



The Zero-Trust Security Model.

Mohamad Bouchi
Consultant

Who am I?

Mohamad Bouchi

Consultant at MT GmbH since 2022

Previously worked as a data warehouse developer

Oracle APEX developer since 2017

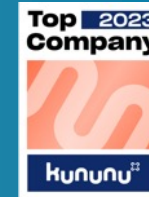
Blog author

Born in 1989



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.
- Challenges of Zero Trust Security.
- Zero Trust Security areas.
- Zero Trust Model in the Cloud.
- Wrap up.



Zero Trust Security Overview.

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.

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



Zero-Trust is a security concept and approach.

Zero Trust principles.



Verify explicitly



Use least-privilege access



Assume breach

Never Trust...



...always verify

Challenges of Zero-Trust security.

Why implementing the Zero trust security model is challenging?

Challenges of Zero-Trust security.



ZERO TRUST SECURITY
REQUIRES ONGOING
MANAGEMENT



ZERO TRUST SECURITY
IS NOT A TURNKEY
SOLUTION



COMPLEXITY



COMPANIES MUST
SECURE THEIR
HARDWARE

Zero Trust Security areas.

Challenges of Zero-Trust security.



IDENTITIES



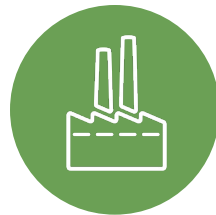
ENDPOINTS



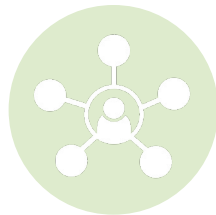
APPS



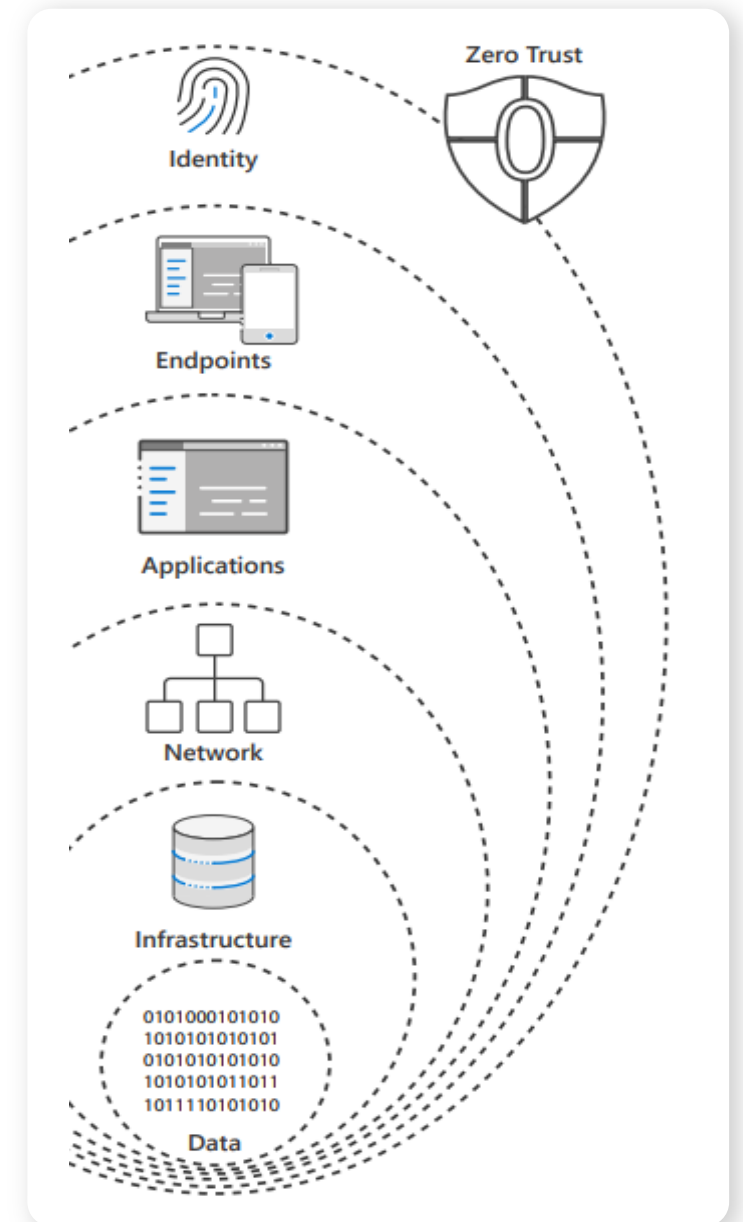
DATA



INFRASTRUCTURE



NETWORK



Zero Trust Model in the Cloud.

Shared Security Responsibility Model.

On-premise	IaaS Infrastructure as a service	PaaS Platform as a service	SaaS 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

