IBM Technical Summit

Stay ahead.

Seema Kumar
Product Design – IBM Worklight Mobile Platform

Managing the Entire Mobile Environment to Enhance User Experience & Security

Let's Step Through the Three IBM Mobile Initiatives

Build and Connect

Build mobile apps

Connect & run mobile systems

- Building & Deploying Apps
- Mobile Lifecycle Management and Testing
- Data Access & Integration

Manage and Secure

Manage mobile devices, expenses, and apps

Secure my mobile business

- Device Management
- Network & Data Security and Management
- App Management

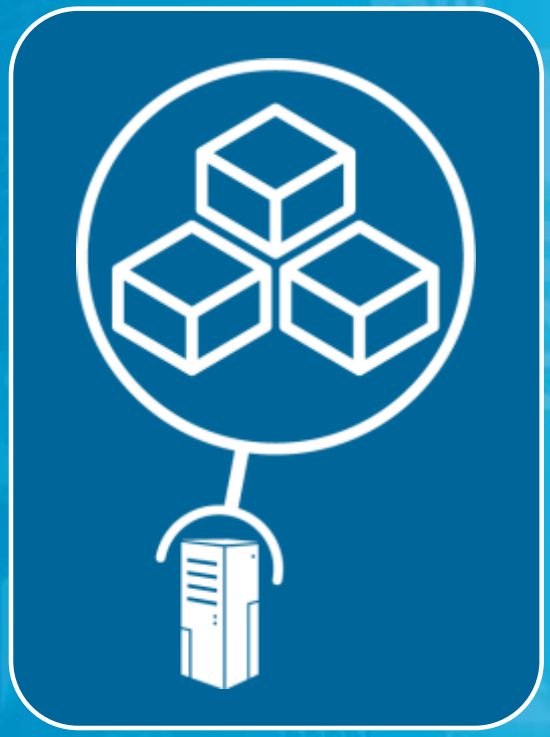
Extend & Transform

Extend capabilities to mobile

Transform my business

- Business Applications
- User Engagement
- Mobile Analytics and Insight

Helping Customers Build and Connect Their Mobile Applications



Mobile "Build and Connect" Imperatives and Challenges

Building & Deploying Mobile Apps

How do I develop & deliver across platforms?

- Secure code and reuse across platforms
- Management needs for B2C / B2B / B2E
- Analytics & continuous improvement
- Address multi-channel and multi-tier
- Rapid Prototyping

Mobile Lifecycle Management & Testing

How do I test and manage the lifecycle of the app?

- Access to device inventory
- Test automation & planning
- Lifecycle management
- Team collaboration
- Fit within existing enterprise development process

Data Access & Integration

How do I integrate into existing systems?

- Short project cycles & integration effort
- Different data usage patterns for mobile
- Content delivered in context
- Driving engagement (push) across multi-tier systems

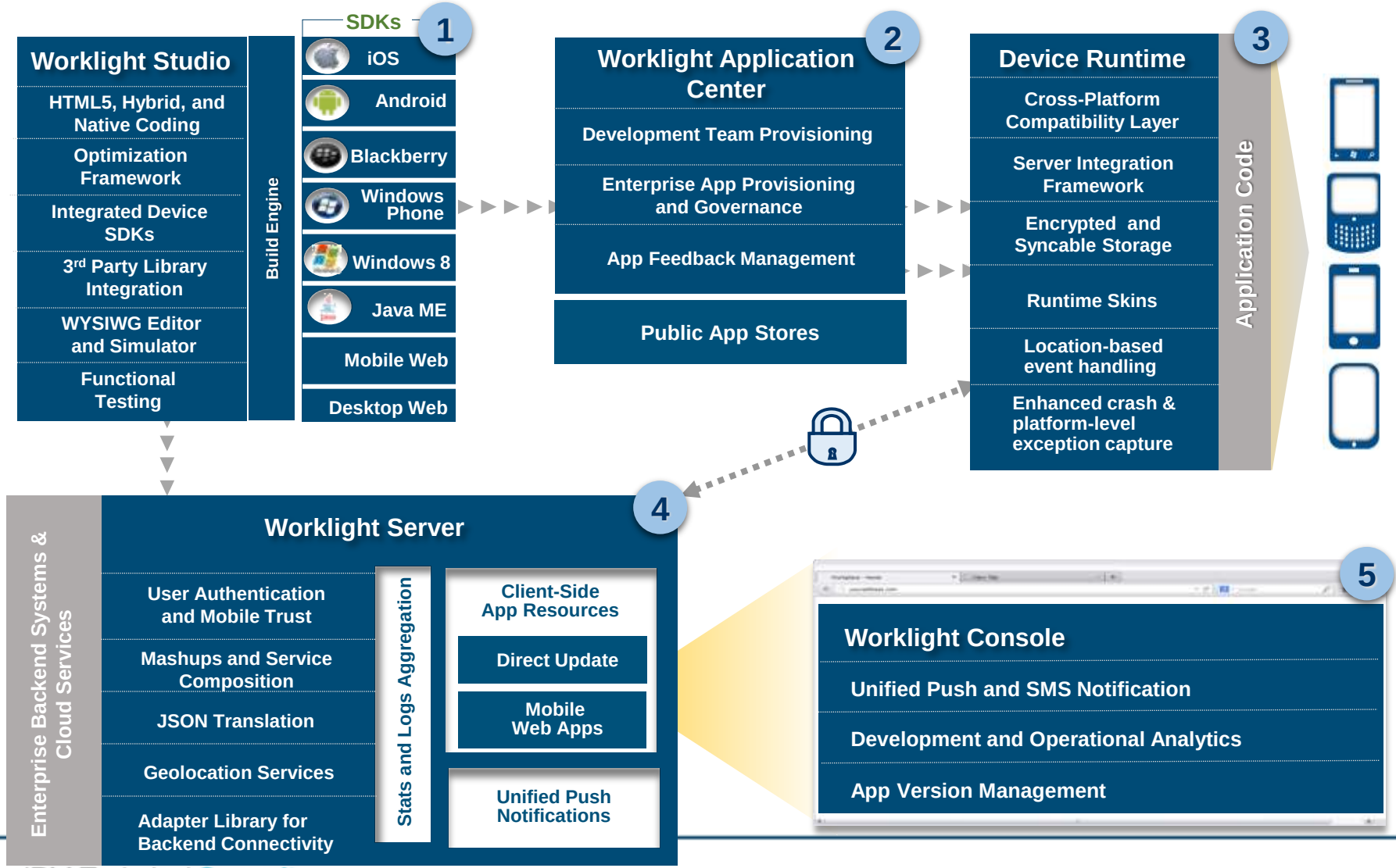
IBM Worklight Overview

Open standards-based development framework optimized for code re-use across device platforms.

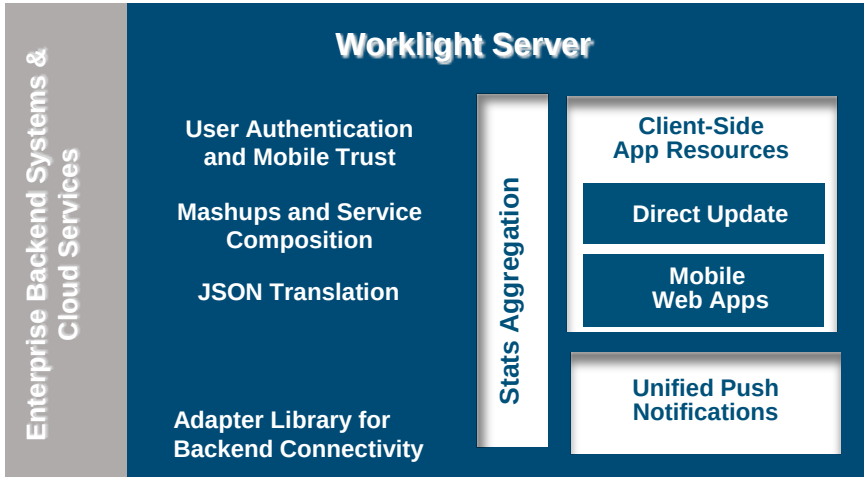
Mobile application server provides mobile-specific administrative, notifications, analytics and security services while leveraging existing investments in data, applications and infrastructure

