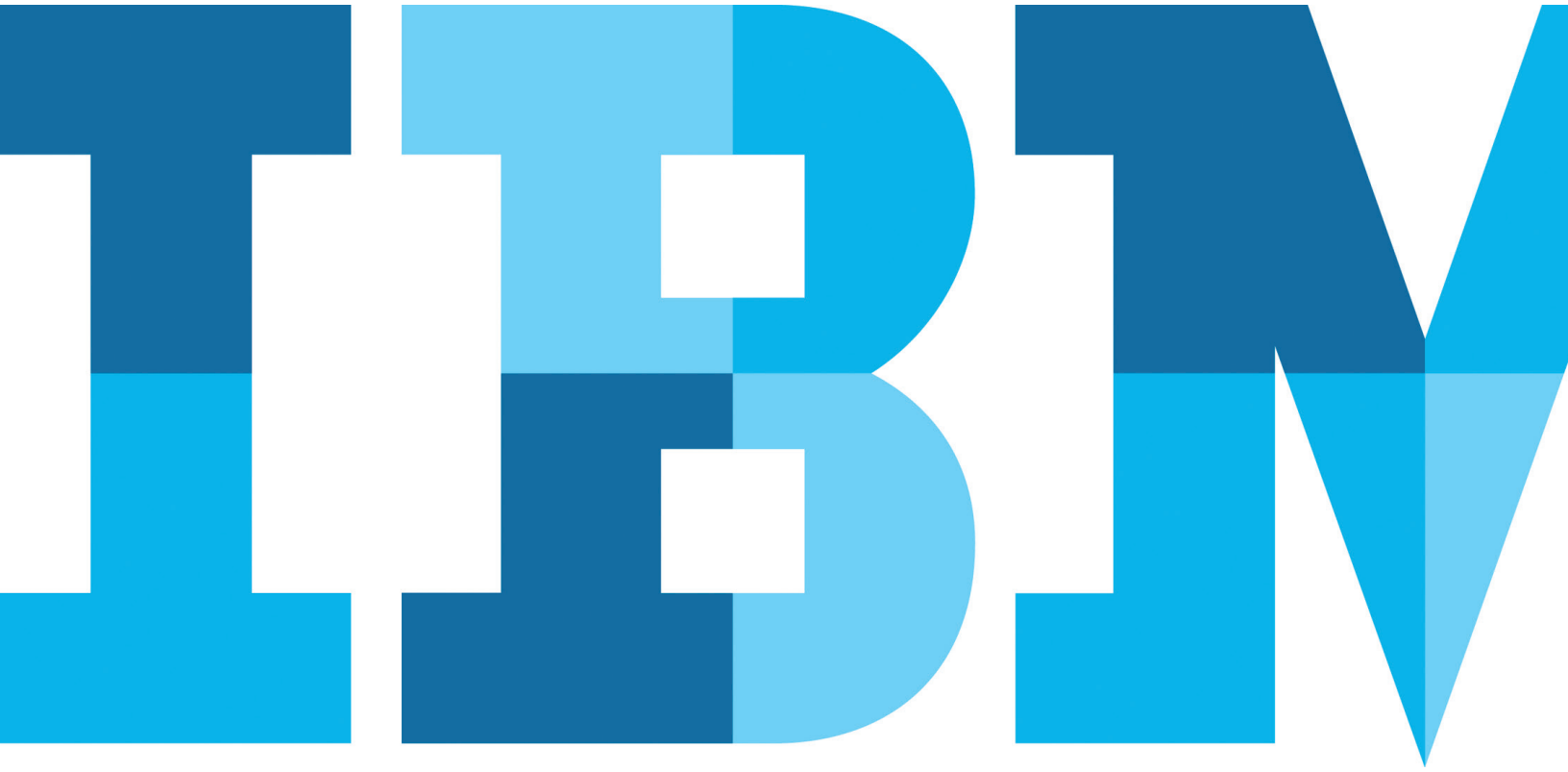
May 2018

Manage application security risks to help protect your organization's critical data

Comprehensive IBM application security testing solutions help identify vulnerabilities and reduce application risk



IBM

Making a case for application security

Many organizations use software applications to run critical business processes, conduct transactions with suppliers and deliver sophisticated services to customers. While organizations understand established security technologies for routine tasks such as networking and operations, many struggle with implementing, managing and maintaining effective application security programs. However, since applications can compromise security across the entire organization, securing them needs to become a top priority. And in today's increasingly sophisticated threat landscape, the bar must be raised to address each and every kind of threat.

