



Cloud Security/Access Control and Identity Management

- Patrick McLaughlin, Oracle Fellow
- SAOUG: 14 November, 2011



Agenda

- Evolution of IT and IdM Requirements
- Building and Securing Clouds
- Oracle Public Cloud – usage of IdM
- Identity as a Service – Customer Case
- Summary





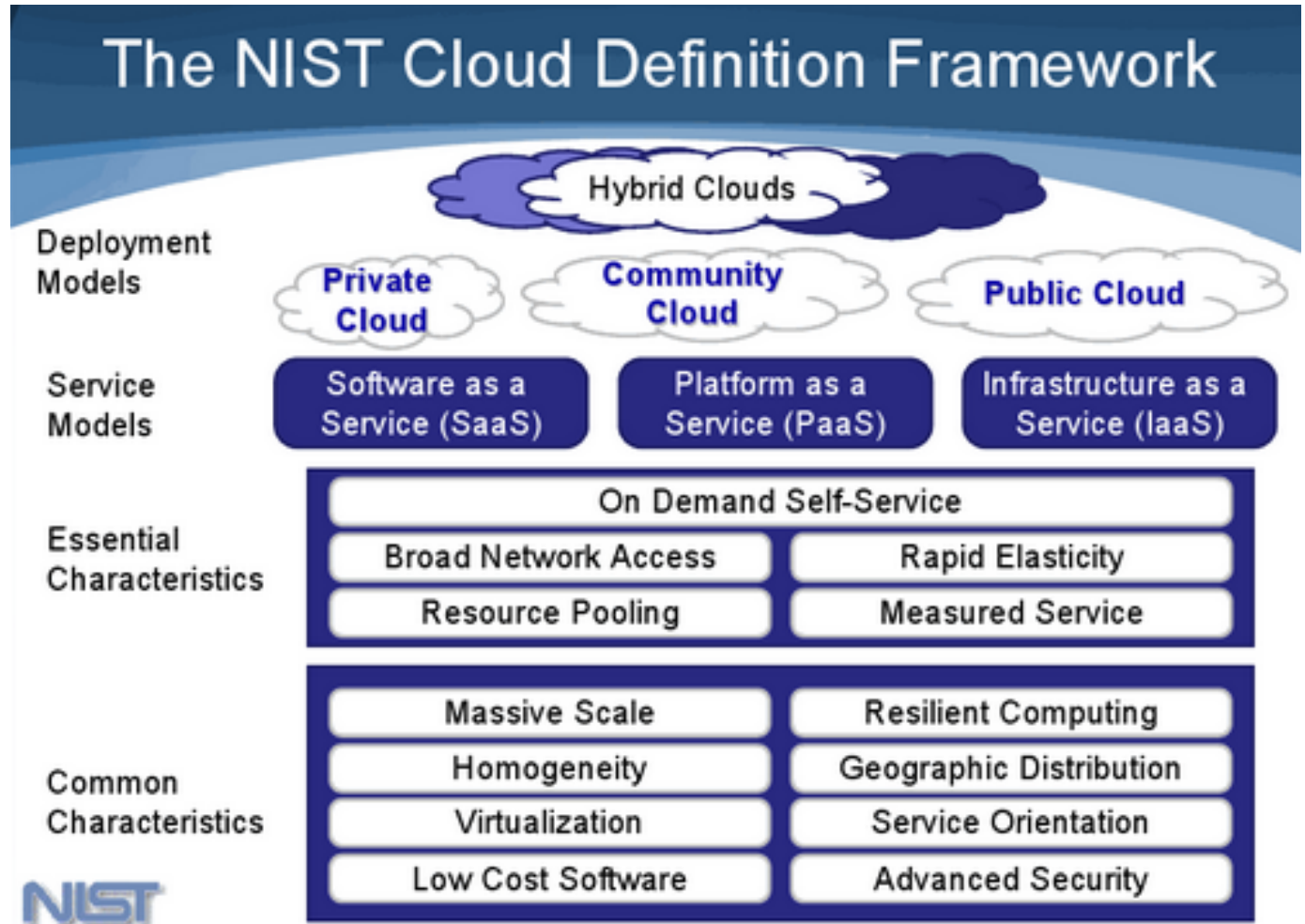
Agenda

- Evolution of IT and IdM Requirements
- Building and Securing Clouds
- Oracle Public Cloud – usage of IdM
- Identity as a Service – Customer Case
- Summary





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.