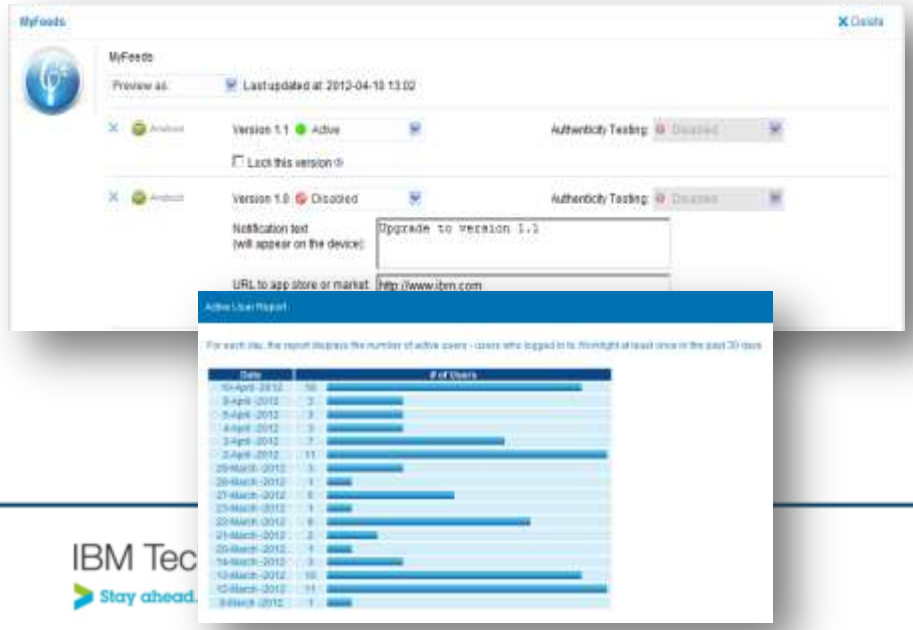
Client device layer enables client-side security, enforces app upgrades, secures local storage and allows access to device features.

IBM Worklight Components Overview



Worklight Server

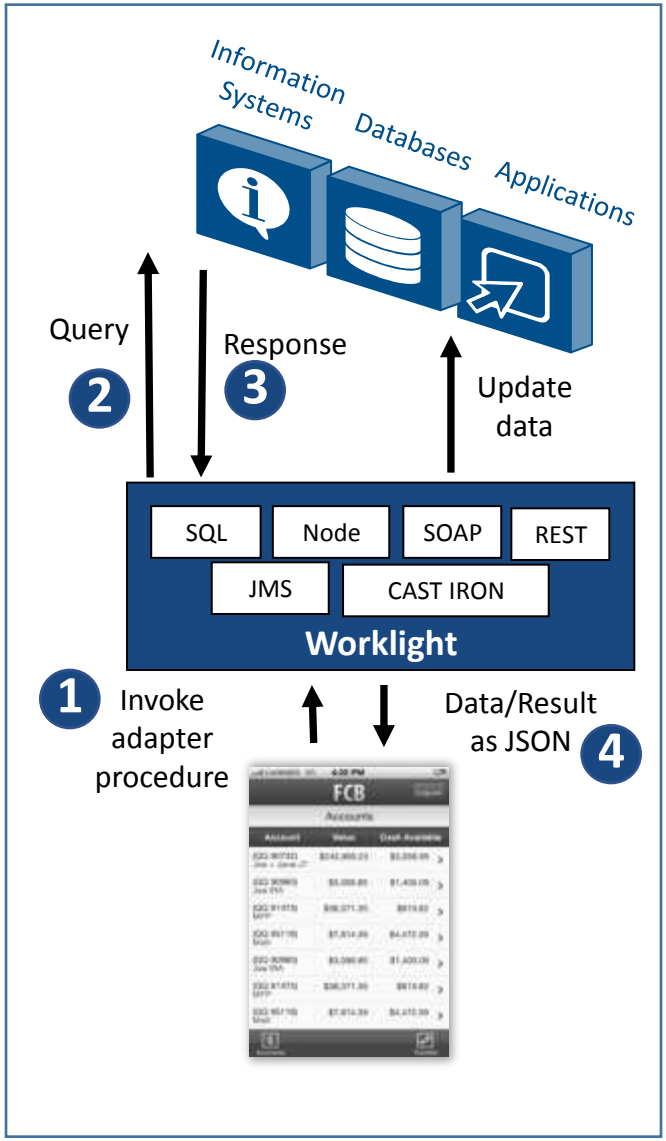




- Adapters with support for SOAP, REST, SQL, JMS, IBM Cast Iron, and Node.js (preview in 6.0)
- Performs Data Transformation to streamline back-end data for mobile consumption
- Server and device Security control
- Supports Physical Clustering for high availability
- Controls Application Deployment and Versioning
- Push Notification administration
- Analytics including user adoption, usage data, app crash and exceptions

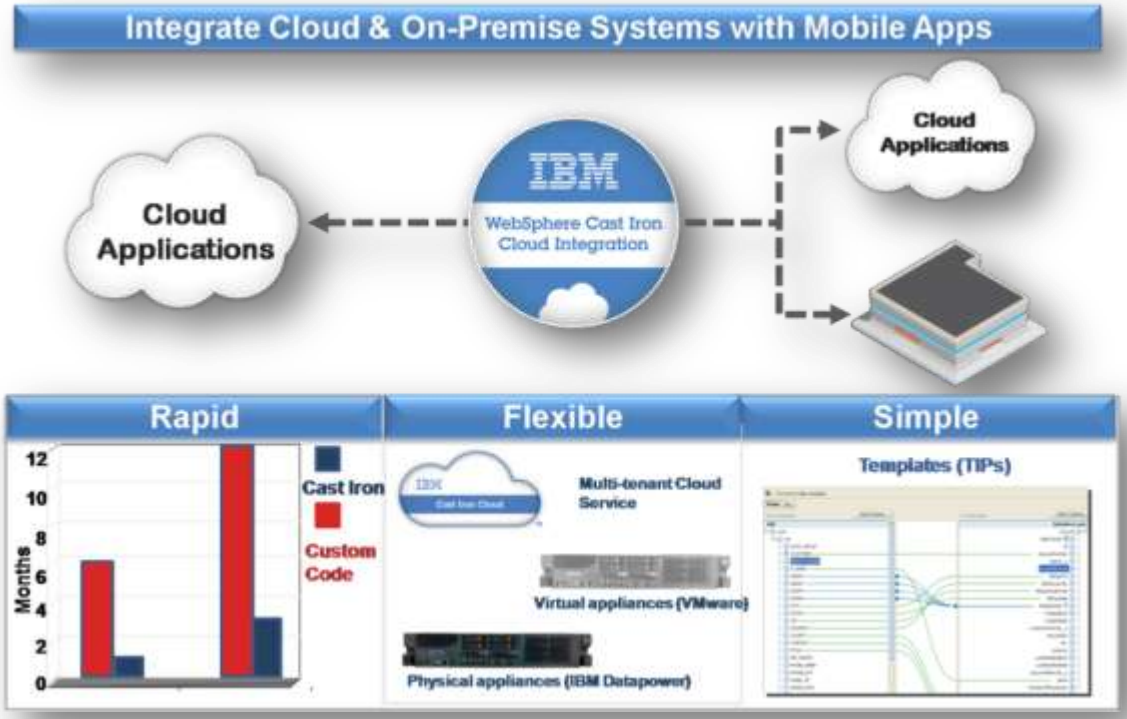
Worklight Server: Adapters

- Simplicity and Rapid Development
  - Defined using simple XML syntax, and easily configure with JavaScript API
- Security
  - Use of flexible authentication facilities to create connections with back-end systems
  - Adapters offer control over the identity of the connected user
- Transparency
  - Data retrieved from back-end applications is exposed in a uniform manner regardless of the adapter type
- Read-only as well as Transactional Capabilities
  - Adapters support read-only and transactional access modes to back-end systems