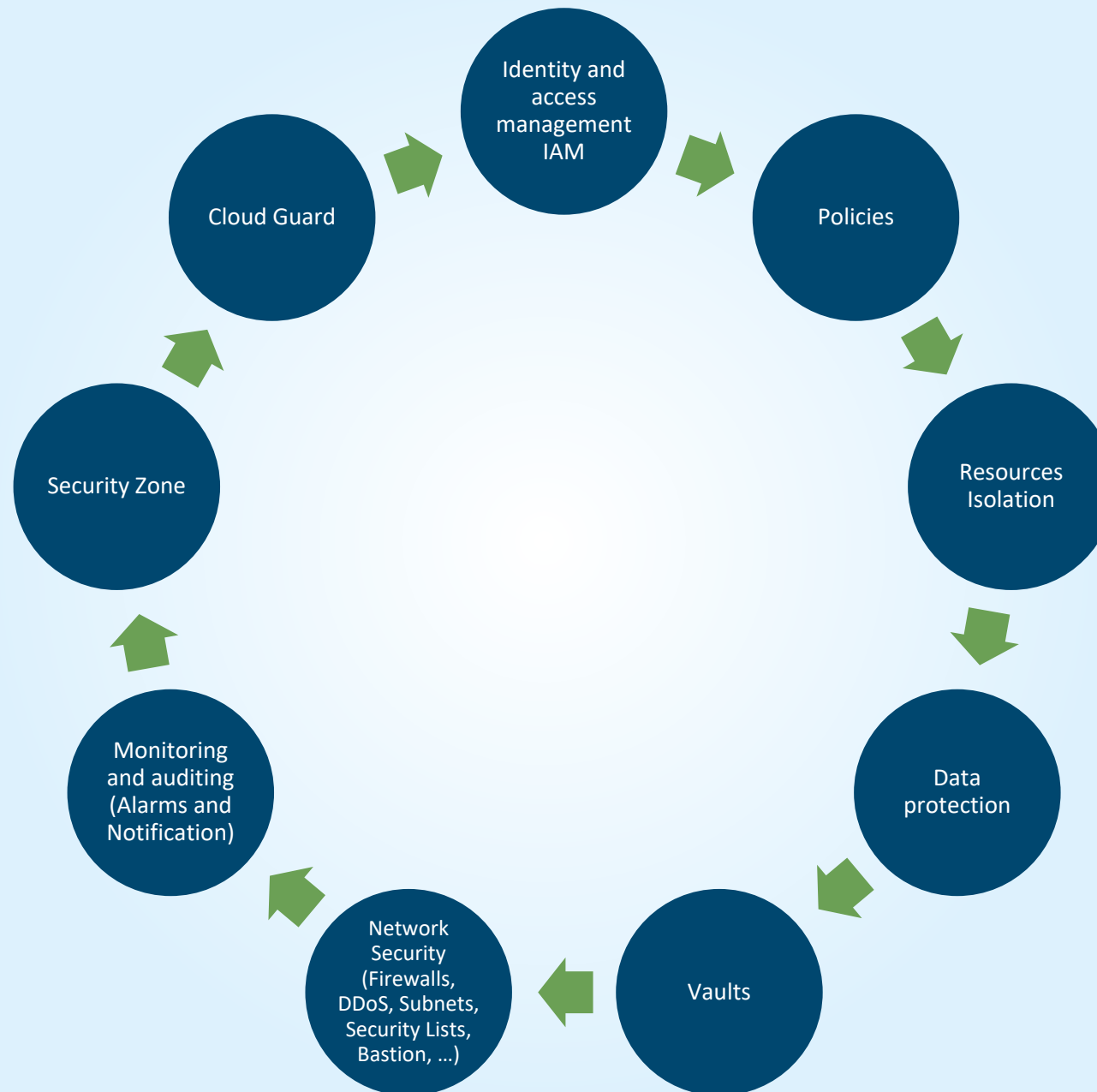


Service consumer responsibility




Service provider assistance

Services and Techniques.



Challenges of Zero-Trust security.



Identity and Access Management (IAM)

- IAM is a service that provides identity and access management features such as AuthN, AuthZ, SSO, and identity lifecycle management.
- AuthN – Who are you?
- AuthZ – What permissions do you have?



