



Mobil biztonság az Oracle szemszögéből

Fábián Péter

peter.fabian@oracle.com

Petrohán Zsolt

zsolt.petrohan@oracle.com



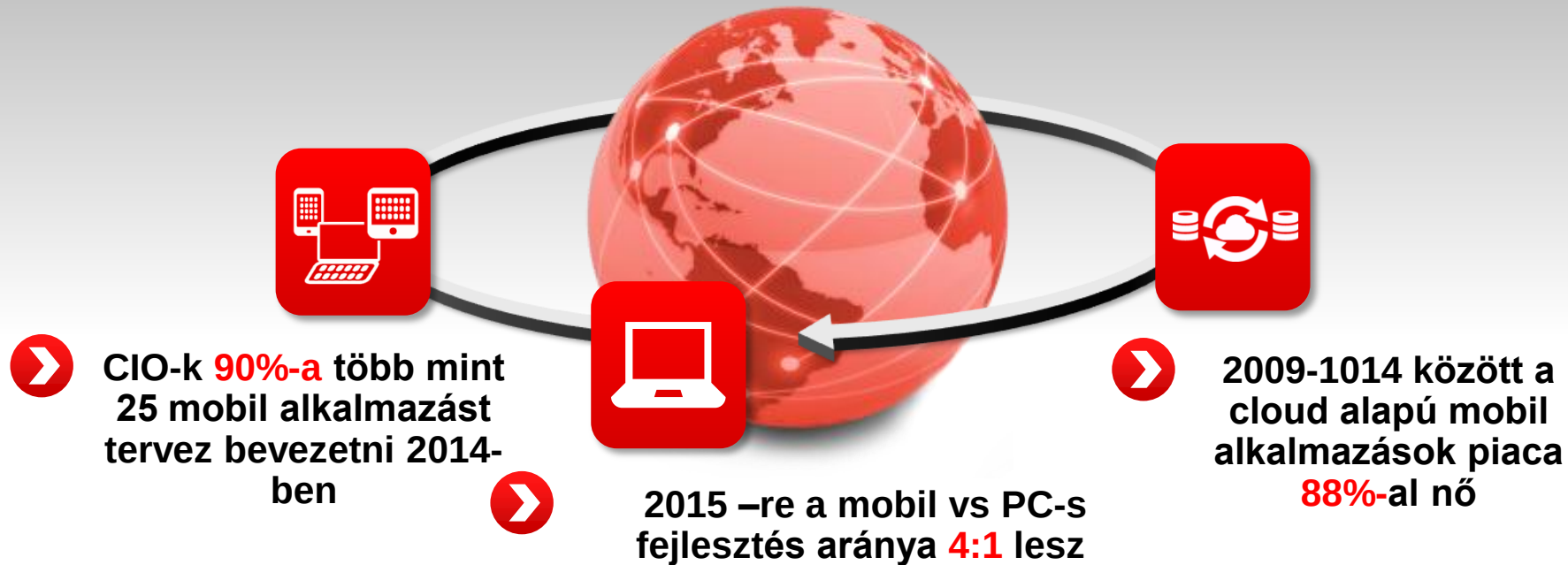
Oracle Security Solutions



Agenda

- Bevezető
- Mobil világ és biztonság fejlesztői szempontból
 - Oracle Mobile Suite áttekintés
 - Mobil biztonság fejlesztési/architektúrális szempontból
- Mobil eszközökön tárol üzleti adatok védelme
Oracle Mobile Security Suite

Mobil & Cloud Computing



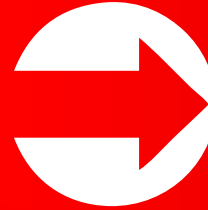
Source: Forbes: Mobile Business Statistics For 2012

Az új világ

Anywhere, Anytime Any Device



Vállalatok 62%-a fog
social login-t használni
ügyfelekkel való
érintkezésben



Vállalatok 90%-a for mobil
alkalmazásokat készíteni
2014-re



Social Login használata

a cégek 62%-a fog social login-t használni

- “three out of every four Internet users leave a website rather than take the trouble to register a new account”
- “Among those who do register, 76 percent say they give false or incomplete information.”
- “research by Forrester, Nielsen and others shows that each customer gained via social login is far more valuable than traditionally-registered users”

<http://blogs.hbr.org/2011/10/social-login-offers-new-roi-fr/>

A Mobil világ komoly kihívás az IT-nek

Bring Your Own Device (BYOD) Gyakorlat 2012-ben



74% engedi a BYOD-t.



Kevesebb mint 10% tudja milyen eszközök érik el a hálózatot

Forbes: Mobile Business Statistics For 2012

Top Mobilítás kihívások

Vállalati információk biztonsága

41%

Integráció más rendszerekkel

31%

Többfajta eszköz támogatása

28%

CIO Insight: Top Challenges of Enterprise Mobility, 2012

Költséges

41%

Szerint a mobil világra való felkészülés drága

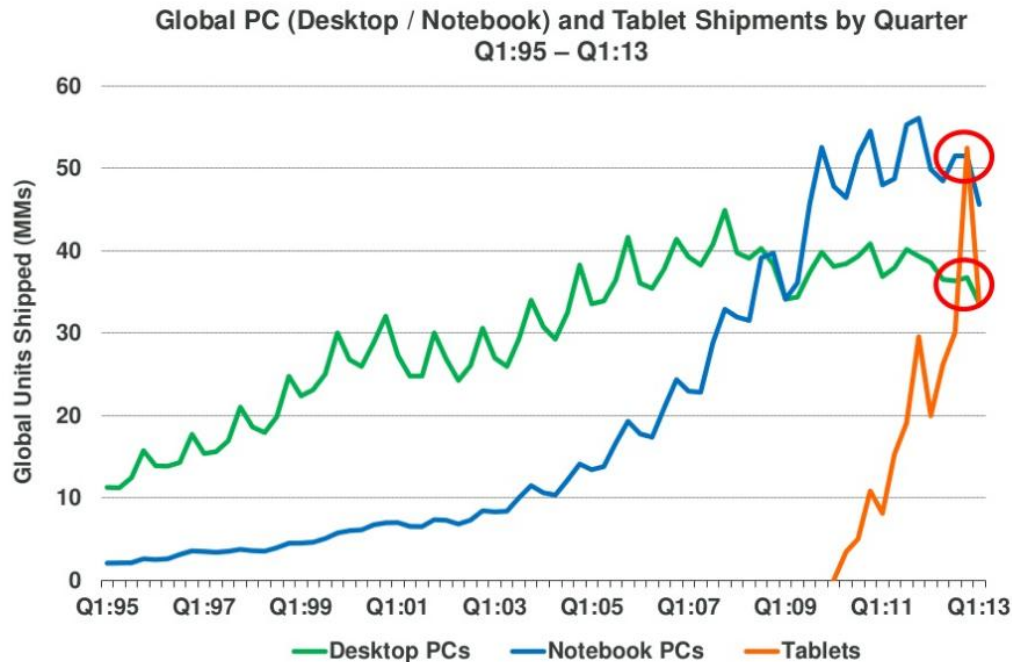
\$250

per eszköz/ évente

Hálózati kapcsolat, infrastruktúra és support

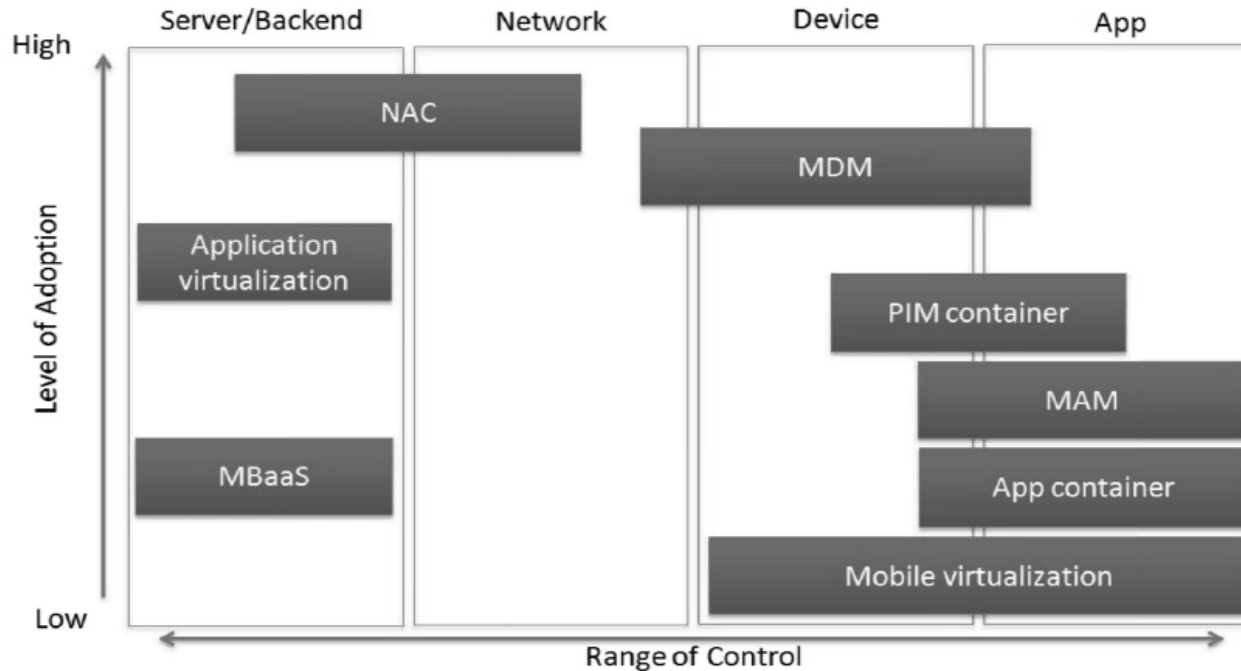
McKinsey, 2012: Mobility Disruption: A CIO Perspective

Okostelefonok + Tabletek—Új végpontok



Source: KPCB

Mobility management



Source: 451 Group

NAC: Network Access Control

MBaaS: Mobile Backend as a Service

MDM: Mobile Device Management

MAM: Mobile App Management

PIM Container: Personal Information Manager (email) Container



Oracle Mobile Suite áttekintés

Petrohán Zsolt

Vezető műszaki tanácsadó



Oracle Mobile Suite

Minden amire szükség van a mobil képes vállalati alkalmazásokhoz



- Application Development Framework Mobile
- Oracle Service Bus
- Technológiai adapterek
- Alkalmazás adapterek
- Dokumentáció és példa kódok

Mik a mobil fejlesztés nehézségei?



