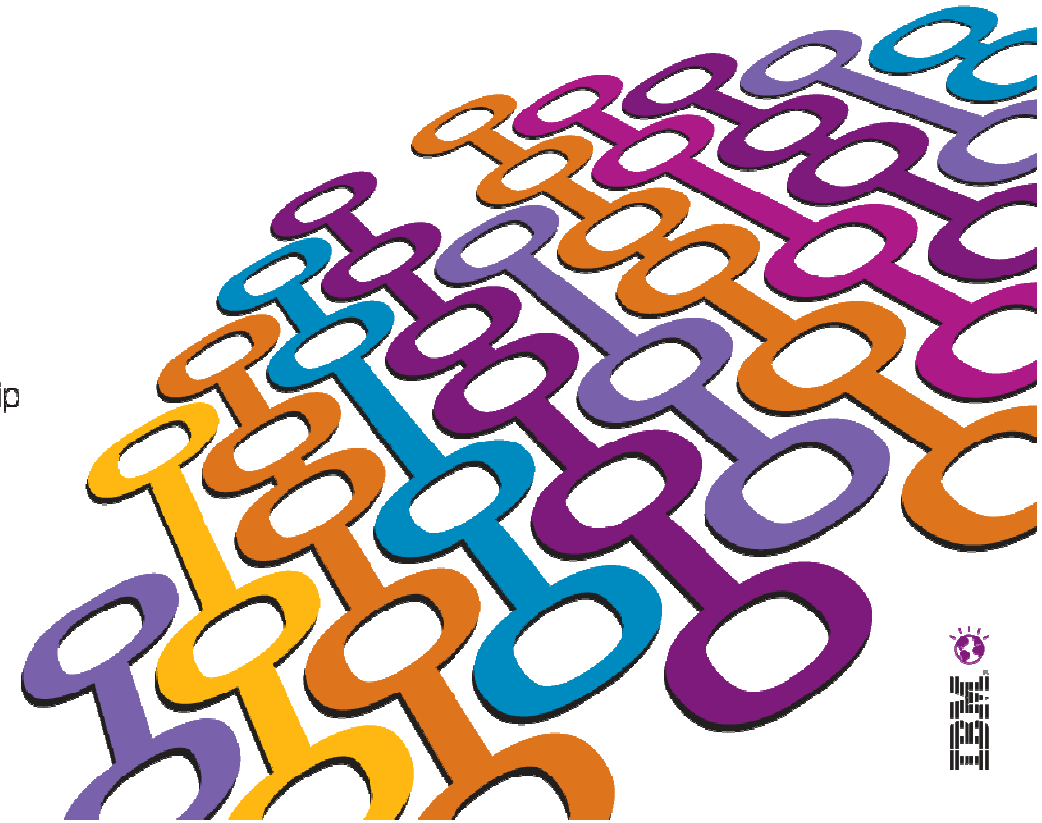
Security and Mobile Application Management with Worklight

Impact2012

The Premier Conference for Business and IT Leadership

Innovate. Transform. Grow.



Please Note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

IBM Has Extensive Approach to Mobile Security

At the Device

Manage device
Register; Set appropriate security policies; compliance; wipe; lock.

Secure Data
Data separation; Encryption.

Secure Application
App security policies; application level controls

Over the Network & Enterprise

Secure Access
Properly identify mobile users & devices; allow or deny access. Connectivity.

Protect from threats
Protect from mobile and web threats

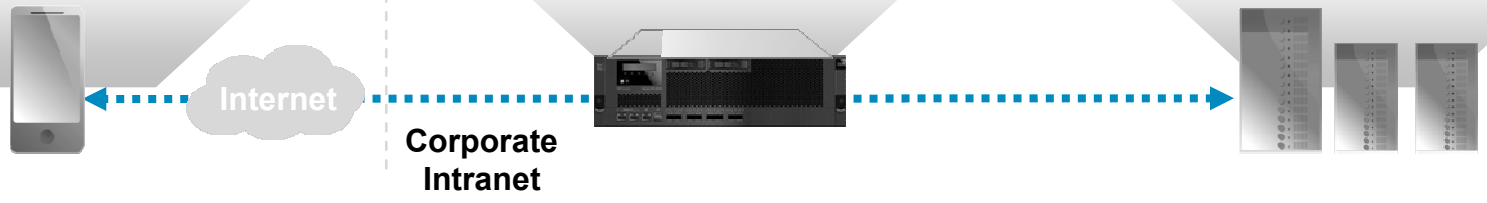
Monitor access
Log network access, events. Monitor & gain intelligence

For the Mobile App

Develop Secure App
Develop secure apps; Utilize secure coding practices.

