

Protecting citizen data using IBM Rational cybersecurity solutions

Help reduce security risks while providing online government services



Highlights

- Enables agencies to scan and test for common web application vulnerabilities to help reduce security risks
 - Supports compliance objectives with standardized reporting for common reporting needs
 - Helps reduce the risk and cost of enabling new services by identifying potential vulnerabilities in the development process
-

A digital, connected government helps simplify processes and makes access to government information more easily accessible for public sector agencies and citizens, which can result in a wealth of benefits, from improving citizen satisfaction and participation to reducing operational costs. Many agencies have initiatives in place to improve their government-to-citizen service model, but the same Internet technologies that are essential to achieving these objectives also open up areas of serious risk. In July 2009 the news cycle included stories about a series of coordinated cyber attacks that were launched against major government, news media and financial websites in South Korea and the United States. As 2010 came to a close, the world had become witness and victim to mounting cyber warfare where public and private entities were at risk. News headlines abounded on cyber attacks and vulnerabilities such as the Stuxnet virus, increasing cyber warfare and the Gawker breach.

Government agency systems are at risk from individuals, organizations, nations and “hactivist” movements looking for ways to wreak havoc either out of malice or simply to cause headaches. Internet threats continue to evolve as well, making compliance with security standards a constantly moving target. Governments need to stay on top of technologies that will enable them to enhance confidentiality, privacy and authentication, both to protect transaction data and citizen information from inappropriate disclosure or use and to ensure that citizens know and understand that they are protected. Furthermore, there has been increased concern over data security on social websites that may affect the military and information on troop movements, plans and private communications.

Many government agencies are aware of the increased need for security; however, they may have challenges executing the necessary steps to protect their infrastructure. Government IT departments, like just about all other areas of government, are facing lower budgets and constrained resources. Agencies need to find ways to maintain the stability and security of their existing systems while creating the next generation of cost-effective, smarter solutions.



IBM Rational® software provides the tools to create these new applications and manage development costs while helping to reduce security risks.

Identifying vulnerabilities to manage risk

Generally speaking, a vulnerability is anything in your computer system that may result in a weakening or breakdown of the confidentiality, integrity or accessibility of the computing system. Over time, the industry has identified thousands of vulnerabilities to computing systems. According to the *IBM X-Force 2010 Mid-Year Trend and Risk Report*, “Web application vulnerabilities continue to be the most prevalent type of vulnerability affecting servers today. ... The number of Web application vulnerabilities continues to climb at a moderately steady rate of 3,000 to 4,000 disclosures per year.”²¹

As you create new online services, it would be ideal if all software used in your applications were developed and tested for security vulnerabilities at each phase of the software

development life cycle (SDLC), but the time and costs to do so can be prohibitive. And unfortunately, hackers regularly demonstrate their ability to circumvent security controls by finding and exploiting new vulnerabilities. Having software tools in place to help analyze vulnerabilities in your services can relieve some of the pressure.

IBM Rational AppScan® software provides web application security vulnerability scanning, testing and reporting. It automates vulnerability assessments for a broad set of technologies including Asynchronous JavaScript and XML (AJAX), Adobe® Flash software, and web services. It provides customization and extensibility for the open source community, advanced remediation recommendations, and a Pyscan framework for penetration testers. Assessments are designed to make organizations aware of problems in advance and to help establish a prioritized road map to address discovered security vulnerabilities.

