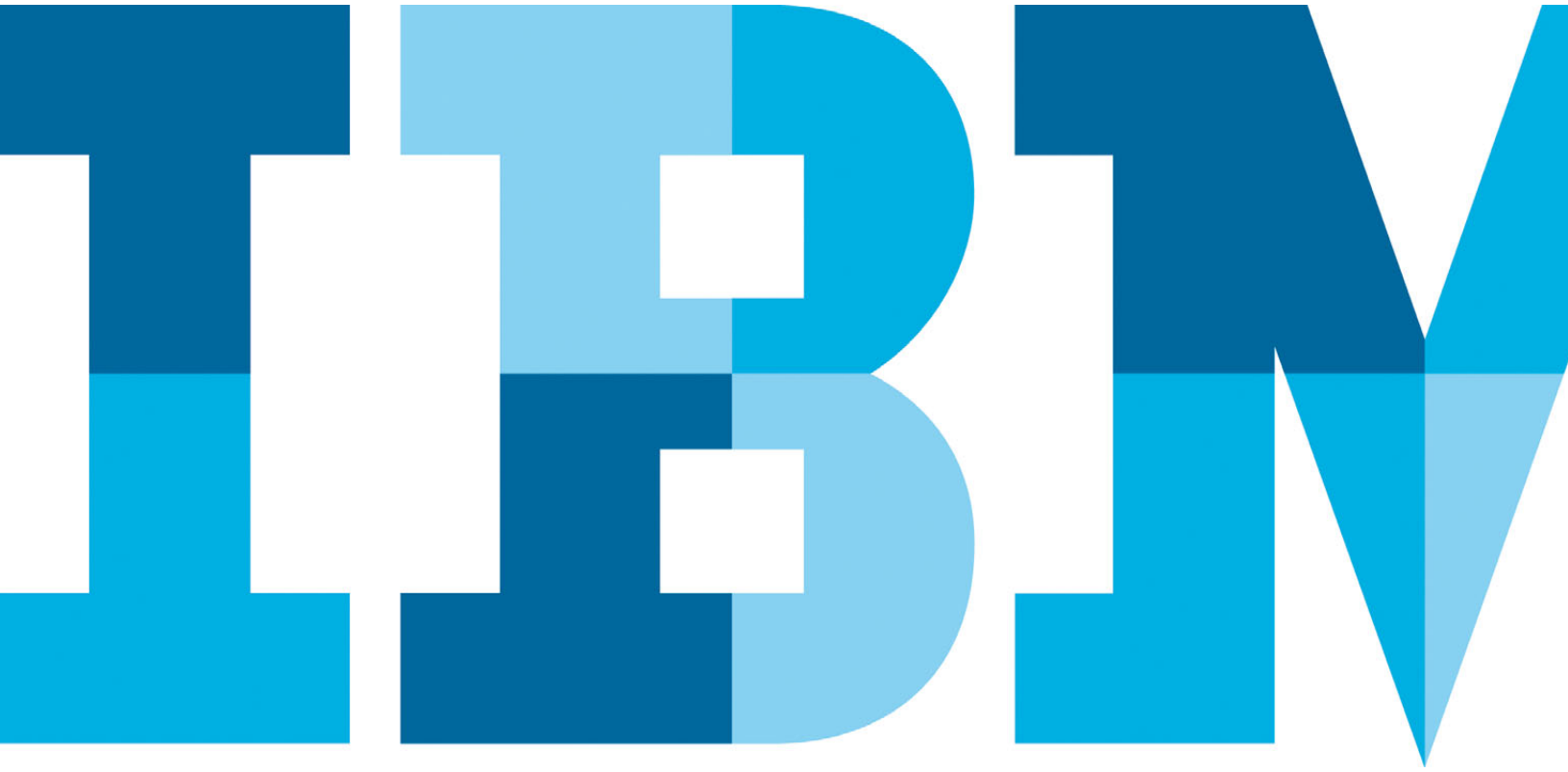
IBM Rational AppScan: Managing application security and regulatory compliance

Identify, prioritize, track and remediate critical security vulnerabilities throughout the application life cycle



IBM

Comprehensive application vulnerability management

Many organizations depend on web-based software to run their business processes, conduct transactions and deliver increasingly sophisticated services to customers. Every application destined for online deployment should address security issues as an integral part of the software delivery process. Unfortunately, in the race to meet deadlines and stay ahead of the competition, many businesses fail to perform adequate security testing, and the resulting vulnerabilities provide ample opportunity for hackers to access or steal corporate or personal data—placing the entire business at risk.

