ORACLE

The Mobile/BYOD flood

Best not to stand on the way of the mobile revolution

James Sadler CISA, CISSP
Security Sales Specialist, Oracle NZ

This document is for informational purposes. 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 in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Additionally to the heretofore mentioned escape clause

Some of the opinions stated in this presentation are entirely mine and not those of my employer.

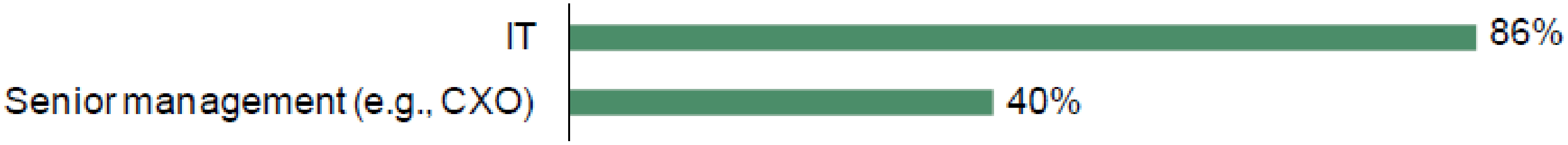
A number of unaccredited images appear in this presentation. That’s my problem as well

Possible Agenda

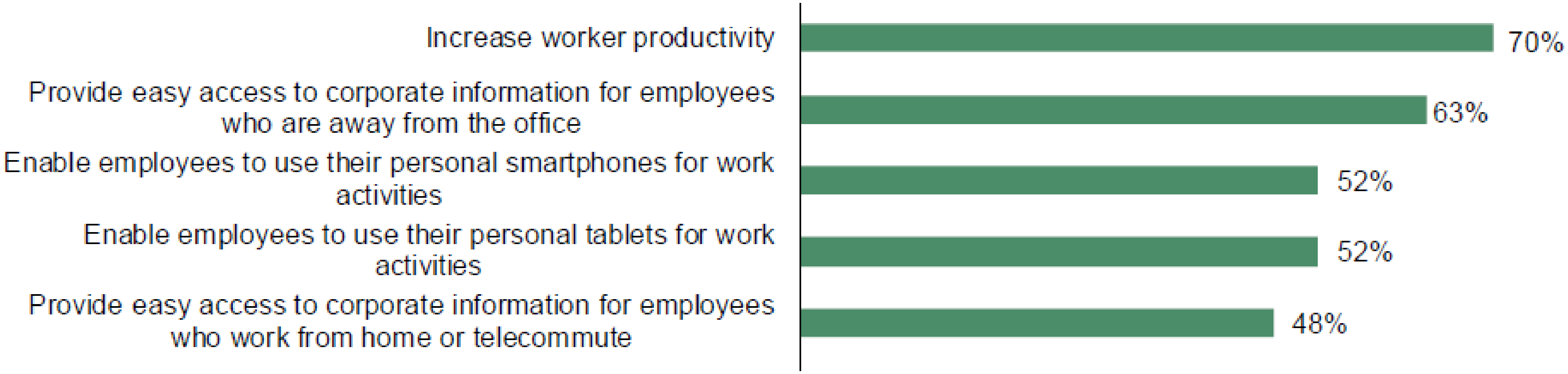
- What it looks like
- It’s not plain sailing
- Technology based controls

The employer view

- Who is developing the BYOD program?