The ramifications of under-secured applications can be dire. Security vulnerabilities during application development can give hackers the ability to destabilize applications and obtain unfettered access to confidential company information or private customer data. This type of data loss can lead to a damaged brand reputation, loss of consumer confidence, disruption of business operations, interruption of the supply chain, threat of legal action and/or regulatory censure.

Addressing application security can be quite challenging. Large organizations manage thousands of applications, and the task of ensuring their security typically falls on the shoulders of a small, overburdened security team.

To protect against any consequences, organizations like yours must enable risk-based application security management. You need solutions that can provide clear visibility across the infrastructure; identify and prioritize applications based on their business impact; assess applications for vulnerabilities; place vulnerabilities into context to determine their risk levels; and mitigate risk by implementing necessary fixes in code or deploying appropriate policies.

Adopting a strategy for managing application security

Many organizations fail to prioritize application security—leaving their entire environment at risk. According to a study conducted by the Ponemon Institute, only 25 percent of respondents rate their organization's ability to stop or curtail application security compromises and exploits as highly effective, and when it comes to security testing, only 44 percent of respondents test for vulnerabilities.[1] Another study shows that only 39 of respondents confess that their mobile applications are tested in production.[2] Are you apportioning your security budget appropriately to align with evolving security risks?

Effective security is really a matter of managing risk. It is imperative that you understand, manage and mitigate the risk to your most critical assets. To develop effective application security, be sure to:

1. **Build an asset inventory:** Know what your assets are and which ones are the most critical. Rather than trying to secure all your applications right away, it is important to focus on the most critical ones first.
2. **Assess the business impact:** After prioritizing your application assets, analyze them for vulnerabilities. Evaluate the risk posed by each application, based on its business impact and the severity of its vulnerabilities.
3. **Prioritize vulnerabilities:** Once you have a risk rating for each application, focus on the ones that present the highest risk, and address the most severe vulnerabilities first.
4. **Plan for remediation:** Mitigating risks can involve fixing coding errors, creating virtual patches via a web application firewall or, in some cases, even taking applications temporarily offline.
5. **Measure return on investment (ROI):** Various metrics can help you monitor your application security status and measure the effectiveness of your ongoing application security program. A recent study by a leading analyst firm revealed that an IBM client achieved a triple-digit ROI by implementing IBM® Security AppScan® Source.[3]

There are five key considerations in a risk-based approach to application security management.

Exploring integrated application security management from IBM

Running an application security initiative in a large organization can be a challenge. A small security team is often responsible for securing thousands of applications built by multiple development teams.

IBM provides integrated capabilities for application security management, enabling security teams to address the vulnerabilities they grapple with on a daily basis. The portfolio includes on-premises and cloud-based options, tailored to your specialized requirements.

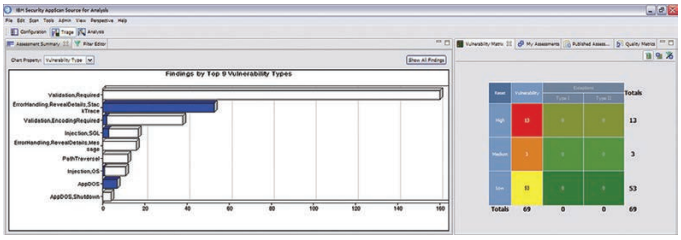
As described above, the most successful application security testing programs focus on mitigating risk. Organizations that are new to application security testing can justify the need for testing by conducting Dynamic Application Security Testing (DAST) on their most valuable applications to identify high-severity vulnerabilities. DAST also permits them to tackle the highest risks in the organization's application portfolio and quickly demonstrate success. Today, each organization must determine whether its primary concern is identifying and addressing its highest-risk application vulnerabilities, or establishing a secure coding culture and enforcing best practices. DAST can help developers improve secure coding practices over time and build a business case for application security testing. Static Application Security Testing (SAST) is often a more strategic effort intended to help enforce secure coding best practices and to eventually mitigate risk that exists in applications, as code quality improves.

