Andiamo in **Cloud** con **Sicurezza**

Ettore Fabbiano: *Client Delivery Manager (Vantea Smart)*
Angelo Bosis: *Technology Sales Consulting Director (Oracle Italia)*

Security Summit – Roma - 07 Giugno 2017

Oracle Community For Security

Di cosa vi parleremo oggi ?

Come sono cambiati i requisiti di sicurezza con l'adozione delle architetture Cloud

Quali le tecnologie disponibili per indirizzare i nuovi requisiti

Premessa

- l'adozione di soluzioni in Cloud rappresenta oggi un **trend in costante e rapida crescita**
- favorisce **l'accesso** e l'utilizzo di servizi e applicazioni **da qualsiasi luogo**
- fruibilità dei servizi e applicazioni attraverso una **pluralità di dispositivi** sempre maggiore e in evoluzione rispetto al recente passato
- Il **79% delle organizzazioni** hanno già attivato un piano di **migrazione verso il Cloud** *(Crowd Research Partner)*

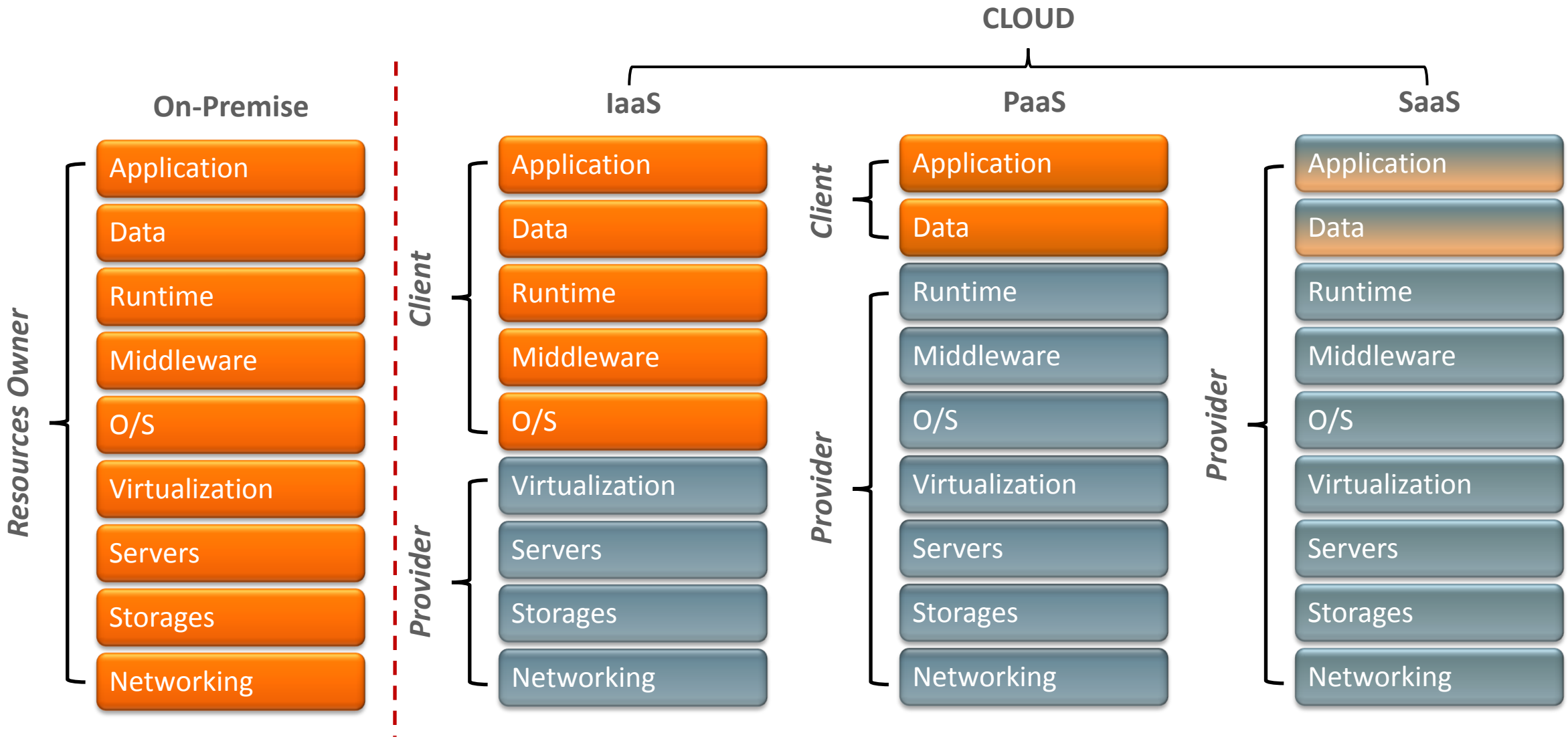
Gartner:

- **by 2020** a Corporate **"No-Cloud"** Policy will be as **rare as a "No-Internet" Policy is today**
- **by 2020** "Cloud Shift" will affect more than **$1 Trillion** in **IT Spending**
- **Hybrid** will be the most **common use** of the Cloud

- **Time To Market**
- **Maggiore efficienza**
- **Maggiore flessibilità**
- **Deployment veloci**

- **Riduzione costi manutenzione IT**
- **Riduzione dei *"Capital Costs"***
- **Riduzione dei *"Opportunity Cost"***
- **Riduzione rischi di backup & recovery**

Le Responsabilità in una nuova era dell'IT



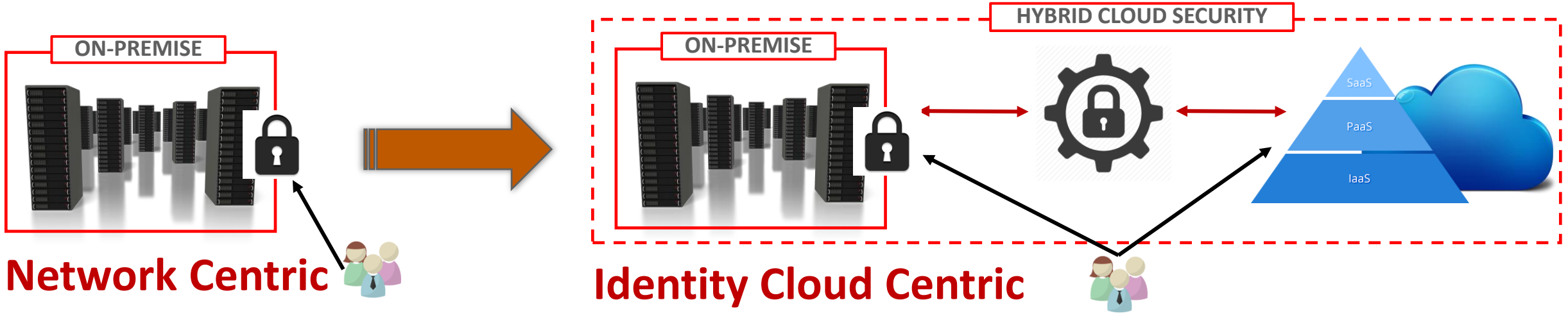
La Sicurezza in una nuova era dell'IT

Le organizzazioni devono fornire un **accesso sicuro ai sistemi IaaS e on-premise**, senza impedire la produttività, sia di business che in termini di operatività IT.

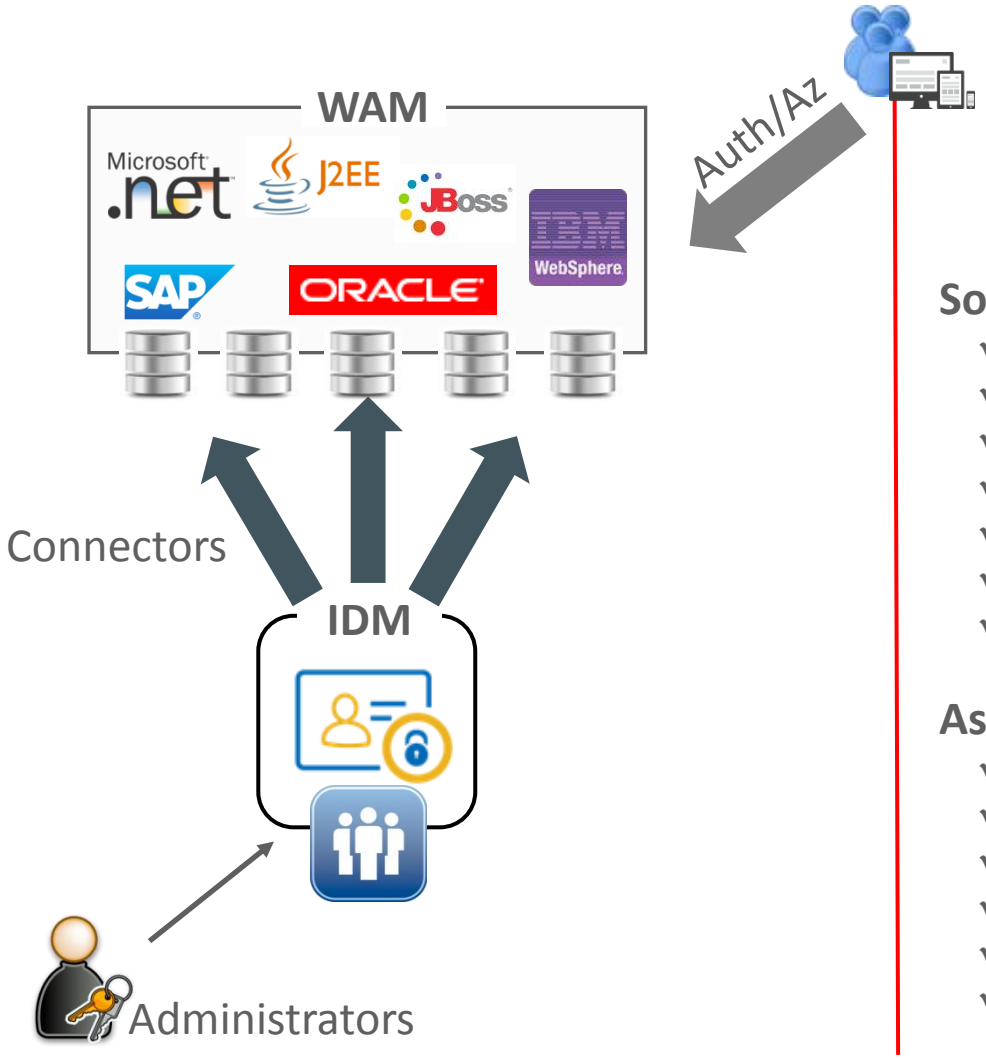
Oggi, il personale IT e i relativi referenti di Sicurezza di un azienda, sono consapevoli che le moderne architetture Cloud o Hybrid, presentano **requisiti** di accesso e **di sicurezza diversi dai tradizionali sistemi on-premise**.