- Eltérő eszközökre való alkalmazás fejlesztés
- Mobilra optimalizált & IT adat megfelelés/rendszer hozzáférés
- Egyszerű integráció a vállalati rendszerekkel
- Mobil adat biztonság (a készüléken & útközben)

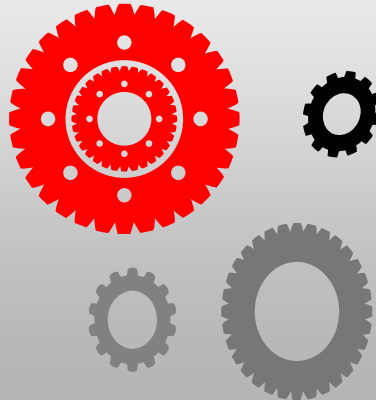
Oracle Mobile Suite



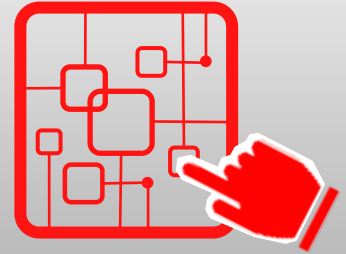
Mobile
Development
Framework



Enterprise
Service Bus

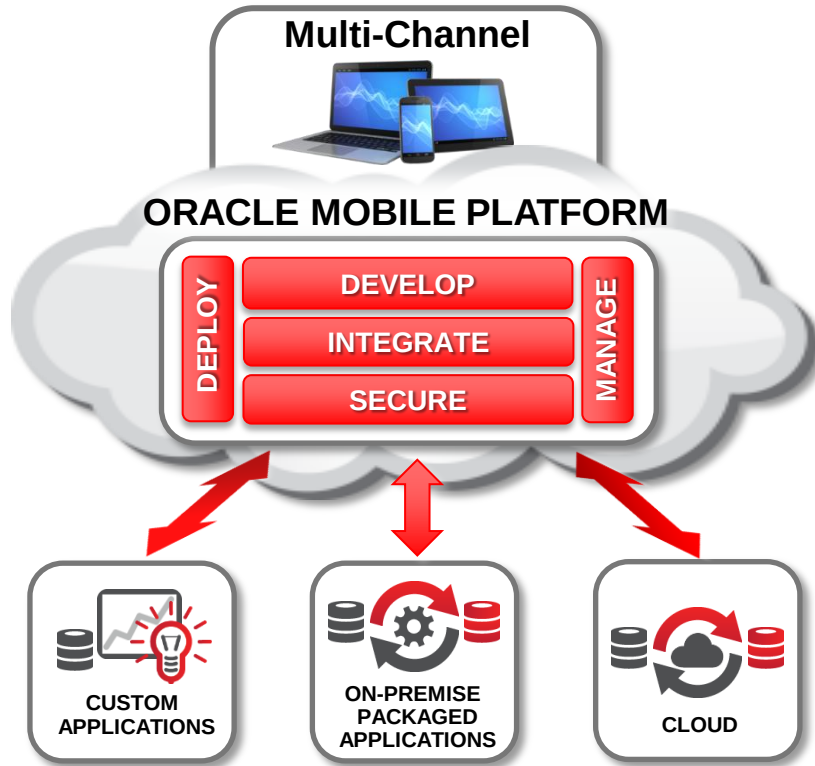


Adapterek



Oracle Mobile Suite

Egy platform bármilyen alkalmazásra/adatra/eszközre - biztonsággal



Meglévő IT befektetés maximalizálása

- **Fejlesztés** eltérő platformra & több csatornás és több eszközös alkalmazásokat
- **Integráció** adatok és szolgáltatások a vállalat és a mobil eszközök között
- **Telepít & Menedzsel** felhő és helyi alkalmazások többcsatornás kézbesítése
- **Biztonság** információ egység a vállalat és a mobil alkalmazás minden szintjén

Fejlesztés: Mobile Application Framework

Termelékeny fejlesztői keretrendszer



- Egyszeres fejlesztés, több platformon futtatás
 - Telefonok, Tabletek, iOS, Android
- Egyszerű UI fejlesztés
 - Komponensek, HTML5/JavaScript
- Üzleti logika Java-ban
- Kapcsolat nélkül: SQLite titkosítással
- Teljes hozzáférés az eszköz natív funkcióihoz
- Moduláris, újrafelhasználható alkalmazás komponensek

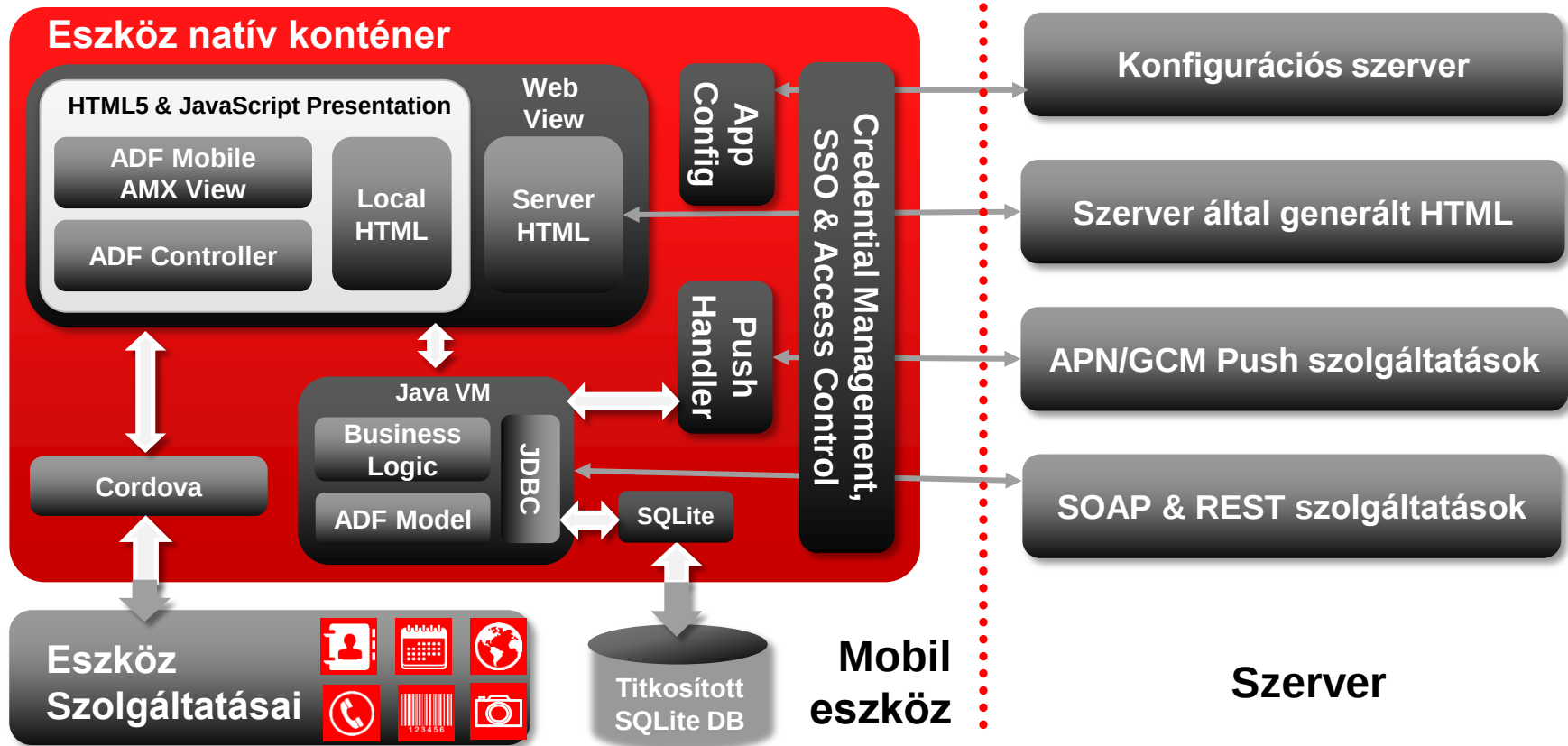
Mobil Web - Oracle ADF Faces használatával

Zökkenőmentes átmenet

- Érintő képernyőre optimalizált
- Grafikai komponensek HTML5 renderelése
- Új mobil/érintés optimalizált komponensek
- Automatikus renderelés beállítás
- Alkalmazkodó elrendezés

