



# OCI Identity & Access Management

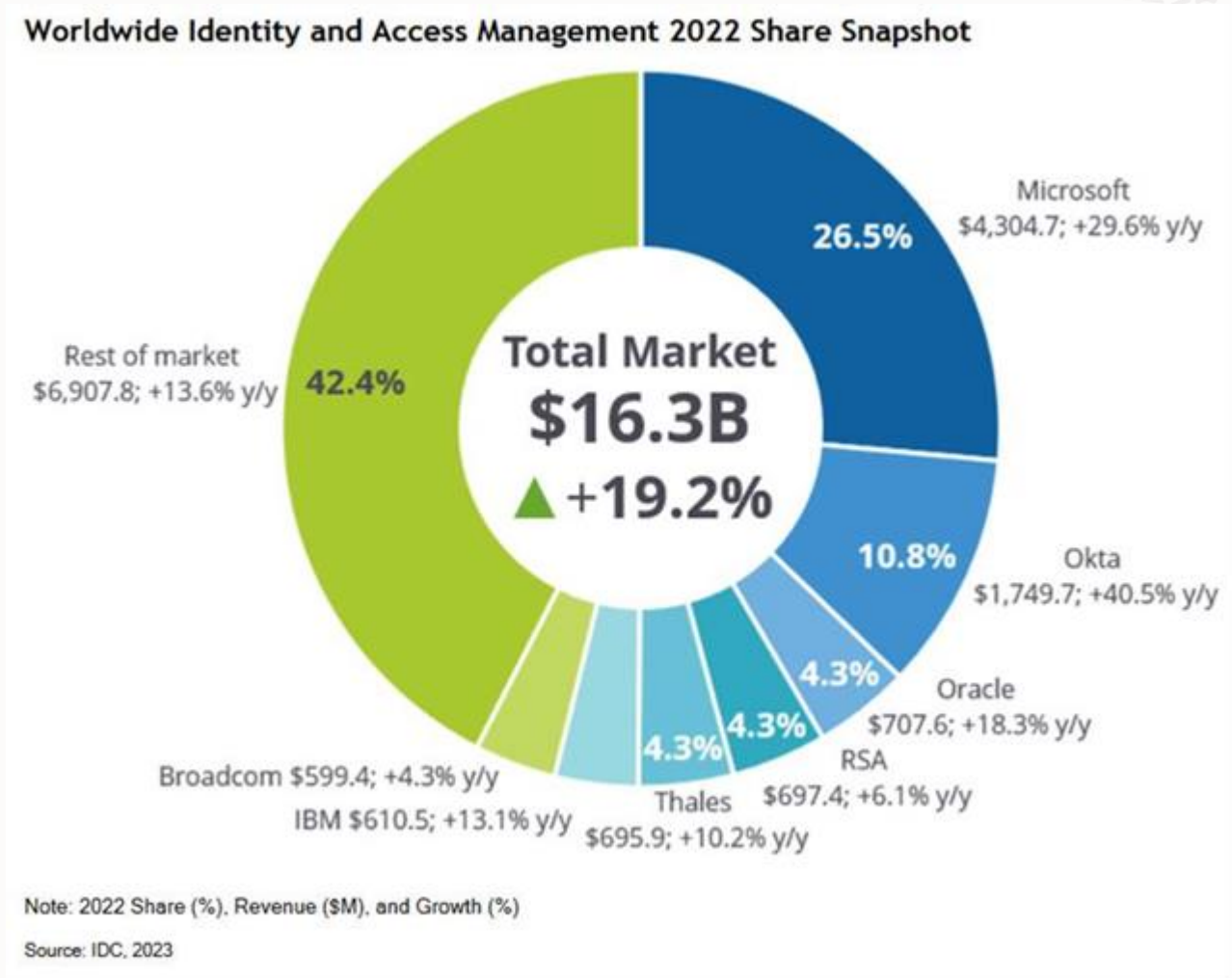
## Introduction and Overview



Alexandre Fagundes  
Cloud Architect | Oracle Latin America



# IDC Worldwide IAM Market Shares, 2022 (June 2023)



# IDC Worldwide Identity and Access Management Forecast

## Key Advice for Technology Suppliers

- Half the total market will be placing long-term bets in the next two to three years as they migrate away from clunky on-premises systems and replace inadequate homegrown solutions.
- Add AI/ML technology everywhere it makes sense, driving value from risk-based analytics... Pinpoint where people are involved and strive to replace them with supervised logic.

(full section text in slide notes)





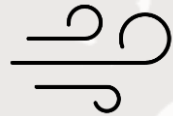
20+ years of leadership in IAM



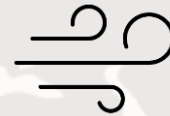
# There's a high-pressure system developing...

## Zero Trust

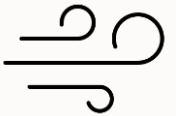
Distributed IT across on-prem, SaaS, and multiple clouds.



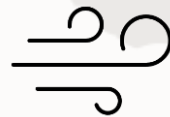
User credentials among top targets for hackers.



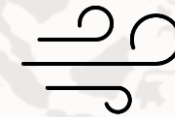
IAM is too complex to manage; there are multiple IAM silos.



Distributed stakeholders with limited control over devices, networks, etc.

