refactoring an application to fit a **PaaS/Serverless-based model** or refactoring code to deliver on new business opportunities.
- **Drivers:** faster and shorter updates, code portability, greater cloud efficiency (resources, speed, cost)

Innovate: rearchitect

- Modify existing applications into managed **containers** to take advantage of cloud native benefits
- **Drivers:** application scale and agility, easier adoption of new cloud capabilities, mix of technology stacks

Innovate: rebuild

- A new code base is created to align with a **cloud-native** approach. **App Data and AI Services**
- **Drivers:** accelerate innovation, build apps faster, reduce operational cost

DevOps

- Culture
- Development
- Testing
- Release
- Monitoring
- Management

Govern

Policy definition ensures consistency across adoption efforts. Alignment to governance/compliance requirements is key to maintain a well-managed cross-cloud environment.

Business risk

- **Document** evolving business risk
- Document risk tolerance based on **data classification**, and **application criticality**

Policy & compliance

- Convert risk decisions into **policy statements**
- Establish cloud adoption boundaries

Processes

- Establish processes to **monitor violations**
- Adhere to corporate policies
- **Cloud Center of Excellence**

Cost management

- Evaluate and monitor cost
- Limit IT spend
- Scale based on business demand
- Create cost accountability

Security baseline

- Compliance with IT Security requirements
- Apply security baseline to all adoption efforts

Resource consistency

- Consistency in resource configuration
- Enforce on boarding, recovery and discoverability practices

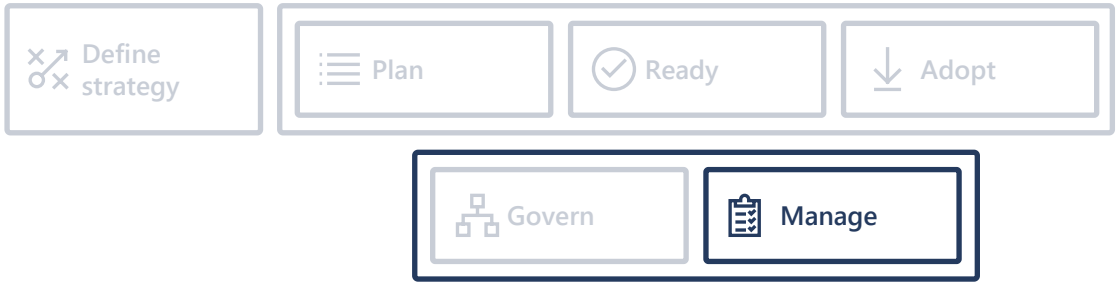
Identity baseline

- Enforce identity and access baseline
- Apply role definitions and assignments

Deployment acceleration

- Centralize templates
- Drive consistency and standardization

Manage and operations



Manage and operations enumerates, implements, and iteratively reviews related to the expected operational behavior of the service.

Management

- Identify critical operations for business operations
- Map operations to services
- Analyze services dependencies
- Create high level view service dashboards

Monitoring

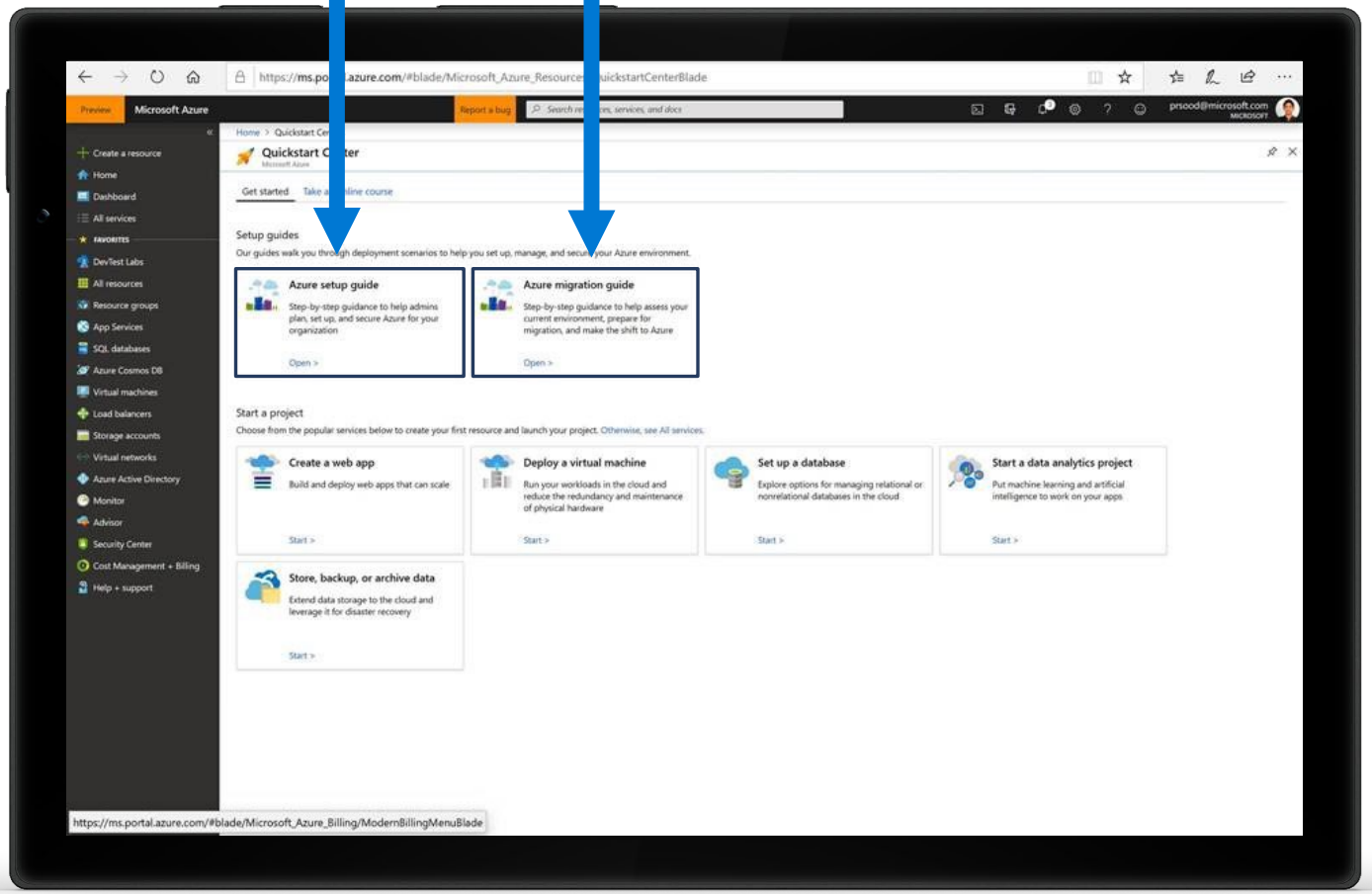
- Enable data collection
- Identify operations baseline
- Generate alerts
- Measure Service Metrics and generate SLAs

Resiliency

- **Enable a resilient** platform
- Recover from failures with minimal downtime and minimum data loss before
- **Evolve to a highly available platform**

Azure Setup Guide

Azure Migration Guide



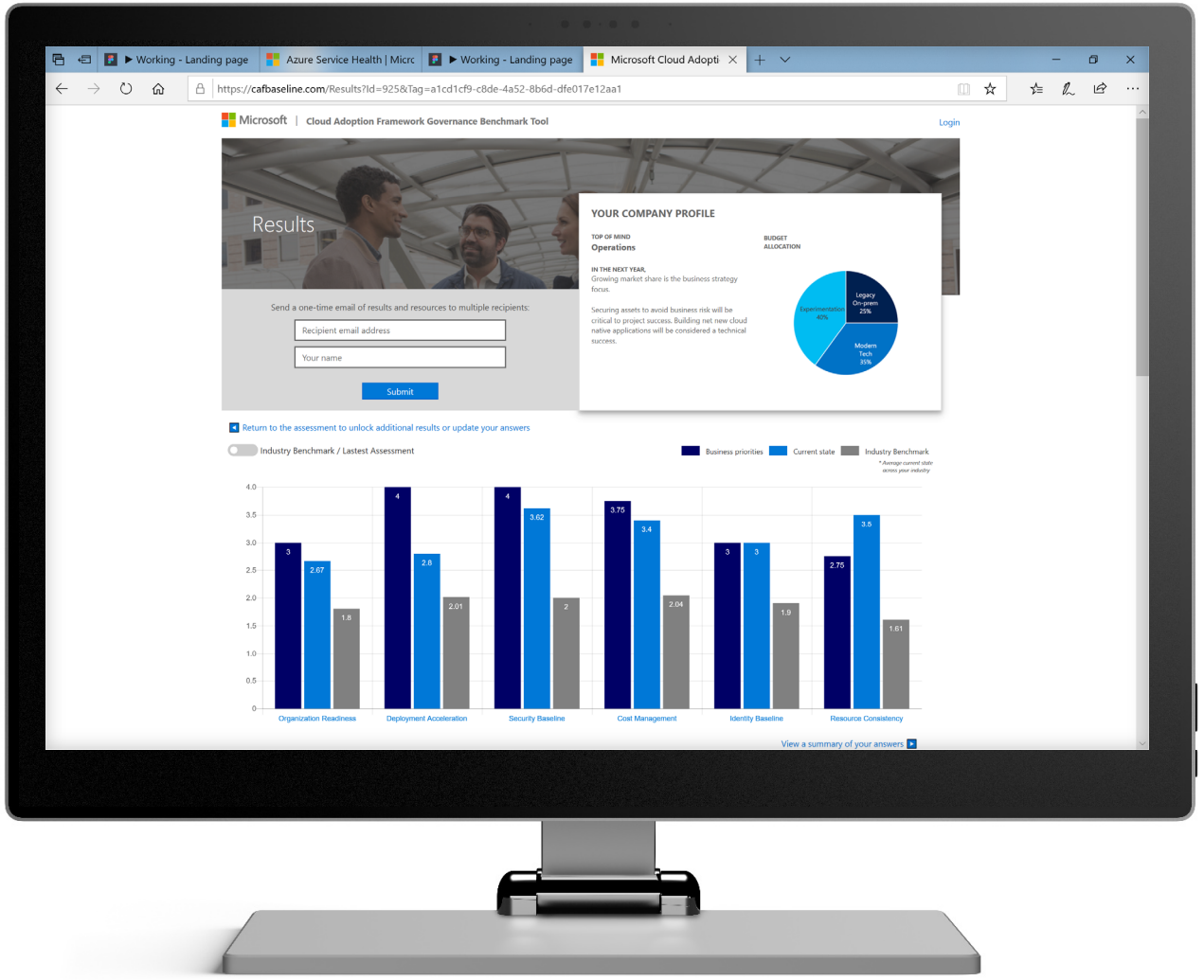
Implementation Guides are available in Azure Quickstart Center inside the Azure portal (portal.azure.com)

azure.com/cloudadoptionframework

Understand your current state and prepare for your cloud journey using

the Governance benchmark tool

http://aka.ms/adopt/gov/assess



azure.com/cloudadoptionframework

Microsoft Azure Advisor

Your personalized recommendation guide to Azure best practices

Name
Microsoft

Microsoft

November 2017
v111717

Optimize your Azure resources with Azure Advisor

https://aka.ms/azureadvisor/

High Availability

Improve the availability of your business-critical applications

Security

Enhance protection of your Azure resources from potential security threats

Performance

Optimize performance to make the most of your resources

Cost

Maximize the return of your IT budget investment

Azure Advisor available for portal.azure.com customers. More information https://aka.ms/azureadvisor/overview/.

Microsoft Azure Advisor

https://aka.ms/azureadvisor/

YOUR PERSONALIZED GUIDE

to Azure best practices

Review your personalized recommendations at no cost

- Generated based on your configuration and usage patterns
- Available for all your Azure subscriptions in Azure portal*
- View recommendations at no cost **

Prioritize recommendations and configure Advisor to your needs

- Assess recommendation impact
- Select your Azure resources you care most about
- Adjust usage thresholds for low usage virtual machines
- Download reports

Implement recommendations and monitor your progress

- Implement most critical recommendations for your solutions
- Review progress and new recommendations regularly

*Azure Advisor available in public Azure cloud at GA (March 2017).

** Implementing recommendations may increase your monthly cost, varies per recommendation, review azure.microsoft.com/pricing for more details

Advisor recommendatic

portal.azure.com/#blade/Microsoft_Azure_Expert/AdvisorBlade

Microsoft Azure Advisor recommendations

jerryf@contoso.com
CONTOSO

Advisor recommendations

Download as CSV | Download as PDF | Configure

Subscriptions: 2 of 24 selected – Don't see a subscription? Switch directories

2 subscriptions | All types | Active | No grouping

Overview | High Availability (8) | Security (20) | Performance (1) | Cost (3) | All (32)

High Availability

8 **Recommendations**

1 High impact | 7 Medium impact | 0 Low impact

25 **impacted resources**

Security

20 **Recommendations**

20 High impact | 0 Medium impact | 0 Low impact

59 **impacted resources**

Performance

1 **Recommendation**

1 High impact | 0 Medium impact | 0 Low impact

1 **impacted resource**

Cost

1,876 USD savings/mo *

3 **Recommendations**

3 High impact | 0 Medium impact | 0 Low impact

10 **impacted resources**

Tips & tricks

- You can customize Advisor to process recommendations for resources that matter to you the most.
- You can optimize underutilized virtual machines to reduce your monthly Azure spend.

Download recommendations as PDF

Download recommendations as CSV

Advisor recommendatic

portal.azure.com/#blade/Microsoft_Azure_Expert/AdvisorBlade

Microsoft Azure Advisor recommendations

jerryf@contoso.com
CONTOSO

Advisor recommendations

Download as CSV | Download as PDF | Configure

Subscriptions: 2 of 24 selected – Don't see a subscription? Switch directories

2 subscriptions | All types | Active | No grouping

Overview | High Availability (8) | Security (20) | Performance (1) | Cost (3) | All (32)

For more cost management and optimization capabilities, try Azure Cost Management →

Total recommendations
3

Recommendations by impact
High 3
Medium 0
Low 0

Impacted Resources
10

Potential monthly savings
1,876 USD

IMPACT	DESCRIPTION	POTENTIAL MONTHLY SAVINGS	IMPACTED RESOURCES	UPDATED AT
High	Right-size or shutdown underutilized virtual machines	13.39 USD	1 Virtual machine (classic)	10/23/2017 9:29:30 AM
High	Use SQL elastic database pools		2 SQL servers	10/23/2017 9:29:25 AM
High	Right-size or shutdown underutilized virtual machines	1,862.98 USD	18 Virtual machines	10/23/2017 9:02:02 AM

Shut down or resize your virtual machine

Feedback | Download as CSV | Download as PDF | Configure recommendation rule

We've analyzed the usage patterns of your virtual machine over the past 14 days, and identified virtual machines with low usage. While certain scenarios can result in low utilization by design, you can often save money by managing the size and number of virtual machines. Learn more

2 selected | No grouping

18 Virtual machines **1,862.98 USD** potential monthly savings

*You can save up to the stated amount if you choose to shut down the virtual machine. Your actual savings may vary.

