

AppScan® Reporting Console

A Web-based Application Security Management and Reporting Solution

Web applications are regularly a point of weakness for enterprise IT, yet secure application development has continued to prove elusive for many companies. Security teams, for the most part, lack visibility and control over their enterprise web application security posture, and are grappling with how best to increase application security awareness throughout their organization.

Watchfire's AppScan® Reporting Console is the industry's first web-based, multi-user solution to aggregate vulnerability data and provide scalable report access across the enterprise. As a centralized, web-based management and reporting solution, AppScan Reporting Console provides the ideal mechanism for communicating application security information to non-security professionals such as the Quality Assurance (QA), development and management teams.

AppScan Reporting Console is fully integrated with AppScan, the worldwide market-share leading web application security assessment software (according to Gartner and IDC). Backed by an enterprise-class database, AppScan Reporting Console consolidates scan results from multiple AppScan clients, creating one centralized application vulnerability repository. The product also provides granular controls for security teams, who can use AppScan Reporting Console to set both the scan permissions of AppScan desktop installations, and set role-based access permissions to reports. And, because AppScan Reporting Console is web-based, scan results can be easily distributed to QA and development teams without requiring the installation of additional desktop software—critical for companies looking to facilitate the communication of security issues and how to fix them across the organization.

A unique feature of AppScan Reporting Console is its built-in Issue Management functionality. Issue Management allows users to filter and prioritize security issues, thereby providing a convenient means to focus and fix the most critical issues first. As well, Issue Management establishes a critical feedback mechanism between the development and security teams by allowing users to classify security issues as “Open,” “In Progress,” and “Closed.” This visibility into issue status ensures that all defects identified during a scan are remedied before the application moves into production. For those companies utilizing their own bug tracking system, AppScan Reporting Console integrates seamlessly with Mercury's Quality Center, Rational and Bugzilla.

AppScan Reporting Console Overview

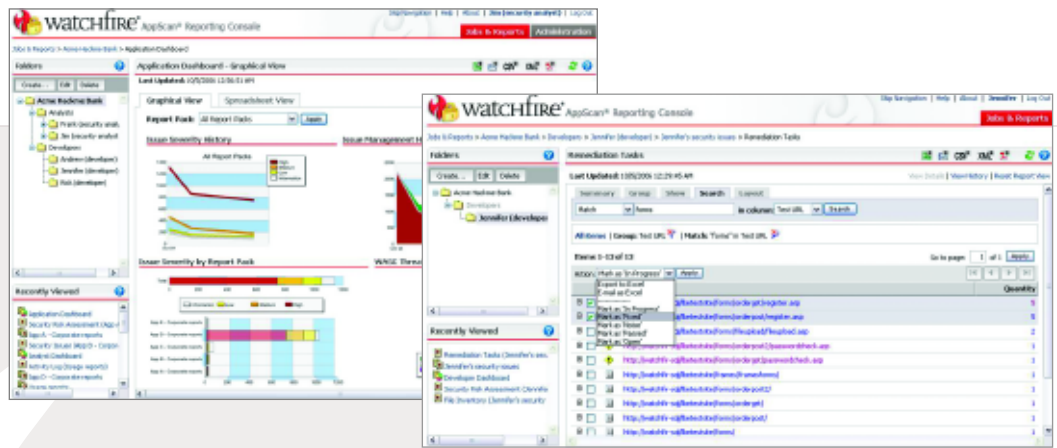
- **Visibility & Control:** Through full integration with AppScan at the desktop, AppScan Reporting Console helps companies consolidate scan results and create a central repository of web application vulnerabilities.
- **Flexible Web-based Reporting:** With AppScan Reporting Console, users can easily distribute vulnerability results to different stakeholders – including QA and development teams. This approach is faster and less expensive than alternatives.
- **Multiple Dashboards for Multiple Users:** AppScan Reporting Console gives individuals the ability to slice and dice security data in the most meaningful ways for their business. Vulnerabilities can be viewed by application, business units, geography, third-party provider, etc.
- **Built-in Issue Management Functionality:** AppScan Reporting Console facilitates more efficient resolution of vulnerabilities through its built-in Issue Management, which lets the user

APPSCAN REPORTING CONSOLE HIGHLIGHTS

- **Web-based:** zero footprint client
- **Enterprise Architecture:** built from the ground-up to easily scale and accommodate enterprise-wide use
- **Enterprise Database:** MS SQL Server
- **Interoperable with AppScan:** import scan results and set scan permissions of any AppScan instance
- **Interoperable with Fortify Software's SCA Suite:** import scan results from Fortify Software, then correlate white box/black box security issues
- **API:** integrates with other third-party systems including Mercury, Rational and Bugzilla

WATCHFIRE

880 WINTER STREET
WALTHAM MA 02451
TEL: 781 810-1450
FAX: 781 890-2087
www.watchfire.com



filter and classify security issues, and prioritize which web application vulnerabilities to fix first.

- **Integration with Existing QA Solutions:** AppScan Reporting Console can integrate with Mercury's Quality Center, Rational and Bugzilla.
- **Role-based Access and Scan Permissions:** AppScan Reporting Console provides granular control over who can access sensitive vulnerability data by facilitating role-based access permission to reports. In addition, AppScan Reporting Console can be used to set the scan permissions for any AppScan instance.

Brings Order to Growing Application Security Efforts

AppScan Reporting Console is the logical next step for companies already aware of the importance of application security, and already investing in AppScan licenses.

- Companies make an initial investment in application security assessments by deploying multiple AppScan seats.
- AppScan Reporting Console is then used to consolidate all scan data generated from the multiple desktop installations, and streamline the management and remediation of those issues.
- Companies that continue to increase their number of deployed web applications eventually mature to Watchfire's AppScan Enterprise product, which provides both web-based application security testing functionality, as well as the web-based reporting and management functionality of AppScan Reporting Console.

System Requirements

- Processor: Pentium III PC, 800 MHz
- Memory: 512 MB RAM (1 GB recommended for scanning large sites)
- Free Disk Space: 1 GB
- Network: 1 NIC 10/100 MBPS for network communication with configured TCP/IP (100 Mbps recommended)
- Operating System: Windows 2000 with SP2 or higher, Windows XP, Windows 2003 Enterprise Edition
- Internet Explorer 5.5 or 6.x
- Microsoft .Net Framework version 2.0
- JRE 5.0 (for Watchfire HTTP Proxy only)

About Watchfire

Watchfire is the leading provider of web application vulnerability assessment software and the only company to offer an end-to-end solution including intelligent fix recommendations to evaluate, understand and resolve issues. More than 800 enterprises and government agencies, including AXA Financial, SunTrust, HSBC, Vodafone, Veterans Affairs and Dell rely on Watchfire to identify, report and help remediate security vulnerabilities. Watchfire has been the recipient of several industry honors including: winning an unprecedented three out of five 2007 SC Magazine Excellence Awards (including Best Security Company); the HP/IAPP Privacy Innovation Award; Computerworld's Innovative Technology Award; finalist for the pending Dr. Dobb's 2007 Jolt Product Excellence Awards; and "Recommended" rating by Computer Reseller News. For two years in a row, Watchfire has been named by IDC as the worldwide market share leader in web application vulnerability assessment software. Watchfire's partners include IBM Global Services, Fortify, PricewaterhouseCoopers, Sapient, Microsoft, Interwoven, EMC Documentum and Mercury. Watchfire is headquartered in Waltham, MA. For more information, please visit www.watchfire.com