Cast Iron Integration

- IBM Worklight let organizations leverage the IBM Cast Iron Hypervisor through a simple adapter
  - Simply provide the Cast Iron orchestration name
- Can be used to integrate Worklight with 150-200 cloud and on premise apps
  - SaaS apps: Salesforce.com, Oracle CRM, Taleo.
  - Packaged apps: SAP, Oracle PeopleSoft EBS
  - Web Services, DBs, flat files/FTP



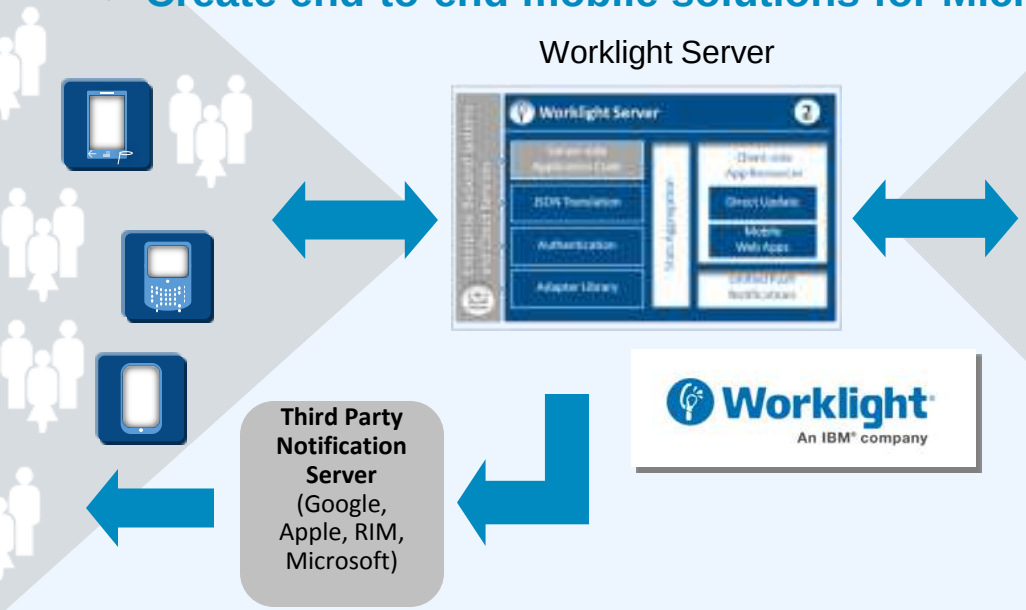
Leverage the Cast Iron tools to visually explore existing services and data sources and connect them to your mobile applications

Easy to Mobile Enable Enterprise Services

Secure, scalable access to critical data and back-end systems

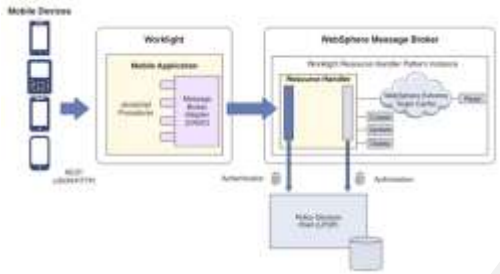
Built-in Patterns in IBM Integration Bus (previously IBM Message Broker)

- ✓ Mobile enable any enterprise service in as few as 2 clicks!
- ✓ Build robust solutions with integrated caching & security
- ✓ Push data to mobile users from enterprise applications
- ✓ Create end-to-end mobile solutions for Microsoft .NET



Mobile-enable your Enterprise

*Accelerate access to enterprise applications, systems and data from mobile devices**



Choose: Select your pattern

Configure: Accept default values or tailor for your scenario

1

2

IIB Patterns are configurable templates for common integration scenarios

Inform mobile users of key information with push notifications

Realize secure and scalable access to backend services with elastic caching

4

3

Write: Use Worklight studio – write once, run anywhere

Integrate: Generate Worklight adapter ready for deployment

Stay ahead.

*First Available in 3Q12

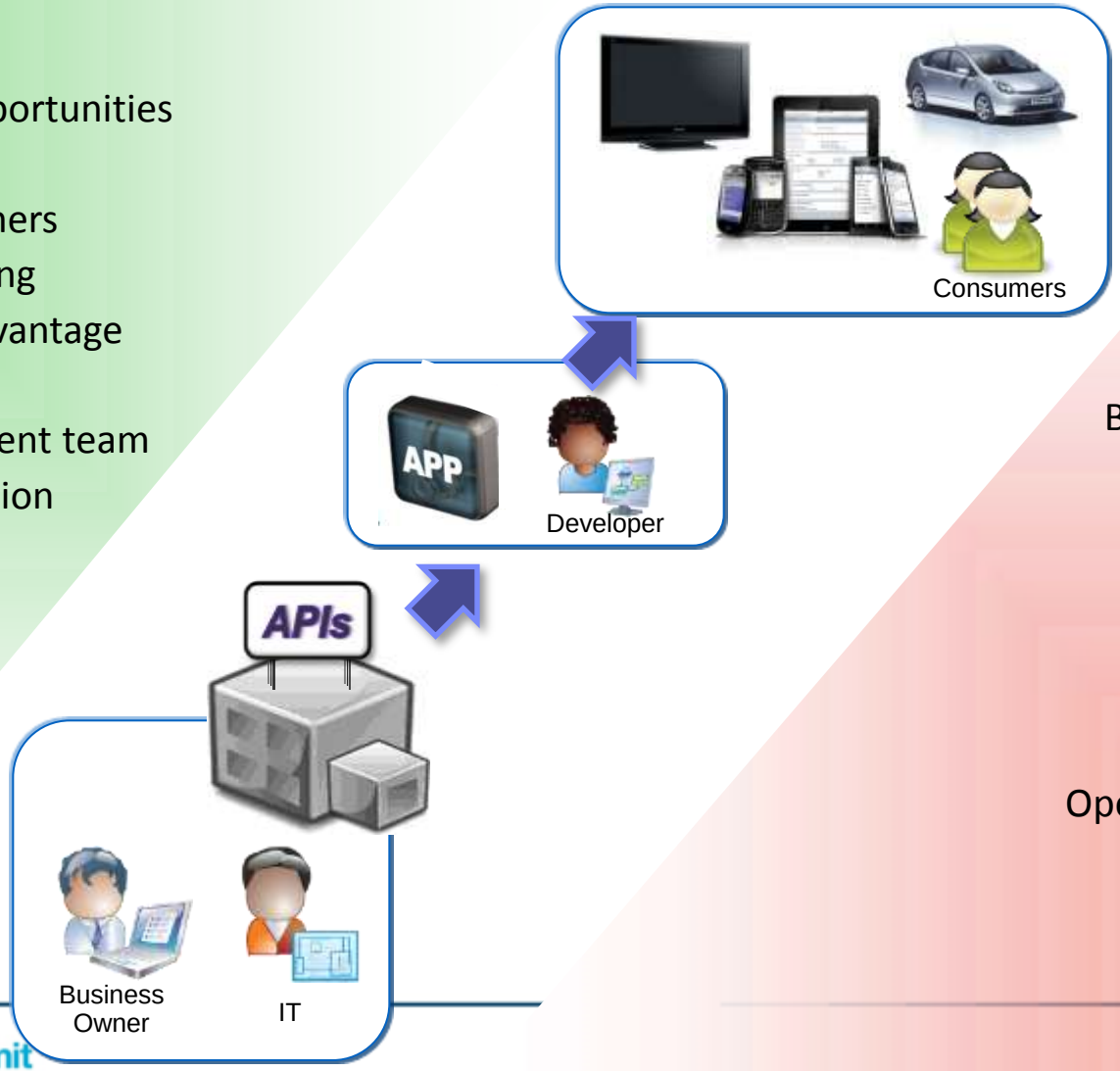
Apps, APIs and API Mgmt…

Benefits

New business opportunities
- New markets
- Increase customers
- Enhance branding
- Competitive advantage

Extend development team
- Increase innovation
- Increase scale

Partner/supplier alignment



Challenges

Business strategy

Infrastructure
- Security
- Creation
- Scalability

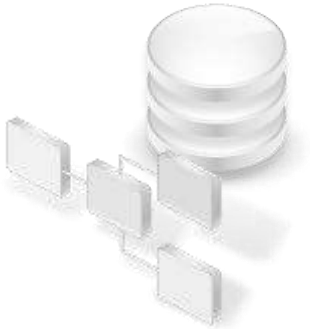
Operational control
- Publish
- Analyze
- Monitor