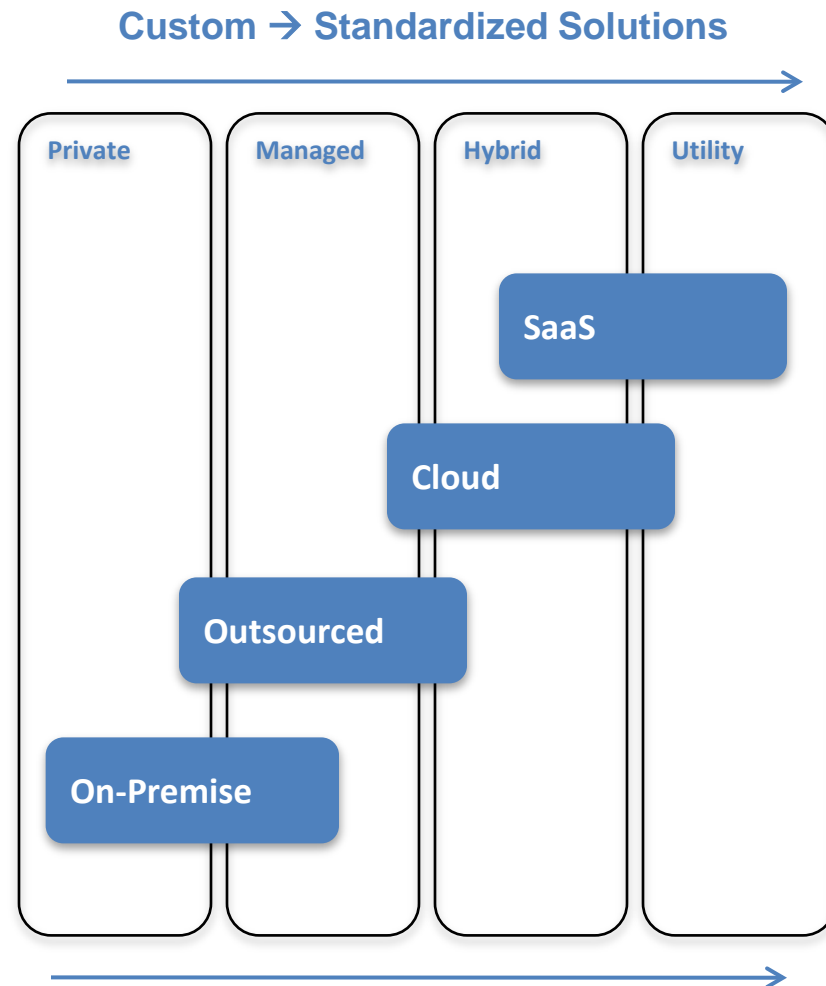


Cloud computing is a model for enabling convenient, **on-demand** network **access** to a shared pool of configurable **computing resources** (e.g., networks, servers, storage, applications, and services) that can be **rapidly provisioned** and released with **minimal management effort** or service provider interaction.

Evolution Towards Cloud



- Customer Benefits
 - Reduce Capital Expenses With Subscription Pricing
 - Reduce Management Costs And Simplify Upgrading
 - Leverage Elastic Scalability Services
 - Enable Hybrid Cloud Computing
- Natural Maturation Of The IT Industry
 - Customers Want Fully Integrated Industry-vertical Business Solutions
 - Cost To Integrate & Deploy Is A Major Inhibitor To Idm's Success; Far Exceeds Cost To Acquire & Manage
 - In The End Very Few Customers Will Want "Parts"





End User Requirements are Changing



There is a growing fragmentation
between the Enterprise and the
cloud mobile and social world

87% Security main barrier to
Cloud Adoption

Source: IDC Enterprise Panel, 3Q09

66% Concerned about
maintaining compliance on
social sites

Forrester, 2010

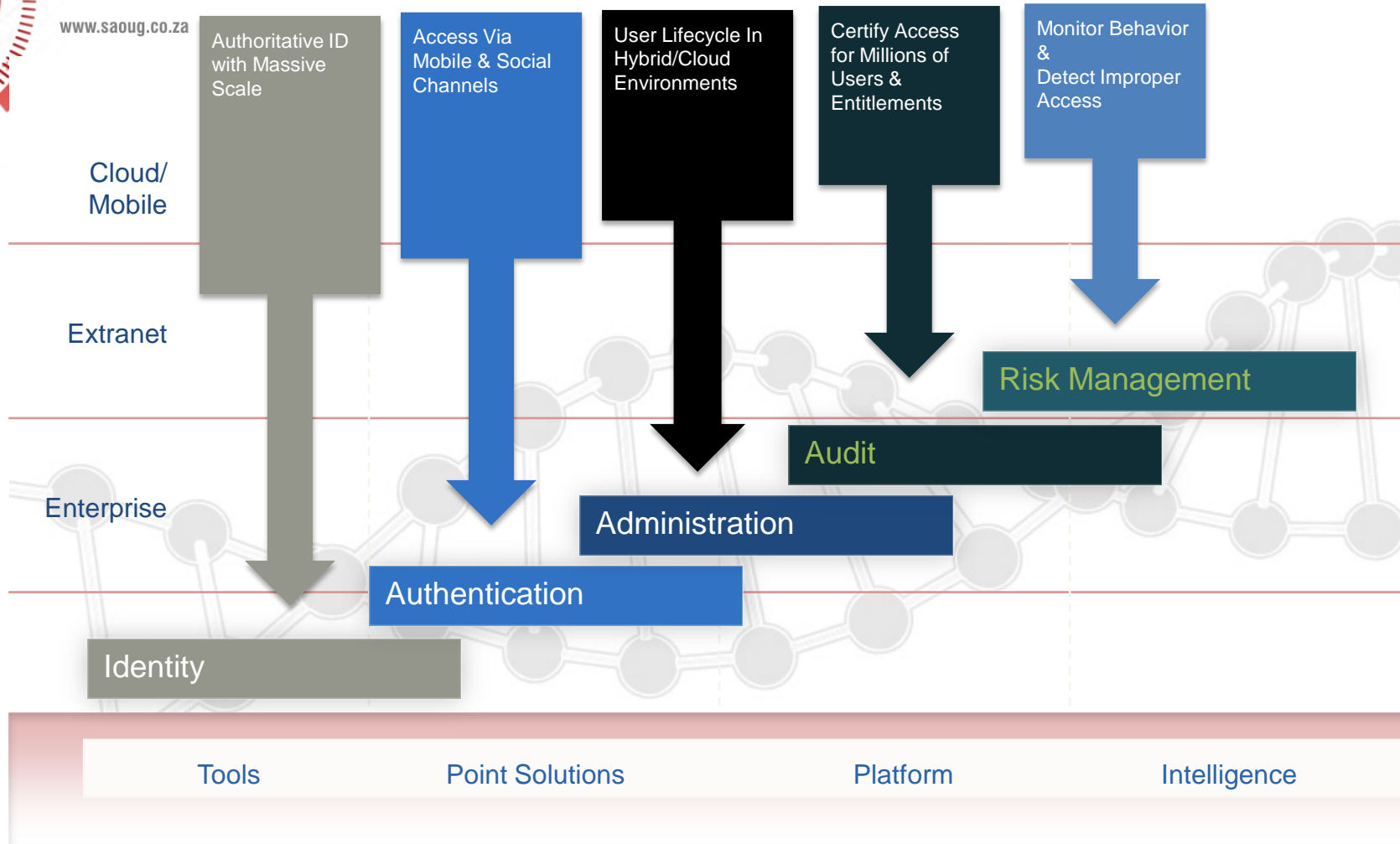
58% Building Corporate Mobile
app stores