The most efficient way to stay ahead of application security vulnerabilities is to build software securely, from the ground up. The challenge is that the majority of developers are not security experts, and secure coding is historically not identified as a priority relative to delivering functionality on time and on budget. As a result, web-based and non-web based applications alike continue to be deployed riddled with vulnerabilities ready for exploitation, easily risking sensitive data to a breach.

The onerous task of vulnerability identification and remediation cannot be successfully addressed by limited IT security resources. So the best way to engage development in the process of application security is to provide them with tools that fit into their existing environment and workflow, and that generate results in a language they understand. The IBM® Rational® AppScan® software portfolio enables organizations to embed application security testing throughout the development life cycle to help increase visibility and control while employing a risk mitigation strategy.

From requirements, through design and code, security testing, and into production, Rational AppScan software helps to ensure that critical security vulnerabilities are identified, prioritized, tracked, and remediated across the application life cycle. In short, Rational AppScan software helps you to design security into your application infrastructure.

The IBM Rational AppScan software product suite includes:

Licensed offerings

- IBM Rational AppScan Express Edition
- IBM Rational AppScan Standard Edition
- IBM Rational AppScan Source Edition
- IBM Rational AppScan Build Edition
- IBM Rational AppScan Tester Edition
- IBM Rational AppScan Reporting Console
- IBM Rational AppScan Enterprise Edition

SaaS offerings

- IBM Rational AppScan OnDemand
- IBM Rational AppScan OnDemand Premium
- IBM Rational AppScan OnDemand Production Site Monitoring
- IBM Rational AppScan OnDemand Source Code Analysis

Training and service options

- IBM Rational web-based training for AppScan
- IBM Rational Professional Services

Each of these solutions provides scanning, reporting and fix recommendation functionality, and each is designed for a variety of users, including information security managers, penetration testers, security auditors, application developers, build managers, and quality assurance (QA) teams.

Protect critical web-based business assets

Offering comprehensive security capabilities for complex web applications, the Rational AppScan software suite scans and tests for common web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification. Rational AppScan solutions share an extensive range of powerful, flexible core features to provide robust application scanning coverage for the latest Web 2.0 technologies, including enhanced support for Adobe® Flash technology and advanced JavaScript frameworks, coupled with comprehensive support for AJAX-based applications.

IBM Rational AppScan core features

Feature	Benefits
Scanning efficiency and ease of use	• The user interface provides a view selector for the application tree, along with hierarchical security issues results lists, developer remediation views and details panes. • An adaptive test process helps users to analyze application parameters and select only relevant tests that do not impede the development process. • Complex authentication support allows testing for multistep authentication procedures. • Advanced session management performs automatic re-logins when required. • Real-time results views help users to act on issues before a scan is complete. • Prebuilt pattern search rules facilitate security testing around credit card, social security or other numerical sequences.
Customization and control	• Rational AppScan eXtensions Framework technology helps users create, share and load powerful add-ons that extend testing capabilities. • Pyscan, which couples Rational AppScan software with the capabilities of Python scripts, lets users leverage scanning capabilities without the limitations of a user interface. • Rational AppScan software development kit (SDK) helps users invoke actions, from executing a long scan to submitting a custom test. The SDK interfaces are designed to ease integrations and support customized use of the scan engine, along with Rational AppScan eXtensions Framework and Pyscan options.
Vulnerability detection	• Coverage for global validation analyzes test responses for inadvertently triggered issues, Secure Sockets Layer (SSL) certificate testing and cross-site request forgery (CSRF) testing. • Hacker simulations aid in the search for current, known vulnerabilities. • Notifications on the latest threats are delivered automatically when users launch a Rational AppScan application. • A bundled utility suite helps penetration testers and security consultants develop, test and debug web applications. • Security testing coverage for web services.

