IBM Security AppScan Source

Secure traditional and mobile applications and build secure software with static application security testing

Highlights

- Identify vulnerabilities in your source code, review data and call flows, and identify the threat exposure of each of your applications
- Isolate mobile-specific application security risks
- Scan source code early in the development cycle to simplify the adoption of security testing by development
- Integrate security testing with application development tools and the IBM® Rational® Collaborative Lifecycle Management solution
- Create, push and enforce consistent policies that can be used throughout your organization

Today's economy depends upon interconnected, intelligent systems with custom software and web applications. And now interconnected software also extends to mobile devices. These products and applications generate or interact with vast amounts of data. Eager to take advantage of opportunities in the marketplace, organizations are developing these smarter products and applications at an increasingly rapid rate. But in the race to stay ahead, many organizations fail to give application security the attention and priority it requires.

Unfortunately, the headlines have made one thing clear: if you don't take the appropriate measures to protect your organization's systems, applications, private data and customer information, the consequences for your bottom line and your brand can be devastating. They range from heavy financial penalties and lost revenue to system outages that erode customer confidence and damage your organization's reputation. Can your organization weather that kind of storm? Not many can. That's why it is essential to have a comprehensive application security strategy in place.

Identifying vulnerabilities in your source code

The IBM Security AppScan® portfolio of application security testing and risk management solutions is designed to address this wide range of application risks. As a key component of the portfolio, IBM Security AppScan Source is a static application security testing solution that helps you identify vulnerabilities in your source code, review data and call flows, and identify the threat exposure of each of your applications.

Deployed throughout the software development lifecycle, IBM Security AppScan Source makes it easier for you to understand your threat exposure for audit and compliance purposes. It also helps facilitate a partnership between development and security teams by providing both groups with the information they need, when they need it.

Reducing vulnerabilities early in the development lifecycle

IBM Security AppScan Source software provides a comprehensive approach to source-code analysis. It is designed to deliver fast scans of more than one million lines of code in an hour, enabling you to scan complex enterprise applications. It also provides actionable, prioritized information—down to the line of vulnerable code. This helps you find and address vulnerable code early in the development cycle, review applications that are already in use and perform security and quality checks on applications or components that you have outsourced for development. For example, you can build security requirements into your outsourcing contracts and use IBM Security AppScan Source to help ensure that your acceptance criteria have been met.

Right out of the box, IBM Security AppScan Source provides report cards, detailed metrics and the remediation advice you need to find and eliminate the vulnerabilities in your applications. However, merely identifying buffer overflows or Structured Query Language (SQL) injections does not secure an application. Improper implementation of other security mechanisms, including access controls, authentication and encryption, can pose an even greater risk to your organization.

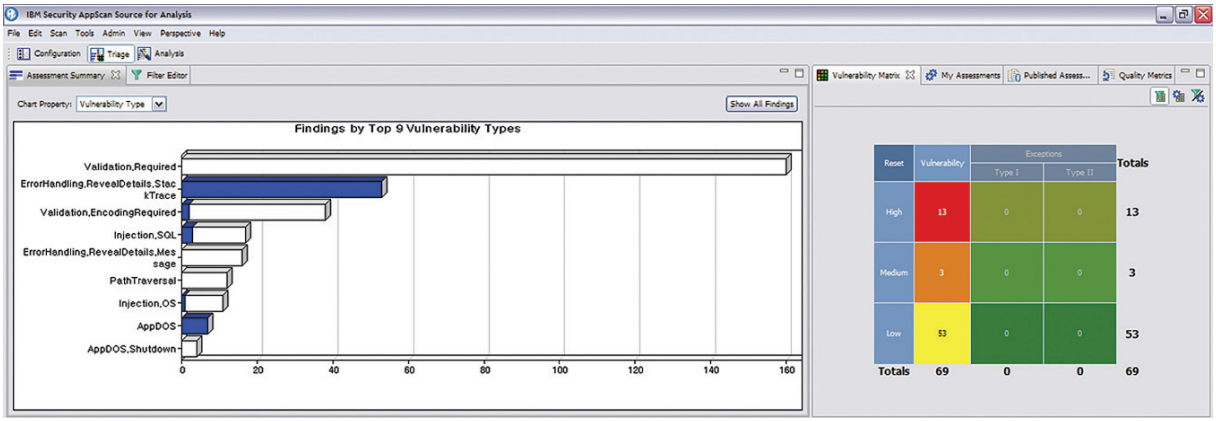

Figure 1. IBM Security AppScan Source software provides assessment summaries that map to application risk and provide insight into the vulnerabilities affecting your applications.