Partnerpedia Survey Aug 2011

79% Of fortune 500 use social
media to connect with
customers

Burson-Marsteller, 2009

Evolution of Identity Management





Agenda

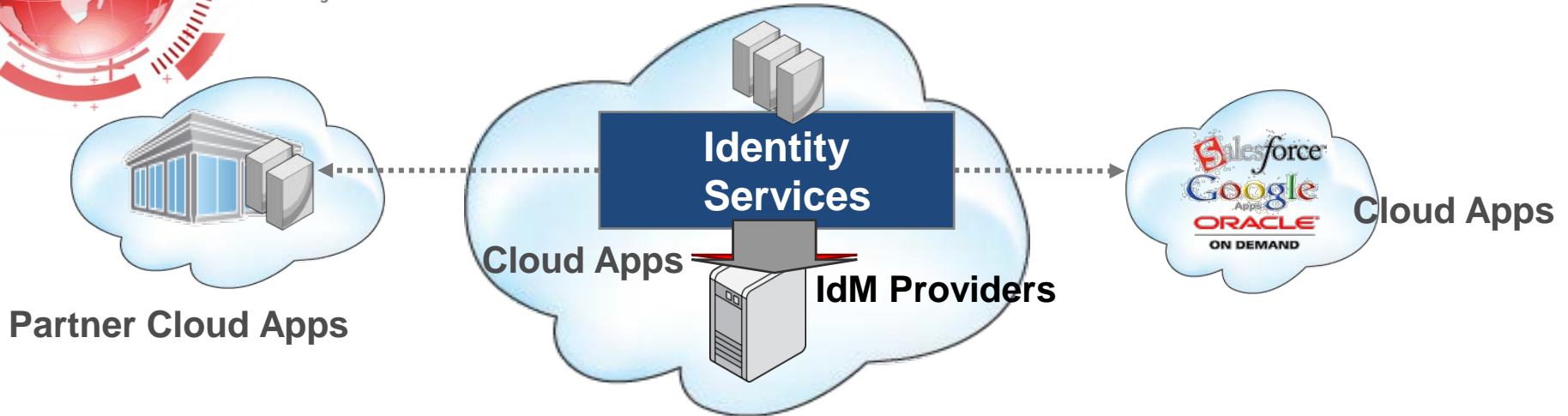
- Evolution of IT and IdM Requirements
- **Building and Securing Clouds**
- Oracle Public Cloud – usage of IdM
- Identity as a Service – Customer Case
- Summary



Building and Securing Cloud Apps

deliver the
PROMISE
www.saoug.co.za

Private, Public or Hybrid Cloud



- Customers looking to build Cloud Apps & Services
 - Telco Clouds and SDPs
 - Trust and Federation Clouds
 - Clouds offering Consumer Services
 - MSPs that need to manage customer identities across environments
- Need to integrate with in-house, customer , or partner ID Services
- **Key Solution Ingredients:**
Standards-based - SAML, SPML, OAUTH, OpenID...



Securing a Cloud App

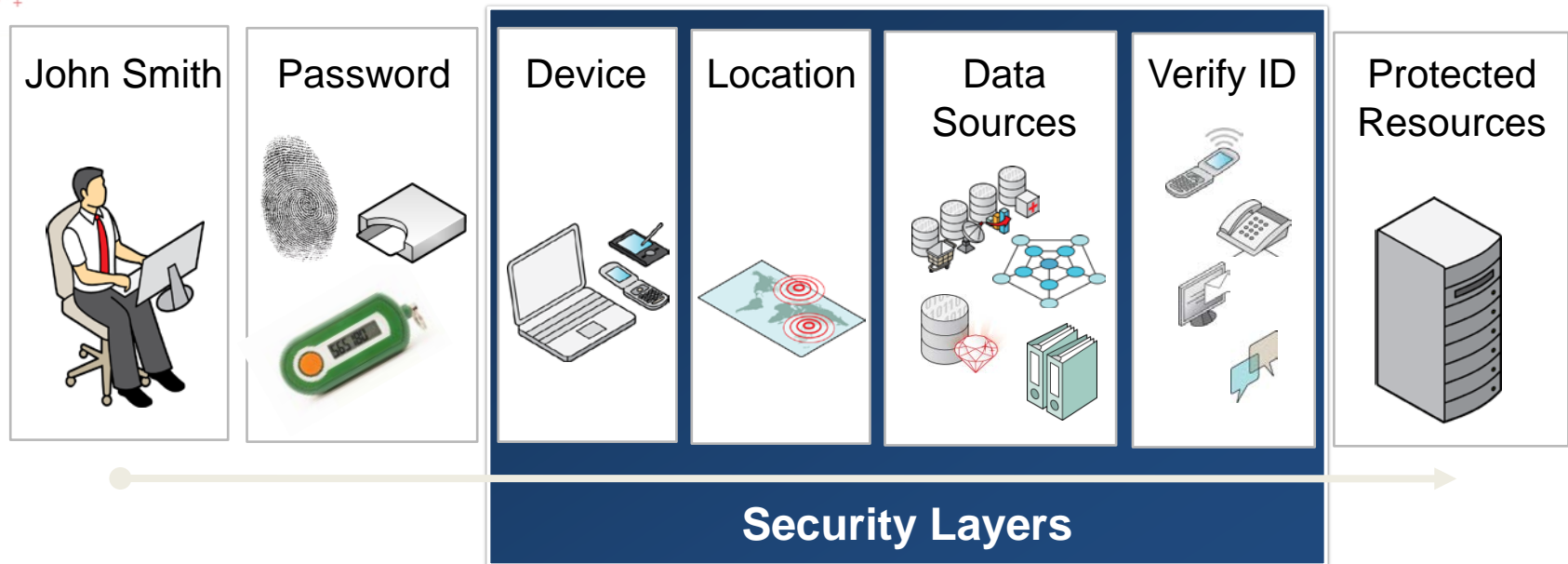
Standards-based Interoperable Identity Services