"We turned to IBM Rational because they offered both the technology leadership and the deep security expertise required to help us implement an analysis strategy that could be embedded in our existing development process. By doing so we have been able to vastly improve the security of our software while reducing costs by finding vulnerabilities earlier where they are less costly to repair."

—Marek Hlávka, Chief Security Officer, Skoda Auto

IBM Rational AppScan Express Edition
IBM Rational AppScan Standard Edition

Gain robust web application security features

Organizations with small or limited application development teams also need to consider security testing as part of the development life cycle. Yet these organizations often have to sacrifice functionality for affordability. Rational AppScan Express Edition software meets the requirements of mid-size organizations by delivering the uncompromising security testing functionality at an attractive price point. Designed for ease of deployment, Rational AppScan Express Edition software can help lower the time and costs associated with manual vulnerability testing, allowing your teams to focus on other IT and security-related needs within your organization.

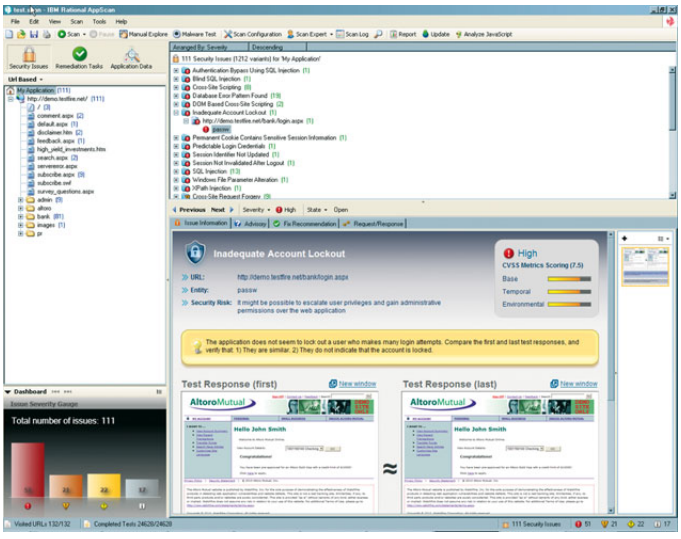


Figure 1: Rational AppScan Standard software helps you identify vulnerabilities in your website before the hackers do.

Conduct security audits and production monitoring

Automating web application testing processes to help security auditors and penetration testers quickly and efficiently do their jobs requires sophisticated and intelligent scanning technologies. Rational AppScan Standard Edition software includes features designed to support moderate and power users.

Rational AppScan Express Edition and Standard Edition software features

- JavaScript Analyzer: Leveraging dynamic and static analysis to help deliver scanning hybrid analysis and identify previously unknown vulnerabilities.
- Scan expert: A wizard tool that offers guidance for scan creation and set-up based on best practices, including the use of additional tools. Users can authorize a pre-scan that profiles the target application and recommends actions required for a successful scan.
- State inducer: Scans and tests complex business processes (such as multistep online shopping carts and order tracking) and maintains parameter values and cookies throughout.
- Predefined scan templates: Helps users to quickly choose and launch configuration options.
- Rapid scan configuration wizard: Guides users through important settings as well as conditional steps for proxy/platform authentication and in-session detection information.
- New request/response tabs: Offer syntax highlighting, request/response, collapse/expand, as-you-type search and additional right-click options.
- Microsoft® Word template-based reporting.
- Embedded web-based training modules: Help explain issues and demonstrate exploits.
- Automated web services assessments: Help locate application-layer vulnerabilities, SOAP and XML parser vulnerabilities and web services infrastructure vulnerabilities.

IBM Rational AppScan Build Edition

Automate security testing

Rational AppScan Build Edition software supports automated security testing at the build stage of the software development life cycle. By integrating with multiple build management systems, such as IBM Rational Build Forge® software, it provides security testing coverage for scheduled builds. It also routes the results back to development though defect-tracking solutions such as IBM Rational ClearQuest® software, or through security reporting solutions such as Rational AppScan Enterprise Edition software or Rational AppScan Reporting Console software.