A complete API strategy should address API creation and consumption

Grow revenue through new channels

Deliver a differentiated customer experience

Creation



Assets & Services

- Assembly
- Transformation
- Rationalization

External APIs

Partner APIs

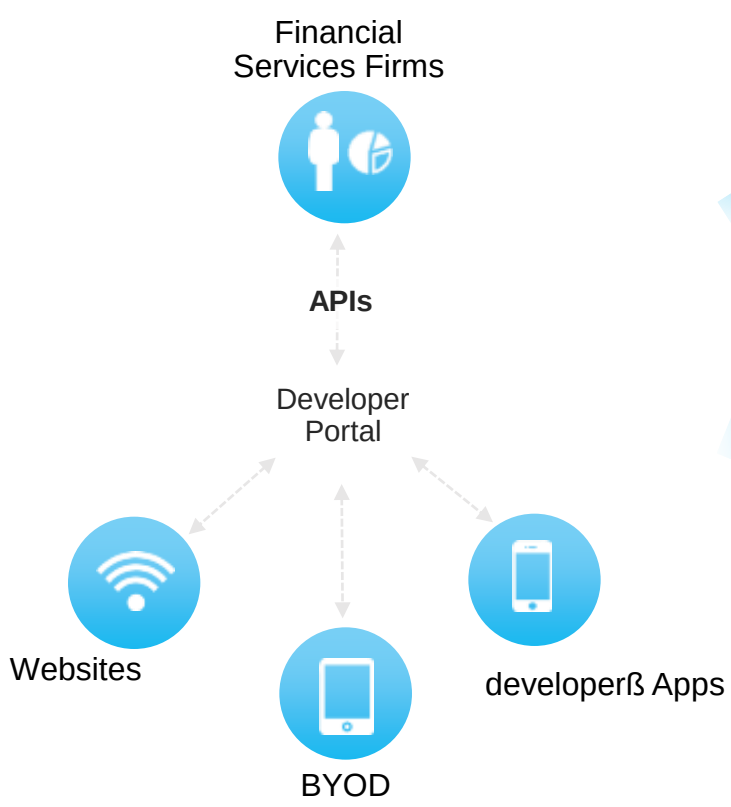
Internal APIs

Consumption

- Discovery
- Composition
- Deployment

Application End Points

Introducing IBM API Management
A single, comprehensive solution to design, socialize and manage APIs



1 In the cloud

OR

2 On-premise

MULTI-TENANT

Key capabilities in IBM API Management solution

Industry best security and integration in one solution

- Based on IBM market leading DataPower gateway
- Available as a service, providing risk free, full featured, no hassle 90 day trial
- Sign in and begin deploying APIs in less than 5 minute

Configuration, no coding

- Create and deploy a new API in just minutes
- Create a developer portal in minutes, and socialize your APIs to over 1 million developers
- ROI in a matter of days instead of months and years

Out of the box business analytics and operation insight

•Ability to pinpoint key market fluctuations and find correlations related to your business

•Drill down debug inspections of request and response messages reduce the time to problem determine of orchestrated APIs in production and development time.

Support for continuous iterative development

- Provide updates to the APIs with minimal to no interruption to your consumers.
- Test out minor fixes and push to production in matter of minutes
- Revert to a previous snap shot to restore last know good configuration at the touch of a button

API Developer

Helping Customers Manage and Secure Their Mobile Environments

Mobile Presents Management and Security Challenges

1 in 20 Mobile devices stolen in 2010

155% by which mobile malware increased 2011

70% of Mobile device spam is fraudulent financial services

77% growth in Google Android malware from Jun 2010 to Jan 2011

350% by which WiFi hotspots are set to increase by 2015, providing more opportunities for “man-in-the middle” attacks

10 Billion Android app downloads reached by the end of 2011 – over 90% of the top 100 have been hacked

Source: Evans Data Mobile Developer Survey Mobile Development Report 2012 Volume
Source: Business Insider (September 2012)

Thinking Through Mobile Management and Security

IBM Mobile Management and Security Strategy

- Management and safe use of smartphones and tablets in the enterprise
- Secure access to corporate data and supporting privacy
- Visibility and security of enterprise mobile platform

At the Device

Enroll
Register owner and services

Configure
Set appropriate security policies

Monitor and Manage
Ensure device compliance and mange Telecom expenses

Reconfigure
Add new policies over-the-air

De-provision
Remove services and wipe

On the Network

Authenticate
Properly identify mobile users

Encrypt
Secure network connectivity

Monitor and Manage
Log network access and events manage network performance

Control
Allow or deny access to apps

Block
Identify and stop mobile threats

For the Mobile App

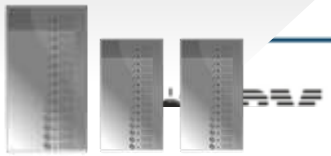
Develop
Utilize secure coding practices

Test
Identify application vulnerabilities

Monitor and Manage
Correlate unauthorized activity and Manage app performance

Protect
Defend against application attacks

Update
Patch old or vulnerable apps



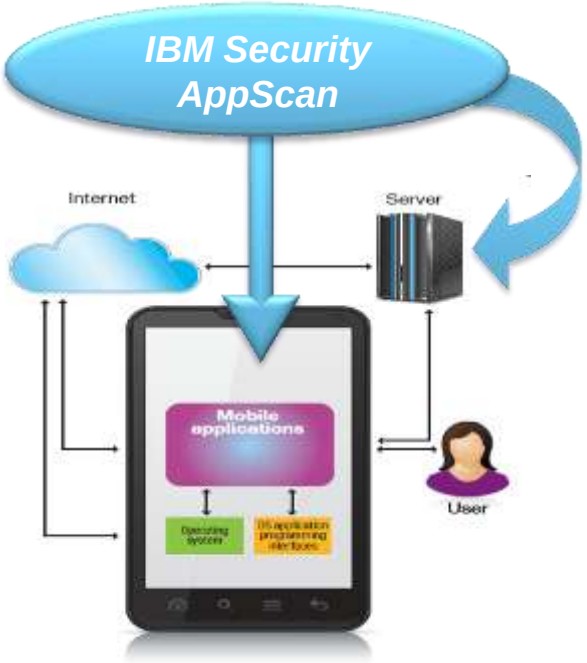
Internet

Corporate Intranet

IBM Security AppScan

Identify vulnerabilities in web and mobile application source code

- **Native Android** and **iOS** application support
- Better vulnerability detection from:
  - **Risk assessment of over 40,000 APIs**
  - **Full call** and **data flow analysis** for Java, JavaScript, Object-C (Mac OS X)
- Provides identification of **sensitive data leak** sources
- Helps reduce **malware susceptibility** of mobile apps

