



Good Enough Application Security

Getting Started by Testing in the Cloud



Table of Contents

Introduction.....	3
Steps to Get You Started Towards “Good Enough” Security	3
Cloud Solutions for Application Security	4
Cenzic Cloud.....	4
About Cenzic	5



Introduction

Sony, Nintendo, CIA, Citibank and the US Senate

What do these organizations have in common? You probably know that they were all hacked in 2011.

According to Gartner over 97% of Web applications are vulnerable to cyber-attack, so it's critical to defend your information assets and brand, regardless of your company size.

With over 250M websites out there and mobile apps being published continuously, most of which are insecure, hackers have a huge pool of targets. No organization is safe. Universities, banks, government agencies, retailers, high-tech companies, and social networking sites like Twitter and Facebook have all been victims of repeated attacks. Organizations have lost billions of dollars because of these breaches. Hacktivism and cyber terrorism have become mainstream and the number of people behind them is growing.

In spite of these breaches, most corporations are doing very little to secure their Cloud, Mobile and Web applications. With network infrastructure pretty secure, albeit not perfect, hackers are putting their efforts toward going after the weakest link – Cloud, Mobile and Web applications. Many application vulnerabilities have a public exploit and even when patches are available, most companies still haven't deployed these patches.

People have good intentions, but the task of securing applications can seem daunting and cause them to delay patch initiatives. The problem is that these vulnerabilities in Cloud, Mobile and Web applications represent serious risk. In a study conducted by the Ponemon Institute, 72 percent of respondents test less than 10 percent of their applications, even though 73 percent admitted that they have been hacked at least once in the last 24 months.

Good Enough Security

Despite the alarming statistics, it's still understandable why people don't produce more secure applications. The endeavor is daunting and never ending. It has to be done correctly, continuously, and within a tight budget. Not fun. But there are ways to make it more tolerable, even rewarding. Analysts recommend that companies start out with a "good enough" security approach. By chipping away at the problem, you'll be more prone to improve upon it over time. You don't have to find every single flaw in every single Cloud, Mobile or Web application, but addressing the big problems first will make a significant improvement in your application security posture. The suggestions below will help guide you, regardless of your company size.

Steps to Get You Started Towards "Good Enough" Security

Bust Those Myths

You should bust some of the myths around application security. For example, SSL does not protect you from hackers exploiting your application vulnerabilities and neither does a network firewall or IDS. Once people understand this, be aware of the buzz word vendors. Many of them say they can detect application security vulnerabilities even though their solutions are focused on a completely different set of problems.

Application Scanning

There are a lot of ways to detect application security flaws, including automated, black box testing. Black box testing the most popular as it yields the fastest results with the least amount of effort. And you're more likely to get buy-in from the rest of your company team if you choose a managed service or cloud offering, as there is a quicker ROI with fewer resources needed.

Use a Quantitative Score for Prioritization of Vulnerabilities

Assuming you have the budget and you have started testing your applications for vulnerabilities, you will find that almost every application will have hundreds of vulnerabilities. This can be overwhelming and demoralizing. But if you prioritize these vulnerabilities based on some kind of quantitative score, the task becomes much more manageable for InfoSec and for development.



Interim Protection

Vulnerabilities typically don't get fixed overnight. With developers already under pressure to get their Cloud, Mobiles and Web applications out on time, they have to make time for security. Until you fix these vulnerabilities, you have to protect your infrastructure. You can do this by configuring your web application firewalls (WAF) for specific vulnerabilities and by removing some functionality.

Test Continuously

There are hundreds of new application vulnerabilities every month. You have to use a continuous testing process to detect new vulnerabilities. If you don't follow a continuous process, your applications will be at risk.

Leverage Outside Resources

You don't have to do it all yourself. Take advantage of powerful solutions for identifying vulnerabilities in Cloud, Mobile and Web applications. You may be surprised at what's available – you can even do your app testing from your desktop using cloud-based tools.

Trends show that attacks on Cloud, Mobile and Web applications are increasing in frequency and sophistication. Hacking is a lucrative career and these applications are an easy target as they offer an easy point of entry. Take some easy steps to reduce your application risk by eliminating known application vulnerabilities. With so many applications to choose from, hackers will seek the path of least resistance – don't make that your Cloud, Mobile and Web applications.

Cloud Solutions for Application Security

Cenzic Managed Cloud

Cenzic Managed Cloud, powered by Hailstorm, is a managed service that offers a range of Cloud, Mobile and Web application assessments remotely – no software, no hardware and no installation needed. With Cenzic Managed Cloud, Cenzic's security experts remotely perform full vulnerability testing on Cloud, Mobile and Web applications with minimal resources and budget.