Tali requisiti oggi **non possono essere completamente soddisfatti basandosi solo su strumenti tradizionali** o solamente implementando le best practices indicate dal Vendor IaaS.

Le nuove architetture devono prevedere l'introduzione di una piattaforma di sicurezza che possa **controllare tutto il perimetro IT**: dall'on-premise ai servizi in Cloud adottati dall'organizzazione.



Architetture tradizionali “Pre Cloud”



Soluzioni IAM (IDM+WAM) on-premise

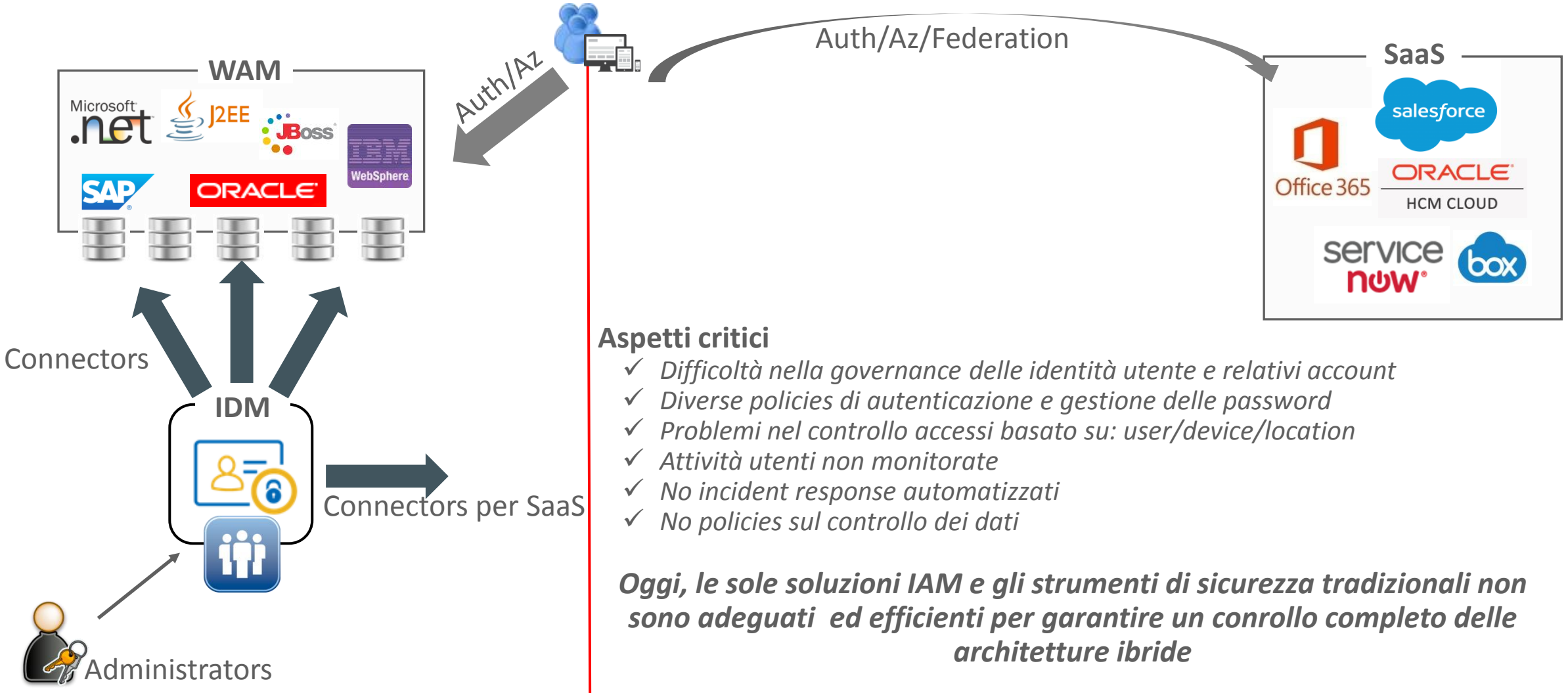
- ✓ *Provisioning/De-provisioning/Riconcializione*
- ✓ *Attestation*
- ✓ *Self Service Request*
- ✓ *Authentication & Authorization*
- ✓ *Multifactor/Strong Authentication*
- ✓ *Single Sign On*
- ✓ *Federation*

Aspetti critici

- ✓ *Costi per il setup HW & SW*
- ✓ *Opportunity Cost*
- ✓ *Capex Cost*
- ✓ *Progettazione per l’avviamento*
- ✓ *Maintenance*
- ✓ *Time to Market lunghi*

ON PREMISE **CLOUD**

Architetture attuali “Hybrid Cloud”

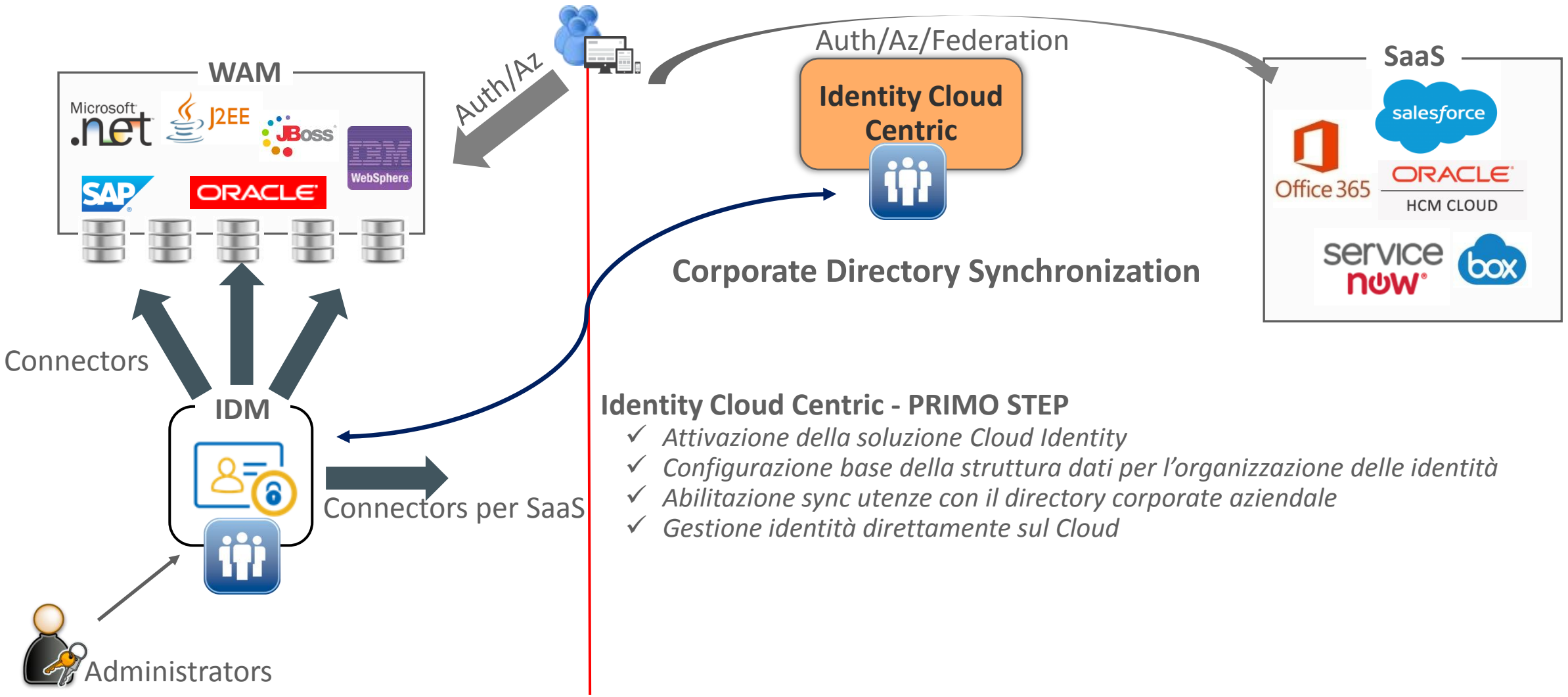


Aspetti critici

- ✓ *Difficoltà nella governance delle identità utente e relativi account*
- ✓ *Diverse policies di autenticazione e gestione delle password*
- ✓ *Problemi nel controllo accessi basato su: user/device/location*
- ✓ *Attività utenti non monitorate*
- ✓ *No incident response automatizzati*
- ✓ *No policies sul controllo dei dati*

