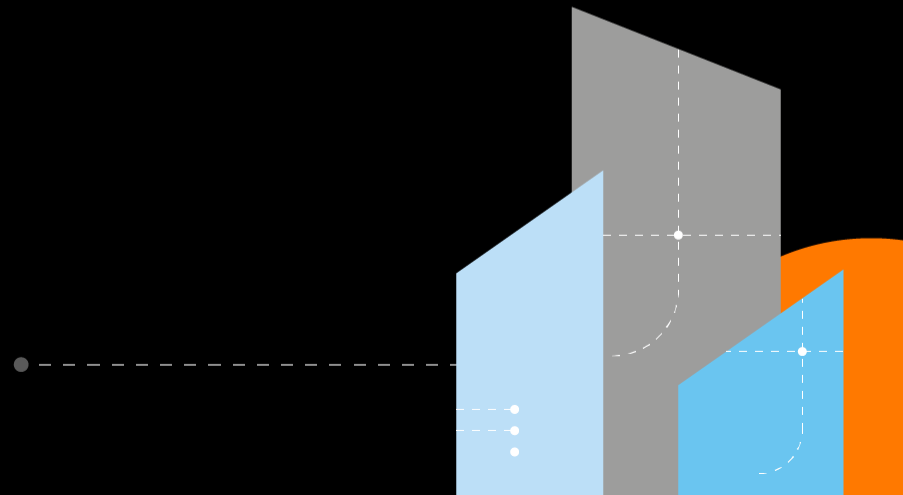
Orange
Cyberdefense

Zero trust Exempel 1

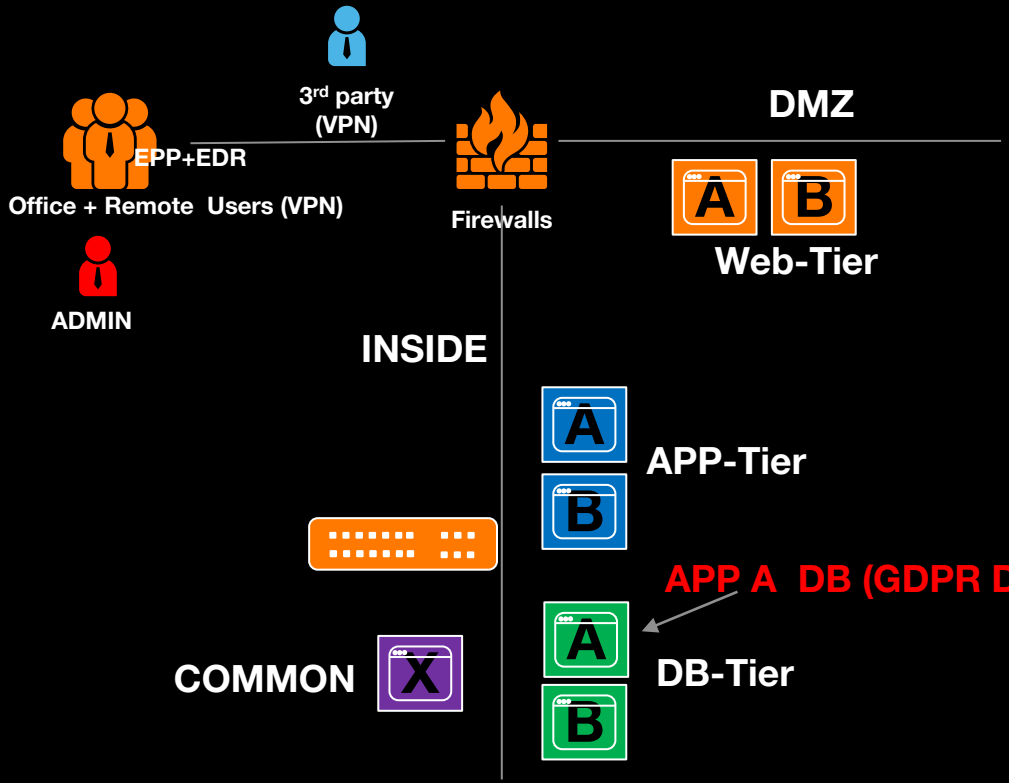
On-prem GDPR applikation

Lars-Göran Christiansson

Solution Architect



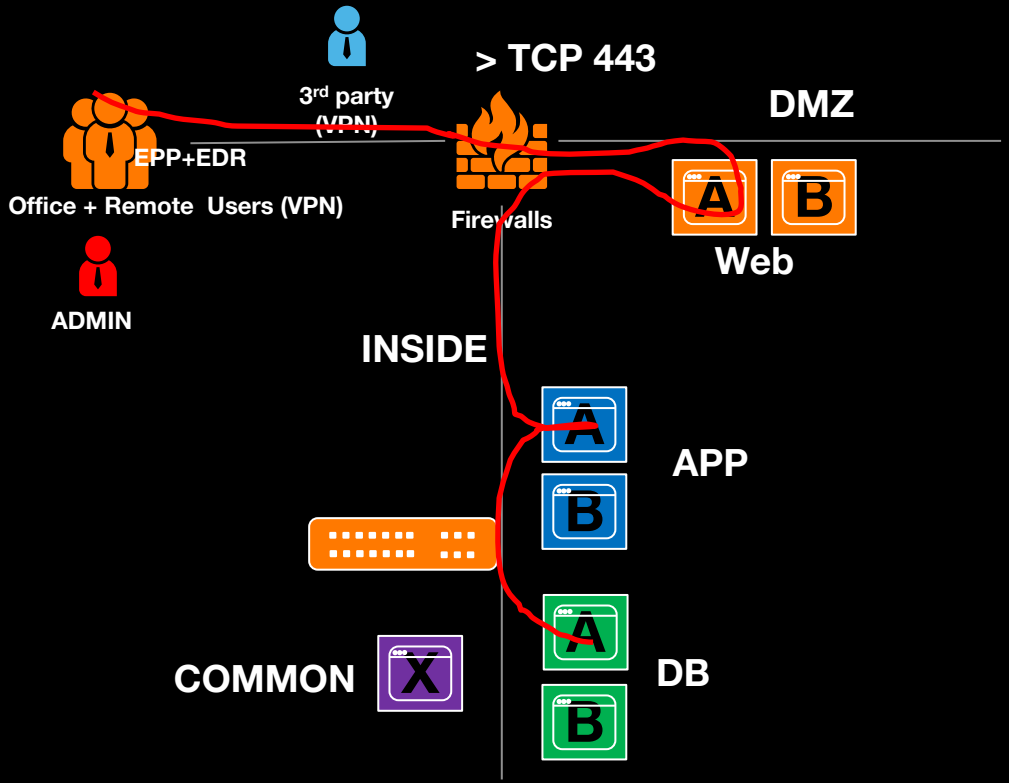
Zero-Trust example 1
On-prem legacy GDPR application A



