



# Der Zero-Trust-Aspekt – Wie APEX-Apps sicher in der Cloud betrieben werden.

Timo Herwix, Senior Consultant
APEX Connect Conference 2023

# Who am I?

## Timo Herwix

- Senior Consultant at MT GmbH since 2019
- Previously worked as a Data Warehouse Developer
- Oracle APEX since 2016
- Oracle Databases since 2008
- Blog author, conference speaker
- Born in 1983, two children and living in Germany

Oracle ACE Associate

# Facts and figures.

Your partner for digital transformation.
Individual IT solutions from one single source.

Foundation 1994

**Headquarter**
Ratingen
**Branches**
Frankfurt am Main,
Köln, München, Hamburg

> 360 Employees

approx. 48 Mio. €
Turnover in 2021

> 125 Customers
Cross-sector

Manufacturer-neutral

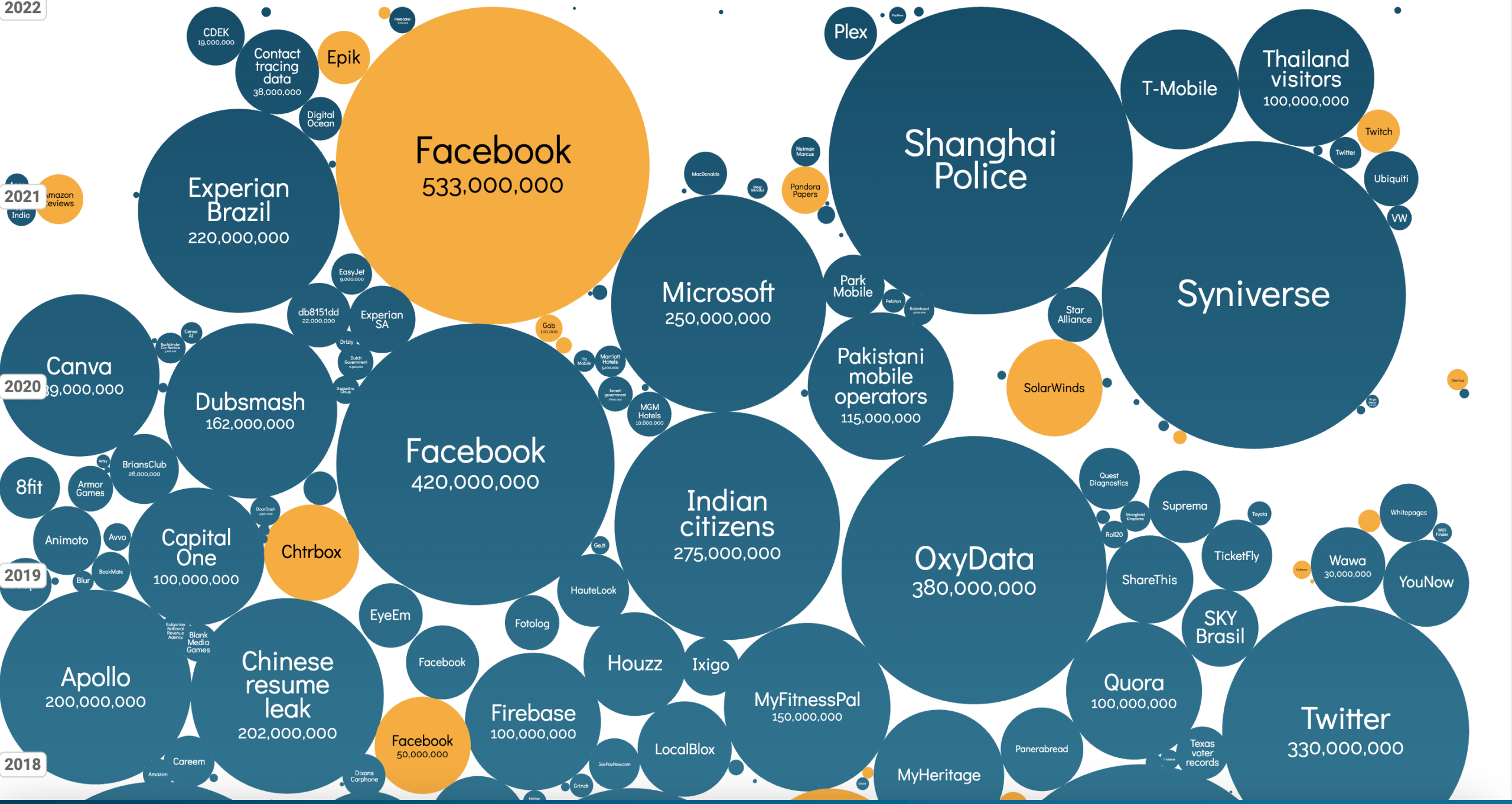
Certified partner
leading technology
manufacturer

Training company,
Partner in dual studies

# Agenda.

- Zero Trust Security Overview
- Quick Start
- Wrap-up

Zero-Trust is a **security model** based on the principle of maintaining strict access controls and **not trusting anyone by default**, even those already inside the network perimeter.