Oggi, le sole soluzioni IAM e gli strumenti di sicurezza tradizionali non sono adeguati ed efficienti per garantire un conrollo completo delle architetture ibride

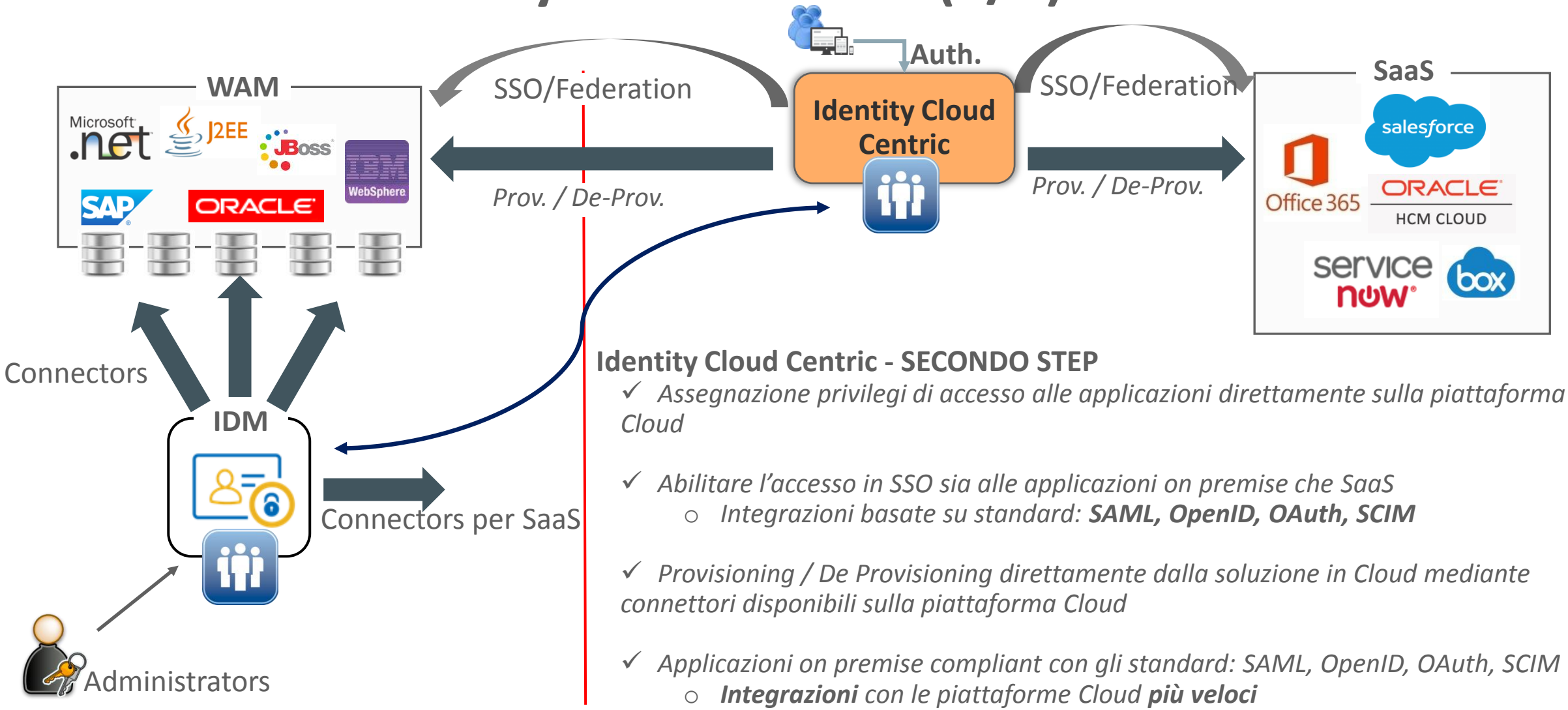
Architetture Identity Cloud Centric (1/3)



Identity Cloud Centric - PRIMO STEP

- ✓ *Attivazione della soluzione Cloud Identity*
- ✓ *Configurazione base della struttura dati per l'organizzazione delle identità*
- ✓ *Abilitazione sync utenze con il directory corporate aziendale*
- ✓ *Gestione identità direttamente sul Cloud*

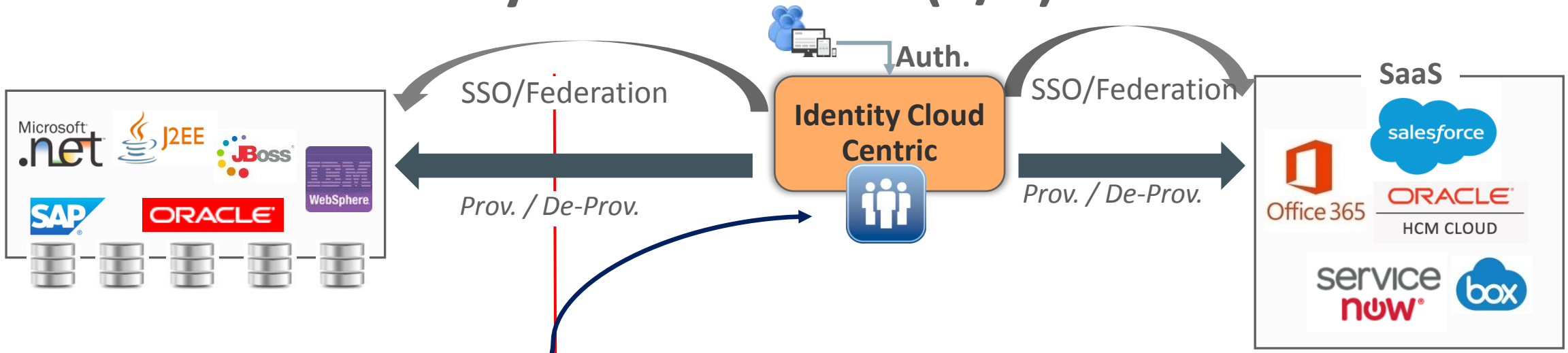
Architetture Identity Cloud Centric (2/3)



Identity Cloud Centric - SECONDO STEP

- ✓ *Assegnazione privilegi di accesso alle applicazioni direttamente sulla piattaforma in Cloud*
- ✓ *Abilitare l'accesso in SSO sia alle applicazioni on premise che SaaS*
  - *Integrazioni basate su standard: **SAML, OpenID, OAuth, SCIM***
- ✓ *Provisioning / De Provisioning direttamente dalla soluzione in Cloud mediante connettori disponibili sulla piattaforma Cloud*
- ✓ *Applicazioni on premise compliant con gli standard: SAML, OpenID, OAuth, SCIM*
  - ***Integrazioni** con le piattaforme Cloud **più veloci***

Architetture Identity Cloud Centric (3/3)