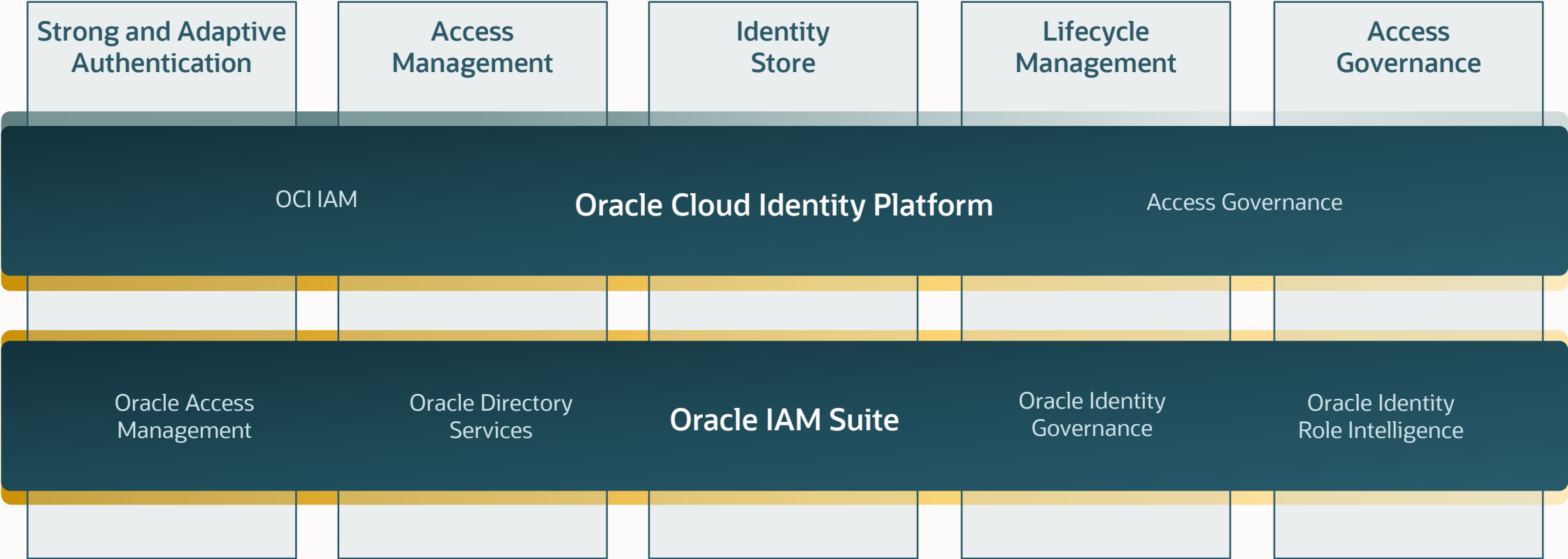


Lack of visibility across 100's of apps that may include shadow IT



## IAM is the New Perimeter

# Oracle Identity & Access Management Portfolio







OCI  
Identity and Access  
Management

# Oracle Cloud Applications

Complete suite of  
integrated applications



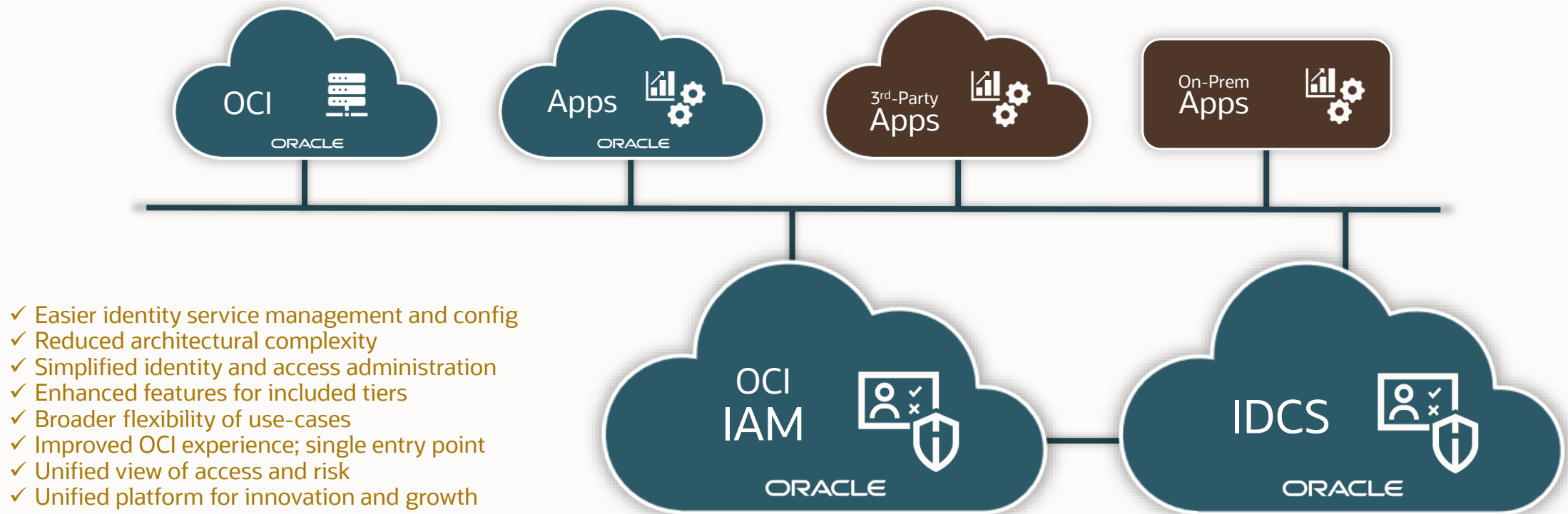
# Oracle Cloud Infrastructure

Secure, high-performance  
platform for all your workloads

# OCI IAM Identity Domains

Oracle is merging IDCS and OCI IAM services under the OCI IAM brand

OCI IAM will provide a single, unified IDaaS for Oracle and non-Oracle apps across hybrid cloud environments with robust MFA options, Adaptive Access, and Lifecycle Management





## Built for Scale and Performance

102K

Customer Accounts

450M

Identities

30+

Commercial regions  
globally

Oracle's Internal Deployment

140K

Employees

4500

Applications

# OCI IAM Functional Overview

---

# OCI Identity & Access Management (OCI IAM)

## Key Functional Pillars

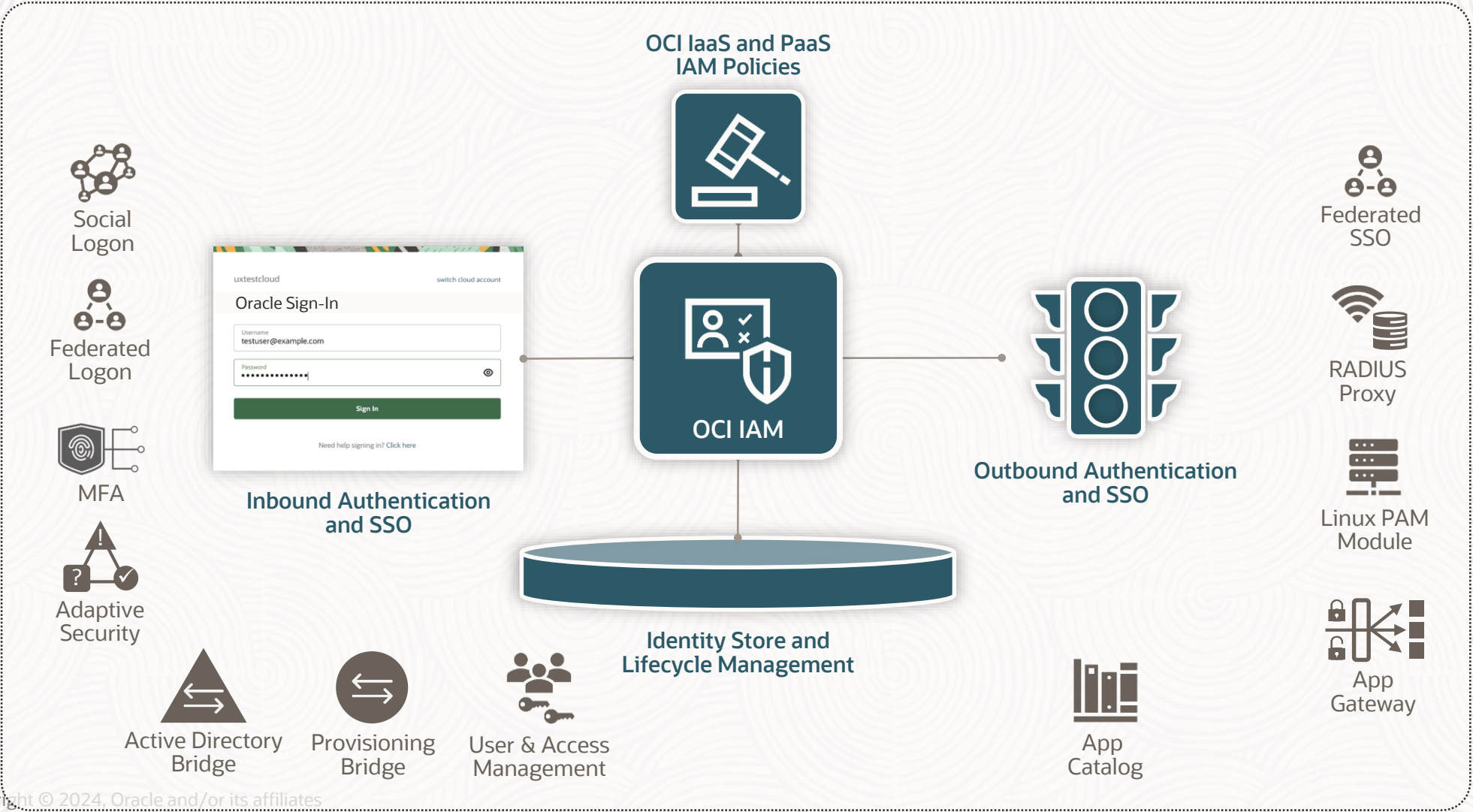
**Enterprise Identity  
& Access Management**  
for complex, hybrid IT  
environments