- Need to extend identity administration and **access review/certification** to cloud applications
- Need to handle customer on-boarding / **provisioning using SPML**
- Need to provide **SSO** and simple user experience
- At the same time cloud consumers may want to **have local authentication** and federate to the cloud provider (SAML) or to **delegate authentication to the cloud provider**
- Also, cloud consumers need to ensure users can securely access applications from **a range of different devices**...this too creates the need for local security enforcement.



Securing a Cloud App

Stronger, Risk based Authentication



Authentication is valid but **is this really John Smith?**

Is **anything suspicious** about John's access request?

Can John answer a **challenge** if the risk is high?



Securing a Cloud App

Stronger, Risk based Authentication

- ✓ Analyses risk in Real-Time
- ✓ Profiles Behaviors
- ✓ Recognises Patterns
- ✓ Detects Anomalies
- ✓ Takes Preventative Actions

Predictive Analysis

- Indicates probability a situation would occur
- Is the probability less than 5% that an access request would have this combination of data values?

Pattern Detection

- Dynamic behavioral profiling in real-time
- In the last month has Joe used this device for less than 3% of his access requests?
- In the last three months have less than 1% of all users accessed from the country?

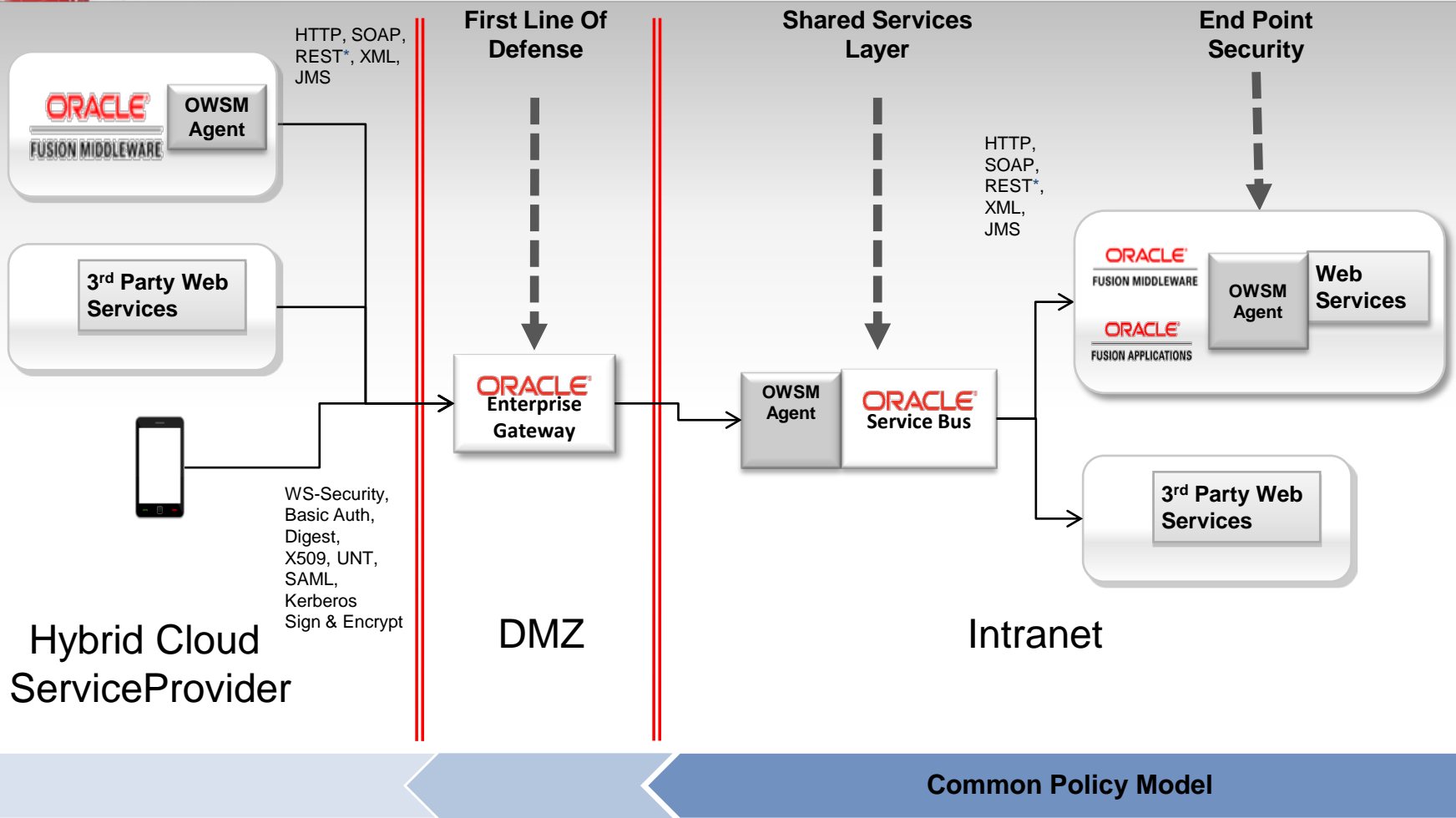
Static Scenarios

- Specific scenarios that always equate to risk
- If a device appears to be traveling faster the jet speed between logins the risk is increased.