Gestione del Corporate Directory

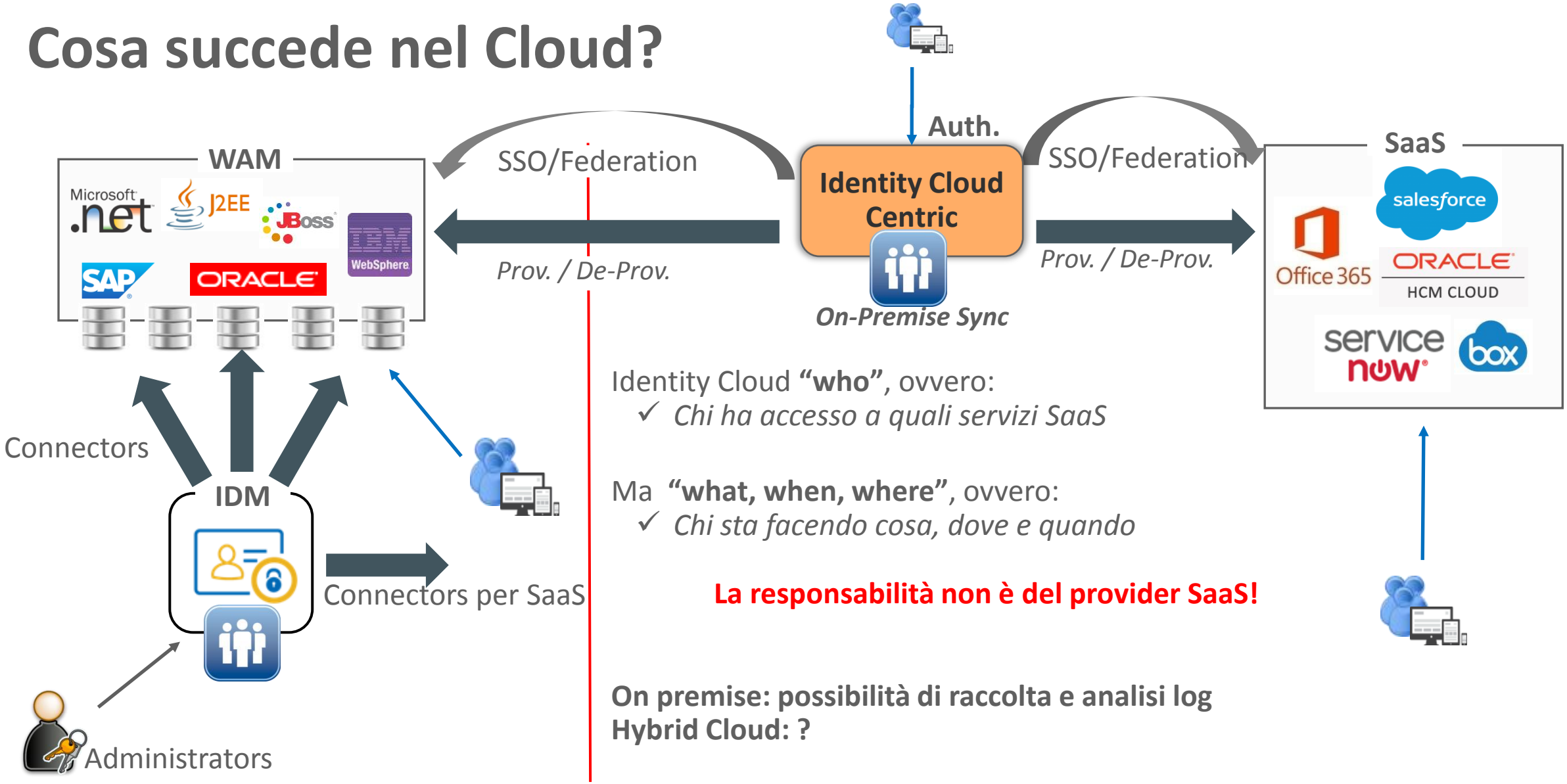
Administrators

Identity Cloud Centric – STEP FINALE

- ✓ *Dismissione soluzioni IDM e WAM on-premise*
- ✓ *Applicazioni on premise compliant con gli standard: OAuth, OpenID, SAML*
  - *Veloce integrazione con le piattaforme Cloud*
  - *Affrontare il piano di migrazione delle applicazioni on premise verso il Cloud*

ON PREMISE **CLOUD**

Cosa succede nel Cloud?



Identity Cloud **"who"**, ovvero:

- ✓ *Chi ha accesso a quali servizi SaaS*

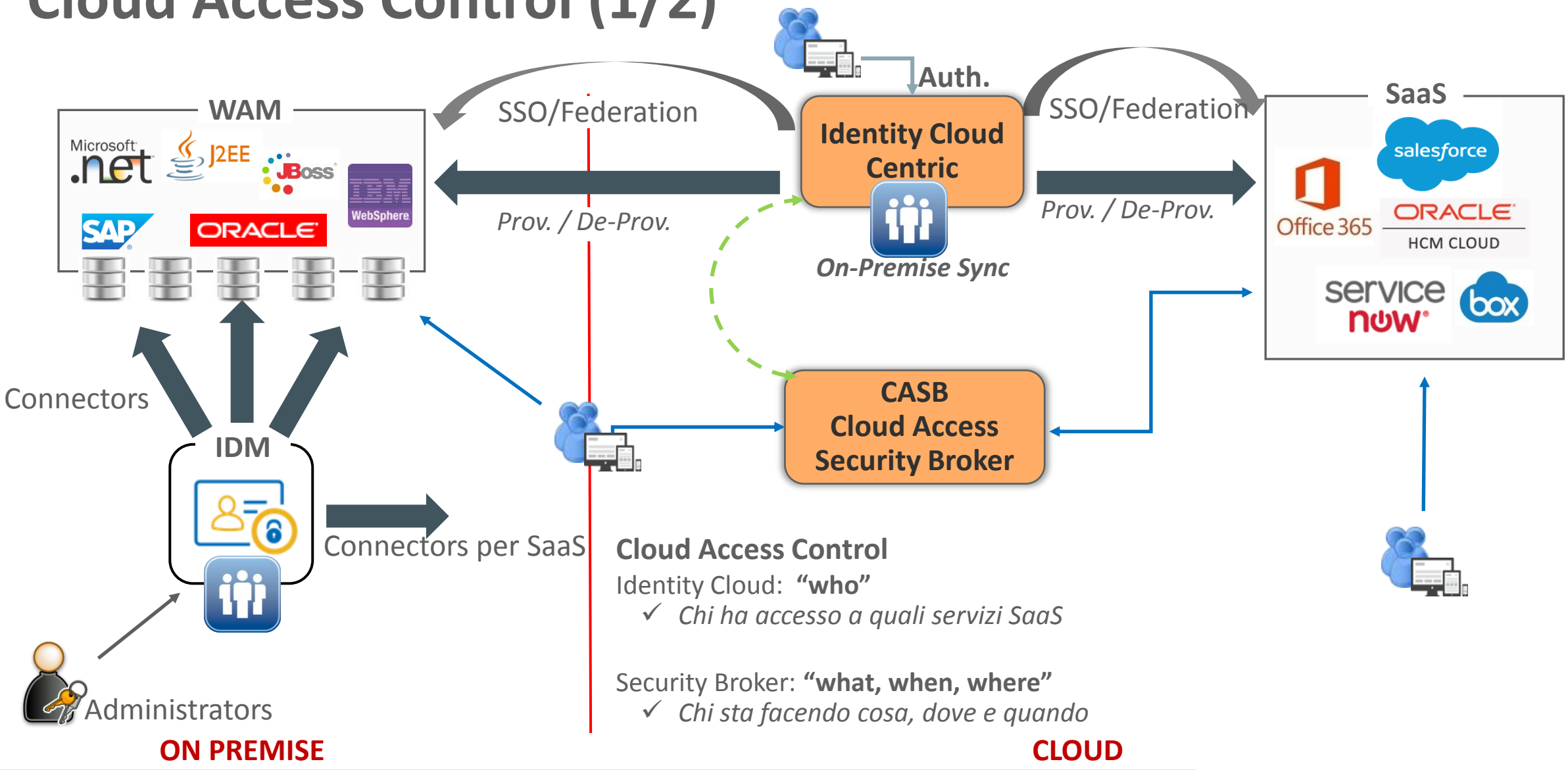
Ma **"what, when, where"**, ovvero:

- ✓ *Chi sta facendo cosa, dove e quando*

La responsabilità non è del provider SaaS!

On premise: possibilità di raccolta e analisi log
Hybrid Cloud: ?

Cloud Access Control (1/2)