**Access Control Plane**  
for Oracle Cloud  
and SaaS applications

**Developer-friendly  
IAM engine**  
for custom and  
consumer applications

# OCI Identity & Access Management (OCI IAM)

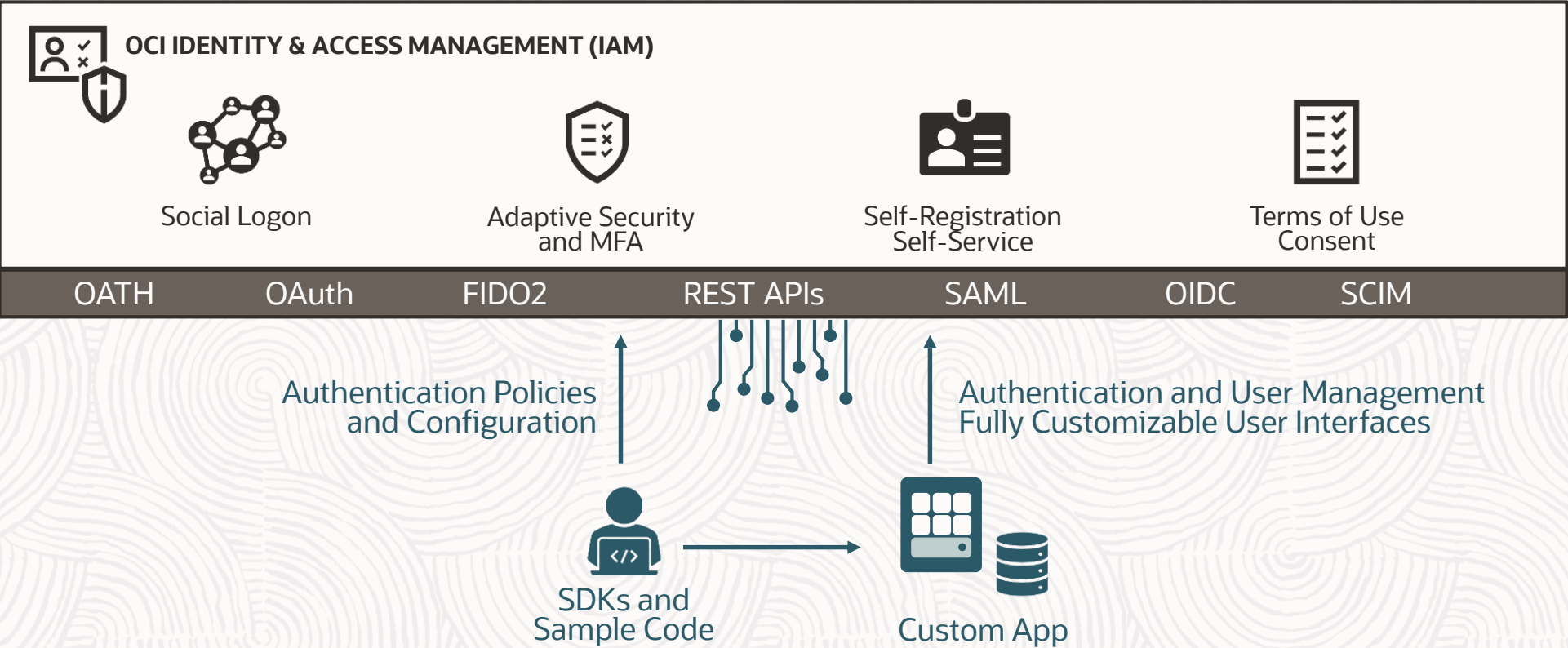
## Enterprise Identity & Access Management



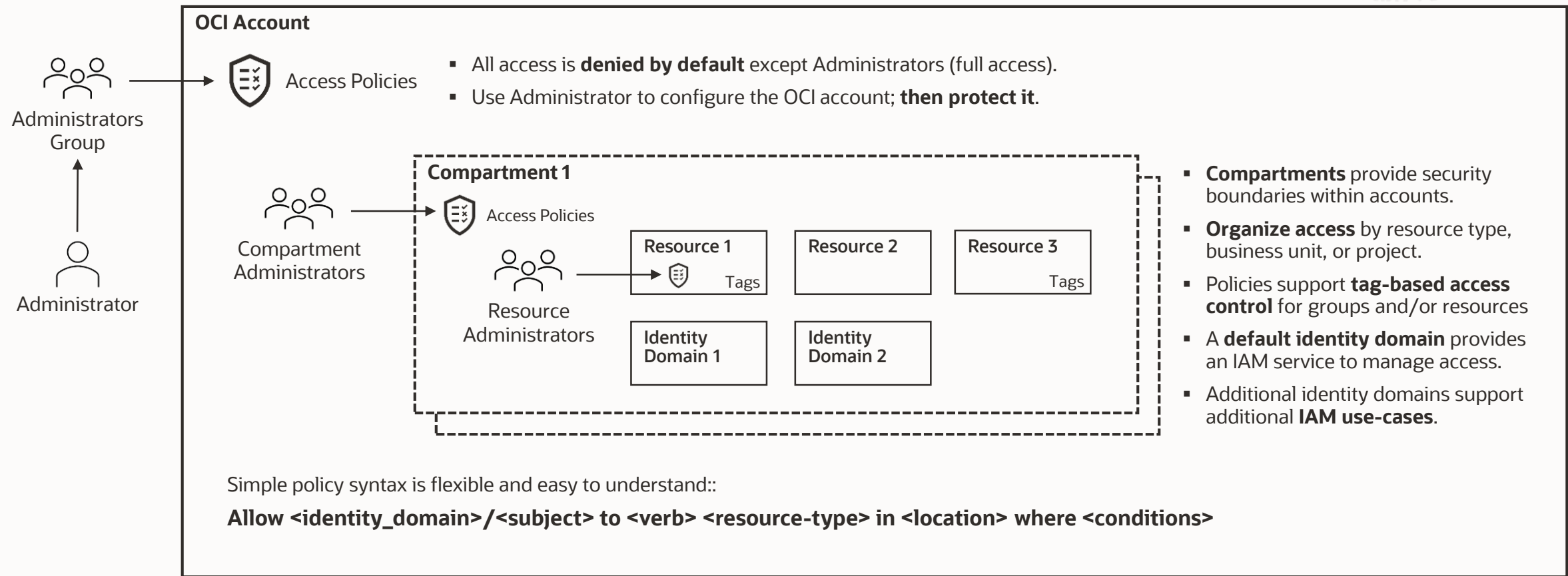


# OCI Identity & Access Management (OCI IAM)

For Application Developers



# Getting Started with OCI IAM



# OCI IAM Features and Functionality

---

Oracle Cloud Infrastructure Identity & Access Management

# Inbound Authentication and SSO

## Strong, flexible authentication options

- Supports basic authentication via username and password
- Supports common federation protocols and social logon with multiple identity providers  
*SAML, OpenID Connect, OAuth*
- Numerous options for Multi-Factor Authentication (MFA)  
*Included mobile app supports passwordless logon*
- Adaptive security evaluates risk in real-time based on context and session awareness
- Delegated Authentication to Active Directory



Leverage open standards for easy configuration of inbound SSO.



Native support for popular social Identity Providers.



Numerous options for MFA including a mobile app, Email, SMS, KBA, third-party and FIDO2 authenticators.



