IBM Security

IBM

# Effectively manage application security risk in the cloud

## Simple, automated testing can streamline and strengthen your security regimen

IBM Security White Paper

# Why is application security vital?

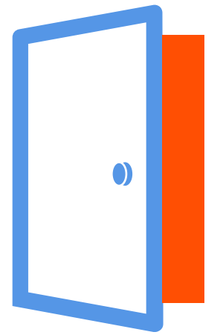
You've probably done a lot to encourage data security—but could the applications you run be the equivalent of a front door to your enterprise that's been left wide open? The security of the data in your organization's hands depends on a lot more than just locking down individual files and records. You need to tighten security at the *application* level, too, because applications can control access to your data—and even to your organization's Internet of Things (IoT) infrastructure.

Many notorious security breaches have occurred not because of poor data security practices, but because of vulnerable applications. Deploying application security helps prevent rogue or vulnerable software from allowing cybercriminals to siphon data that you thought was secure.

Even so, application security remains an often-neglected area of cybersecurity,[1] and breaches continue to occur. Why? In part, because locking down applications is more complicated than encrypting files or safeguarding networks with firewalls. Applications have also grown in number and type, with the advent of app stores and specialized applications that access cloud-based infrastructure. Meanwhile, widespread adoption of bring-your-own-device (BYOD) policies has resulted in an increase in unvetted applications, and application-connected IoT data sources proliferate rapidly.

Application security is vital to:

- Prevent reputational damage
- Maintain customer trust
- Avoid remediation costs
- Detect and respond to security risks before they cause damage



*In one study,*

**77%**

*of responding developers say applications are vulnerable because pressure to release applications quickly prevents adequate testing.[2]*

▸ Watch a demo of what IBM Application Security on Cloud can accomplish for you.

1 "How to Make Application Security a Strategically Managed Discipline," *Ponemon Institute*, March 2016.

2 "The State of Mobile Application Insecurity," *Ponemon Institute*, February 2015.

# Why do organizations struggle to achieve application security success?

Application security is complicated by factors that span developers, IT staff and end users. In combination, these factors can make organizations susceptible to vulnerabilities.

**Rush to release**
A pervasive "rush to release" atmosphere means developers are often short of testing resources. But application security doesn't just rest with developers. There's a parallel rush to install applications quickly, as users seek the efficiencies that new software can deliver.

**Complex applications**
Software varies wildly in scope, data requirements, language and platform. A compromised application with a direct line to company data can be as risky as a misplaced laptop loaded with similar data—perhaps worse, if the gap goes unnoticed. An insecure or malicious application could expose your data, whether it has been exploited by a security vulnerability or because it began life insecure.

**Application security not a priority**
Application-layer vulnerabilities are often viewed as low priorities, and organizations typically do not rank applications by importance for protection. And applications are often dispersed throughout an organization—along with accountability for their security—with little visibility into which ones are in use or which ones are most vulnerable.

**Lack of standards**
Users can't devote time to security testing—and don't know how to test effectively. There are few universal application security standards, so guidance and on-site expertise can be difficult to assess or employ.

*A recent Ponemon Institute study found that*

**47%**

*of respondents said mobile application risk in their organizations was increasing or significantly increasing.*[1]

Learn more about risk-based application security management.

1 "How to Make Application Security a Strategically Managed Discipline," *Ponemon Institute*, March 2016.

# What is effective application security?

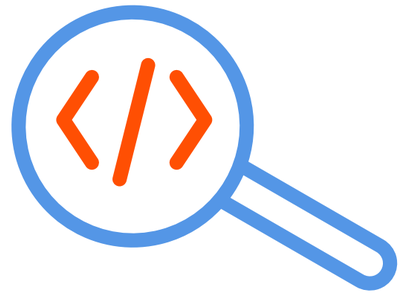
Effective application security practices confirm that security should be viewed as a process, not as a series of items to check off a list. As such, application security testing must be comprehensive and ongoing.

For developers, the application security testing process should be embedded in the software development lifecycle, with ongoing source code analysis. For end-user organizations, the process continues, with vetting of all new software that's deployed, as well as re-testing applications on which the organization already relies.

Comprehensive application security should involve:

- **Discovering and cataloging** applications that are currently in use
- **Static testing**—scanning application source code for vulnerabilities is the most direct way to find the actual code behind a particular security vulnerability
- **Dynamic testing**—evaluating what the software does when it's deployed (for instance, is it vulnerable to potential cross-site scripting and SQL injection attacks?)
- **Mobile application security testing**, due to the proliferation of new mobile applications in the market
- **Deployment** of new software only after it's been vetted

Applications should be re-evaluated regularly, and this evaluation should be informed by sources such as the Open Web Application Security Project (OWASP) Top Ten list[1]—new threats can put formerly safe applications at risk.



*As of September 2016, there were*

**2 million**

*Apple iOS applications available for download,[2] and more than*

**2.4 million**

*Google Android applications.[3]*

▸ Learn more about the risks that make application security vital.