Cloud Access Control

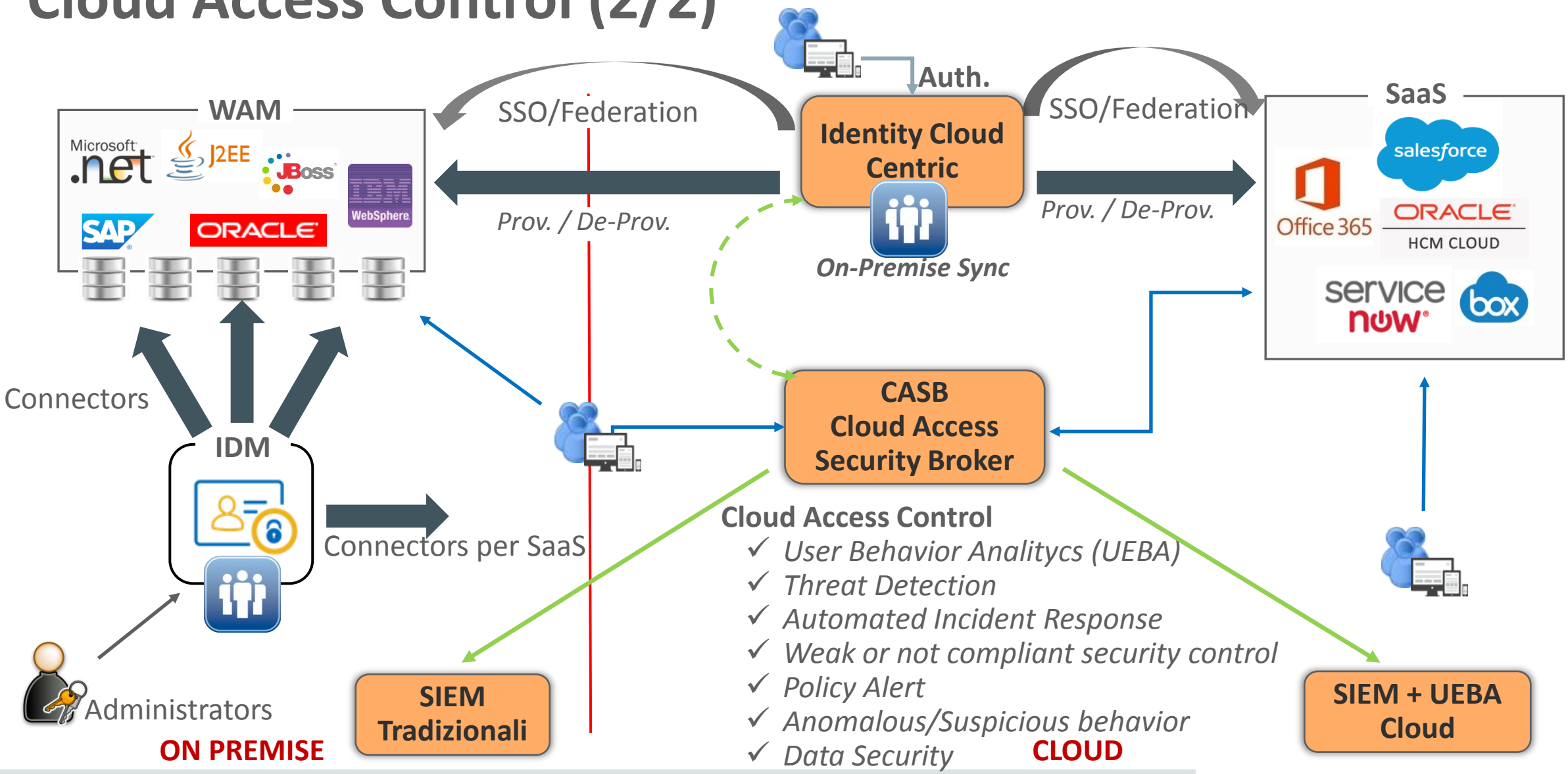
Identity Cloud: **"who"**

- ✓ *Chi ha accesso a quali servizi SaaS*

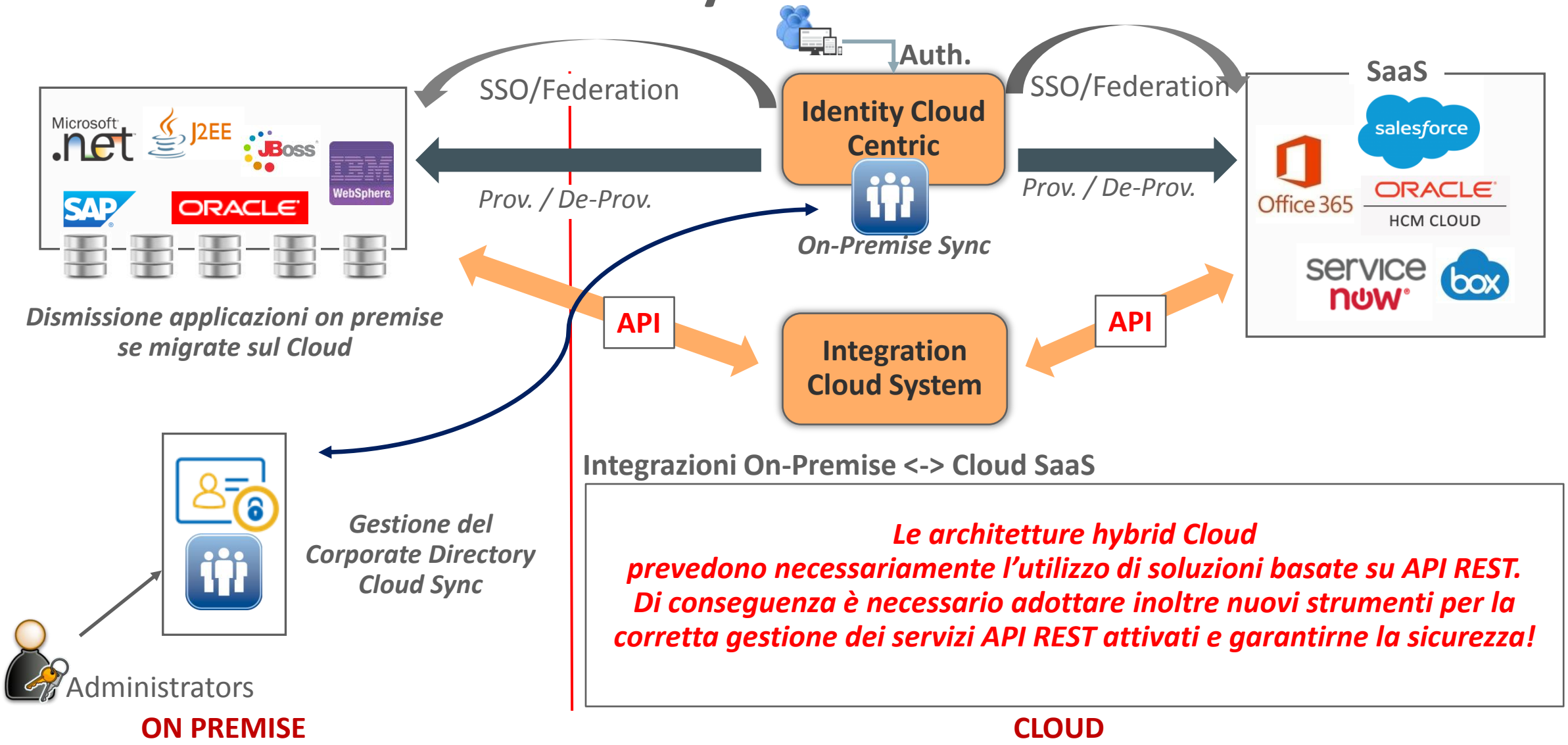
Security Broker: **"what, when, where"**

- ✓ *Chi sta facendo cosa, dove e quando*

Cloud Access Control (2/2)

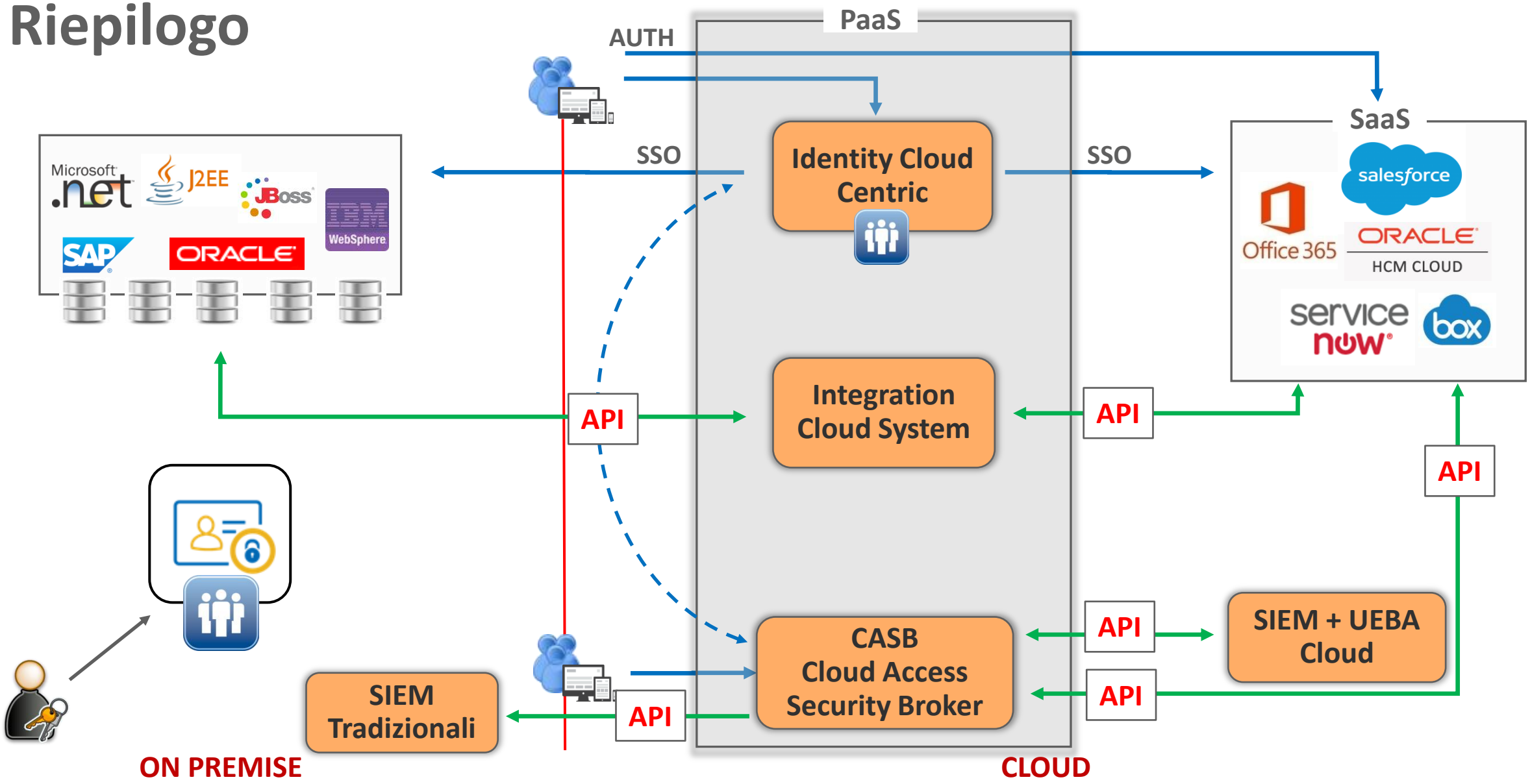


Estensione architettura “Hybrid Cloud”



Le architetture hybrid Cloud prevedono necessariamente l’utilizzo di soluzioni basate su API REST. Di conseguenza è necessario adottare inoltre nuovi strumenti per la corretta gestione dei servizi API REST attivati e garantirne la sicurezza!

