

Whitepaper

# **Continuous Testing of Production Web Applications**

Executive Summary ..... 3

Web Application Security Optimization (W.A.S.O.) ..... 4

Continuous Assessment of Production Applications ..... 5

Two Easy Ways to Perform Continuous Assessments ..... 6

About Cenzic ..... 7

## Executive Summary

Web application security is a key top-of-mind concern for general managers, CISO's, CIO's and security staff for businesses ranging from Fortune 100 multinationals 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 shows information security teams the importance of focusing on Web application security.

Current methods of addressing the application security problem 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 Web 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 Web applications, and not just the ones in development and quality assurance stages, but live applications already performing business critical functions. Remarkably, these are the applications which are tested the least, if at all.

Business managers and security leaders in Fortune 2000 corporations tell us that over 90% of their 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 from legacy systems with Web-enabled front ends to internal systems. These often support mission critical processes from business operations to supporting infrastructure providing 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 Web 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; no longer putting production web applications at risk.

Companies can now easily and quickly, add vulnerability testing to their list of activities for all of their Web applications including production applications. Using a continuous testing methodology across a company's Web application portfolio will significantly enhance the security of all Web applications.

## Web Application Security Optimization (W.A.S.O.)

Due to the unceasing onslaught of hackers' employing new methods to get to valuable customer data organizations simply must understand that securing 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 Web applications – both developed and in production is vital to overall Web application security.



Cenzic has defined a process called the Web Application Security Optimization (W.A.S.O.) 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 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 the Fix and Block vulnerabilities stage (Development and QA Team). Since the process is a continual cycle, the fixing or blocking of the Web 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 Web Application Security Optimization.

Together, the development team, QA team, and Operations team can easily employ this W.A.S.O. process. With W.A.S.O. the entire team can stay on top of vulnerabilities that affect all the company's Web applications – the ones 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

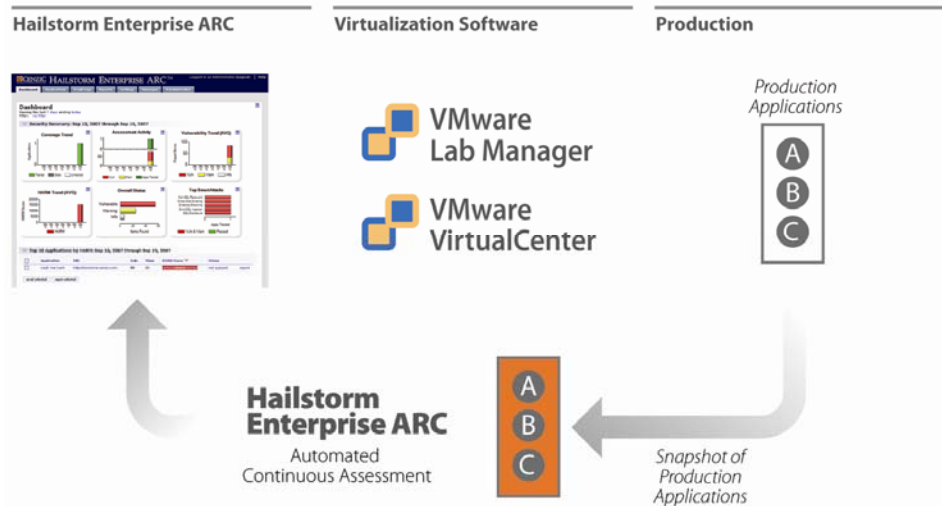
Until now most companies have not tested production applications because application security assessment is an invasive process with the potential to pollute and corrupt databases and impair application performance. Without great risk it has simply not been possible or practical to conduct a thorough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

Cenzic is introducing an innovative solution to this problem. Cenzic is announcing integration with VMWare solutions that allow customers to test their production applications in a virtualized environment seamlessly from the Cenzic Hailstorm Enterprise ARC product. This integration allows customers to continuously test previously virtualized applications in Q.A. with new attacks on a weekly or monthly basis. In addition, customers will be able to test their production applications in real time by taking a snapshot using VMware and then testing them with Hailstorm ARC.

Cenzic is the only company that now offers continuous security testing through all stages of an application's lifecycle – from development to Q.A. to production (operations). All in an automated fashion.

Automating the Web application security assessment by combination VMWare, used in the product environment and Cenzic Hailstorm Enterprise ARC is an obvious way to test and then re-test production application without risk. 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.