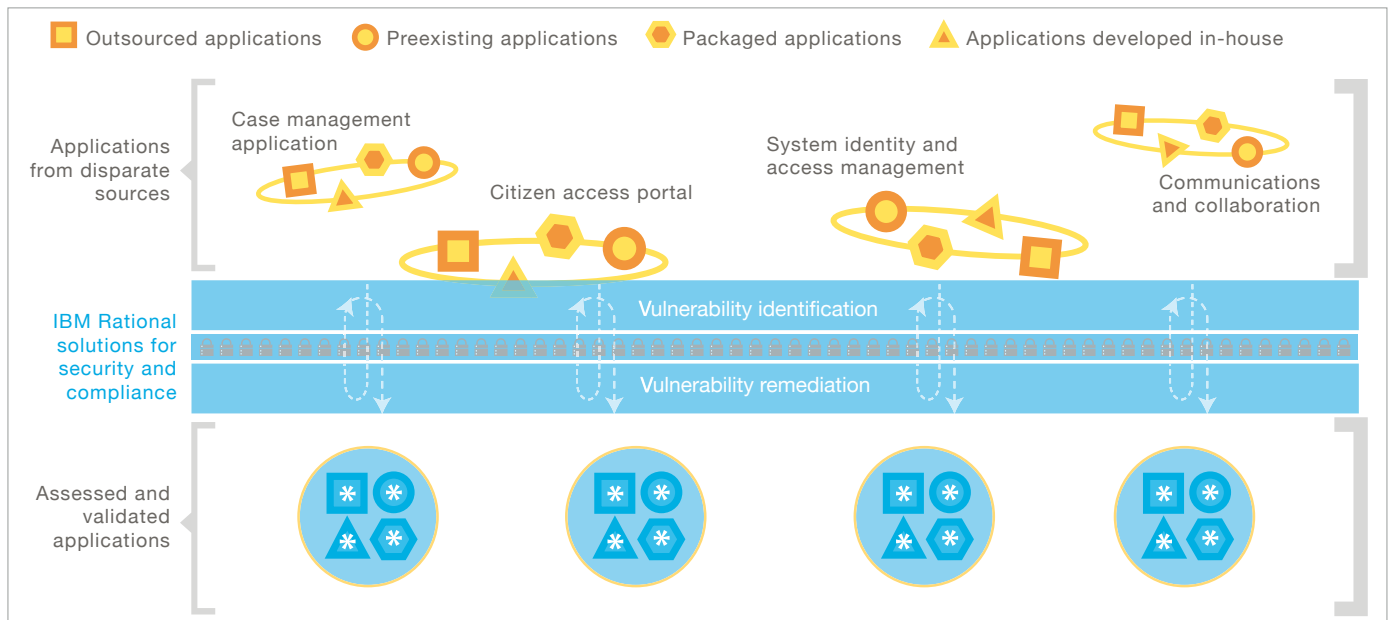


Figure 1: Rational solutions for security can help you manage potential vulnerabilities across your application infrastructure.

Automating compliance tasks to reduce workload

To maintain the public trust and address regulatory obligations, you need the ability to demonstrate that you have taken reasonable steps to safeguard your systems. But performing these assessments consistently and cost-effectively requires significant effort. Automation can help alleviate that burden.

IBM Rational Policy Tester™ software helps organizations reduce their online risk and exposure by identifying issues that affect website compliance and usability. Inventory and privacy reports help you determine the makeup of your site and whether you are adhering to posted privacy policies. From an analysis perspective, IBM Rational website compliance solutions automate content scanning to facilitate compliance with privacy, accessibility and key industry regulations, such as the Sarbanes-Oxley Act, as well as internal web quality standards.

To ease the burden of reporting, Rational AppScan software includes more than 40 standardized regulatory compliance reports, including reports for the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST), the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA) and many others. Rational Policy Tester privacy reports can help support compliance requirements for the Safe Harbor Act, Section 208; Sarbanes-Oxley; HIPAA, the Gramm-Leach-Bliley Act (GLBA); the Children's Online Privacy Protection Act (COPPA) and others.

Managing the life cycle to control costs

If you're building your own applications, reducing vulnerabilities early in the life cycle may be one of the best ways to help optimize security and reduce development costs. Assessing applications during the development phase can be an ideal way to reduce vulnerabilities and to simplify the assessment and reporting process later on. IBM Rational software development

tools work in conjunction with Rational AppScan and Rational Policy Tester software to help you design, develop and deliver security-rich software and systems that address the needs of your citizens.

For organizations that may not have internal web application security and compliance expertise, IBM can deliver Rational AppScan and Rational Policy Tester functionality as a full-service, turnkey, software-as-a-service (SaaS) offering that is hosted, managed and run for you by IBM Rational experts. We can explain results and findings in detail and guide you through the remediation process. SaaS is designed to provide a low-cost, fast-time-to-value alternative to licensed software.

Why IBM?

IBM is one of the only vendors in the marketplace today that can address virtually the entire spectrum of IT security and risk. IBM is trusted by thousands of organizations worldwide to reduce their risk exposure across the business—including its people, data, applications, network and endpoints, and physical infrastructure. With IBM Rational software, we can help you build security into the fabric of your infrastructure to help you better protect data and address regulatory compliance requirements for applications and websites. And with automated regulatory report generation, you can spend less time on your compliance obligations and more time on making your services smarter and your citizens more satisfied.

IBM Rational solutions can help protect government agencies from the increased security risk exposure caused by the online delivery of government services. IBM Rational software can help you build security into the fabric of your infrastructure to help better protect data and address regulatory compliance requirements for applications and websites. IBM is well positioned to help you safeguard your infrastructure because it is one of the only vendors in the marketplace today that can address virtually the entire spectrum of IT security and risk.

For more information

To learn more about IBM Rational security solutions for the government sector, contact your IBM sales representative or IBM Business Partner, or visit:

ibm.com/rational/solutions/government

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



© Copyright IBM Corporation 2010

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

Produced in the United States of America
December 2010
All Rights Reserved

IBM, the IBM logo, ibm.com, Rational, AppScan, and Policy Tester are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

¹ IBM, *IBM X-Force 2010 Mid-Year Trend and Risk Report*, August 2010.



Please Recycle