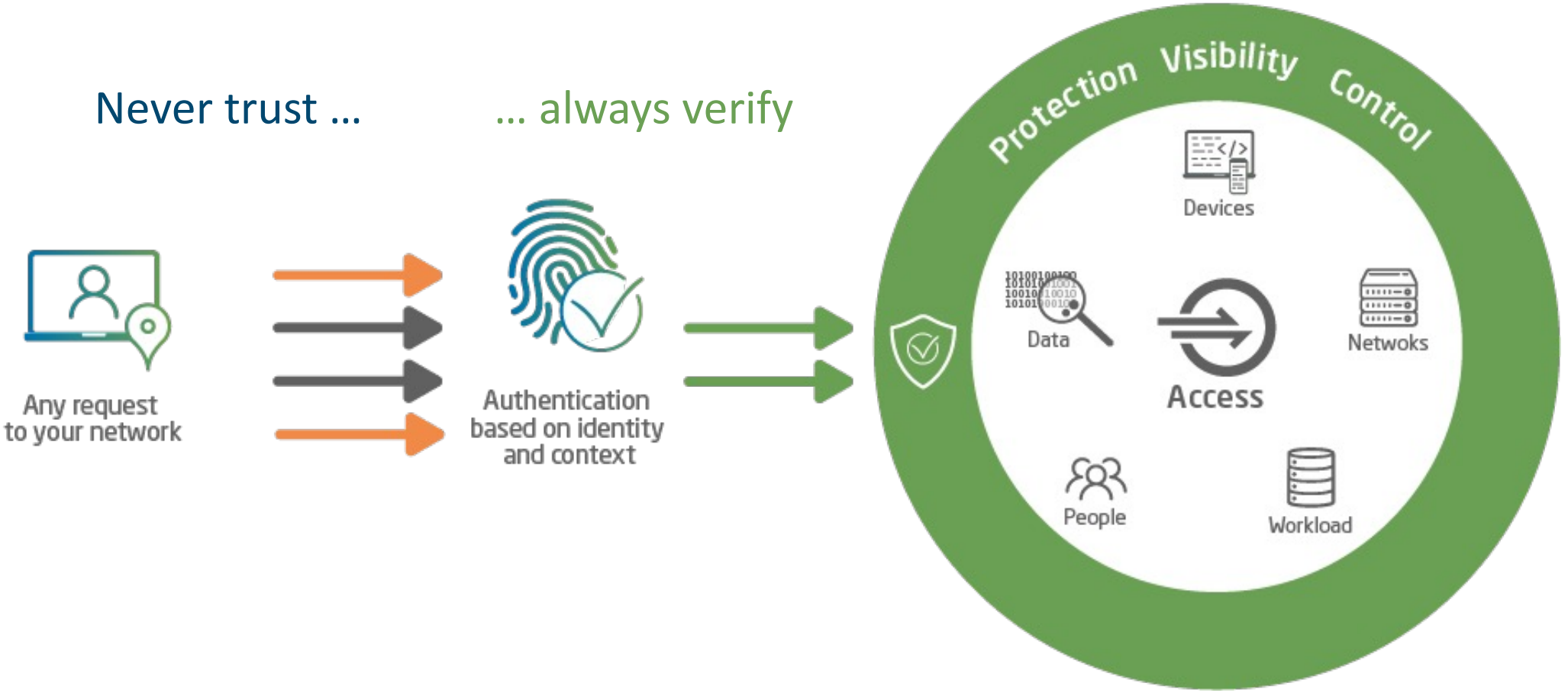

2022
2021
2020
2019
2018
CDEK 19,000,000
Contact tracing data 38,000,000
Epik
Digital Ocean
Facebook 533,000,000
Experian Brazil 220,000,000
Plex
Shanghai Police
T-Mobile
Thailand visitors 100,000,000
Twitch
Twitter
Ubiquiti
VW
Syniverse
Neiman Marcus
Pandora Papers
MacDonalds
Microsoft 250,000,000
Park Mobile
Peloton
Star Alliance
SolarWinds
Pakistani mobile operators 115,000,000
EasyJet 9,000,000
db8151dd 22,000,000
Experian SA
Gab 100,000
Marriott Hotels 5,200,000
MGM Hotels 10,500,000
Canva
Dubsmash 162,000,000
Facebook 420,000,000
Indian citizens 275,000,000
OxyData 380,000,000
Quest Diagnostics
Suprema
Roll20
ShareThis
TicketFly
Toyota
Whitepages
Wawa 30,000,000
YouNow
SKY Brasil
BriansClub 26,000,000
8fit
Armor Games
Animoto
Avvo
Blur
BookMate
Capital One 100,000,000
Chtrbox
DoorDash
HauteLook
Ge.tt
EyeEm
Fotolog
Houzz
Ixigo
Facebook
Apollo 200,000,000
Chinese resume leak 202,000,000
Blank Media Games
Firebase 100,000,000
Facebook 50,000,000
LocalBlox
MyFitnessPal 150,000,000
Quora 100,000,000
Twitter 330,000,000
Panerabread
Texas voter records
MyHeritage
Careem
Amazon
Dixons Carphone
Grindr

# Never trust …

… always verify

Never trust …

… always verify



Zero-Trust Security is not a product or a checkbox within an application.

**Zero-Trust** is a security concept that requires all users, **even those inside the organizations enterprise network**, to be **authenticated**, **authorized**, and continuously **validating** security configuration and posture, before being granted or keeping **access to applications and data**.

This approach leverages advanced technologies such as

- ✓ Multifactor-Authentication
- ✓ Identity and Access Management (IAM)
- ✓ Endpoint security technology

to verify the users identity and maintain system security.

# Shared Security Responsibility.

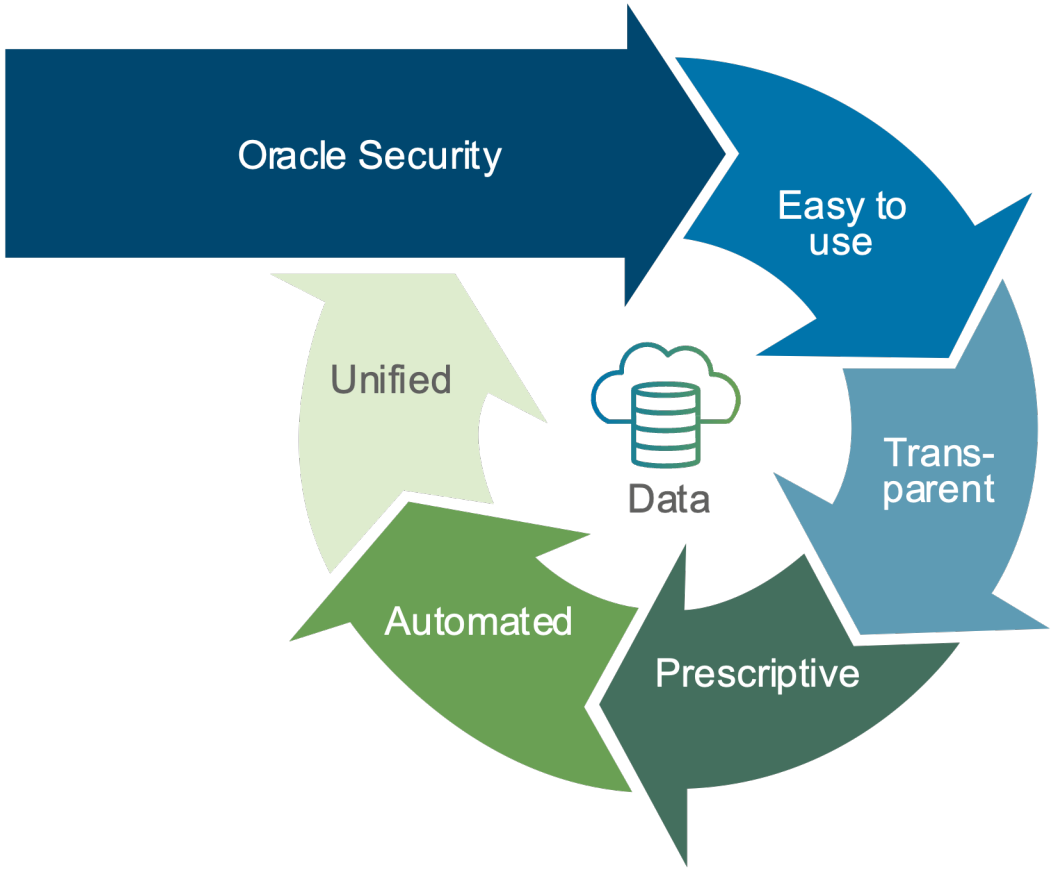
# Shared Security Responsibility Model.