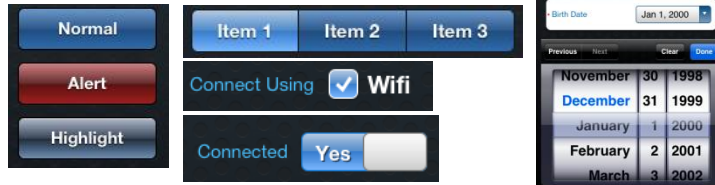


ADF mobil architektúra

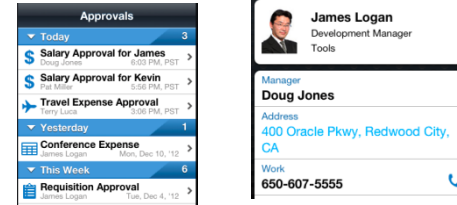


Adatmegjelenítési komponensek

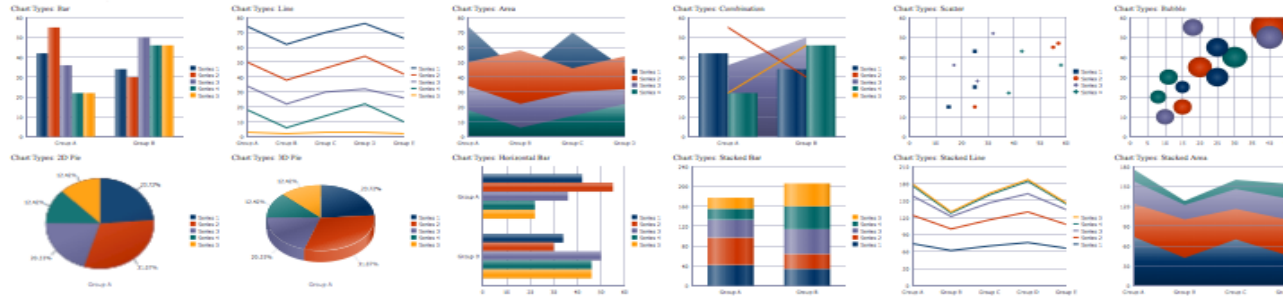
- Alap komponensek



- Lista nézet
- Formok



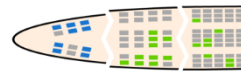
- Táblázatok



- Műszer



- T-Maps



- Karusszel

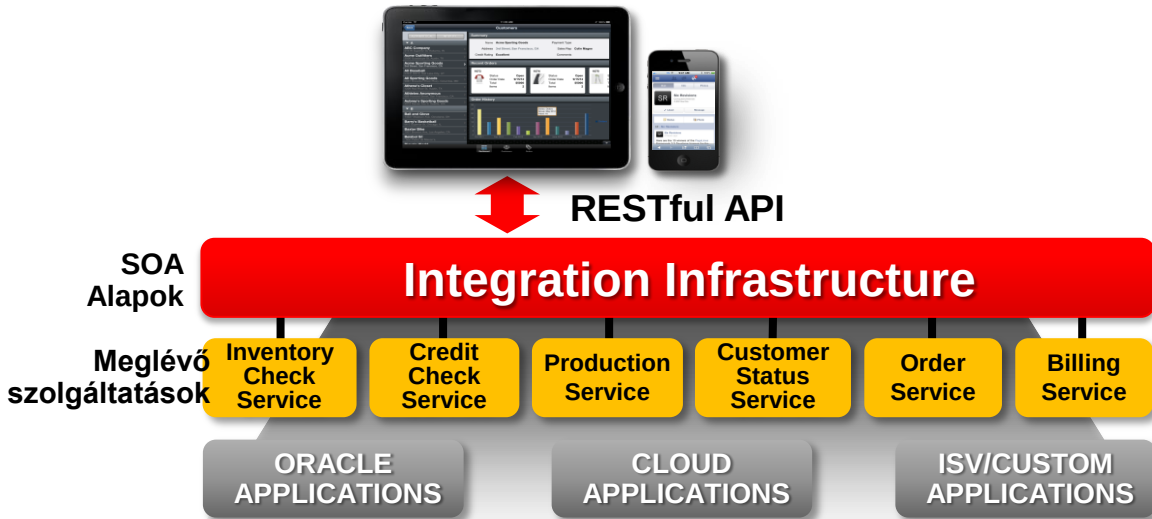


- GeoMap



Integráció: Oracle Service Bus

Szolgáltatás mobil engedélyezése, menedzsment és integráció



- **Újrafelhasznál** meglévő alkalmazások szolgáltatásait
- **Gyors** válasz új üzleti kérésekre
- **Azonnali** hozzáférés az adatokhoz és szolgáltatásokhoz az egész vállalaton belül és külső forrásokból
- **Megbízható** és szilárd integrációs platform

Mobil alkalmazásra optimalizált

Hogyan tud az integrációs réteg segíteni

- Csak a mobil alkalmazásnak szükséges adatot tölti le és minimalizálja az adatforgalmat
- Mobilra optimalizált protokollt használ (REST)
- Csökkenti az adat várakozási időt
- Rugalmas annyira, hogy támogatja a köteget adatszinkronizálást
- Lehetővé teszi, hogy a mobil alkalmazások részt vegyenek hosszú futású „stateful” folyamatokban

Nagy számú mobil felhasználó támogatása

Oracle Service Bus

- Alkalmazás és szolgáltatás virtualizáció
- Non-intrusive
- Nem kell a meglévő rendszeren architektúráján változtatni
- Ellenőrzés és SLA



Szerver oldali gyorsítótár (cache)

Coherence cache engedélyezés jelölőnégyzettel

- Nem kell a kódon változtatni
- A lejárat lehet specifikus vagy változó alapú

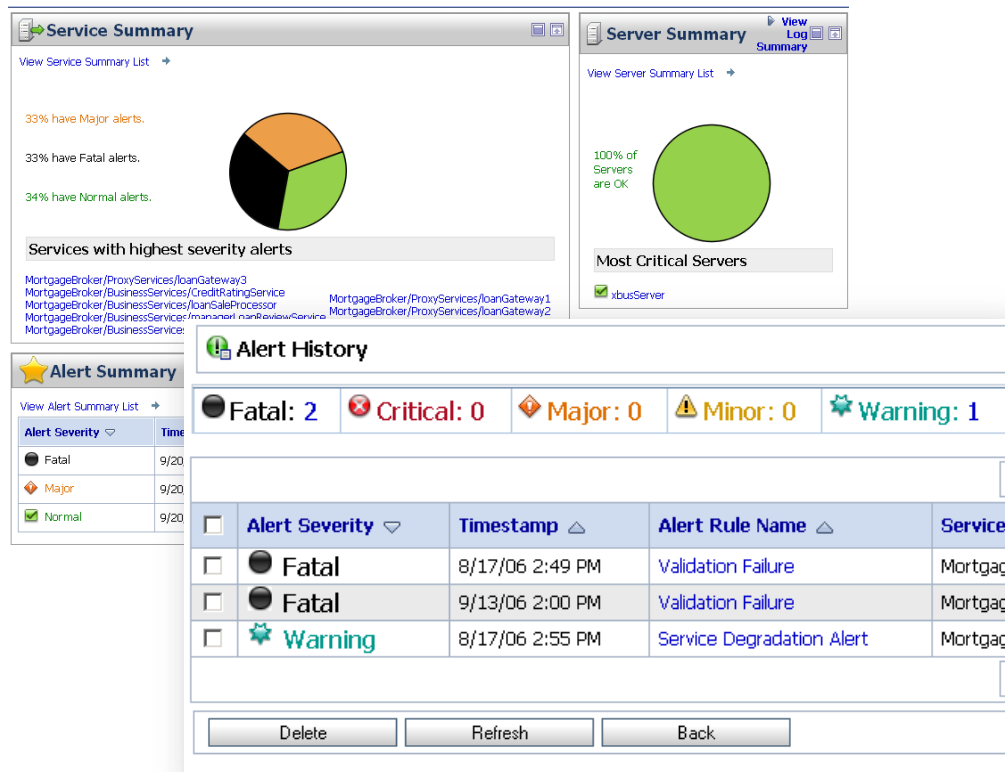
Edit a Business Service (demo/stock/StockQuote)

Advanced Settings

Result Caching	☒ Supported				
Expression Namespaces	<table border="1"><thead><tr><th>Prefix</th><th>Namespace</th></tr></thead><tbody><tr><td>stock</td><td>http://www.example.org/StockQuote/</td></tr></tbody></table>	Prefix	Namespace	stock	http://www.example.org/StockQuote/
Prefix	Namespace				
stock	http://www.example.org/StockQuote/				
Cache Token Expression	<code>\$body/stock:getQuote/ticker/text()</code>				
Expiration Time	☐ Use Default ☒ Duration 0 days 02 hours 00 min				

Ellenőrzés és figyelmeztetés

- Aktuális állapot
- Egyedi lekérdezések
- SLA mérése
- Szabály alapú



Integráció: Hozzáférés vállalati alkalmazásokhoz és adatokhoz

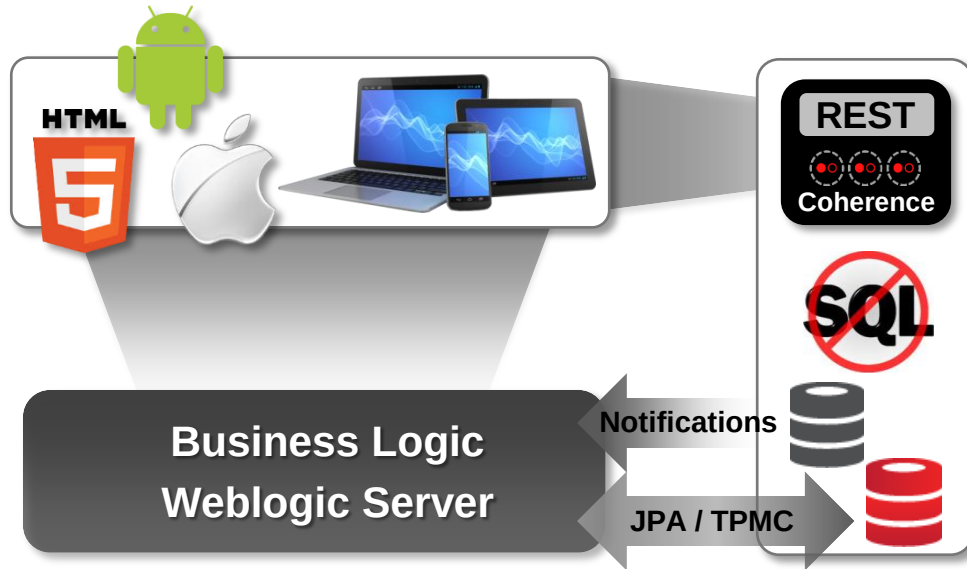
- Technológiai adapterek
 - Egyszerű integráció számos szerver oldali technológiával
- Alkalmazás csomag adapterek
 - Egyszerűsített hozzáférés adatokhoz és szolgáltatásokhoz