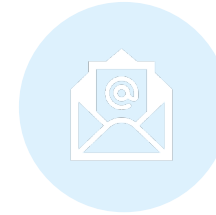
SECURITY QUESTION



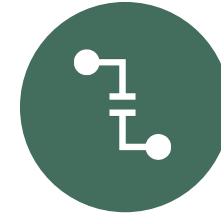
MOBILE
AUTHENTICATOR
APPLICATION



TEXT MESSAGE



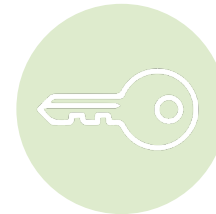
EMAIL



BYPASS CODE

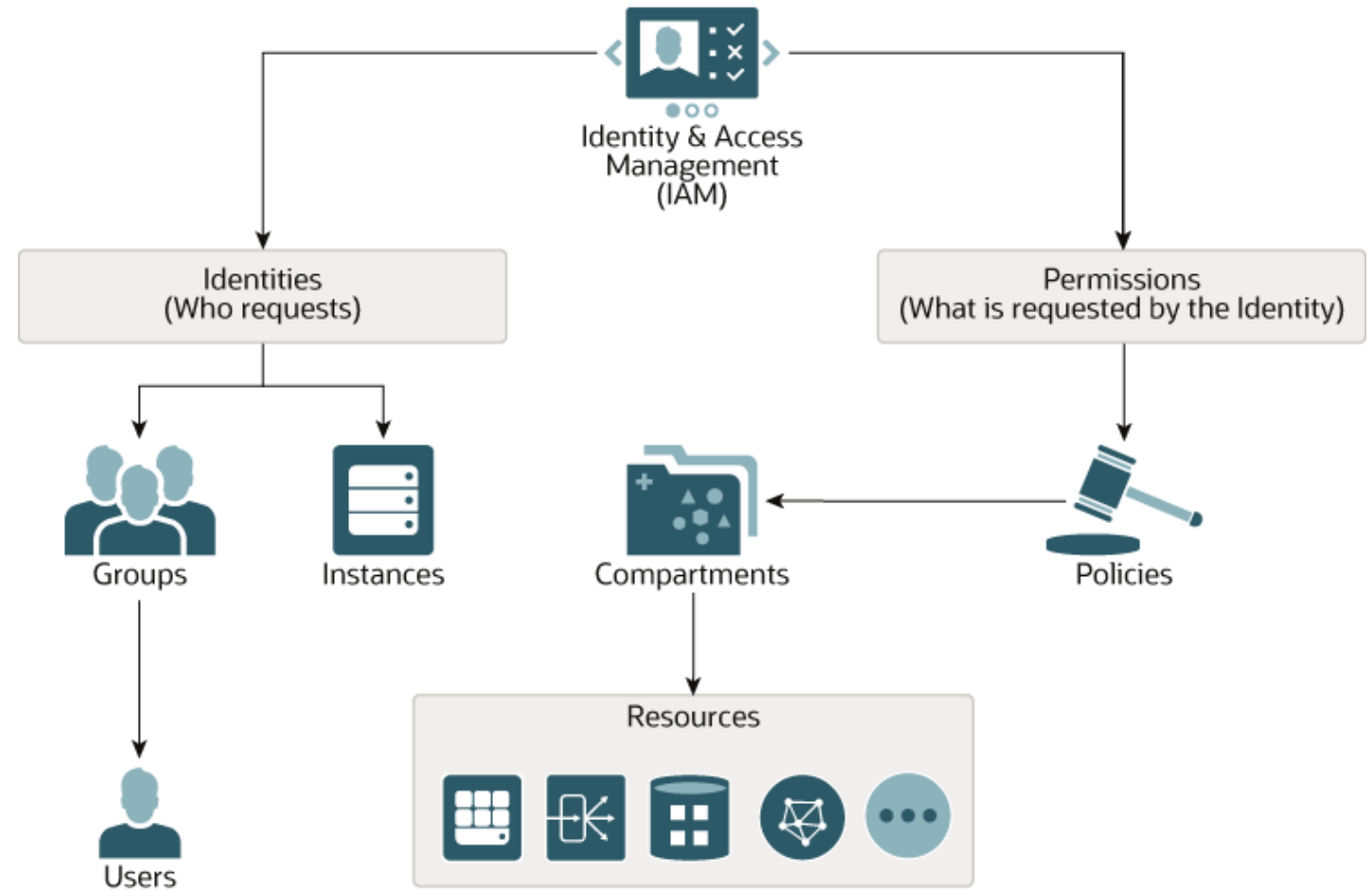


PASSWORD ROTATION



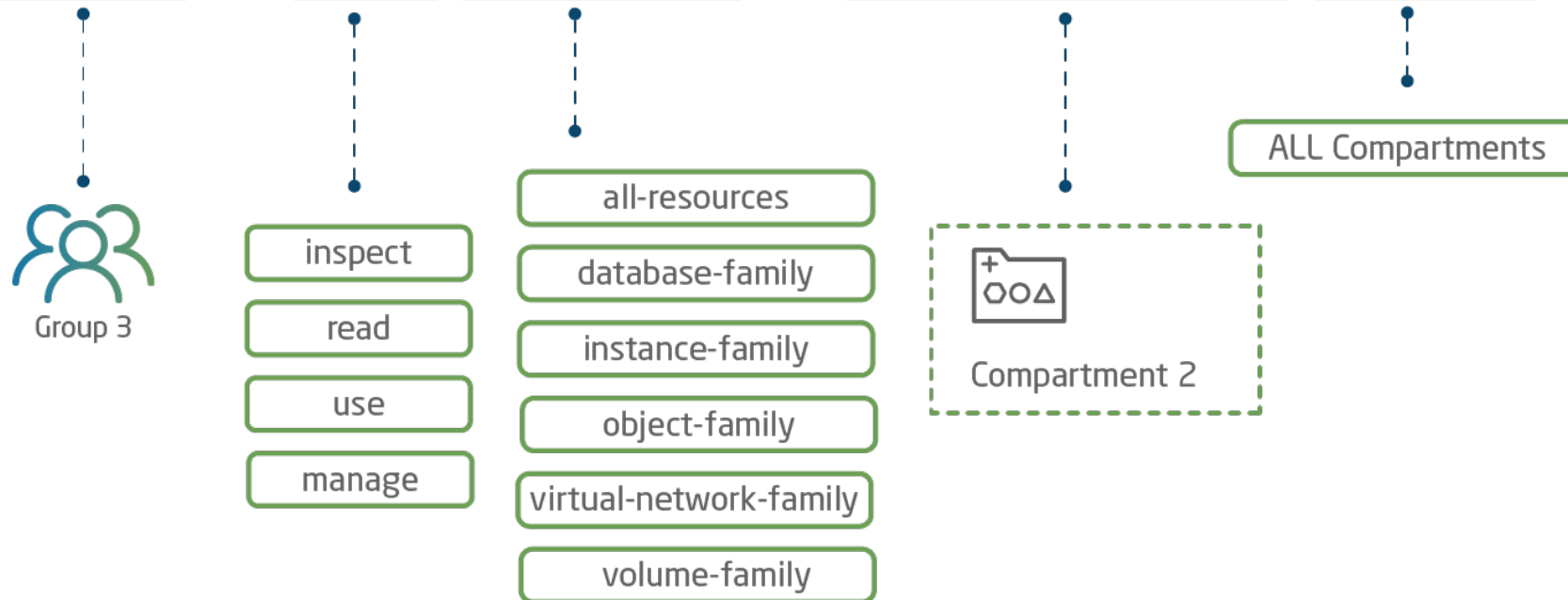
STRONG PASSWORD

AuthZ

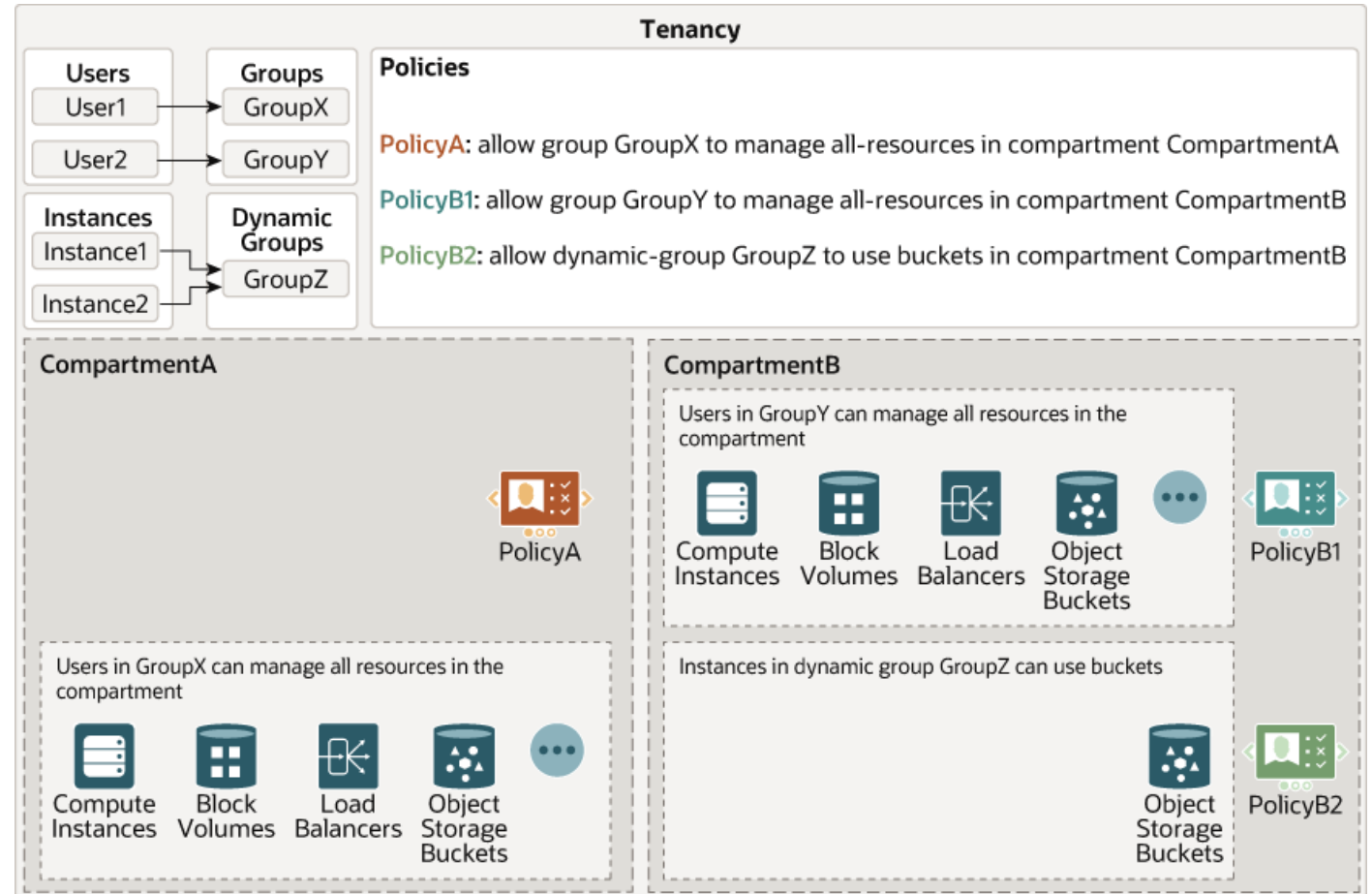


Policies.

allow subject to verb resource in compartment/tenacy conditions



Resources Isolation



Network security.



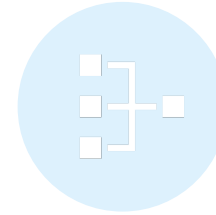
VIRTUAL NETWORKS