| On-premise | Iaas<br>Infrastructure as a service | Paas<br>Platform as a service | Saas<br>Software as a service |
|---|---|---|---|
| User Access/Identity | User Access/Identity | User Access/Identity | User Access/Identity |
| Data | Data | Data | Data |
| Application | Application | Application | Application |
| Guest OS | Guest OS | Guest OS | Guest OS |
| Virtualization | Virtualization | Virtualization | Virtualization |
| Network | Network | Network | Network |
| Infrastructure | Infrastructure | Infrastructure | Infrastructure |
| Physical | Physical | Physical | Physical |

Service consumer responsibility

Service provider assistance

# Shared Security Responsibility Model.




## Security principles and customer benefits

- Simple: Reduces learning curve
- Transparent: Always on security posture
- Prescriptive: Guardrails minimize errors
- Automated: Reduces workload and human error
- Unified: Full stack view across platform tool

## Results

- Shifts the security burden from the customer
- Eliminates cost versus security trade-offs

# What are the benefits/challenges of Zero-Trust Security?

# Benefits of Zero-Trust Security.

Security extended beyond single network locations

Simple collaboration with an environment-agnostic model

Efficient threat detection and containment

Improved user experience and employee productivity

Long-term network security cost savings

Greater visibility and simplified compliance

Flexibility and adaptation

# Challenges of Zero-Trust Security.

Configuration issues with legacy tools

Excessive disruption

Mitigating insider threats

Security gaps from poor planning

# The 8 design principles of a Zero-Trust Architecture.

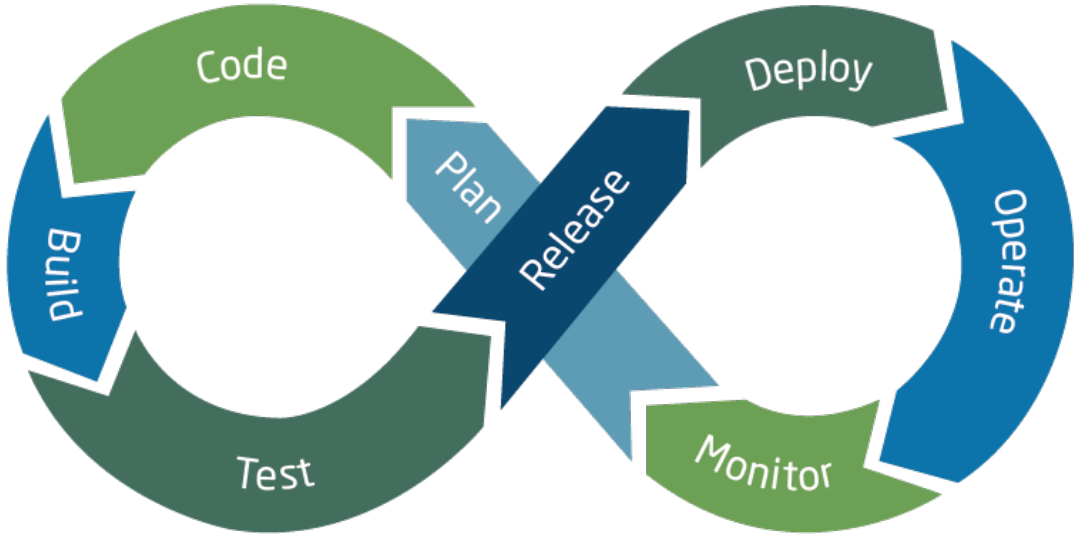
# 1.

# Know your architecture, including users, devices, services and data.

# Know your architecture, including users, devices, services and data.

**To get the benefits from Zero-Trust, you need to have a clear understanding about each component of your architecture so that you can identify:**

- Where your key resources are
- The main risks to your architecture
- How to avoid integrating legacy services that do not support Zero-Trust