Riepilogo


PaaS
AUTH
SSO
SSO
Identity Cloud Centric
SaaS
Microsoft .net
J2EE
JBoss
WebSphere
SAP
ORACLE
Office 365
salesforce
ORACLE HCM CLOUD
service now
box
API
Integration Cloud System
API
API
CASB Cloud Access Security Broker
API
API
SIEM + UEBA Cloud
API
SIEM Tradizionali
ON PREMISE
CLOUD

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Security Gaps Are Widening

Growing Threat Sophistication + Shrinking Visibility + Accelerated Change + Overwhelmed SOC

- ! New and unknown vectors
- ! Low & slow, multi-stage threats
- ! Targeted attacks

- ! Cloud adoption, shadow IT
- ! BYOD, unmanaged devices
- ! "Identity" - the only remaining perimeter

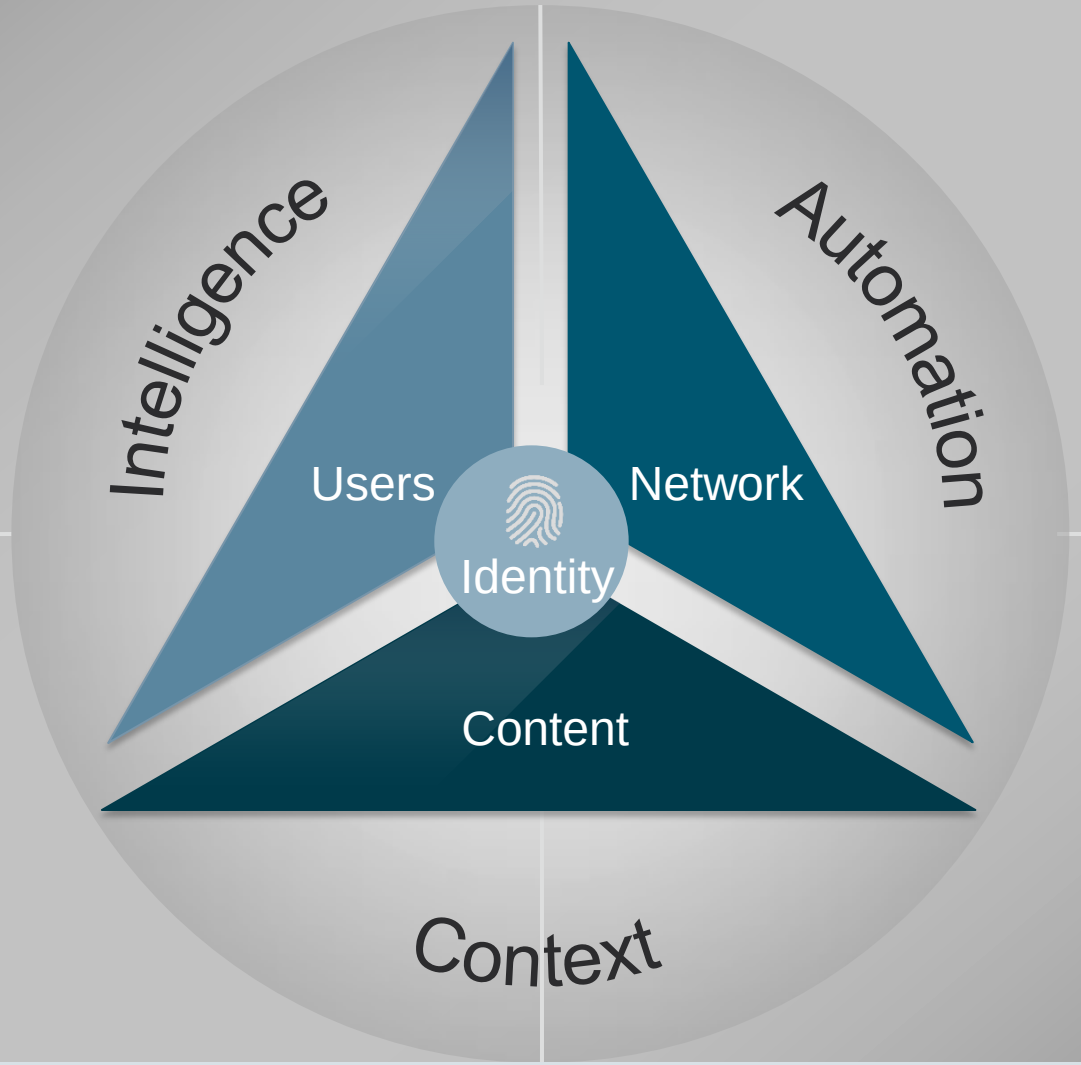
- ! Continuous integration/delivery
- ! Higher risk of mis-configuration
- ! Shrinking detection windows

- ! More things to monitor
- ! More tools, more alerts
- ! Staffing shortages

Security Intelligence Delivered with Identity

Predict

Prevent



Respond

Detect

Identity SOC Technologies

Oracle Identity SOC Solution

One-Stop SOC Dashboard

Security Monitoring & Analytics + Compliance Cloud Services

Content Security	User Security	Services Security
CASB Cloud Service	Identity Cloud Service	API Platform Cloud Service

Security Posture

Applications, data and user activity analytics, threat intelligence, and compliance

Automated Incident Response & Remediation
(Orchestration Cloud Service)

Identity Cloud Service

Modern App Security

Centralized authentication, authorization, user management and self-service based on latest open standards for rapid integration of applications

Hybrid Identity

Manage user identities for both cloud and on-premises applications with enterprise-grade hybrid deployments

Secure Defense In-depth

Gain layers of defense with Identity hosted as an Oracle Public Cloud (OPC) service, integrated with cloud security fabric and implementing behavioral authentication for application access control

ORACLE

CLOUD PLATFORM

Intelligence
Risk & Context, Threat

Multi Factor Auth
Strong Auth.

Provisioning
Account, LC mgmt.

Oracle Identity Cloud Service

Access Mgmt.
SSO, Federation

Governance
Certs, Access Requests, SoD

ID Admin
User Mgmt.

Cloud Directory
ID Store

Employee

Partners

Consumers

Google Apps · box · WordPress · SharePoint · salesforce · workday. · Office 365

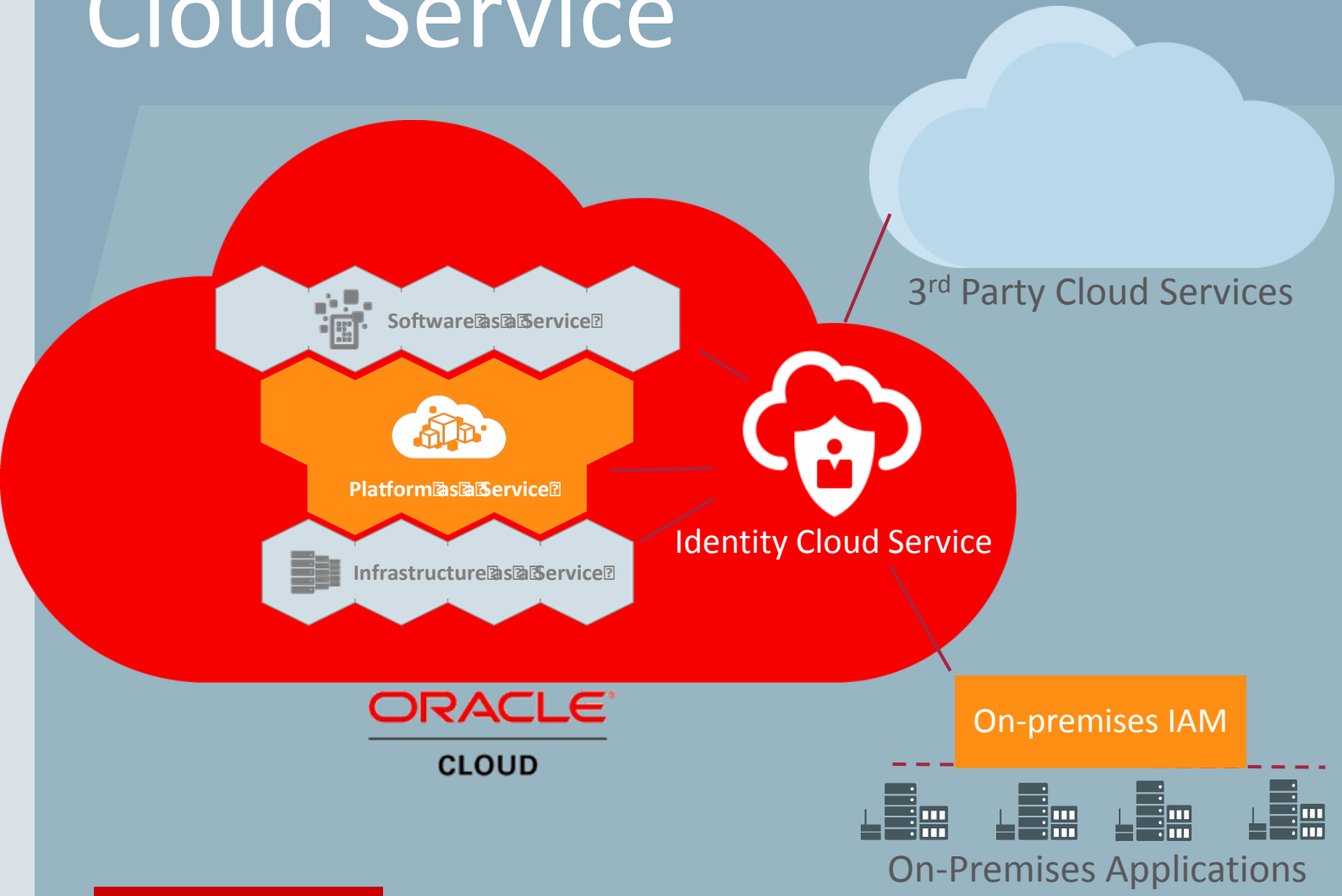
Cloud applications

On Premises

Apps

Apps

Identity Cloud Service



- Cloud-Native Multi-tenant platform on the Oracle Cloud
- Manage Users
  - Sync identities, SSO, Federation
- Manage Applications
  - Integrate using open standards
- Manage Policies
  - Protect Applications using strong access control policies

CASB
Cloud Service

Discover

Continuous visibility into cloud risk covering sanctioned and unsanctioned SaaS, PaaS, and custom applications on IaaS

