Manage data security and application threats with a multi-tiered approach

IBM application security testing solutions and the IBM Security portfolio bolster preparedness

Highlights

- Proactively protect vulnerable applications
- Reduce the cost of remediating vulnerabilities by detecting them earlier in the development cycle and enhancing security awareness within organizations
- Actively monitor database transactions to help block attacks
- Facilitate effective incident response through enhanced real-time threat identification
- Effectively manage risk with integrated security for mobile, cloud and social media

Protecting valuable assets requires a layered security approach. Consider that when historic sites and museums implement security plans to protect priceless treasures, their plans go far beyond simply locking their doors at the end of the day. Rather, they employ a layered security approach that includes 24x7 security patrols, video cameras, visitor inspections and more. Thanks to numerous costly attacks on business-critical applications, IT organizations should adopt a similar layered security approach to protect their priceless digital data assets.

As attacks on data and applications have grown in frequency and sophistication, it has become obvious that no single security solution can provide complete protection against data breaches. At the same time, recent findings from the IBM® X-Force® team reveal that 33 percent of reported vulnerabilities are targeted at web applications[1]—with the greatest threats coming from cross-site scripting and SQL injections.[1] Of the top 100 paid applications, 97 percent of Google Android and 87 percent of Apple iOS applications have been hacked. Of the top 20 free applications, 80 percent of Android and 75 percent of iOS applications have been hacked.[2] Organizations everywhere, as a result, must find effective approaches to address continued threats posed by application-related attacks.

Many organizations are establishing application security programs that span the security auditor, software development and IT security manager domains. And given the highly visible and costly breaches that routinely occur, these security investments are justified. However, by adopting *secure-by-design* and risk management governance models, organizations can address security issues comprehensively.

Building a comprehensive security solution

The application security testing portfolio is a core component of IBM Security offerings. It includes advanced security testing capabilities and a platform for managing application risk, along with the expertise, critical application lifecycle management and secure integration options required to identify application vulnerabilities and reduce application risk. The application security testing portfolio includes:

On-premises solutions

- **IBM Security AppScan® Enterprise:** Enables organizations to mitigate application security risk and achieve regulatory compliance; security and development teams can collaborate, establish policies, scale testing, and prioritize and remediate vulnerabilities throughout the application lifecycle
- **IBM Security AppScan Source:** Helps lower costs and reduce risk exposure by identifying software vulnerabilities early in the lifecycle so they can be eliminated before deployment
- **IBM Security AppScan Standard:** Helps decrease the risk of web application attacks and data breaches by automating application security vulnerability testing

IBM Business Partner solutions

- **Arxan Application Protection for IBM Solutions:** Extends vulnerability analysis capabilities to mobile application hardening and runtime protection
- **Cigital Application Security Testing Managed Services:** Delivers flexible application security testing as a service model to map changing application portfolio; the offering is designed to mitigate security risks at scale across an application portfolio through actionable vulnerability insight, penetration testing and expert remediation provided by Cigital, a leading application security partner
- **IBM Security AppScan solutions for SAP:** Virtual Forge CodeProfiler for AppScan Source helps automate the analysis of SAP applications—for web portals and Advanced Business Application Programming (ABAP) applications—to identify security vulnerabilities and manage application risk

Cloud-based solutions

- **IBM Security AppScan Mobile Analyzer:** Helps secure mobile applications by detecting dozens of the most pervasive published security vulnerabilities
- **IBM Security AppScan Dynamic Analyzer:** Helps secure web applications deployed on IBM Bluemix™ by detecting published security vulnerabilities

Testing and analysis capabilities

Application security testing solutions from IBM provide dynamic and static application security testing, as well as innovative technologies such as glass-box testing and runtime analysis, to help users stay ahead of the latest threats and drive precise, actionable results.

