There is no more products to buy to achieve “cyber resilience”

We need a different security design principle and an organizational vision

ZeroTrust

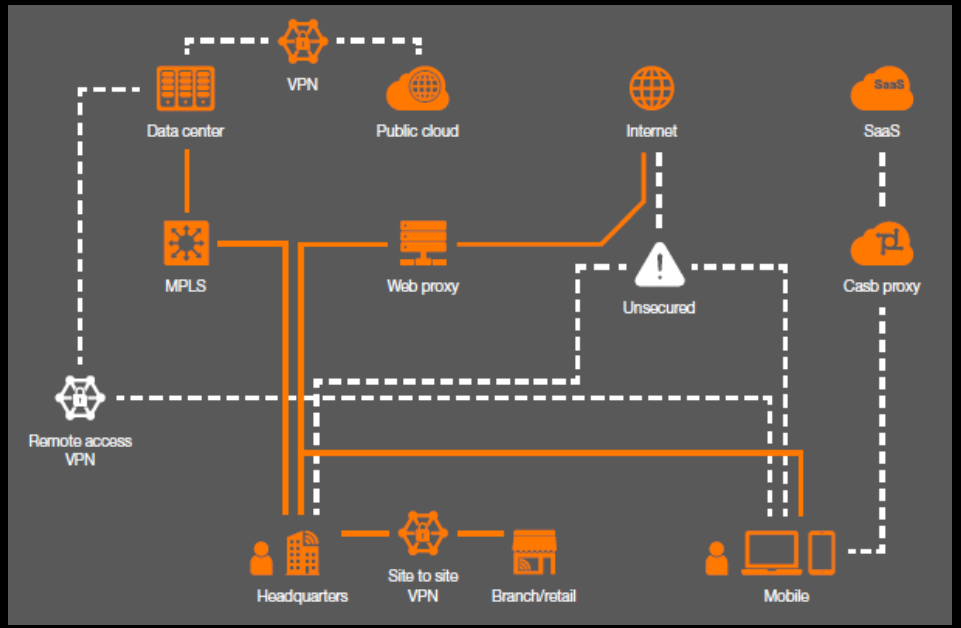
orange™ Cyberdefense

Lars-Göran Christiansson
Solution architect

Current state

- Market-leading solutions
- Cyber SOC monitoring
- CSIRT – Incident response
- Public breach information
- Continued investments and ongoing security work
- Defence in depth

- But we still get breached and impact of Cyberattacks are getting worse



Why Zero Trust?

Secure your digital transformation

Drastically reduce attack surface

- Still to easy to be breached and work unnoticed
- Cyber Security Insurances are not the future
- Hard to find Cyber Security resources

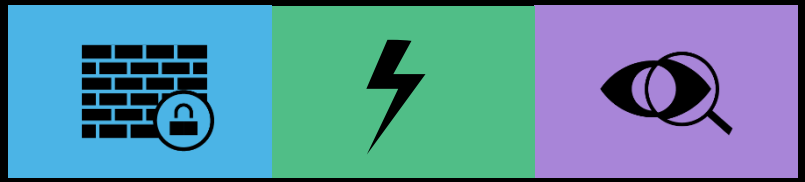
Increase Cyber resilience - NIST

- The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Compliance

- By 2025, 60% of organizations will use cybersecurity risk as the primary determinant in conducting third-party transactions and business relationships. (Gartner)

There are three important principles in this ideology:



1	2	3
Apply the concept of least privilege.	Assume that breach is inevitable or has likely already occurred.	Every transaction must be authenticated and authorized.

What is Zero Trust?

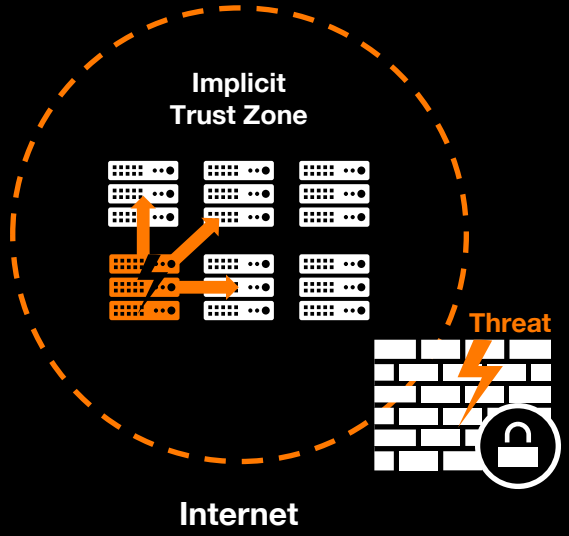
Zero Trust is a design ideology that state threats can be anywhere
- All networks are considered equal
There are no internal or external

Overall goal of implementing Zero Trust:

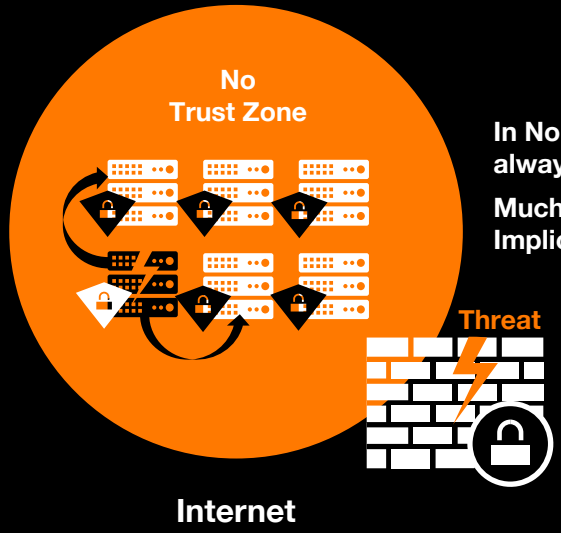
Limit the blast radius of an attack to protect business continuity and limit the cost of it.

Zero Trust

Traditional Single Perimeter Defense



Zero Trust Defense Focuses on Resourec Protection



In No trust Zone, never trust, always verify first!

Much smaller Implicit Trust Zone

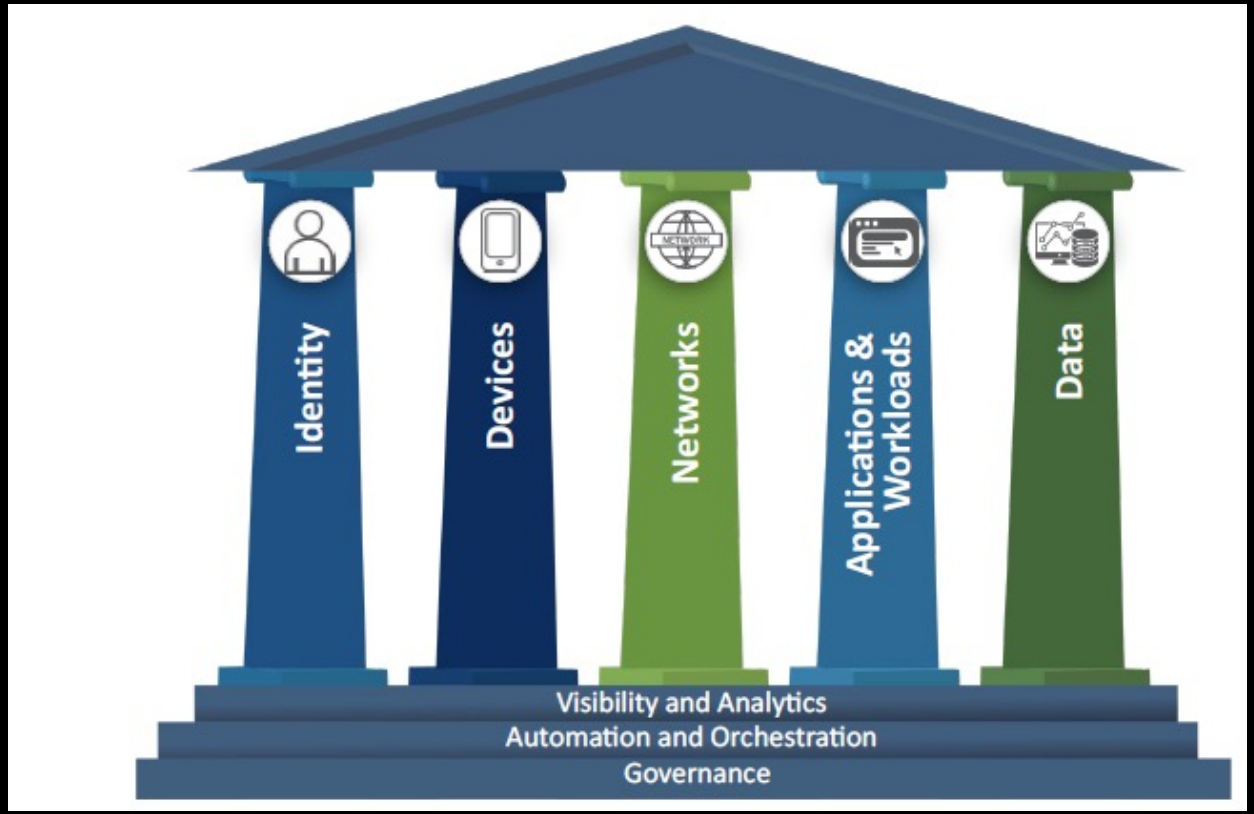
Top 8 Cybersecurity predictions for 2022-23

60% of organizations will embrace Zero Trust as a starting point for security by 2025.
More than half will fail to realize the benefits !

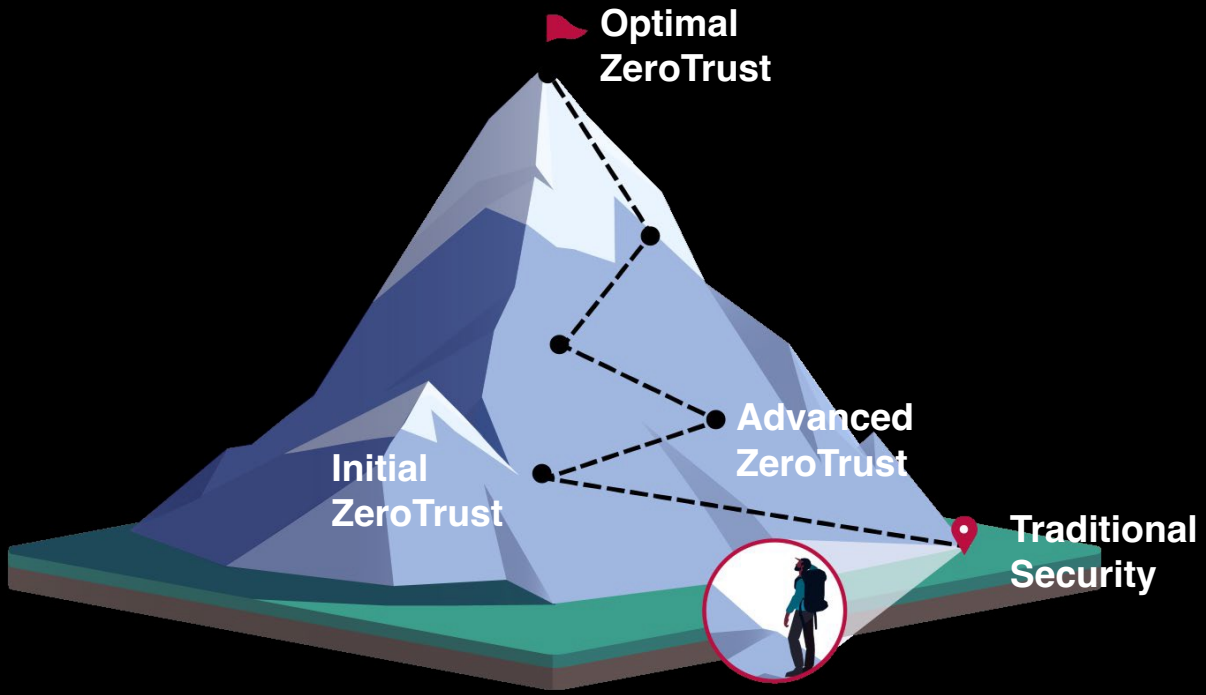
However, as zero trust is both a security principle and an organizational vision, it requires a cultural shift and clear communication that ties it to business outcomes to achieve the benefits.