IBM Security AppScan Source enables you to take action on your most critical vulnerabilities by integrating with the Rational Collaborative Lifecycle Management solution to:

- *Collaborate* among and between business, development and test teams with dynamic process- and activity-based workflows for test planning and execution
- *Automate* labor-intensive security testing and audits to catch security issues early, reduce time to market, cut project costs and mitigate business risk
- *Empower* non-security experts, such as developers and quality professionals, to execute security tests, identify vulnerabilities and remediate their code
- *Report* prioritized metrics tailored for individuals and teams, facilitating greater visibility and enabling decision makers to act with confidence and document compliance
- *Deliver* greater predictability by mapping successful deployment patterns to operational key performance indicators (KPIs)

Improving efficiency using automated security testing

Manually testing your software applications can result in late releases or inconsistent test results. An automated solution can help your team test software more thoroughly and quickly, while freeing your testers for more value-generating tasks. Plus, IBM Security AppScan Source prioritizes the results you need to eliminate the coding errors and design flaws that put your data at risk. The application is easy to install and configure, so you can implement it quickly and begin to automate your workflows with minimal disruption to your existing processes.

IBM Security AppScan Source makes it easy to find and prioritize vulnerabilities. Specialized features such as the Application Discovery Assistant automate time-consuming configuration steps while providing more accurate and complete dependency analyses. Security experts can spend their time focusing on securing applications—not configuring them. Flexible and customizable scan configurations help to speed analysis time while allowing organizations to focus on what is most important to them.

Facilitating consistency with centralized policies, processes and reporting

IBM Security AppScan Source helps you set, push and enforce consistent policies that can be used throughout your organization. Security analysts use IBM Security AppScan Source for Analysis to manage all static testing, execute advanced source-code scans and build the globally shared test policies that can be executed either in build systems or by developers in their integrated development environment (IDE). IBM Security AppScan Source for Automation software works with a wide range of build applications, including IBM Rational Build Forge® software, CruiseControl, Apache Continuum, Maven, Jenkins, and Microsoft MSBuild software, to automatically trigger source-code scans as new code is checked into the build system.

Developers can use IBM Security AppScan Source to scan their code, remediate vulnerabilities and resolve assigned work items in their IDE. For developers to scan their own code, IBM offers IBM Security AppScan Source for Development software as an IDE module or plug-in. For developers who just want to analyze results from scans executed in the build system and work on issues assigned by security analysts, IBM Security AppScan Source for Remediation software delivers the IDE module without the scanning capability. Both IDE options offer robust support for resolving vulnerabilities with detailed explanations of the defect and recommended code corrections.

All test results are centrally managed with IBM Security AppScan Enterprise Server. The server provides the centralized platform for application security testing and risk management. IBM Security AppScan Enterprise Server:

- Aggregates both dynamic and static tests
- Correlates results for hybrid analysis
- Provides executive-level dashboards with KPIs
- Integrates with the Rational Collaborative Lifecycle Management suite
- Includes more than 40 out-of-the-box compliance reports for regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), EU Data Protection Directive, Security Control Standard (ISO 27001) and more
- Provides available integration with IBM Security Network Intrusion Prevention System, IBM Security SiteProtector™ and IBM Security Server Protection solution to block attacks that target vulnerabilities identified by IBM Security AppScan software
- Provides available integration with IBM Security QRadar® solutions to incorporate application vulnerabilities as part of overall security intelligence monitoring and reporting