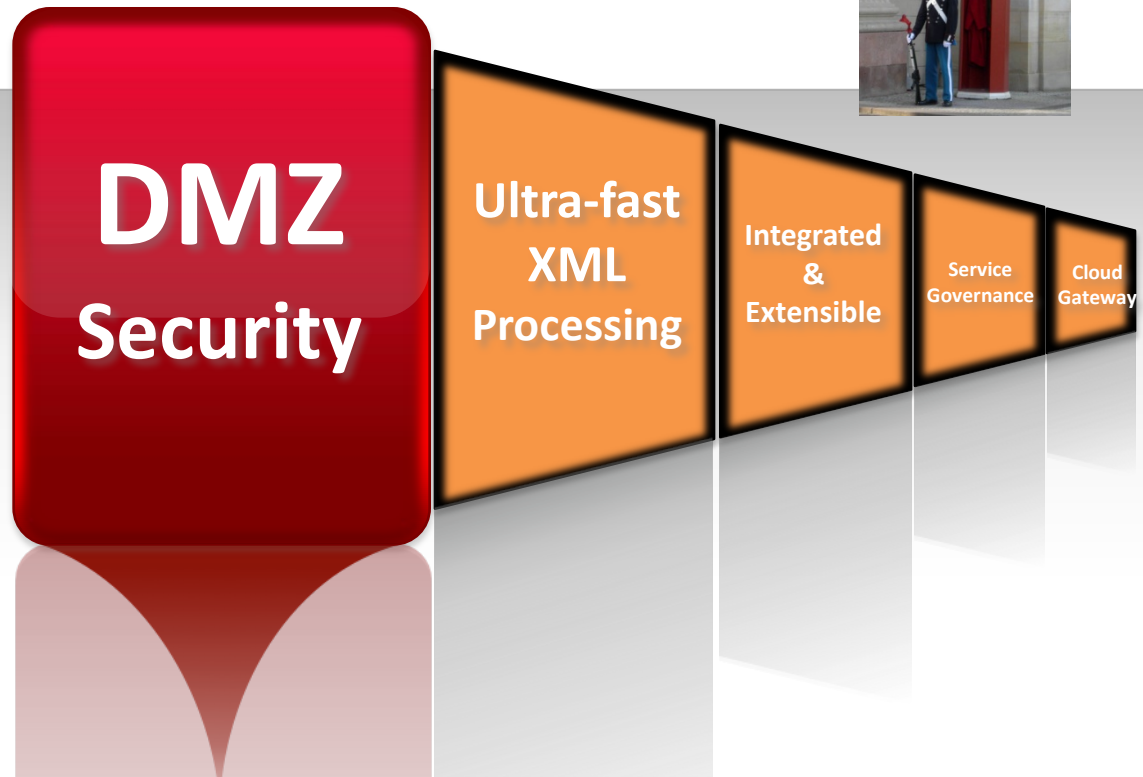


Securing a Cloud App

Securing Services in a Hybrid Cloud



Oracle Enterprise Gateway



XML INTRUSION DETECTION

- ☑ Content Attack
- ☑ Schema/DTD Attack
- ☑ Crypto Attack
- ☑ Virus Scanning

ACCESS ENFORCEMENT

- ☑ Authentication, ID Propagation
- ☑ Fine Grained AuthZ
- ☑ Throttling
- ☑ Transport/Message Security

MONITORING AND AUDIT

- ☑ Real-time Monitoring
- ☑ Reporting
- ☑ Audit and Compliance

Oracle Enterprise Gateway



Cloud Gateway

IAAS PAAS SAAS

- ☑ Deployments on EC2, Oracle VM

- ☑ Control cloud services
- ☑ Regulate service usage
- ☑ Continuous traffic monitoring

- ☑ Data Redaction
- ☑ Detect rogue usage
- ☑ REST security
- ☑ OAuth Support



Agenda

- Evolution of IT and IdM Requirements
- Building and Securing Clouds
- Oracle Public Cloud – usage of IdM
- Identity as a Service – Customer Case
- Summary





Welcome to the Oracle Public Cloud

An Enterprise Cloud for your Business



Notify Me of Updates >

Application Services



Fusion CRM

Sell smarter with Fusion CRM in the cloud.



Fusion HCM

Bring power to your people with Fusion HCM.



Social Network

A secure collaboration tool for everyone you work with.

Platform Services



Java

All the productivity of Java, without the IT.



Database

The Oracle database you love, now in the cloud.