https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

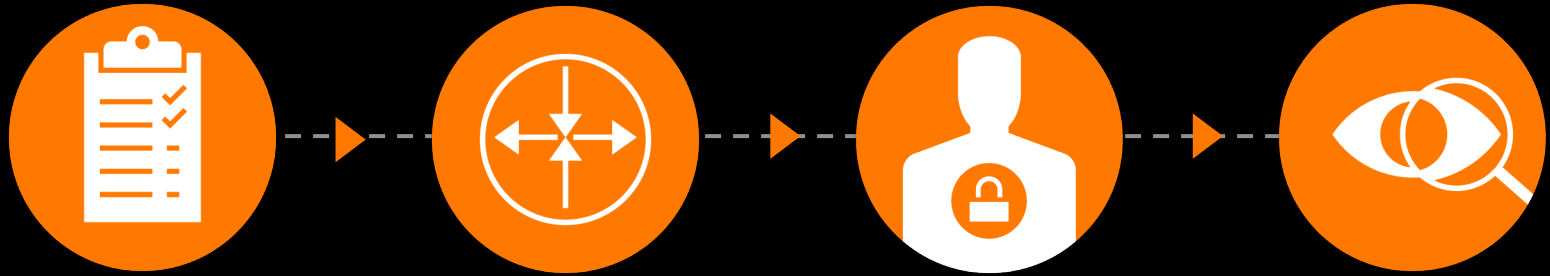
Zero Trust Maturity Model Pillars



Zero Trust Maturity Journey
An Incremental process that may take years to implement fully



Zero Trust
Design principles



Outcomes
By focusing on business, outcomes security can be seen as an enabler

Inside to out
Understand what you need to protect. Design outward from there.

Access
How and what should have access.

Inspect and log
Log and inspect all Traffic up to layer 7

5 steps to implementing Zero Trust

1

Define the protect surface.

2

Map the transaction flows.

3

Build Zero Trust architecture.

4

Create Zero Trust policy.

5

Monitor and maintain the network.

1 Define the protect surface.

Single DAAS element – Critical to your business
You will have many protect surfaces
A protect surface is much smaller compared to your attack surface

- Smaller focus
- Well defined and documented

DAAS:
Data – Sensitive data (Toxic)
Assets – Scada, Point of sales terminals, medical equipment, IoT
Applications – off the shelf or custom software
Services – DNS, DHCP, Active Directory

2 Map the transaction flows.

To properly design a network. It's critical to understand how systems should work and how various **DAAS components** interact with other resources.

The way traffic moves across the network, specific to the data in the protect surface, determines how it **should be protected.**

3 Build a Zero Trust architecture

With your protect surface defined and flows mapped, you can then begin to build your Zero Trust architecture.

- IDP
- Networksegmention
- Microsegmentation
- VPN / Security Service Edge
- Conditional Access
- Privileged Access management

4 Create Zero Trust Policy

Context based policy to determine who or what can access to your protect surface

Who should be accessing a resource?
What application (DAAS)
When is the asserted identity trying to access the resource?
Where is the packet destination?
Why is this packet trying to access this resource
How is the asserted identity of a packet accessing the protect surface

5 Monitor and maintain the network.

Monitor and maintain the environment:

Inspect and log all traffic

The telemetry provided by this process will not just help prevent data breaches and other significant cybersecurity events but will provide valuable security improvement insights.

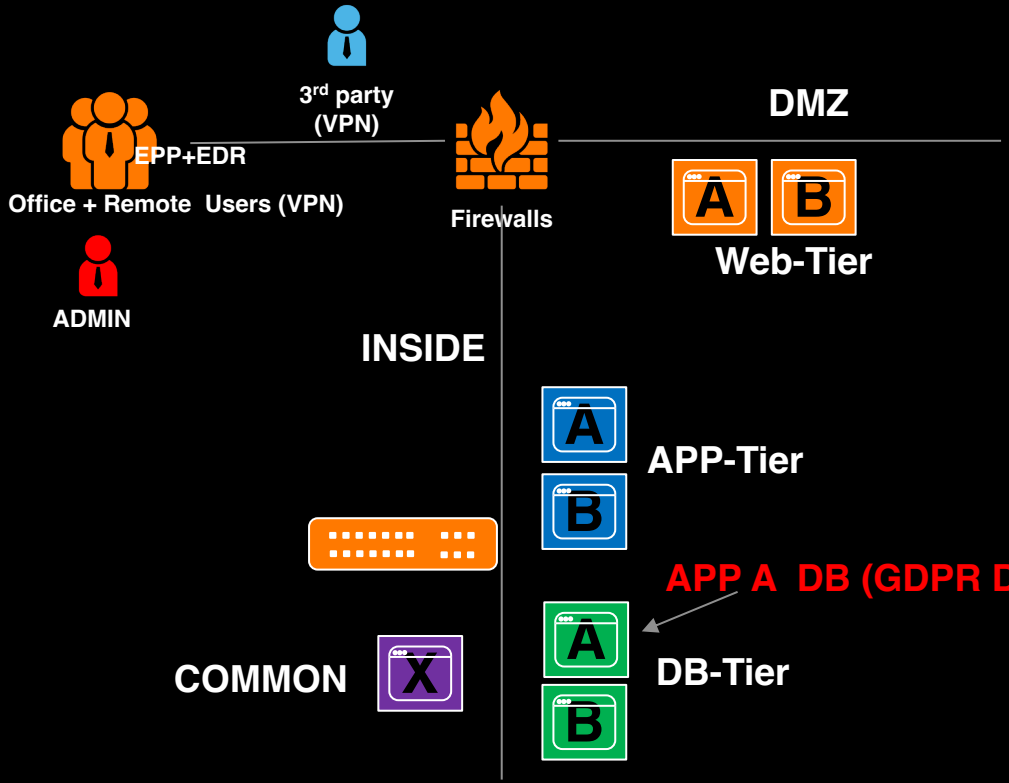
Zero trust Example 1

On-prem GDPR application

Lars-Göran Christiansson
Solution Architect

orange™ Cyberdefense

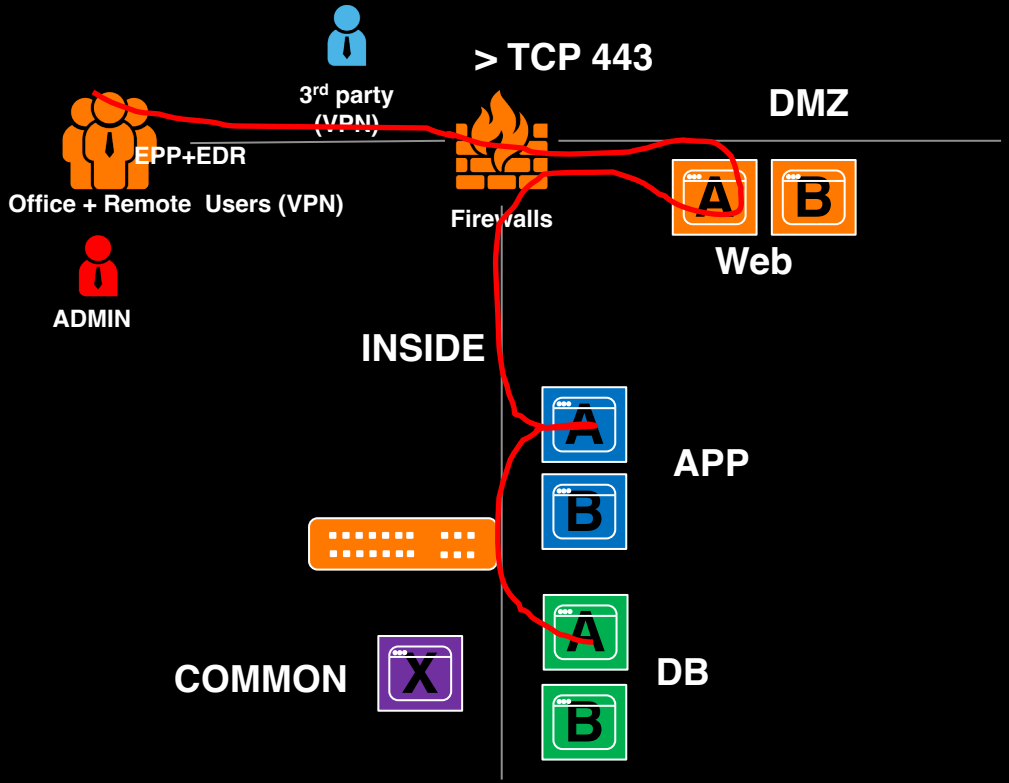
Zero-Trust example 1
On-prem legacy GDPR application A



1. Define the protection surface.

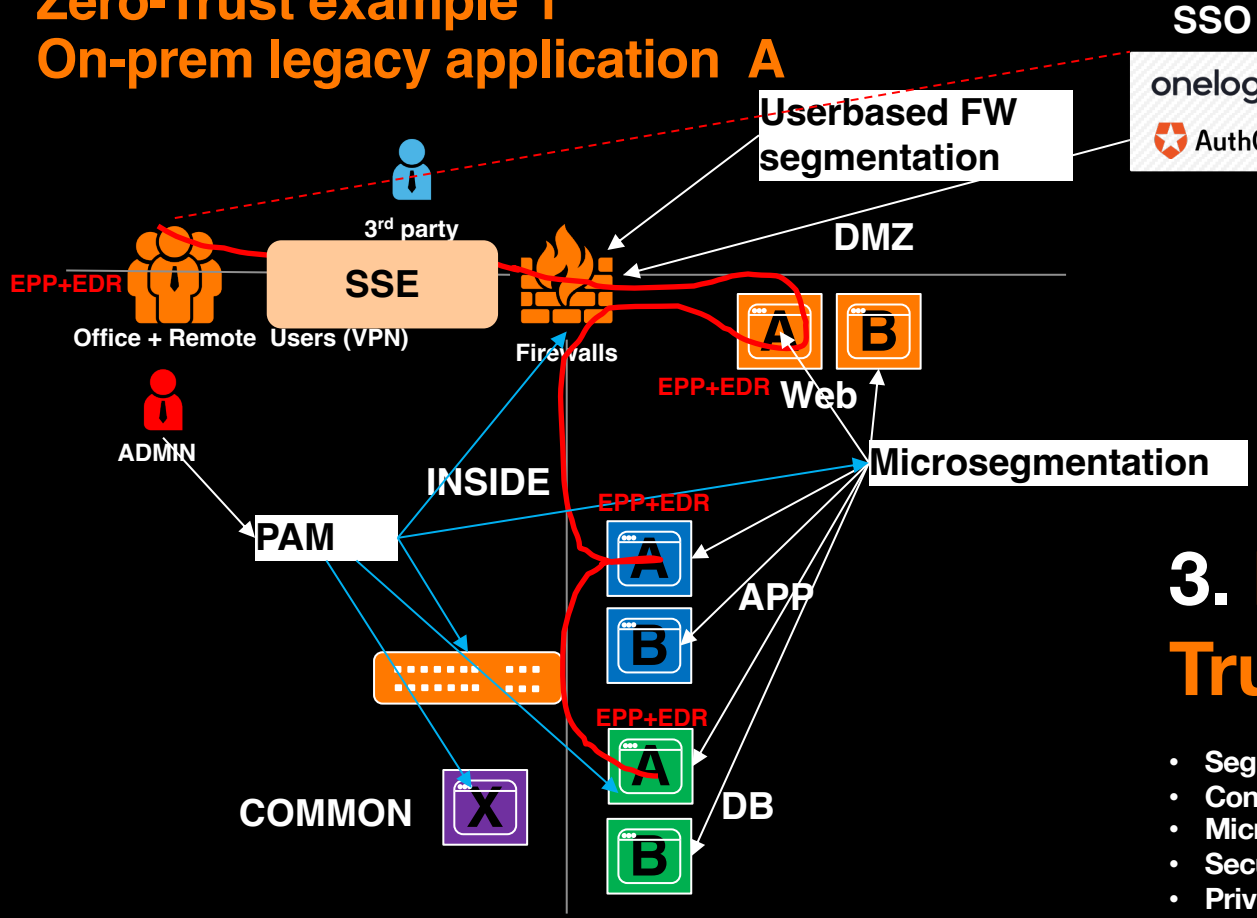
- Business custom-built “Application A” with personal data