AND SUBNETS



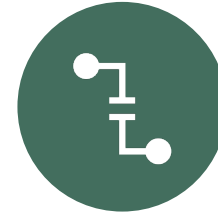
SECURITY LISTS SL,
SECURITY GROUPS
NSG



ROUTE TABLE



GATEWAYS
(IG, NAT, SG, DRG)



WEB APPLICATION
FIREWALL (WAF)
AND DDOS

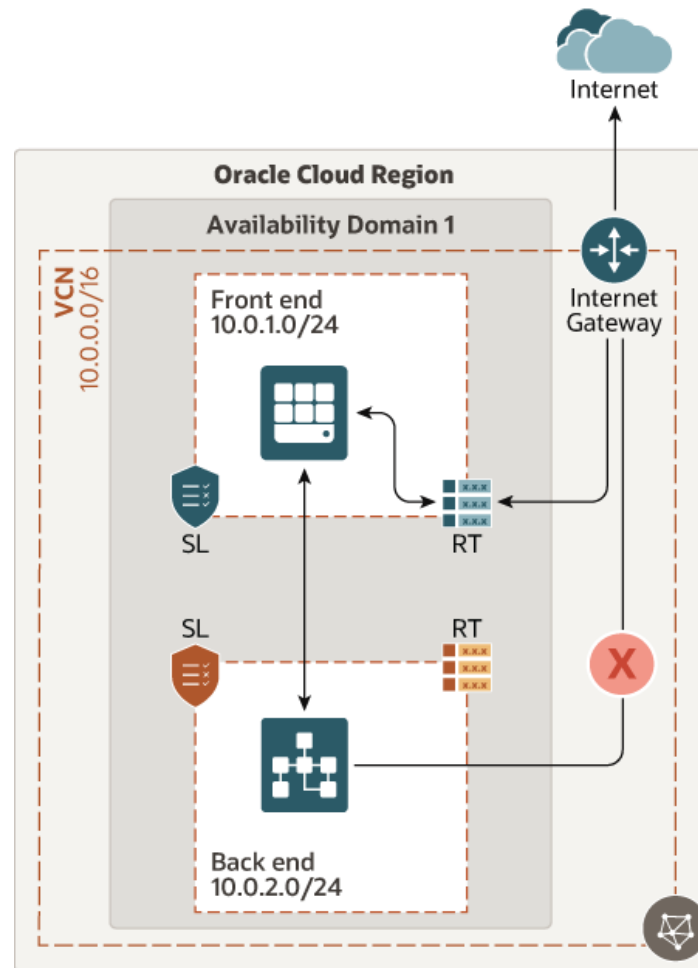


SECURE VPN



FASTCONNECT

Network Security



Route Table

Destination CIDR	Route Target
0.0.0.0/0	Internet Gateway

Security List

Type		CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	10.0.2.0/24	TCP	All	1521

Route Table

Destination CIDR	Route Target
0.0.0.0/0	NAT Gateway/Service Gateway /Dynamic Routing Gateway