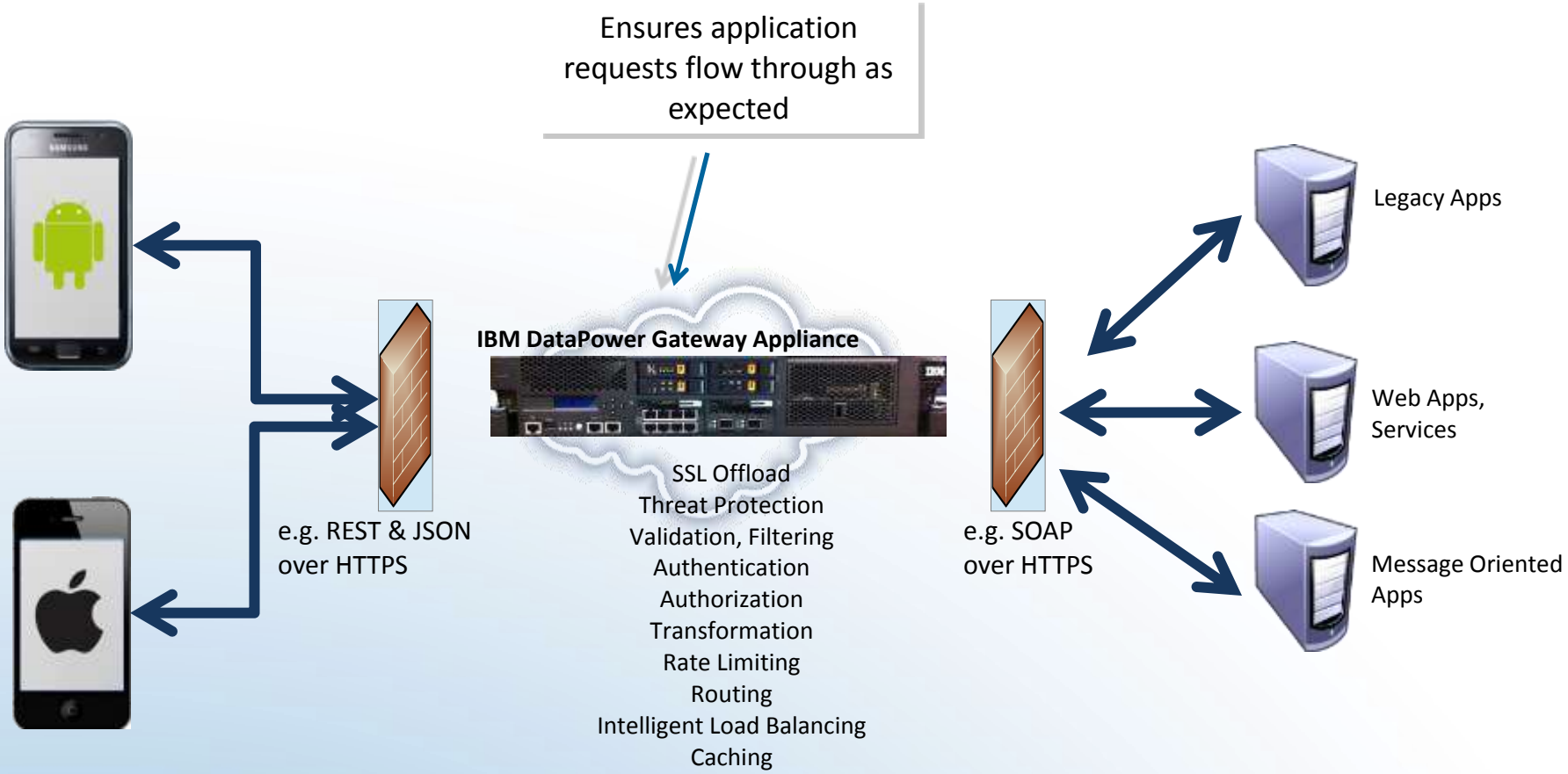


New!

What's new in IBM Security AppScan V8.7

- ✓ Native support extended for iOS to accelerate enterprise usage
- ✓ Enhanced support for JavaScript analysis in hybrid mobile apps
- ✓ Out-of-the-box support for IBM Worklight built apps to incorporate context aware risk-based access

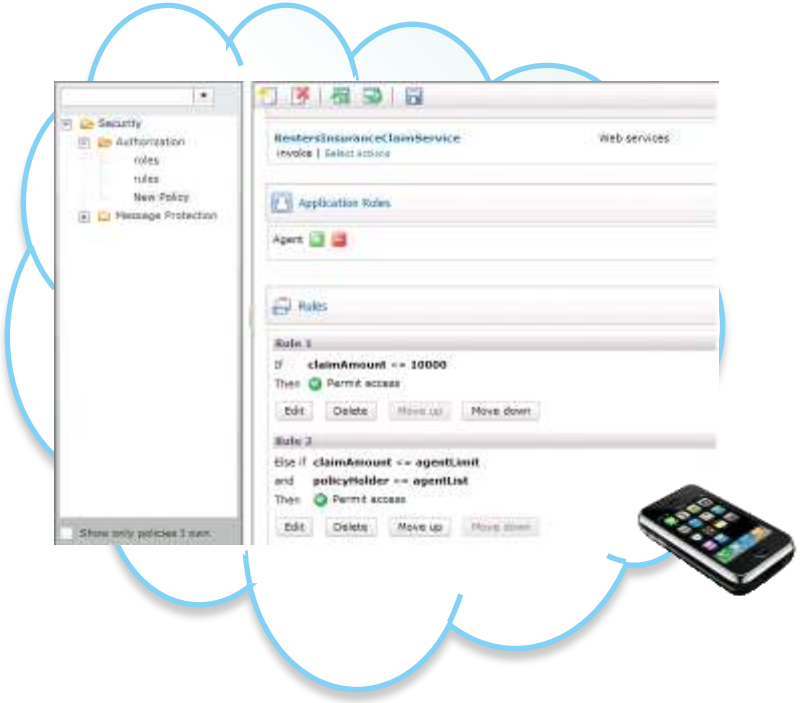
Securely & Rapidly connect Mobile Apps with Enterprise Services



IBM Security Access Manager for Cloud and Mobile

Extend user-access protection to cloud and mobile environments

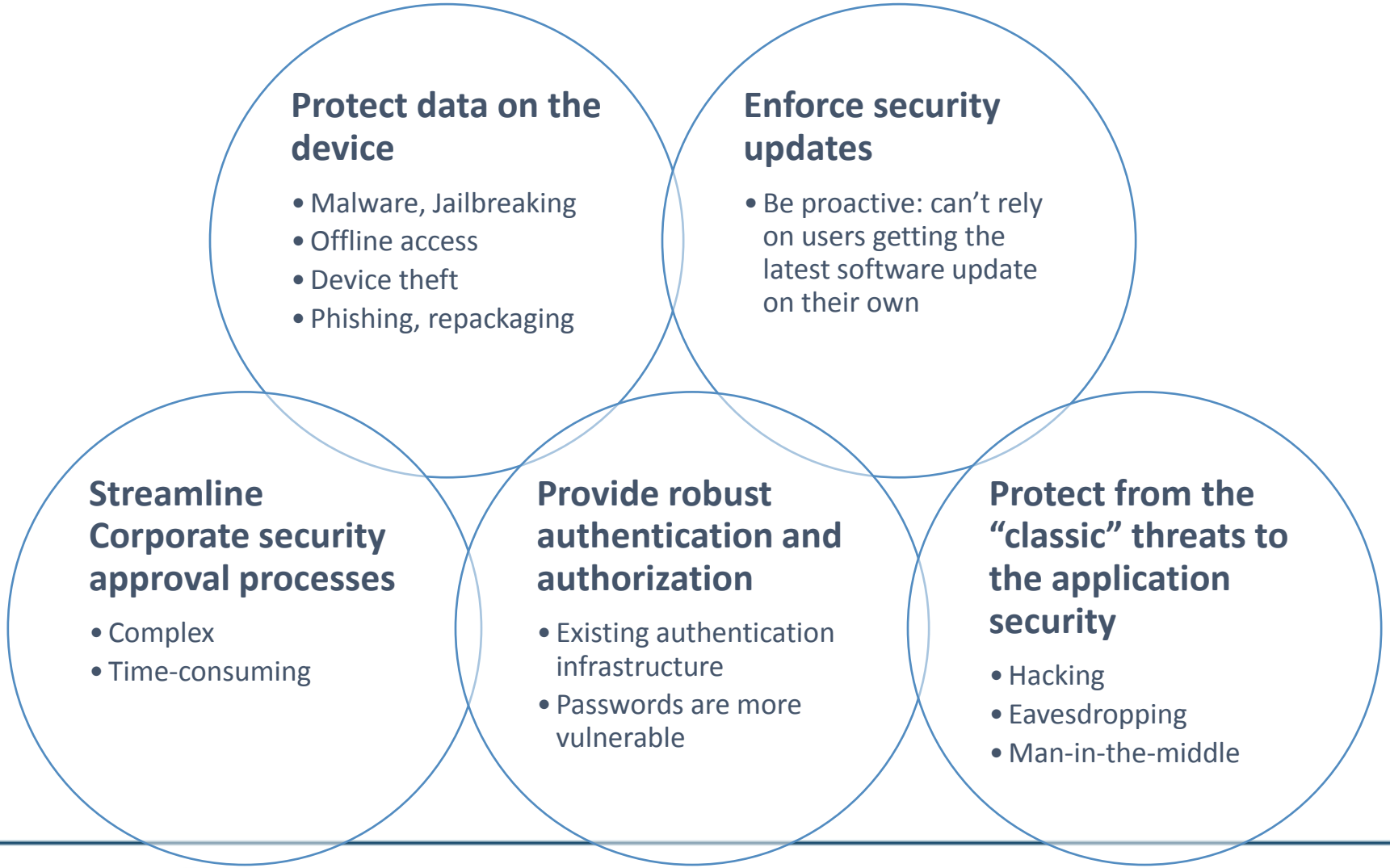
- **Context-aware detection and prevention** capabilities
- Enable **federated single sign-on** (SSO) and identity mediation across different service providers
- **Mobile authentication** and **one-time password support**
- **Consistently execute security policies** across multiple applications and users



