June 2012

IBM Security AppScan: Application security and risk management

Identify, prioritize, track and remediate critical security vulnerabilities

IBM

Organizations today rely on software applications to drive essential business processes, from online transactions to advanced mobile access for customers, business partners and employees. The critical nature of these processes—and the data they collect—make these applications a top target for attacks and the number one source of data breaches. For this reason, organizations require solutions specific to the challenges of application security that go beyond basic security testing to manage application risk.

The greatest source of application risk comes from security vulnerabilities that create the opportunity for attacks. These can compromise the integrity of business processes and may allow an attacker to access, create, change or delete data without authorization. But application risk also includes compliance demands that require businesses and public entities to secure sensitive data. To stay ahead of these threats, applications must be *secure by design*.

IBM Secure by Design is the IBM philosophy that security and privacy must be fully considered and prioritized throughout the lifecycle of your applications, systems, networks and business processes. When applied to the specific risks and demands of applications, IBM Secure by Design integrates security throughout the software development process. To address the wide range of application risk, the IBM Security AppScan® portfolio integrates into application lifecycle management to identify risk, facilitate timely remediation and monitor the state of application security and risk over time.

After applications are developed, they are deployed into operational environments where threat protection systems are used to deflect attacks and security intelligence systems are used to manage the overall security posture. IBM Security AppScan integrates with the IBM Security Advanced Threat Protection platform to provide data about known vulnerabilities and to incorporate risk data into vulnerability remediation decisions. Quite simply, IBM Security AppScan enables you to deliver and maintain applications that are *secure by design*.

With a rich history of innovative application security research, the IBM Security AppScan portfolio combines advanced security testing with the strengths of the IBM Rational® Application Lifecycle Management suite to enhance productivity through automation and accelerate better decision making throughout the development organization.

Application security: A shared responsibility

Application security has traditionally been the responsibility of security teams that conduct audits before applications launch. While some vulnerabilities can be corrected, organizations often face a difficult decision when a security defect is identified just before launch. They can:

1. Add development cycles that may delay the launch and increase project costs

2. Accept the risk of data loss from targeted attacks, application downtime or compliance penalties by launching the application with the security vulnerabilities and compliance issues

The IBM Security AppScan portfolio includes solutions for both security teams and development organizations to collectively address application security by identifying and remediating vulnerabilities early in the software development lifecycle, when they are easier and less expensive to correct. IBM research drives IBM Security AppScan solutions to identify the latest threats with advanced security testing for application security analysts. With more than a decade of application security experience, IBM Security AppScan solutions deliver some of the most advanced testing features that combine expert analysis with ease of use.

The IBM Security AppScan portfolio includes solutions specifically designed for non-security experts to execute automated test scripts configured by the security team to identify common vulnerabilities, such as SQL injection and cross-site scripting (XSS). By enabling developers and quality assurance professionals to address application security as part of their normal processes, security teams can dedicate their efforts to the more advanced testing to identify sophisticated threats like client-side JavaScript vulnerabilities.

Integrate security into application lifecycle management

Security vulnerabilities are just like quality defects—they occur naturally in any application development process. Organizations require tools and solutions that empower them to identify and remediate these vulnerabilities as part of their standard practices for application lifecycle management.

"We turned to IBM Security 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 when they are less costly to repair."

—Marek Hlávka, Chief Security Officer, Škoda Auto

Secure your mobile applications

The recent explosive growth of mobile adoption and applications has dramatically broadened the typical organization's attack surface. The 2011 IBM Technology Trends Report indicated that security and privacy are top concerns for mobile adoption within the enterprise.[1]

IBM Security AppScan allows you to integrate mobile security testing throughout the application lifecycle:

- **Easy and quick mobile application scan setup with predefined templates**
- **Dynamic application security testing (DAST) and static application security testing (SAST) of server and client vulnerabilities**
- **Ability for security and non-security experts to test mobile applications**
- **Enhanced visibility of mobile applications through shared reporting and metrics**

By applying the principles of IBM Secure by Design, the IBM Security AppScan portfolio leverages the strengths of the IBM Rational Collaborative Lifecycle Management solution to integrate security throughout the application lifecycle and enable organizations 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, enabling decision makers to act with confidence and documenting compliance
- *Deliver* greater predictability by mapping successful deployment patterns to operational key performance indicators (KPIs)

From requirements—through design and code—to security testing and production, IBM Security AppScan software helps to ensure that critical security vulnerabilities and compliance issues are identified, prioritized, tracked and remediated across the application lifecycle. In short, IBM Security AppScan software helps you to design security into your application infrastructure.

Start application security at the requirements and design phases

Just like quality standards, application security is not limited simply to security testing. Security starts by building applications that are *secure by design*. For this reason, the security experts who built IBM Security AppScan provide templates for application security requirements. By including security requirements early in development, project teams can write use cases that reflect security risks, reduce project rework and improve the overall security of the application.

