IDC VENDOR SPOTLIGHT

Australia, March 2009

Benefits of IBM Rational AppScan

Sponsored by IBM

> "The need for web application security has never been greater. There are 1.4 billion people who have access to hundreds of millions of websites generating US$6.9 trillion in worldwide Internet eCommerce. Most of those websites are potential cash machines for attackers. Some estimates are that over 80% of websites have at least one serious vulnerability. IDC research indicates that at least 25% of all enterprises have been exploited through a web application flaw. A majority of websites also have hosted malicious content or contained a masked redirect to a malicious site. To uncover and remedy these vulnerabilities, organisations turn to web application vulnerability assessment products, such as IBM's Rational AppScan. For nearly a decade, AppScan has been at the forefront of the market with technologically advanced solutions, and as the market's leading product."
>
> *Charles Kolodgy, Research Director, Secure Products, IDC*

A Web Application Vulnerability Assessment (WAVA) identifies mistakes in application logic, configurations and software coding that jeopardise the availability, confidentiality and integrity of data.

Overview

Using advanced websites, organisations continue to expand the use of the Internet for commerce. These sites are potentially exploitable because even the best developers can write insecure code. The more vulnerabilities there are, the greater the attack surface. The increasing number of threats make it more difficult to build secure websites. The only way to accurately discover vulnerabilities within custom web applications is to expose them to known classes of vulnerabilities. By performing a web application vulnerability assessment, underlying vulnerabilities can be found and corrected. Security testing tools alone do not make software secure, but as part of a software security program, they do help reduce the attack surface.

WAVA Market

- The WAVA market includes those products that are specifically designed to test the robustness of an application to resist both specific attacks and those based on hacking techniques. Application scanners concentrate on vulnerabilities associated with direct interaction with applications and encompass deployed applications, as well as those that review source code.
- The market generated A$277 million in worldwide revenue in 2007. The leading vendor, on the strength of its AppScan product, is IBM as a result of its acquisition of Watchfire in late 2007. The AppScan product has been the market leader for the past 3 years, commanding 14% of the worldwide market in 2007.
- Although relatively small in total revenue, the WAVA market is expected to grow at a very strong 28.7% Combined Annual Growth Rate from 2007 to 2012. By the end of the forecast period, IDC estimates that vendor revenue will be nearing a billion Australian dollars. IDC estimates that the Application vulnerability assessment's share of the total vulnerability assessment market will be 47% by 2012, up from 29% in 2007.

Vendor Profile

- Rational AppScan, the first commercially available automated web applications vulnerability assessment product, extends the security capabilities involved in web application development, testing, fielding, and maintenance. The tools are designed for developers, quality assurance testers and security professionals. The product is available in desktop and enterprise scalable formats and as a Software as a Service.
- Rational AppScan products provide:
  - Automated Web application scanning and testing for all common Web application vulnerabilities, such as SQL-Injection, Cross-Site Scripting, and Buffer Overflow.
  - Broad application coverage, including integrated Web services scanning, JavaScript execution (including Ajax), and parsing.
  - Advanced remediation capabilities, including a comprehensive task list necessary to fix issues uncovered during the scan.
- In addition to AppScan Standard Edition, the suite now includes Enterprise Edition, Developer Edition, Tester Edition, Build Edition, and Express Edition. Each is designed for a variety of enterprise sizes and users, including security managers, penetration testers, security auditors, application developers, build managers and quality assurance (QA) teams.