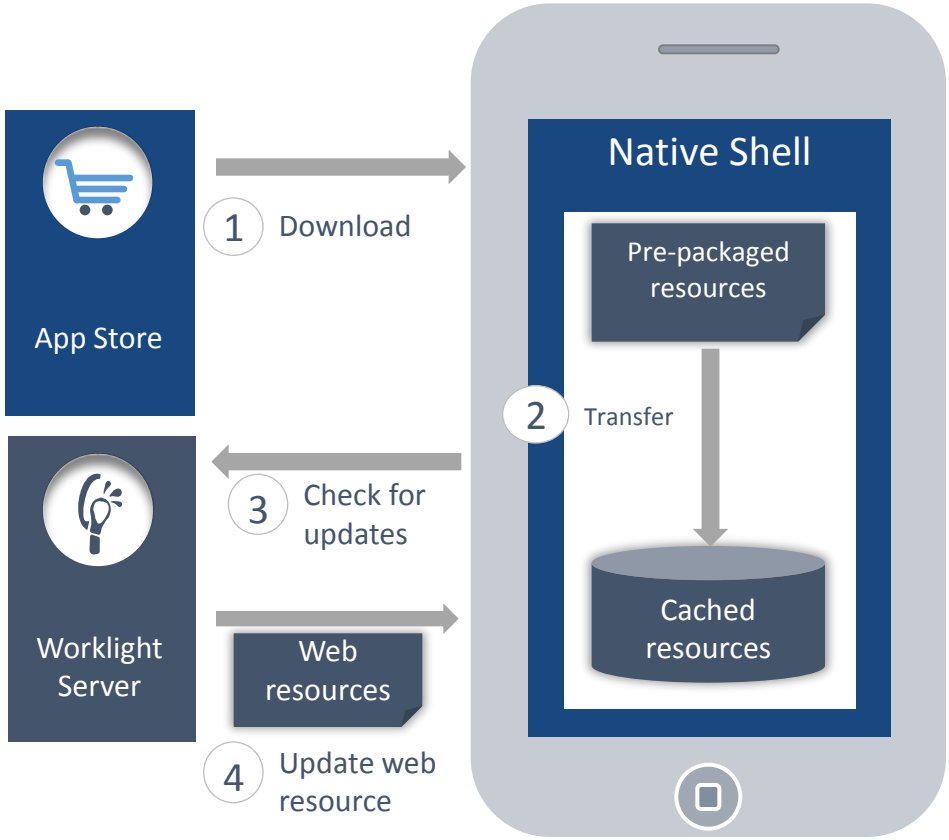
Security-rich cloud services access to mobile users with IBM Security Access Manager and IBM WebSphere DataPower

- ✓ Authentication and authorization to back-end services
- ✓ Security-rich integration and federated single sign-on with third party service providers

Mobile Application Security Objectives



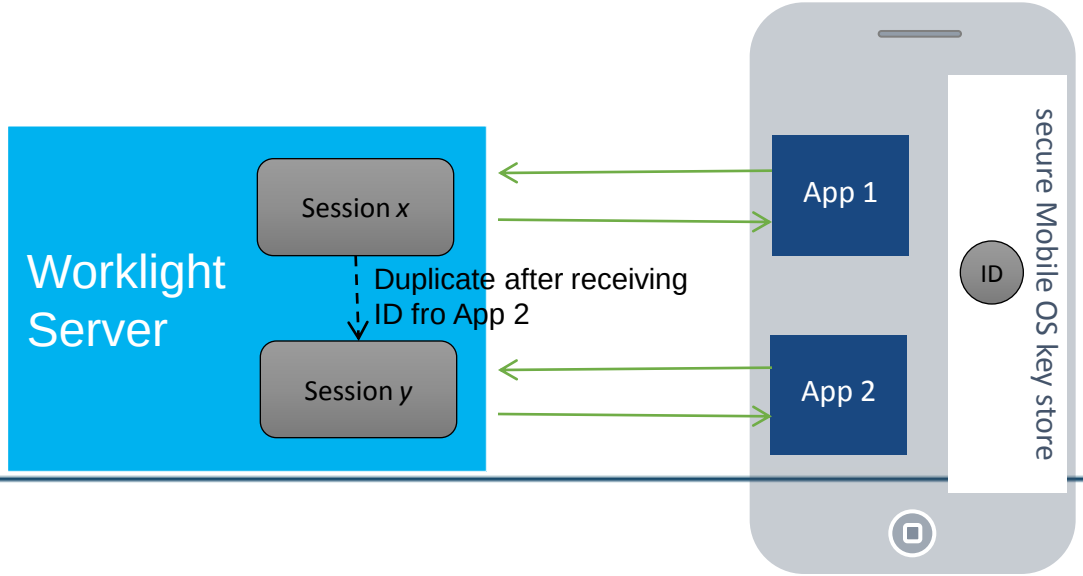
Worklight Runtime – Direct Update On-device Logic



1. Web resources packaged with app to ensure initial offline availability
2. Web resources transferred to app's cache storage
3. App checks for updates on startup and foreground events
4. Updated web resources downloaded when necessary, with user confirmation or silently

Device Single Sign-On (SSO)

- Device SSO Capability:
  - Device-side SSO enables a mobile user to authenticate him/her-self once and gain access to all apps from the same developer without being prompted to log in again at each of them
- Device SSO implementation:
  - Implemented using combination of server-side capabilities (realms) and unique device identification (device ID)
  - On successful login the authentication state is saved in the database and used for validations in subsequent sessions from the same device.



Worklight Runtime - Shell Approach

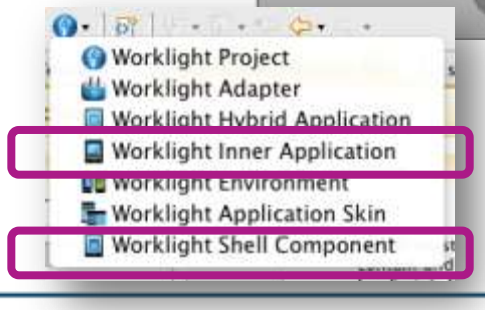
Organizations can develop “custom shells” that include corporate services, such as authentication and security services, integration services, and branding. Web developers can then use sanctioned shells to develop the business logic of the application using only HTML5

•Inner Application:

- Implements the application’s logic
- Common web code
- Utilizes External Shell API’s
- Required to comply with shell parameters

•External Shell:

- Customizable container
- Provides JS access to native functionality
- Branding, Security, Authentication
- Built with the Inner App to create a native App (IPA/APK file)