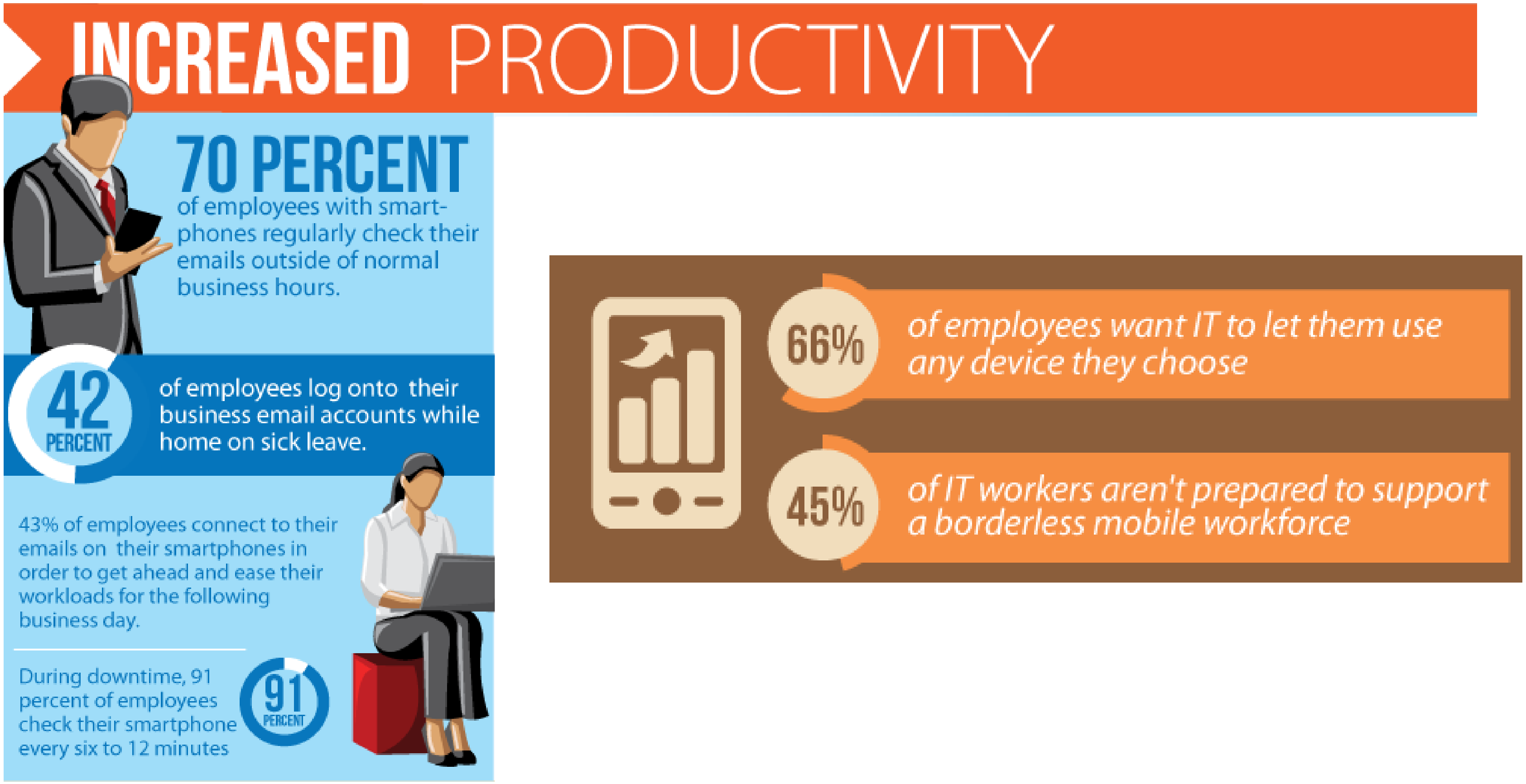


- What are the key factors driving your BYOD program?



Forester Research -Key Strategies to Capture and Measure the Value of Consumerization of IT, July 2012

Mobile Workforce Survey - *Click Software*



INCREASED PRODUCTIVITY

70 PERCENT of employees with smartphones regularly check their emails outside of normal business hours.

42 PERCENT of employees log onto their business email accounts while home on sick leave.

43% of employees connect to their emails on their smartphones in order to get ahead and ease their workloads for the following business day.

During downtime, 91 percent of employees check their smartphone every six to 12 minutes

91 PERCENT

66% *of employees want IT to let them use any device they choose*

45% *of IT workers aren't prepared to support a borderless mobile workforce*

We are conservative in A/NZ

Use their iPad at work

37% vs 60 to 70% in Europe and North America

Professionals view their iPad as a laptop replacement

40% vs 64% worldwide

iPad provided by work

20% of the time vs 40% in Europe an 13% in North America)

IDC Ipad for Business 2012 survey

How to explain a modern mobile device (to a 10yr old)

Ubiquitous

“by 2013, mobile phones will overtake PCs as the most common web access device worldwide.”

Gartner 2010, *www.gartner.com/it/page.jsp?id=1278413*

and

Gartner Oct 2012 http://www.gartner.com/newsroom/id/2209615

The Mobile and Social Access Promise

Anytime Anywhere Access

New

Pers

Mobile, Social and Cloud Access

“Nearly three-quarters of organizations deploying user-focused BYOD report improvements in employee productivity, customer response times and work processes. “

Dell Global BYOD Survey 2013

ging
the landscape

The Mobile and Social Access Problems

Security

Proliferation of Devices

Cannot leverage existing security

Limited device control

A compliance challenge

How to centrally manage the security and be complaint?

