Improve your mobile application security with IBM Worklight

Contents

Introduction

Mobile applications are now the preferred interaction model for mobile users who are browsing the Internet or making use of the different capabilities of a mobile device. Mobile applications are available to users predominantly from app stores. These app stores act as online application distribution systems for mobile devices that run on popular mobile operating systems such as iOS and Android. Mobile users increasingly use these applications instead of the in-built web browser on the mobile device to access information, collaborate with other users and perform transactions online. Many organizational leaders realize that a mobile application strategy is critical to the growth of an organization as it evolves into a mobile enterprise to serve the rising demands of its employees, customers and partners.

Adopting new strategic enterprise-wide IT initiatives usually brings with it concerns related to security and risk mitigation. Mobile application security has a unique set of requirements to address new challenges. Key components in the enterprise security infrastructure are designed to secure browsing activity. However, the integration of downloadable applications into the enterprise back end requires more development effort. Mobile applications may be run on devices compromised by malware. The threat of malware necessitates the need for an application to protect its data and to also recognize when the data or the application itself might have been compromised. External attacks by hackers and malware are just a couple of examples but they highlight the special focus on the demands of mobile application security.

IBM offers an extensive portfolio of products to enable mobile security on the mobile device, over the network, in the enterprise and for the mobile application itself. IBM® Worklight™ mobile application platform helps organizations develop, deploy, host and manage mobile enterprise applications. IBM Worklight addresses the requirements for mobile application development and provides tools to help at every stage of the development and deployment process. IBM Worklight helps organizations to integrate security into the overall mobile application lifecycle related to development, delivery and execution. Using IBM Worklight, developers in your organization can help create and deliver security-rich mobile applications to an ever growing number of stakeholders who are using mobile devices such as smartphones and tablets.

IBM Worklight overview

Security is a platform-wide consideration for all components of the IBM Worklight platform. The platform consists of four main components that participate in providing a robust solution for mobile application security.

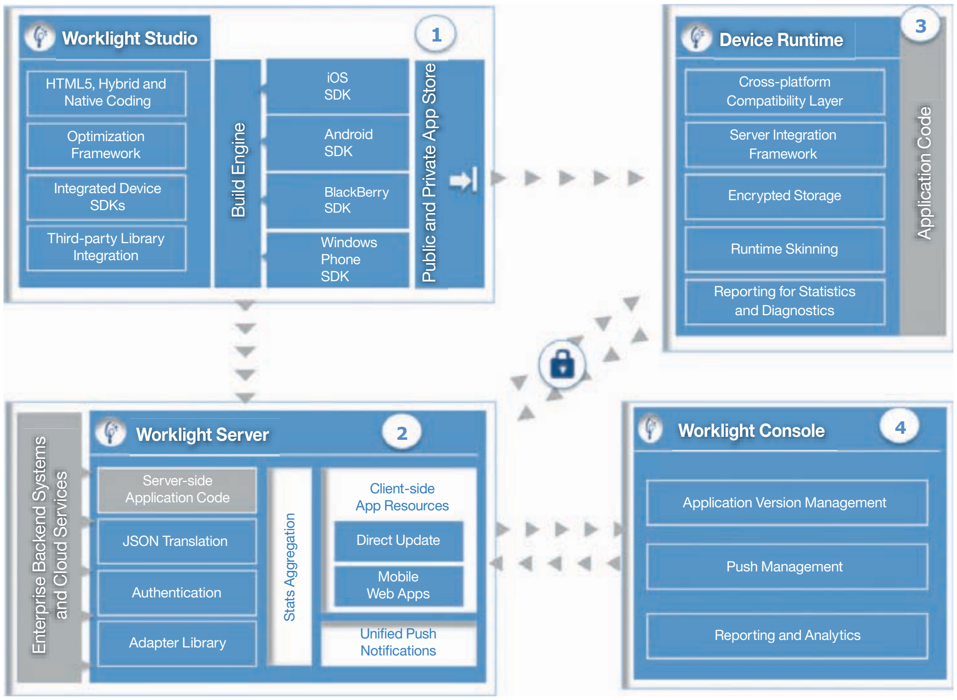

Figure 1: Four main components of the IBM Worklight platform

IBM Worklight Studio is an Eclipse-based integrated development environment (IDE) that enables you to perform the coding and integration required to develop a fully operational application for various mobile operating systems. Eclipse users do not require any additional learning while using Worklight Studio for developing mobile applications because of the assisted code development features. Using the basic tools in Eclipse with the various features provided by the Worklight plug-in helps Worklight Studio streamline the application development and facilitate enterprise connectivity.