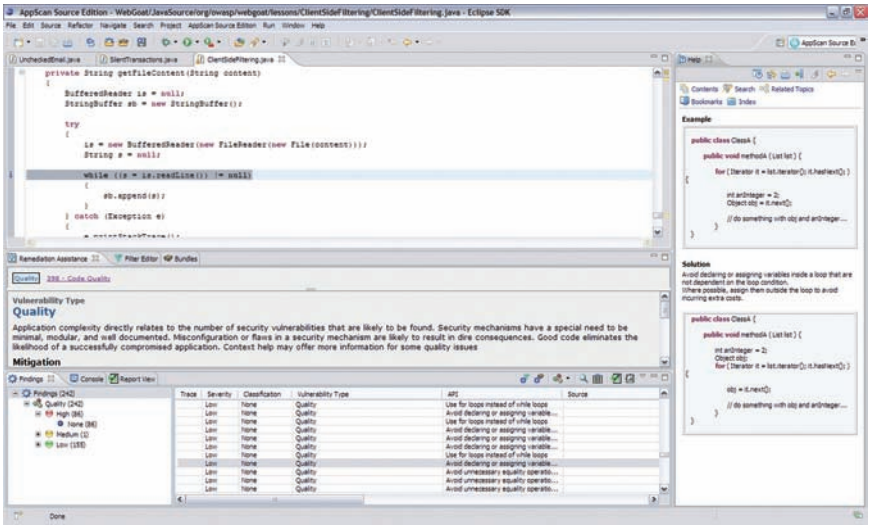

Figure 2. IBM Security AppScan Source software includes options to scan from the IDE or simply access results from the IDE with details about the defect, explanation of the risk and guidance on how to correct the defect.

Providing comprehensive and scalable testing capabilities

IBM Security AppScan Source is based on a patented design that enables it to accommodate a comprehensive portfolio of the largest and most complex applications for a wide range of languages. Plus, it identifies a broad range of security vulnerabilities, pinpointing the coding flaws and design errors that put data and operations at risk. Its in-depth analysis is able to isolate confirmed vulnerabilities to immediately target the most critical security flaws. Of course, in order to identify security flaws, the analysis software must be able to test against a range of languages and application frameworks. The IBM Security AppScan Source software's unique, extensible web application framework provides greater visibility into data-flow analysis for both commercial, open-source and in-house, custom-developed web application frameworks.

Customizing analysis, reporting and workflows

With IBM Security AppScan Source, you can customize the analysis to fit your policies and critical security concerns. There is flexibility to adjust the severity of existing vulnerabilities and adjust the priority of those most critical to you. IBM Security AppScan Source provides customizable reporting that enables you to decide how the information is selected, grouped and represented for remediation, compliance and risk-management reporting. The software also delivers flexible triage and remediation configurations so you can automate the flow of information between security and development teams using the workflow that best suits your organization.

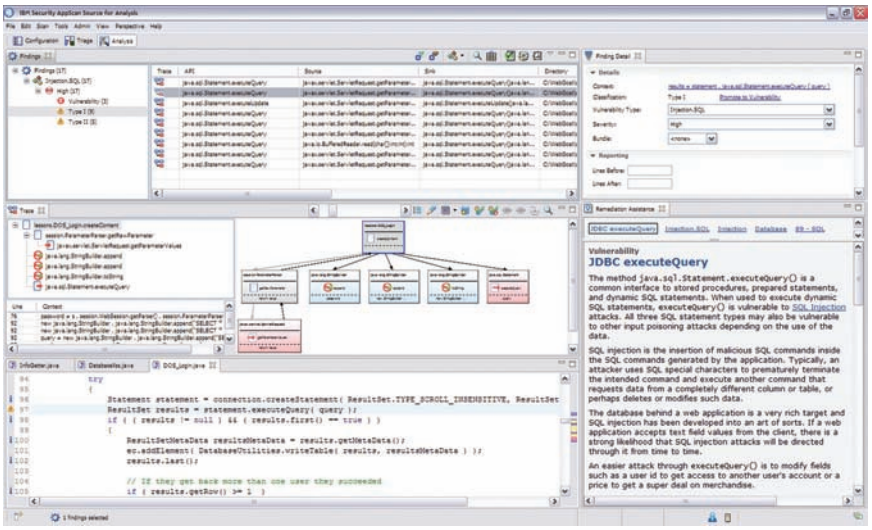

Figure 3. IBM Security AppScan Source provides remediation assistance for every vulnerability, including isolating the line of code corresponding to the security risk.

IBM Security AppScan Source integrates with defect tracking systems (DTS) with a framework that helps you dispatch IBM Security AppScan Source software issues in conjunction with your existing processes using your current priority and severity nomenclature and your existing workflows.

Securing mobile applications

Organizations are under siege to provide mobile applications. Requirements are being driven by both internal and external audiences, and scores of bring-your-own-device users are pressuring IT organizations to open up internal applications to mobile devices. Line-of-business groups are driving new mobile application requirements for customers. However, the security risk and exposure from mobile applications is unmanageable without an automated solution.

While IBM Security AppScan Source has always been able to protect the server-based components of mobile applications, it now provides support for native code written for Android and Apple iOS applications. By leveraging extensive Android and iOS software developers' kits (SDKs) and security research, common mobile security risks such as data leakage can now be detected and corrected—so organizations can proactively address Android and Apple iOS security risks on mobile devices.