Security List

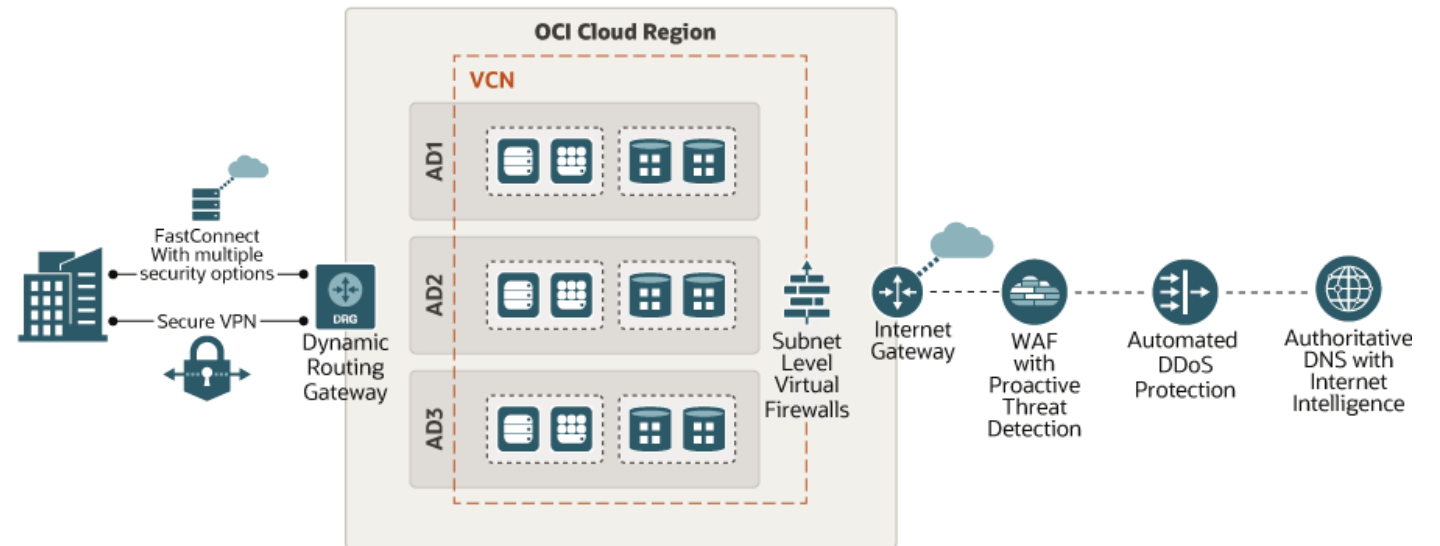
Type		CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	10.0.1.0/24	TCP	All	1521
Stateful	Egress		All	All	

Key

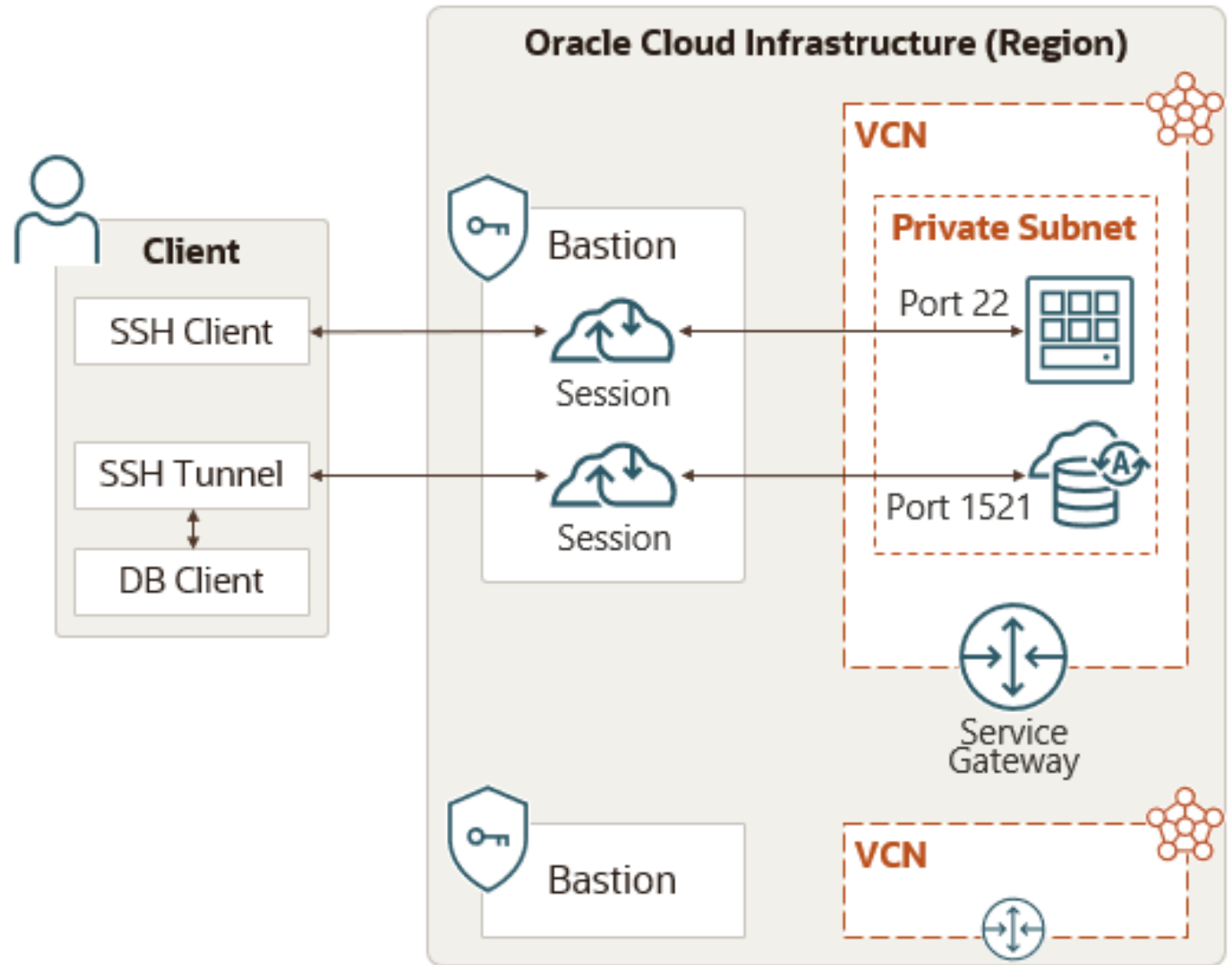
RT = Route Table

SL = Security List

Network Security



Bastion



Data Protection.