1. Define the protection surface.

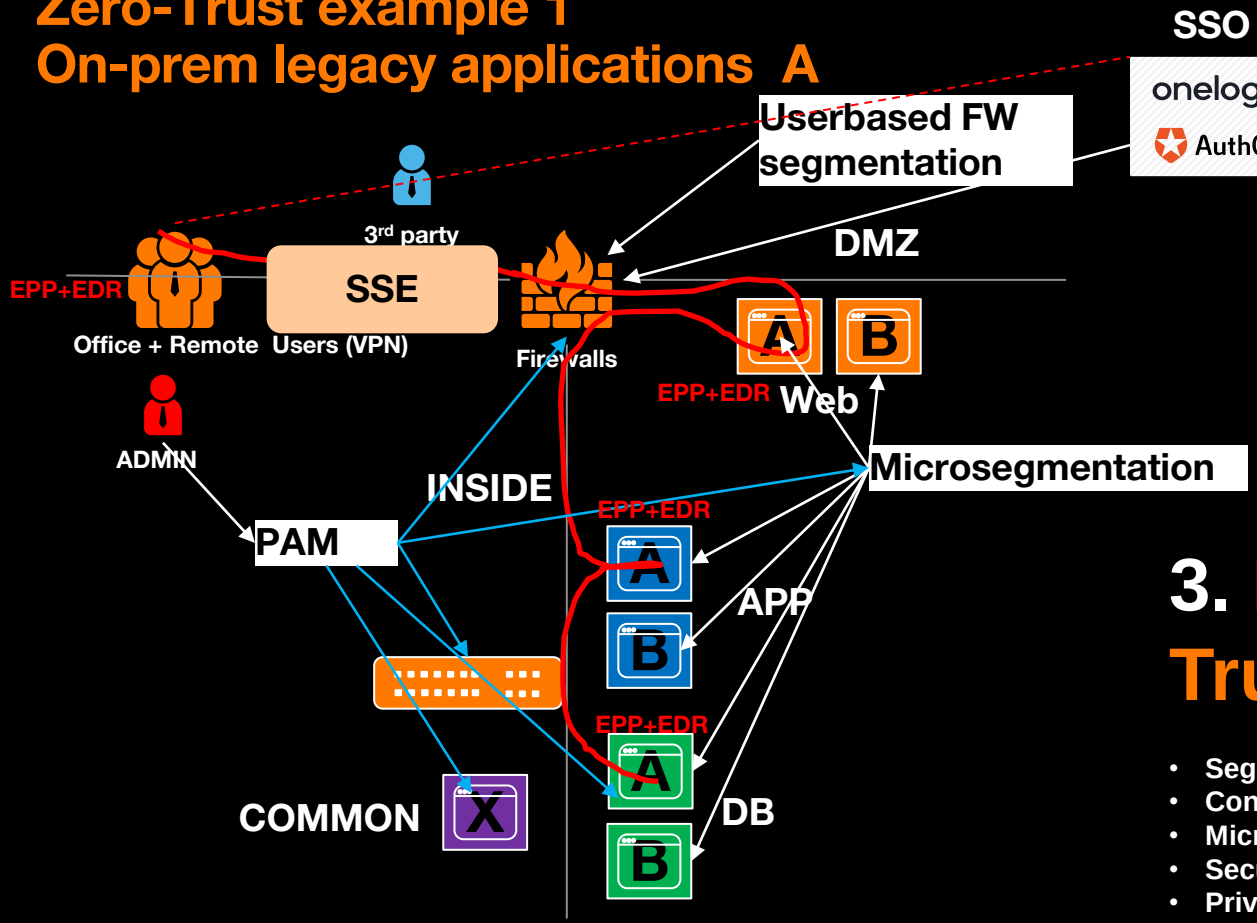
- Business custom built Application A with personal data