IBM Worklight Server is a Java-based server that works as a security-rich and scalable gateway between applications, external services and the enterprise back-end infrastructure. The server facilitates secure connectivity, multi-source data extraction and manipulation, authentication, direct update of web and hybrid applications, analytics and operational management functions.

IBM Worklight Device Runtime Components consist of runtime client application programming interfaces (APIs). These are essential libraries that complement the server by exposing APIs for accessing server functionality, implementing client-side portions of security features, allowing the use of JavaScript and HTML for cross-platform development, facilitating interaction between JavaScript and native code and more.

IBM Worklight Console is a web-based administrative console that supports the ongoing monitoring and administration of the Worklight Server and its deployed applications, adapters and push notifications. The Worklight Console helps you to control and manage the access of deployed applications to the enterprise network based on configurable preset rules of the application version and device type. The console also helps you customize the accompanying messages the user receives.

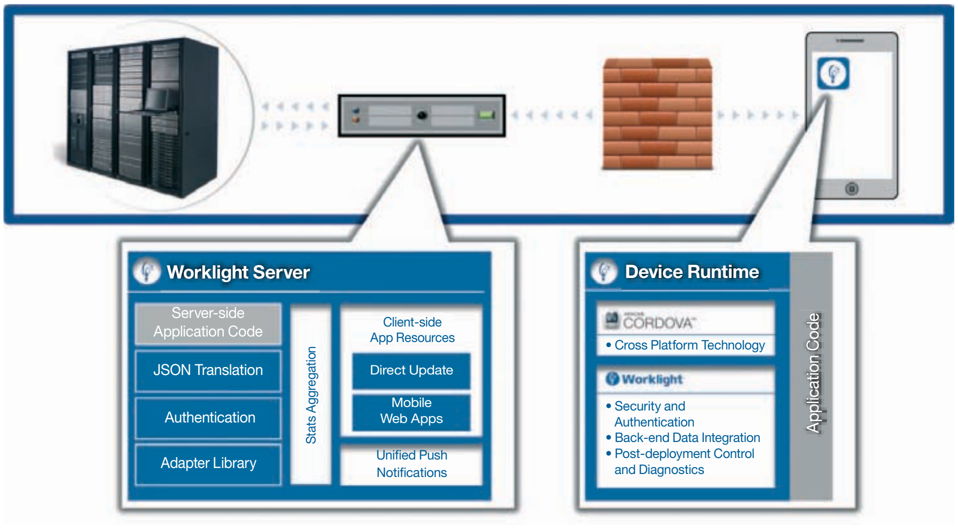
Worklight Server
Server-side Application Code
JSON Translation
Authentication
Adapter Library
Stats Aggregation
Client-side App Resources
Direct Update
Mobile Web Apps
Unified Push Notifications
Device Runtime
CORDOVA
• Cross Platform Technology
Worklight
• Security and Authentication
• Back-end Data Integration
• Post-deployment Control and Diagnostics
Application Code

Figure 2: Typical setup of the IBM Worklight platform

In a typical IBM Worklight platform setup, the Worklight Server is installed behind a firewall or a reverse proxy and the mobile applications are installed and run on mobile devices that reside outside the enterprise network at least part of the time. The Worklight Server acts as a gateway that mediates the communication and access of mobile applications to back-end systems that are located in the enterprise network.

Enabling mobile security with IBM Worklight

On-device data protection

It is common for a mobile application in an enterprise context to provide the user with access to sensitive data. Once the application obtains the data from the back-end systems, the data is stored by the application on the mobile device—subjecting it to two primary risks related to malware or if your device is lost or stolen. Malware on your device can potentially steal the existing data or tamper with it. This scenario is common especially on devices that have been "jailbroken" or rooted by the user intending to run software not authorized by the device manufacturer. On the other hand the mobile device can get lost or be stolen and consequently get subjected to examination and data extraction by malicious third parties.