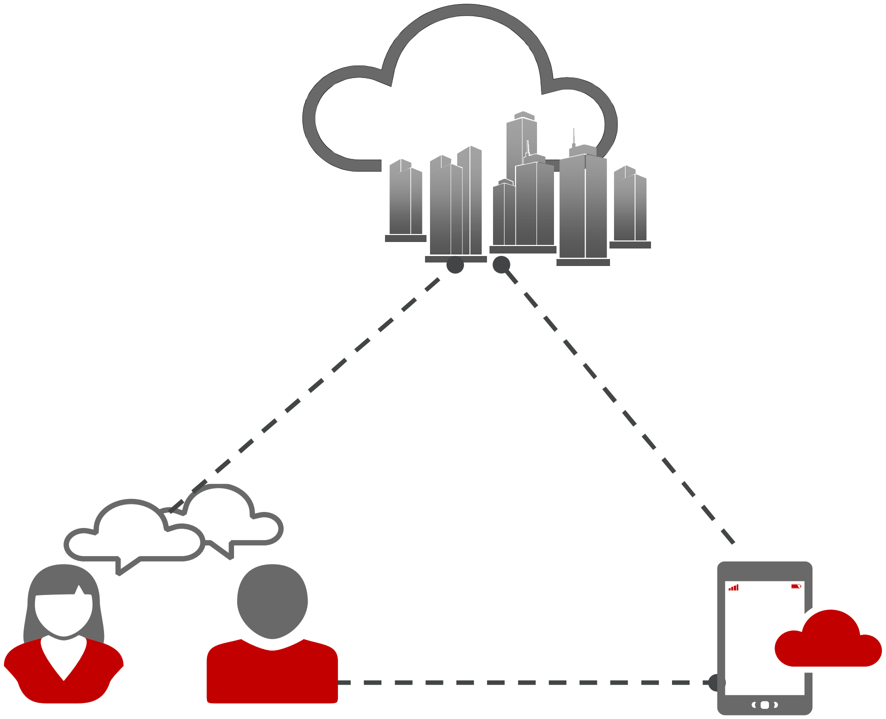
The Mobile and Social Access Problems

Information Access

- Corporate Resources & Information
- Need for Anywhere, Anytime Access
- Often stored in Non-Secure Systems
- Need to Control & Monitor Access

How to make internal information available, quickly & securely

Mobile Security is Beyond Device Management



46% Of organizations that allow BYOD reported experiencing a data or security breach

Source: Trend Micro Survey, Feb 2012

50% Of helpdesks struggle to keep up with mobile apps support

Source: Mobility Revolution Redux, March 2012

58% Building corporate app stores

Source: Partnerpedia Survey, Aug 2011

MOBILE SECURITY STARTS FROM INSIDE

Other problems

It isn’t all plain sailing

- Laptops are well understood in terms of ongoing operational requirements – mobile is new
- Impact of confidentiality and availability due to theft, loss or damage
  - Personal/corporate information used for phishing / identity theft
- Lack of corporate policies on use, acquisition, replacement
  - e.g. can you take the persons personal device if required?
- Data leakage to the device
- Auto connection to any wireless point, network bridging, etc
- Data costs
- Unknown installed applications
- Patching / anti-malware
- Usernames and passwords stored on the devices in cleartext

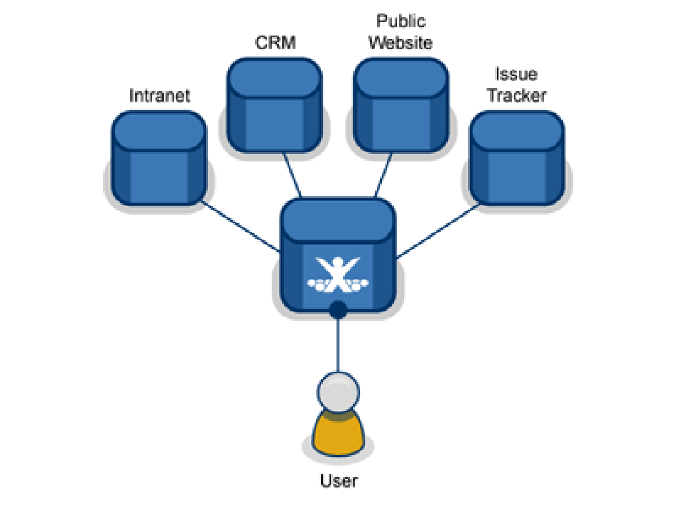
Some steps you can take

- Implement technology safeguards, leveraging known frameworks as guidelines for policy development.
- Classify data, making the most sensitive data (personal, financial, client-sensitive or confidential) unreadable or inaccessible.
- Regularly update the operating systems and software of work devices to ensure security improvements are quickly proliferated throughout the enterprise.
- Design a device management program that includes where the users connect, etc.
- Take into account the applicable legislation and regulations on privacy around the world

The Mobile and Social Access Problems

User Experience

- Native Applications
- No Native Single Sign-on
- Password Help Desk Calls
- Inconsistent Login Experience