Zero-Trust example 1
On-prem legacy applications A



2. Map the transaction flows.

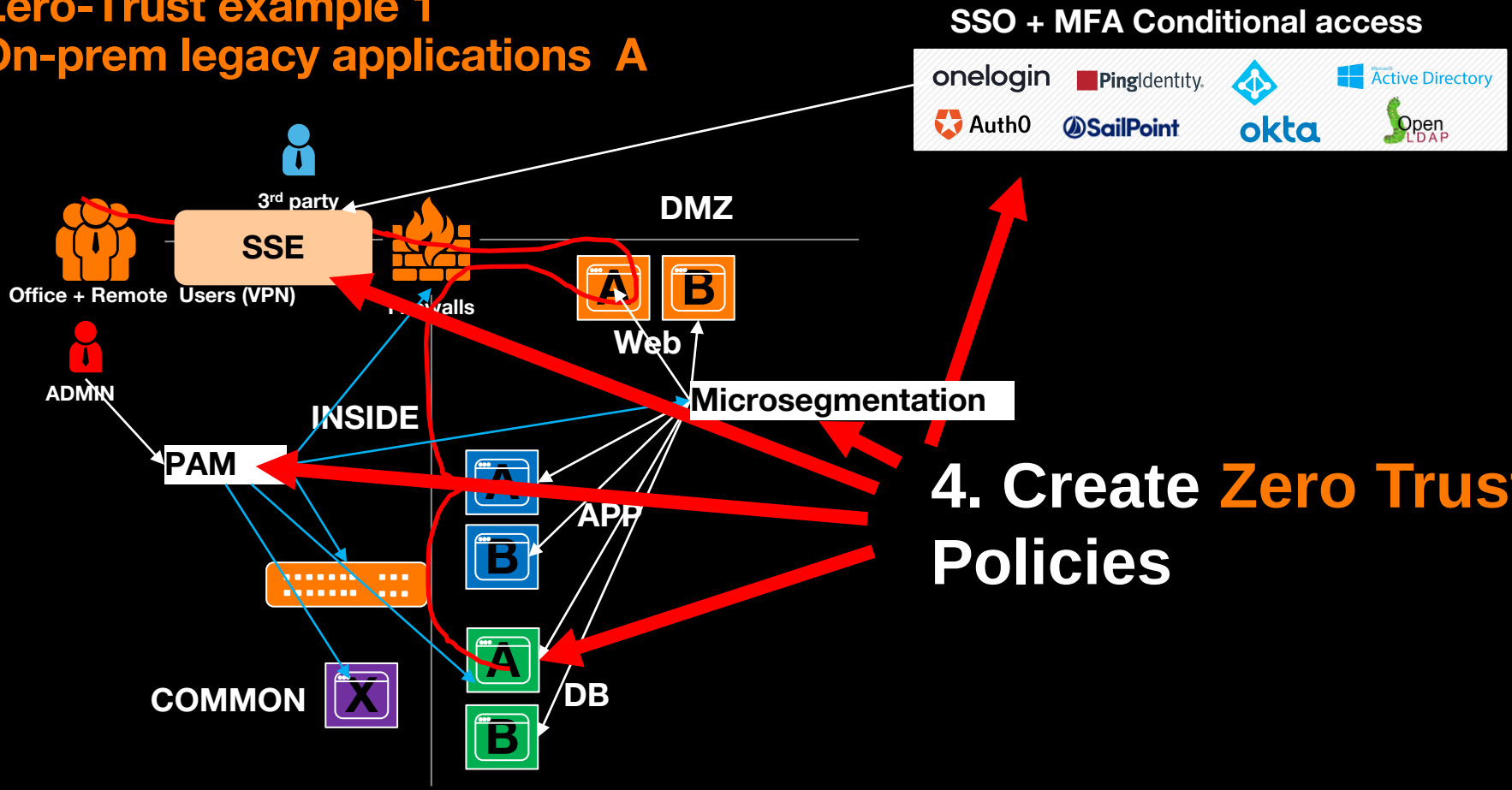
Zero-Trust example 1
On-prem legacy applications A