### Continuous Testing in a Virtualized Environment

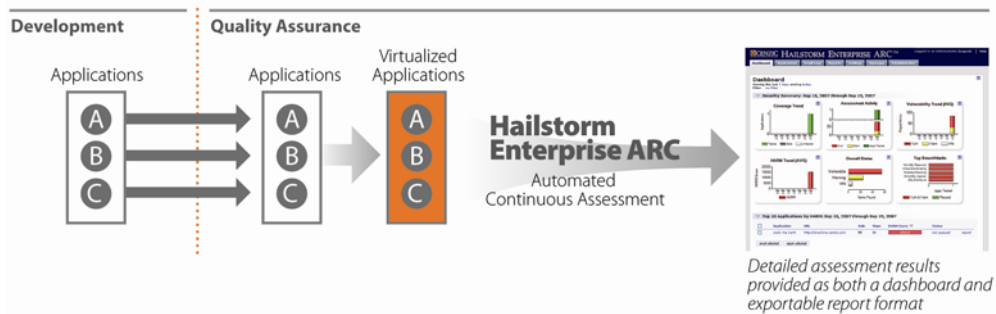


## Two Easy Ways to Perform Continuous Assessments

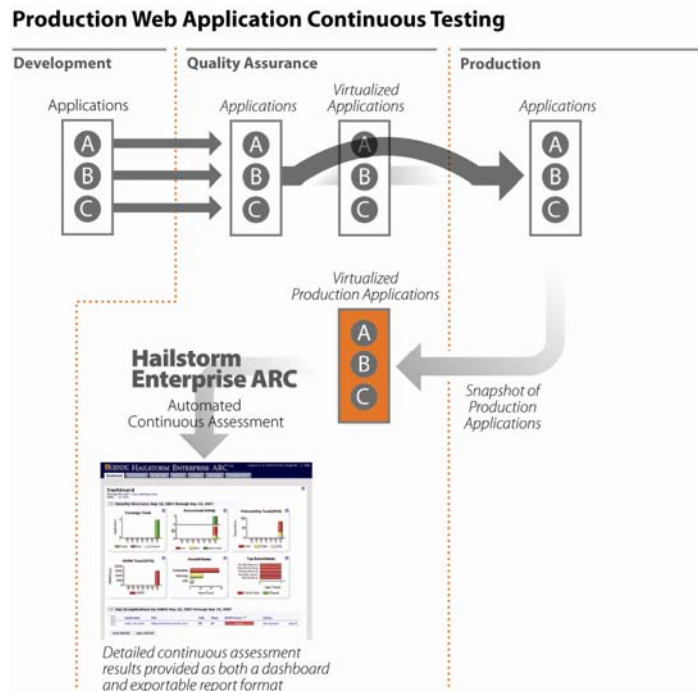
Vulnerability testing for production applications can be initiated from the Hailstorm Enterprise ARC Web environment in two simple ways.

**#1.** If you have a virtualized server with your applications running in QA you can test those Web applications by turning on the virtual servers from Hailstorm ARC, running assessments, reporting results into the dashboard, and then turning off the servers. Because these virtualized applications were images of the production applications when they were deployed, the code hasn't changed, therefore they are true replicas of production applications. By doing continuous testing with new attacks, organizations can stay ahead of the new vulnerabilities unleashed by malicious hackers.

### Web Application Pre-production Testing



**#2.** Or you can take a snapshot in real-time of your production applications and test the snapshot of the applications. In order to test the production applications in real-time, companies will have to take snapshots of the production applications, and using Hailstorm Enterprise ARC, deploy the virtual machines, test using Hailstorm assessments, report results to the dashboard, and release the virtual servers.



Using either of the two methods you can test and re-test your applications as many times as necessary without the risk of corrupting the databases or the applications themselves.

## About Cenzic

Cenzic is the innovative leader of next-generation application security assessment and risk management solutions that quickly and accurately find application vulnerabilities and are the only solutions in the market to provide continuous testing for all Web applications including the ones in production. The Cenzic suite of application security solutions can fit any Company's needs from remote assessment ([ClickToSecure®](#)), to a full enterprise-wide solution ([Cenzic Hailstorm® Enterprise ARC](#)) for effectively managing application security risk across an enterprise. Cenzic solutions, targeted at financial services, e-retail, high-tech, energy, healthcare and government sectors, are the most accurate, comprehensive, and extensible in the industry.