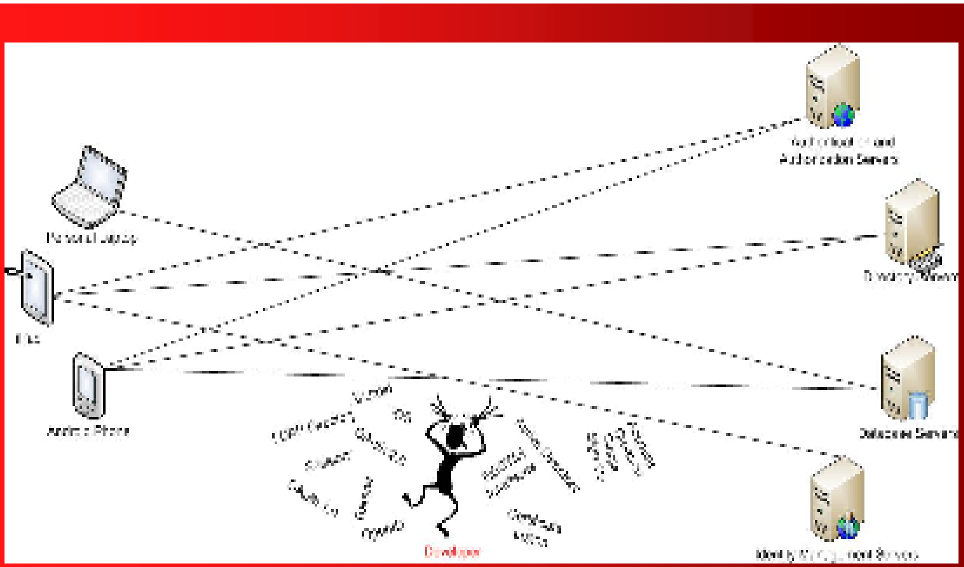


How to improve user experience and productivity?

The Mobile and Social Access Problems

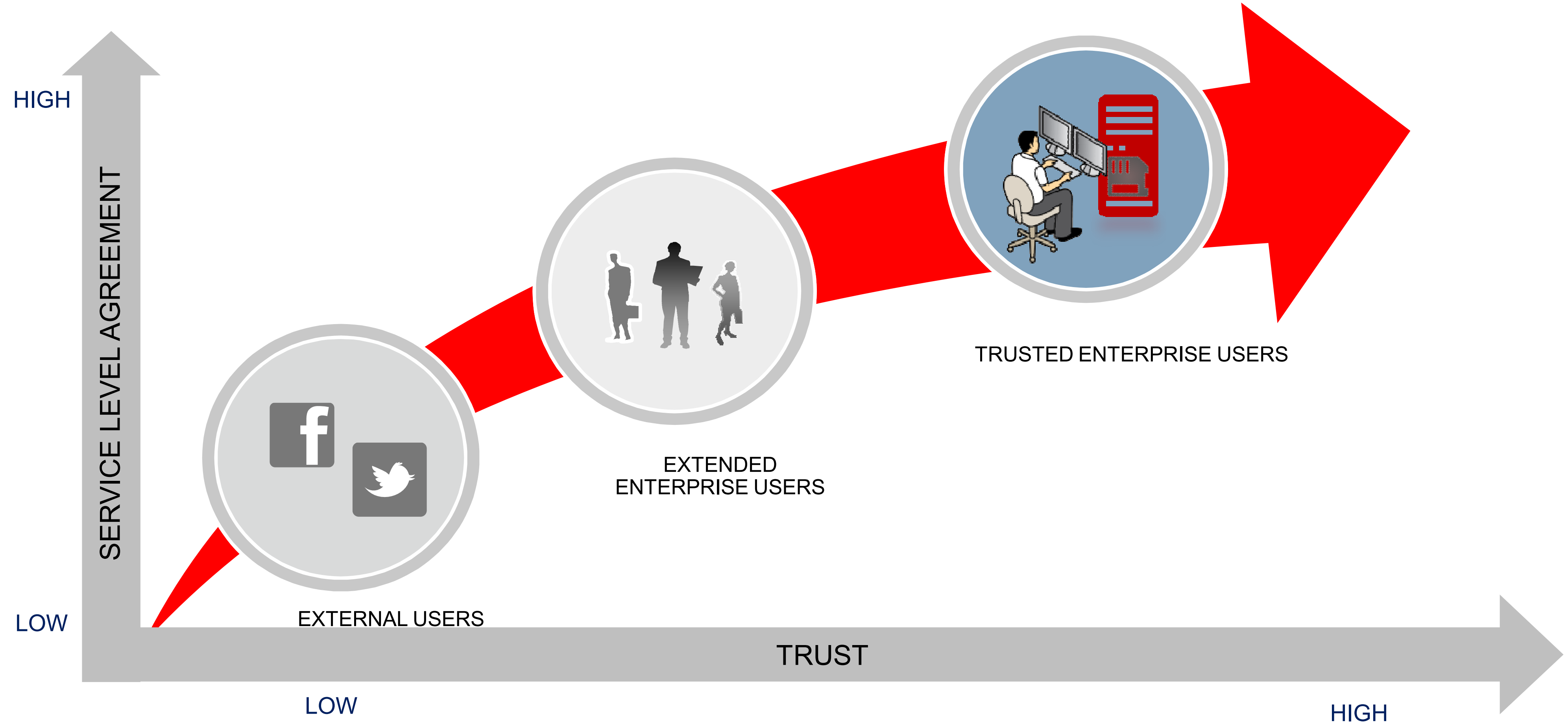
Developer Experience

- Security Coded Into Each Application
- Lack of Security Experience
- Longer Cycle with Weak Security
- Inconsistent Login Experience



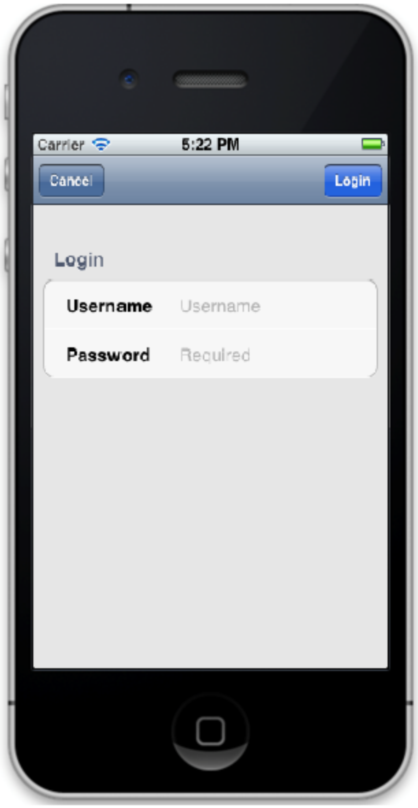
How to simplify app development with strong security?

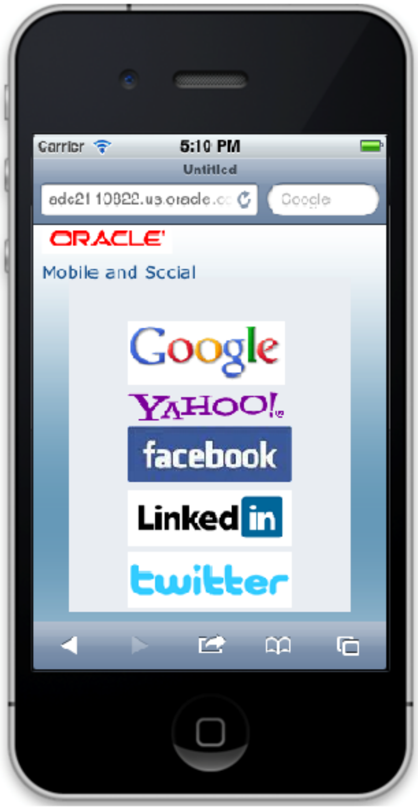
Diverse Users Accessing Corporate Resources

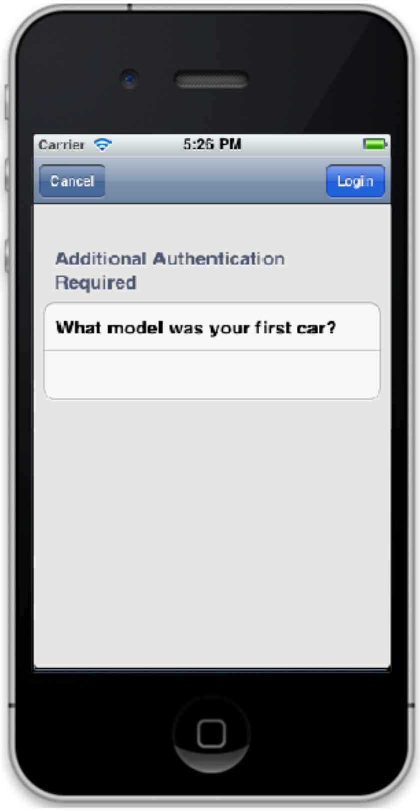


Mobile Authentication

Flexible Options for Devices, Applications and Users

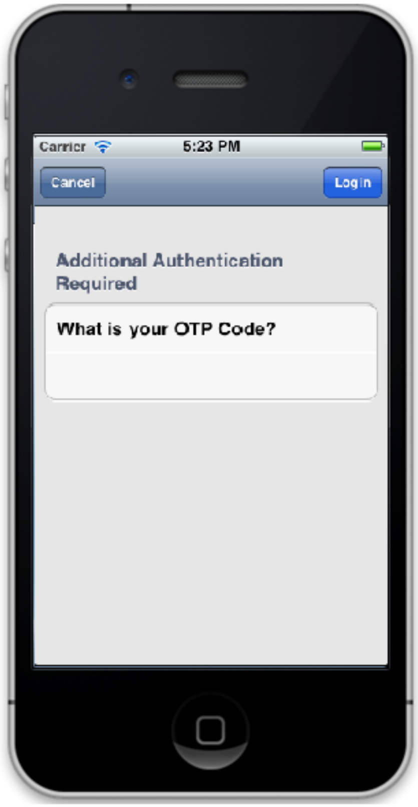






Additional Authentication Required

What model was your first car?



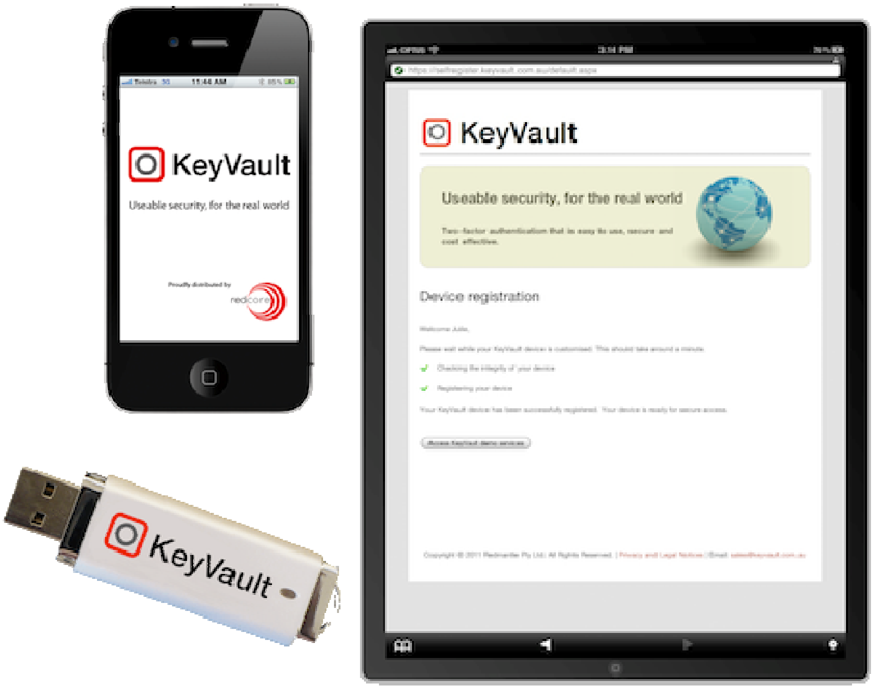
Additional Authentication Required

What is your OTP Code?

KeyVault from Redcore

Two factor authentication for the web

- Safe from Man-in-the-Middle & Man-in-the-Browser threats)
- Cryptographic security
  - Digital keys and certificates
  - Keys are “locked” to the device or token
  - Web transactions can be digitally signed
- Identrust^{TM} certified
- Allows transactions to be “digitally signed”.


KeyVault
Useable security, for the real world
redcore
KeyVault
Useable security, for the real world
Device registration
KeyVault

Device Based Security

Mobile Device Information
(OS, Carrier, Jailbroken, IP/MAC)

Device Registration/ Fingerprint

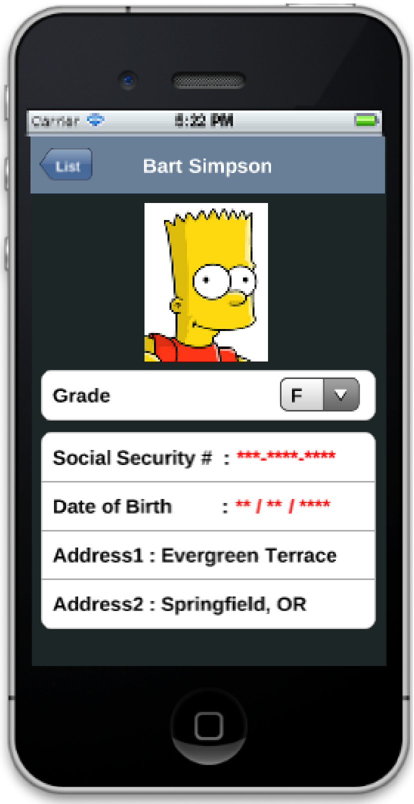
Blacklist/ Whitelist

Stronger Authentication (KBA, OTP, etc)

Device Based Security

Context Aware Authorisation

- *Selective* Data Redaction



Carrier 5:22 PM

Bart Simpson

Grade F

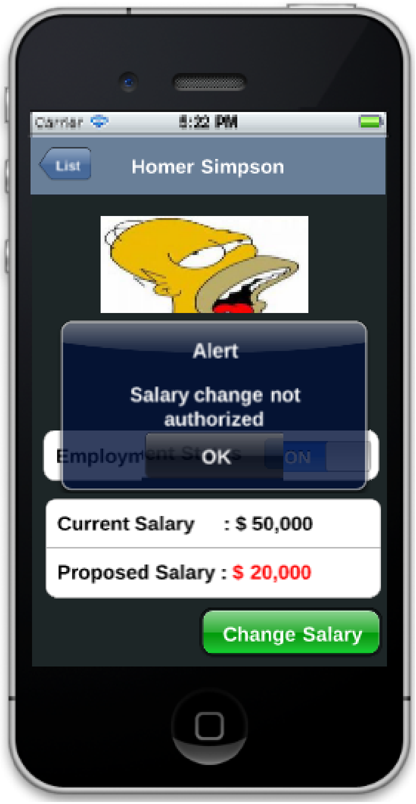
Social Security # : ***-****-****

Date of Birth : ** / ** / ****

Address1 : Evergreen Terrace

Address2 : Springfield, OR

- Business Transactions



Carrier 5:22 PM

Homer Simpson

Alert

Salary change not authorized

Employment Status ON

Current Salary : $ 50,000

Proposed Salary : $ 20,000

- Context Aware
- Standards Based
- Full Audit Trail
- No Code Changes Required

Client SDKs

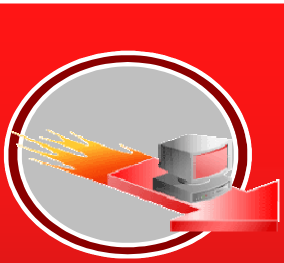
Native Libraries for iOS, Android and JAVA

