



Watchfire AppScan Enterprise

Strategically integrate application security throughout the software development lifecycle

For chief information security officers (CISOs), now is the time to tackle the challenge of Web application security. While they recognize that integrating application security testing early in the software development lifecycle is critical to success, they struggle to find solutions that are both accessible and able to close the security knowledge gap for nonsecurity professionals like quality assurance (QA) teams and developers. What CISOs need is a solution that helps accelerate the adoption of security testing throughout the software and systems development lifecycle.

A Web-based, multiuser application security solution

Many organizations utilize manual testing or tactical desktop tools to manage Web application security, but too often these approaches overburden security resources and become organizational bottlenecks. Forward-thinking organizations are quickly adopting the strategic, enterprise approach of Watchfire AppScan Enterprise software. Built on Watchfire's leading AppScan technology, AppScan Enterprise is a Web-based, multiuser system designed to manage Web application security across organizations. AppScan Enterprise can provide users with:

- **Complete application coverage.** The processing power of the server-based scanning engine allows you to test Web sites with thousands of applications, analyzing multiple applications simultaneously.
- **Comprehensive reporting and issue management.** The robust, database-driven reporting engine can automatically aggregate scan results, creating a central repository of data that accommodates multiple views and ongoing analysis.
- **Visibility and control.** The enterprise-wide consolidation of data allows executives to see

the security status of all scanned applications and make more informed decisions about resource allocation, bug-fix prioritizations and employee training needs.

- **Better asset protection.** The AppScan Enterprise comprehensive approach to Web application security helps ensure that vulnerabilities will be found and fixed before applications are publicly released.

Accelerated adoption of application security throughout the software development lifecycle

AppScan Enterprise now extends its utility to include integrated computer-based training and a new point-and-shoot testing tool called QuickScan to accelerate the adoption of security testing by QA and development teams. QuickScan is a simplified scanning method that shields busy developers from the complexities of application security. Requiring no installation or configuration at the desktop, QuickScan relies on administrator-defined scan templates. Developers simply point QuickScan at their application and shoot. The results are delivered in the form of a developer task list, making it easy for nonsecurity professionals to focus on fixing the offending code.

Centralized control, scalability and enterprise-wide visibility

AppScan Enterprise analyzes Web sites by running thousands of platform- and application-specific tests to detect hundreds of types of vulnerabilities. The solution has the unique ability to scan and test Web sites containing a multitude of applications. It does so simultaneously and stores the results in an enterprise-class database that can generate interactive Web-based reports. It incorporates sophisticated security algorithms and combines them with enterprise scanning, reporting and trending capabilities to provide a uniquely strategic approach to Web application security management.

BENEFITS

- Enables centralized control of Web application testing across the organization
- Helps increase application testing coverage by involving more development stakeholders
- Provides enterprise-wide visibility of your application security posture
- Helps ensure that defects are identified and fixed before applications are publicly released
- Provides comprehensive support throughout the software development lifecycle





AppScan Enterprise is used to extend application security testing throughout the software development lifecycle.

AppScan Enterprise centralized control	
Features	Benefit
Granular access controls to help manage reports and scan permissions	Enables security teams to monitor and control Web application vulnerability testing across the organization
Administrator-defined scan templates to help control scan parameters	
Interoperability with AppScan licenses, enabling you to control scanning rights at the desktop level	

AppScan Enterprise scalability	
Features	Benefit
Web-based architecture to easily distribute report access and scan permissions across the software development lifecycle	Increases application testing coverage by affording the involvement of more software development lifecycle stakeholders
Capabilities to simultaneously analyze multiple applications across the enterprise	
Features that allow you to retest multiple Web applications frequently	

AppScan Enterprise enterprise-wide visibility	
Features	Benefit
Consolidation capabilities to gather all test results in one repository of application security data	Allows you to truly understand your application security posture across the enterprise, instead of in silos
Integration with third-party vulnerability testing tools, including Fortify software	
Capabilities to segment and trend vulnerabilities by business unit, geography, third-party provider, etc.	
Features that afford the creation of executive-level dashboard reports for management oversight	

Unique remediation workflow

Unlike alternative application security tools that overwhelm users with unactionable data, the Watchfire AppScan solution is designed to

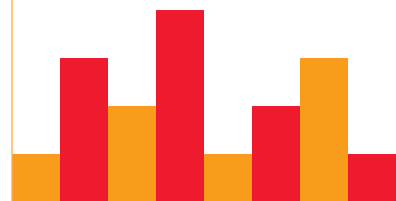
uncover security flaws and help you fix them. AppScan Enterprise incorporates features that allow you to evaluate, understand and resolve issues.

AppScan Enterprise remediation workflow	
Features	Benefit
Advisories, fix recommendations and educational material written in language nonsecurity professionals can understand provided with all reported security issues	Helps security teams ensure that all defects identified during a scan are remedied before the application moves into production
Issue management that lets you classify security issues as “open,” “in progress” or “closed,” providing a convenient means to focus and fix your most critical issues	
A developer task list report to help improve developer productivity by identifying the exact items within the application that need to be fixed	
A Web-based architecture that efficiently facilitates communication of issues and how to address them across the organization	

Deployment options

AppScan Enterprise is also available as a managed service to help you take advantage of product benefits while avoiding extra costs. This option provides value for those who are interested in managing Web application security at the enterprise level, but who prefer not having to purchase, install or upgrade hardware. As a

managed service, the AppScan Enterprise service offering includes a dedicated AppScan Enterprise administrator and security expert to help you manage your Web application vulnerabilities. All that is required from you is an Internet connection and defined user permissions.



© Copyright IBM Corporation 2007

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

Produced in the United States of America
07-07

All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both.

AppScan, Watchfire and the Watchfire Flame logo are trademarks or registered trademarks of Watchfire Corporation in the United States, other countries or both. Watchfire is an IBM company.

Other company, product and service names may be trademarks or registered trademarks or service marks of others.

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.

Customers are responsible for ensuring their own compliance with various laws and regulations. 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 regulations that may affect the customer's business and any actions the customer may need to take to comply with such laws and regulations. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

This publication contains other-company Internet addresses. IBM is not responsible for information found on these Web sites.

Why IBM and Watchfire?

A leading provider of Web application security software, Watchfire, an IBM company, offers clients a complete solution that includes intelligent fix recommendations to evaluate, understand and resolve their security issues. More than 800 enterprises and government agencies — including global financial services, communications and high-tech companies — rely on Watchfire products to help them identify, report and remediate security vulnerabilities.

For more information

To learn more about Watchfire AppScan Enterprise software, contact your IBM Watchfire representative or visit:

www.watchfire.com/products/appscan/appscanenterprise.aspx