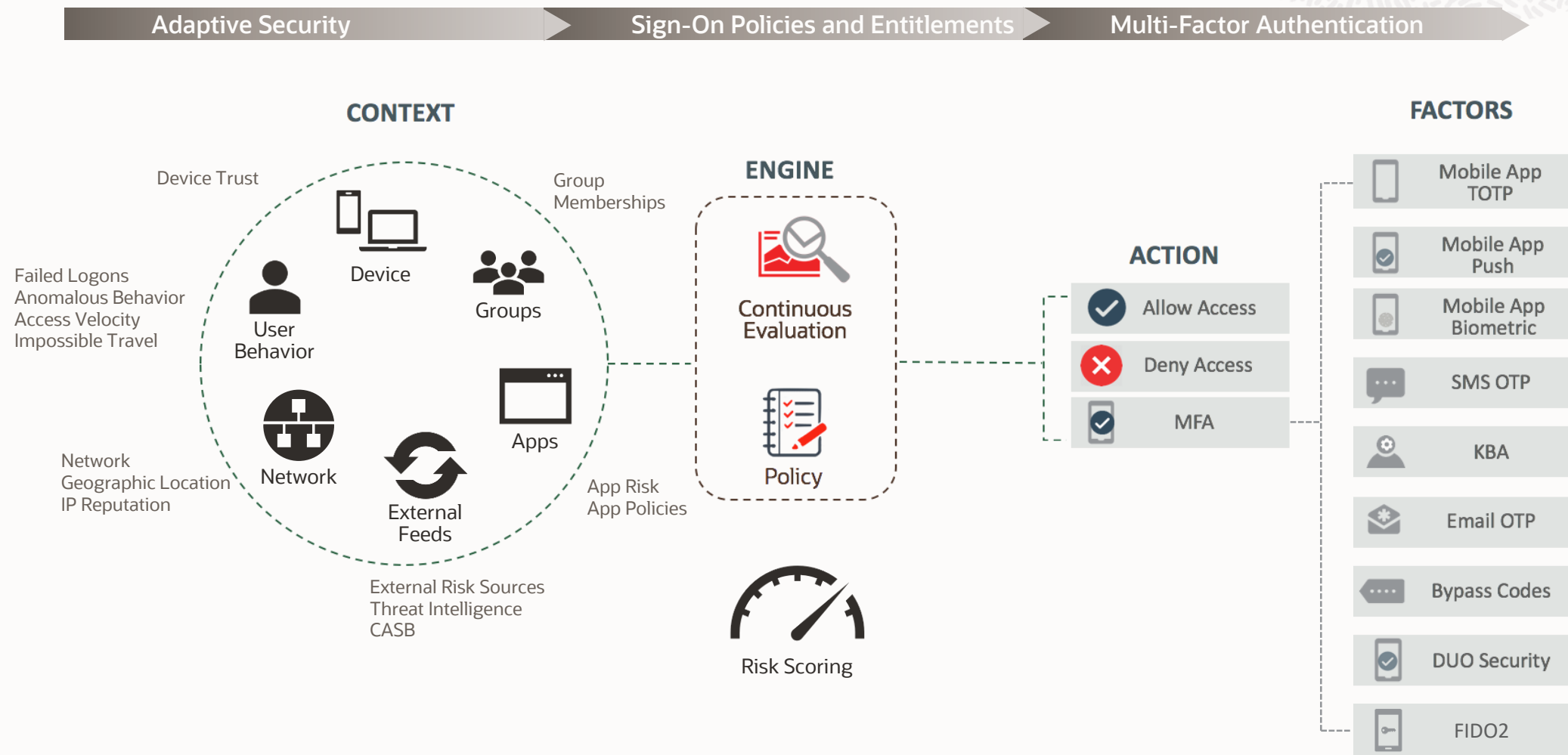
Evaluates risk based on several factors including device, network, location, and user behavior.



Enables delegated authentication to Active Directory (leverage AD credentials).



# Inbound Authentication and SSO



# Inbound Authentication and SSO

## Multi-Factor Authentication (MFA) Factors

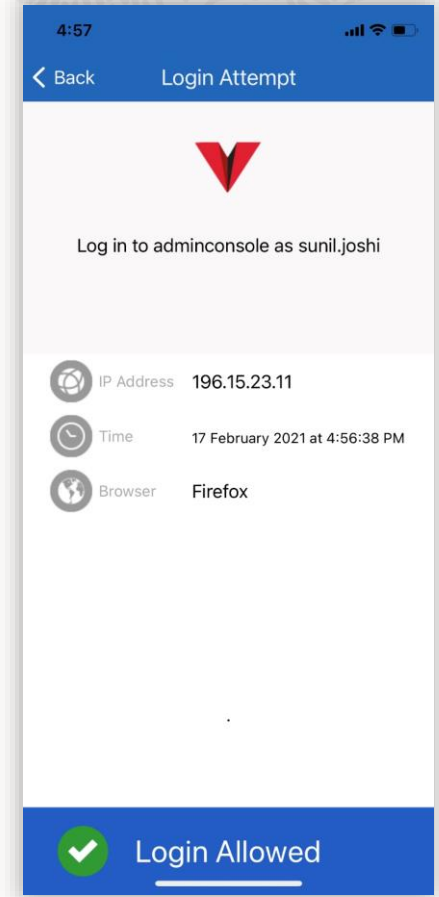
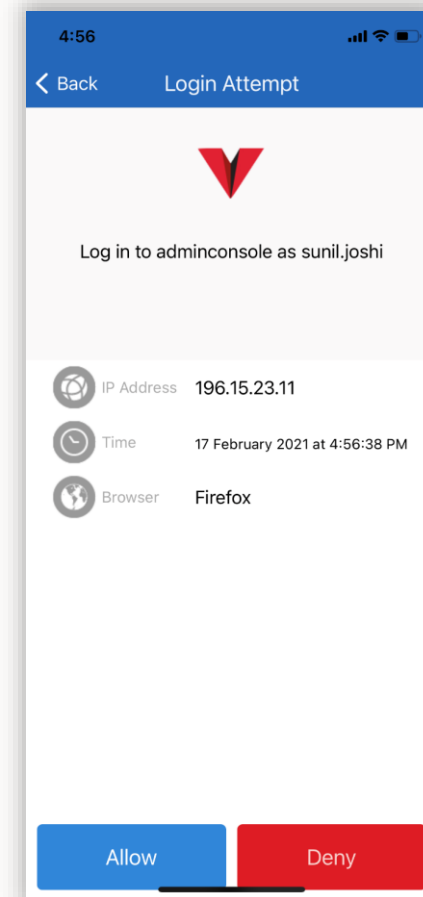
- FIDO2 Authenticators
- Voice Phone Call
- Mobile App Passcode or Notification
- SMS Text
- Security Questions
- Email
- Bypass Code
- Third-Party Authenticators  
*Duo, Yubico, etc.*
- Trusted Devices



# Inbound Authentication and SSO

## Passwordless Authentication

1. User creates profile at first logon
2. User enrolls device and MFA app
3. When user attempts to authenticate, they can logon via a push notification in the MFA app – no password required!



# Identity Store and User Lifecycle Management

## Automate user lifecycle management

- Manage via console, CLI, APIs, or automation
- Custom schema support
- Auto- and Just-in-Time (JIT) provisioning
- Auto-manage entitlements for Oracle apps and databases
- User self-service enrollment and management of profile, password, and terms-of-use consent
- Support for virtually any SaaS, cloud-hosted, or on-prem apps
  - Generic SCIM support enables integration with most apps
  - 400+ SaaS apps natively supported via partner gateways



User & Access  
Management

Manage users manually via console, CLI, or APIs. Bulk imports available with full or incremental updates.



App  
Catalog

Pre-configured automation of onboarding, offboarding, and synchronization flows for numerous apps. Generic templates support virtually any other apps.



Provisioning  
Bridge

Provisioning to/from virtually unlimited apps hosted on-prem or in the cloud using ICF connectors. Supports heavy customization as-needed. Supports High Availability.



Active Directory  
Bridge

Synchronize AD Users and leverage AD Security Groups to manage IAM permissions.



# OCI IaaS and PaaS IAM Policies

## Control who has access to OCI cloud resources

- Easy to understand policy syntax
- Authentication policy can restrict by IP address
- Group-based entitlement management
- Compartments provide security boundaries inside of OCI tenancies
- Time- and Location-based restrictions
- IAM auto-replication to subscribed regions
- Supports Tagging for groups and/or resources

CompanyA Tenancy

Policies attached to the tenancy:

● Allow group Administrators to manage all-resources in tenancy

● Allow group NetworkAdmins to manage virtual-network-family in compartment Networks

● Allow group NetworkAdmins to manage instance-family in compartment Networks

● Allow group A-Admins,B-Admins to use virtual-network-family in compartment Networks

● Allow group A-Admins to manage all-resources in compartment Project-A

● Allow group B-Admins to manage all-resources in compartment Project-B

● Allow group A-Admins to use users in tenancy where target.group.name='A-Users'

● Allow group A-Admins to use groups in tenancy where target.group.name='A-Users'

● Allow group B-Admins to use users in tenancy where target.group.name='B-Users'

● Allow group B-Admins to use groups in tenancy where target.group.name='B-Users'

● Allow group A-Admins,B-Admins to inspect users in tenancy

● Allow group A-Admins,B-Admins to inspect groups in tenancy

Users

Alex

Cheri

Dylan

Fred

Helali

Jenna

Jorge

Laura

Leslie

Tarik

Wenpei

Groups

Administrators

Wenpei

Alex

NetworkAdmins

Leslie

A-Admins

Jorge

A-Users

B-Admins

Cheri

B-Users

Compartments

Networks

Project-A

Project-B



# Outbound Authentication and SSO

Easy Single Sign On (SSO) experience across extended, hybrid enterprises

- Support common federation protocols  
*SAML, OpenID Connect, OAuth*
- App catalog provides out-of-the-box integrations with 1000+ apps
- Generic and custom templates support any other apps that support federation protocols
- Password vaulting (form-fill) for apps that don't support federation protocols
- Just-in-Time provisioning to target applications
- Gateways and Proxies support SSO to hybrid environments.