Rational AppScan Build Edition software includes the same set of analysis techniques as the Rational AppScan Developer Edition software, providing a high level of accuracy plus code coverage that helps you identify which code has been tested.

IBM Rational AppScan Tester Edition

Make security testing part of your quality management program

Rational AppScan Tester Edition software, available as a desktop application, offers capabilities to help QA teams integrate security testing into existing quality management processes, thereby easing the burden on security professionals.

Because Rational AppScan Tester Edition software integrates with leading testing systems, QA professionals can use its functionality in test scripts and can conduct security checks within their familiar testing environments, facilitating the adoption of security testing along with functional and performance testing.

IBM Rational AppScan Reporting Console

Access centralized reporting on web application vulnerability data

IBM Rational AppScan Reporting Console software is a powerful web-based management and reporting application. Fully integrated with Rational AppScan Express, Standard, Source, Tester and Edition software, Rational AppScan Reporting Console software is backed by an enterprise-class database that allows you to consolidate scan results from multiple Rational AppScan Express and Standard clients to create a centralized application vulnerability repository. Scan results can be easily distributed to QA and development teams without having to install additional desktop licenses, helping to simplify the remediation process and integrate vulnerability analysis across the software development life cycle. Rational AppScan Reporting Console software allows you to create multiple dashboards for multiple users, giving individuals the ability to segment security data by application, business unit, geography or third-party provider.

Rational AppScan Reporting Console software features

In addition to the convenience and extensibility of centralized administration, Rational AppScan Reporting Console software features include:

- **A central data repository: Automatically stores and aggregates static and dynamic analysis test results for enterprise-wide access and multiple views.**
- **Automated correlation of analysis test results: Static and dynamic (hybrid analysis).**
- **A web-based reporting console: Provides role-based access to security reports and facilitates communication across the organization.**
- **Executive dashboards and delta analysis reports: Highlight changes from one scan to the next, including fixed, pending and new security issues.**
- **Centralized controls: Monitoring and control web application vulnerability testing across the organization.**

IBM Rational AppScan Source Edition

Embed security testing seamlessly into your development environment

The most efficient way to stay ahead of application security vulnerabilities is to build software securely from the ground up. The challenge is that most developers are not security experts, and writing security-rich code is not always their top priority. So the best way to engage development in the process of application security is to provide them with tools that work in their environment and that generate results in languages they understand.

Rational AppScan Source Edition software is designed to help developers and build managers invoke application security testing from within their development or build environment. It helps the development organization to address the volume of security issues that can be introduced in code, streamlining the development life-cycle workflow and helping to reduce costly security testing bottlenecks that can occur at the end of the release cycle.

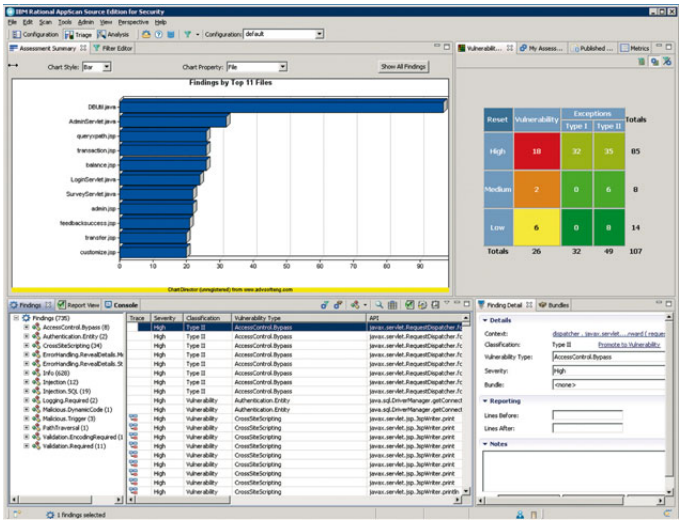


Figure 2: Rational AppScan Source Edition software provides a workbench to configure applications and projects, scan code, analyze, triage, and take action on priority vulnerabilities. You can also publish assessments to Rational AppScan Enterprise Edition software for correlation.