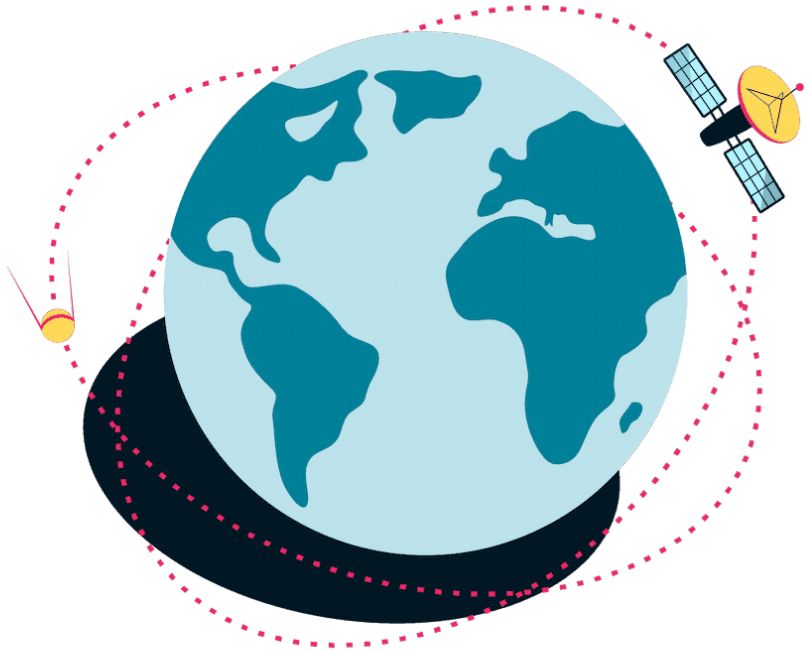


# Discover your assets.

REST API/CLI/SDK: Enumeration through programmatic access to OCI tenancy, tagging

Auditing: Understand the calls to all supported OCI public API endpoints giving visibility into what, who, when, how

Terraform: Build Infrastructure-as-Code scripts based on the existing deployed footprint



# 2.

# Know your user, service and device identities.

# Know your user, service and device identities.

**Each identity should be uniquely identifiable in a Zero-Trust architecture!**

**An identity can represent a:**

- User (human)
- Service (Software Process)
- Device

Identity is the core tenet of this principle!

# Identity Key Capabilities.

Cloud Directory

Identity Lifecycle Management


API Security

MFA


Adaptive Authentication


Single Sign On

# 3.

## Assess user behaviour, service and device health.

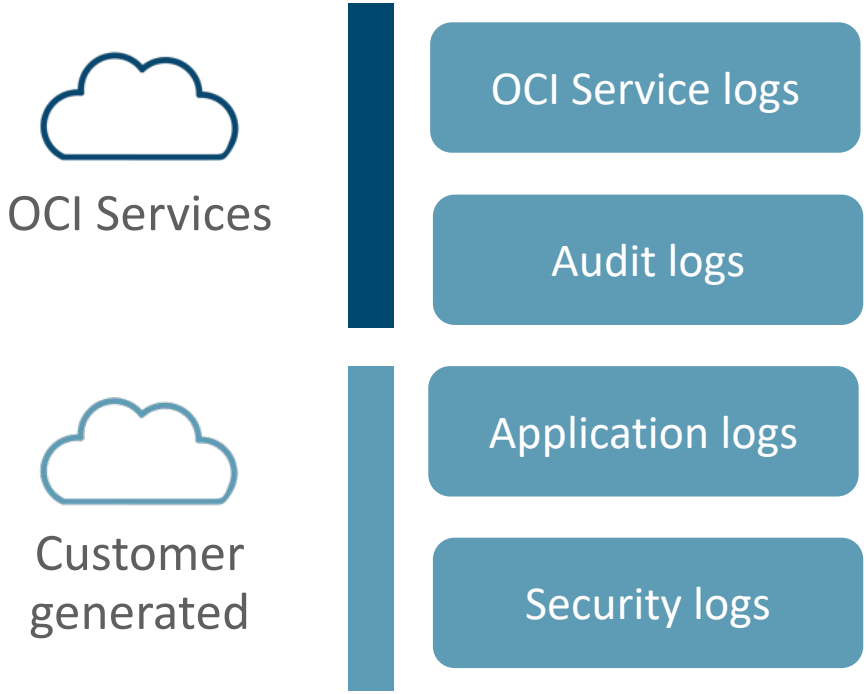
# Assess user behaviour, service and device health.

The most important indicators when looking to establish confidence in the security of your systems are:

- User health
- Service health
- Device health

Zero-Trust policy engines need to be able to measure user health, device health and service health.

## Collect and Manage



# 4.

# Use policies to authorise requests.

## Coarse-grained authorization.

*Does the user have access to this application?*

## Fine-grained authorization.

*What a user is authorised to do within an application or service?*

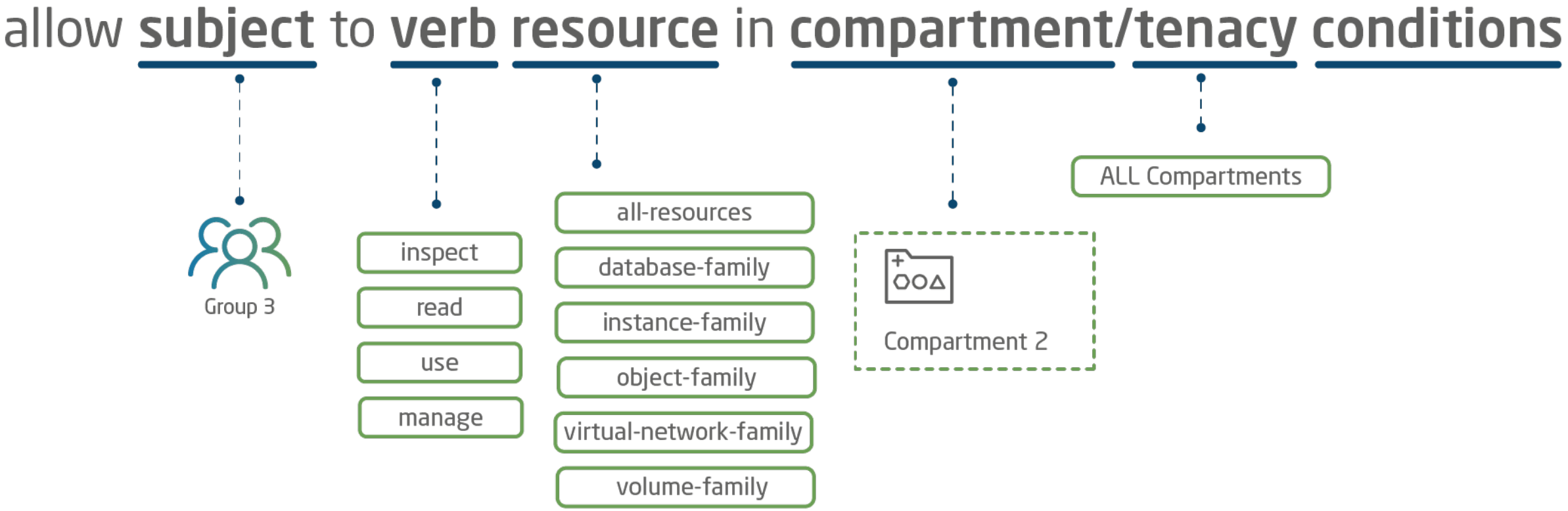
# Use policies to authorise requests.