Leverage open standards for easy configuration.



Pre-configured SSO and Just-in-Time provisioning for numerous apps.



SSO to virtually unlimited apps hosted on-prem or in the cloud that may not support open standards.



Support SSO to VPN clients and Oracle Databases.



Support SSO to Linux hosts running on OCI

# OCI IAM Best Practices



- Create a [security model](#) (tenancy, compartments, tagging) before adding users, resources.
- Enforce Least Privilege; gradually add permissions as needed.
- Do not use OCI default Administrator or [Administrators](#) group after initial account setup.
- Leverage [situational permissions](#) (time- or location-based) where possible.
- Leverage [compartments and tagging](#) to simplify access management. Align your OCI compartment design with your department or project structures.
- Use [instance principals and dynamic groups](#) to manage machine access to APIs.
- Enforce [multi-factor authentication](#) and leverage [adaptive security](#) whenever possible.
- Use different [identity domains](#) for each user population.
- Whitepaper: [Best practices for identities and authorization](#).

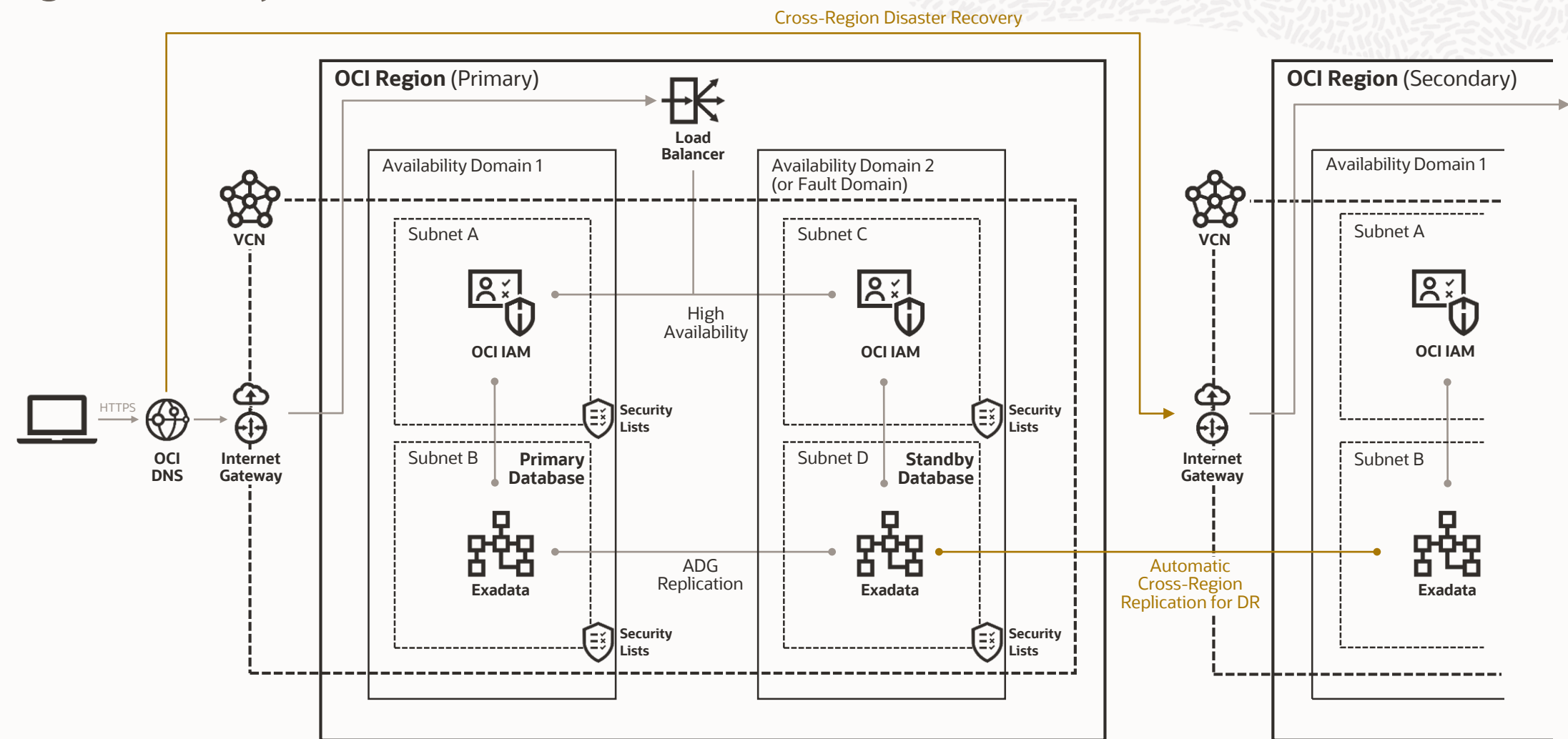
# OCI IAM High Availability (HA) and Disaster Recovery (DR)