Data encryption

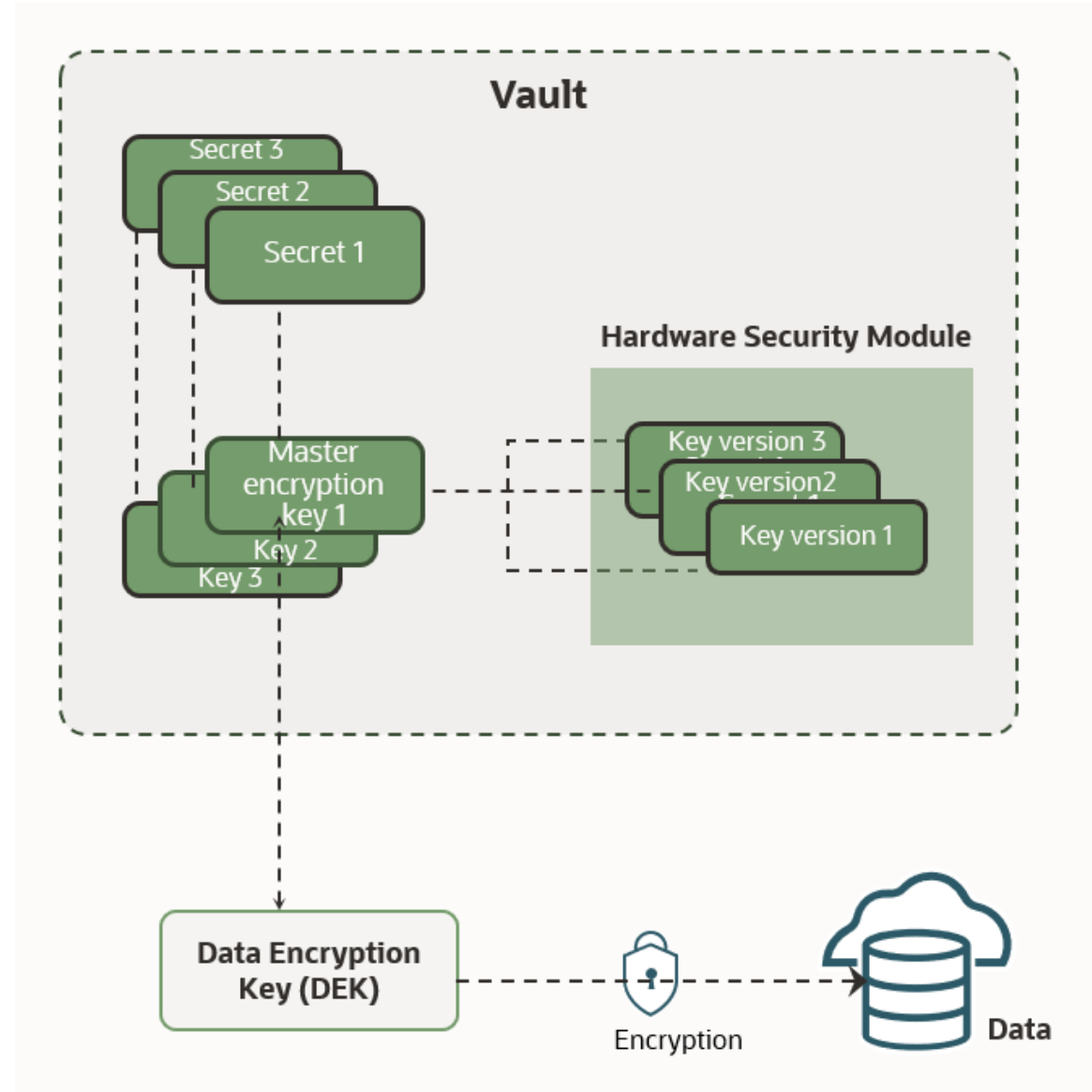


Data backups

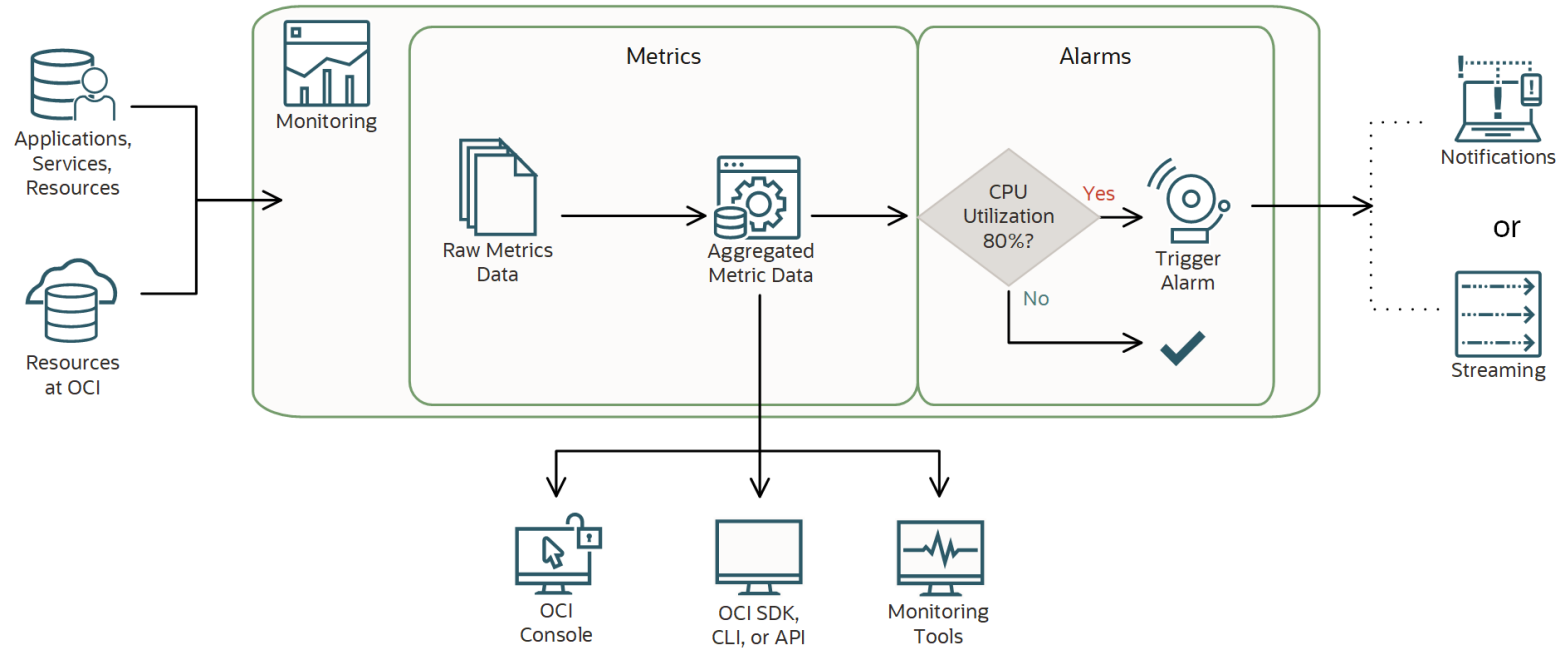


Data lifecycle management

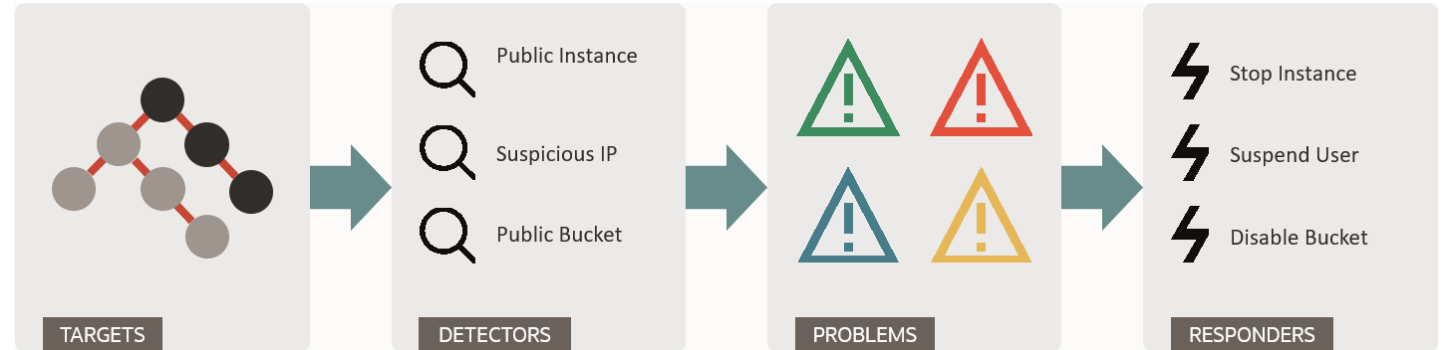
Vaults