Széleskörű csatlakoztathatóság

- Protokollok
 - SOAP over HTTP/JMS
 - HTTP/S
 - JMS
 - RMI/IIOP (EJB)
 - Tuxedo
 - MQSeries
 - Email (SMTP/POP/IMAP)
 - FTP/Secure FTP
 - Custom
 - Oracle Adapters
- Üzenet formátumok
 - XML
 - Text
 - Custom Binary (EDI, etc.)
- Alkalmazás adapterek
 - SAP
 - PeopleSoft
 - Siebel
 - Oracle
 - SWIFT

Telepítés : Oracle WebLogic Server

Telepítés & menedzsment: vállalati skálázhatóság



- **Teljesítmény:** Rendkívül jó válaszidő a gyorsítótár használatával
- **Skálázhatóság:** Több millió konkurens mobil alkalmazást és felhasználó támogatása
- **Elérhetőség:** 24X7



Mobil biztonság fejlesztési/architektúrális szempontból

ORACLE®

Fábián Péter

Security Solution Architect

peter.fabian@oracle.com

Mobil Access

Anytime Anywhere Access

Új eszköz a Business számára

Személyes és üzleti eszközök

Mobile, Social és Cloud Access



Mobile és Social Access megváltoztatja az IT világot

Mobil Problémák

Security

Eszközök burjánzása

Létező biztonsági megoldások nemigen használhatóak

Korlátozott eszközkontroll

Compliance kihívás



Központosított biztonság és compliance??

Mobil Problémák

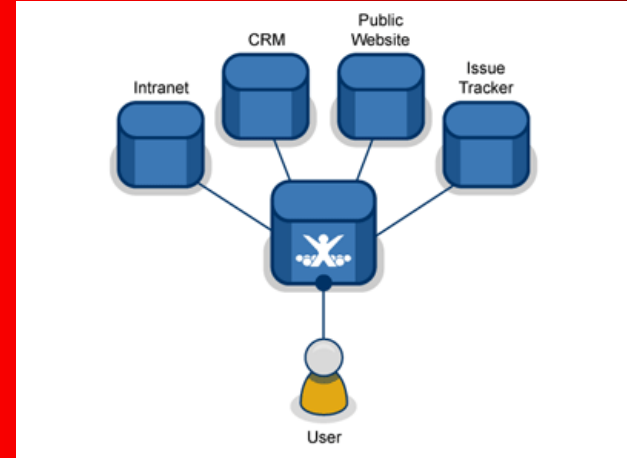
Felhasználói élmény

Native és webes alkalmazások

Nincs Native Single Sign-on

Password Help Desk hívások

Inkonzisztens Bejelentkezés



Felhasználói élmény és produktivitás növelése?

Mobil Problémák

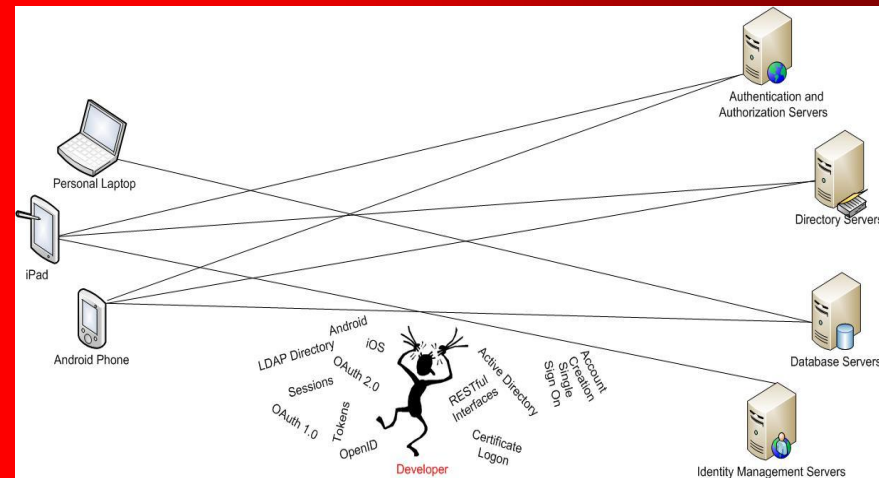
Fejlesztési szempontból

Alkalmazásokba kódolt security

Nincs security tapasztalat

Hosszabb fejlesztési ciklus, gyengébb biz

Inkonzisztens Bejelentkezés



Egyszerűbb fejlesztés és mégis nagyobb biztonság?

Mobilitás kihívásai

Új mobilalkalmazások autentikációja és autorizációja

- Hagyományos megközelítések:
 - Hack-eljünk azonosítást és autorizációt az alkalmazásba → autentikációs szigetrendszerek
- Oracle megközelítés
 - *Terjesszük ki* a webes autentikációs rendszert mobilalkalmazásokra
 - Kockázati tényezőket figyelembe vevő hozzáférés menedzsment
 - Csomagolt security: iOS és Android SDK access menedzsmentre

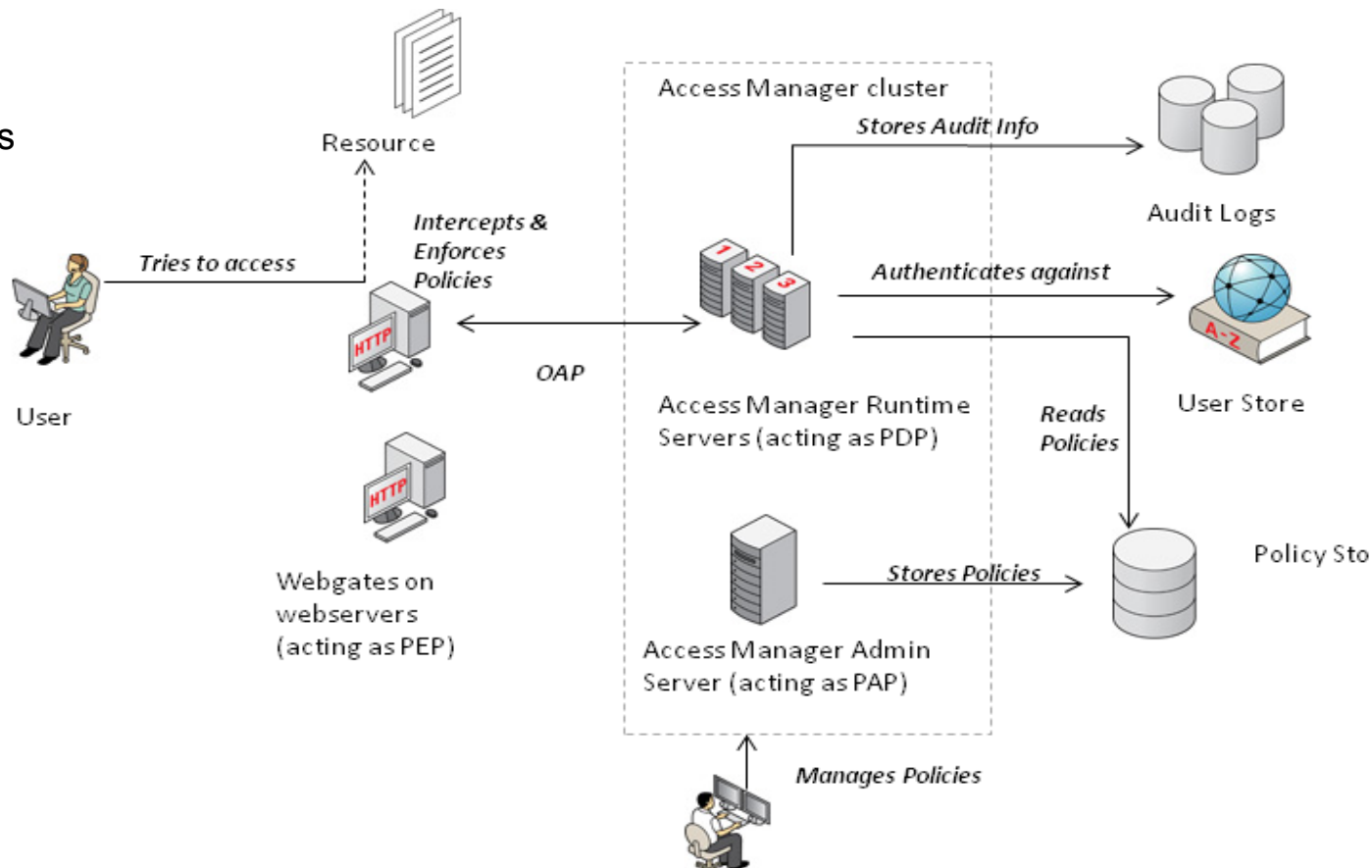
Oracle Access Manager

autentikáció-authorizáció web-es rendszerekhez

Központosított autentikáció és
authorizáció

Webes single signon

Munkamenet kezelés



L. törvény releváns pontjai

4,5 szinten

3.3.5.5.2. **Jelszó** (tudás) alapú hitelesítés

3.3.5.5.2.1. Az érintett szervezet:

a jelszóra a következő elvárásokat érvényesíti: kis- és nagybetűk megkülönböztetése;
a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek,
és minimális jelszóhosszúság; meghatározott szám karakterváltozást kényszerít ki új jelszó létrehozásakor;

3.3.5.5.2.1.3. a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel
a jelszóból képzett hasító érték tárolást) és nem továbbítja;

3.3.5.5.2.1.4. a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy,
hogy meghatározott számú új jelszói megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első
lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.

3.3.5.5.3. **Birtoklás** alapú hitelesítés

5. szinten

3.3.6.9. **Egyidejű munkaszakasz kezelés**

Az érintett szervezet az elektronikus információs rendszerben meghatározott számra korlátozza az egyidejű
munkaszakaszok számát, a meghatározott fiókok vagy fiók típusok számára külön-külön.