1 Paul Ionescu, "The 10 Most Common Application Attacks in Action," *IBM Security Intelligence*, April 8, 2015.

2 "Number of apps available in leading app stores as of June 2016," *Statista*, June 2016.

3 "Number of Android Applications," *AppBrain*, Accessed October 13, 2016.

# Leverage our time-tested application security best practices

In vetting applications for security risks, organizations operate under constraints that range from limited budgets to heavy workloads of their security and IT staffs. But such constraints cannot get in the way of improving security protection. Instead, your organization should employ best practices that include:

- **Oversight**—Planned, automated testing delivers more thorough and reliable results than ad-hoc testing
- **Continuity**—Applications should be built and tested for security and re-tested to keep up with vulnerabilities
- **Prioritization**—Ranking application security issues based on severity and potential business impact permits problems to be tackled in the order that makes the most business sense
- **Flexibility**—Avoiding restrictive implementation requirements is critical to evaluate the full range of applications deployed by your organization
- **Adaptability**—Threats change over time; a flexible approach results in fewer changes to remain in control of application security
- **Timeliness**—To avoid disrupting—or redoing—development processes, applications should be tested throughout all stages of the development lifecycle

An integrated application security solution such as IBM® Application Security on Cloud can help you minimize security gaps and identify potential vulnerabilities. Integration with other security products and practices makes risk mitigation for applications part of a comprehensive security program, not an afterthought.

**58%**

*of organizations say security concerns inhibit full deployment of a mobile security strategy.*[1]

See how IBM Application Security on Cloud identifies and remediates vulnerabilities.

1 "2016 Mobile Security & Business Transformation Study," *Information Security Media Group*, Sponsored by IBM Corp., 2016.

# Comprehensive, cloud-based application security testing

Bolster your application-security risk management by implementing an integrated solution, rather than relying on disparate tools. IBM Application Security on Cloud is a comprehensive, cost-effective, user-friendly and easy-to-deploy cloud-based solution for web and mobile applications that unites all phases of application security testing. Our cloud-based offering is based on years of IBM experience in on-premises security testing, and interoperates with other security tools to facilitate comprehensive cyber-defense protection.

IBM Application Security on Cloud is a complete, subscription-based solution that permits you to test applications and improve security protection by providing actionable data. With IBM Application Security on Cloud, you can quickly assess application risk ratings, so you can focus remediation efforts on your most significant vulnerabilities.

- Register for a trial version of IBM Application Security on Cloud, or download an on-premises IBM Security AppScan® trial.

You can perform static security testing of application code written in a wide number of programming languages, conduct dynamic analysis for pre-production and in-production software web applications; and test Android and iOS applications, prior to their deployment. IBM Application Security on Cloud identifies and reports security issues, ranks them according to exposure and criticality, and recommends remediation steps. All of the results can be integrated into a number of DevOps systems and integrated development environments (IDEs).

A full range of companion consulting services is also available, enabling your security team to take full advantage of the capabilities IBM Security has to offer.

Click image to enlarge. Click again for original size.


The IBM Application Security on Cloud dashboard view.

# Real-world IBM Application Security on Cloud use cases

Organizations that deploy application security solutions from IBM realize the value of integration and automation as part of their overall security strategies, whether they're creating applications, or deploying them.

**Protecting code throughout the software development lifecycle**

- Concur Technologies of Bellevue, Washington specializes in corporate expense management, so it manages confidential financial information on an everyday basis. Protecting that information is paramount, but also difficult to achieve. As an organization with a large mobile presence, including its own mobile applications, Concur deployed AppScan with the same vulnerability testing technology that powers IBM Application Security on Cloud. With AppScan, Concur can test its applications for security risks as they're developed and conveniently analyze production code.

**Managing risk in a fast-growing enterprise**

- Migros, a Turkish retail giant that's experiencing break-neck growth at home and abroad, has a large-scale infrastructure to protect, with applications transmitting inventory and payment information over a network that encompasses nearly 1,500 stores and more than 100,000 Internet-connected endpoint devices. In orchestrating its growth, the company faced challenges in moving operations to the cloud as it implemented a BYOD policy. By leveraging IBM application security solutions, Migros has been able to scale its business while minimizing risk.

*IBM offers a*
**complete portfolio**
*of application security testing tools, used by leading companies in fields as diverse as manufacturing[1] and financial services[2] to help protect applications, devices and data.*

▸ Sign up for a complimentary trial plan of IBM Application Security on Cloud.

1 "Large global automaker: Protecting the Connected Car Ecosystem," *IBM Corp.*, July 2016.

2 "Progressive Insurance: Proactively Protecting Data by Creating Appropriate Controls," *IBM Corp.*, May 2016.

# For more information

To learn more about IBM Security solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/applicationsecurity

**About IBM Security solutions**

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

You can also leverage IBM Security Services to fit your organization's evolving needs, as you build and execute application security programs. This gives you access to application security expertise when and where you need it, for as long as you need it. Whether you need a quick engagement to get your team up to speed, deep consulting services, ethical hackers to manually interrogate your applications, or anything in between, IBM has you covered.



IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
January 2017



WGW03254-USEN-01