Zero-Trust example 1
On-prem legacy GDPR application A



2. Map the transaction flows.

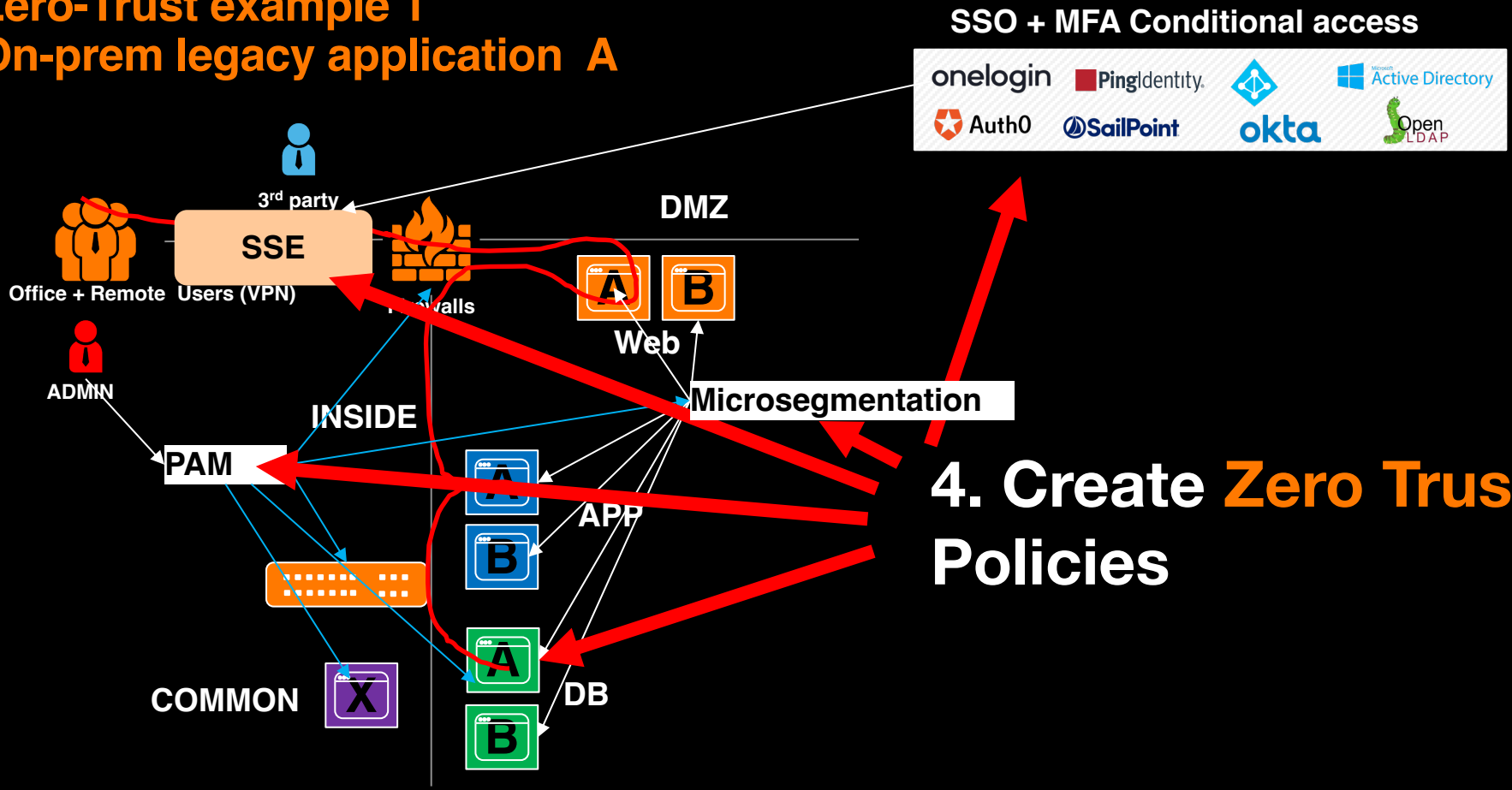
Zero-Trust example 1
On-prem legacy application A



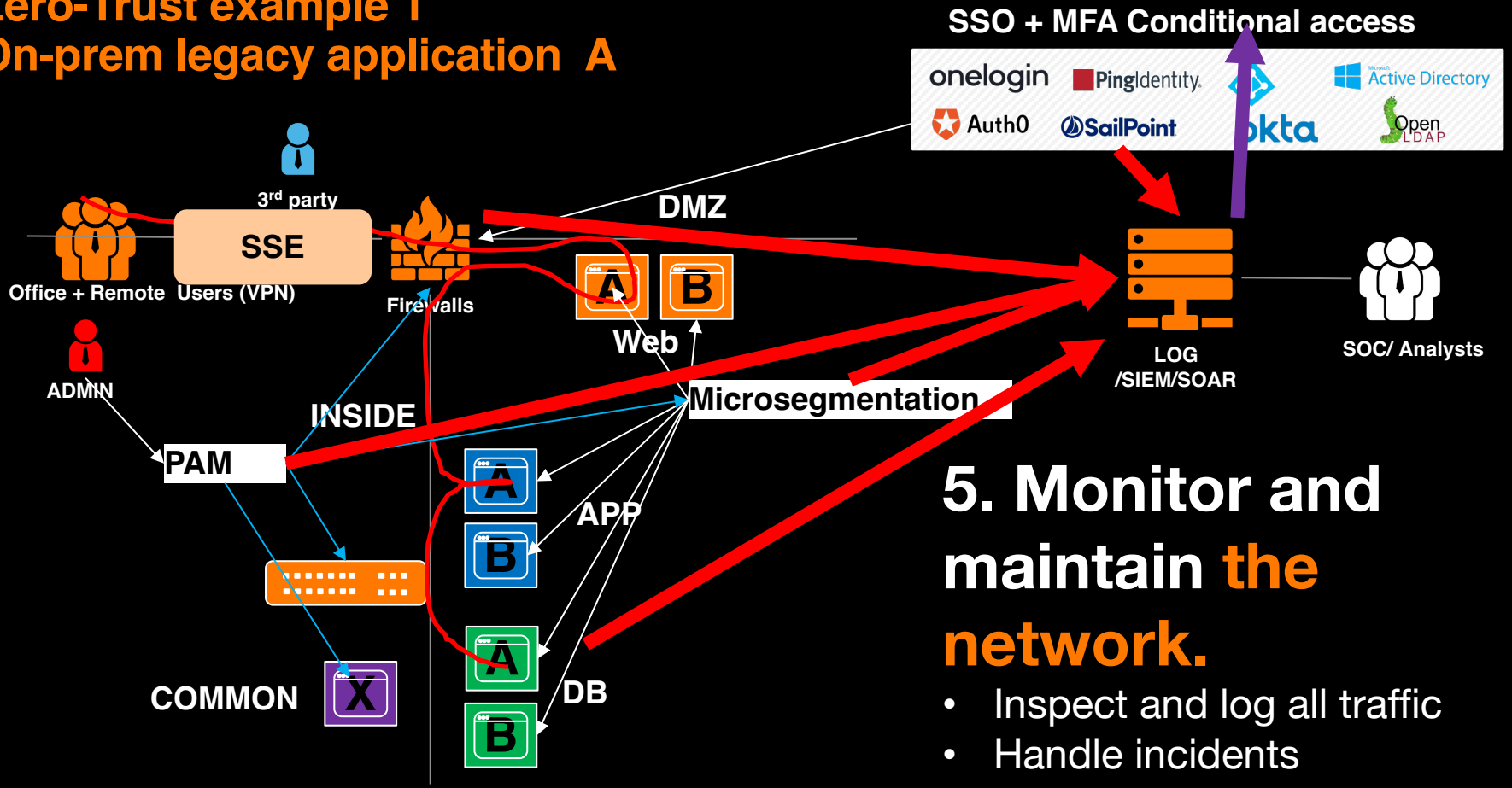
3. Build a Zero Trust architecture

- Segmentation
- Conditional Access
- Microsegmentation
- Security Service Edge
- Privileged Access Management

Zero-Trust example 1
On-prem legacy application A



Zero-Trust example 1
On-prem legacy application A



5. Monitor and maintain the network.

- Inspect and log all traffic
- Handle incidents
- Tune policies

Zero trust Example 2

Public Cloud based Application

Marcus Hilmersson/Lars-Göran Christiansson

Solution Architect

orange™ Cyberdefense

Zero-Trust Examples: Cloud-based Application

1a. Identify Application Components.

Storage Account

Service: PaaS
Type: Private
Data: Sensitive

Azure WebApp

Service: PaaS
Type: Public
Data: Public

Azure SQL

Service: PaaS
Type: Private
Data: Confidential

API Gateway

Service: PaaS
Type: Public
Data: Sensitive

Azure Kubernetes Services

Service: PaaS
Type: Private
Data: Sensitive

Github

Service: SaaS
Type: Public
Data: Confidential

Service: SaaS
Type: Public
Data: Confidential

Zero-Trust Examples: Cloud-based Application

1b. Identify Application Users.