Since no single automated analysis technique can detect all possible vulnerabilities, IBM has incorporated several different analysis techniques into the portfolio:

- **Static analysis** examines source code for potential vulnerabilities, facilitating detection of vulnerabilities earlier in the development cycle.
- **Dynamic analysis** tests running applications at later stages in the development cycle by probing them in a similar fashion as potential hackers might. This makes it easier for organizations to connect vulnerabilities with potential exploits.
- **Hybrid analysis** brings dynamic and static analysis together to correlate and verify results. It traces issues identified through dynamic analysis to the offending line of code and validates issues identified in static analysis with external testing.
- **JavaScript client-side analysis** analyzes code downloaded to the client. The more functionality the organization performs client-side, the greater the potential for client-side vulnerabilities and exploits.
- **Interactive analysis** places runtime agents on the application machine and analyzes applications as they are tested. By combining aspects of dynamic and static analysis at run time, organizations can detect more vulnerabilities with higher accuracy.

Complementary solutions

The following complementary IBM Security products integrate with the application security testing portfolio to meet specific security challenges:

- **IBM Security Network Intrusion Prevention System portfolio:** Protects business-critical applications from malicious threats
- **IBM InfoSphere® Guardium® portfolio:** Defends against potential database attacks
- **IBM Security QRadar® portfolio:** Improves visibility into threat detection and prioritization
- **IBM mobile security solutions:** Integrates the mobile application scanning capabilities of AppScan

Protecting business-critical applications from malicious threats

IBM Security intrusion prevention solutions combine detection and prevention capabilities to protect against vulnerabilities and help stop threats before they impact the business.

IBM Security SiteProtector™ System provides centralized management of IBM intrusion prevention solutions, including the ability to centrally define security policies and monitor detected events in real time. SiteProtector System is capable of receiving vulnerability information from AppScan, which it can correlate with web application attack events to show whether vulnerabilities are being actively exploited.

Defending against database attacks

InfoSphere Guardium monitors database activity with support for fine-grained auditing, automated compliance reporting, data-level access control, database vulnerability management and auto-discovery of sensitive data. Designed to prevent unauthorized or suspicious activities by privileged insiders and hackers, InfoSphere Guardium enables organizations to assess database vulnerabilities and configuration flaws, ensure that configurations are locked down after changes, and capture and examine transactions with secure, tamper-proof audit trails.

Improving visibility into threat detection and prioritization

IBM QRadar Security Intelligence Platform provides a unified architecture for integrating security information and event management (SIEM) data with log, flow, vulnerability, user and asset data—for near real-time correlation and behavioral anomaly detection to help identify high-risk threats.

IBM Security QRadar Vulnerability Manager delivers a unified view of vulnerability information integrated with security intelligence data and context. Integrated with AppScan, it provides visibility into application vulnerabilities including correlation with attacks, exploitability from potential threats or untrusted sources, and user activities—for improved incident response.

Integrating mobile application security testing capabilities

AppScan integrates with **IBM mobile security solutions** to enable effective management of potential security vulnerabilities on mobile applications and improve operational efficiency. IBM solutions effectively address the Open Web Application Security Project (OWASP) Top 10 Mobile Threats[3] on both Apple iOS and Google Android devices.

IBM MobileFirst™ Platform Foundation provides an open, comprehensive platform to build, run and manage HTML5, hybrid and native mobile applications. It can help organizations reduce application development and maintenance costs, improve time to market and enhance mobile application governance and security.

Why IBM?

The IBM security approach isn't based upon point solutions, but rather a comprehensive portfolio of security products and risk management capabilities that provide an integrated, holistic approach to security protection. IBM Security offerings are supported and enhanced by research from the elite X-Force team, which studies and monitors the latest trends in threat environments—including vulnerabilities, exploits, active attacks, viruses, other malware, spam, phishing and malicious web content.

For more information

To learn more about the IBM application security testing portfolio, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/applicationsecurity

For more information on other IBM Security offerings, please visit: **ibm.com**/security

To learn more about improving application security protection for mobile devices, download the IBM white paper, "What can you do differently to guard against threats from rapidly evolving mobile malware?" now.

[1] IBM X-Force, "IBM X-Force Threat Intelligence Quarterly, 1Q 2014," *IBM Corporation*, February 2014. https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov21294&S_TACT=102PW99W

[2] Arxan Technologies, "State of Mobile App Security: Apps Under Attack," November 2014. https://www.arxan.com/assets/1/7/State_of_Mobile_App_Security_2014_final.pdf

[3] Open Web Application Security Project (OWASP), "Top Ten Mobile Risks," *OWASP Mobile Security Project*, May 2013. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2015

WGS03006-USEN-02