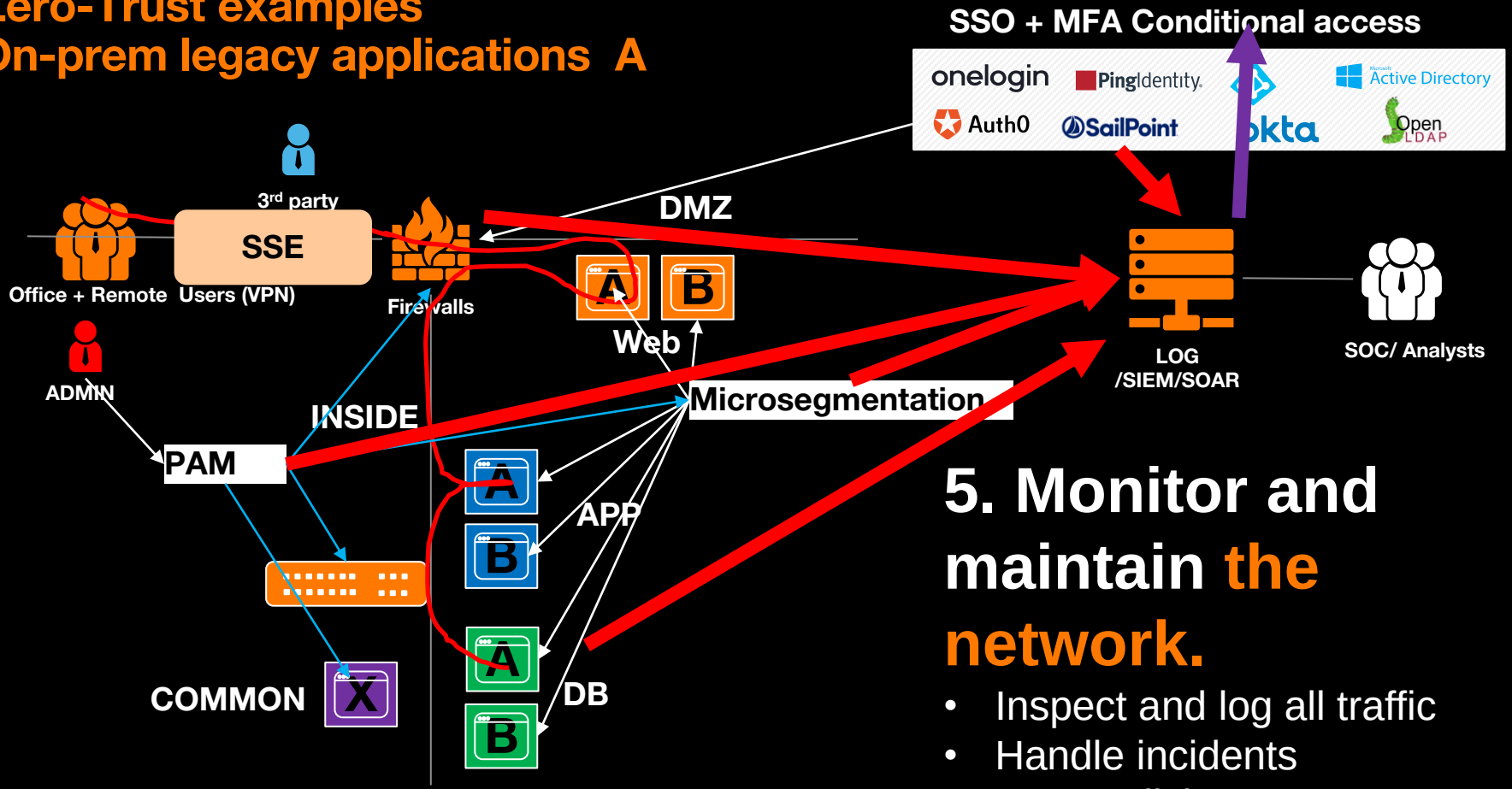
3. Build a Zero Trust architecture

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

Zero-Trust example 1
On-prem legacy applications A



Zero-Trust examples
On-prem legacy applications A



5. Monitor and maintain the network.

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

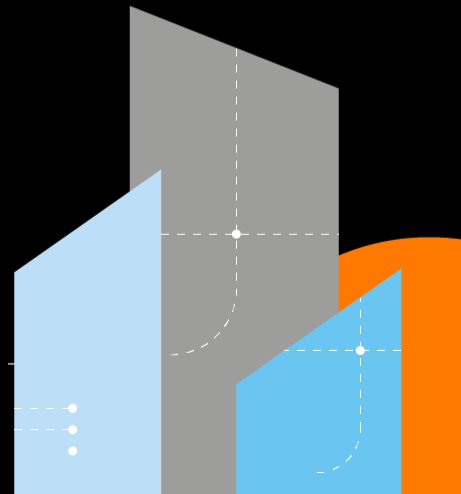
Orange
Cyberdefense

Zero trust Exempel 2

Public Cloud baserad Applikation

