



Continuous Testing of Production Cloud, Mobile and Web Applications



Table of Contents

Executive Summary3
Application Security Optimization3
Continuous Assessment of Production Applications5
About Cenzic6



Executive Summary

Cloud, Mobile and Web application security is a top-of-mind concern for general managers, CISOs, CIOs and security staff at organizations ranging from Fortune 100 companies to educational institutions. Widespread data breaches and intellectual property thefts have left few organizations untouched or unaware. Almost 70% of the vulnerabilities disclosed each month are related to Cloud, Mobile and Web application security.

Current methods of addressing application security problems focus on improving the security process within the software development lifecycle. Testing early in the development cycle has great merit, but it leaves production applications' exposure unaddressed. Only a small percentage of applications are in the development or quality assurance stage at any point of time, leaving a vast majority of the applications in production exposed and vulnerable. With over 400 new application vulnerabilities every month, it is imperative that organizations test and re-test all their Cloud, Mobile and Web applications.

Business managers and security leaders in Fortune 2000 corporations tell us that over 90% of their Cloud and Web application portfolio already exists in production – largely untested from an application security perspective. This means that current application security testing methods are mitigating less than 10% of the actual threat facing these organizations. The threat to production applications present major risks, including financial loss, lack of regulatory compliance, loss of credibility and customer trust, as well as system downtime and direct intellectual property theft – all critically impacting both the companies and consumers.

A large number of untested applications also reside in legacy systems with Web-enabled front ends to internal systems. These often support mission-critical processes from business operations to supporting infrastructure that provides core database and data management services. These systems, like other public facing Internet applications, are also largely insecure and at risk of attack. Protecting these other Internet-facing production applications are critical priorities, since many advanced application attacks can compromise users' browsers. Those internally compromised browsers can then perform surveillance of the internal application network as well as conduct further attacks against applications deep within a corporation. The question is what to do about the security of production applications fundamental to running the business.

Cenzic recommends a process of continuous assessment for applications in development and production environments – a process that can equally apply to Intranet and public-facing applications alike. Continuous testing can now be easily and safely done in a virtualized environment to identify security vulnerabilities in Cloud, Mobile and Web production applications.

Application Security Optimization

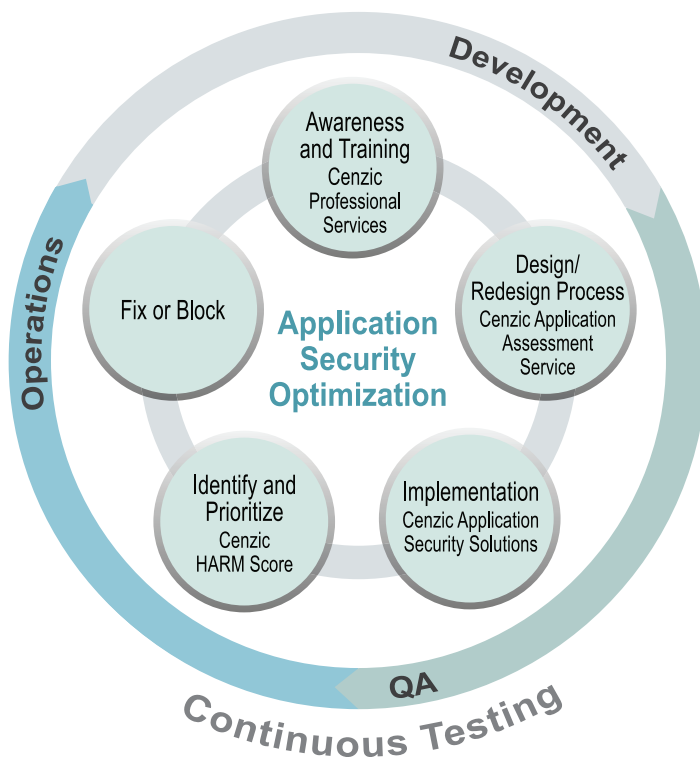
Due to the unceasing onslaught of hackers' employing new methods to get to valuable customer data organizations simply must understand that securing Cloud, Mobile and Web applications is not a one-time event but a discipline of testing and re-testing; in other words continuously – over an applications lifecycle. Without continuous testing, there is no hope of truly getting ahead and staying on top of the 400 plus new threats that come out every month.

The importance of employing a process by which they optimize the security of Cloud, Mobile and Web applications – both developed and in production is vital to overall application security.