Secure

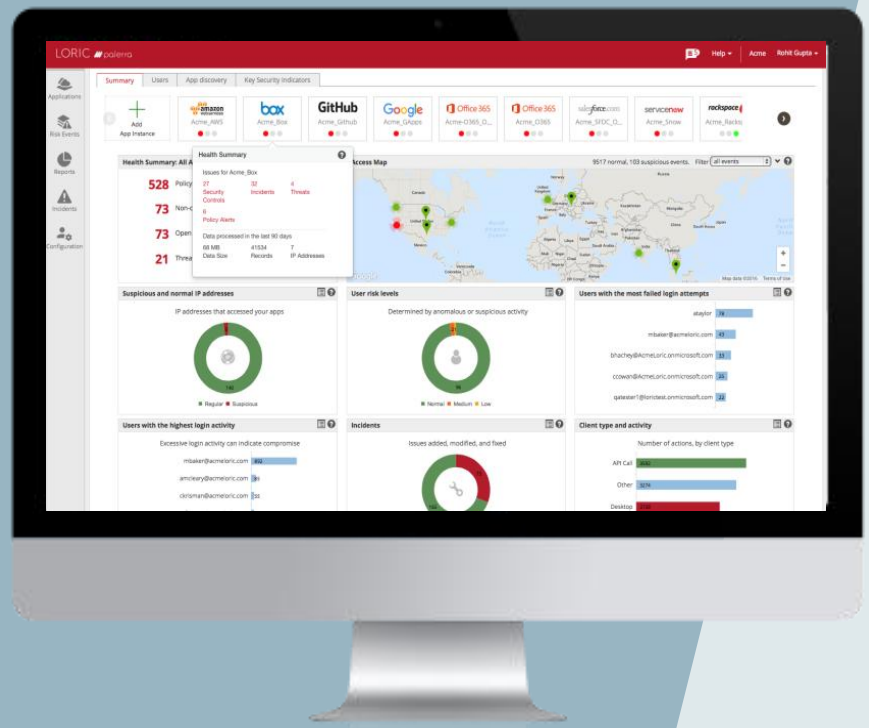
Automated controls covering users, data, content, applications, settings, and infrastructure with actionable intelligence

Monitor

Continuous monitoring of user activity and security configurations identifying threats and compliance risks

Respond

Automate incident management and remediation through native features as well as integration with existing solutions



Securing Clouds: Iaas Paas Saas

CASB CS

- Visibility
- Compliance
- Data Security
- Threat Protection

My mission-critical apps need deep monitoring and governance!

amazon web services
Office 365
salesforce
G Suite
box
servicenow
rackspace
GitHub
slack
ORACLE HUMAN CAPITAL MANAGEMENT CLOUD
Custom apps in AWS
Oracle Cloud Infrastructure as a Service

I need broad visibility into all apps in use!

ORACLE

CASB Cloud Service

ENTERPRISE

MOBILE USERS AND DEVICES

INSIDE PERIMETER

SIEM
IDaaS
NGFW
DLP
MDM

Direct Cloud Service Access

API Access

CASB CS

- Visibility
- Compliance
- Data Security
- Threat Protection

Enterprise Security Integration

box
amazon web services
Office 365
G Suite
GitHub
salesforce
slack
ORACLE
servicenow

IaaS PaaS SaaS

The only CASB to be deployed in <5 minutes

API Platform Cloud Service

Build - Create APIs on top of existing services to enable access to data formerly locked inside your legacy apps and data stores.

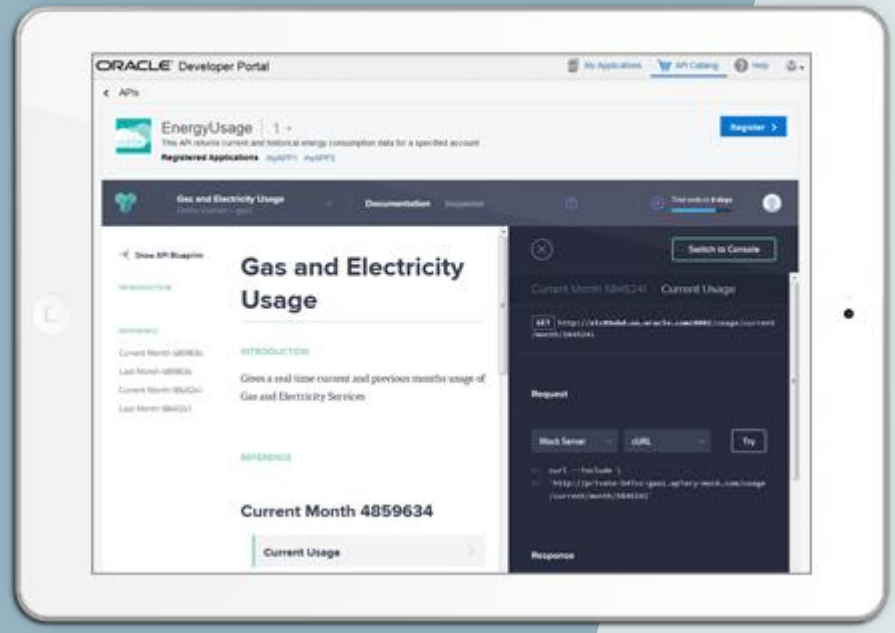
Secure – Assign standard security & threat protection to APIs with no coding, including OAuth 2.0, IP filtering, and rate limiting.

Deploy - Choose Cloud or on-premises gateway deployment with the ease of a single-click.

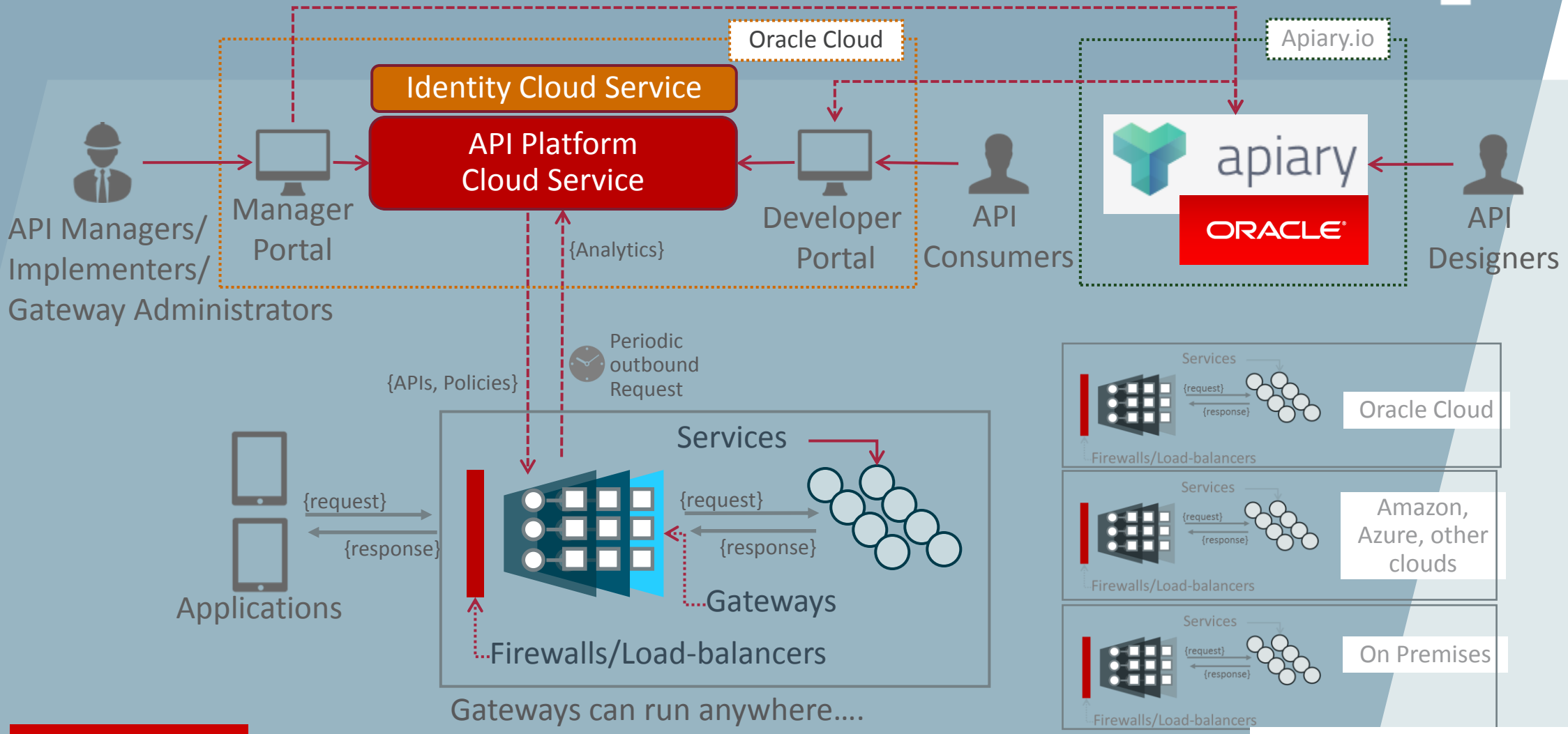
Publish - Browse a comprehensive list of proven APIs from Oracle, the community, and your own organization.

Consume - Register third-party apps easily to allow them the same seamless API utilization as pre-loaded Oracle SaaS APIs.

Monitor - View operational API metrics on a single dashboard to take action quickly.