—  
OCI Identity and Access Management



# OCI Identity & Access Management (OCI IAM)

## High Availability Architecture

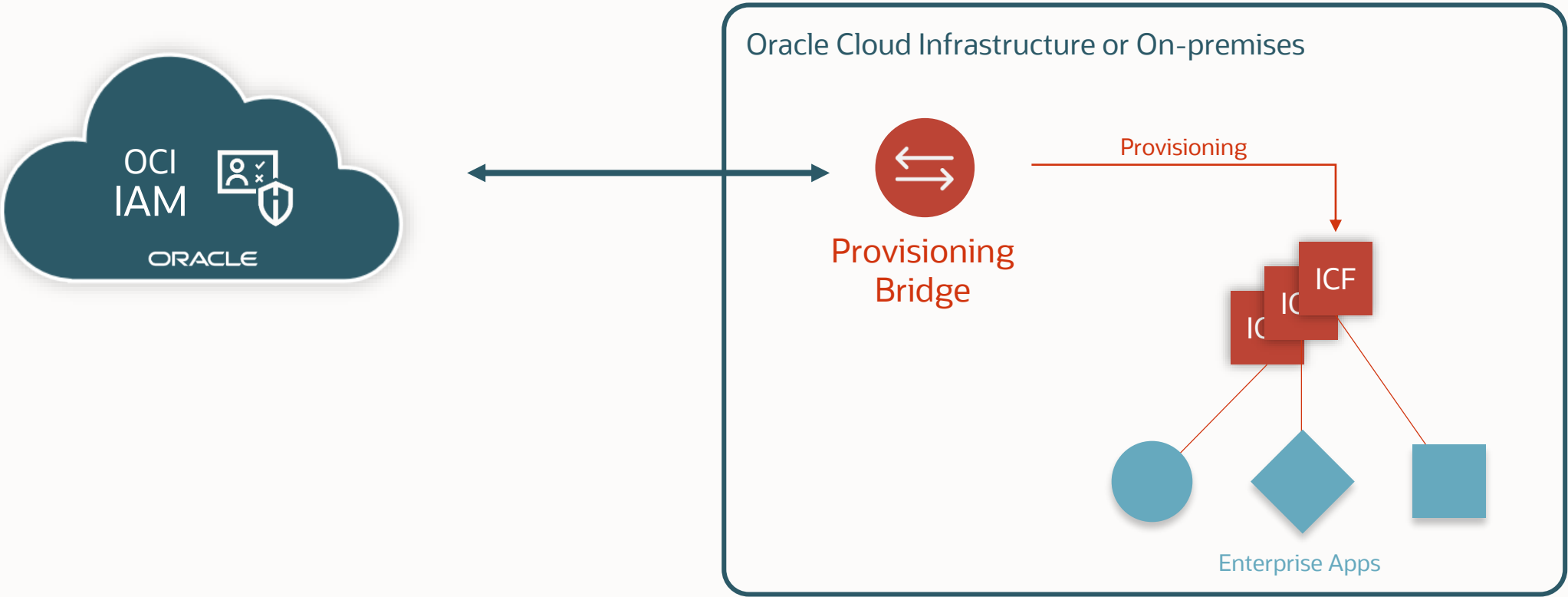


# Common Hybrid IAM Use-Cases

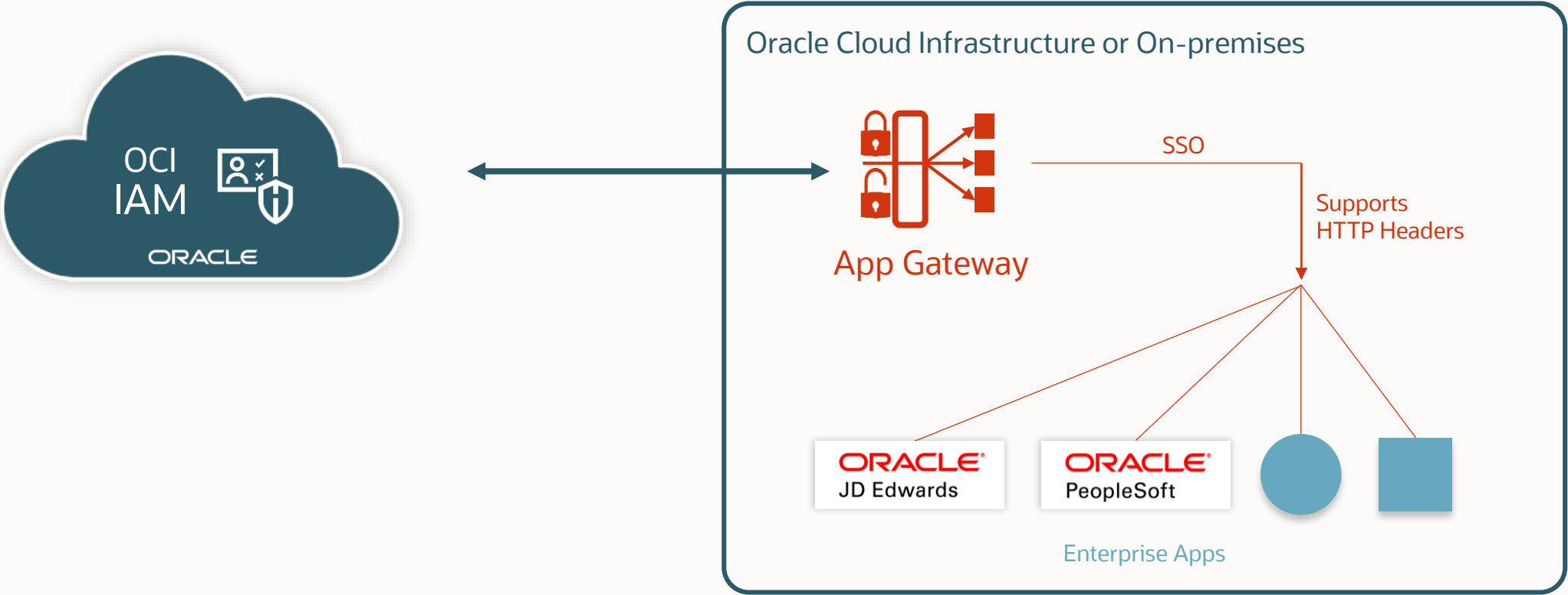
---

OCI Identity and Access Management

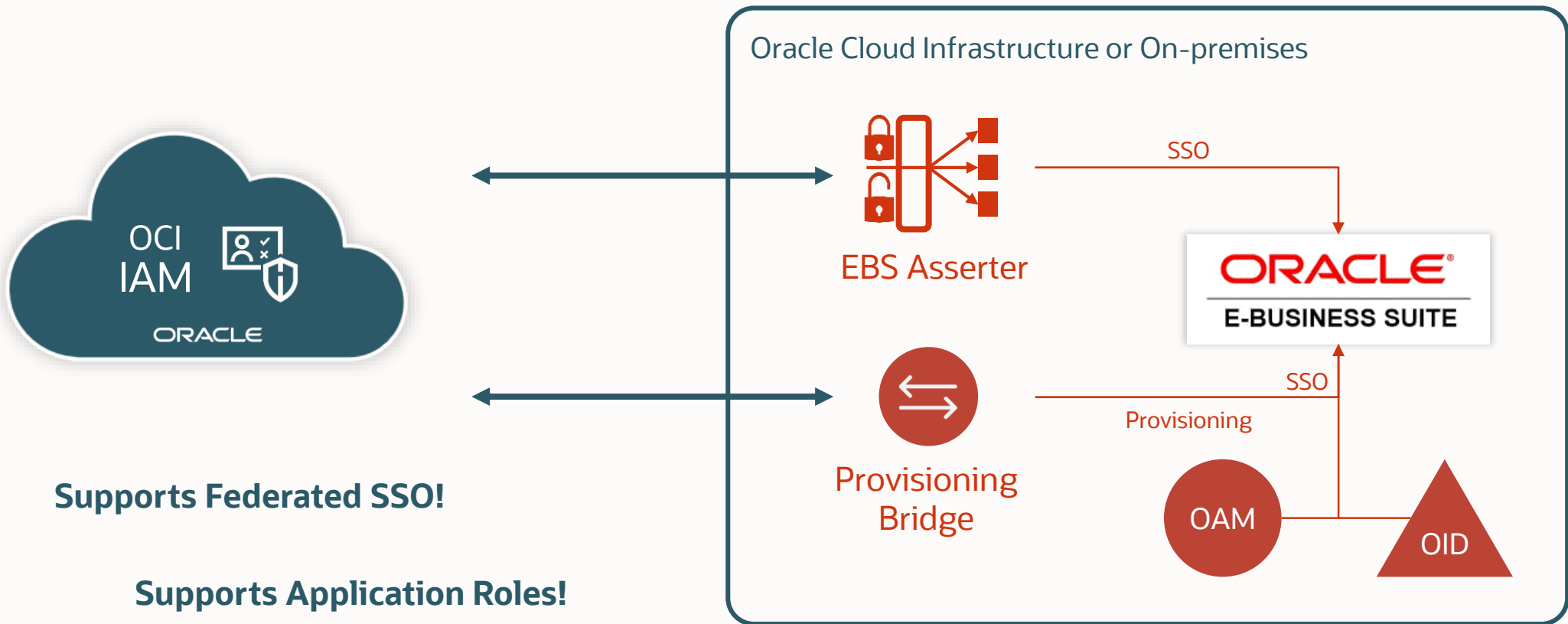