Test for Vulnerabilities
Test and Identify application vulnerabilities

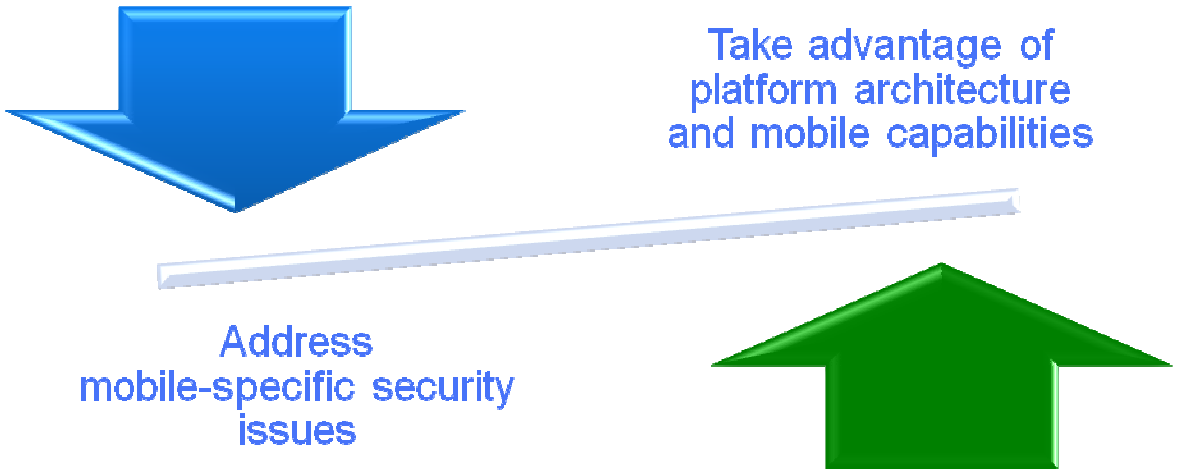
Integrate Securely
Secure connectivity to enterprise applications and services



IBM Mobile Security Strategy

- Safe usage of smartphones and tablets in the enterprise
- Secure access to corporate data and supporting privacy
- Visibility and security of enterprise mobile platform

Worklight Security Focus: Support Creation and Delivery of Secure Mobile Apps



- Security is a platform-wide consideration, relating to all components:
  - Server
  - Device run-time
  - Studio
  - Console

The Difference Between Secure Apps and Device Management

Mobile Device Management

Device-level control:

- Password protection
- File-system encryption
- Managed apps
- Jailbreak detection

Requires consent of user to have enterprise manage entire device

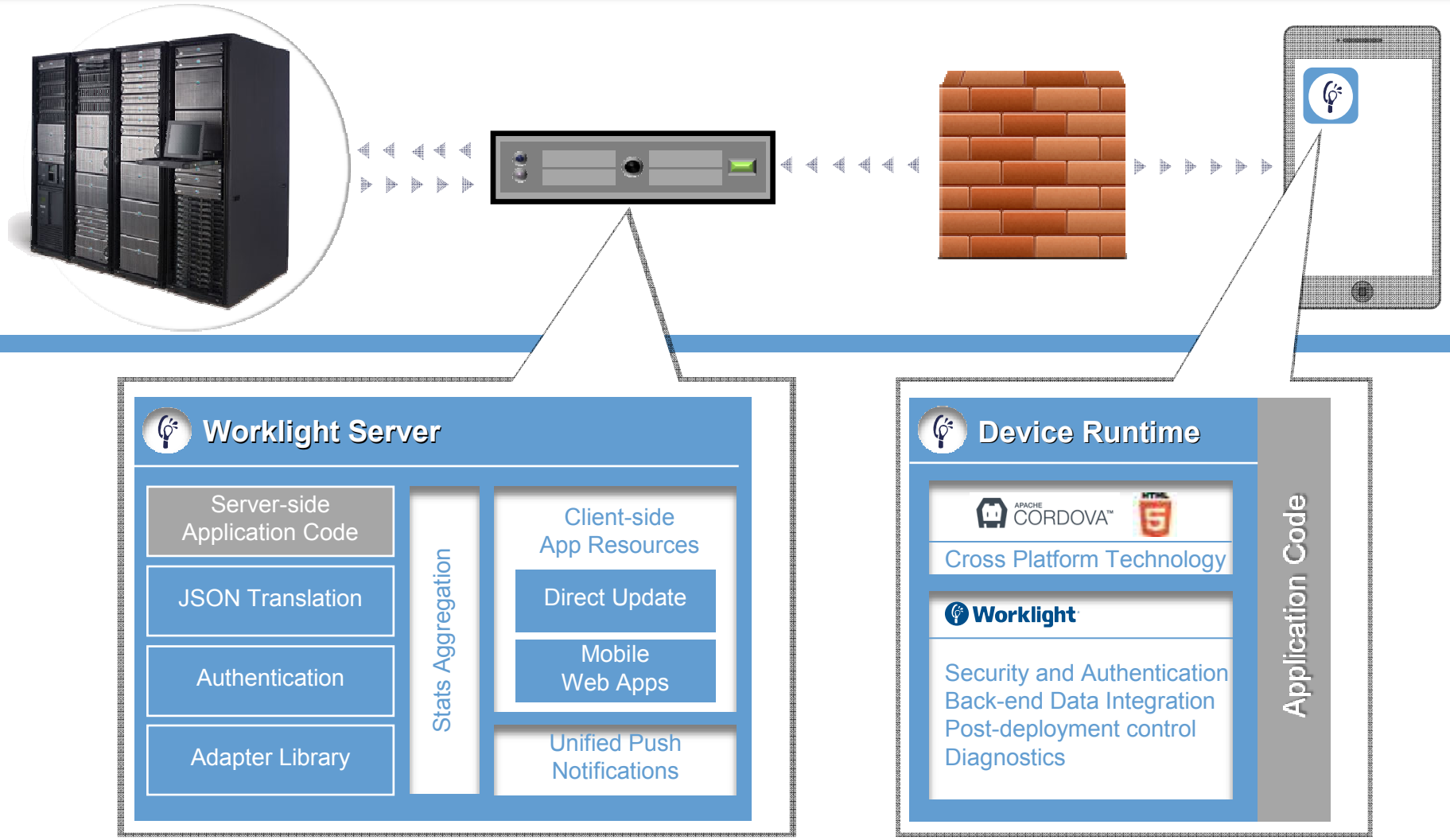
Application-Level Security

App takes care of itself:

- Authentication
- File encryption
- Remote administration
- Adaptive functionality

Applicable in all scenarios, including BYOD and consumer-facing contexts

Worklight Runtime Architecture

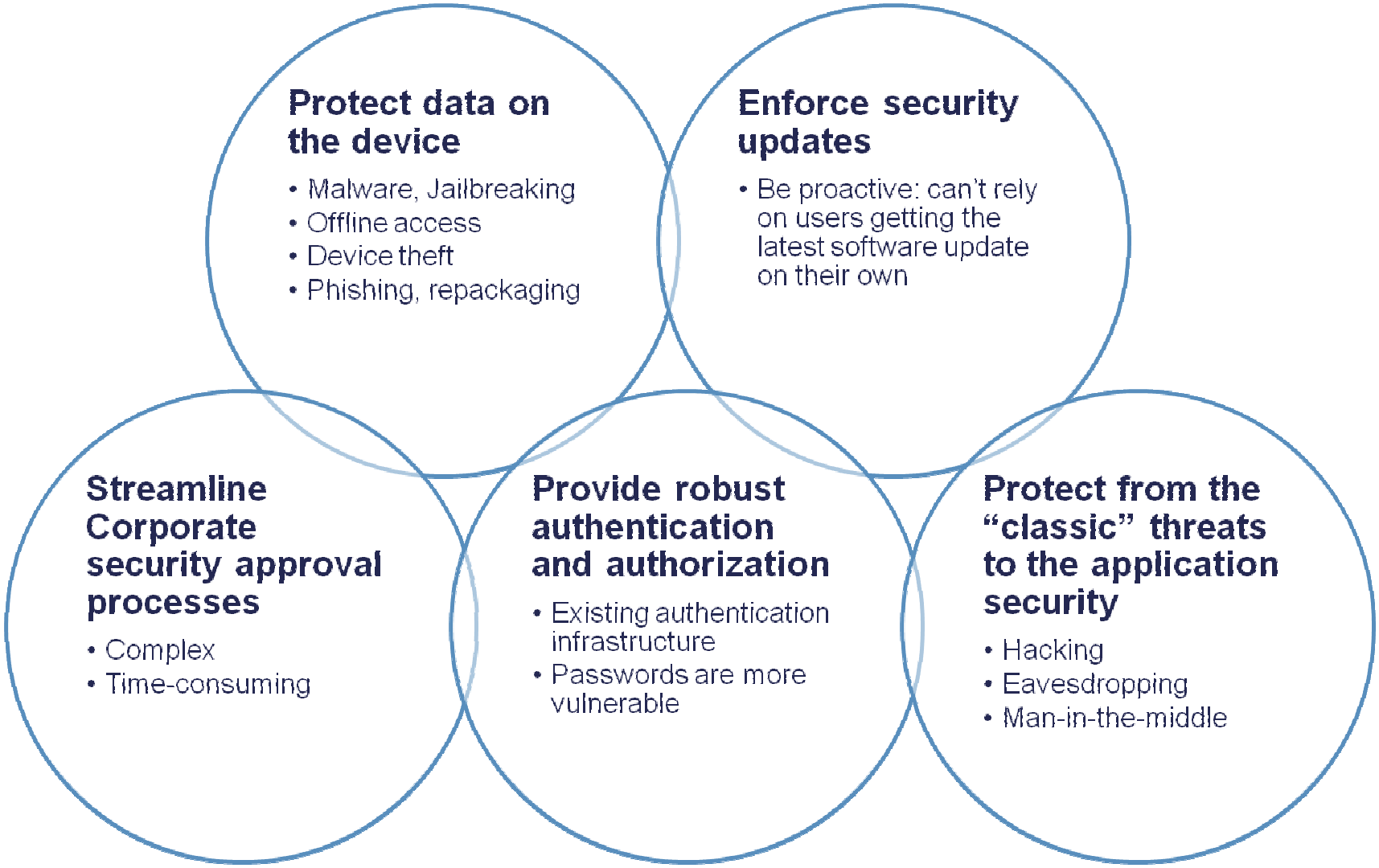


Taking Advantage of Platform Architecture and Mobile Capabilities

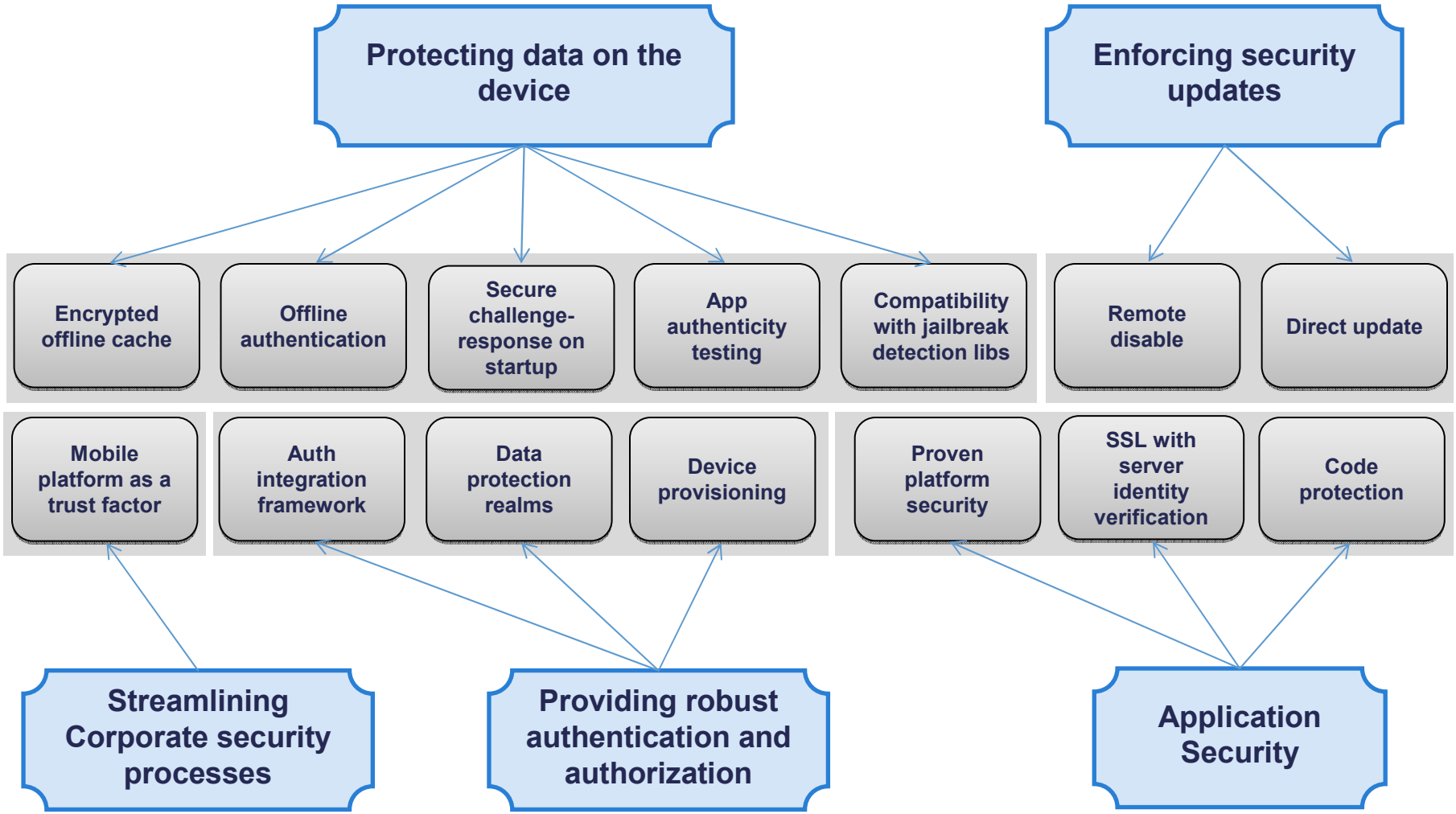
- Platform architecture benefits:
  - Combining server-side and client-side functionality to provide a comprehensive set of security features
  - Opportunity to simplify security approval process

- Mobile capabilities:
  - The device itself can be used as a second factor for user authentication (i.e., “what you have”)
  - Use built-in support for secure communications
  - Leverage security APIs when available (e.g., keychain services API, app signatures)
  - Some app stores provide high confidence in app legitimacy

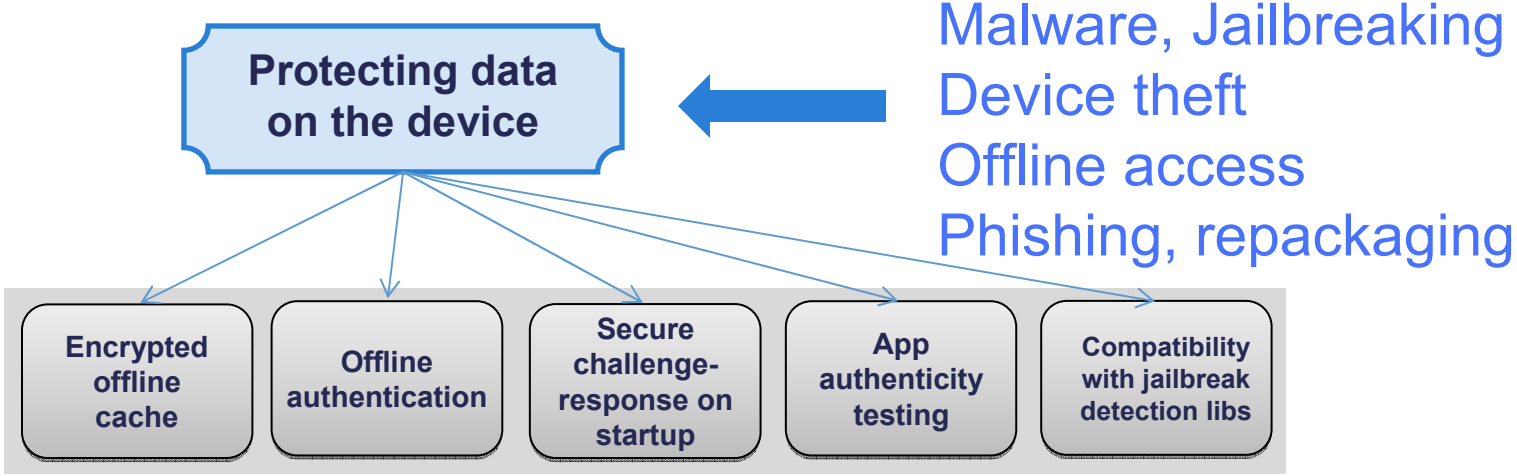
Mobile Application Security Objectives



Security Features Mapping

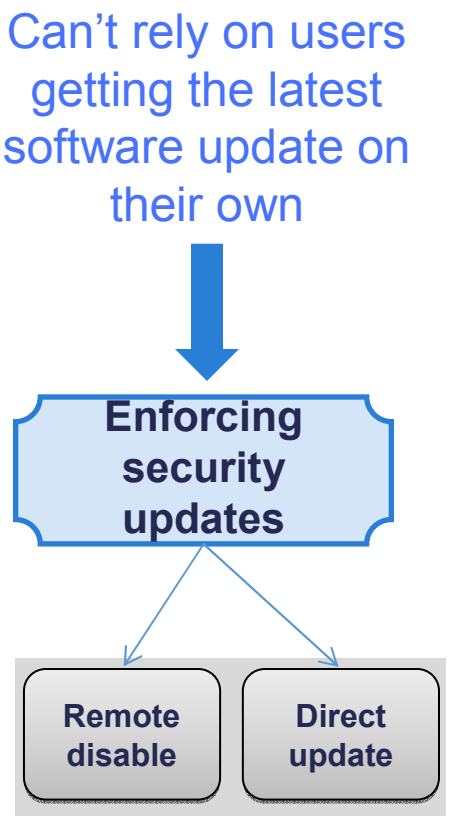


Protecting data on the device



- Encrypted offline cache
- 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

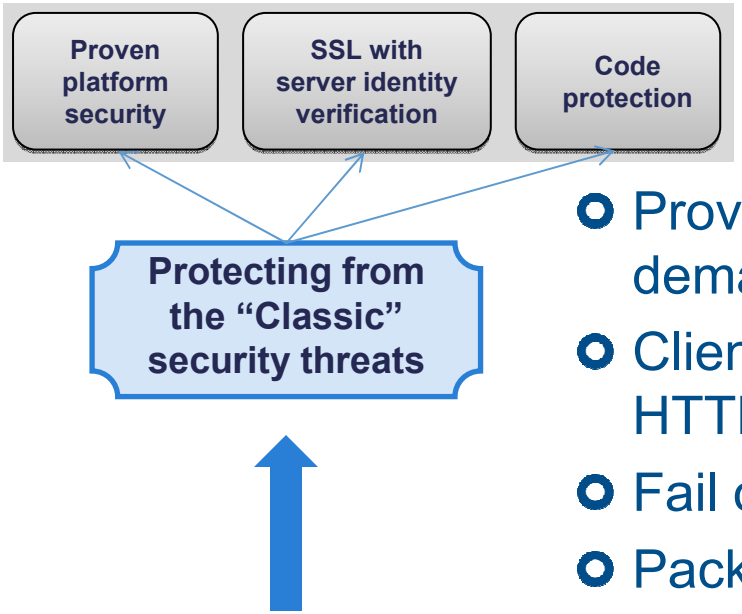
Enforcing security updates



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

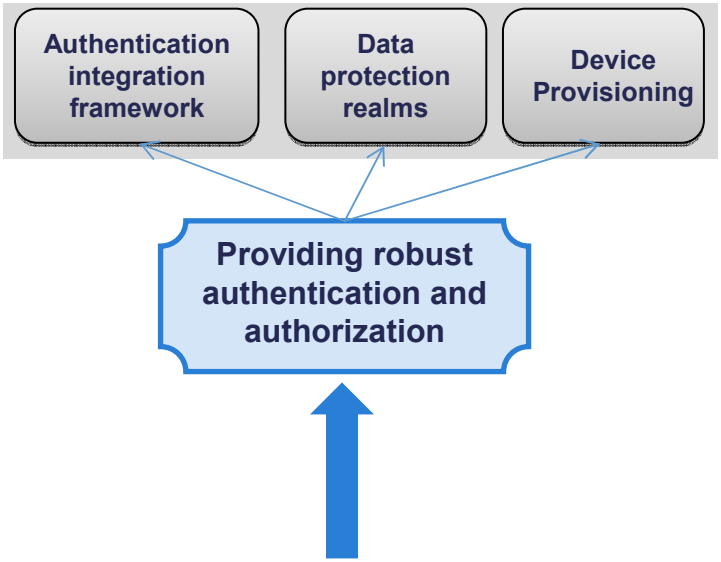
- Direct Update: automatically send new versions of the locally-cached HTML/JS resources to installed apps

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
- Fail on server certificate verification error
- Packaged JS code can be encrypted on desktop to make static analysis more difficult
- JS code integrity verification on startup
- SQL adapter designed to mitigate SQL-injection
- Built-in audit trail

Authentication and Authorization



Need to integrate with existing authentication infrastructure

Authenticate users when offline

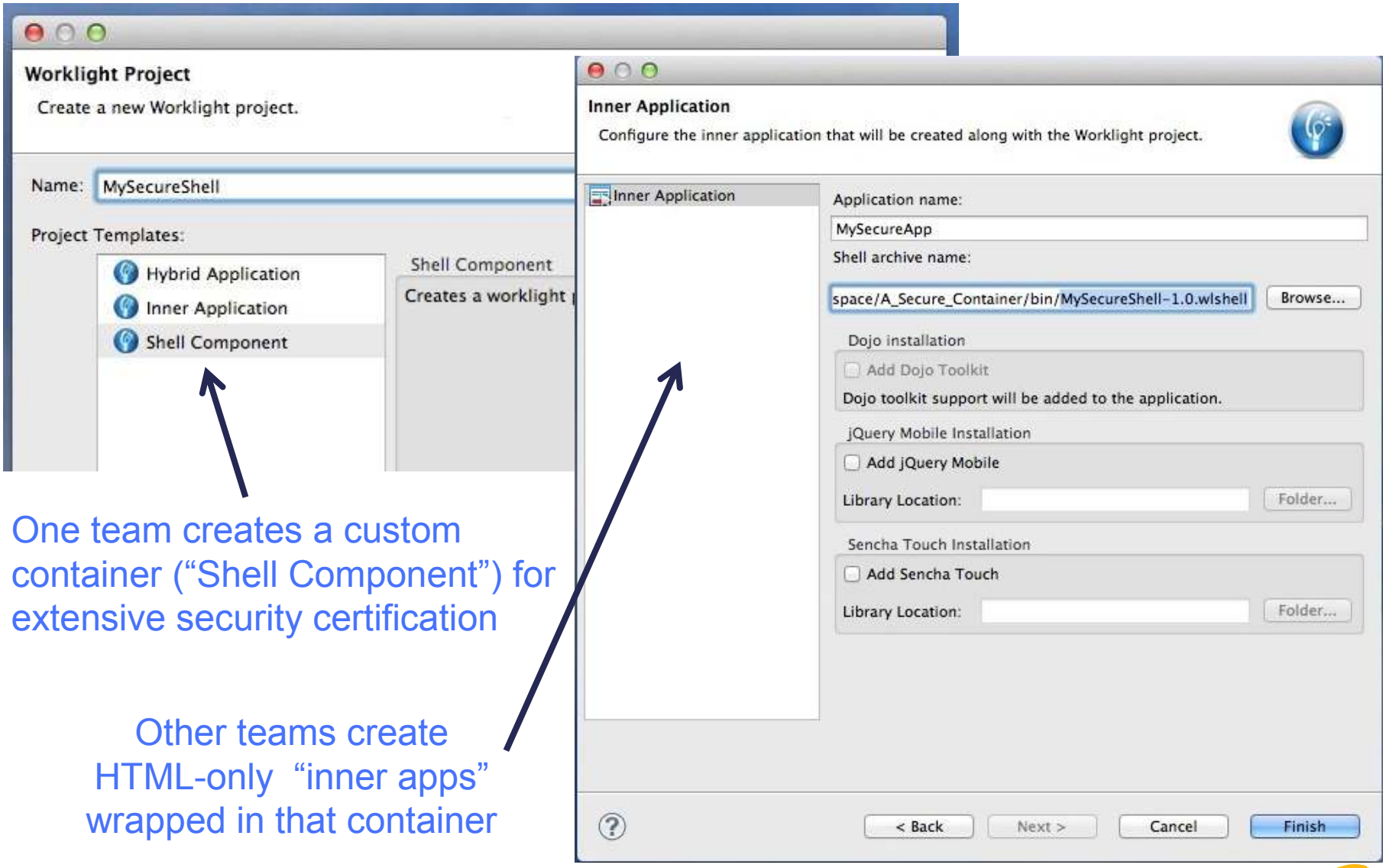
Mobile passwords are more vulnerable (keyboard more difficult to use, typed text is visible)

- Very flexible framework for simplifying integration of apps with enterprise identity & access management solutions
- 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
- Secure device ID generated as part of extensible provisioning process

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.

Worklight Studio simplifies the reuse of custom containers across the organization



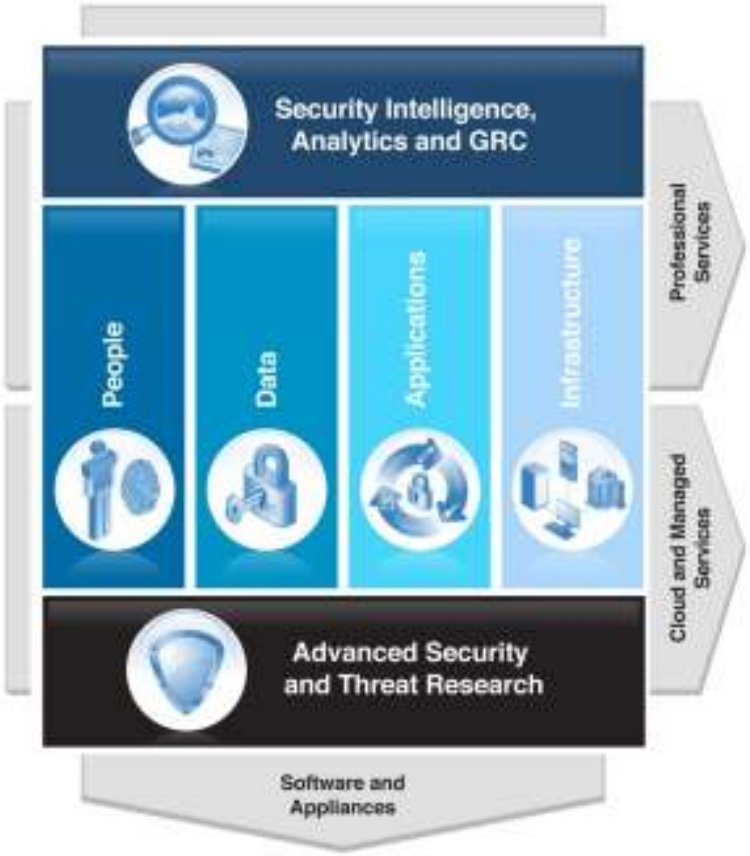
One team creates a custom container ("Shell Component") for extensive security certification

Other teams create HTML-only "inner apps" wrapped in that container

Centralized Build System Provides Control Over Coupling of Shell and Inner App

Mobile Security Enabled with IBM Solutions

IBM brings together a broad portfolio of technologies and services to meet the mobile security needs of customers across multiple industries



IBM Security Framework

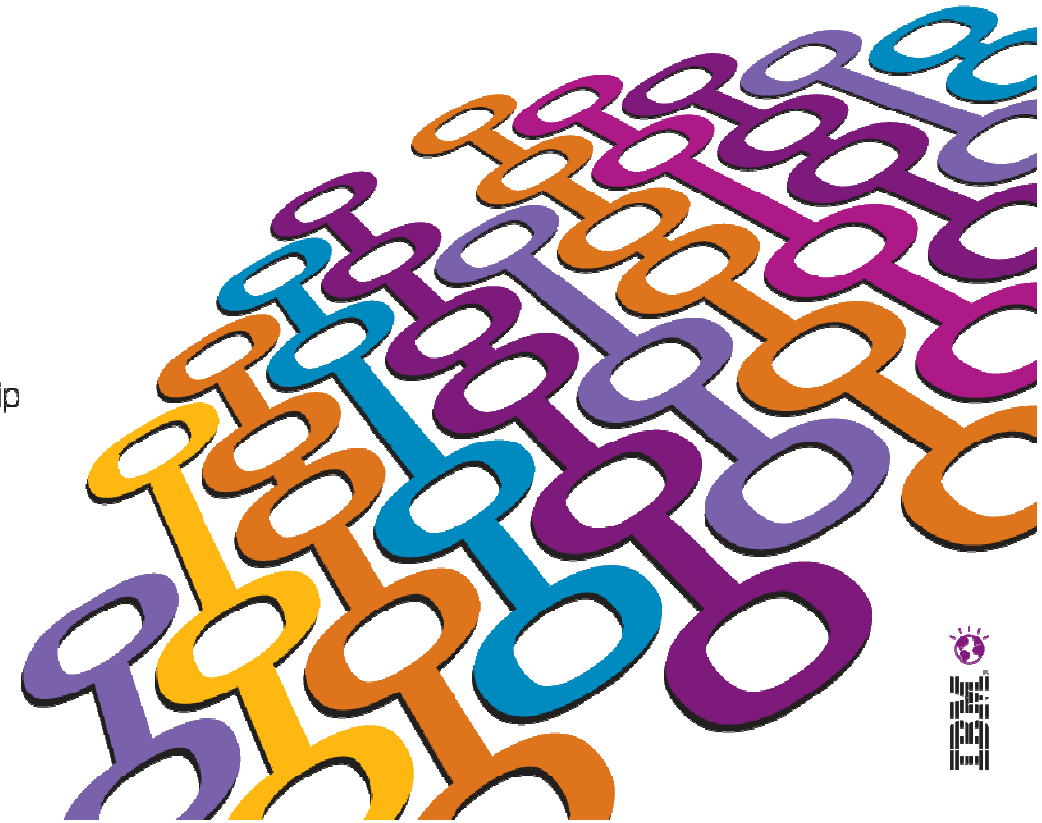
- Application security
  - Worklight
  - IBM Rational AppScan
- Mobile device management
  - IBM Endpoint Manager for Mobile devices
  - IBM Hosted Mobile Device Security Management
- Secure enterprise access
  - IBM Security Access Manager
- Security Intelligence
  - IBM QRadar

Questions?

Impact2012

The Premier Conference for Business and IT Leadership

Innovate. Transform. Grow.



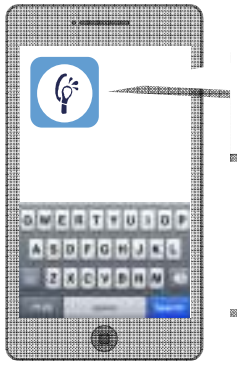
Copyright and Trademarks

Session Authentication Management
Step 1 – Unauthenticated Session

Session:

- Created on first access from client
- Identified using session cookie
- Associated data is stored on the server

Session Authentication Management
Step 2 – Authentication

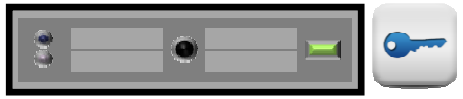


1. Obtain credentials from user and device

2. Forward credentials

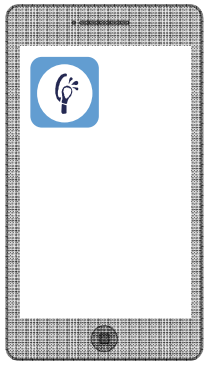
Worklight Server

Process authentication data



3. If necessary:
- Consult with authentication servers
- Perform device provisioning
- Receive authentication token
- Associate token with session

Session Authentication Management
Step 3 – Authenticated Session



1. Procedure call on authenticated session

3. Procedure result

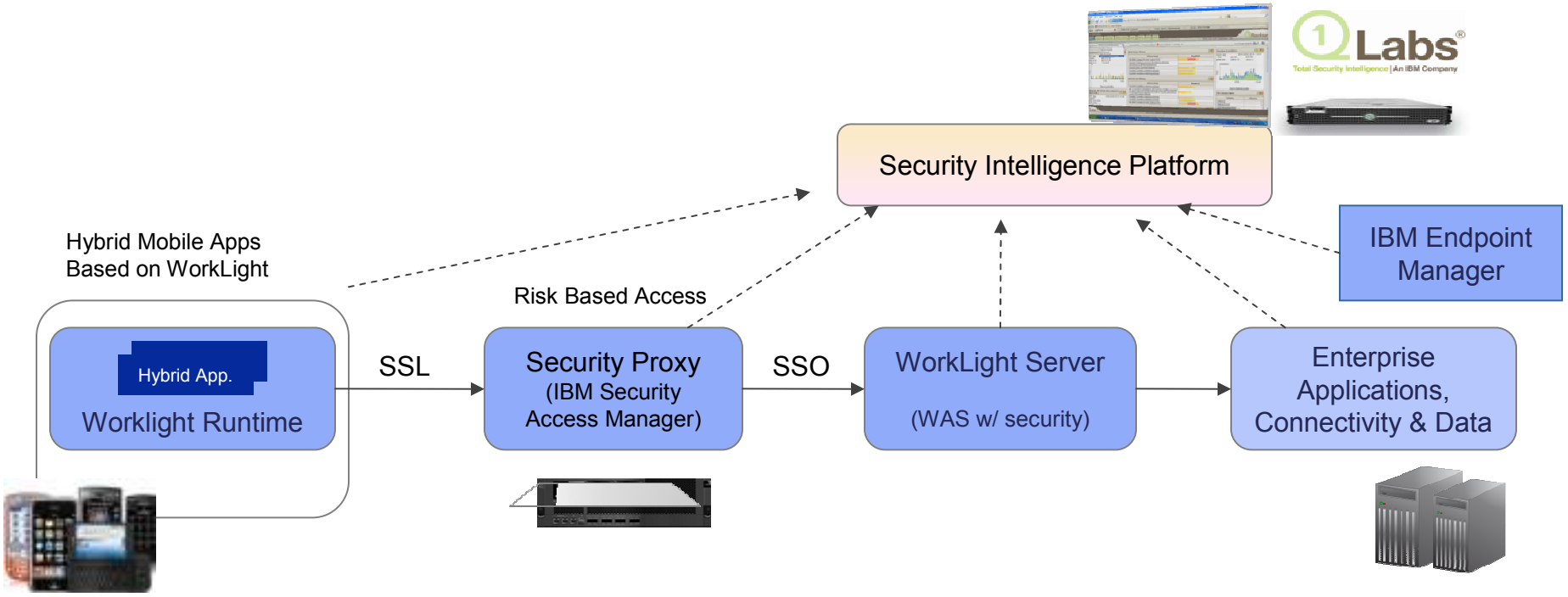
Worklight Server

Authenticated token associated with session

Session ID	Auth Tokens/State
2bd4296a3f29	Realm 1: 25487 Realm 2: ------
25617ff82a90	Realm 1: ------ Realm 2: a6c9a
89a77921b02	Realm 1: 7b8df Realm 2: 6a8a0

2. Access back-end service using authentication token

Deployment for SSO and Security Intelligence



- Security Proxy
  - Risk based access decisions and authentication - Context awareness
  - Single SignOn and Federation – standards based support OAuth, SAML, OpenID
  - Added value through integration of Security proxy with Mobile application platform (Worklight) – offline authentication, secure cache, app authenticity,..
- Security intelligence with mobile context
  - Intelligence around malware and advanced threats in mobile enabled enterprise
  - User identity and device identity correlation, leading to behavior analysis
  - Geo-fencing, anomaly detection based on device, user, location, and application characteristics