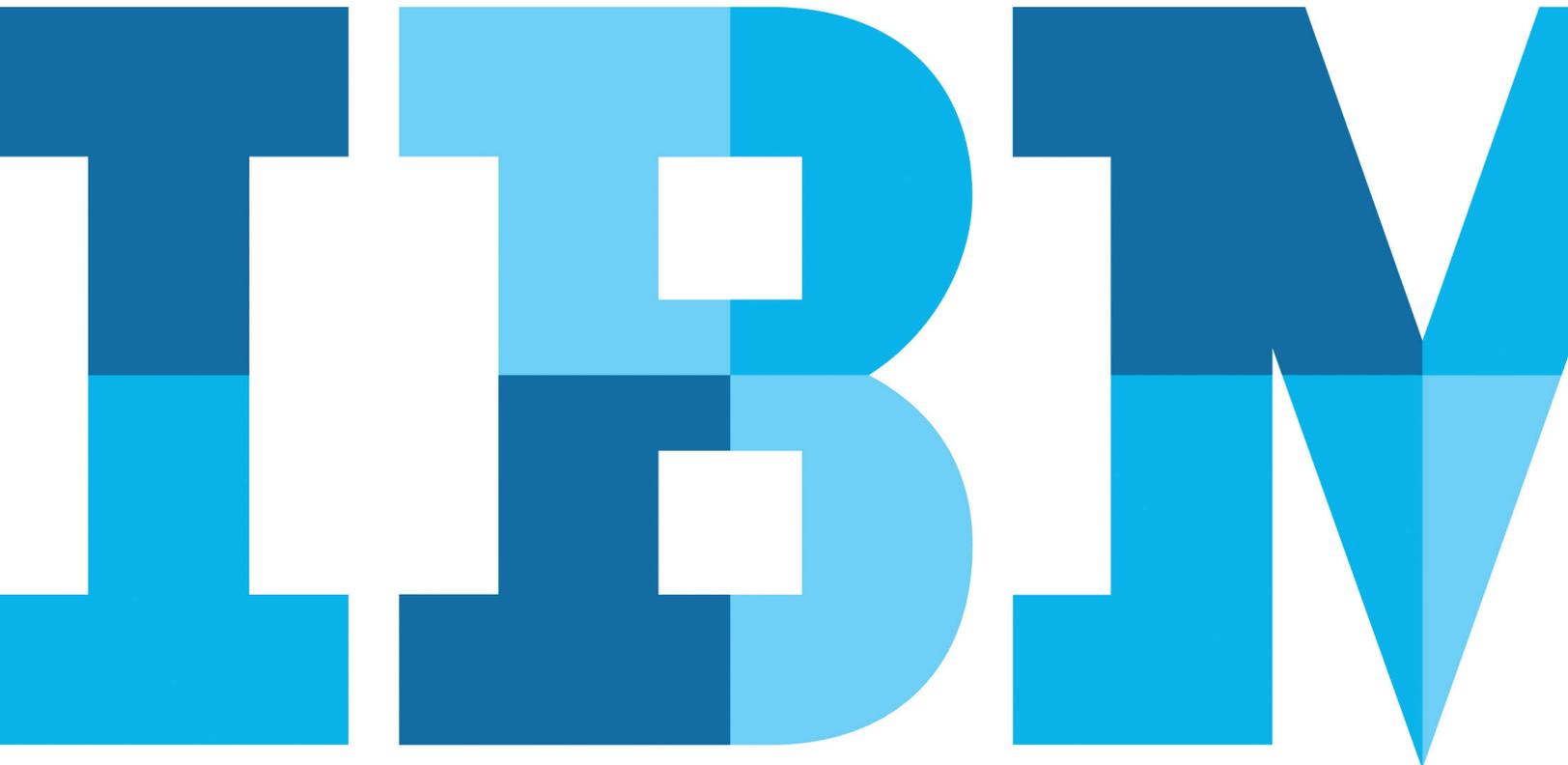


Manage application security risks to help protect your organization's critical data

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



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. Interestingly, while organizations depend on such applications to run their businesses, many invest little to no effort ensuring that they are adequately secure. While these organizations understand established security technologies for routine tasks such as networking and operations, and for managing security procedures such as access control and authentication, many struggle with implementing, managing and maintaining effective application security programs. But in today's increasingly sophisticated threat landscape, the bar must be raised. Since applications can compromise security across the entire organization, securing them needs to become a top priority.