**The power of a Zero-Trust architecture lies in the defined access policies. Each request for services or data should be authorised against a specific security policy.**

The key characteristics of a policy engine in a zero trust architecture:

- Uses multiple signals
- Provides a secure and flexible access control mechanism
- Adapts to the resources being requested

# Use policies to authorise requests.



# 5.

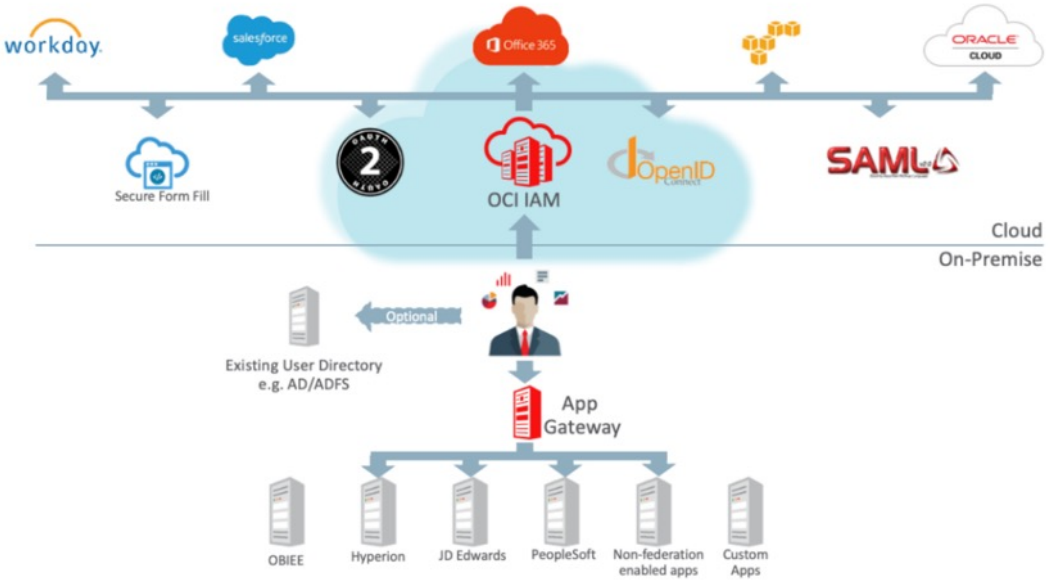
# Authenticate and authorise everywhere.

# Authenticate and authorise everywhere.

**Network is hostile**

- Authenticate all connections that access data or services.
- Requests between services also need to be authenticated

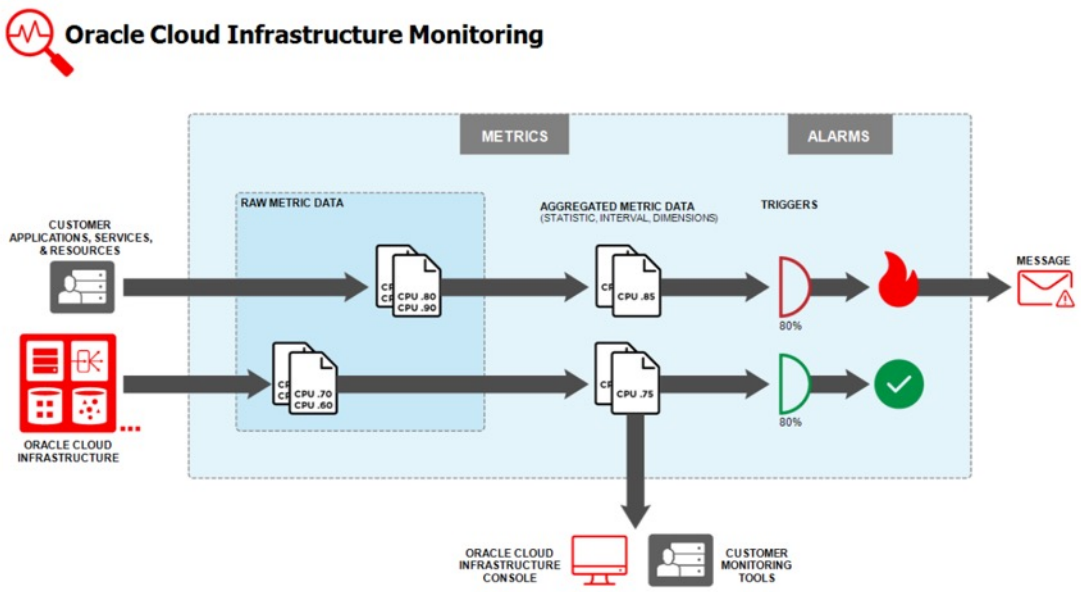
Adaptive and strong authentication must not hinder the usability of a service



# 6.

# Focus your monitoring on users, devices and services.

# Focus your monitoring on users, devices and services.




**Comprehensive and continuous monitoring is a good cyber hygiene to identify indicators of compromise.**

- Logging and monitoring to identify patterns of activity on your networks – "Who did what and when?"
- Continuously collect key metrics from various resources
- Trigger automated alarms and remediations when some abnormal activities happen

# 7.

# Don’t trust any network, including your own.

One of the OCI core design principles is a security-first approach, ensuring that security is built into the platform from the ground up and not bolted on as an afterthought.