Write secure code and identify vulnerabilities

Once security is identified as a high-priority requirement for application development, development organizations can then implement secure development practices by empowering developers to identify and remediate security vulnerabilities—while measuring the group's progress at meeting the objectives of secure applications.

The IBM Security AppScan portfolio delivers the solutions that empower these non-security experts to analyze their code and compiled applications for security vulnerabilities, then take action to remediate the issue. IBM Security AppScan Source includes plug-ins into the integrated development environment (IDE) to analyze the source code with SAST technology and pinpoint the precise line of code that contains the vulnerability.

IBM Security AppScan Enterprise includes options for DAST that tests compiled applications. With its QuickScan web interface designed for non-security experts, IBM Security AppScan Enterprise enables developers to easily execute predefined test scripts to identify vulnerabilities by simulating security attacks against the application. With both static and dynamic testing, the IBM Security AppScan solutions include detailed vulnerability descriptions that explain the risk and recommended code corrections that give developers the information needed to remediate the issue.

Tools like IDE integrations and QuickScan provide developers with information on improper coding practices to reduce the costs of remediation and help prevent similar security defects from being introduced as they develop additional code.

Integrate security testing with build verification

Security testing is a natural extension to build-acceptance tests. Before a build is released to the test team, development organizations can run static and dynamic tests against the build to identify and remediate known vulnerabilities. IBM Security AppScan Source includes options for automatically triggering static analysis of the source code with each build. Through their IDE plug-in, developers then access the results to view issues in their code—as well as detailed descriptions of risk and recommended remediation.

By automating attacks against the compiled application, dynamic testing from IBM Security AppScan Enterprise or IBM Security AppScan Standard provides powerful analysis of how the application withstands security attacks while providing the detailed vulnerabilities that should be addressed before releasing the build.

Make security an element of quality in test planning

When application security is integrated into test planning, quality assurance (QA) managers can build and execute test plans that map to security requirements. With these test plans in place, QA managers can then use DAST from IBM Security AppScan Enterprise that automates test scripts predefined by the security team. IBM Security AppScan Enterprise integrates with IBM Rational Quality Manager software to execute and manage security tests within the familiar testing environment.

IBM Security AppScan offering	Integrations with IBM Rational Application Lifecycle Management solutions
AppScan Enterprise	• IBM Rational ClearQuest® • IBM Rational Quality Manager • IBM Rational Team Concert™
AppScan Source	• IBM Rational Application Developer • IBM Rational ClearQuest • IBM Rational Quality Manager • IBM Rational Build Forge®
AppScan Standard	• IBM Rational ClearQuest

Provide advanced security testing before launch

With common security vulnerabilities identified and corrected in the development, build and testing stages of the process, security teams can now focus on advanced security testing. The IBM Security AppScan portfolio has a deep history of innovation to deliver broad coverage of application risk with precise results. IBM Security AppScan software's advanced security testing delivers:

- Scanning of rich Internet applications that use Adobe Flash, JavaScript, Ajax and more
- Coverage for top threats as ranked by the Open Web Application Security Project (OWASP) and Web Application Security Consortium (WASC)
- Advanced testing for Simple Object Access Protocol (SOAP) web services
- Static taint analysis of client-side JavaScript
- Innovative interactive application security testing (IAST) that combines DAST with an internal agent that monitors application behavior during a simulated attack to provide more accurate test results and identify specific lines of code, providing details that help facilitate remediation

Ensure security of production applications

In 2011, web application vulnerabilities comprised 41 percent of all vulnerability disclosures.[2] To keep up with the new threats and meet compliance requirements, security teams must routinely scan their critical applications and remediate new vulnerabilities identified in their production applications. Advanced application security research at IBM drives regular content updates to the IBM Security AppScan portfolio so clients can be confident they are keeping up with the latest threats.

Organizations expand beyond security testing into application risk management when they apply the centralized management features of IBM Security AppScan Enterprise to:

- *Schedule* routine scans of production applications—and execute the scans concurrently
- *Measure* results over time and across multiple scans for each application to track improvement and recognize areas of concern
- *Monitor* aggregate risk throughout all applications for executive-level views with KPIs
- *Integrate* with defect-tracking systems and the IBM Rational portfolio for collaborative lifecycle management
- *Deliver* more than 40 ready-to-use-without-modification compliance reports for global regulations including PCI, HIPAA, EU Data Protection Directive, ISO 27001 security control standard and more

Mitigate risk by blocking attacks with IBM Security defenses

As organizations execute their regular scans for their production applications, they are likely to find new vulnerabilities that create the opportunity for hackers to exploit. When organizations identify security defects in their mission-critical applications, they need a solution that allows them to keep these applications online and protect them from attacks while they wait for their development teams to create a software patch or release a new version of the application.