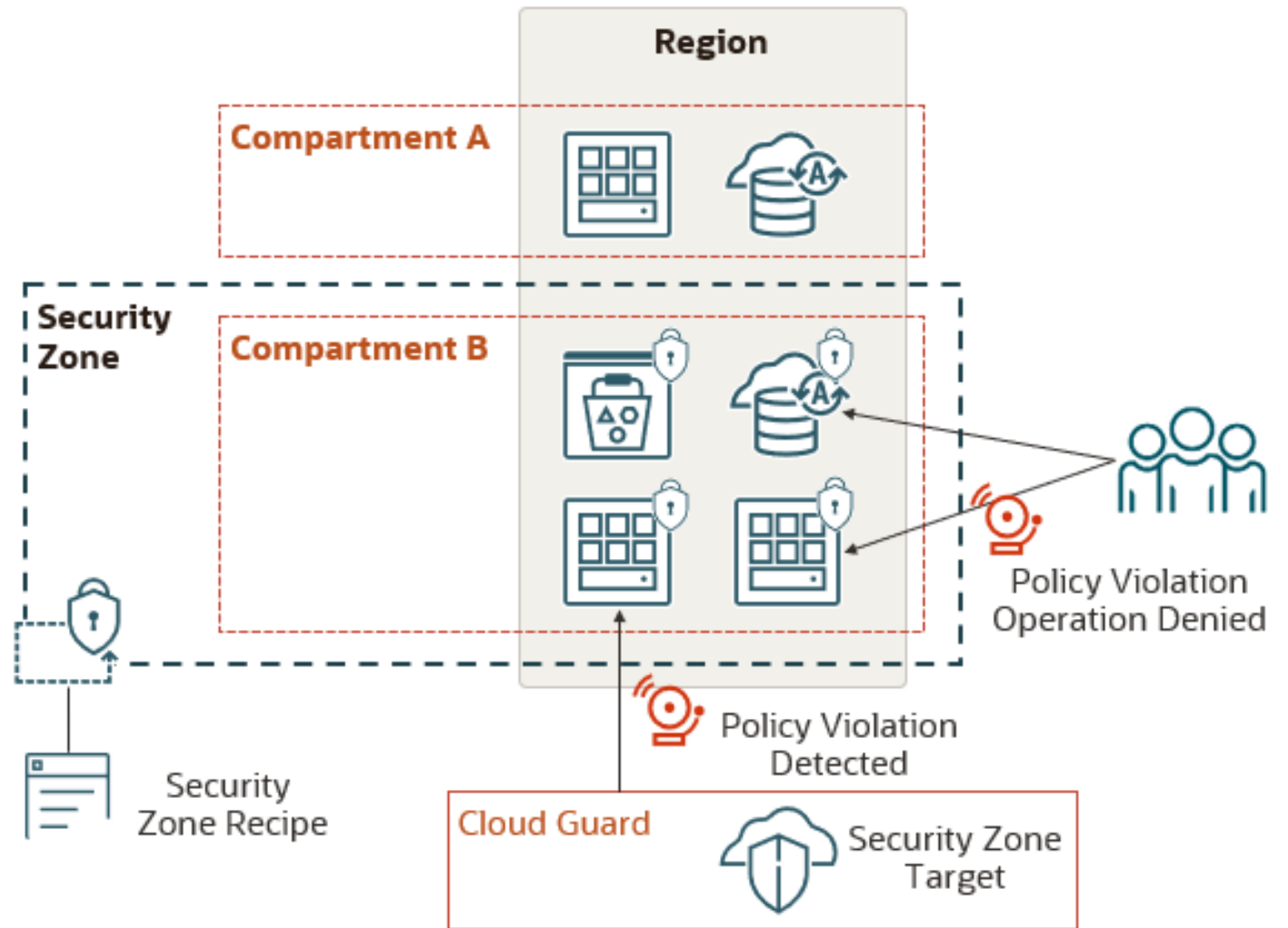
Security Monitoring and auditing



Cloud Guard



Security Zones





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 the 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.