- *Security analysis of native Android and Apple iOS mobile applications:* Enables organizations to build secure enterprise mobile applications, regardless of technology choice, for employees and partners
- *Complete Language Support for Objective-C, JavaScript and Java:* Includes the ability to do call and data-flow analysis that will generate trace information to help isolate mobile specific security risks
- *Xcode IDE (Integrated Development Environment) interoperability:* Facilitates integration into the Apple iOS mobile development workflow
- *Android and Apple iOS APIs analysis:* Researches and characterizes approximately 40,000 Android and Apple iOS SDK APIs to determine mobile security risk

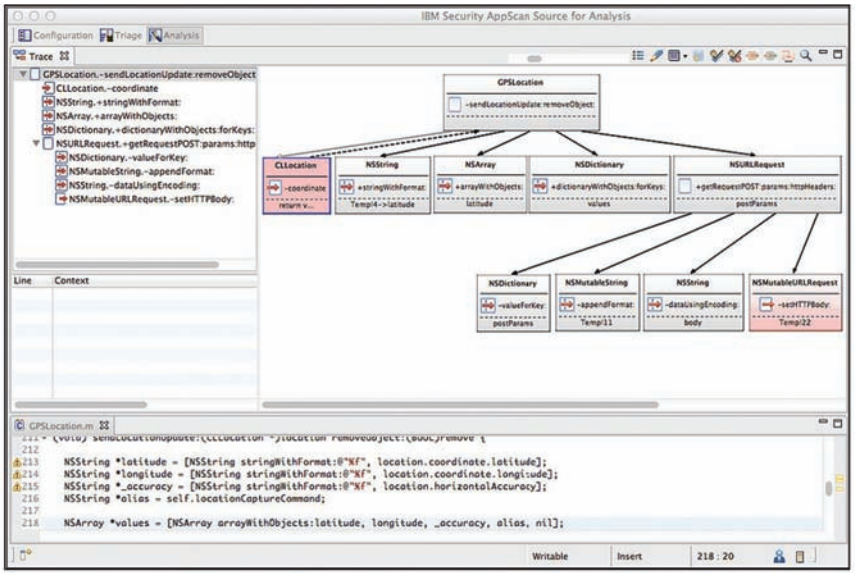

Figure 4. Comprehensive call and data-flow analysis help to isolate mobile application security risks.

Managing the risk in enterprise modernization

Enterprise modernization of legacy applications can also be a source for application risk. COBOL still accounts for nearly 80 percent of the world's actively used code,[1] and web interfaces for these legacy applications open them to threats that did not exist when the code was written 20 to 40 years ago.

The IBM Security AppScan software portfolio delivers complete security coverage for enterprise modernization projects to secure the web interfaces and analyze the legacy code to identify security vulnerabilities. With extensive language support that includes Java, .NET, C/C++, PHP, SAP ABAP, COBOL and Objective-C, as well as robust integration with IDEs such as IBM Rational Application Developer, Eclipse and Microsoft Visual Studio, IBM Security AppScan Source helps manage security risk and protects legacy assets by proactively securing the applications. Key benefits include:

- Cost-effectively managing risk with proactive remediation of application vulnerabilities
- Protecting legacy assets by securing applications early in the application lifecycle
- Identifying vulnerabilities and risks associated with multiple languages, including Java, JavaScript, JSP, ColdFusion, C, C++, Objective-C, .NET (C#, ASP.NET and VB.NET), Classic ASP (JavaScript/VBScript), PHP, Perl, VisualBasic 6, PL/SQL, T-SQL, SAP ABAP and COBOL

Extending static testing to include code quality

Many leading organizations integrate security with their software development processes by making security an element of quality management. As security and quality converge, the static code analysis capability of IBM Security AppScan Source has extended to include identification of quality defects. IBM Security AppScan Source also includes the capabilities offered by IBM Rational Software Analyzer, which:

- Identifies code-level quality defects at the time of coding, helping save both time and money
- Improves overall code quality and predictability by identifying and resolving potential coding errors
- Provides KPIs to help developers learn best practices
- Enhances project visibility and more effectively manages governance and compliance using customizable and out-of-the-box reporting
- Automates code quality analysis as part of the build process for a centralized software code scan solution