On-premises solutions

IBM Security AppScan solutions offer components specially designed to benefit application security managers and development teams at organizations of all sizes. The on-premises offerings include:

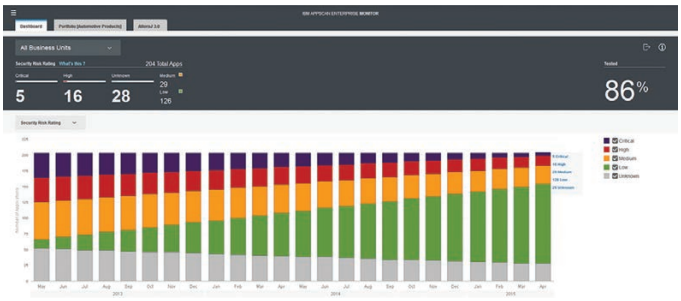
- **IBM Security AppScan Standard:** Helps decrease the risk of web application attacks and data breaches by automating application security vulnerability testing and leveraging advanced DAST capabilities

- **IBM Security AppScan Source:** Helps lower costs and reduce risk exposure by integrating SAST into DevOps automation for testing applications early in the development lifecycle, so they can be eliminated before deployment



AppScan Source software provides assessment summaries that map to application risk and provide insight into vulnerabilities that affect your applications.

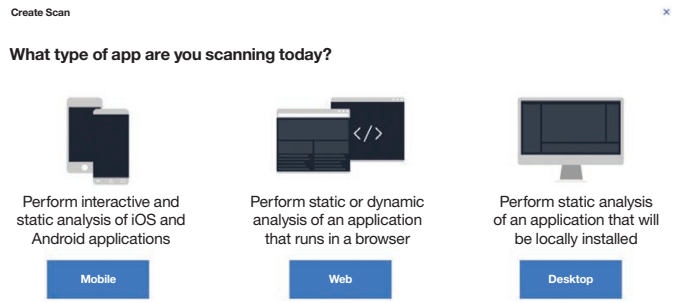
- **IBM Security AppScan Enterprise:** Enables organizations to mitigate application security risk and achieve regulatory compliance, help security and development teams to build inventories of their applications, classify applications based on business impact, and prioritize and remediate vulnerabilities throughout the application lifecycle



AppScan application security management capabilities enable security teams to address the vulnerabilities they grapple with on a daily basis.

Cloud-based solutions

IBM Application Security on Cloud helps secure your organization's web and mobile applications by detecting dozens of today's commonly exploited vulnerability types. IBM Application Security on Cloud provides DAST, Mobile Application Security Testing (MAST), SAST and Open Source Analyzer to find vulnerabilities in applications before they are placed into production and deployed. Convenient, detailed reporting permits you to effectively address application security risk, enabling application users to benefit from a more secure experience.



IBM Application Security on Cloud makes it extremely easy to test mobile, web and desktop applications. Users simply choose which type of application they want to scan.

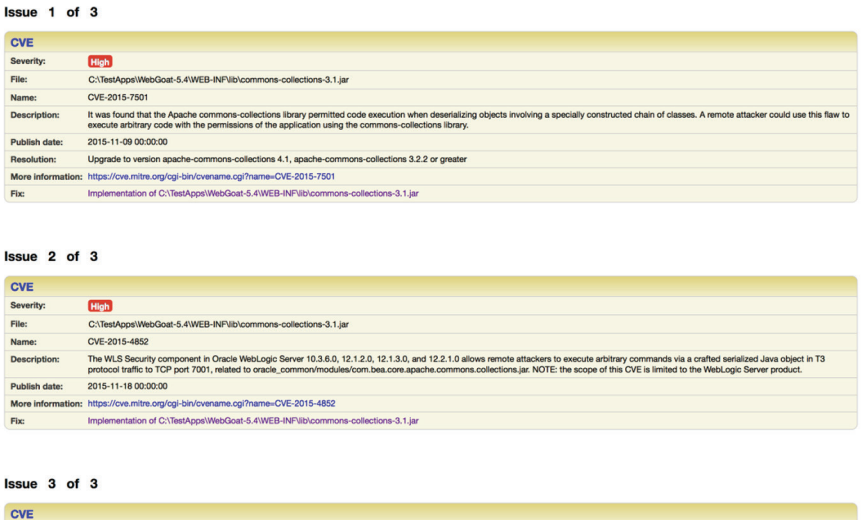
Cognitive benefits of IBM Application Security on Cloud include the following:

- Intelligent Finding Analytics (IFA), which uses machine learning to analyze scan findings, intelligently reduce false positives and dramatically decrease scan times that rely on application security experts to review scan results
- Intelligent Code Analytics (ICA), which automates analysis of any code frameworks used by development teams, eliminating costly manual reviews and false negatives while delivering on the goals of fully-automated DevOps testing

Solution capabilities

IBM solutions for application security testing, including AppScan and IBM Application Security on Cloud, enable organizations to manage security throughout the application lifecycle. Key capabilities include:

- **High-level visibility**—Provides enterprise-level visibility into application security status and compliance risk across the organization, via an application-risk dashboard
- **Scalable application security testing**—Enables you to choose the solution that is right for your organization and add components to customize it as your application security program matures
- **Issue remediation**—Creates a fully prioritized list of vulnerabilities that are found with each scan, enabling the highest-priority issues to be fixed first
- **Secure DevOps strategy**—Integrates with key build environments and integrated development environments (IDEs) to provide seamless testing and rapid, targeted remediation for your applications
- **Fix groups**—Locate and collect findings that share one or more common locations, or crossroads, into groups so that it becomes easier to review and remediate the findings, leading to less work for developers, faster DevOps turnaround, and greater security of the applications being deployed
- **Management of regulatory requirements**—Enables users to choose from more than 40 predefined reports and map scan results to key industry and regulatory compliance standards, helping meet the needs of organizations that face key compliance demands associated with their web applications
- **Security testing governance**—Enables you to create, push and enforce consistent security policies you can use throughout the organization, using provided test policies and scanning templates
- **Security intelligence**—Integrates with other IBM Security offerings to further enhance threat evaluation and prioritization of security issues



Issue 1 of 3

CVE	
Severity:	High
File:	C:\TestApps\WebGoat-5.4\WEB-INF\lib\commons-collections-3.1.jar
Name:	CVE-2015-7501
Description:	It was found that the Apache commons-collections library permitted code execution when deserializing objects involving a specially constructed chain of classes. A remote attacker could use this flaw to execute arbitrary code with the permissions of the application using the commons-collections library.
Publish date:	2015-11-09 00:00:00
Resolution:	Upgrade to version apache-commons-collections 4.1, apache-commons-collections 3.2.2 or greater
More information:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7501
Fix:	Implementation of C:\TestApps\WebGoat-5.4\WEB-INF\lib\commons-collections-3.1.jar

Issue 2 of 3

CVE	
Severity:	High
File:	C:\TestApps\WebGoat-5.4\WEB-INF\lib\commons-collections-3.1.jar
Name:	CVE-2015-4852
Description:	The WLS Security component in Oracle WebLogic Server 10.3.6.0, 12.1.2.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to execute arbitrary commands via a crafted serialized Java object in T3 protocol traffic to TCP port 7001, related to oracle_common/modules/com.bea.core.apache.commons.collections.jar. NOTE: the scope of this CVE is limited to the WebLogic Server product.
Publish date:	2015-11-18 00:00:00
More information:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4852
Fix:	Implementation of C:\TestApps\WebGoat-5.4\WEB-INF\lib\commons-collections-3.1.jar

Issue 3 of 3

CVE

IBM Open Source Analyzer displays vulnerabilities as fix groups, to enable easier review and remediation.

Advanced application testing

Because there are different ways to approach application security, AppScan software uses a variety of complementary testing techniques to automate deep application testing early in your DevOps processes. Early detection provides development teams the best ROI for fixing vulnerabilities before the application is deployed into production.

Application security testing solutions from IBM provide DAST, SAST and open-source testing capabilities to help users stay ahead of the latest threats and drive precise, actionable results. AppScan testing methods also include:

- **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, you can detect more vulnerabilities with higher accuracy.
- **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.
- **IBM Application Security Open Source Analyzer:** Helps to secure and manage your open-source components, by automating security testing and configuring scanning for open-source vulnerabilities. It enables you to gain control and visibility over your open-source risk, by continuously identifying vulnerable software components.
- **JavaScript client-side analysis:** Helps you analyze code downloaded to the client. The more functionality the organization performs client-side, the greater the potential for client-side vulnerabilities and exploits.