Are you interested?



Mohamad Bouchi
Consultant

Mail: mohamadsubhi.bouchi@mt-itsolutions.com

MT GmbH

Balcke-Dürr-Allee 9
40882 Ratingen

www.mt-itsolutions.com



[Mohamad Subhi Bouchi](#)



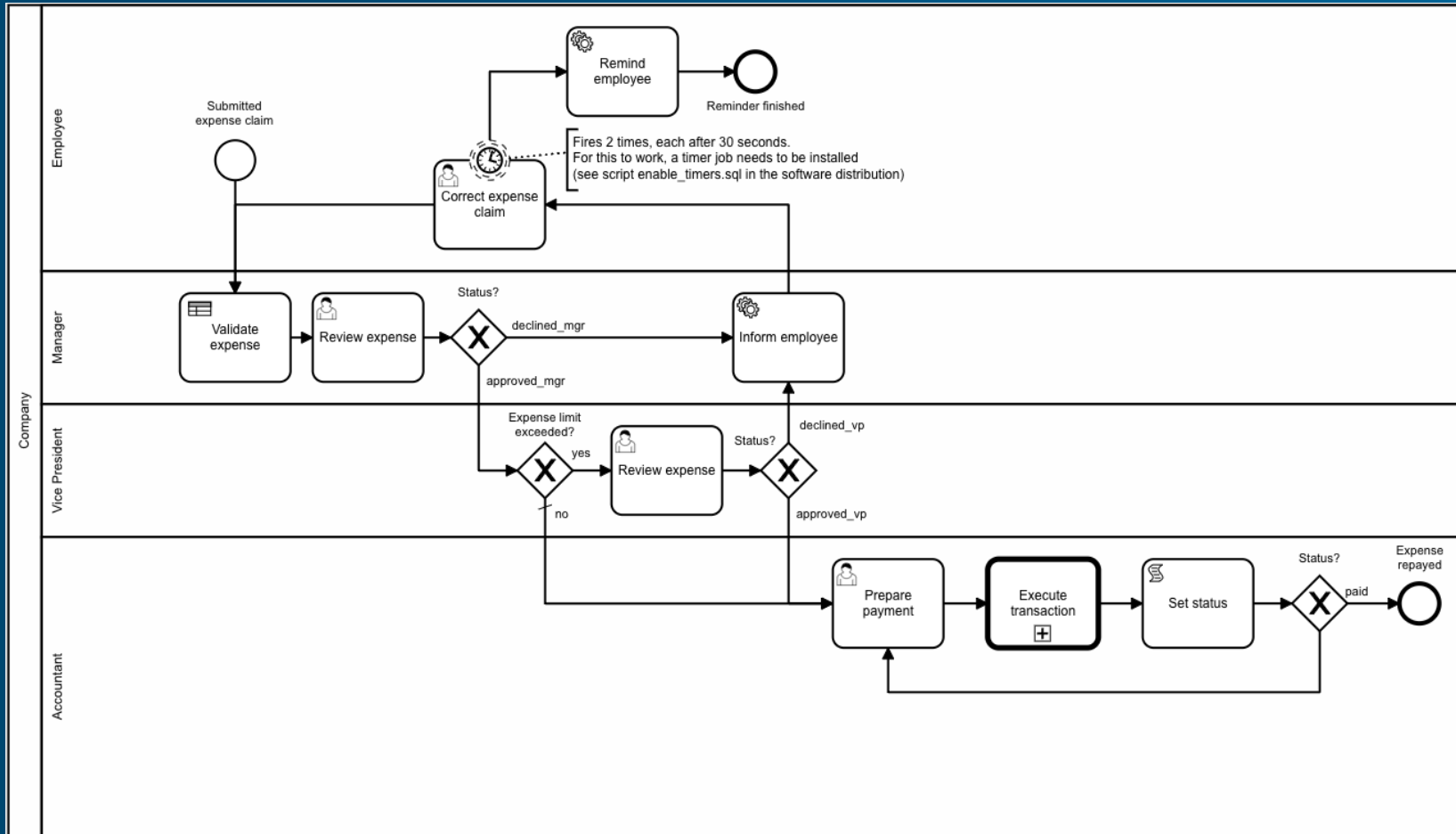
[@BouchiMohamad](#)



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.

- Low Code Test platform
- Access Application Metadata
- 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



Thank you for your attention! 😊

Sources.

- Seite 7: <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- Seite 10: <https://www.microsoft.com/en-us/security/business/zero-trust>
- Seite 13: <https://zpesystems.com/how-to-overcome-5-challenges-of-zero-trust-security/>
- Seite 15: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWlrfk>
- Seite 17: [Whitepaper „Approaching Zero Trust Security with Oracle Cloud Infrastructure“ von Oracle](#)
- Seite 19: <https://docs.oracle.com/en-us/iaas/Content/Identity/getstarted/identity-domains.htm>
- Seite 21: <https://docs.oracle.com/en/solutions/oci-security-checklist/authorization1.html>
- Seite 23: <https://docs.oracle.com/en/solutions/oci-security-checklist/resource-isolation1.html#GUID-5A0FFE48-2B88-45A7-B3D6-421B1553E7FD>
- Seite 25-26: <https://docs.oracle.com/en/solutions/oci-security-checklist/network-security1.html#GUID-B9BA6A84-375F-47E9-BD2C-C2B10C413944>
- Seite 27: <https://docs.oracle.com/en-us/iaas/Content/Bastion/Concepts/bastionoverview.htm>
- Seite 29: <https://docs.oracle.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm>
- Seite 30: <https://docs.oracle.com/en-us/iaas/Content/Monitoring/Concepts/monitoringoverview.htm>
- Seite 31: <https://docs.oracle.com/en-us/iaas/cloud-guard/using/cg-concepts.htm>
- Seite 32: <https://docs.oracle.com/en-us/iaas/security-zone/using/security-zones.htm>