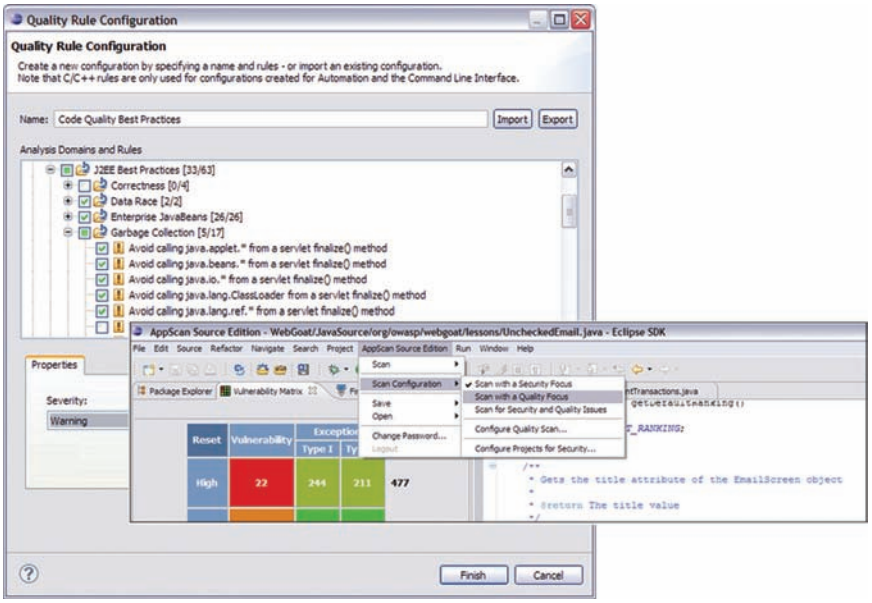

Figure 5. IBM Security AppScan Source includes code quality analysis that is executed from the IDE or in the build system, just like security tests.

IBM Security AppScan Source software provides options for executing quality testing from the IDE, including IBM Security AppScan Source for Developer software and IBM Security AppScan Source for Remediation software, or in the build system with IBM Security AppScan Source for Automation software. By extending static analysis to include quality testing, IBM Security AppScan Source can help clients continuously enforce code-quality best practices for faster time to market and higher customer satisfaction.

Why IBM?

With advanced security testing and a platform managing application risk, the IBM Security AppScan portfolio delivers security expertise and critical integrations to application lifecycle management that enable organizations to identify vulnerabilities and reduce overall application risk. IBM designed the portfolio to include advanced static and dynamic analysis, as well as innovative technologies to keep up with the latest threats and drive precise, actionable results.

Solution components	Features and benefits
IBM Security AppScan Enterprise Server (required)	• Provides centralized platform for managing application security testing and risk management for hundreds or thousands of applications • Drives collaboration between security, development and testing teams to remediate vulnerabilities and reduce risk • Offers enterprise-wide view of application security and compliance risk with more than 40 out-of-the-box report templates for measuring compliance, trending and KPIs • Correlates and triages security testing results from dynamic and static scans • Integrates with IBM Security Network Intrusion Prevention System, IBM Security SiteProtector and IBM Security Server Protection software to block attacks that target vulnerabilities identified by IBM Security AppScan software • Integrates with IBM Security QRadar SIEM to provide application vulnerability data, which QRadar uses to reduce all of these events into a handful of actionable offenses prioritized according to their business impact
IBM Security AppScan Source for Analysis (required for static analysis)	• Uses workbench to manage static application security testing policies—configures and scans • Triages results from static testing and takes action to remediate vulnerabilities • Provides integration into defect-tracking systems including IBM Rational ClearQuest®, HP Quality Center, Rational Team Concert™ and Microsoft Team Foundation Server
IBM Security AppScan Source for Automation (optional)	• Seamlessly integrates static application security testing, publishing and reporting into build environments • Automates code quality analysis as part of the build process
IBM Security AppScan Source for Development (optional)	• Provides IDE module with the ability to scan source code and to understand and address critical vulnerabilities at the line of code • Remediates security vulnerabilities from the IDE with detailed explanations of the defect and recommended source-code corrections • Identifies and remediates non-security software code-level quality defects
IBM Security AppScan Source for Remediation (optional)	• Provides IDE module with the ability to process and address critical vulnerabilities at the line of code • Remediates security vulnerabilities from the IDE with detailed explanations of the defect and recommended source-code corrections • Identifies and remediates non-security software code-level quality defects
IBM Security AppScan Enterprise Dynamic Analysis Scanner (optional)	• Adds advanced, dynamic application security testing
IBM Security AppScan Enterprise Reporting Console (optional)	• Enables a web-based user to triage testing results, collaborate with development teams, create reports and drive application risk management
Virtual Forge CodeProfiler for IBM Security AppScan Source (optional)	• Extends static code analysis to SAP ABAP applications to identify and remediate security vulnerabilities and performance issues