Rational AppScan Source Edition software features

- Address the root cause of data breach risk through the identification and remediation of security defects in the source at the early stages of the application life cycle.
- Create, distribute and enforce consistent policies and empower enterprise-wide metrics and reporting with a centralized policy and assessment database.
- Accommodate a broad portfolio of large and complex applications across a wide range of languages.
- Build automated security into development by seamlessly integrating security source code analysis with automated scanning during the build process.
- Facilitate collaboration between security and development by offering flexible triage and remediation that automates flow of information between these teams.
- Provide a method to certify outsourced applications by building security requirements into outsourcing contracts and leveraging Rational AppScan Source Edition software to manage acceptance criteria.
- Provide options for security, development and remediation types of users.
- Allow security teams to scan, triage, manage security policies and prioritize the assigning of results for vulnerability remediation.
- Help development teams to pinpoint vulnerabilities and provide precise, detailed remediation advice for rapid fixes, all within the developer IDE.

IBM Rational AppScan Enterprise Edition

Scale application security testing across the enterprise

With its web-based architecture, Rational AppScan Enterprise Edition software is designed to help organizations distribute responsibility for security testing and provide visibility and access to multiple stakeholders. Scalability and centralized control facilitate the necessary governance, collaboration, and risk management capabilities to effectively manage security testing across the enterprise. AppScan Enterprise Edition helps ensure timely communication and coordination across multiple teams as results are prioritized, tracked, and remediated. It provides regulatory compliance reports and an overall compliance view, while management views offer real-time graphical dashboards and trending of the organization's security posture. Enterprise Edition is also available as a SaaS offering, allowing you to leverage Rational's expertise and proven processes, easily scale and add users as needed, and gain better control of costs.

Rational AppScan Enterprise Edition software features

In addition to the convenience and extensibility of centralized administration, Rational AppScan Enterprise Edition software features include:

- The ability to distribute security testing to multiple teams to ease the testing burden on the security organization, and to scan and test hundreds of applications simultaneously and retest them frequently, following changes.
- A QuickScan testing tool to execute administrator-defined scan templates for developers and other non-security professionals, without desktop installation or configuration.
- A central data repository that automatically stores and aggregates static and dynamic analysis test results to enable multiple views and enterprise-wide access.
- Automated correlation of static and dynamic analysis test results (hybrid analysis) for more precise results and the ability to pinpoint issues to individual lines of code to speed remediation tasks.

Rational AppScan Enterprise Edition software features

- A web-based console that provides role-based user access to security reports, tracking and trending over time, which facilitates communication across the organization.
- Executive dashboards and delta analysis reports that highlight changes from one scan to the next, including fixed, pending and new security issues.
- Centralized controls for monitoring and controlling web application vulnerability testing across the organization.

IBM Rational AppScan OnDemand

Leverage IBM security expertise and proven processes in an outsourced, turnkey SaaS model

By accessing Rational AppScan software capabilities as a managed service, you can take advantage of product benefits without the costs of adding staff or hardware.

Rational AppScan software features as a managed service

- A state-of-the-art security testing environment.
- A focus on protecting your operating environment: these services are built with sophisticated security tools and techniques.
- Dedicated security and compliance assistance from IBM professionals
- Rational AppScan Standard Edition software or Rational AppScan Enterprise Edition software SaaS customers can engage an IBM security analyst to help:
  - Configure and tune scans to potentially ensure comprehensive coverage for each application.
  - Review and analyze results to help eliminate false positives, identify patterns, prioritize issues and highlight remediation tasks.
  - Track remediation progress by maintaining trend data, tracking resolution from scan to scan, and reporting on remediation effectiveness.

For more information

To learn more about IBM Rational AppScan products, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/rational/offerings/testing/webapplicationsecurity

Web-based training

IBM offers web-based application security training, delivered online and in 15-minute intervals. In addition to basic product instruction, the training service provides targeted advice for developers, QA teams and security professionals.

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
December 2010

Please Recycle

Rational. software

RAB14001-USEN-03