- Store/Access Keys, Tokens, Handles and other secure data
- Access Mobile Device Information (OS, Carrier, Geolocation, IP/MAC)
- Support KBA, OTP via Email and SMS
- Manage Single Sign-on

Quickly build security into your mobile applications

Secure API's

Enable Mobile Transactions and Access to Corporate Data



Secure
REST API's

API Control &
Governance

Threat
Protection

Client
Throttling

Transformation

API Management
& Monitoring

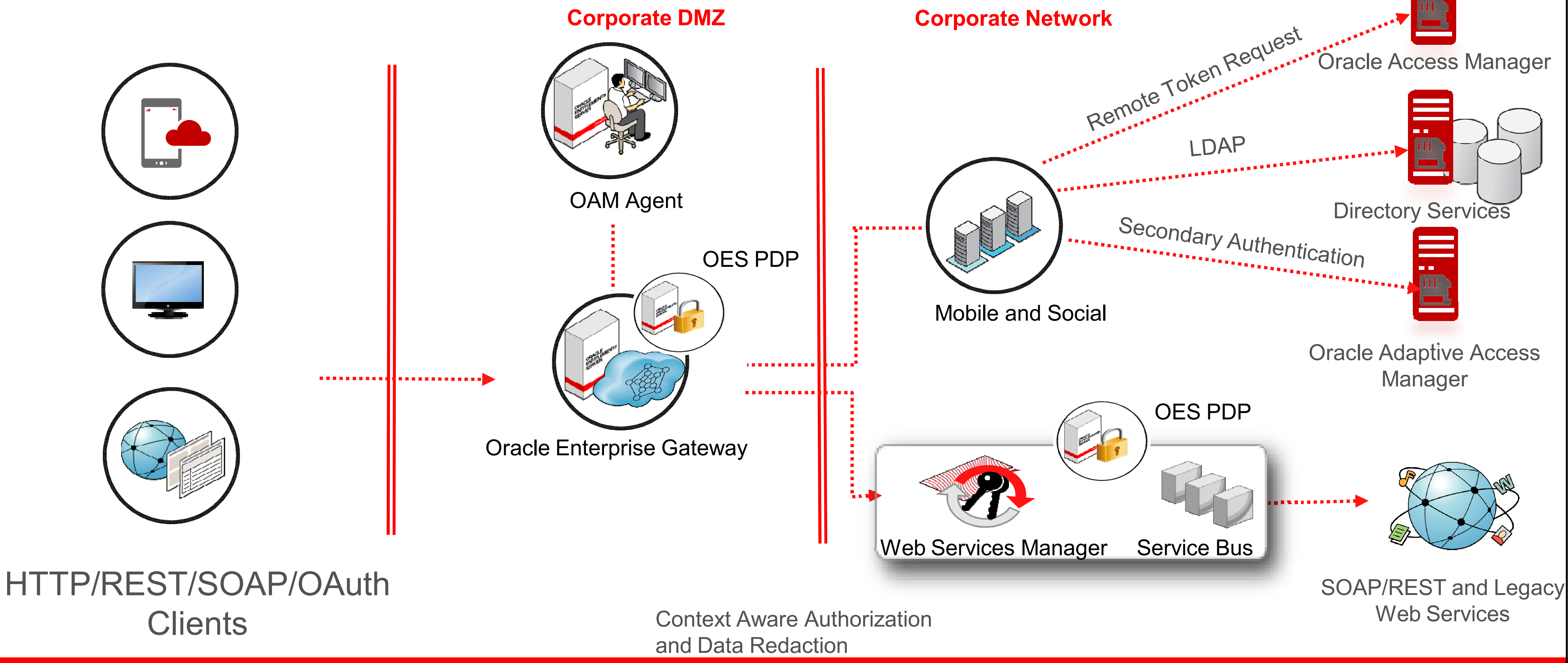
ORACLE Access Management

Extend
Access Management
to REST API's

- Context Aware
- Authentication
- Authorization
- Fraud Detection
- Security Tokens
- Data Redaction
- Audit

Mobile & Social Access Management

Deployment Architecture



Corporate DMZ

Corporate Network

OAM Agent

OES PDP

Oracle Enterprise Gateway

Remote Token Request

LDAP

Secondary Authentication

Oracle Access Manager

Directory Services

Mobile and Social

Oracle Adaptive Access Manager

OES PDP

Web Services Manager

Service Bus

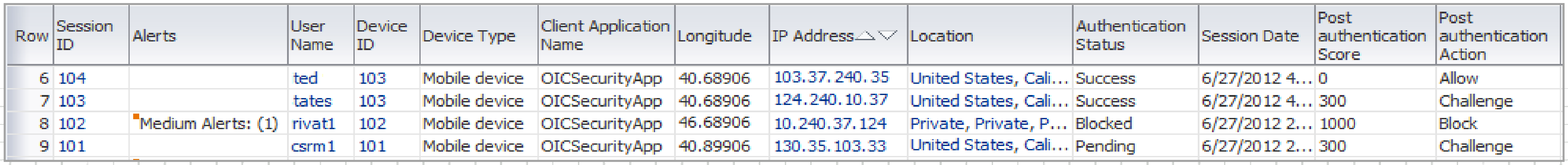
HTTP/REST/SOAP/OAuth Clients

Context Aware Authorization and Data Redaction

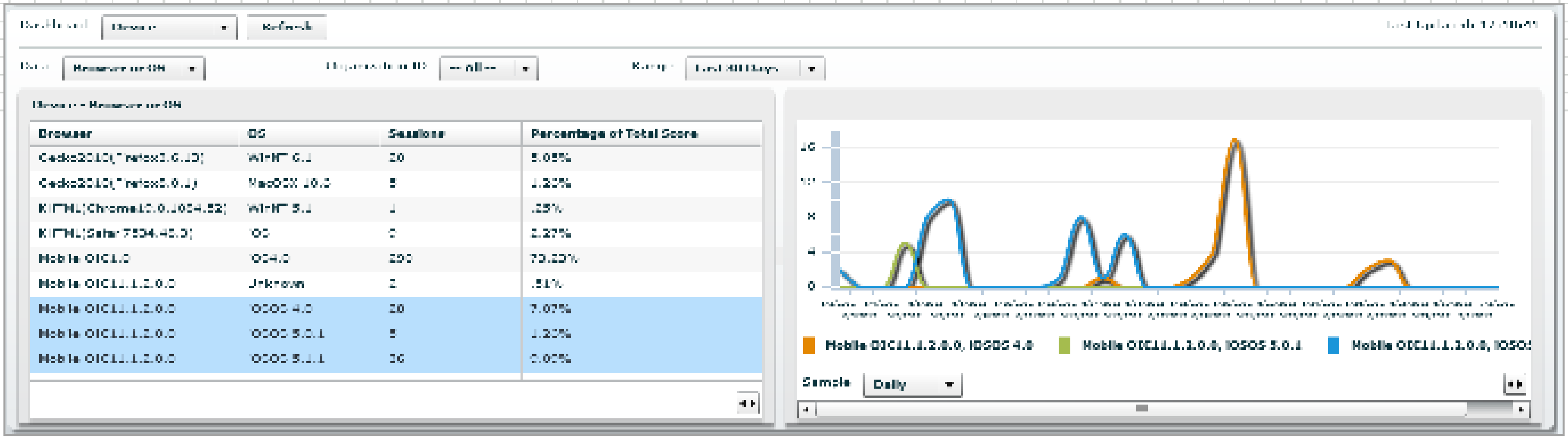
SOAP/REST and Legacy Web Services

Copyright © 2011, Oracle and/or its affiliates. All right

Detailed Mobile Visibility



Row	Session ID	Alerts	User Name	Device ID	Device Type	Client Application Name	Longitude	IP Address	Location	Authentication Status	Session Date	Post authentication Score	Post authentication Action
6	104		ted	103	Mobile device	OICSecurityApp	40.68906	103.37.240.35	United States, Cali...	Success	6/27/2012 4...	0	Allow
7	103		tates	103	Mobile device	OICSecurityApp	40.68906	124.240.10.37	United States, Cali...	Success	6/27/2012 4...	300	Challenge
8	102	Medium Alerts: (1)	rivat1	102	Mobile device	OICSecurityApp	46.68906	10.240.37.124	Private, Private, P...	Blocked	6/27/2012 2...	1000	Block
9	101		csrm1	101	Mobile device	OICSecurityApp	40.89906	130.35.103.33	United States, Cali...	Pending	6/27/2012 2...	300	Challenge



Dashboard: Device Refresh

Data: Browser and OS Organization ID: -- All -- Range: Last 30 Days

Device - Browser and OS

Browser	OS	Sessions	Percentage of Total Score
Gecko2010(Firefox3.6.13)	WinNT 6.1	20	5.05%
Gecko2010(Firefox5.0.1)	MacOSX 10.6	5	1.26%
KHTML(Chrome10.0.1004.52)	WinNT 5.1	1	.25%
KHTML(Safari7534.48.3)	iOS	9	2.27%
Mobile OIC1.0	iOS4.0	290	73.23%
Mobile OIC11.1.2.0.0	Unknown	2	.51%
Mobile OIC11.1.2.0.0	IOSOS 4.0	28	7.07%
Mobile OIC11.1.2.0.0	IOSOS 5.0.1	5	1.26%
Mobile OIC11.1.2.0.0	IOSOS 5.1.1	36	9.09%

16
12
8
4
0
🟧 Mobile OIC11.1.2.0.0, IOSOS 4.0
🟩 Mobile OIC11.1.2.0.0, IOSOS 5.0.1
🟦 Mobile OIC11.1.2.0.0, IOSOS

Sample: Daily

Summary

- Either embrace it, or block it
  - Don’t compromise security
  - Support current service level agreements
- Enterprise access platform extends to mobile
  - Security
  - Enhance user experience
  - Standards
- It’s not all about technology
  - Governance, policies and standards,