*Application security and compliance solutions*
*To support your business objectives*

Rational. software

# Protect your business with a security and compliance solution for financial services organizations from IBM.

## Highlights

- ***Helps identify and remediate vulnerabilities in Web applications and services before they are deployed***
- ***Includes static analysis security testing that enables you to identify vulnerabilities within your source code as it's being developed***
- ***Supports your efforts to comply with a number of common financial services regulations***
- ***Improves Web application scanning coverage and improves developer and tester productivity through automation***
- ***Helps reduce risks and lower costs related to compliance with industry regulations***

It's a disaster waiting to happen. At the same time that financial services organizations are becoming more reliant on Web technology to deliver innovative features and services to their customers, hackers are increasingly targeting Web applications. According to a recent IBM Internet Security Systems X-Force® research and development team report, 50.4 percent of all vulnerabilities disclosed so far in 2009 are Web application vulnerabilities.[1] Undetected vulnerabilities in Web applications or Web services can leave organizations at risk of security breaches from external or even internal sources.

And network security measures such as firewalls and intrusion detection systems don't address the risks presented by vulnerable Web applications, which often expose valuable and confidential back-end resources, such as customer databases.

Unfortunately, these aren't the only issues financial services organizations are facing. Compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act can be a challenge.

> *"Despite the enormous number of attacks and despite widespread publicity about these vulnerabilities, most Web site owners fail to scan effectively for common flaws and become unwitting tools used by criminals to infect the visitors who trusted those sites to provide a safe Web experience."*[2]
>
> *— The SANS Institute*

You need to find a cost-effective way to protect your organization's systems, applications, private data and customer information, while supporting compliance with applicable regulations. If you fail to protect your valuable data and adhere to regulations, the consequences to your bottom line and your brand can be devastating. The consequences range from heavy financial penalties and lost revenue to system outages that can and will most likely erode customer confidence and damage your organization's reputation. To avoid these scenarios, you need to have a comprehensive security and compliance strategy in place.

**A comprehensive security and compliance solution for Web and networked applications**

The IBM Rational® AppScan® portfolio provides comprehensive security and compliance capabilities for complex Web and networked applications. Rational AppScan software scans and tests for common Web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification. Rational AppScan software shares 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™ languages, coupled with comprehensive support for the asynchronous JavaScript and XML (AJAX) programming language.

IBM Rational AppScan Source Edition software provides static analysis security testing that enables you to identify vulnerabilities within your source code, review data flows and identify the threat exposure of each of your applications—during development. By managing your security policies, you'll have the ability to take action on priority vulnerabilities. By testing your applications as they're being developed, you can gain an understanding of your threat exposure at the executive level for audit and compliance purposes and throughout the software development lifecycle. You can also address vulnerabilities earlier, which can help reduce costs. The Rational AppScan portfolio enables you to deploy application security testing—using both dynamic and static analysis techniques—that is integrated across the software delivery cycle.

### Providing support for your compliance efforts

The Rational AppScan offerings include reports to help your organization track its compliance with key industry and regulatory requirements, including the PCI DSS, COPPA, GLBA, Sarbanes-Oxley Act, Freedom of Information and Protection of Privacy Act (FIPPA) and Payment Application Best Practices (PABP). Plus, users can produce custom security reports and select which data points should be included in each report, making it possible to address critical compliance requirements. Using these features, you can provide assurance to your customers that their valuable data is protected.

### Enabling you to do more with less

Consumers expect the most convenient and innovative applications and services. To be able to deliver them—and deliver them quickly—you have to find a way to become more efficient. By automating your security and

compliance testing, you can free your developers and testers for more value-generating tasks. Which means your organization will be better positioned to focus on innovation.

### Reducing costs and improving scan coverage using automation

Your organization likely already has governance policies designed to ensure that your Web sites comply with relevant legislation. However, the size of today's Web sites—which can include thousands of pages—combined with an increasing volume of rules and updates, makes manual compliance checking far too time consuming and expensive to be feasible. Nor can visual checks reveal all potential security flaws and vulnerabilities. Support from automated scanning tools that can quickly check and monitor complex Web sites is a necessity for organizations that need to reduce their exposure to security vulnerabilities. Automated support can yield other benefits as well, such as fewer technical support requests, fewer abandoned Web sessions and greater consumer trust in your online channel. Collectively, these changes help boost confidence in your brand and improve customer retention.

*Challenge*

*One company needed to create security-rich applications that could handle the clearance and settlement of more than US$1 quadrillion in securities transactions per year. With such a large amount of money at stake, the company needed to be able to implement rigorous security practices as part of its application development process.*

*Solution*

*The company educated its application developers on building security into the Web application development lifecycle, using Rational AppScan offerings to identify, analyze and remediate security issues from early development through live deployment.*

*Benefits*

*The company is now able to perform automated security, compliance and integration testing on its Web-based applications, while adding roughly 225 new applications per year, improving its developer productivity and speeding time to market for new applications.*

### A marketplace-leading suite of security and compliance solutions

The IBM Rational AppScan suite of marketplace-leading Web application security and compliance applications can help address the critical challenge of application security and compliance. All of the solutions provide scanning, reporting and fix recommendation functionalities. And they're all designed to be efficient and easy to use. So whether your people are just getting started with Web application security or are advanced users who can create custom add-ons to extend your company's testing capabilities, they'll be able to take advantage of the Rational AppScan portfolio.

### End-to-end Web application security made easier by IBM

You need an integrated solution from a trusted vendor that provides a holistic and cost-effective approach to IT security. IBM offers a security solution that can help you reduce risk for Web-enabled applications, Web sites and Web traffic, while protecting your service-oriented architecture (SOA) environments.

- ***Discover application vulnerabilities*** *and how to fix them using IBM Rational AppScan software.*
- ***Help protect applications from potential attacks*** *with IBM Proventia® Web application security software.*
- ***Protect XML and Web services traffic, as well as SOA deployments,*** *with the IBM WebSphere® DataPower® SOA Appliances.*
- ***Help ensure that only authorized users have the appropriate access to Web applications*** *with IBM Tivoli® Access Manager software.*

## Why IBM?

Your business is only as secure as the applications that support it. By combining software and hardware solutions with professional and managed services, IBM can help your organization adopt a comprehensive approach to Web application security. The considerable benefits of Web application security solutions from IBM include:

- *Reducing the risk of Web application outage, defacement or data theft.*
- *Improving your ability to address compliance requirements.*
- *Protecting your brand and reputation.*
- *Enhancing your ability to integrate business-critical applications.*
- *Lowering long-term security costs by focusing on building security features into application development and delivery, instead of retrofitting them after the fact.*

## For more information

To learn more about IBM Rational security and compliance solutions for the financial services industry, contact your IBM representative, or visit:

**ibm.com**/software/rational/solutions/financial

To learn more about solutions for comprehensive application security from IBM, visit:

**ibm.com**/security/application-process.html



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

Produced in the United States of America
December 2009


---

1 IBM Global Technology Services, *IBM Internet Security Systems™ X-Force® 2009 Mid-Year Trend and Risk Report*, August 2009.

2 The SANS Institute, "The Top Cyber Security Risks," (http://www.sans.org/top-cyber-security-risks), September 2009.

RAS14037-USEN-00