Adaptív Access Manager

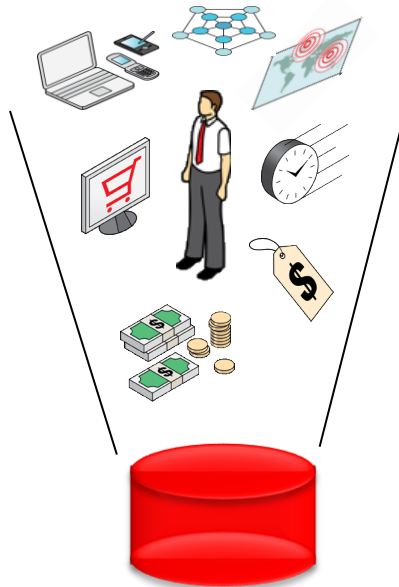
Szokások és környezet figyelembevétele

Eddig csak munkaidőben lépett be, Most pedig éjjel. Használjunk erősebb autentikációt, pl knowledge based, one time password

Kivülről is bejelentkezett, de már van egy aktiv bejelentkezés a belső hálózaton

Melyik az igazi session?

Környezet vizsgálata,
Viselkedésminták

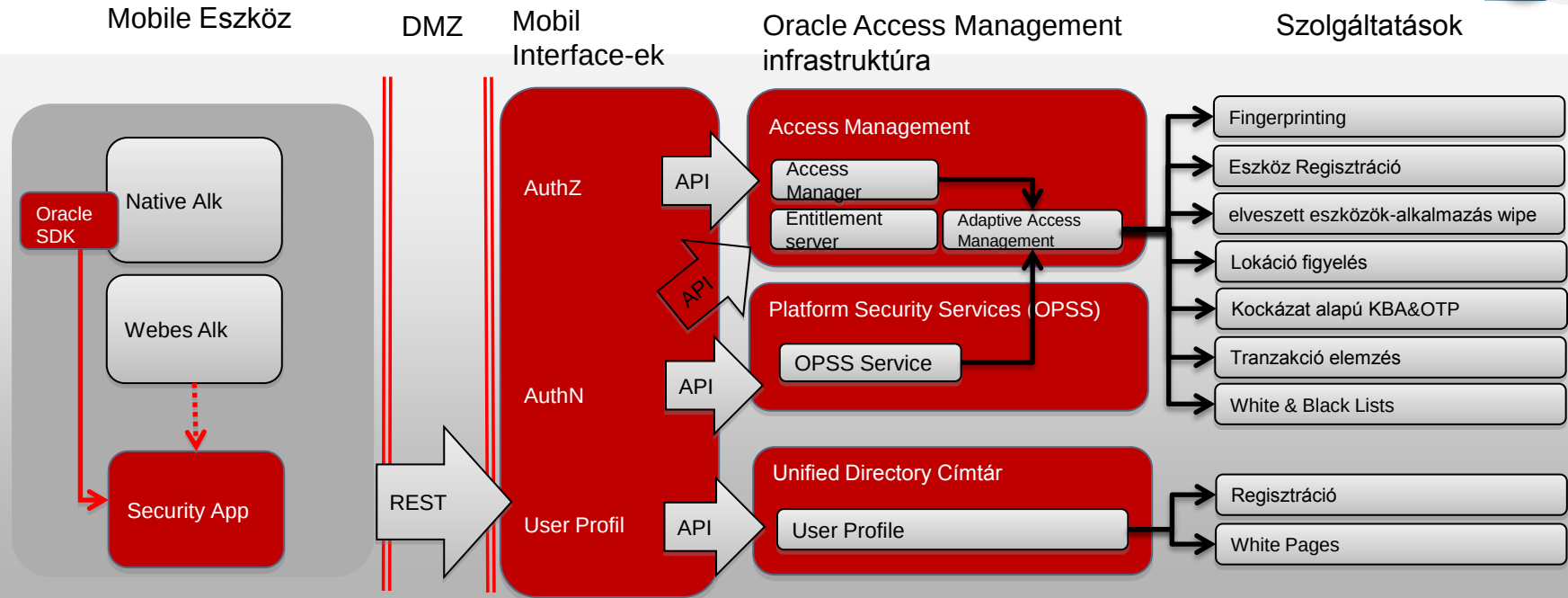


Használta ezt a mobil eszközt 20%-nál többször az elmúlt 3 hónapban?
eszköz ujjenyomatvétel

Megszokott-e hogy nagy összegeket utal?
Viselkedés figyelése

Fél órája Budapestről lépett be, most pedig Kínából??
Geolokáció!

Mobil Access Management



Mobile SDK

Natív SDK iOS &Android-ra

Kulcsok-tokenek biztonságos tárolása, használata

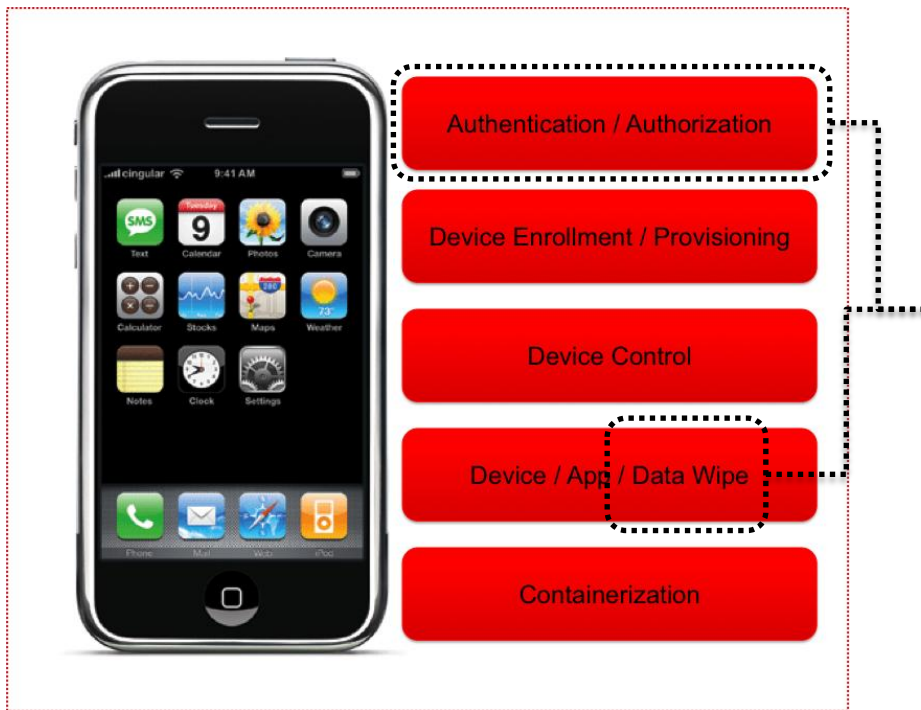
Eszköz információk elérése és továbbítása
(OS, Lokáció, IP/MAC, fingerprint)

Backend szolgáltatások egyszerű igénybevétele

Single Sign-on

„Csomagolt” security az alkalmazáshoz

Oracle Mobile & Social



Oracle Access Management – Mobile & Social

- IAM infrastruktúra kiterjesztése a mobil alkalmazásokra:
webes és mobil csatornák egységes access managementje
- Authentikáció, single sign-on
kockázat alapú autentikáció, audit
- Csomagolt biztonság:
iOS és Android) SDK a fejlesztés megkönnyítésére
- Web, Hybrid és Natív alkalmazások támogatottak

API biztonság

Általános problémák

- Hogyan nyissuk meg webszolgáltatásainkat/API-jainkat az Interneten?
- Hogyan szűrjük, hitelesítsük a bejövő (és kimenő) xml-json állományokat?

Mobil alkalmazások megjelenése

API security, transzformációk szükségessége

SOAP

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap12:Envelope xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
<soap12:Body>
<tns:GetQuote xmlns:tns="http://www.webserviceX.NET/">
<tns:symbol>ORCL</tns:symbol>
</tns:GetQuote>
</soap12:Body>
</soap12:Envelope>
```

Vagy REST

<http://server:8081/getprice?symbol=ORCL&output=json>

Mobil alkalmazások megjelenése

XML

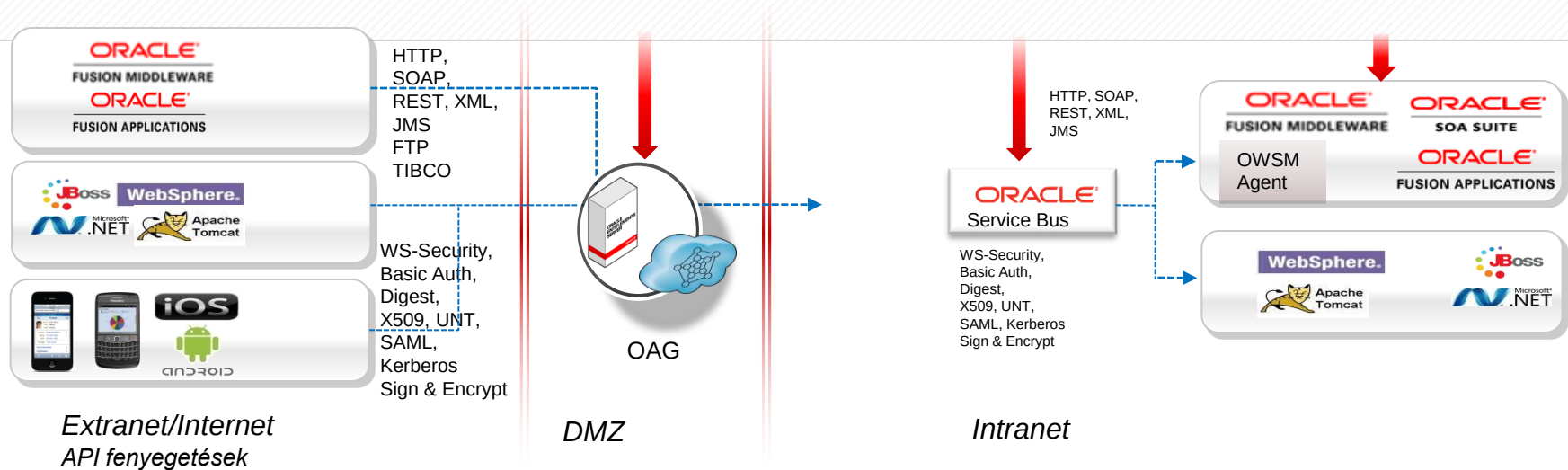
```
<widget>
<debug>on</debug>
<window title="Sample Konfabulator Widget">
<name>main_window</name>
<width>500</width>
<height>500</height>
</window>
<image
<hOffset>250</hOffset>
<vOffset>250</vOffset>
<alignment>center</alignment>
</image>
<text data="Click Here" size="36" style="bold">
<name>text1</name>
<hOffset>250</hOffset>
<vOffset>100</vOffset>
<alignment>center</alignment>
<onMouseUp>
sun1.opacity = (sun1.opacity / 100) * 90;
</onMouseUp>
</text>
</widget>
```

Or JSON