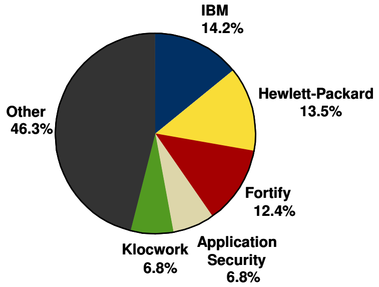
Conclusion

- Online outlaws are working overtime to exploit security holes they find in web applications. To ensure organisations can conduct online business with confidence, web application security is imperative. Vulnerabilities in custom web applications need to be discovered and resolved in the most efficient manner possible. IDC believes the best way to address software and application security in its entirety is to complement perimeter security with a software development lifecycle that includes security testing of the inner workings of applications. This would cover all applications, but is critical for web applications because of their outward focus.
- IDC believes organisations need to conduct security testing as part of the software development process. Vulnerabilities need to be uncovered and eliminated before a program goes live. Flaws and errors are much easier and much less costly to repair when found earlier in the process. Developers and quality assurance staff should be held responsible for security, not just functionality and quality. Scans also need to be performed on active websites to ensure they stay secure.
- Organisations cannot take a cavalier attitude towards web application security: there is too much at stake. Organisations must select WAVA tools that integrate with the software development lifecycle; uncover vulnerabilities associated with multiple attack methods; can handle both security- and policy-compliance issues; educate the user; and have central reporting capabilities.

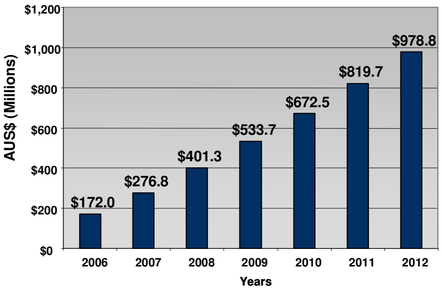
Source: Worldwide Security and Vulnerability Management Software 2008-2012 Forecast and 2007 Vendor Shares: Making Security Smart, IDC #214144

(Note: Australian Dollar Exchange rate on March 8, 2009: 1 USD = 1.56426 AUD)

Market Shares



Market Growth Forecast (CAGR 28.7%)



IDC
Analyze the Future

IDC VENDOR SPOTLIGHT

Australia, March 2009

Benefits of IBM Rational AppScan

Sponsored by IBM

Market Trends

- The industry has been moving to the realisation that finding and removing web application vulnerabilities should be part of the software development lifecycle process. When security is implemented early in development, and is a partner with performance and quality, it becomes easier to implement. Web application security requirements and coding techniques provide benefits beyond reducing vulnerabilities, such as enhancing code reliability, which should reduce maintenance and downtime costs.
- The WAVA market segment has expanded with additional vendors now offering services. Network vulnerability assessment vendors Qualys and nCircle, and network penetration testing vendor Core Security are providing WAVA capabilities. The expanding number of vendors illustrates that there is a demand and increasing budgets for this type of testing.
- Web application vulnerability testing was originally the purview of experts, but as demand has grown, the tools have had to become more accessible to all types of users. For example, Rational AppScan Tester Edition offers capabilities to help QA teams integrate security testing into existing quality management processes. Likewise, AppScan Express Edition meets the requirements of midsize organisations that need to consider security testing on a limited budget.
- Accuracy is critical. If an assessment tool produces a high number of alarms, many of which are false, those items need to be validated manually. Tools that are more accurate allow for a scaleable application testing process, reduce the number of people on the job, and improve remediation. Accuracy equals efficiency. IDC believes the success of a source-code assessment should be measured by the thoroughness of the analysis and the accuracy of the results.
- Today's scanners must address advanced Web 2.0 technologies. As such, WAVA products have continued to advance considerably, from the expansion of the classes of vulnerabilities tested, to the regulations covered. For example, AppScan automates over 2,000 security and compliance tests and can generate 44 out-of-the-box compliance reports. AppScan includes the ability to audit Adobe Flash applications. Effective WAVA products need to identify an application's complex business logic and be able to piece together a complete picture of the application. AppScan provides this with expanded Web Services code testing.