OFFERINGS

[Fusion CRM](#)

[Fusion HCM](#)

[Social Network](#)

[Java](#)

[Database](#)

LEARN MORE

[How It Works](#)

[Why Oracle?](#)

[Architecture](#)

[FAQ](#)

CONTACT

[Interest List](#)

[Press](#)

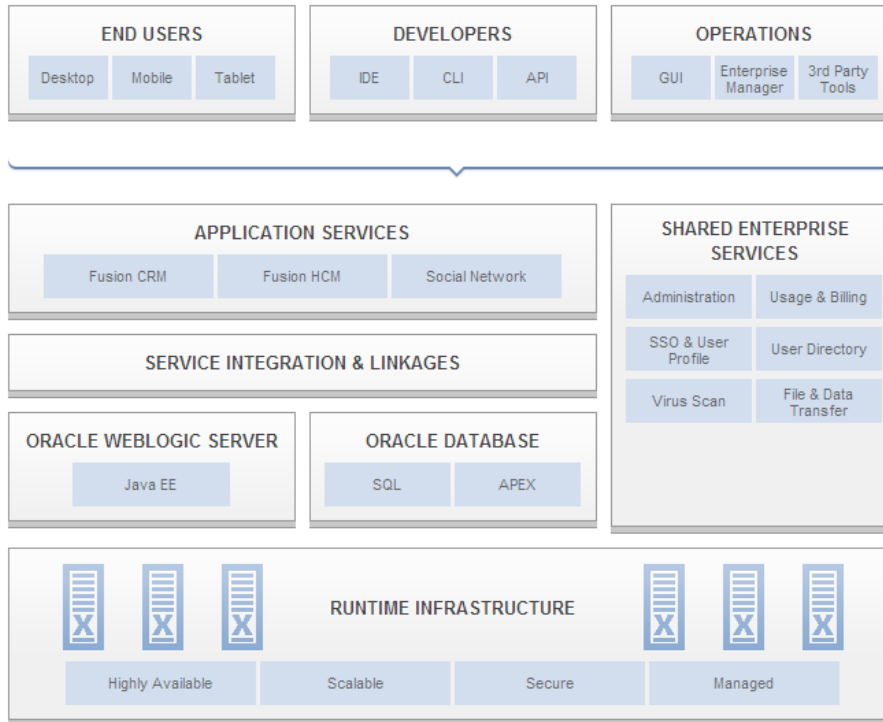
NAVIGATE

[Home Page](#)

For information about Oracle's other offerings for cloud computing, go to oracle.com/cloud.

[About Oracle](#) | [Oracle and Sun](#) | [Subscribe](#) | [Careers](#) | [Contact Us](#) | [Site Maps](#) | [Legal Notices](#) | [Terms of Use](#) | [Your Privacy Rights](#)

20111005_01



Architecture

Oracle's Public Cloud gives you all the benefits you want without the limitations you don't.

For us, it's a lot of work. For you, it's the ease of the cloud and the power of Oracle.

[Why the Oracle Public Cloud? >](#)

OFFERINGS

[Fusion CRM](#)

[Fusion HCM](#)

[Social Network](#)

[Java](#)

LEARN MORE

[How It Works](#)

[Why Oracle?](#)

[Architecture](#)

[FAQ](#)

CONTACT

[Interest List](#)

[Press](#)

NAVIGATE

[Home Page](#)



Oracle Public Cloud

Security/Identity Management Services

- Built on industry-leading Oracle Identity Management
- Single Sign On
- Full delegated administration and self service
- Tenant administration and dashboards
- Bulk on-boarding
- Customisable UIs for customer branding
- Premium services
 - Identity Federation down to desktop for streamlined user experience
 - Multi-factor authentication to reduce risk of unauthorized access



ORACLE®
PUBLIC CLOUD



Virus Scanning and White List Audit Service

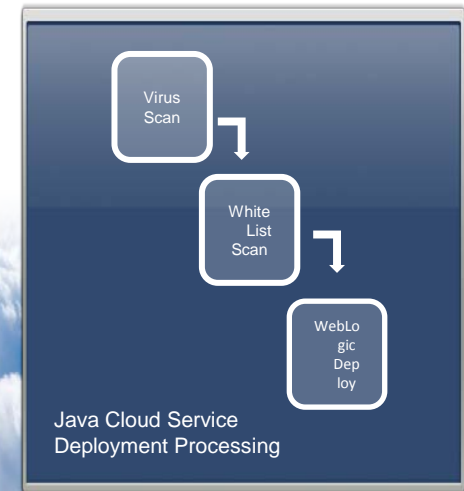


- Virus scanning and white list audit for all services
- Example, for Java Cloud Service:
 - All Java deployment archives run through enterprise class virus scanner
 - Automatically occurs before deployment
 - Detects usage of Java APIs not supported by the Java Cloud Service
 - Automatically occurs before deployment
 - Tightly integrated with Oracle Public Cloud IDEs