# OCI IAM Provisioning Bridge



# OCI IAM App Gateway



# OCI IAM Support for E-Business Suite (EBS)





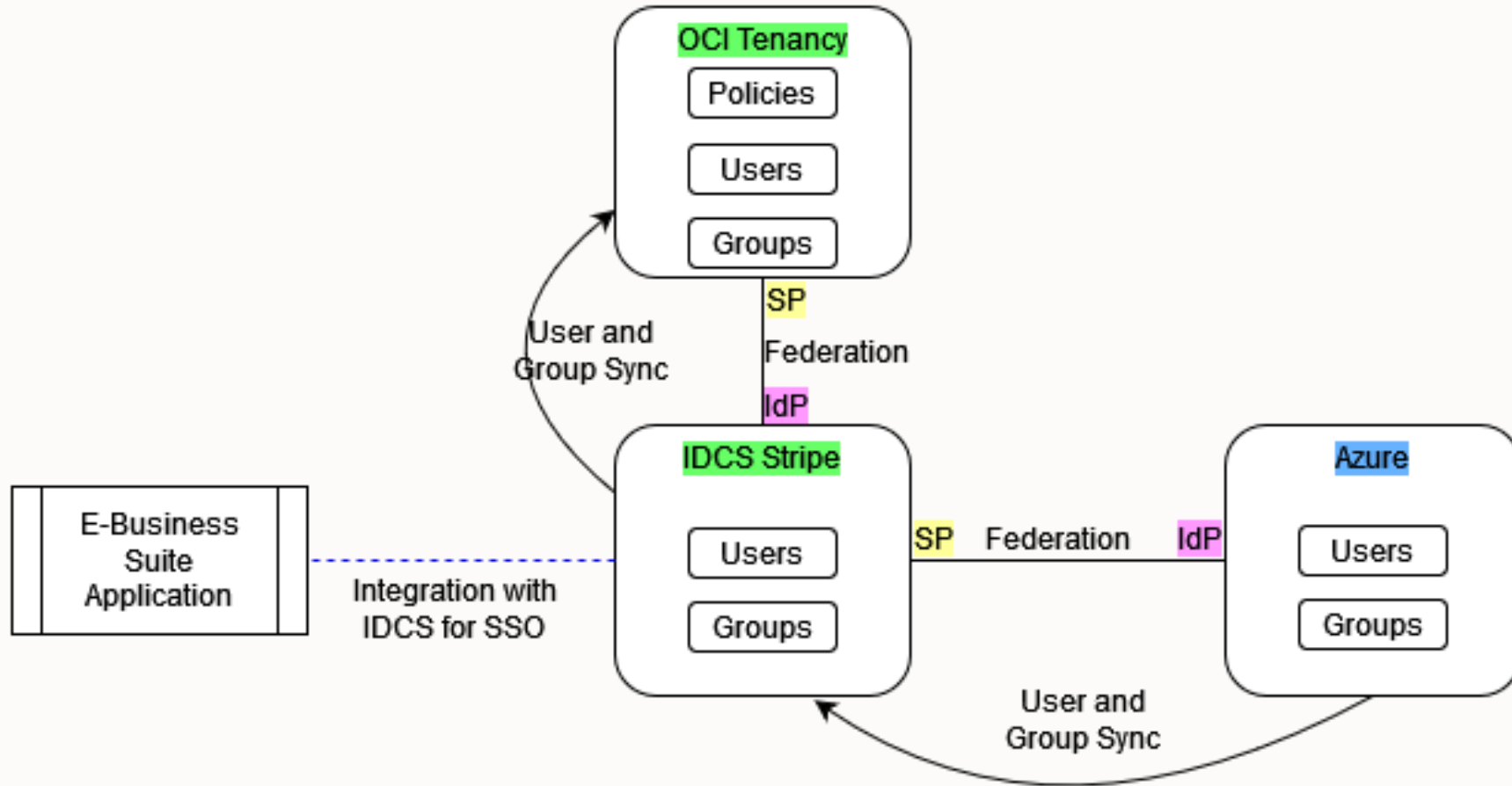
# Federation from Azure AD

---

OCI Identity and Access Management

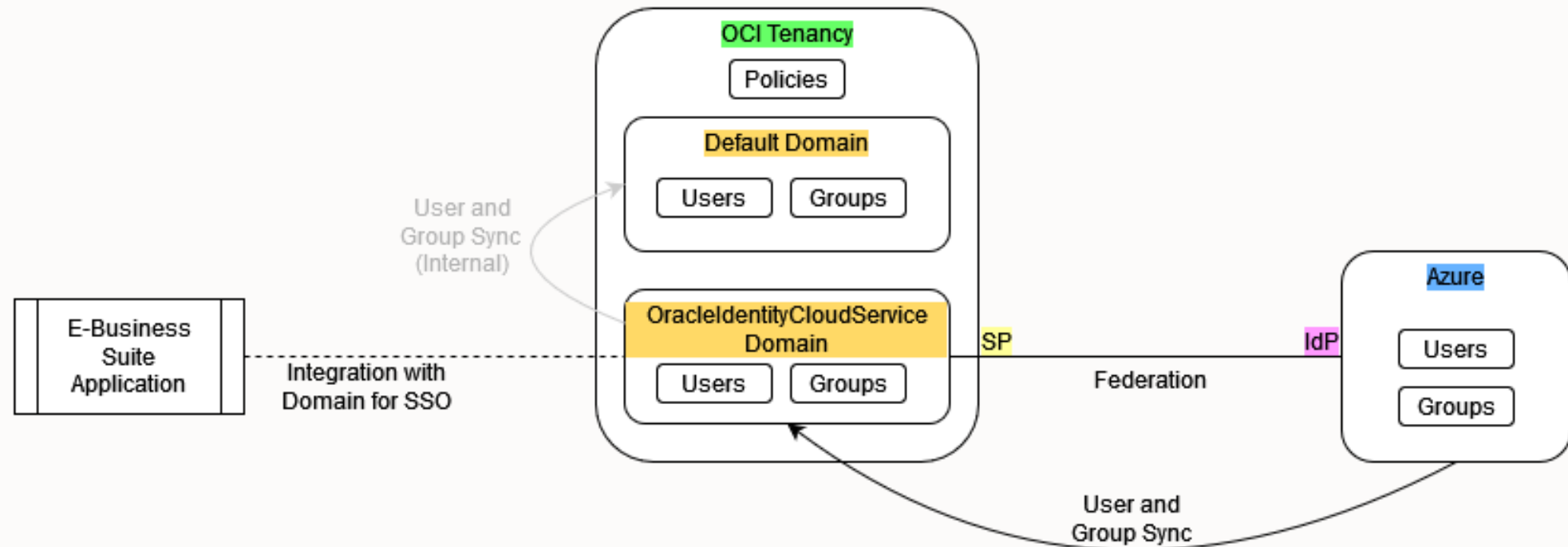
# Azure AD Federation

via IDCS (Before)