The ramifications of under-secured applications can be dire. Vulnerabilities inadvertently introduced during 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—all consequences that can ultimately impact profitability.

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 these 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 the appropriate policies. Adopting an application security strategy that can protect web-based and mobile applications—during every phase of the application lifecycle—is a solid first step.

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 30 percent of respondents say their organizations allocate sufficient budget to protect mobile and Internet of Things (IoT) devices, and when it comes to security testing, an even greater share of respondents (39 percent and 59 percent, respectively) report that their security testing is primarily done on applications already in production.¹ Are you apportioning your security budget appropriately to align with these 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.²

The journey to application security



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

Exploring integrated application security management from IBM

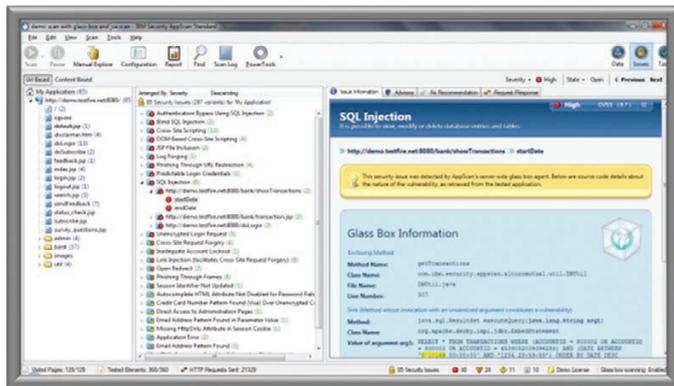
Running an application security initiative in a large organization can be a challenge. A small security team is often responsible for securing thousands of applications built by multiple development teams. IBM provides integrated capabilities for application security management, enabling security teams 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, eventually, mitigate risk that exists in applications as code quality improves.

On-premises solutions

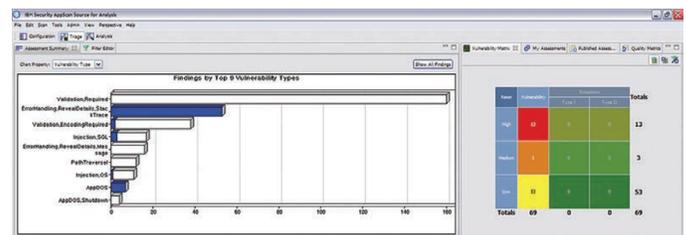
IBM Security AppScan solutions offer components specially designed to benefit application security managers and development teams at organizations of all sizes. The on-premises offerings include:

- **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



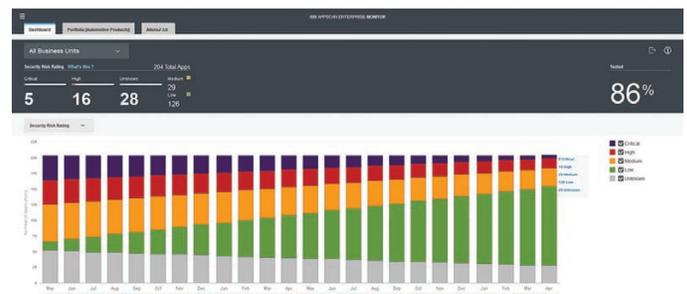
AppScan Standard software includes glass-box testing with runtime analysis to identify more vulnerabilities, simplify scan configurations and provide more actionable results.

- **IBM Security AppScan Source:** Helps lower costs and reduce risk exposure by identifying software vulnerabilities in web and mobile applications early in the development lifecycle, so they can be eliminated before deployment

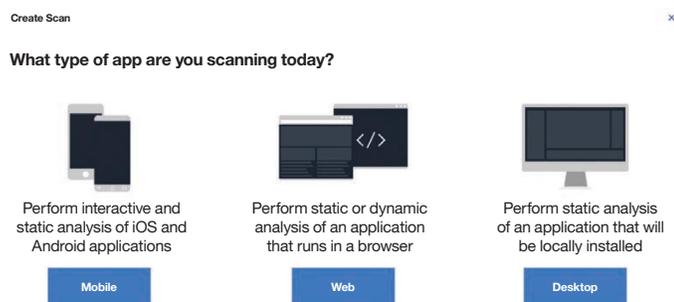


AppScan Source software provides assessment summaries that map to application risk and provide insight into vulnerabilities that affect your applications.