Who benefits from application security testing solutions from IBM?

Application security testing solutions from IBM are designed to benefit four primary groups:

- Line-of-business owner or chief information security officer (CISO): Those ultimately responsible for application security—and the consequences of inadequate protection—can benefit from a better understanding of the organization's security risks and overall compliance status.
- Application security team: The team responsible for managing—and mitigating—application security within the organization can benefit from knowing exactly which assets they have, the priority of their importance, their level of security and which vulnerabilities are most critical.
- Application development team: The team developing applications can benefit from integrating application security tests into their DevOps process to easily detect security vulnerabilities early in the development cycle.
- Developers: Individuals who create, test and program applications need to understand probable security risks in order to incorporate security in the coding process and plan and create applications that are less vulnerable to potential security threats.

Creating end-to-end security solutions

Application security is not just about performing scans and finding vulnerabilities; it's about managing risk. Deploying integrated and automated solutions for application security can provide more streamlined, cost-effective and reliable outcomes. Integration enables a risk-based approach that can help your organization deal with the impossibility of immediately protecting all applications. Security intelligence, for example, is necessary to prioritize applications and determine which ones should be addressed when, and how.

That's why application security testing solutions from IBM are designed to integrate with complementary IBM Security offerings, to provide organizations with not only application security, but also the capabilities to better assess threats and prioritize vulnerabilities based on the risks they present. These offerings include:

- **IBM QRadar® Security Intelligence Platform**, which integrates security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management to deliver superior threat detection, greater ease of use and lower cost of ownership.
- **IBM Security Guardium®**, which offers a comprehensive data-security platform providing a full range of capabilities—from discovery and classification of sensitive data, to vulnerability assessment of data and file activity to monitoring, masking, encryption, blocking, alerting and quarantining to protect sensitive data.
- **IBM mobile security solutions**, which integrate with IBM Application Security on Cloud mobile application security testing capabilities to help you proactively resolve potential security vulnerabilities on mobile applications and improve operational efficiency.
- **IBM cloud security solutions**, which provide on-demand computing resources—everything from applications to data centers—over the Internet on a pay-for-use basis.

Summary

The seriousness of application security is clear, and the challenges are complex. Without the necessary infrastructure visibility and the right security solutions, protecting your organization can seem overwhelming. IBM has outlined a clear roadmap for application security, providing you with critical steps your organization can take to create an effective, successful application security testing program.

With advanced security testing and a platform for managing application risk, AppScan is designed to help organizations more easily implement and manage the latest security strategies. This solution delivers the security expertise and the critical integrations with application lifecycle management that you need to not only identify vulnerabilities, but also reduce overall application risk.

Along the way, as your organization advances to different application security maturity levels, you can customize IBM application security testing solutions using components that are best suited for your specific needs.

To access a complimentary trial of AppScan today, please visit the AppScan web page.

To access a complimentary trial plan of IBM Application Security on Cloud, please visit the IBM Application Security on Cloud web page.

For more information

To learn more about application security testing solutions from IBM or for information on complementary IBM Security offerings, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/application-security/appscan/

To view detailed system requirements for each application security testing solution, click on the following links:

- AppScan Standard
- AppScan Source
- AppScan Enterprise
- IBM Application Security on Cloud

[1] "Ponemon Institute State of Application Security Risk Management: "How to Make Application Security a Strategically Managed Discipline," *Ponemon Institute*, sponsored by IBM Security, March 2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGL03106USEN&attachment=WGL03106USEN.PDF

[2] "2017 Study on Mobile and Internet of Things Application Security," *Ponemon Institute*, sponsored by IBM and Arxan Technologies, January 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03136USEN&

[3] Neil Jones, "Recently Released Industry Research Study Reveals Triple-Digit ROI for IBM Application Security Testing Solution," *SecurityIntelligence*, July 19, 2016. https://securityintelligence.com/recently-released-industry-research-study-reveals-triple-digit-roi-for-ibm-application-security-testing-solution/

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2018

WGB03009-USEN-07