Java Cloud Service Console



↓
WAR FILE



* Example using a Java Cloud Service



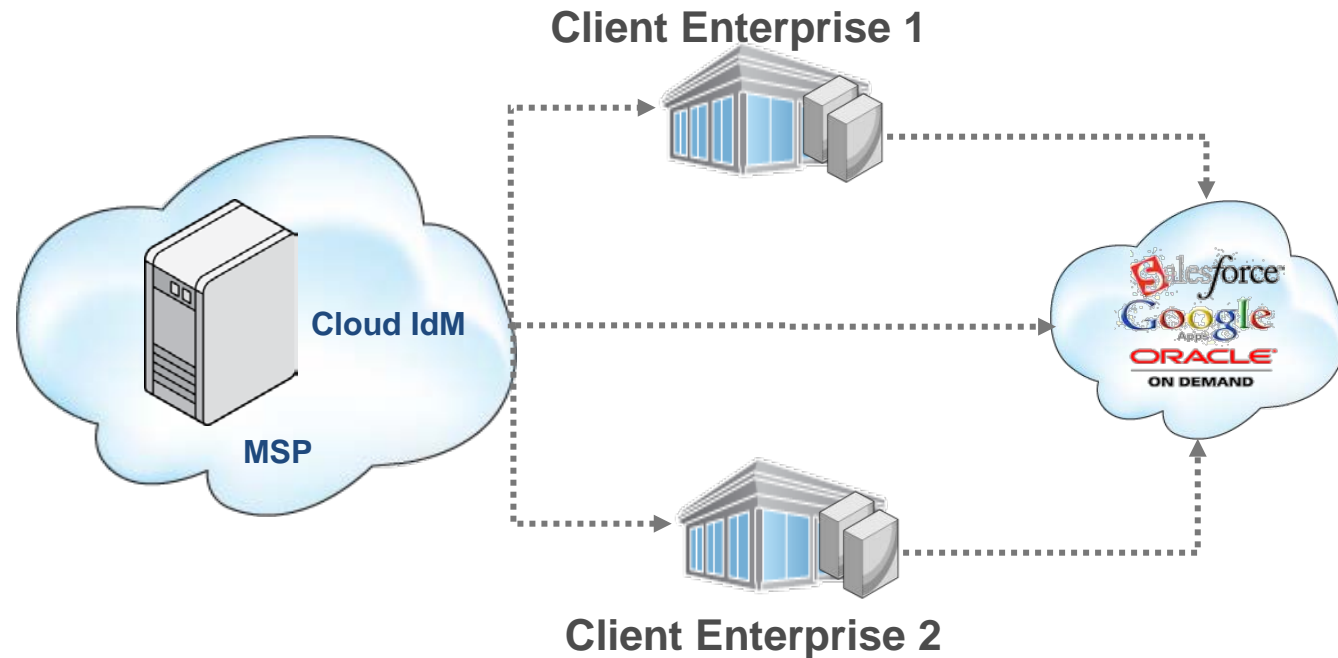
Agenda

- Evolution of IT and IdM Requirements
- Building and Securing Clouds
- Oracle Public Cloud – usage of IdM
- **Identity as a Service – Customer Case**
- Summary





IdM as a Cloud Service



- Customers are looking to outsource IdM
 - Want to augment in-house IdM or replace parts of it
 - IT Staff expertise is a challenge
- MSPs looking to offer IdM as a Service
 - Cost benefits of shared service model over hosted instances
 - Maintenance simplicity
- Requires many technical features: M/T, Federation, Metering/Billing



SaskTel

Background

- Regional Telco owned by the Province of Saskatchewan
- Traditional provider (Wireline, Wireless, Data ...)
- Canadian Telco innovation leader for 100 years +

Revenue: \$1.15B (CAD)

Staff: 4800 Customers: 560,000 +



SaskTel

Vision & Opportunity

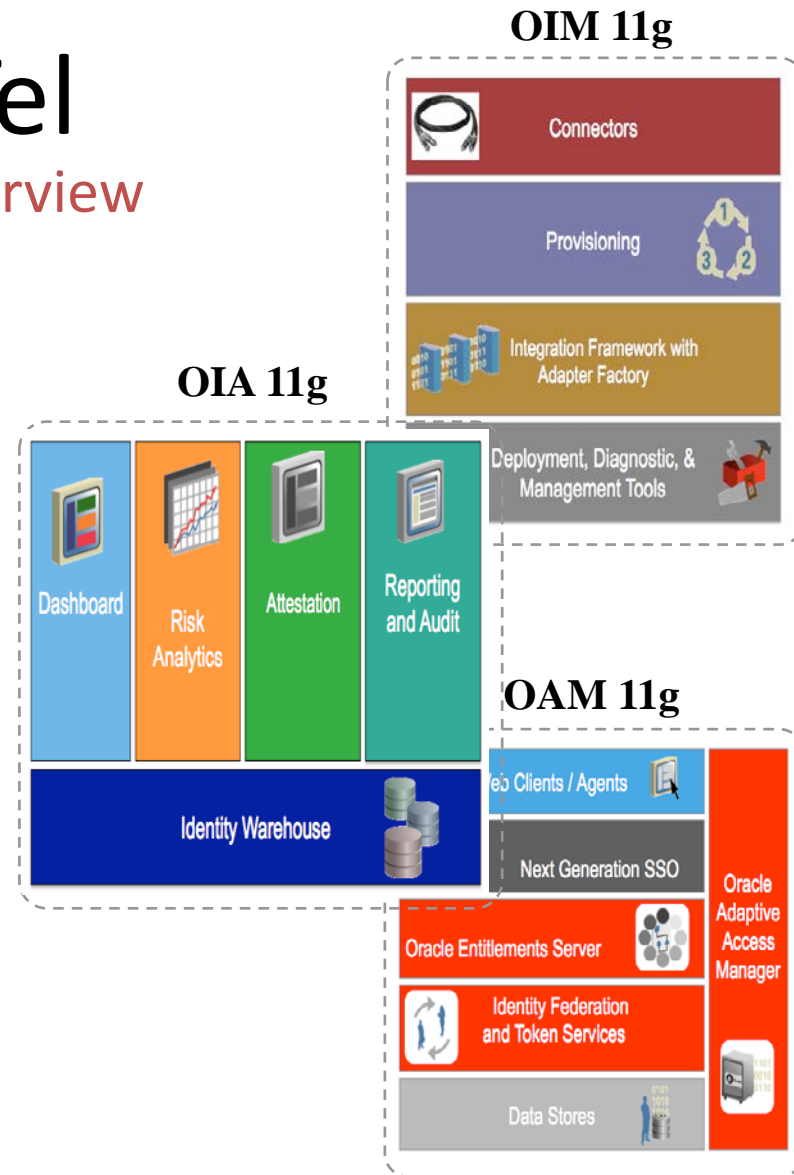
- Provide Midsize organisations with affordable, scalable and sustainable Identity Management solutions based on world leading technology platforms
- Generate net new revenue for SaskTel to offset declining margins in traditional ILEC services
- Continue growing Saskatchewan's strong economy by monetising information technology innovation