In addition, the mobile context often requires that the data retrieved from back-end systems be stored on the device to ensure offline availability. This presents the application developer with the task of ensuring that the data is protected from unauthorized access and is available only to legitimate users.

Another risk to consider when allowing mobile applications to access sensitive data is the growing industry of hackers and application "trojanization" operations. The most common distribution channel for mobile applications is the app store. The companies operating the app stores have mechanisms to identify malicious software and prevent such applications from reaching mobile users. However, hackers have developed ways of working around these mechanisms and in many situations they are able to get their malicious code onto the devices of unsuspecting users.

IBM Worklight provides several features and capabilities that help address these risks such as:

Encrypted on-device storage

Developers can use IBM Worklight to encrypt any sensitive data that is stored locally for offline availability, helping to protect the device from malware attacks and theft. The platform uses advanced encryption standards (AES) and public-key cryptography standards (PCKS) such as AES256 and PCKS #5-generated encryption keys that are used in the process of storing application generated data locally on the mobile device. The encrypted cache API requires a password provided by the user to gain access to the cache. Once the cache has been successfully opened the application can insert and retrieve data which is stored on the device in an encrypted format.

Offline authentication

When an application is running on a mobile device that is connected to the network, user authentication usually involves the processing of credentials by the enterprise authentication infrastructure. However, when the mobile device does not have connectivity, the enterprise authentication infrastructure cannot be reached by the application and there is still a need to verify user credentials. In scenarios such as these, IBM Worklight has an encrypted cache that can be utilized by mobile applications to authenticate users. Because the offline cache can only be unlocked using the correct password, mobile applications can use the encrypted cache mechanism to help achieve more secure offline authentication.

Authenticity testing

In most situations, downloadable mobile applications run outside the company firewall. Allowing such applications to access company data and even perform transactions requires the opening of a channel to the outside world. This channel can be exploited by attackers in various ways including the distribution of modified or re-engineered versions of the original application developed by the company. In fact, hackers are making use of practices that involve obtaining legitimate applications, "unpackaging" and then "repackaging" them with malicious code and distributing them in the pretense of being the original legitimate application. Sometimes hackers can also set up fake app stores to host these tampered applications, directing unsuspecting users to these stores using mobile advertising messages. This malicious technique is used by attackers to distribute tampered copies of the original application and presents a significant risk to enterprise data and the company brand.

IBM Worklight includes mechanisms that help prevent the mass distribution of tampered copies of the original application. The server tests the authenticity of applications that contact it and differentiates between connections that are created by the legitimate mobile application and connection attempts made by the tampered or re-engineered application. When the server identifies that it is being accessed by a non-original application, the server can deny access to enterprise data. This mechanism significantly increases the effort required by hackers to exploit the mobile channel for malicious purposes.

Differentiating between approved and unrecognized mobile devices

IBM Worklight applications can generate a unique device ID on iOS and Android devices and can store this ID on the device in a security-rich manner. Organizations can integrate the applications with a custom provisioning process ensuring that an application or a group of applications can only be installed on sanctioned devices. This feature helps organizational leaders support the bring your own device (BYOD) trend allowing employees to use personal devices for work purposes and at the same time maintain control and enforce security protocols on those devices. This also helps your IT staff ensure that applications with access to sensitive data are not run on unauthorized devices.

Security updates enforcement

In the context of web applications client-side code is under the direct control of the IT administrator. Distribution of code updates is such a fundamental mechanism of web technology that it has become a standard within that context. Downloadable mobile applications present a different scenario because mobile operating systems do not force users to update applications to their latest version. If a security flaw is discovered in a deployed mobile application, the author of the application can upload a fixed version to the app store. However, users are free to choose whether or not to download the updated version. Unfortunately, the mobile app store distribution mechanisms and contractual restrictions placed by some mobile operating system vendors make it very difficult for administrators to make sure their users are using the correct version. IBM Worklight provides two features that can help administrators regain control—because administrators cannot leave the installation of updated application versions with critical security fixes in the hands of mobile users.

Direct update

Using the direct update feature enables developers to drive updates of the web content of their deployed HTML5 and hybrid applications directly from the Worklight Server upon application launch. This mechanism helps developers ensure that critical updates to JavaScript code reach the user in a timely manner silently or by user confirmation, while maintaining compliance with mobile OS terms of service.