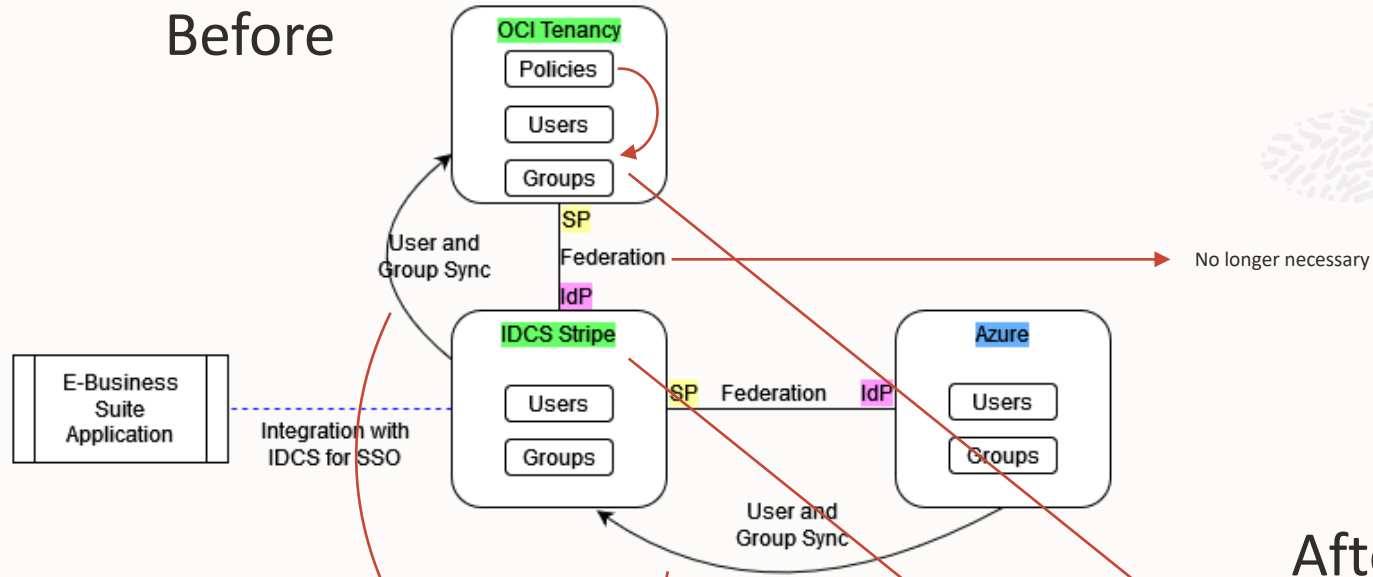


# Azure AD Federation

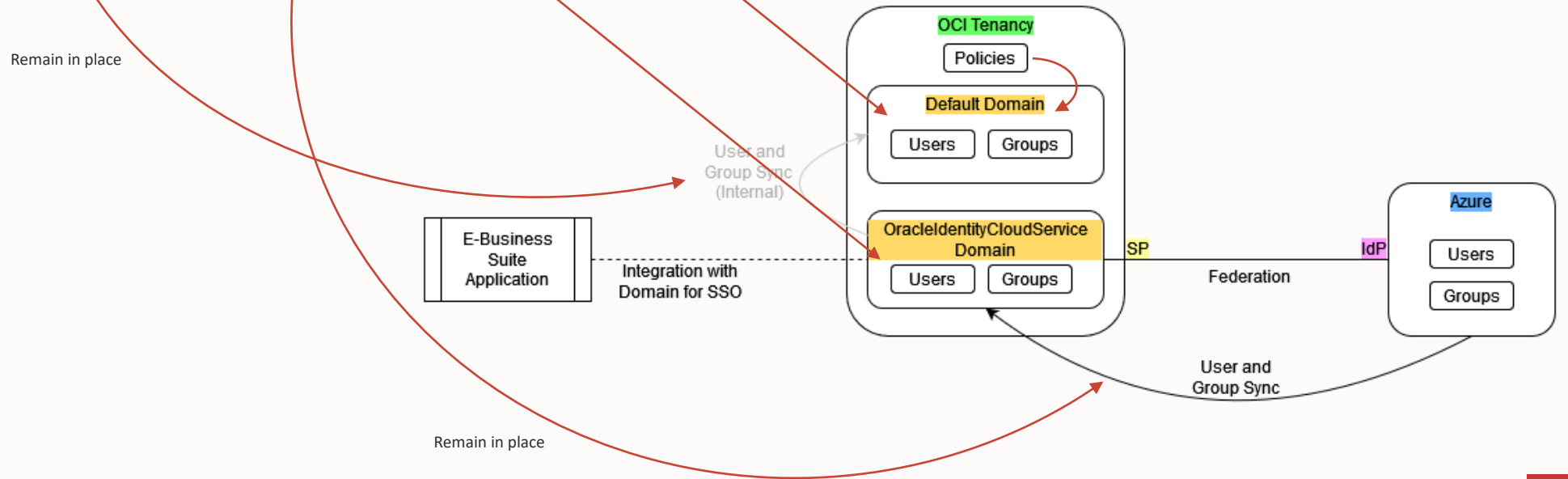
Via OCI IAM identity domains (After)



# Before



# After



# OCI IAM Vision and Roadmap

OCI Identity and Access Management





OCI  
Identity and Access  
Management

# Oracle Cloud Applications

Complete suite of  
integrated applications



# Oracle Cloud Infrastructure

Secure, high-performance  
platform for all your workloads



# OCI IAM Vision

Simplicity, Visibility, and Automation



## Enterprise Identity & Access Mgmt. for complex, hybrid IT environments

- High value proposition with more included features
- Unified IDaaS for access management, governance, and privileged access
- Robust set of risk indicators and analytics
- Far reach of control across hybrid, heterogeneous IT
- Enhanced ML and analytics via OCI service integrations

## Developer-focused IAM engine for custom and consumer-facing applications

- Integrated experience via APEX and Visual Builder
- Shared fabric via APIs with hooks across OCI, security services and apps exposing user, session, app, platform, and access pattern data
- Leverage automation for easier integrations
- Enhanced risk analytics for CIAM use-cases

## Access control plane for Oracle Cloud and SaaS applications

- Zero-touch IAM integrations with Oracle apps for access, roles, and lifecycle mgmt.
- Deep security and risk visibility, insights for OCI and Oracle apps
- Improved automation for service operations
- Auto-tuning security policies based on risk
- Shared security models

# Why choose Oracle for IDaaS?

## Strong Value

- Strong value for cost
- Improved user experience via better performance and scale as a native OCI service
- Peace of mind that OCI IAM will continue to incorporate latest and best approaches
- Presence across 30+ cloud regions; meets data residency requirements
- World-class, global support

## Depth for Oracle Targets

- Reduced effort and easier integrations for EBS, Fusion Apps, Oracle Databases, etc.
- Simplified entitlement management via App Roles
- Reduced management overhead via strong hybrid support for apps running on-premises, hosted on OCI, or SaaS
- Migration expertise, support, and discounts moving from OAM

## IAM Experience

- Oracle has led in IAM for past two decades; working with the world's largest, most complex organizations
- Strong hybrid IT support supporting on-prem apps, App Gateway, Provisioning Bridge, AD Bridge, RADIUS, Linux, etc.
- Powerful provisioning to on-prem via ICF connectors.
- Easier to get support from strong SI partner ecosystem.



# Customers Across Verticals and Geographies



# Thank you



Alexandre Fagundes

Cloud Architect | Oracle Latin America



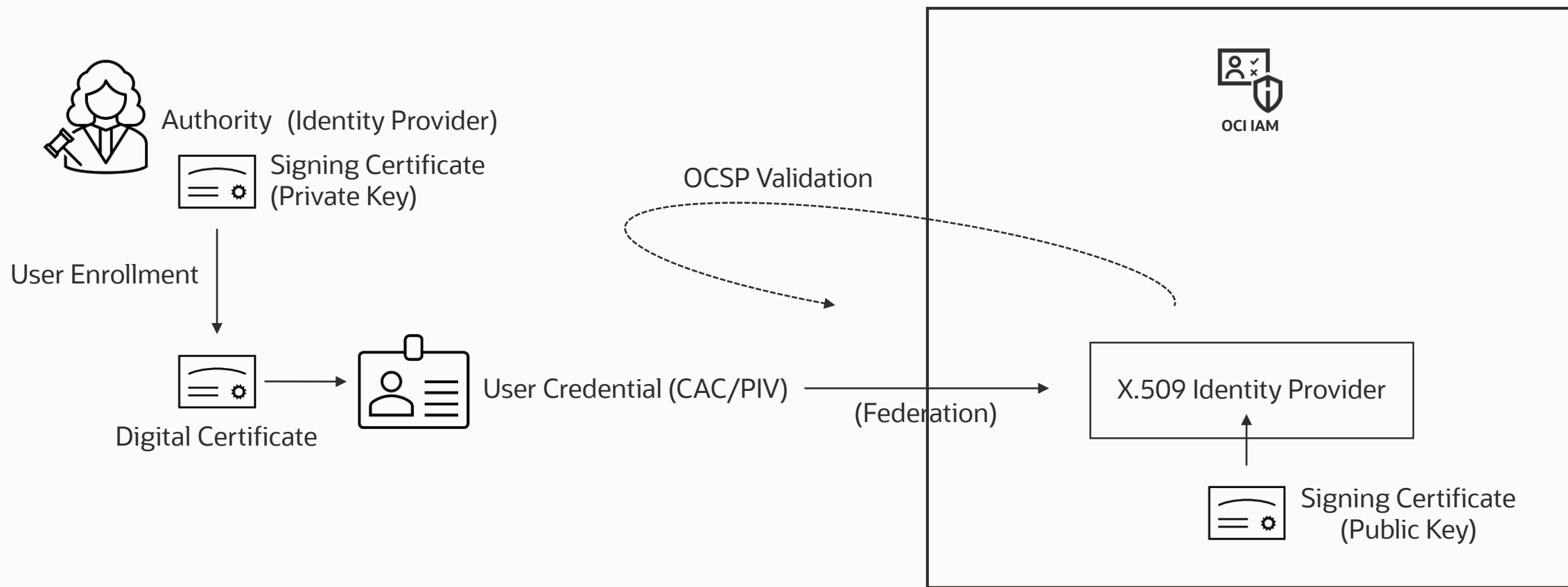
ORACLE

# Appendix Content

---

## OCI Identity and Access Management

# X.509 | Common Access Card (CAC) | Personal Identity Verification (PIV)



# Using Credentials Across Multiple Tenancies



- Today, you can configure any Identity Provider (inc. OCI IAM) to federate to multiple OCI tenancies.
- OCI IAM is planning for improved use of credentials across multiple OCI tenancies. This is part of a broader effort to create a single Oracle identity for use across all Oracle services. Timing TBD.
- Design approaches under consideration include:
  - Associate DNS domain names with an identity domain making it authoritative for that DNS domain name suffix. Users who authenticate with matching credentials see available resources.
  - Authoritative identity domains with links to user identities in non-authoritative identity domains which can exist in other tenancies. Organizations could leverage authoritative identity domains making it easier to manage users across parent and child tenancies.