# Security Design Principles.

| Principle highlights | Security Features |
|---|---|
| Security-first architecture | **Hardware-based Root of Trust** – mitigate server attacks and backdoor attacks<br>**Isolated Network Virtualization (INV)** – mitigate hypervisor attacks<br>**Hyper Segmentation, WAN encryption, TLS public endpoints, DDoS Protection** –mitigate network threats Supply Chain Security to enhance governance |
| Networking Controls | **OCI DNS** – Global anycast DNS Service with built-in layer 3 and 4 DDoS protection<br>**Security Lists & Network Security Groups** – Limit traffic flow through configurable rules & policies<br>**Gateways** – Internet, NAT, Dynamic routing, Service, Local peering<br>**OCI IAM** – Prevents unauthorized users from viewing and/or changing any network configuration<br>**Private & Public subnets** – Segregation of resources<br>**Private endpoints** – Control how traffic is routed from your VCNs subnet to destinations outside the VCN. |
| Monitoring Controls | **Cloud Guard, Web Application Firewall, Maximum Security Zones** as discussed in the earlier principles |

# 8.

# Choose services that have been designed for zero trust.

# Choose services that have been designed for zero trust.

- Do not reinvent the wheel
- Look for standards
- Managed services in the cloud

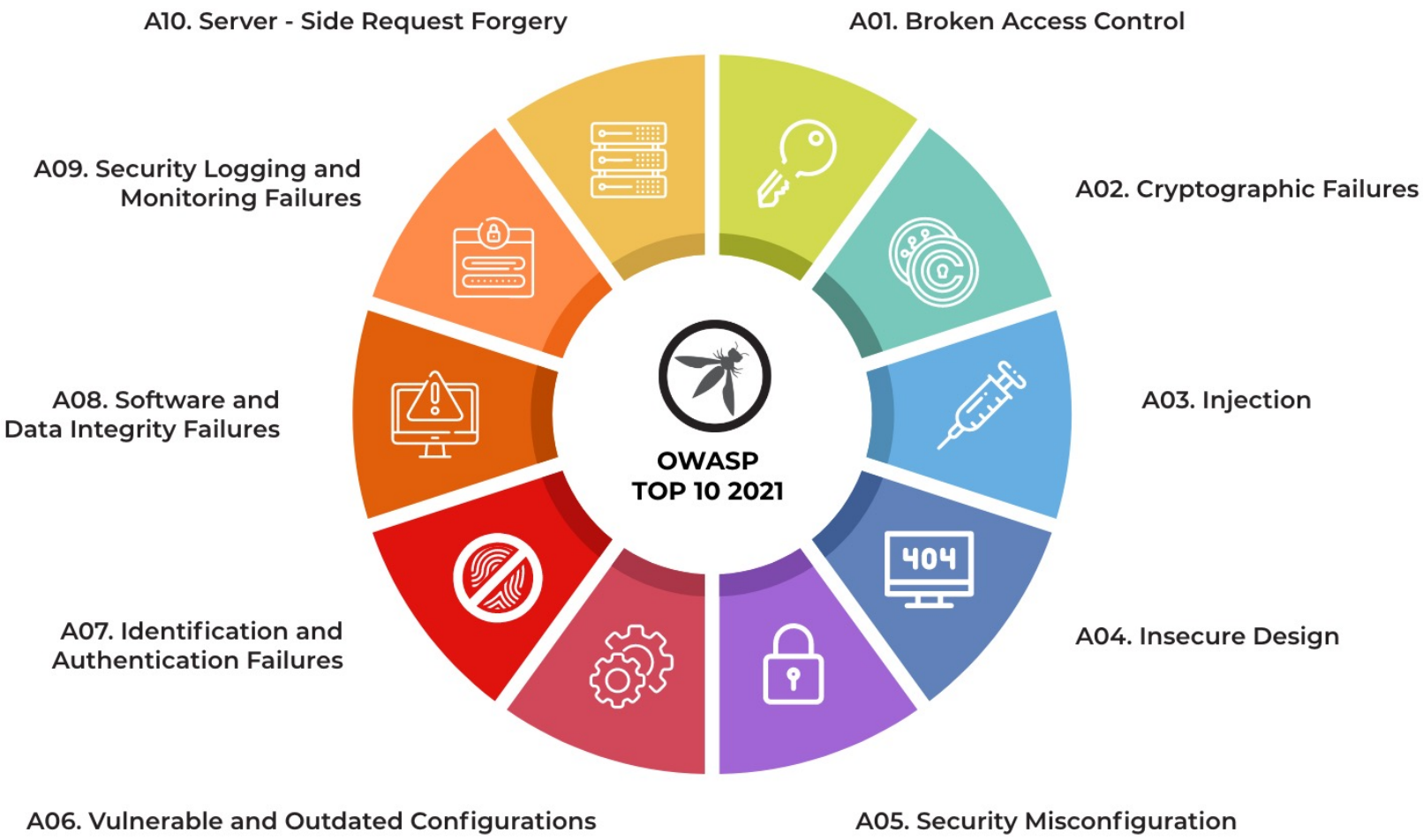
# What about APEX?

# Write good quality Code!

**“Quality is more important than quantity”**

*Steve Jobs*

# Top 10 Web application security risks.



# Social sign-in!

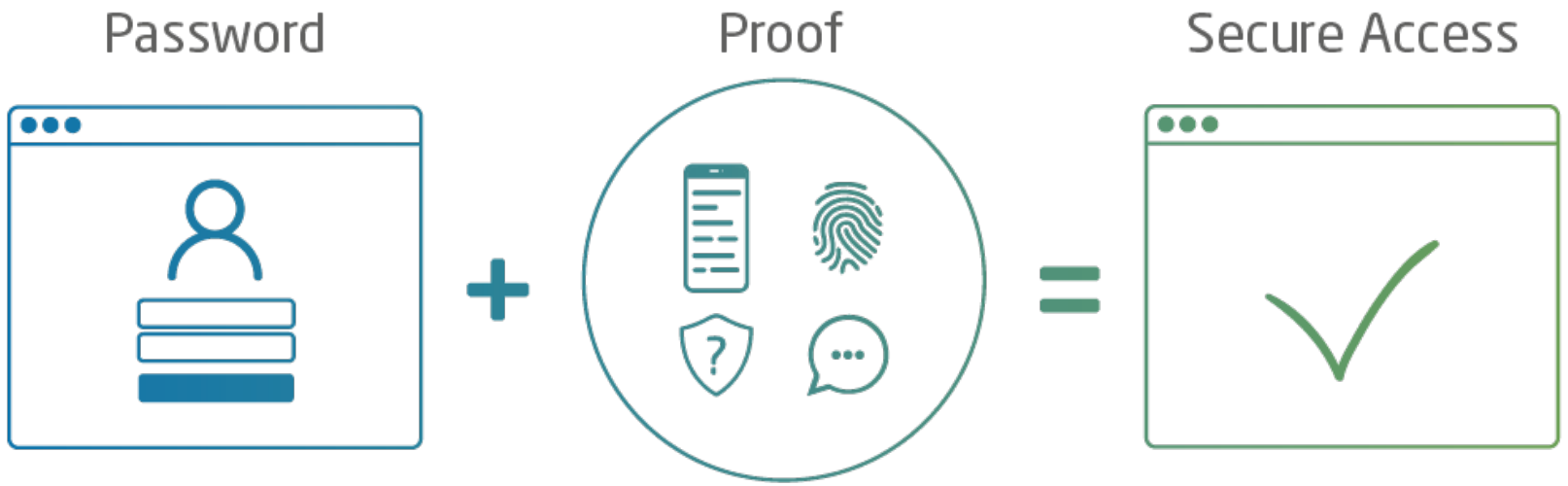
# Use OCI to access APEX.