Marcus Hilmersson/Lars-Göran Christiansson

Solution Architect



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

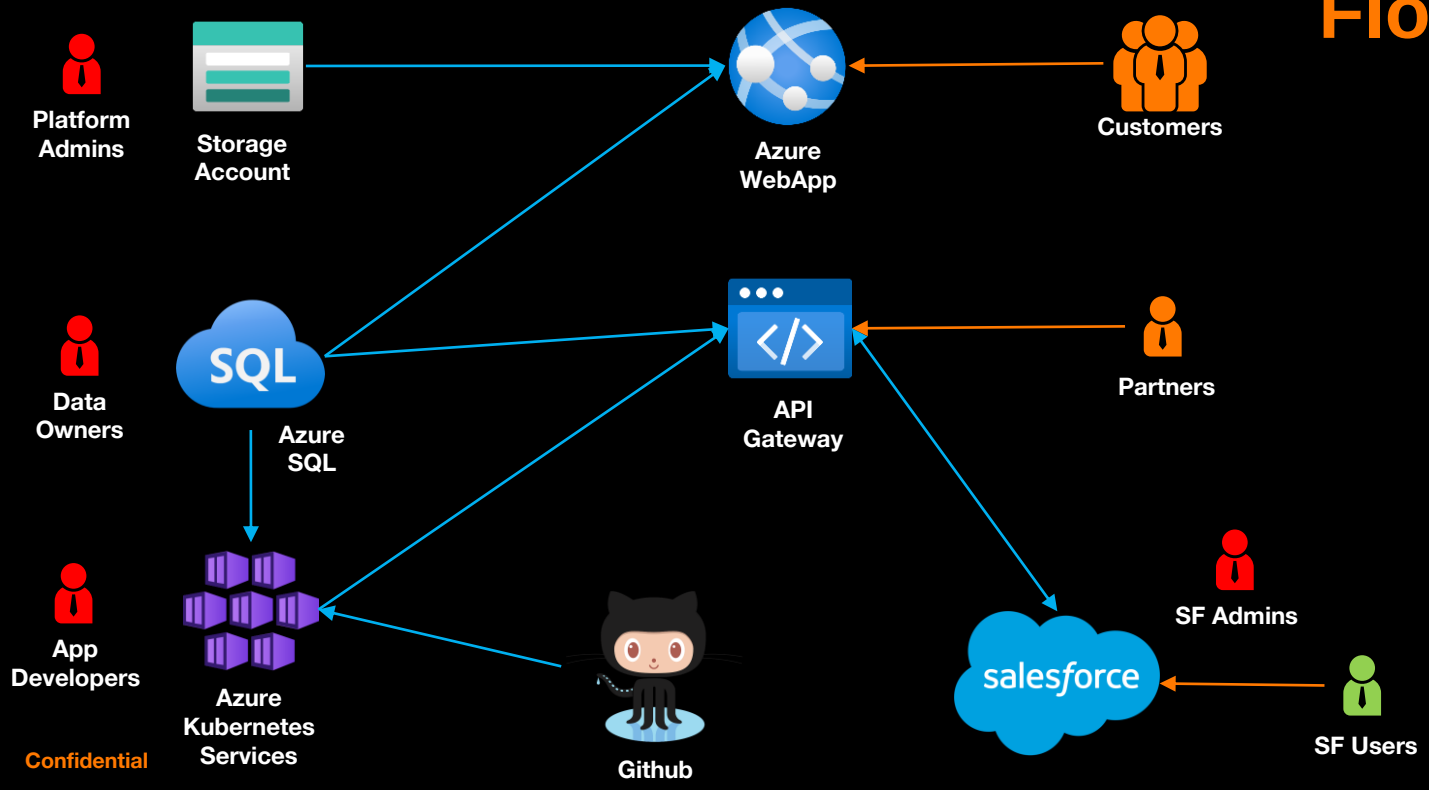
SF Admins

Service: SaaS
Type: Public
Data: Confidential

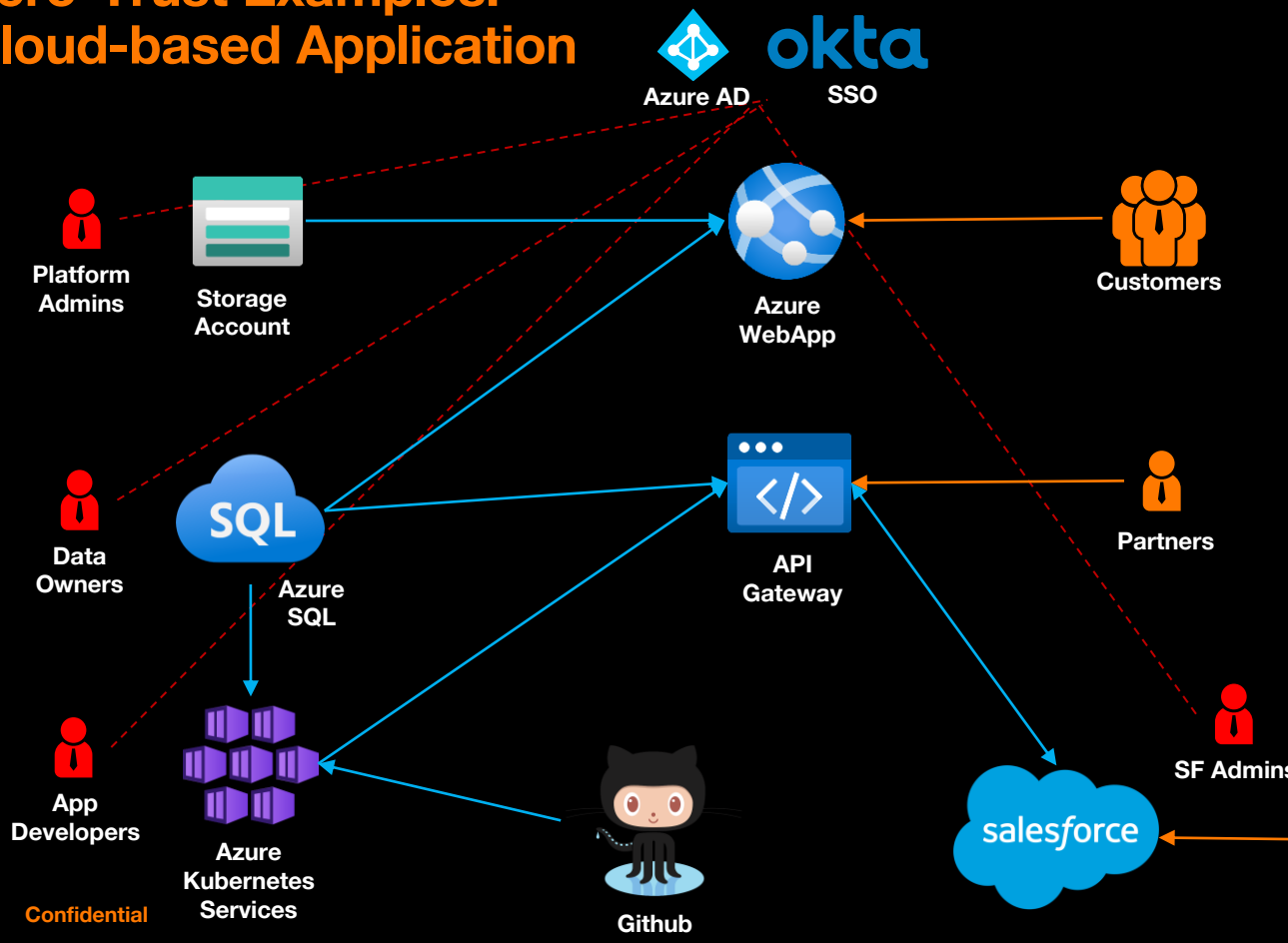
SF Users

Zero-Trust Examples: Cloud-based Application

2. Map Transaction Flows.



Zero-Trust Examples: Cloud-based Application



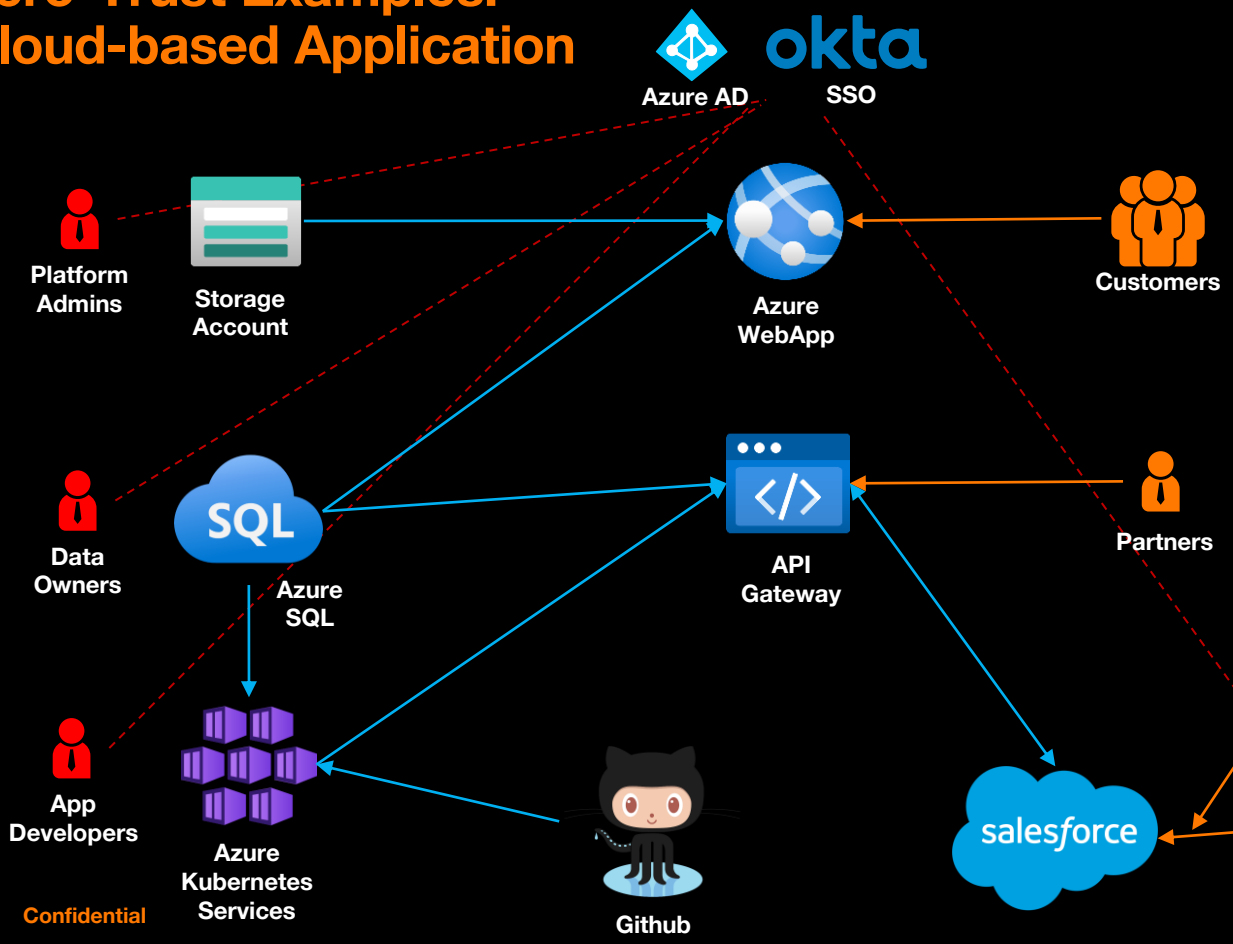
3. Build Zero-Trust Architecture.