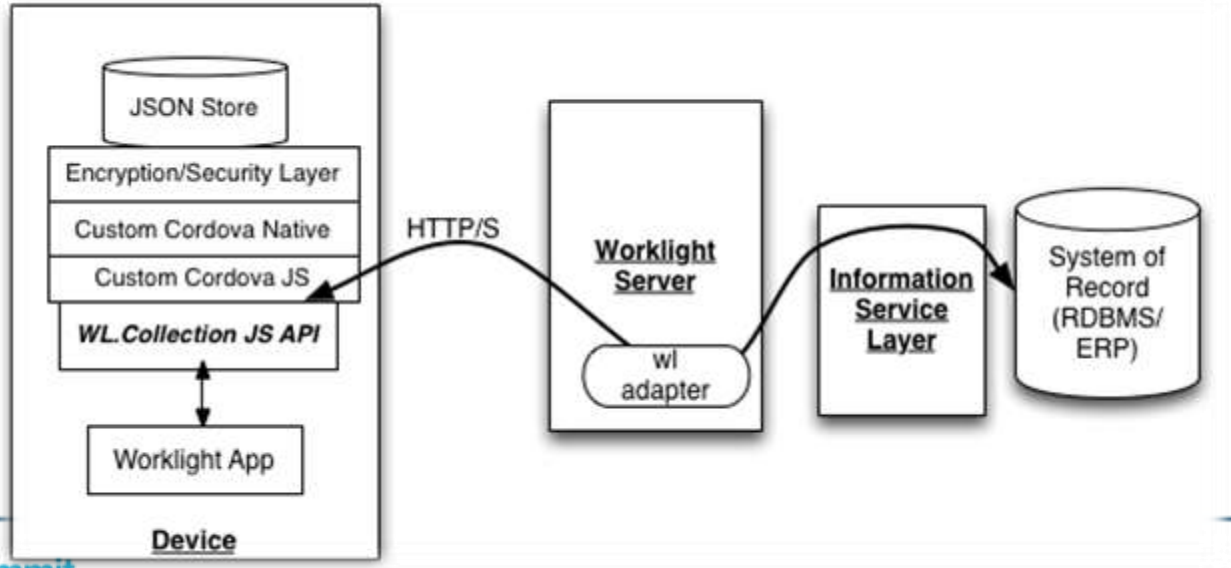
Secure device ID and provisioning

•Applications built with IBM Worklight create a unique device ID on iOS and Android devices and store this ID securely on the device. Organizations can integrate the apps with a custom provisioning process, ensuring that an app (or a group of apps) is only installed on sanctioned devices.

•This feature helps organizations support the Bring Your Own Device (BYOD) trend, allowing employees to use personal devices for work purposes, but maintaining control and enforcing security protocols.

Mobile Data support

- **On-device, mobile database support:**
  - Embedded JSON mobile database
  - JavaScript APIs to store, query and update the data in offline mode using MongoDB like APIs
- **Encrypt sensitive data:** Using a key provided by developer or obtained as user's password
- **Server-to-client Sync:** Retrieve, store and keep data store up-to-date using adapters
- **Client-to-server Sync:** Simplify write actions on data while the app is offline and send these actions to the server

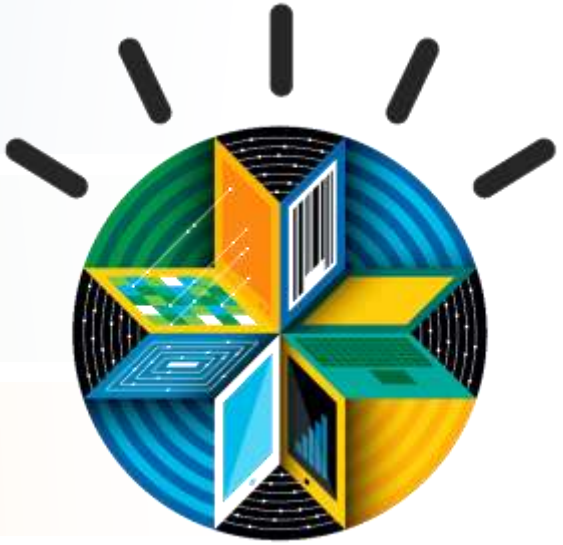


Three ways to get started with IBM MobileFirst

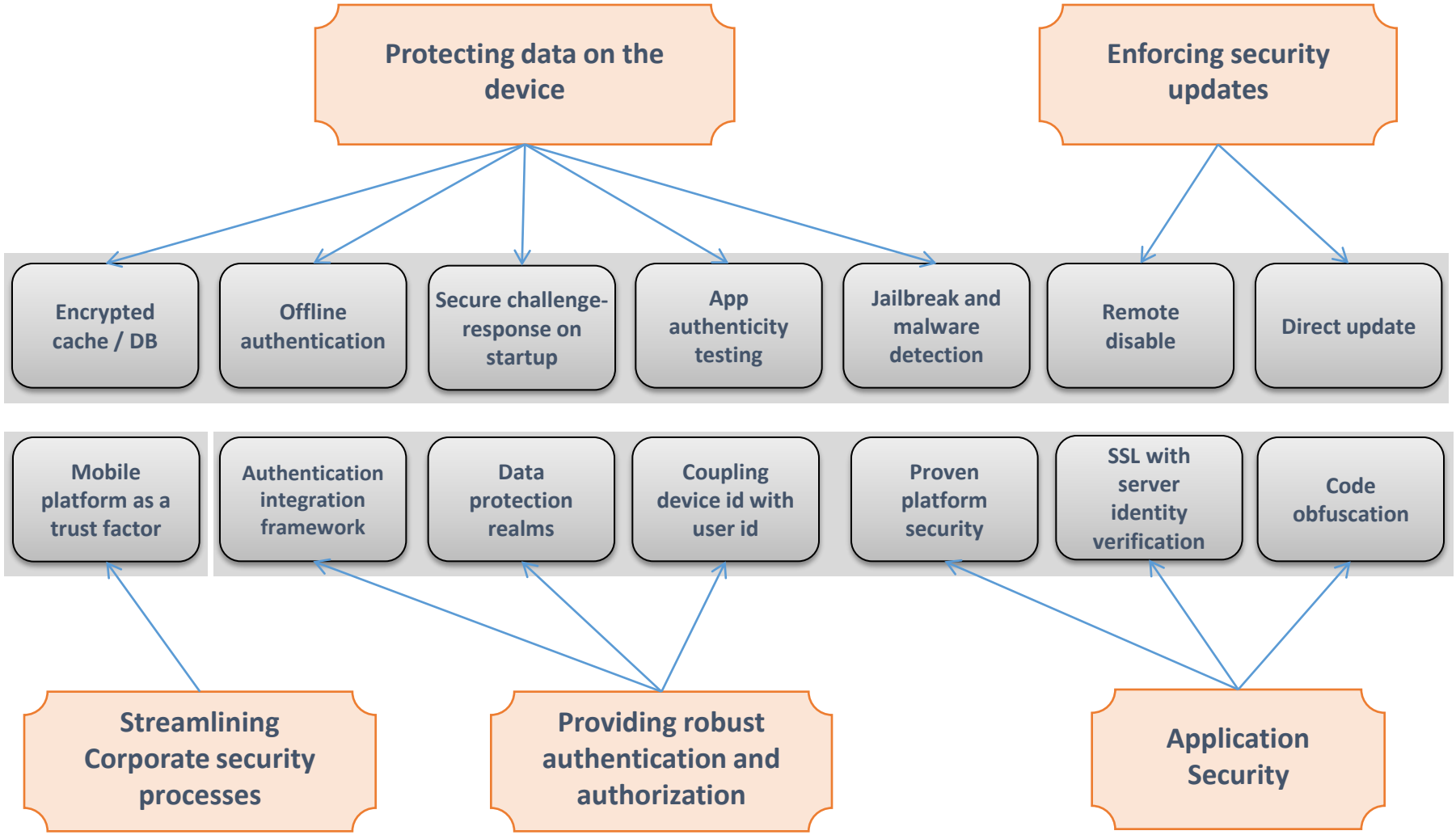
1. **Learn more about our mobile-enabled apps and solutions:** www.ibm.com/socialtogo

2. **Learn more about IBM MobileFirst:**
   ibm.com/mobilefirst
   twitter.com/IBMMobile (#IBMMobile)
   facebook.com/IBMMobile

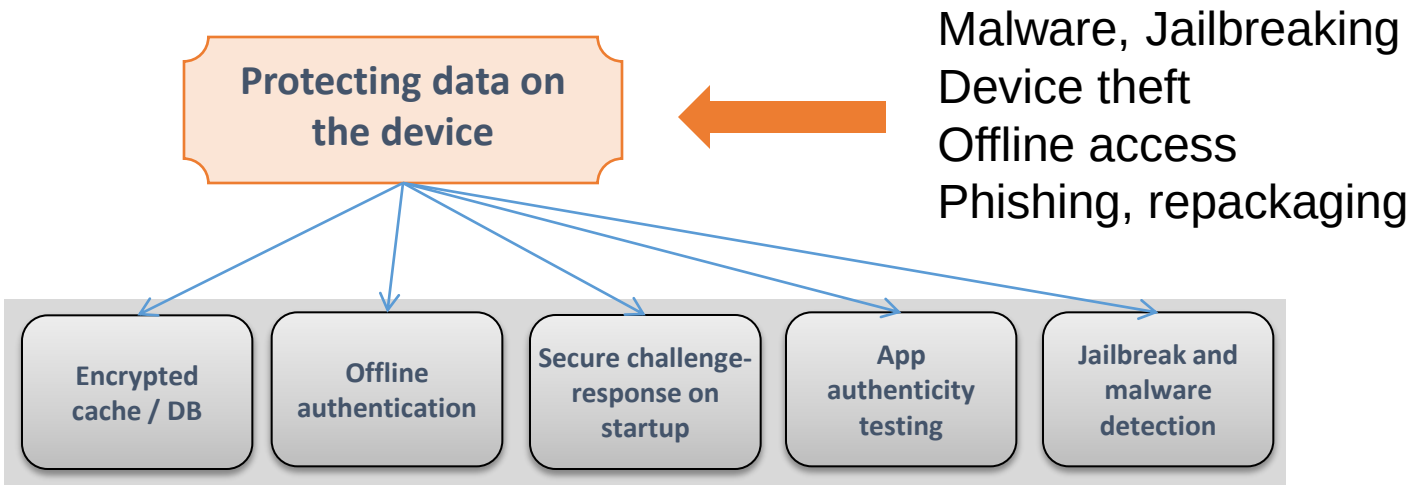
3. **Talk with your IBM representative or Business Partner to find the right next step for you**



Security Features Mapping



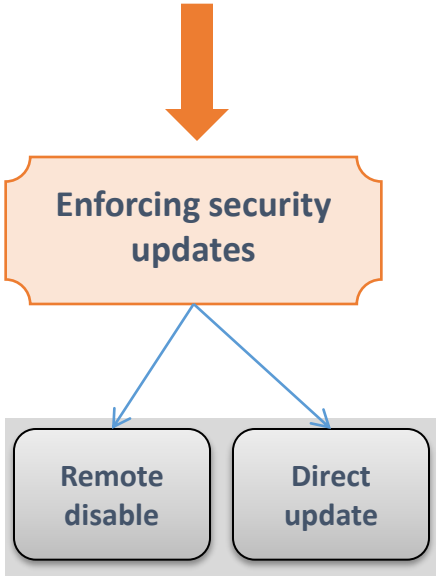
Protecting data on the device



- Encrypted cache / DB
- Offline authentication using password
- Extended authentication with server using secure challenge response
- App authenticity testing: server-side verification mechanism to mitigate risk of Phishing through repackaging or app forgery
- Compatibility with various jailbreak and malware detection libraries

Enforcing security updates

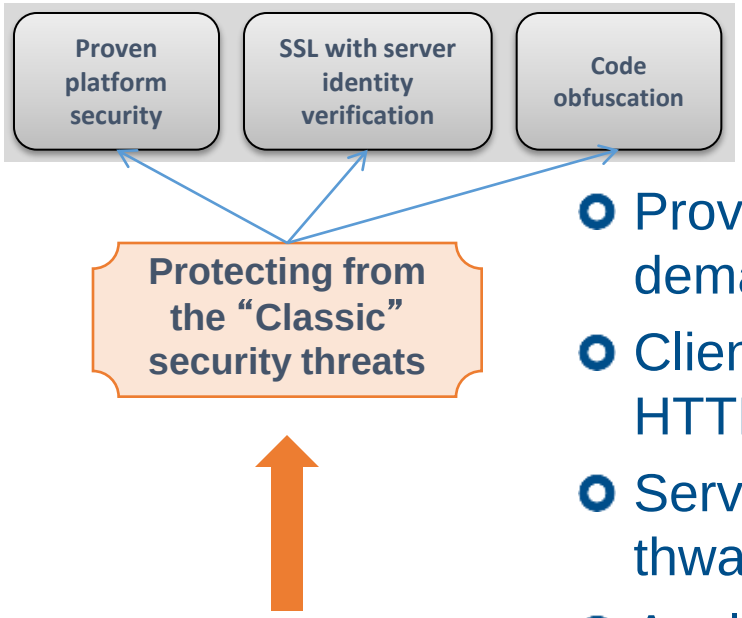
Can't rely on users getting the latest software update on their own



- Remote Disable: shut down specific versions of a downloadable app, providing users with link to update

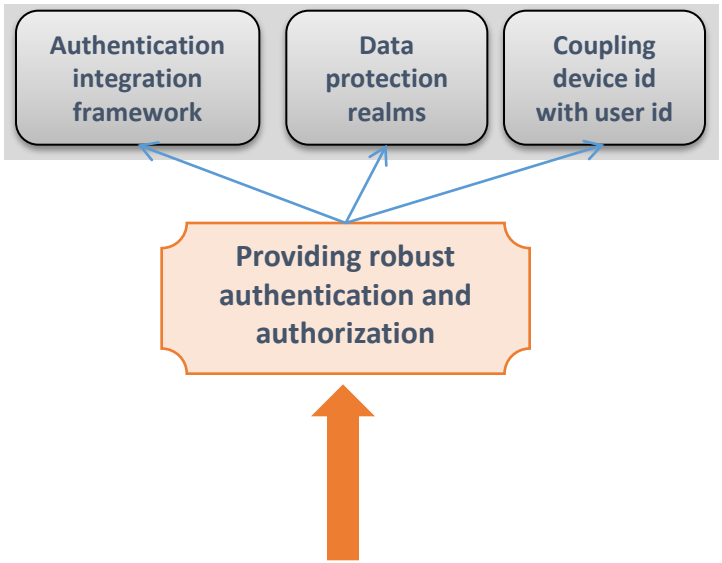
- Direct Update: automatically send new versions of the locally-cached HTML/JS resources to installed apps

Application Security



- Proven platform security: tested by the most demanding customers (e.g., top tier banks)
- Client<->Middleware communications over HTTPS to prevent data leakage
- Server certificate is automatically verified to thwart man-in-the-middle attacks
- Application JS code can be obfuscated to make static analysis more difficult
- SQL adapter designed to mitigate SQL-injection
- Built-in audit trail

User Authentication and Authorization



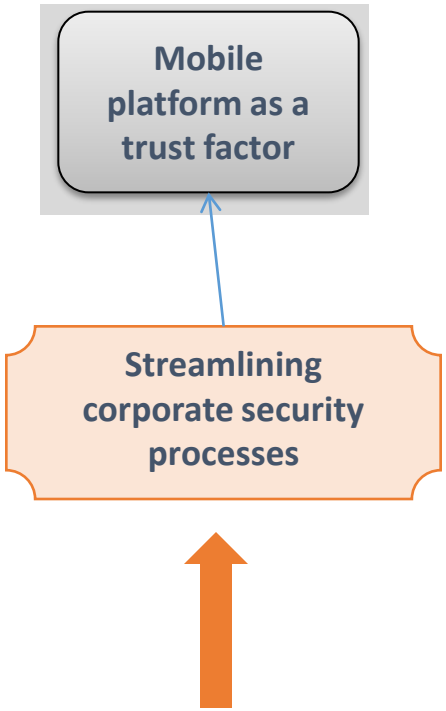
Need to integrate with existing authentication infrastructure

Authenticate users when offline

Mobile passwords are more vulnerable (keyboard more difficult to use, typed text is visible)

- Very flexible framework for simplifying integration of apps with existing authentication infrastructure
- Manages authenticated sessions with configurable expiration
- Open: e.g., custom OTP as anti-keylogger mechanism
- Server-side services grouped into separate protection realms for different authentication levels
- Two-factor authentication using device id as “what you have” factor

Simplifying corporate security processes



- Objective: apps developed on the platform will be easier for the security group to approve
- Mechanisms: pre-approve platform with security group. Identify corporate-specific concerns and provide solutions within the platform framework.
- Result: release cycle for apps made by independent development groups within the organization significantly shortened.

Mobile Application Spectrum Coverage