## Single sign-on for everybody!

- Use the same username/password credentials as OCI
- OCI allows multi-factor authentication

## Get the most out of it!

- OCI has inbuilt reports auditing sign-on
- OCI can link to one or more third-party identity providers (e.g. Azure AD etc.) without additional code



By providing an extra barrier and layer of security that makes it incredibly difficult for attackers to get past, MFA can block over 99.9 percent of account compromise attacks.
With MFA, knowing or cracking the password won't be enough to gain access.

# Sign-on policy!

# Define your own sign-on rules.

The **identity providers** that will be used to authenticate

The **groups** that will be used to authenticate


The **frequency** that will be used to authenticate

# Passwordless authentication!

# Passwordless authentication.

# Passwordless authentication.

## Advantages

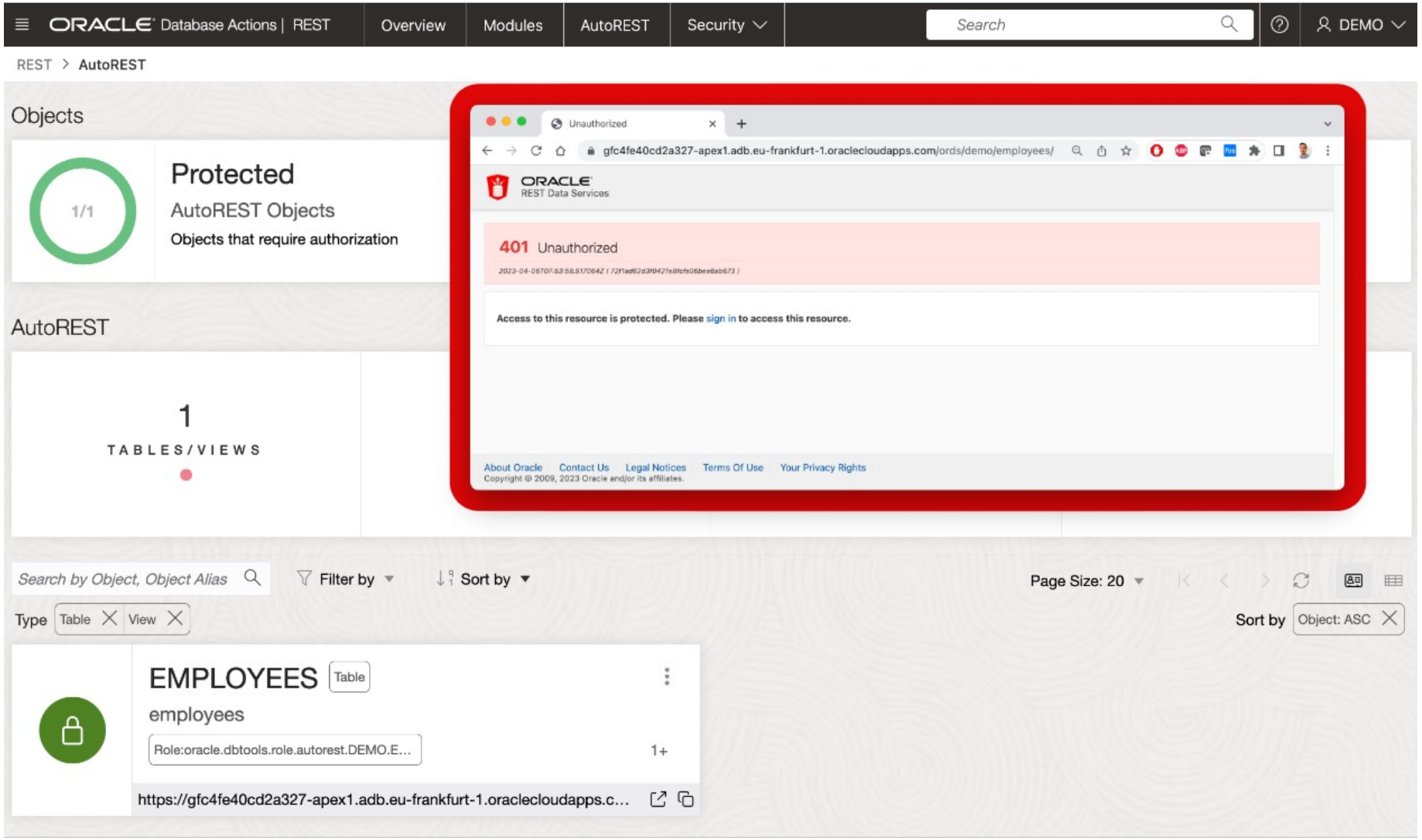
- Improved user experience and productivity
- Better or greater security
- Reduced helpdesk costs

## Disadvantages

- Dependency on the device or authenticator apps where you get your one-time password.
- Single point of failure if a user has only "mobile" factor configured. You can't login into applications if you do NOT have access to your mobile device where you get/see OTP and do push notifications (ex: device switch off, poor cell reception, lost or stolen).

