



# **Why You Need to Test All Your Cloud, Mobile and Web Applications**



## Introduction

In a recent survey of security executives, over 70 percent of respondents acknowledged that they are performing vulnerability tests on less than 10 percent of their Cloud, Mobile and Web applications. In the same survey majority of them also confessed that they had been hacked at least once in the last two years. We have heard similar responses in conversations with various companies. While most large companies have started to test more and more of their applications for vulnerabilities, there is a long way to go. You are as strong as your weakest link and in this case the weakest links are untested applications.

Hackers attack any application that has security weaknesses. Although testing high-value applications and mission-critical applications is better than not testing at all, the problem is that hackers will exploit one of the other applications and once they are in your infrastructure they'll figure out a way to get to your other applications as well.

## Challenges in Protecting All Web Applications

So why is it that in spite of all the risks, organizations are not taking extra measures to identify vulnerabilities in all their Cloud, Mobile and Web applications? In talking to various security professionals and in our recent surveys, here are some of the most common reasons we get:

### Limited budget

There's just not enough money in the budget to test all applications. Whether it is additional headcount or technology needed, it costs money and most organizations have not set aside enough. We certainly found this to be true in our survey where most respondents said their coffee budget was bigger than their application security budget.

### Limited expertise

Application security is still not a mature science and there are very few people out there who really understand application security.

### Compliance driven

PCI and other standards have traditionally only required external facing applications although PCI has expanded the scope to include internal applications as well. Most organizations are driven by compliance and unfortunately not security. So the focus is only on these applications that help them get compliant and all the other applications are for the most part ignored. And, in reality the situation is even worse than that. The applications that are assessed for security, in many cases, are tested only to get a checkbox for compliance and not necessarily to make sure that they are secure.

### Misconceptions

Lack of adequate knowledge can be dangerous. This is certainly true in case of application security where there are many misconceptions. One of them is that companies shouldn't worry about all their Cloud, Mobile and Web applications. For example, why would you want to test your internal applications that have no external interface? Those are secure, correct? Wrong. Think of insider threats. What if you have an internal Human Resource application with access to employee confidential information like health records, compensation, performance metrics, etc? Now, let's say one of your less-than-ethical employees logs in as a user and exploits a privilege escalation vulnerability to give themselves admin rights? Voila! They have access to all the confidential records and your company is now non-compliant with various standards.

While these are all legitimate reasons, a breach won't allow you to use these with regulatory bodies or with your customers in protecting your brand. And, it's not that hard to protect yourself. Here are a few recommendations to do identify application vulnerabilities.



## Recommendations

### ROI and impact of hacking

Various studies show that one breach can cost millions of dollars. According to research done by Forrester and Ponemon Institute, average cost per record in case of a breach is at least \$300. Most companies have thousands of records. And over 75 percent of attacks are occurring through web applications.

### Outsource

You don't have to do everything yourself. There are solutions available as a managed service and a cloud service to help you secure your Cloud, Mobile and Web applications quickly and affordably.

### Process for testing all applications

Not all applications are created equal. You can cut down your costs by creating a pyramid of all your apps. Yes, the first step is to find out what applications do you have. Now run a basic test on all of these applications and based on what you find out you can prioritize applications that need deeper testing. This way, you'll get coverage on all your applications without spending a fortune and taking many years. Automated solutions and a good process can help you get there quickly.

### Manage your risk

You will find hundreds of vulnerabilities in your web applications. Guaranteed. And, you won't have time to fix them all. Take a risk management approach and prioritize these vulnerabilities based on a quantitative score. The ones with the highest score i.e. most likely to be exploited on applications that are most sensitive should be addressed first and right away. All the other ones should be blocked with a Web Application Firewall (WAF) or other methodologies.

## Summary

The bottom line is that any breach can have a severely adverse impact on your bottom line. Cloud, Mobile and Web application vulnerabilities are low hanging fruits for hackers and they would rather pick these rather than going for the harder stuff. Hacking, unfortunately for the rest of us, has become a lucrative profession. And, hackers will continue to attack you to earn their living. Whether it's for financial exploits, to steal intellectual property, or for cyber war and cyber terrorism, hackers will continue to fire shots until they penetration. In this case, we can't fire back at the enemy, and we can't be 100 percent secure, but we can certainly raise the walls of our castle to thwart their attempts.





## About Cenzic

Cenzic provides an application security intelligence platform to continuously assess Cloud, Mobile and Web vulnerabilities. This helps brands of all sizes protect their reputation and manage security risk in the face of malicious attacks. Today, Cenzic secures more than half a million online applications and trillions of dollars of commerce for Fortune 1000 companies, all major security companies, government agencies, universities and SMBs.

## Cenzic Products

Cenzic Enterprise	Cenzic Enterprise is a software solution that assesses the security of Cloud and Web applications and supports security risk management throughout the software development lifecycle. Cenzic Enterprise provides a company-wide view of security vulnerabilities and status to executives as well as customized views for other users from a Web-based dashboard.
Cenzic Desktop	Cenzic Desktop is a single-user version of Cenzic Enterprise. It is designed for the power user that wants to run their security assessments on Cloud and Web applications from a single system.
Cenzic Managed Cloud	With Cenzic Managed Cloud, Cenzic's security experts remotely perform full vulnerability testing on Cloud, Mobile and Web applications. From a Web-based dashboard, users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Cloud	Cenzic Cloud allows users to test their own Cloud and Web applications for basic attacks and receive actionable results all within their own Web portal – no security experts needed.
Cenzic Hybrid – Software + Cloud	Cenzic Hybrid provides access to both Cenzic Enterprise software and Cenzic Managed Cloud services. Vulnerability testing can be done either by using the software on premise or by leveraging Cenzic's expert security services team.
Cenzic Mobile	Cenzic Mobile service is delivered as a managed service. Cenzic's security experts remotely perform full vulnerability testing on mobile applications. All testing is managed from a Web-based dashboard where users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Services	Cenzic services and training help those responsible for Cloud, Mobile and Web application security to implement best practices and procedures to protect data from hacker attacks.