IBM Security AppScan Enterprise software delivers the security intelligence to integrate vulnerability management with application-protection strategies. IBM Security AppScan Enterprise integrates with the IBM Security solutions for network and server security to protect specific vulnerabilities with a "virtual patch"—including specific protection policies designed to address the vulnerability. Organizations can then deploy these protection policies to block attacks either on the network before they reach your applications with IBM Security Network Intrusion Prevention System or on the application server with the IBM Security Server Protection solution. These customized security policies provide the virtual patch to protect the application from attack and allow organizations to correct the vulnerabilities as part of their normal patch-management processes and release cycles.

IBM Security AppScan offering	Integrations with IBM Security offerings
AppScan Enterprise	• QRadar SIEM • QRadar Risk Manager
	• IBM Security Network Intrusion Prevention System • IBM Security Server Protection
	• IBM Proventia® Management SiteProtector™ System

Expand your security intelligence with application-vulnerability data

The QRadar Security Intelligence platform collects, stores and analyzes informational data and provides real-time event correlation for use in threat detection and compliance reporting and auditing. With some organizations creating millions or billions of events per day, distilling that data to priority offenses can be a daunting task. IBM AppScan Enterprise integrates with QRadar to provide application-vulnerability data, which QRadar uses to reduce and prioritize all these events into a handful of actionable offenses according to their business impact.

In addition, application-vulnerability data is provided to the QRadar Risk Manager analytics engine to enable security experts to simulate attacks, determine the exploitability of vulnerable application assets and understand the risk they present to the organization.

Managing the risk in enterprise modernization

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

The IBM Security AppScan portfolio delivers complete security coverage for enterprise modernization projects to secure the web interfaces and analyze the heritage-application code to identify security vulnerabilities. With extensive language support that includes COBOL and C++ and robust integration with IDEs, IBM Security AppScan Source helps manage security risk and protect heritage assets by proactively securing the applications. Key benefits include:

- Cost-effectively manage risk with proactive remediation of application vulnerabilities
- Protect heritage assets by securing applications early in the application lifecycle
- Identify vulnerabilities and risks associated with multiple languages including COBOL, Java and .NET (Microsoft Visual C#, VB.NET, ASP.NET)

IBM Security AppScan portfolio summary

IBM Security AppScan offering	Description
AppScan Enterprise	• Provide a platform for managing application security and risk management • Identify application risk with advanced security testing • Mitigate risk by collaborating with developers to remediate security vulnerabilities • Measure, monitor and drive risk reduction with reporting, issue tracking, KPIs and trending • Empower security teams to drive security testing throughout the software development life cycle (SDLC) • Collaborate with developers to remediate security vulnerabilities • Integrate with web-application firewalls to provide custom tuning based on actual vulnerabilities • Plan and execute DAST against applications in development and production • Utilize hybrid analysis to perform correlation of DAST and SAST results • Integrate with IBM Rational Quality Manager software for QA managers to use in test scripts and for conducting security checks within their familiar testing environments
AppScan Source	• Add source code analysis to IBM Security AppScan Enterprise Edition to identify the latest security threats with SAST • Enable quick analysis and recommended corrections, all within the IDE • Automated security testing within build environments
AppScan Standard	• Desktop application for security analysts and penetration testers • Advanced security testing based primarily on DAST, but also includes static analysis for client-side JavaScript • Glass box testing, a form of IAST, is runtime analysis that applies an internal agent to monitor application behavior during a dynamic test, providing more accurate test results and identifying specific lines of code and details to help facilitate remediation • Coverage of the latest rich-Internet applications and web technologies (web services, SOAP, Flash, Ajax and more) • Designed for ease of use

Why IBM for application security and risk management

IBM delivers the most complete portfolio of application-security and risk-management solutions. With advanced security testing and a platform managing application risk, the IBM Security AppScan portfolio delivers the security expertise and critical integrations to application lifecycle management that empower organizations to not just identify vulnerabilities, but also reduce overall application risk. The IBM Security AppScan portfolio includes advanced SAST and DAST—as well as innovative technologies like IAST testing and runtime analysis that keep up with the latest threats and drive precise, actionable results. Application security is a core component of the IBM Security framework. The software portfolio of IBM Security AppScan is complemented by software-as-a-service delivery options and robust professional service offerings, including application security assessments, deployment services, advanced application security training, product training and more. In addition to application security testing, IBM Security Systems delivers application security solutions that protect against attacks and securely manage identity and access for application users.

For more information

To learn more about IBM Security AppScan solutions for application security, please contact your IBM sales representative or IBM Business Partner, or visit the following website: **ibm.com**/software/products/us/en/category/SWI10

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

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] The 2011 IBM Tech Trends Report, IBM, 2011; **ibm.com**/developerworks/mydeveloperworks/files/app/file/110ccd08-25d9-4932-9bcc-c583868c9f31

[2] IBM X-Force 2011 Trend and Risk Report, IBM, 2012; **ibm.com**/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03012USEN&attachment=WGL03012USEN.PDF

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
June 2012

RAB14001-USEN-05