- **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.



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

Cloud-based solutions

IBM Application Security on Cloud permits you to easily manage the security risk of your application portfolio and perform web and mobile application security testing from the cloud. The solution supports SAST and DAST analysis, in a comprehensive all-in-one offering.

Cognitive advantages of IBM Application Security on Cloud:

- **Automation:** Automated testing makes application security a default component of your security approach.
- **Speed:** Intelligent Finding Analytics, also available with IBM Security AppScan Source, uses machine learning to analyze results, intelligently reduce false positives and decrease turnaround time.
- **Coverage:** Cognitive capabilities improve the speed and depth of scans for fully automated DevOps testing.

IBM Application Security on Cloud Consulting Services enable organizations to leverage the IBM team of security experts for guidance and “concierge” consulting services. IBM Application

Security on Cloud Consulting Services offer a simple, streamlined way to augment an existing application security program with the right skill sets at the right time to help take the organization’s application security capabilities to new heights.

Solution capabilities

IBM solutions for application security testing enable organizations to manage security throughout the application lifecycle.

Key capabilities include:

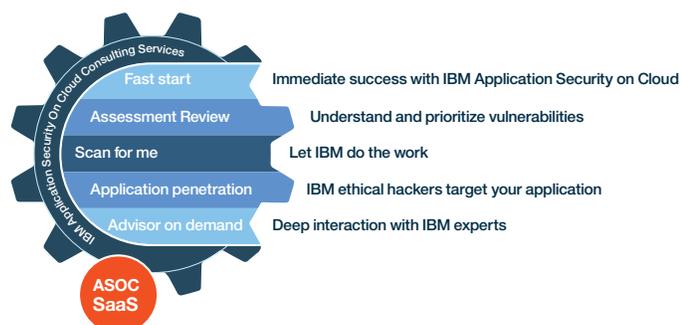
- **Scalable application security testing**—AppScan enables you to choose the solution that is right for your organization and add components to customize it as your application security program matures.
- **High-level visibility**—Via an application-risk dashboard, AppScan provides enterprise-level visibility into security status and compliance risk of applications and processes across the organization.
- **Management of regulatory requirements**—To help meet the needs of organizations that face key compliance demands associated with their web applications, AppScan enables users to choose from more than 40 predefined reports and map scan results to key industry and regulatory compliance standards.
- **Security testing governance**—With AppScan, you get test policies and scanning templates that enable you to create, push and enforce consistent security policies you can use throughout the organization.
- **Issue remediation**—AppScan creates a fully prioritized list of vulnerabilities found with each scan, enabling the highest-priority problems to be fixed first.
- **Security intelligence**—AppScan integrates with other IBM Security offerings to further enhance threat evaluation and the prioritization of security issues.

Advanced application testing

Because there are different ways to approach application security, AppScan software uses a variety of testing techniques to enable deep application analyses during all phases of the application lifecycle.

Application security testing solutions from IBM provide DAST and SAST capabilities—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. 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 three 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 development and operations (DevOps) process to easily detect security vulnerabilities early in the development cycle.

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 Network Intrusion Prevention System**, which provides appliances and systems that automatically block malicious attacks while preserving network bandwidth and availability.
- **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 roll out and manage the latest security strategies. This solution delivers both the security expertise and the critical integrations with application lifecycle management you need to not only identify vulnerabilities, but also to 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 best suited for your specific needs.

To access a trial of AppScan today at no charge, please visit the [AppScan](#) web page.

To access a trial plan of IBM Application Security on Cloud at no charge, please visit the [IBM Application Security Analyzer](#) web page.

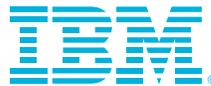
For more information

To learn more about application security testing solutions from IBM, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/applicationsecurity

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

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](#)



© Copyright IBM Corporation 2017

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2017

IBM, the IBM logo, ibm.com, AppScan, Guardium, and QRadar are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

¹ “2017 Study on Mobile and IoT Application Security,” *Ponemon Institute*, January 2017. <https://securityintelligence.com/10-key-findings-from-the-ponemon-institutes-mobile-iot-application-security-testing-study/>

² 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/>



Please Recycle