Remote disable

IBM Worklight also provides administrators with the ability to disable the old version of the application for situations in which the distribution of a security fix requires that users get the new application version from the app store. The Worklight Server can be configured to restrict the access of certain applications based on their version and the device type on which they are installed.

Dealing with classic application security threats

Apart from the variety of new threats that keep emerging, mobile application developers are still required to address the wide scope of traditional security pitfalls, such as standard hacking, eavesdropping and "man-in-the-middle" (MITM) attacks.

Proven platform security

IBM Worklight has security mechanisms that have been deployed by enterprises with extreme security requirements such as top-tier financial institutions. Running IBM Worklight on the IBM WebSphere® Application Server further strengthens its security features with those provided by the WebSphere Application Server.

SSL with server identity security

IBM Worklight enables a security-rich client and server communication over HTTPS to prevent data leakage and to prevent automatic server certificate verification to thwart known attacks such as man-in-the-middle attack.

Additional measures

IBM Worklight also provides additional measures of security that include encryption of JavaScript resources prior to app store distribution, client-side integrity testing of application resources and much more.

Streamlining the corporate security-approval process

IBM Worklight has been designed to integrate with existing security protocols and to streamline and augment the existing security-approval process. This helps companies ensure that applications built using IBM Worklight are trusted entities that adhere to corporate security policies. The result is a quicker approval process, faster time to market and increased confidence that risks are being mitigated. IBM Worklight has a customizable and open approach helping you vet and pre-approve the application and identify specific security concerns that can be addressed within the platform framework.

Integrating IBM Worklight with enterprise security

IBM Worklight integrates with the existing security infrastructure of an enterprise in a number of ways. All of the integration with various enterprise security components are made possible by using the powerful framework provided by IBM Worklight. This framework is part of the core IBM Worklight runtime used for handling authentication and data protection.

Typical enterprise security requirements include integrating with traditional Lightweight Directory Access Protocol (LDAP) servers for user authentication, working behind application firewalls and reverse proxies and integrating with security gateways that protect backend resources.

Powerful framework for custom integration

Many companies have developed identity management and authentication infrastructures that are more complex than the simple situation of having a single reverse proxy take care of authentication. The integration of mobile applications with such infrastructures is not a trivial task. There are a few scenarios such as:

- Common enterprise authentication protocols are not always provided by the mobile operating system.
- Enterprise authentication infrastructure may require non-trivial management of tokens or credentials.
- Client application logic can become overly complex due to re-authentication of users outside the normal functional flow if and when sessions expire.
- Advanced authentication mechanisms such as two-factor authentication may be required due to the weak nature of passwords on mobile devices.

Authentication integration framework

The Worklight server-side architecture has been designed to simplify the task of connecting mobile applications with the enterprise back-end authentication infrastructure. The IBM Worklight framework provides both server-side and client-side mechanisms for assisting with this issue. Server modules define the collection and handling of credentials (authenticator) and mechanisms to validate or verify the credentials (login module). On the client side, IBM Worklight supports an authentication framework for asynchronous login requests on session expiration.

In addition, IBM Worklight also supports a number of commonly used mechanisms for authentication such as forms based, cookie based or header based and others. For IBM Worklight runtime on WebSphere Application Server, there is full support for all authentication mechanisms that are supported by the WebSphere Application Server such as LDAP directory and custom user registry. IBM Worklight provides authentication extension or customization either leveraging the platform's adapters such as configurable server-side XML files responsible for channeling back-end enterprise systems to the end-user, coded using JavaScript. IBM Worklight also provides authentication extension or customization through direct coding of authenticator and login module using Java.

Data protection realms

IBM Worklight makes it possible to achieve advanced integration of a single mobile application with multiple back-end authentication frameworks and providing granular control over the level of authentication required to reach different types of resources. Resources are protected by authentication realms. An authentication realm defines the process to be used to authenticate users and consists of a mechanism to collect the user credentials and verifying the user credentials either against a database or LDAP directory. When a user attempts to access a protected resource, IBM Worklight checks whether the user is already authenticated according to the process defined for the resource's realm. If the user has not yet been authenticated, IBM Worklight triggers the process of obtaining the client credentials and verifying them, as defined in the realm.