```
{"widget": { "debug": "on", "window": { "title": "Sample
Konfabulator Widget",
"name": "main_window",
"width": 500,
"height": 500 },
"image": { "src": "Images/Sun.png" "name": "sun1",
"alignment": "center" },
"text": { "data": "Click Here", "size": 36, "style": "bold",
"name": "text1",
"hOffset": 250,
"vOffset": 100,
"alignment": "center", "onMouseUp": "sun1.opacity =
(sun1.opacity / 100) * 90;" } }}
```

SOAP2REST és XML2JSON konverziók!

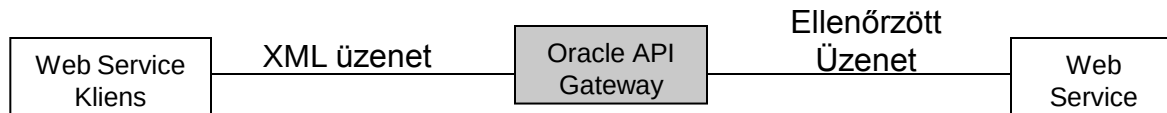
Megoldás: Oracle API Gateway



Integráció

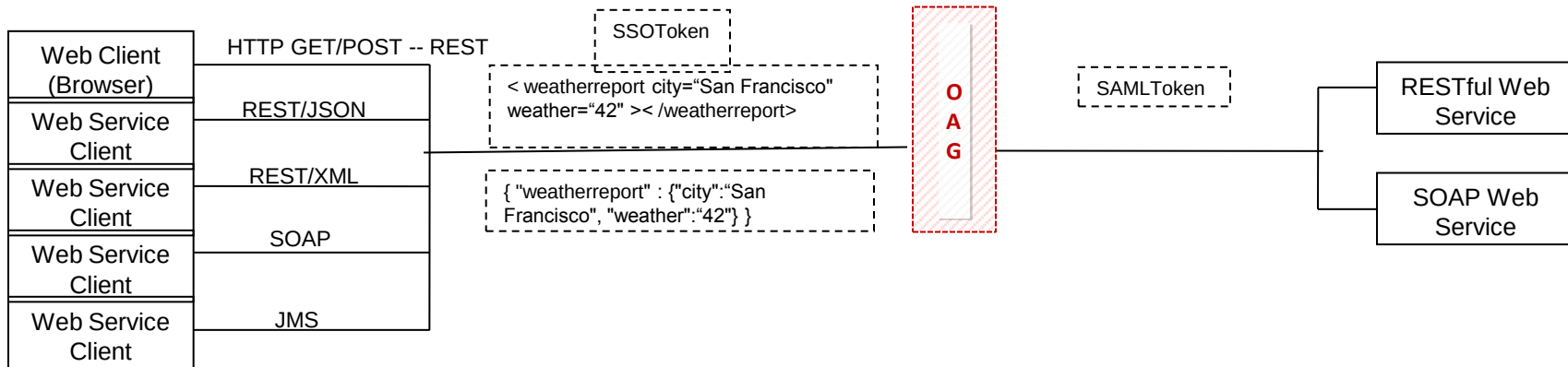


XML Firewall funkcionalitás



- Web service üzenet tartalmazhat ártalmas dolgokat
- OAG XML tűzfal!!
 - *XML tartalom*: XML well-formedness; XML méret; XPath és XQuery injection; SQL injection; XML encapsulation; XML vírusok; érzékeny kimenő adatok detektálása és szűrése, XML bombák; WSDL megfelelés.
 - *XML séma és Document Type Definition (DTD) támadások*: sema megfelelés ellenőrzése; XML entity expansion and recursion; schema poisoning; rekurzív elemek, jumbo tag-names; malicious includes (also called XML external entity (XXE) attacks)
 - *Kriptográfiai támadások*: Public Key denial of service; replay attacks
 - *SOAP támadások*: SOAP szűrés, SOAP attachment ellenőrzés (viruses and other)
 - *Kommunikációs támadások*: HTTP header és query string szűrése; IP address szűrés; traffic throttling

Virtualizáció, adat-protokoll konverzió



- Egy endpoint különböző protokolloknak
- Adatformátum transzformációk
 - XML to JSON és vissza
- Protocol bridging
 - REST to SOAP és vissza

üzenetek tartalmi szűrése



Help desk

Válasz

- Név és kontakt
- Maszkolt TAJ
- Orvos info
- Biztosítás

Válasz

- Név és kontakt
- Maszkolt TAJ
- Orvos info
- Biztosítás
- Fizetési történet

Válasz

- Név és kontakt
- Orvos info
- Egészségügyi adatok



Orvos

Visszadja

Név és kontakt

TAJ

Orvos Info

Receptek

Egészségügyi adatok

Biztosítás

Fizetési történet

Legacy
rendszer



PEP
PDP

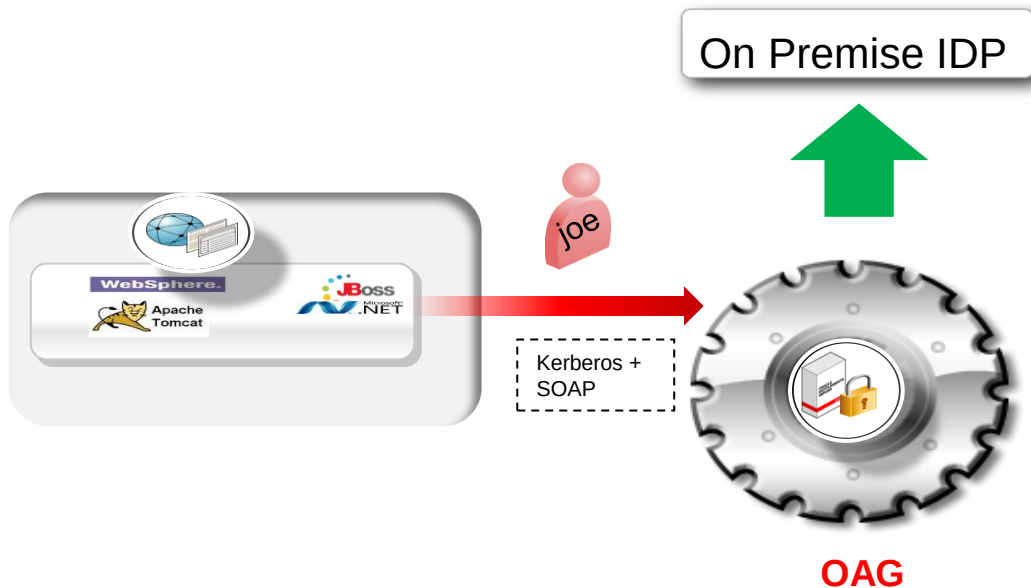
Oracle API
Gateway

Irányítás, szabályozás

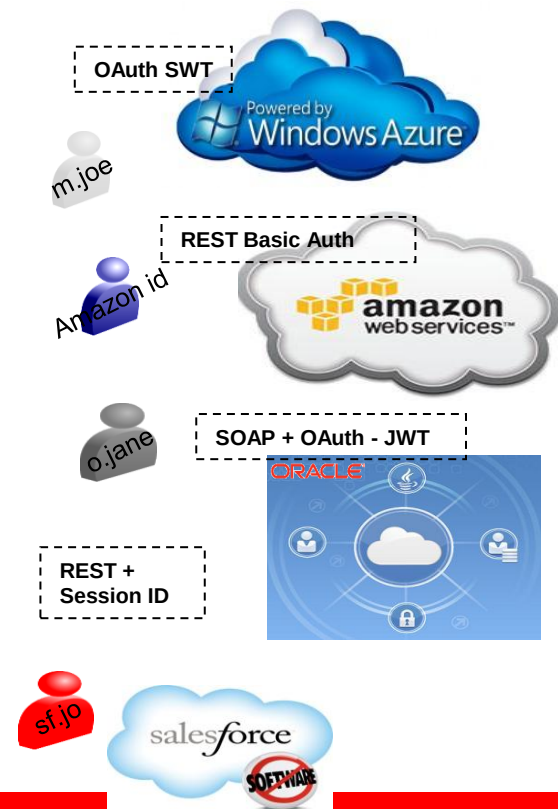
- Üzenetek kliensfüggő feldolgozása
- Intelligens routing
- 100 tranzakció per second (TPS) Kliens1-nek, 250 TPS Kliens2-nek
- SLA riasztások
- Teljeskörű monitoring

Cloud szolgáltatások elérése

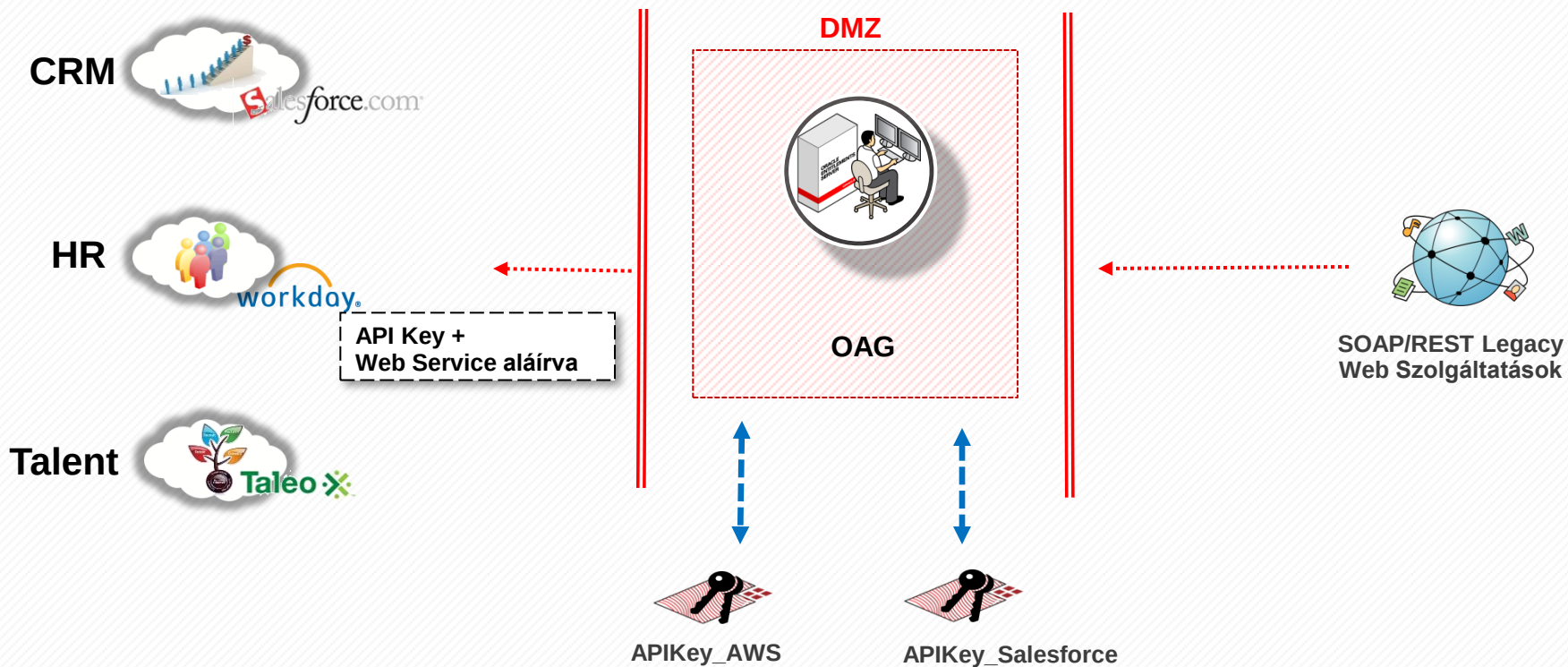
- Cloud elérés API Gatewayen át
- Auditált
- Esetleges aláírási művelet ellenőrizhető



Vállalati hálózat



API Kulcs menedzsment



Social Login



Jó lenne

- Social Login integráció kódolás helyett adminisztrátori klikkelés lenne
- Dobozos támogatás a vezető szolgáltatókhoz (Facebook, LinkedIn, Twitter...)

Social Sign-on

Select



Login



Authorize



Sign in With Local Account

User Name

Password

Login

Sign in With Other Account





SIGN UP

Sign in

Email

Password

Sign in ☐ Stay signed in

Google Accounts

dkillmer@gmail.com
[Sign in as a different user](#)

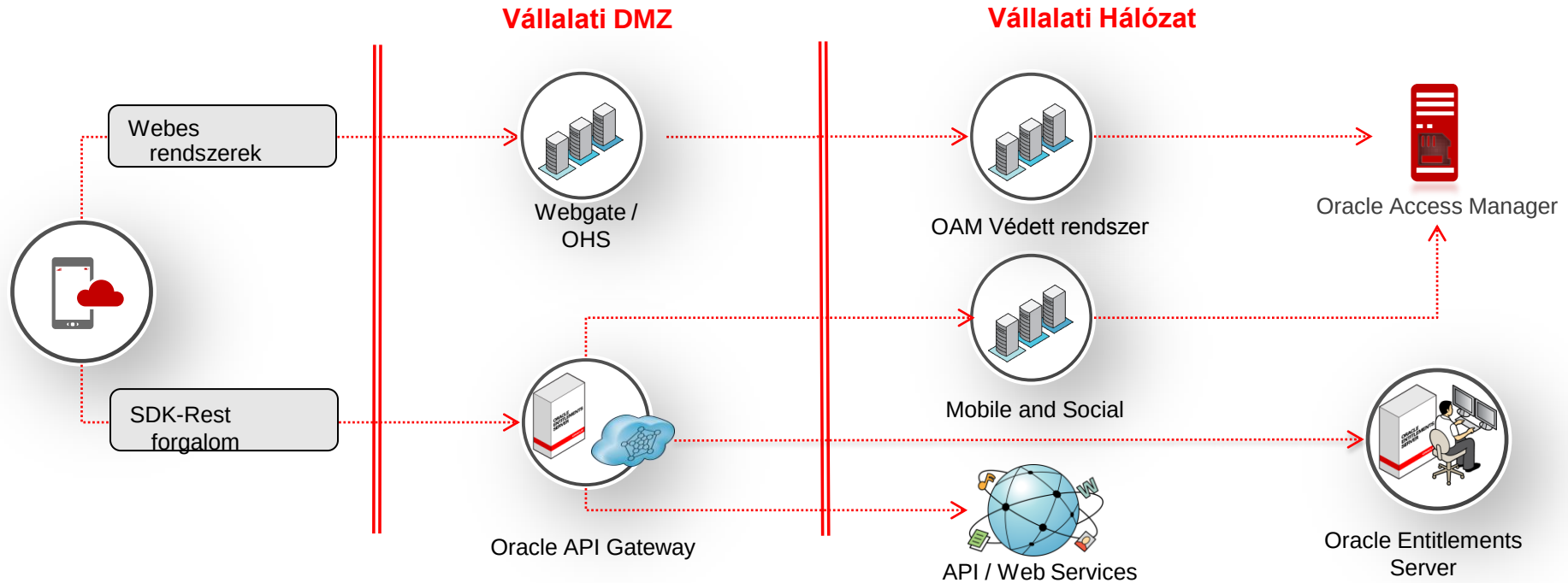
Slc01lwm.us.oracle.com is asking for some information from your Google Account
dkillmer@gmail.com

- Email address: Daniel Killmer (dkillmer@gmail.com)
- Language: English

Allow No thanks

☒ Remember this approval

Teljeskörű Mobil alkalmazás biztonság





Mobil eszközökön tárolt üzleti adatok védelme

Oracle Mobile Security Suite

Fábián Péter

peter.fabian@oracle.com



Oracle Security Solutions



L törvény mobil biztonsági vonatkozásai

3,4,5 szinten

3.3.6.15. Mobil eszközök hozzáférés ellenőrzése

3.3.6.15.1. Az érintett szervezet:

3.3.6.15.1.1. belső szabályozásában felhasználási korlátozásokat, Konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;

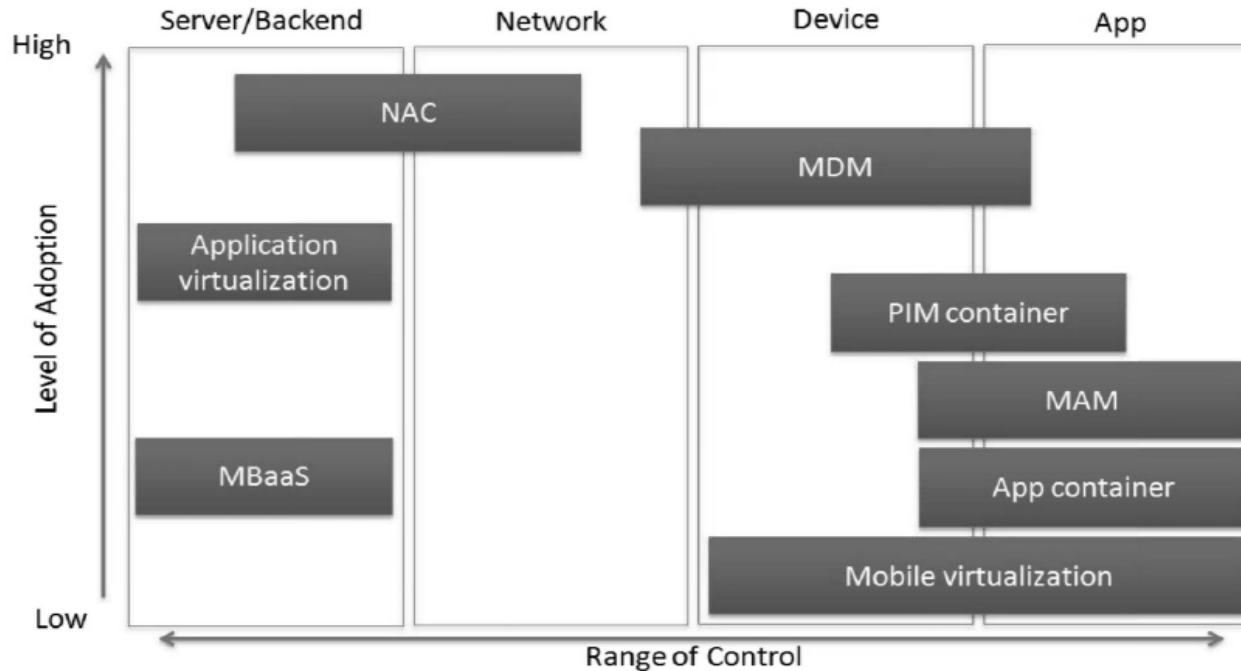
3.3.6.15.1.2. engedélyhez köti az elektronikus információs rendszereihez mobile eszközökkel megvalósított kapcsolódást.

4,5 szinten

3.3.6.15.2. Titkosítás

Az érintett szervezet teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

Mobility management



Source: 451 Group

NAC: Network Access Control
MBaaS: Mobile Backend as a Service
MDM: Mobile Device Management
MAM: Mobile App Management
PIM Container: Personal Information Manager (email) Container

Mobile Device Management

- Telepítsünk agentet
- A teljes eszköz ellenőrzés alá kerül
- Mi történik eszköz törlésekor?

Mobil biztonság??



Mobile **Device**
Management:
Vegyük át az
ellenőrzést a
készülék felett
Nincs személyes
tér

Mobil eszközbiztonság??



Mobile **Application** Management:
elválasztjuk a vállalati és magán adatokat,
alkalmazásokat:
Biztonságos konténer
BYOD kezelhető

Oracle Mobil Security Stratégia

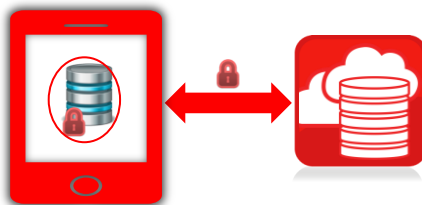
Vállalati adatok és alkalmazások biztonságos elkülönítése és menedzsmentje

Biztonságos konténer alkalmazások elkülönítésére



- Házirend felhasználók korlátozására a konténeren belül illetve a konténerből/be történő adatmozgatásra
- Egységes megközelítés minden mobil platformon

Biztonsági kontrollok és központosított alkalmazásmenedzsment



- VPN infrastruktúra nélküli biztonságos kommunikáció a vállalati rendszerekkel
- Vállalati app store

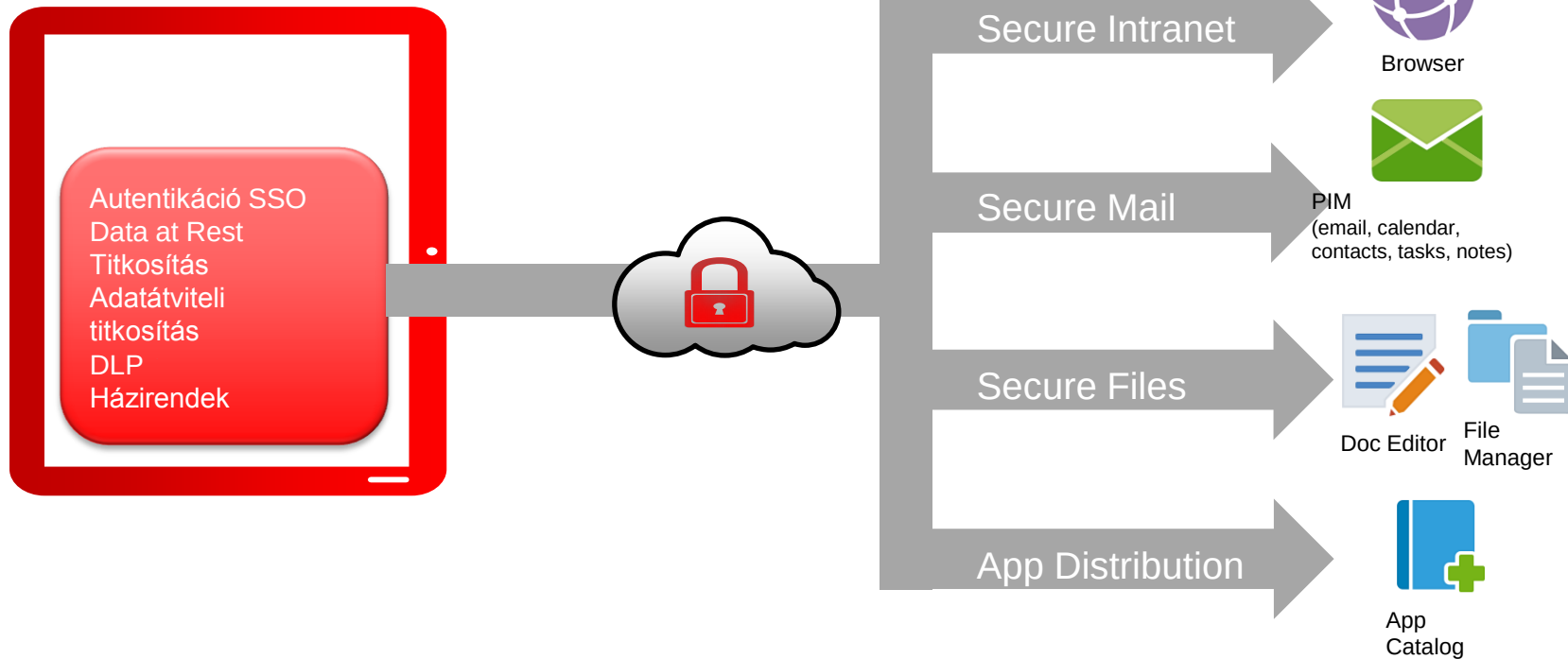
IDM szolgáltatások kiterjesztése



- Nemcsak felhasználók hanem eszközök kezelése is
- Közös felhasználó, szerepkör, önkiszolgálás, felülvizsgálat
- SSO nativ és böngészős alkalmazások számára
- Kockázat alapú autentikáció, eszközfelismerés fingerprinting

Oracle Mobile Security Suite

Elkülönített biztonságos munkaterület



Adatbiztonság kliens oldalon

Data-at-rest

- FIPS140-2 Level 1
- Kódolt tárolás
 - File system
 - Preferenciák
 - SQLite
 - Cache
- Felhasználói jelszavak NEM tárolódnak az eszközön,

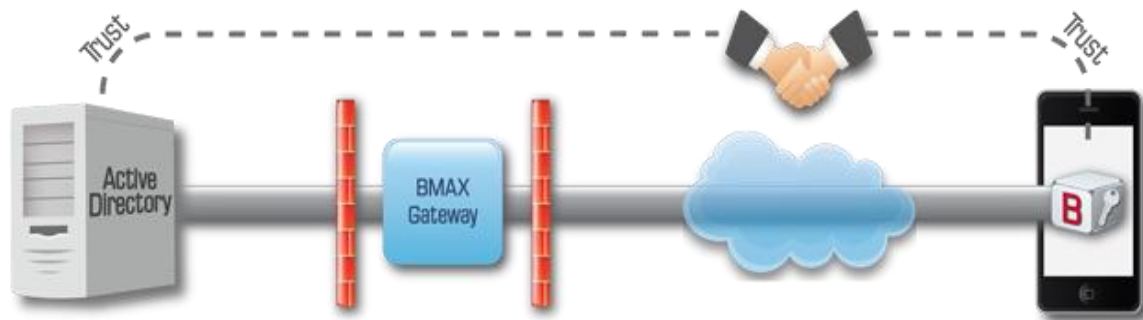
Adatátvitel

- AppTunnel és nem VPN
 - Nem szükséges VPN infrastruktúra
 - Csak trusted alkalmazások
- FIPS140-2 Level 1

AppTunnel

Nincs szükség eszköz szintű VPN-re

- Kölsönösen autentikált SSL tunnel
- Védett a rosszindulatú alkalmazásoktól
- Mobil forgalomra optimalizált
 - Kompresszió
- Wifi-3G váltást tolerálja



Autentikáció

Enterprise Auth/SSO

- Autentikáció
 - Single Sign-on
 - Kerberos, NTLM, SAML, OAuth
 - Erős autentikáció– PKI
 - Több faktoros
 - Virtuális smart card (PIN védett x509 cert)
 - Radius alapú OTP token (RSA certified)
 - Oracle Access Manager autentikáció és Oracle Unified Directory vagy AD mint userstore

Házirendek

Központi szerveren definiáltak

Data Leakage Protection

- Dinamikus, felhasználófüggő szabályok
- Kontrollok
 - No backup
 - Restrict open-in
 - Restrict copy/paste
 - No email, messaging
 - No chat, social sharing
 - No print

Szemponatok

- Alkalmazásonként
- Remote lock/wipe
- Authentikáció erőssége
- App Catalog
- Inaktivitás
- Time-fence / geo-fence

Konténerizációs eszköz

- Saját alkalmazások is behelyezhetők a konténerbe.
- Az alábbi szolgáltatásokat nyújtja a konténer
 - Biztonságos adattranszport: Az AppTunnel segítségével biztonságos kommunikáció a backend alkalmazásokkal
 - Autentikáció: Windows Integrated Authentication/SSO (Kerberos v NTLM) a backend szolgáltatások felé
 - Biztonságos adattárolás: Kódoltan tárolt alkalmazás adatok, fileok, cache
 - Adatszivárgás: file sharing-copy paste, nyomtatás, mentés szabályozható
 - Házirendek hozzárendelése: Több mint 50 féle kontroll pl autentikáció gyakorisága, geo és time fencing, remote lock és wipe.





DEMO

Összefoglalás

- *Mobil alkalmazásfejlesztés szempontból:*

Az Oracle teljeskörű, egységes, mind webes mind natív mobil alkalmazásokat lefedő hozzáférés-menedzsmentet kínál.

- *Mobil biztonsági architektúra szempontjából:*

Oracle megoldásokkal a mobil (és cloud) biztonsági kihívásai megválaszolhatóak (pll API biztonság, adatfolyam tartalmi szűrése, cloud szolgáltatások biztonságos használata), komplett mobil biztonsági architektúra építhető fel.

- *Mobileszköz védelmi szempontból:*

Az Oracle konténer alapú technológiája lehetővé teszi a BYOD probléma hatékony kezelését

Oracle idm közösség



Twitter

twitter.com/OracleIDM



Facebook

facebook.com/OracleIDM



Oracle Blogs

blogs.oracle.com/OracleIDM

<http://oracle.com/identity>