Cenzic Managed Cloud supports security risk management throughout the software development lifecycle. Because Cenzic Managed Cloud can be used in all parts of the software development lifecycle, and most importantly in production, applications are protected against new threats even after being deployed. After application vulnerabilities are identified, Cenzic Managed Cloud provides risk mitigation recommendations to protect data and meet compliance requirements.

With Cenzic Managed Cloud, you get:

- Continuous testing of all applications, including ones in production
- Centralized management of application security risk for the entire enterprise with role-based visibility
- Regulatory compliance assurance, including PCI 6.6
- Part of flexible product suite that offers software, cloud and hybrid deployments
- Unified architecture enables effortless transfer of data between Cenzic products

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. It is the most cost effective, easy-to-use and robust vulnerability assessment solution available.

With Cenzic Cloud, applications can be continuously assessed to reduce online security risk. Because Cenzic Cloud can be used in all parts of the software development lifecycle, and most importantly in production, applications are protected against new threats even after being deployed. After application vulnerabilities are identified, Cenzic Enterprise provides risk mitigation recommendations to protect data and meet compliance requirements.



With CenZic Cloud, you get:

- Fast, cost-effective way to protect Cloud and Web apps from hackers
- Free app re-scanning to confirm all vulnerabilities are fixed
- Continuous testing process to keep ahead of the “hacker curve”
- Minimal false positive reports – under 1%
- Compliance assistance, including for PCI 6.6 and OWASP Top 10

Cenzic Cloud Testing Levels

HealthCheck: Use this service to take initial steps towards a stronger security posture.

Bronze: Check for basic vulnerabilities most often exploited by hackers.

Silver: Find the most common defects that lead to a data breach and brand damage.

Gold: Used for compliancy (e.g., PCI 6.6 and the OWASP Top 10) – combine tests from bronze and silver.

How CenZic Cloud Works

1. Test Cloud or Web App

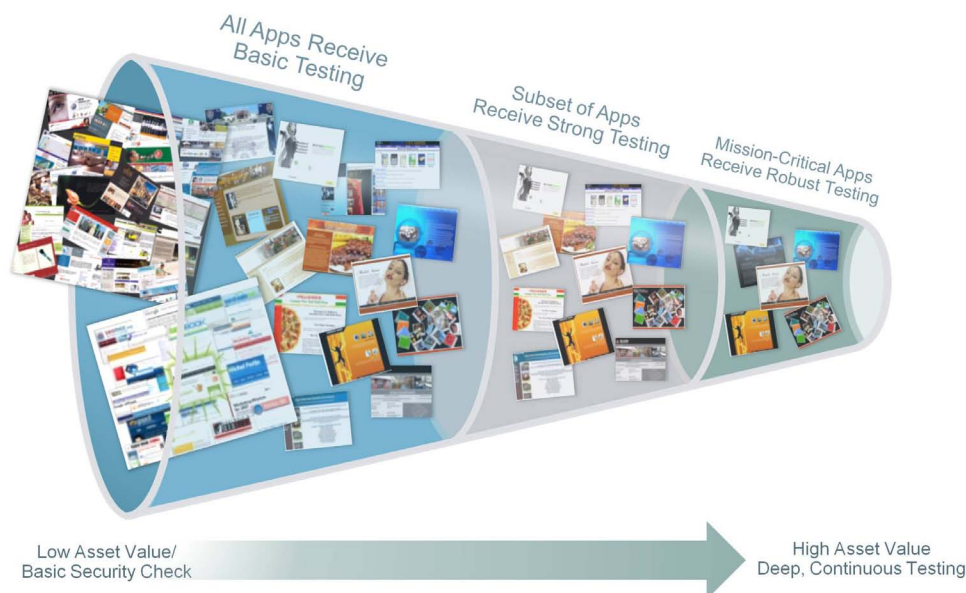
As a new CenZic Cloud customer, you will receive a userid and password for your own Cloud account. Within the customer portal, just enter the URL of the desired Web or Cloud application you want scanned and CenZic Cloud will automatically test it with the at the service level you purchased.

2. Get Results & Fix Flaws

Once the testing is completed, you will be notified that the security report is available in your portal account. Just click on the link to download the PDF report that contains a summary graph of the detected vulnerabilities, details about those defects and how to fix the flaws. See screen shots below for report details.

3. Re-Test

Web and Cloud application security is a never-ending job. It has to be a continuous process of testing, fixing, and re-testing to ensure a strong security posture. After you’ve fixed the detected flaws, you can retest the application to ensure the insecure code no longer exists. Your yearly payment includes 60 free re-tests for your application.





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.