VIRTUAL MACHINE	RECOMMENDED ACTIONS	POTENTIAL SAVINGS*	SUBSCRIPTION	RECOMMENDATION RULE	UPDATED AT	ACTIVATE
ContosoAzADDS2	View Usage Patterns Shut down the virtual machine Resize the virtual machine	96.72 USD	Contoso - Production	Average CPU < 15%	10/23/2017 9:02:02 AM	Snooze
ContosoAzLnx1	View Usage Patterns Shut down the virtual machine Resize the virtual machine	94.49 USD	Contoso - Production	Average CPU < 15%	10/23/2017 9:02:02 AM	Snooze
ContosoWeb1	View Usage Patterns Shut down the virtual machine Resize the virtual machine	193.44 USD	Contoso - Production	Average CPU < 15%	10/23/2017 9:02:02 AM	Snooze
ContosoAzADDS1	View Usage Patterns Shut down the virtual machine Resize the virtual machine	96.72 USD	Contoso - Production	Average CPU < 15%	10/23/2017 9:02:02 AM	Snooze
ContosoWebBF3	View Usage Patterns Shut down the virtual machine	98.95 USD	Contoso - Production	Average CPU < 15%	10/23/2017 9:02:02 AM	Snooze

Is this recommendation helpful?

Dashboard - Microsoft

portal.azure.com/#resource/subscriptions/e4564567-5645-5b45-9c67-3b74b59a6999/resourceGroups/contosoazurehq/providers/Microsoft.Compute/virtualMachines/ContosoAzA

Microsoft Azure | Advisor recommendations > Shut down or resize your virtual machine > ContosoAzADDS2

jerryf@contoso.com
CONTOSO

ContosoAzADDS2
Virtual machine

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

SETTINGS

- Networking
- Disks
- Size
- Extensions
- Availability set
- Configuration
- Properties
- Locks
- Automation script

Connect | Start | Restart | Stop | Move | Delete | Refresh

Resource group (change)
contosoazurehq

Status
Running

Location
South Central US

Subscription (change)
Contoso IT - demo

Subscription ID
e4272367-5645-4c4e-9c67-3b74b59a6982

Computer name
ContosoAzADDS2

Operating system
Windows

Size
Standard DS1 v2 (1 vcpu, 3.5 GB memory)

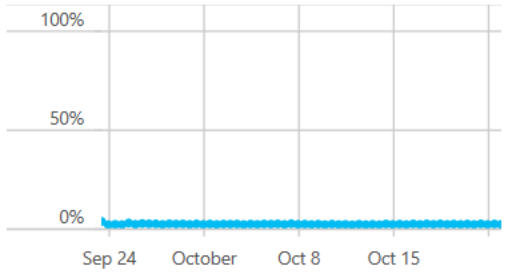
Public IP address
13.85.28.222

Virtual network/subnet
ContosoAzureVNET/ContosoAzureSubnet

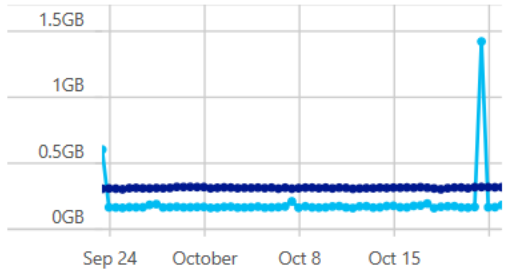
DNS name
Configure

Show data for last: 1 hour | 6 hours | 12 hours | 1 day | 7 days | 30 days

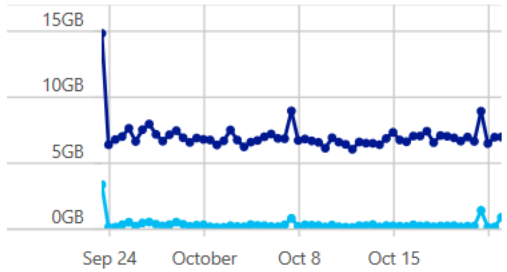
CPU (average)



Network (total)



Disk bytes (total)



Disk operations/sec

What did we learn?
Send questions to iotacademy@microsoft.com
We start tomorrow at 10:15am ET