IBM Security AppScan Source at a glance

System requirements:

- Disk space: Approximately 1.5 GB of available hard-disk space (2 GB required for installation)
- Media drive: CD-ROM or DVD-ROM drive
- Memory: 2 GB of RAM minimum (8 GB or more recommended)
- NIC network driver: 1 NIC (10 Mbps) for network communication with configured TCP/IP (100 Mbps recommended)
- Processor: 2 CPU

Operating systems:

- Microsoft Windows 7 Professional, Enterprise and Ultimate 32- and 64-bit (in 32-bit mode)
- Microsoft Windows XP Professional (SP3)
- Microsoft Windows Vista Business, Enterprise and Ultimate (SP1 and higher) 32- and 64-bit (in 32-bit mode)
- Microsoft Windows Server 2003 Enterprise and Standard (SP2) (32-bit x86)
- Microsoft Windows Server 2003 R2 Enterprise and Standard (SP2) (32-bit x86)
- Microsoft Windows Server 2008 Enterprise and Standard (SP1 and SP2) (32-bit x86)
- Microsoft Windows Server 2008 R2 Enterprise and Standard 64-bit (in 32-bit mode)
- Red Hat Enterprise Linux 5.0 (through Update 8), 6.0 (through Update 3), Workstation and Server 32- and 64-bit (in 32-bit mode)
- Mac OS X Version 10.7 64-bit (in 32-bit mode) and 10.8 (IBM Security AppScan Source for Analysis and IBM Security AppScan Source for Automation only)

Project files:

- Visual Studio 2005, Visual Studio 2008 and Visual Studio 2010; Eclipse 3.3, 3.4, 3.5, 3.6, 3.7 and 3.8; IBM Rational Application Developer V7.5.x, V8.0.x and V8.5.x

Compilers:

- GNU Compiler Collection (GCC) for Linux, Visual Studio 2005 (V8) for Windows, Visual Studio 2008 (V9) for Windows, Visual Studio 2010 (V10) for Windows, Xcode Versions 4.4 through 4.6 for Objective-C (for iOS applications only), Java (Jasper V1 [Tomcat V3], Jasper V3 [Tomcat V5], Weblogic V8 and V9, and IBM WebSphere® Application Server V6.1 and V7)

IBM Security AppScan Source at a glance

Language support for security testing (Windows and Linux):

- Java, ServerSide JavaScript, JSP, ColdFusion, C, C++, .NET (C#, ASP.NET and VB.NET), Classic ASP (JavaScript/VBScript), PHP, Perl, VisualBasic 6, PL/SQL, T-SQL and COBOL

Language support for security testing (OS X):

- Objective-C in Xcode projects, Java, Android, JavaScript and JSP

Code quality scanning support:

- Java, C/C++ (CLI only) on IBM Security AppScan Source supported Microsoft Windows and Red Hat Enterprise Linux platforms

IDE plug-in support:

- On IBM Security AppScan Source supported Microsoft Windows and Red Hat Enterprise Linux platforms: Eclipse 3.3, 3.4, 3.5, 3.6, 3.7 and 3.8; IBM Rational Application Developer V7.5.x, V8.0.x and V8.5.x; Visual Studio 2005, Visual Studio 2008 and Visual Studio 2010
- Rational Application Developer and Eclipse support Java; Visual Studio supports C#, ASP.NET and VB.NET

Defect tracking system support:

- On Windows and Linux: IBM Rational ClearQuest V7.0, V7.1.1, V7.1.2 and V8.0; HP Quality Center V9.2, V10.0 and V11.0; Rational Team Concert V2.0.0.2, V3.0, V3.0.1, V4.0 and V4.0.1; Microsoft Team Foundation Server 2008 and 2010
- On OS X: Rational Team Concert V2.0.0.2, V3.0, V3.0.1, V4.0 and V4.0.1

External database support:

- Oracle 11 g

License management:

- License Server: Rational License Server 8.1.1, 8.1.2 and 8.1.3 (if activating by floating license)

For more information

To learn more about how IBM Security AppScan Source can help you identify vulnerabilities in your source code and identify threat exposures, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/awdtools/appscan

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

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.

[1] "TechBrief: Cobol – still doing the business," Nick Bray, January 2010. http://www.bankingtech.com/bankingtech/article.do?articleid=20000168221

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2013

RAD14105-USEN-04