IBM Worklight differentiates between realms that are used for personalization such as user preferences and those that are used for authentication. Data protection realms are of two different kinds such as:

- Environment realms. Realms used for personalization are called environment realms. In such realms a user can be identified by a persistent cookie or by user identity in the hosting environment for example an iGoogle home page or a Facebook account.
- Resource realms. Realms used for authentication are called resource realms. Such realms will typically use mechanisms such as form-based authentication or single sign-on (SSO) to collect user credentials and an authorization service to validate them.

The definition of these realms is done using a server-side configuration XML file.

Directory server integration

IBM Worklight, when hosted on WebSphere Application Server and the WebSphere Liberty profile can leverage the functionality provided by the underlying JEE runtime to support LDAP directory servers. WebSphere Application Server provides implementations that support multiple types of registries and repositories including the local operating system registry, a stand-alone LDAP registry, a stand-alone custom registry and federated repositories. Hence users can authenticate to IBM Worklight applications using their enterprise logon typically governed by LDAP directory servers.

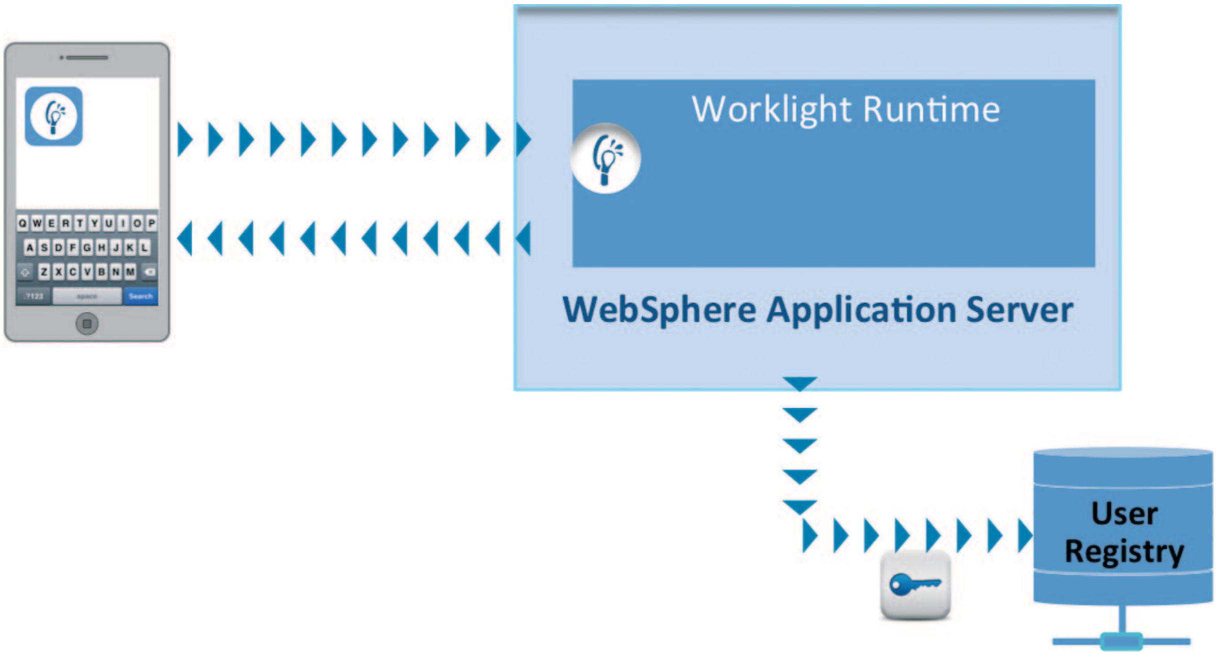

Figure 3: IBM Worklight runtime hosted on IBM WebSphere Application Server

Integrating with reverse proxy and security gateway

Enterprises use reverse proxy and security gateways in their perimeter network to protect web resources. There are several products in the market that function as a reverse proxy and security gateways providing a termination point for HTTPS and user authentication. IBM Worklight can be configured to work with these types of security components using its flexible authentication integration framework. IBM Security Access Manager for Enterprise Single Sign-On, IBM DataPower®, CA Siteminder—can be configured as reverse proxy and a security gateway.

The most common configuration for integrating with these security gateways includes leveraging the header-based authentication mechanism in IBM Worklight by using the header authenticator and login module that is provided with the base product. For example, the Siteminder Reverse Proxy might forward a header with user identity upon successful authentication of the user to IBM Worklight, which can be configured to trust that header and authenticate the session based on the user identity in the header. With IBM Security Asset Manager and DataPower, there are additional mechanisms.