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.

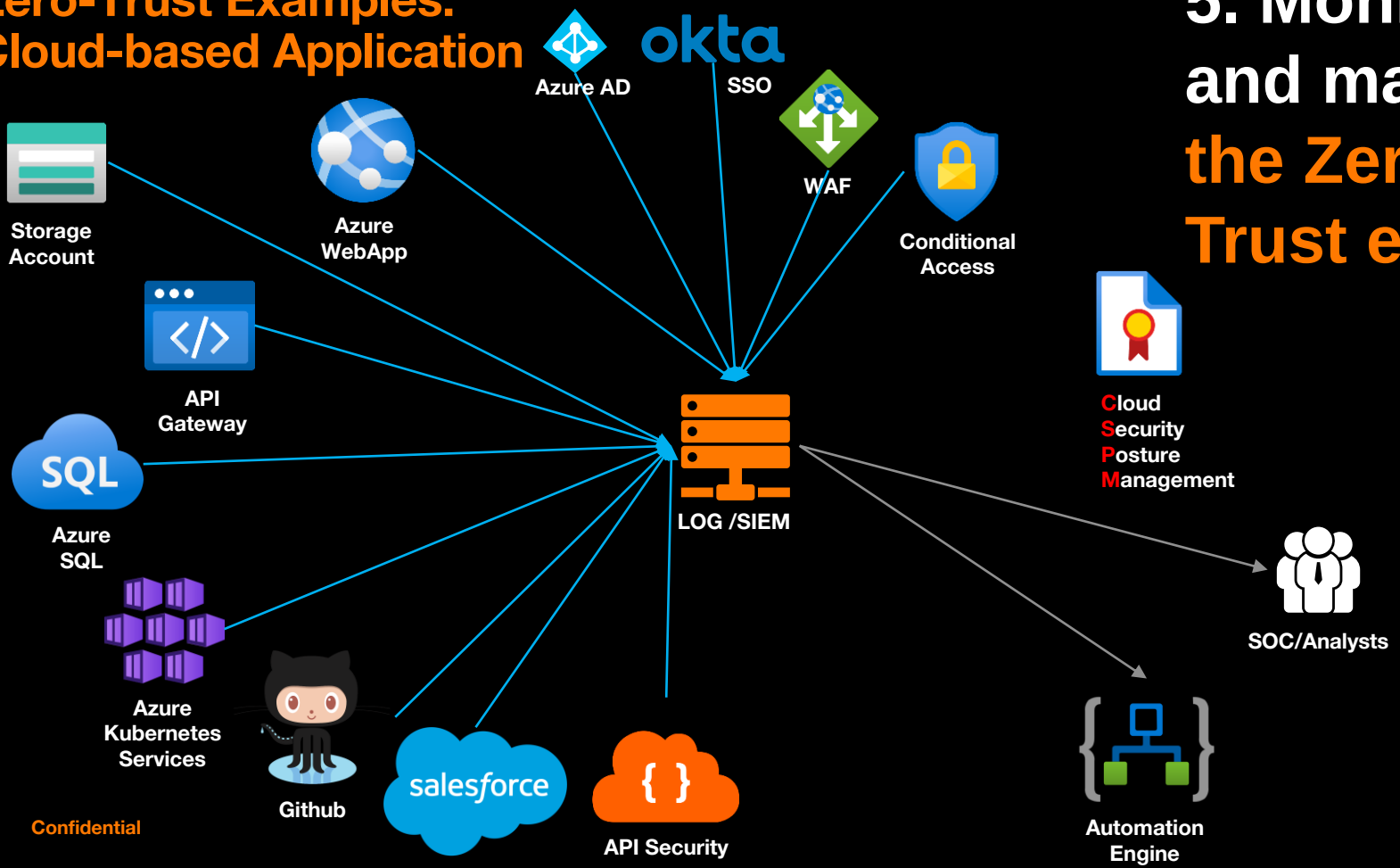
Emphasis on:

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



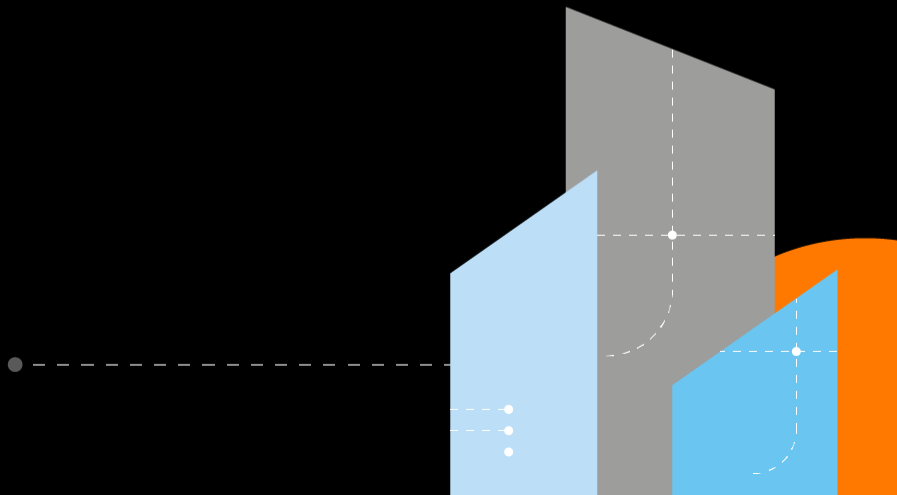
5. Monitor and maintain the Zero-Trust env.

Orange
Cyberdefense

Zero trust Demo 1

SSE – Secure Service Edge

Netskope

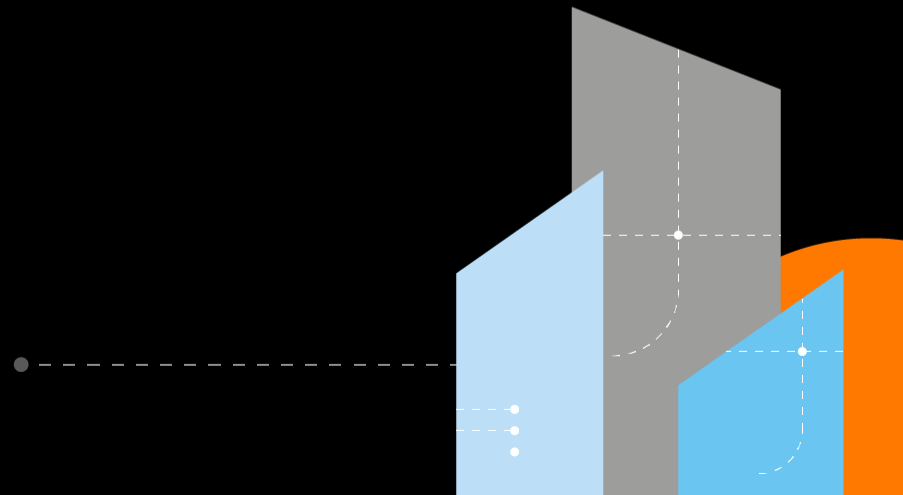


Orange
Cyberdefense

Kaffe !

14.30-15:00

Tillbaka 15:00 !

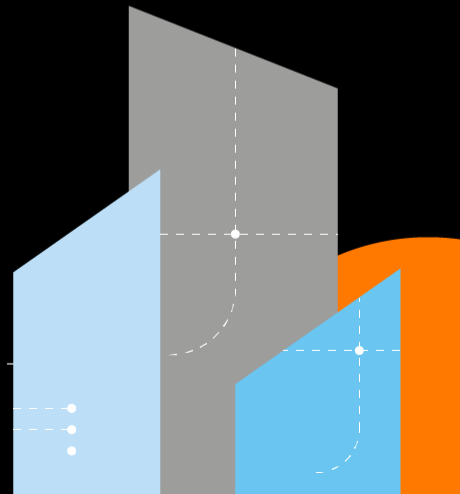


Orange
Cyberdefense

Zero trust Demo 2

Mikrosegmentering

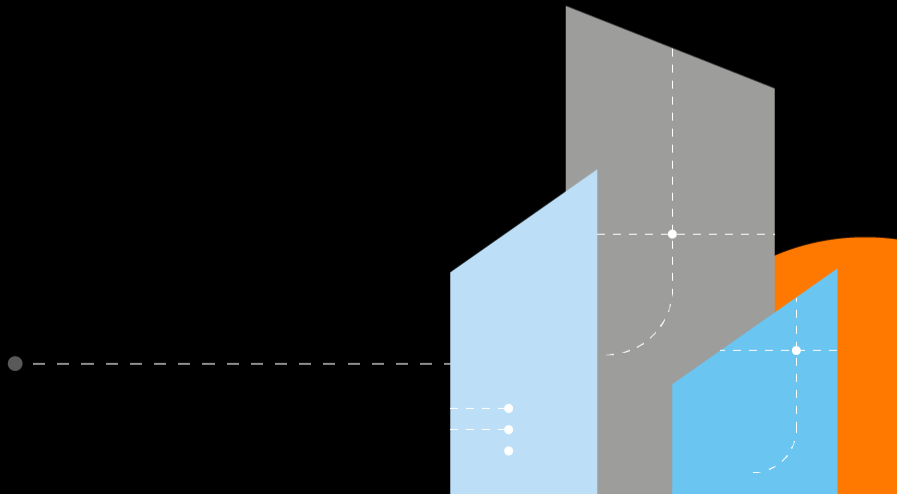
Akamai / Illumio



Orange
Cyberdefense

Recap
Diskussion
Q&A

ALLA



Zero Trust recap

- ❑ Syftet är att kontinuerligt och uthålligt öka motståndskraften och minska skadan vid attacker.

- ❑ 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 är inte i första hand teknologi utan en design process.
- Multipla teknologier behövs och en helhet med processer och personal är minst lika viktiga.

5 steps to implementing Zero Trust

1

Define the protection surface.

2

Map the transaction flows.

3

Build Zero Trust architecture.

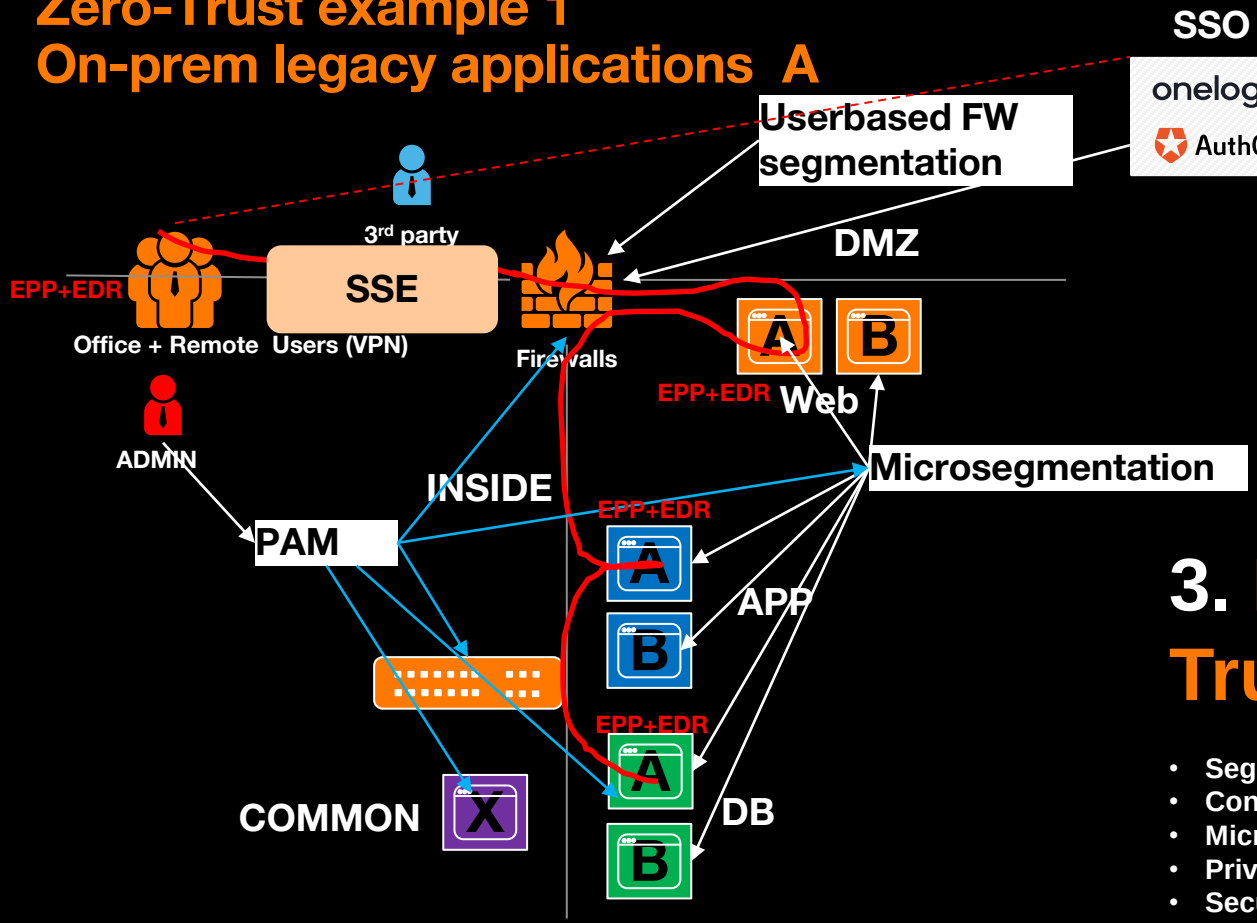
4

Create Zero Trust policy.

5

Monitor and maintain the network.

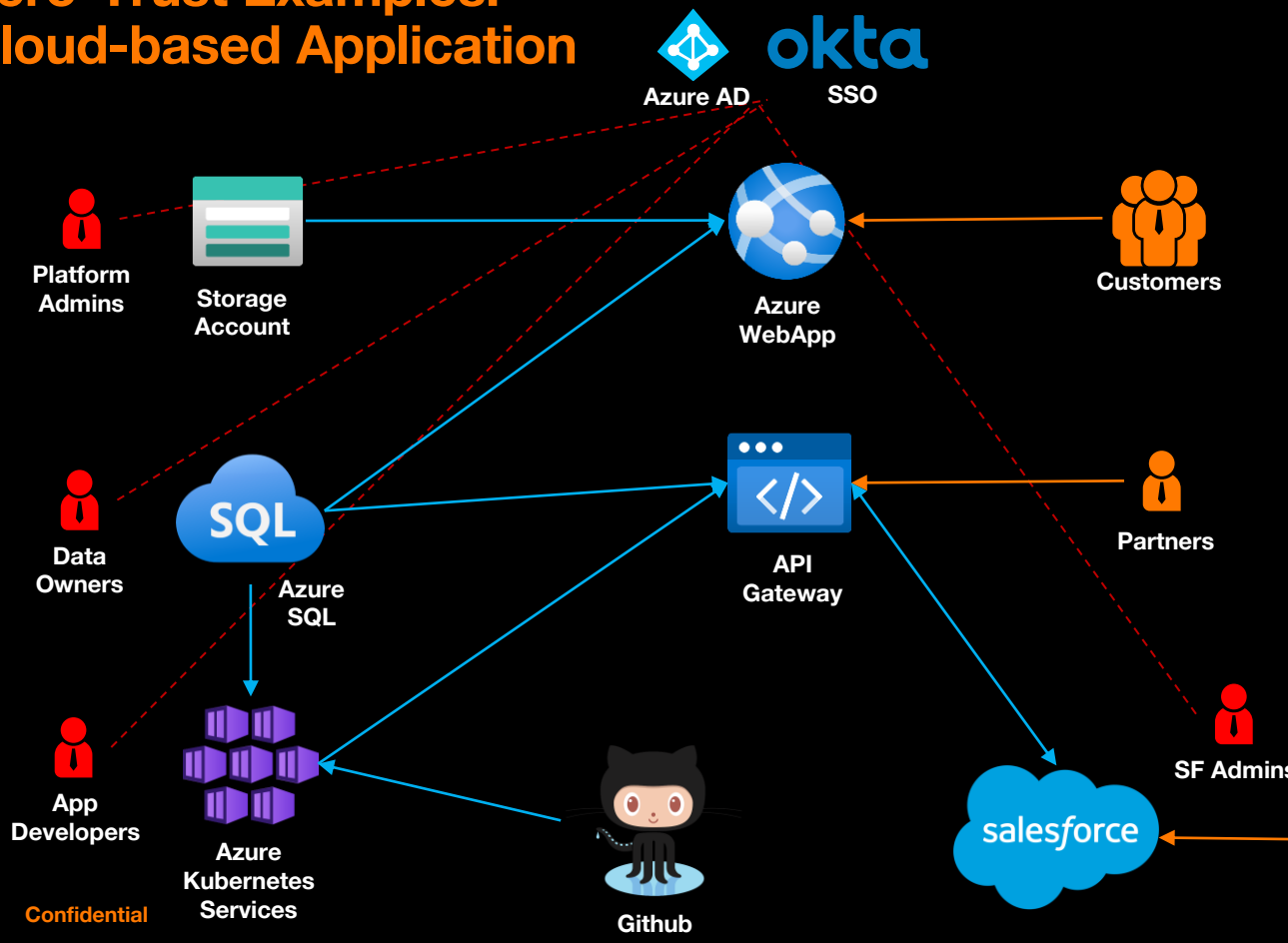
Zero-Trust example 1
On-prem legacy applications A



3. Build a Zero Trust architecture

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

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