Platform Admins

Storage Account

Service: PaaS
Type: Private
Data: Sensitive

Azure WebApp

Service: PaaS
Type: Public
Data: Public

Customers

Data Owners

Azure SQL

Service: PaaS
Type: Private
Data: Confidential

API Gateway

Service: PaaS
Type: Public
Data: Sensitive

Partners

App Developers

Azure Kubernetes Services

Service: PaaS
Type: Private
Data: Sensitive

Github

Service: SaaS
Type: Public
Data: Confidential

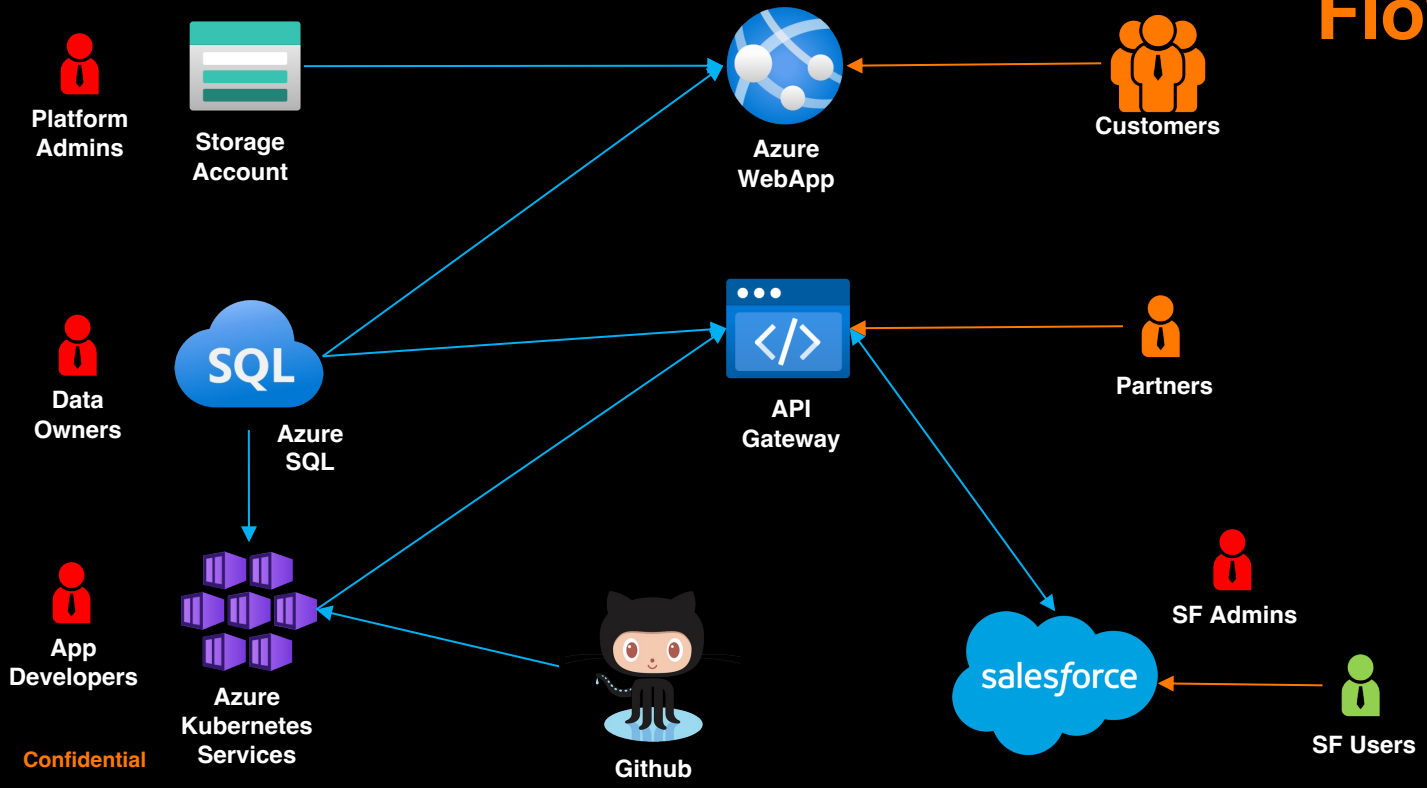
SF Admins

Service: SaaS
Type: Public
Data: Confidential

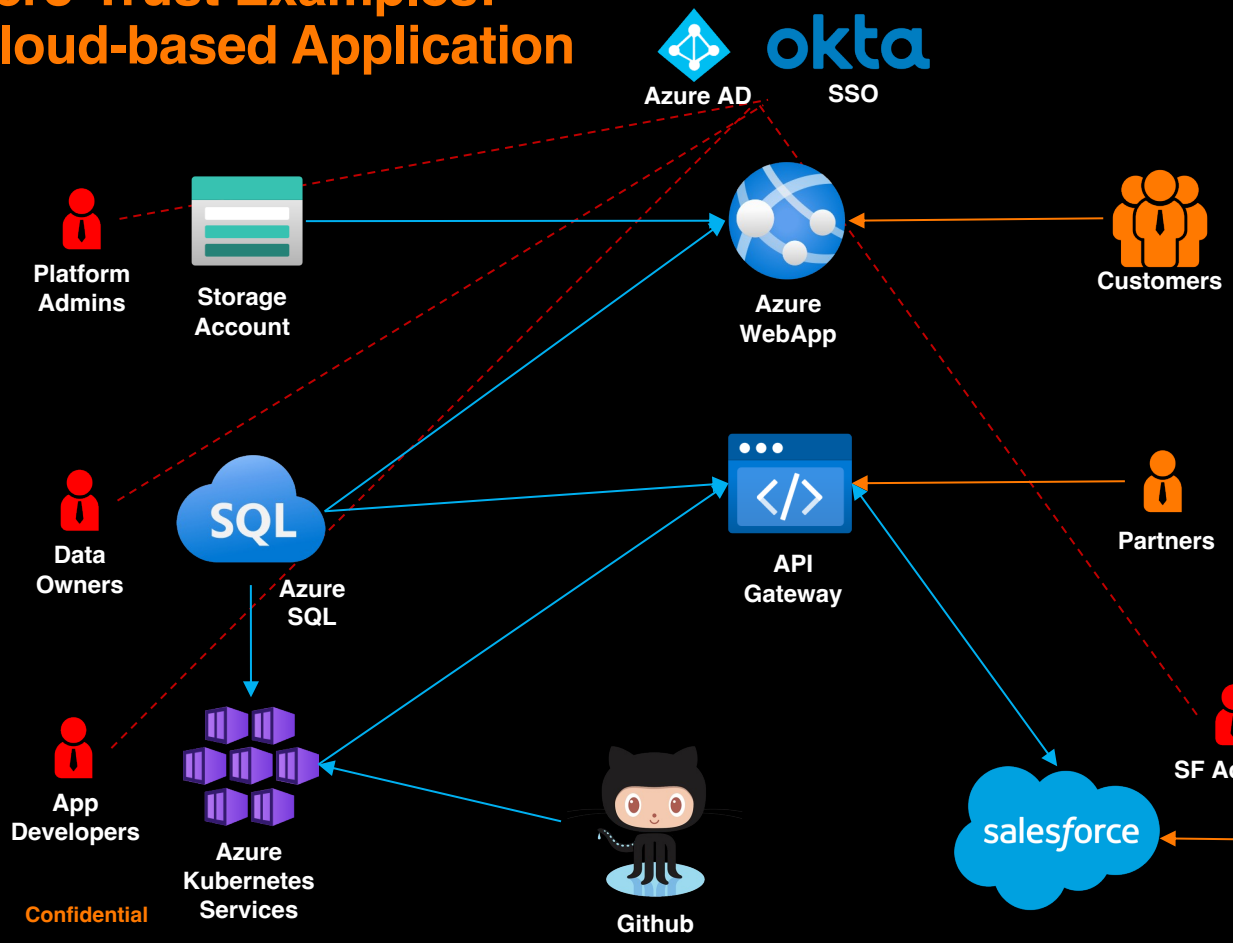
SF Users

Zero-Trust Examples: Cloud-based Application

2. Map Transaction Flows.



Zero-Trust Examples: Cloud-based Application



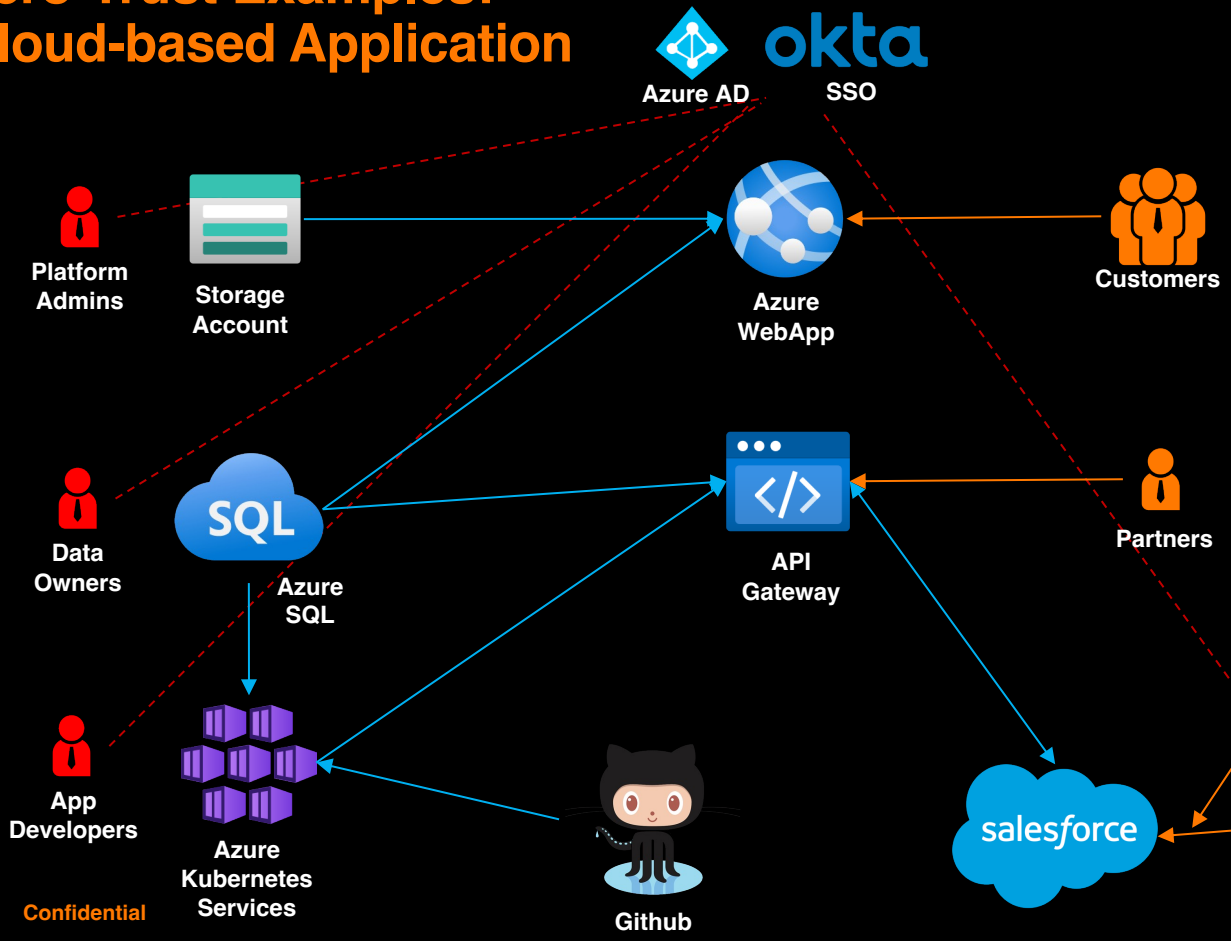
3. Build Zero-Trust Architecture.