SaskTel

Solution Overview

- Red stack (Sparc, Solaris, Fusion)
- Shared or private cloud option
- Per user monthly pricing
- Based on OIM / OAM Suite 11g
- OIA, OAAM, ESSO option
- SaskTel innovation (method / apparatus)





SaskTel

Current Status

- Migrating SaskTel environment to Oracle 11g
 - From CA Siteminder / IDM, Sun IDM, Sun OpenSSO ...
 - Oracle Consulting / Integral providing valued expertise
 - SaskTel Identity Management Centre of Excellence ready for you!
- Active production negotiations with primary sectors
 - Banking, Oil / Gas, Government, Health Care
- Accepting up to 4 Proof of Concept candidates CYQ112



Agenda

- Evolution of IT and IdM Requirements
- Building and Securing Clouds
- Oracle Public Cloud – usage of IdM
- Identity as a Service – Customer Case
- **Summary**





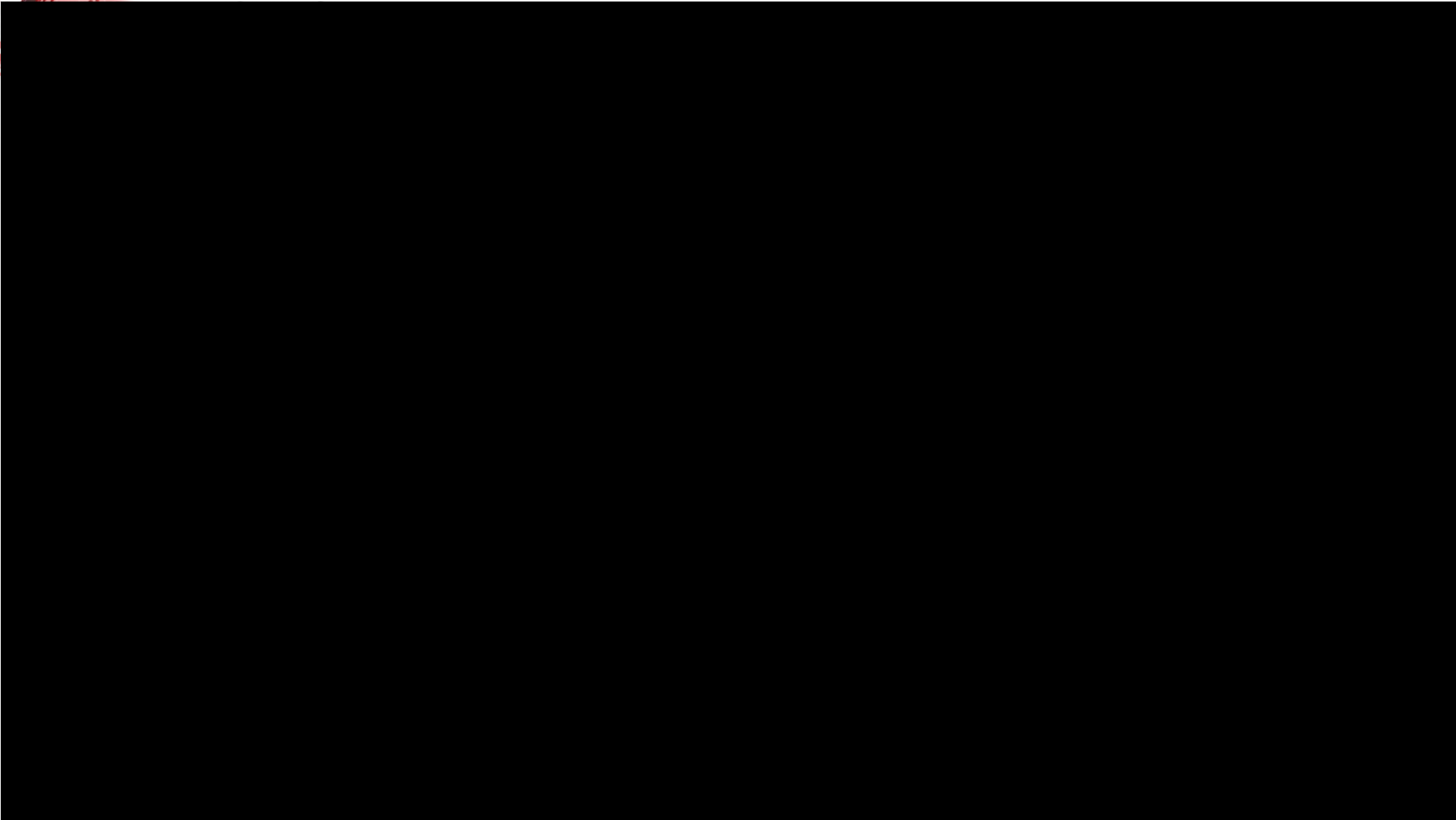
Key Takeaways



- Sketch out all the cloud use cases that apply to you as there is a wide range of possible configurations
- Use standards to provision users into 3rd party clouds (SPML)
- Ensure your access certification processes extend to external cloud services and can meet audit requirements
- Use standards to federate with 3rd part clouds (SAML)
- Use stronger authentication using risk based approach
- Harden the interface between the enterprise and 3rd party clouds, using OEG



deliver the



Q&A

ORACLE®