IBM Security Access Manager and DataPower as reverse proxies can terminate the authentication of the user and forward trusted credential in the HTTP header or a cookie. IBM Worklight can verify the credential from the HTTP header or the cookie and can establish the user session based on that. There are two mechanisms for authentication trust between IBM Security Access Manager and IBM Worklight:

- Header based. IBM Worklight can be configured with header based authenticator and login module to set the user identity based on the value from a custom header. The custom header is set and forwarded by IBM Security Access Manager or DataPower. The header-based authenticator in IBM Worklight consumes this header and the header-based login module establishes the user session based on the value in this header.
- Lightweight Third-Party Authentication (LTPA) based. IBM Worklight on WebSphere Application Server and WebSphere Application Server Liberty Profile can be configured with LTPA realm to set the user based on the LTPA token set and it can be forwarded by DataPower and IBM Security Access Manager. With trust being established between the WebSphere runtime and IBM Security Access Manager/DataPower, the LTPA realm in configuration in IBM Worklight will consume the LTPA token sent as a cookie and it will establish the user session from the LTPA token.

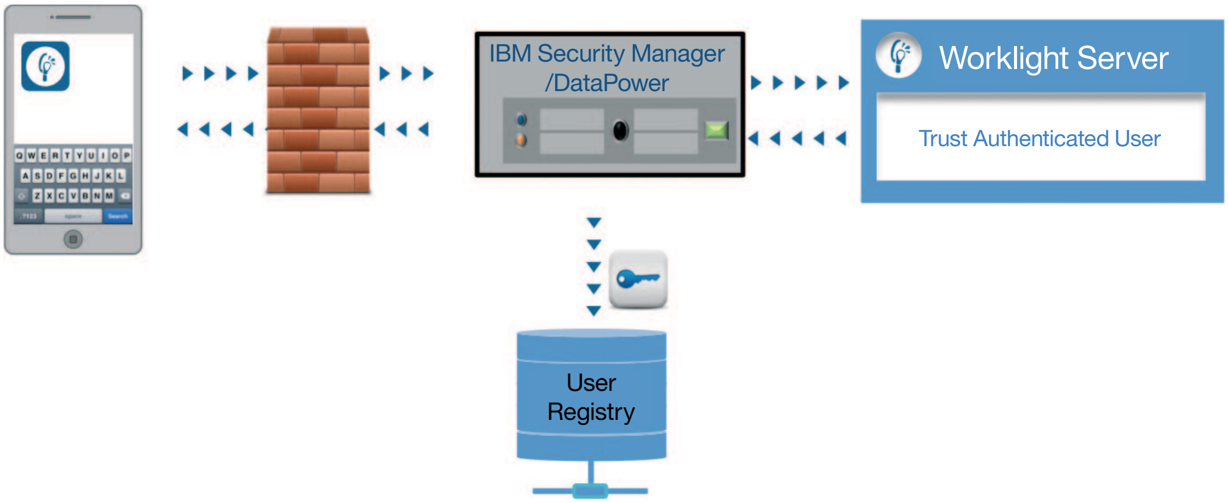

Figure 4: IBM Worklight runtime protected behind a reverse proxy

IBM Worklight is part of the IBM Mobile Foundation family of products, an offering designed to bring together key mobile capabilities that organizations require into a single integrated package that helps customers address the full array of challenges and opportunities that the mobile channel represents. IBM Mobile Foundation delivers a range of application development, connectivity and management capabilities that support a wide variety of mobile devices and mobile application types.

The IBM Mobile Foundation family of products includes the following offerings:

- IBM Worklight to help you build, connect, run and manage cross-platform mobile applications
- IBM WebSphere Cast Iron® Hypervisor Enterprise Edition to help you connect mobile applications to a variety of cloud and back-end systems
- IBM Endpoint Manager for Mobile Devices platform to help you control and manage users' mobile devices

To download and install the IBM Worklight Developer Edition at no charge, visit: **ibm.com**/developerworks/mobile/worklight.html

Notes

For more information

To learn more about IBM Worklight, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/software/mobile-solutions/worklight

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2012

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle