Your Web site is a portal into your corporate data. Isn't it about time you protect it?

While Web sites streamline access to information, they are vulnerable, potentially exposing critical corporate information and consumer data, or otherwise compromising enterprise IT.

Online security breaches can lead to a number of damaging consequences. Many federal and state laws require companies to disclose when customer information has been compromised, and some industry groups recommend or require periodic assessments of Web application risks.

Hackers can compromise vital corporate data, or they can use corporate Web sites to take over the computers of your Web site visitors. Vulnerabilities can lead to bad press, resulting in negative impressions, eroded brands and lost business—or, in the most extreme cases, the demise of your Web site. Executives need to understand these risks and put processes and technology in place to recognize, audit for and rectify these online issues.

Watchfire®, an IBM company, can help. Watchfire software is designed to establish a process for incorporating Web application security into the entire application development lifecycle. By automating manual processes and identifying and prioritizing issues for immediate remediation, Watchfire solutions have helped companies drive significant cost out of their online operations. These same solutions can work for your company.

Products overview

Watchfire products include Watchfire AppScan®, a desktop Web application security testing tool; Watchfire AppScan Enterprise, an enterprise Web application security management solution; and Watchfire WebXM™, an enterprise online risk management platform.

Watchfire AppScan software

Watchfire AppScan helps manage Web application security throughout the software development lifecycle. Named a worldwide marketshare leader, AppScan offers a timesaving solution for all types of security testing—outsourced, desktop user and enterprisewide analysis—and for all types of users—application developers, quality assurance (QA) teams, penetration testers, security auditors and senior management.

The advanced remediation recommendations provided by the AppScan solution deliver unmatched accuracy and efficiencies for developers and security auditors. And the software's comprehensive compliance reporting functionality can help users address compliance with internal security best practices and help reduce business risk.

The AppScan Reporting Console is the perfect addition to a multiseat AppScan license. It enables users to consolidate Web application vulnerability data into one centralized location to better control who has access to sensitive data. And because

AppScan Reporting Console is Web based, you have the flexibility to both create multiple dashboards for multiple users, and easily distribute reports to QA and development teams without requiring additional desktop software.

Watchfire AppScan Enterprise software

Watchfire AppScan Enterprise is a Web application vulnerability scanning and reporting solution for the enterprise. For those intent on centralizing Web applications security testing, AppScan Enterprise provides advanced application scanning, remediation capabilities, executive security metrics and dashboards, key regulatory compliance reporting, and seamless integration with the desktop version of AppScan.

By speeding up security testing and providing reports to those who need them, the AppScan Enterprise solution can increase your security team's productivity. And in addition to catching security issues earlier in the development lifecycle, AppScan Enterprise provides centralized control and visibility through access permissions, high-level reports and trending metrics. It also monitors applications that have been deployed to your live site to protect against new threats.

Watchfire WebXM software

Watchfire WebXM is an automated online risk management solution that audits quality, privacy, brand, accessibility and compliance issues across corporate Web properties. WebXM can help your organization with:

- **Consumer data privacy.** Improve the accuracy and reliability of online privacy assessments by using WebXM for privacy policy management, personally identifiable information (PII) discovery, leak prevention and compliance audits.
- **E-government compliance.** Identify Office of Management and Budget (OMB) compliance risks and increase the efficiency of agency governance procedures for compliance.
- **Banking compliance.** Manage compliance issues associated with federal consumer protection requirements including the Equal Credit Opportunity, Truth in Lending and Truth in Savings acts.
- **Site quality and accessibility.** Uncover issues affecting site quality such as spelling errors, broken links and deep content. WebXM can also perform accessibility checks to improve access for all.
- **Content migration and consolidation.** Analyze Web content and usage prior to migrating to a new site or platform. WebXM can also perform a Web site inventory of servers and technologies to help avoid conducting a manual audit.

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 the Watchfire family of products, contact your IBM Watchfire representative or visit:

www.watchfire.com/products
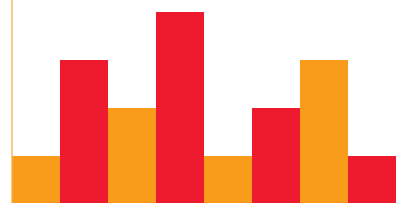
© Copyright IBM Corporation 2007

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.