Cenzic has defined a process called the Application Security Optimization as a way of making sure that a company's entire Information Security team can get and stay on top of the onslaught of current and new vulnerabilities. The process starts the development team with Awareness and Training about existing and new vulnerabilities; this leads smoothly into the next stage of Design Process (or Redesign). After the Design Process has been set, the next stage is to implement the testing and assessment of the Cloud, Mobile and Web applications. This proceeds to the Identify and Prioritize stage where the findings are reviewed often by the QA team. The final stage of the cycle is to fix and block vulnerabilities stage (Development and QA Team). Since the process is a



continual cycle, the fixing or blocking of the Application vulnerabilities starts the cycle again with Awareness and Training of what was missed. The vulnerability findings of the process are utilized into the next cycle of Application Security Optimization.



Together, the development team, QA team, and operations team can easily employ this Application Security Optimization process. With Application Security Optimization the entire team can stay on top of vulnerabilities that affect all the company’s Cloud, Mobile and Web applications – in development, Q.A. and production. In doing so, they can work to see common vulnerabilities and fix them so that with the next cycle of testing they have a more enhanced and extensive knowledge of common vulnerabilities. Taken as a whole, this cycle continually improves the discovery, fixing and training process.

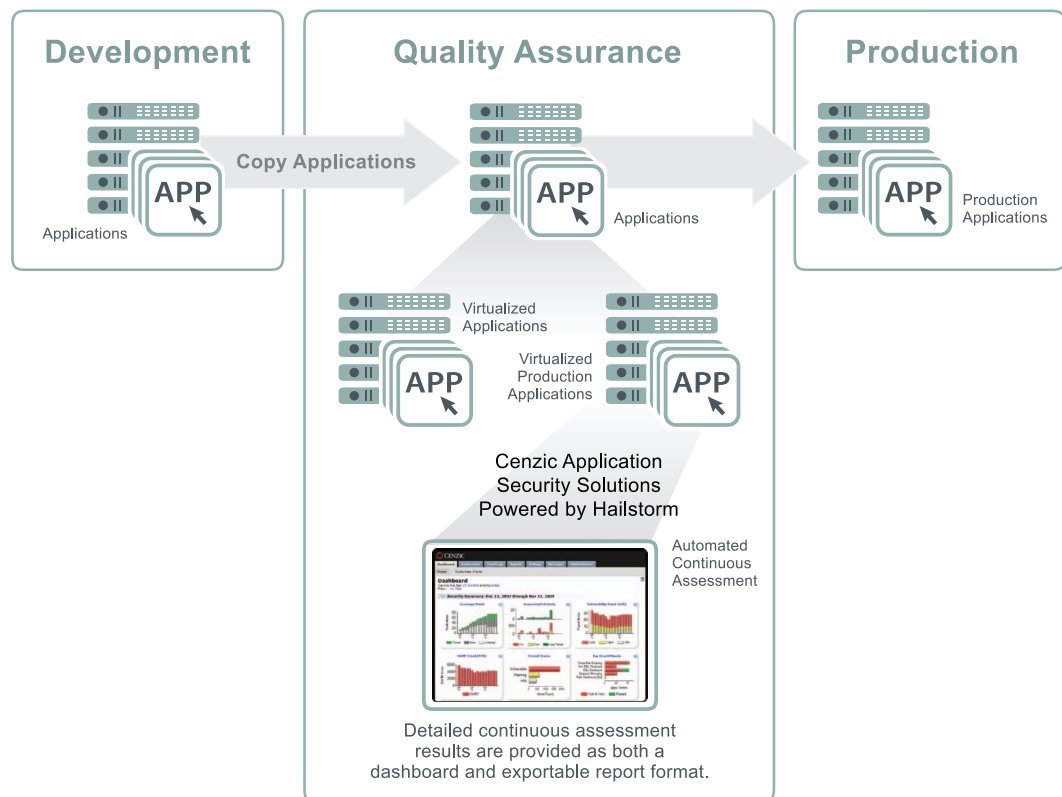
When integrating with virtualization technology, companies can improve upon continually tested production applications by bringing in a virtual or “staging” environment without risk of compromising the production environment.



Continuous Assessment of Production Applications

Until now, most companies have not tested production applications because application security assessment has been an invasive process with the potential to pollute and corrupt databases and impair application performance. Without great risk, it had simply not been possible or practical to conduct a thorough assessment in a production environment.

Cenzic offers an innovative solution to this problem. Cenzic is integrated with VMWare solutions that allow customers to test their production applications in a virtualized environment, seamlessly. This integration allows customers to continuously test previously virtualized applications in Q.A. with new attacks on an ongoing basis. In addition, customers can test their production applications in real time by taking a snapshot using VMware and then testing them with Cenzic.



The images of the production applications on a server become the temporary staging environment upon which the assessments can be safely performed. The ease of configuration, creation of snapshots of existing applications and the restoration of the staging environment to prepare for follow-on assessments combine to easily allow vulnerability testing in a smooth and continuous fashion. And, all application security testing can be automated.



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.