# Securing Your REST-Service!

# Securing Your-REST Service!




# Network-Access-Control!

# Specify IP-addresses that are allowed to access.

## Network Perimeter!

If you or your VPN has a static IP-address, you can configure OCI to reject all connections from unknown IP-addresses.

Please note that there is a significant risk that you will be logged out if your static IP-address changes!!!

# Specify IP-addresses that are allowed to access.

## Access Control List!

The network access rules you create for an access control list provide protection for your autonomous database by allowing only the public and VCN IP-addresses in the list to connect to the database.

This adds an additional layer of security to your autonomous database.

# Wrap-up.

Zero-Trust is not a product to buy or a checkbox to enable within an application.

Instead, Zero Trust is an approach that takes time, effort, and investment to adopt.

# Wrap-up.

- OCI has security architected-in from the ground up using security-first design principles
- OCI provides always-on security to help secure our customers data
- Oracle shifts the security burden from the customers through automated services and embedded expertise
- OCI simplifies customers exercise of shared security responsibilities, leading to a Zero-Trust Security outcome.

# Zero-Trust comes without additional costs.

# Are you interested?

**Timo Herwix**
Senior Consultant

Telefon: +49 2102 30 961-0
Mobil: +49 176 20185455
Mail: timo.herwix@mt-itsolutions.com

**MT GmbH**
Balcke-Dürr-Allee 9
40882 Ratingen

www.mt-itsolutions.com

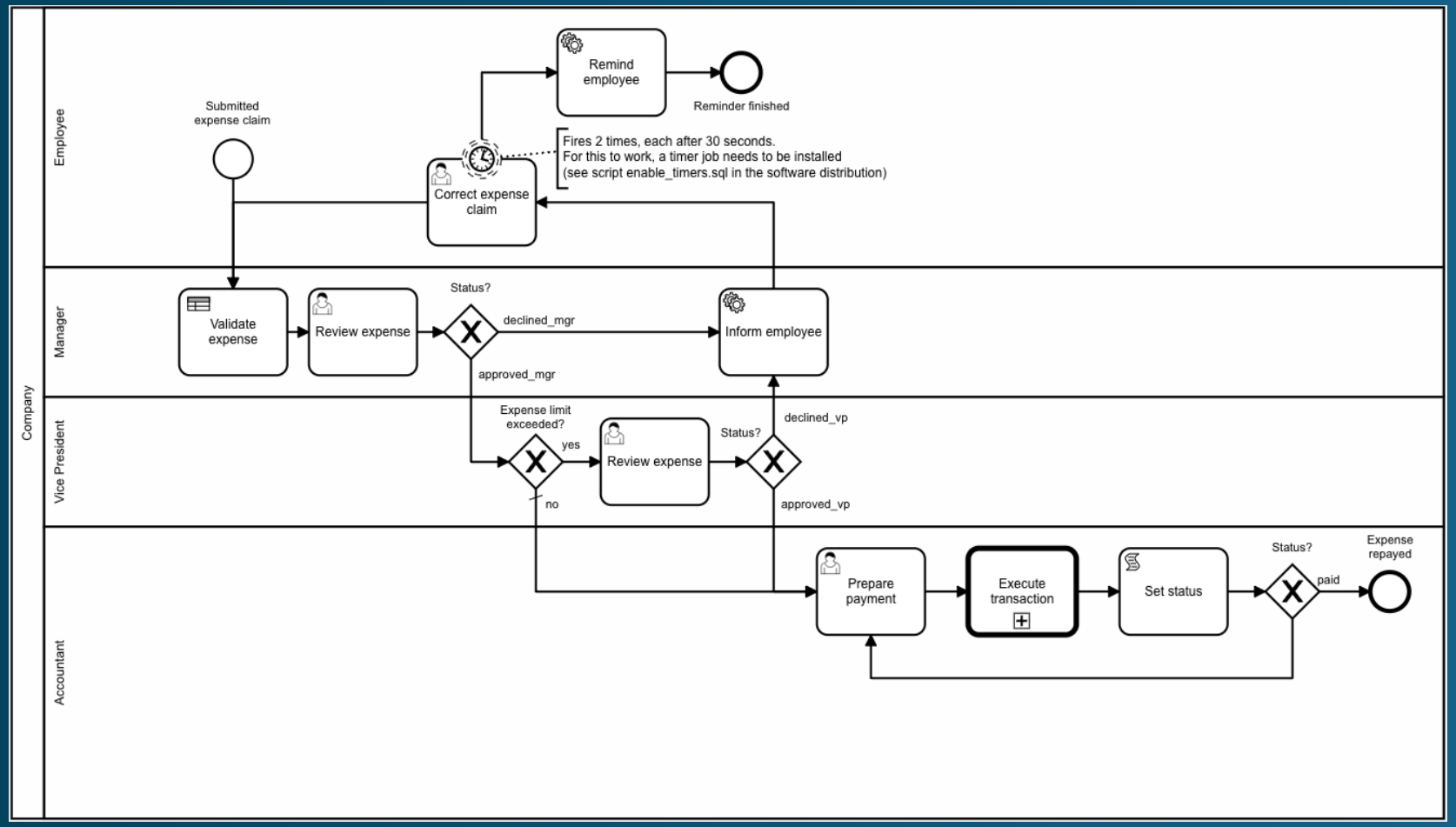
Timo Herwix

@Therwix

tm-apex.hashnode.dev

# Flows for APEX.

## BPMN 2.0 Workflows for APEX




- Open Source
- Community Driven
- Support available

# Testing APEX Apps is now as easy as creating them.


- Tailored to APEX
- Save a lot of time on regression tests
- Use our intuitive LCT-App and don‘t write any test code
- Testing on multiple platforms simultaneously

# Quellen.

- Seite 6: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Seite 32: Whitepaper „Approaching Zero Trust Security with Oracle Cloud Infrastructure“ von Oracle
- Seite 34: Whitepaper „Approaching Zero Trust Security with Oracle Cloud Infrastructure“ von Oracle
- Seite 42: https://owasp.org/www-project-top-ten/
- Seite 54: https://ndisac.org/dibscc/implementation-and-assessment/top-10-high-value-controls/perimeter-hardening/