Management Plane
- Conditional Access
- Privileged Identity Management
- Access Reviews
- SSO
- Service Firewalls/ACLs
- Private Endpoints
- VPN
- CI/CD Pipeline
- Key Vault/HSM

Data Plane
- Encryption
- Data Masking

SaaS
- SSE
- SSPM

Zero-Trust Examples: Cloud-based Application



4. Create Zero Trust Policy.

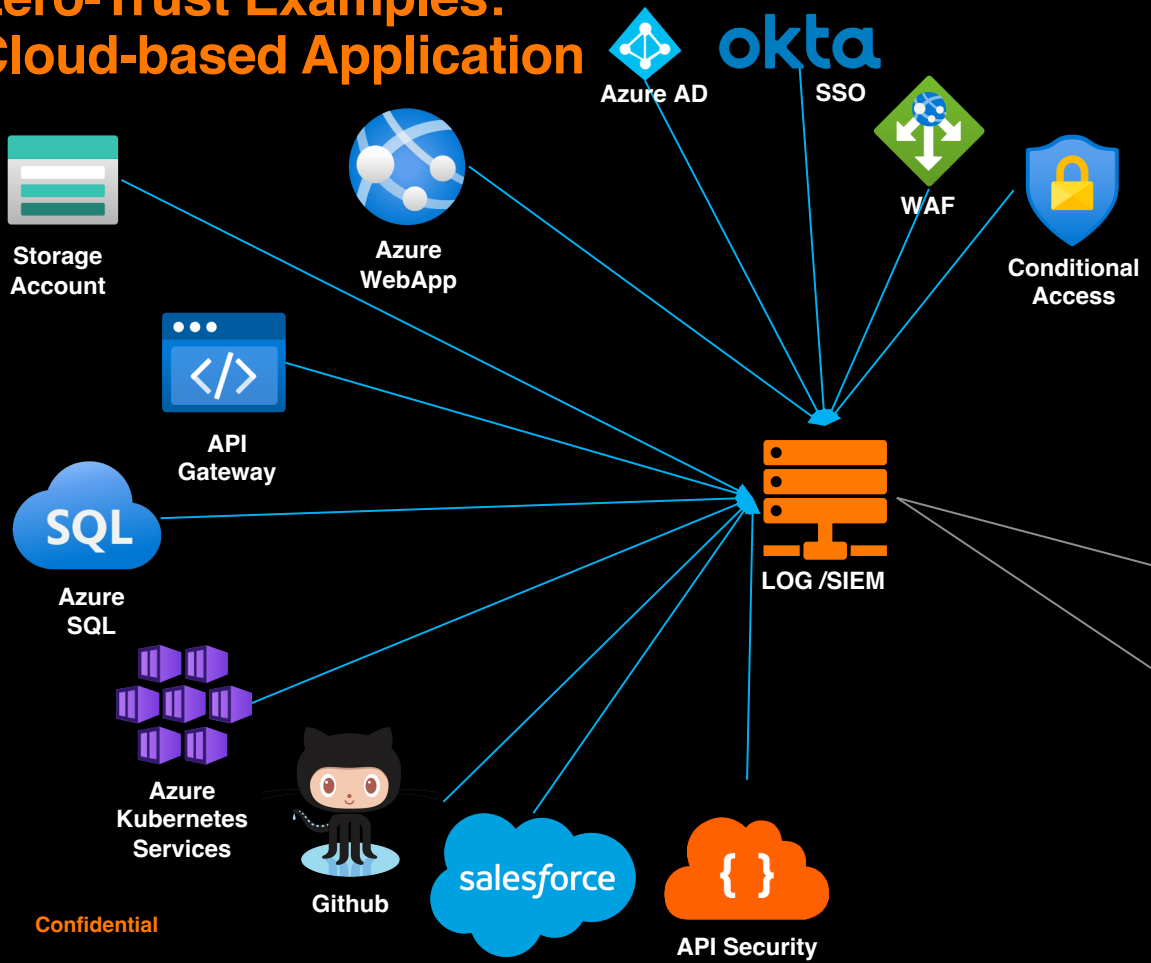
Emphasis on:

- Contextual access controls.
- Least-privilege principles.
- User education.

General advice:

- Use cloud-based tools.
- Seamless user experience.
- Focus on user-access controls primarily, not network-based controls.

Zero-Trust Examples: Cloud-based Application



5. Monitor and maintain the Zero-Trust environment

Zero Trust recap

- ❑ Continuously limit the blast radius of an attack to protect business continuity and limit the cost of it.

- ❑ Apply the concept of least privilege.
- ❑ Assume that breach is inevitable or has likely already occurred.
- ❑ Every transaction must be authenticated and authorized.

=> Zero Trust is not primarily a technology but a design process. Multipel technologies are required, and people and processes are equally important.

How can Orange Cyberdefense help?

Thanks

Lars-Göran Christiansson

Solution Architect

orange™ Cyberdefense