Market Accelerators

- Long gone are the days of websites being static electronic information brochures. Now they conduct critical business functions, such as brand loyalty, customer support, and ordering. Web 2.0 sites are delivered based on users' requests. Websites have become platforms for Web 2.0 content, supporting technologies such as RSS, social networking, multimedia collaboration and long-tail economics. Without automated vulnerability testing, it is extremely difficult to secure this level of website complexity and these sites are the most exposed.
- Attackers are profit motivated and are considerably technically savvy making it even more imperative that measures be taken to stop them. Today's attacker is out to take something, be it money, corporate secrets, or user data. With greater potential losses, web application security is an imperative, especially in difficult economic times when a data breach could result in costly fines or worse, the loss of customer confidence.
- Government and industry organisations are increasingly mandating that accessible personal and financial information be protected. The Payment Card Industry Data Security Standard's (PCI DSS) section 6.6 calls for either a review of all web application code developed, or the installation of an application-layer firewall to protect web applications. Additionally there is a move to require software vulnerability testing as a condition of sale. Organisations and governments are adding conditions to procurement documents mandating a minimum level of software security.

Competitive Landscape

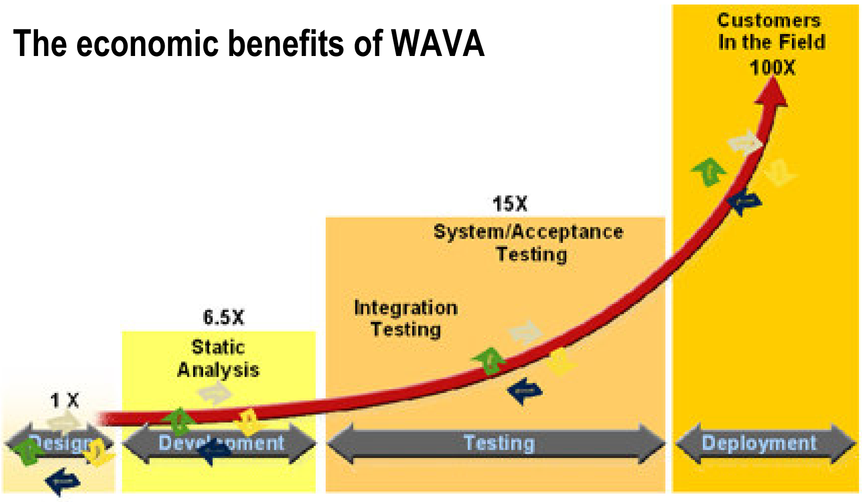
- Leading competitors in the WAVA market are IBM, Hewlett-Packard, Fortify, Application Security and Klocwork. Of these vendors the only two who have a focus on web security are IBM and HP. The other leading vendors in the WAVA market are not primarily focused on web security. Instead, their focus is on source code scanning and analysis or database vulnerability scanning. A company like Fortify usually partners with a web application vendor.

Challenges

- The greatest challenge is to break the inherent inertia against security testing. However the rising popularity and complexity of Web 2.0 applications coupled with a more dangerous threat environment raises the stakes. It is imperative that web application security be presented as an improvement to security, but also shown to enhance application functionality and reliability. In difficult financial times, people might be unwilling to pay for a new product. However they would be missing out on substantial benefits - web security, improved efficiency and reduced software maintenance costs in the development lifecycle - which will have a positive financial impact.

Source: Worldwide Security and Vulnerability Management Software 2008-2012 Forecast and 2007 Vendor Shares: Making Security Smart, IDC #214144

The economic benefits of WAVA



Source: IBM Systems Sciences Institute

Buggy software costs the US national economy $60 billion. Delivering quality applications to the market has become a mandatory requirement. The cost of fixing defects after deployment is almost 15 times greater than detecting and eliminating them during development.

An effective development process assumes that code will be attacked and embeds checks at every iteration and/or phase of the process. Iterative processes are better because they offer more touch/assessment points and allow for capture and remedy of security vulnerabilities early in the SDLC. Also, if something is missed in design, it can be caught in development.