API Platform Cloud Service



Oracle Management Cloud

cloud.oracle.com

END USER EXPERIENCE/ACTIVITY

APPLICATION

MIDDLE TIER

DATA TIER

VIRTUALIZATION TIER

INFRASTRUCTURE TIER

Global Threat Feeds
CASB
Identity

Real Users
Synthetic Users

App metrics
Transactions

Server metrics
Diagnostics
Logs

Host metrics
VM metrics
Container metrics

CMDB/Compliance
Tickets
Alerts

Security Events

Application Performance Monitoring

Log Analytics

IT Analytics

Security Monitoring & Analytics

Compliance

Infrastructure Monitoring

Orchestration

INTELLIGENT, UNIFIED PLATFORM

POWERED BY A COMPLETE DATA SET

HETEROGENEOUS AND OPEN

POWERED BY MACHINE LEARNING

ORACLE

Security Monitoring and Analytics Cloud Service

Comprehensive Detection

Any log, any intelligence feed, any metric, any location (on-premises or cloud) using machine learning driven analytics and visualization

Rapid Investigation

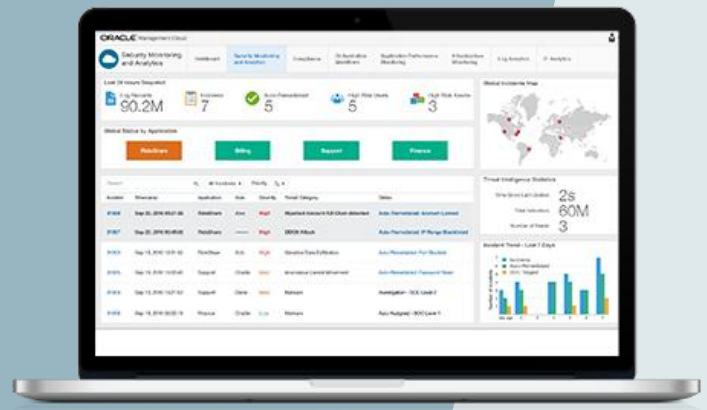
Intuitive visualization of threats and early warning signs

Intelligent Remediation

Powerful auto-remediation framework for any IT stack

Faster Time to Value

Next-gen cloud service with SOC ready content



Compliance Cloud Service

Standards Based

Execute industry standard compliance benchmarks at cloud scale

Application & Cloud Aware

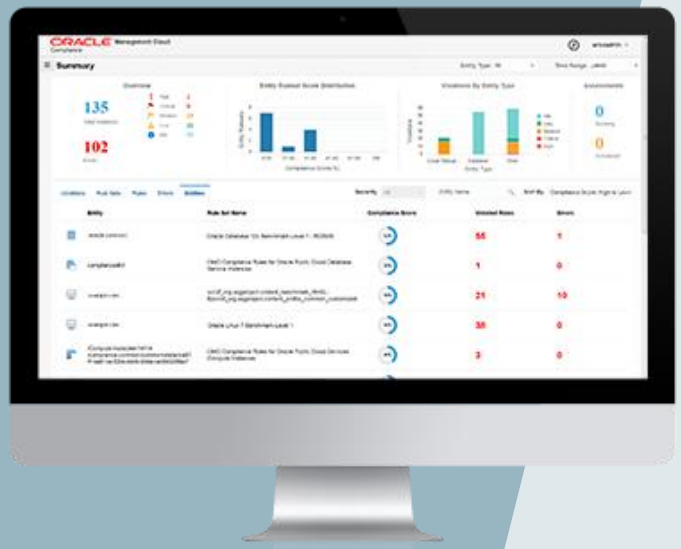
Assess compliance against infrastructure and applications stacks, on-premises or in the cloud

Efficient & Actionable

Quickly determine your enterprise compliance posture and remediate violations

Extensible

Execute custom scripts and enforce your organization's standards



Orchestration Cloud Service

Topology Aware Execution

Execute workflows on dynamic application topologies accurately without change.

Invoke scripts, web service endpoints or 3rd party automation frameworks

For Cloud as well as On-Premise

Integration

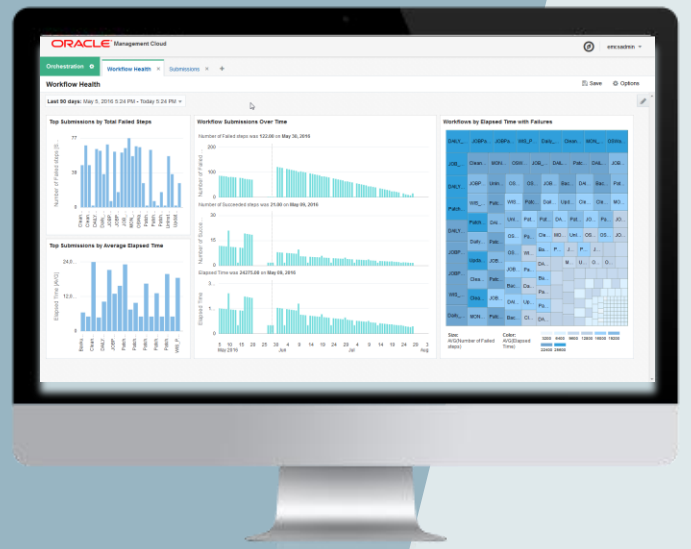
Flexible Workflow Log Retention and Powerful Analytics using built in Log Analytics integration

Enhances other OMC services by providing ability to take action

Pre-Built Dashboards

Role based dashboards for IT Operations and management

Build custom dashboards using UDE

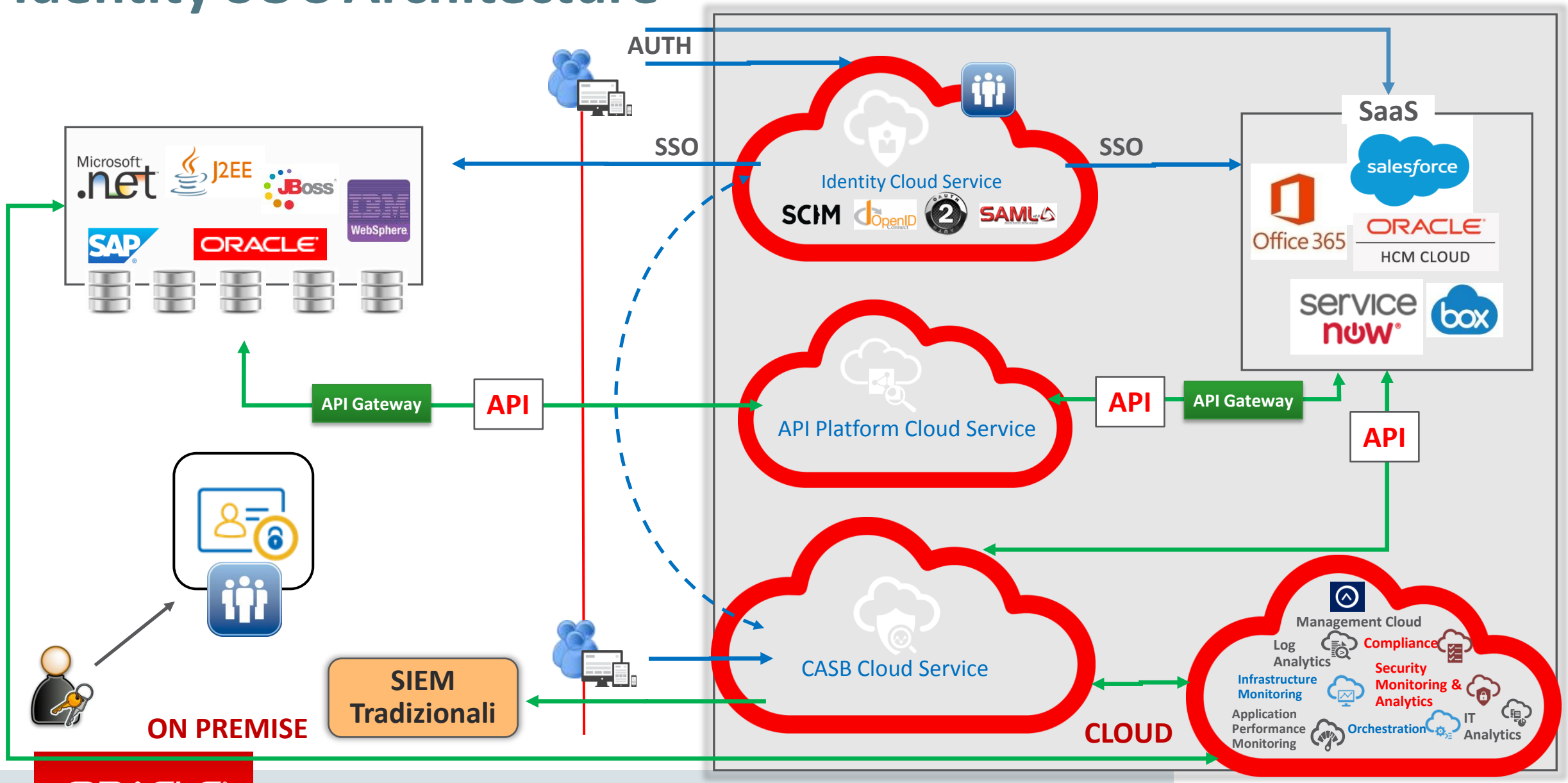


Unified Data, Machine Learning: Better Security

Increased Analysis Sophistication + Complete Visibility + Managed Change + Turbo-charged IdentitySOC

- ✓ Anomaly detection
- ✓ Attack chain awareness
- ✓ 360° user & identity awareness
- ✓ Cross-cloud monitoring
- ✓ User sessionization
- ✓ Complete identity management
- ✓ Continuous assessment
- ✓ Benchmarking
- ✓ Drift analysis
- ✓ Real-time remediation
- ✓ Risk based prioritizatior
- ✓ Single pane of glass
- ✓ Stack-independent orchestration

Identity SOC Architecture



VANTEA SMART

ORACLE

Oracle Community For Security

VANTEA SMART

ORACLE