



Cenzic Hybrid

Application Security Software + Services



Table of Contents

Overview	3
The Need for Cloud, Mobile and Web Application Security	3
Cenzic Hybrid – Software + Services to Test Cloud, Mobile and Web Apps	3
Cenzic Application Assessment Dashboard	4
Software: User Type & Business Case	4
User Type.....	4
Business Case.....	3
Managed Service: User Type & Business Case	5
User Type.....	5
Business Case.....	5
Cenzic Hybrid Offering: User Type & Business Case	5
User Type.....	5
Business Case.....	5
What Makes Cenzic Unique? Technology.....	6
Behavioral-Based Approach to Black Box Testing.....	6
Cenzic’s Attack Arsenal: SmartAttack® Library	6
Cenzic’s Measurement of Risk: HARM® Score	6
Cenzic Hailstorm Technology.....	6
About Cenzic	7



Overview

The Need for Cloud, Mobile and Web Application Security

The Internet is the world's biggest development platform and web-based application development represents 65% of most organization's new application development projects (both internal and external). For a number of these organizations the ability to hire and retain application developers trained in secure coding is limited at best. Many find the same challenge exists within the ranks of their Information Security counterparts. Generally speaking, the number of web application security scanning specialists required to effectively monitor an organization's application risk is one per 100 web applications – and most organizations also have Cloud and Mobile apps deployed. However, due to the associated expense, the rarity of these particular skill sets, and the less-than-predictable demand for these services, they staff to “steady state”.

Steady state is the ability to predict and meet the demand of the number of scanning/compliance requests regardless of the requester, source or technical/logistical challenge. Many organizations say that they are effectively managing to steady state 93-95% of the time, but that they struggle with the exceptions. These exceptions, by nature, represent the most mission-critical, highly-visible, sensitive and strategic applications within an organization. Their challenges include, but are not limited to – an increase in scanning volume, filling air gaps (off network or remote scanning), or monitoring more complex applications/business logic. Consequently, the ability to reach out on demand to supplement and compliment those organizations application security specialists is critical.

Cenzic Hybrid – Software + Services to Scan Cloud, Mobile and Web Apps

Cenzic Hybrid is a combination of software and managed services that allows users to run their own Cloud and Web application vulnerability assessments (using software) as well as leverage Cenzic's security experts (using managed services) to perform additional application vulnerability tests, including testing Mobile apps, when the need arises.

Cenzic Hybrid is unique because Cenzic is the only company that delivers its desktop and enterprise software, as well as managed service solutions, through a common framework. This enables organizations to leverage several deployment options, such as:

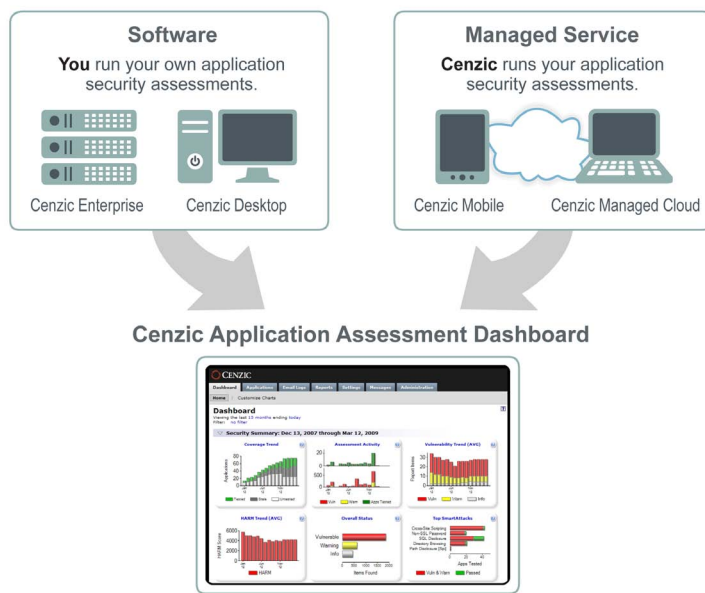
- Start small and grow overtime
- Remote or off-network scanning requirements
- Ability to augment internal teams with Cenzic's scanning resources
- A combination of all three above

Cenzic's unified architecture delivers a common database and central dashboard that enables a holistic, role-based view of your organization's application security risk posture.

- Benefits of this common framework include:
 - Consistent and accurate results
 - Centralized view into security of all applications using Cenzic
 - Minimized learning, as the products use the same reports and dashboard
 - Ultimate product flexibility that mirrors your company's ever-changing security needs.



Cenzic Hybrid



Cenzic Application Assessment Dashboard

Single, Unified View of All Applications Assessments.

Cenzic Hybrid Centralized View into All App Testing

Cenzic Application Assessment Dashboard

The Cenzic’s application assessment dashboard provides a standardized platform to manage Cloud, Mobile and Web application security risk throughout the enterprise. Role-based visibility provides a company-wide view of security status to executives as well as customized views to other users. Access is managed through the dashboard to control permissions of users and govern application access.

The dashboard is designed so that users do not need to be security experts to run application tests and pull reports from Cenzic’s application assessment dashboard. From an intuitive interface, users can quickly see applications tested, vulnerability trends, applications most at risk, performance of business units conducting and remediation assessments. Cenzic’s application assessment dashboard also gives users a summary of testing results including a prioritized listing of vulnerabilities based on Cenzic’s quantitative risk scoring system (HARM®) to show what needs fixing first.

Software: User Type & Business Case

Cenzic Enterprise protects online applications against hacker attacks. It’s used to scan Cloud and Web applications for security vulnerabilities and display results in a drillable dashboard for easy reporting and risk management. The modular architecture scales to handle all the enterprise assessments and supports the entire software development life cycle (SDLC) through a role-based permissions model.

User Type

All user types – from security experts to non-experts – can utilize Cenzic Enterprise. However, security expertise is needed to install, set-up, and manage the enterprise software product. These administrators determine who can conduct robust testing on complex applications versus who can perform basic testing on less critical applications. Such role-based flexibility makes it easy for anyone in the SDLC to conduct security tests – development, QA, information security and management.



Business Case

There is a solid business case for software purchases if companies possess the security expertise needed to manage the product and ensure it is being used effectively. The company must also commit to using the product for at least two to three years to realize an ROI. Often times, however, security budgets are cut along with key security experts who manage these systems, so it is important to have another way to test during such economic times. Whether a software or managed service technology is used, any company will need remediation services (in-house or via a partner) to correct the insecure code once it has been identified.

Managed Service: User Type & Business Case

Cenzic Managed Cloud is a managed service that detects Cloud, Mobile and Web application vulnerabilities before they are exploited by hackers (NOTE: Mobile application services only available with Cenzic Managed Cloud). Cenzic's security experts test applications remotely using its automated testing technology – powered by Cenzic Hailstorm technology. No software. No hardware. No installation needed. It's an ideal way to quickly improve your application security posture with minimal resources and limited budget.

User Type

The typical user type for a managed service offering is someone who is the sole security expert in the company who needs additional help to run Cloud and Web application scans and/or wants to run Mobile application scans. Less knowledgeable security users could use this service, but they would need to rely heavily on others in the company to determine which web applications should be tested, how often, and how vigorously. However, a basic understanding of security is required.

Business Case

A business case can be made for a managed security service if companies want to utilize their security experts solely on remediation and results interpretation instead of software deployment and management. Also, an ROI is realized much faster, as no time is needed with the usual software installation, management, and learning curve. Whether a software or managed service technology is used, any company will need remediation services (in-house or via a partner) to correct the insecure code once it's been identified.

Cenzic Hybrid: User Type & Business Case

Cenzic Hybrid offering is a combination of our software and managed services – it allows users to run their own Cloud and Web vulnerability assessments (using software) as well as leverage Cenzic's security experts (using managed services) to perform additional Cloud and Web app vulnerability tests when volume increases and/or scan Mobile apps.

User Type

The user type for the hybrid offering is not just one kind of person. It is a technology philosophy that a company adopts when they know their security budgets and expertise are ever-changing. The solution is the best way to “hedge your bets” on how to best tackle security challenges. In other words, during good economic times, bigger budgets allow hiring enough security experts to run the software and deliver results. During tougher times when budgets and personnel are cut, companies can rely on a managed service to deliver their website tests.

Ultimately however, the person who runs the software product will also run the managed services offering to ensure all web applications are being tested in the most efficient way.

Business Case

A business case is easily made for the hybrid solution when application security scans are needed immediately and security expertise is in demand. Often, Cenzic Hybrid customers start by purchasing the software, and while the implementation and training are taking place, they utilize the managed services to “kick start” their security posture.



A benefit of this solution is knowledge transfer. Cenzic security experts who run the managed service will work with your company’s security personnel and provide best practices on how to run security scans as well as how best to use Cenzic software.

And unlike other hybrid solutions that use disparate products, Cenzic’s software and managed service technologies use the same technology backbone, so results are consistent and accurate. The benefits include flexible, integrated options for fast results how and when you need it.

What Makes Cenzic Unique? Technology

All Cenzic products are built on the same Hailstorm technology that has made Cenzic one of the most accurate and sought-after companies in the market.

Behavioral-Based Approach to Black Box Testing

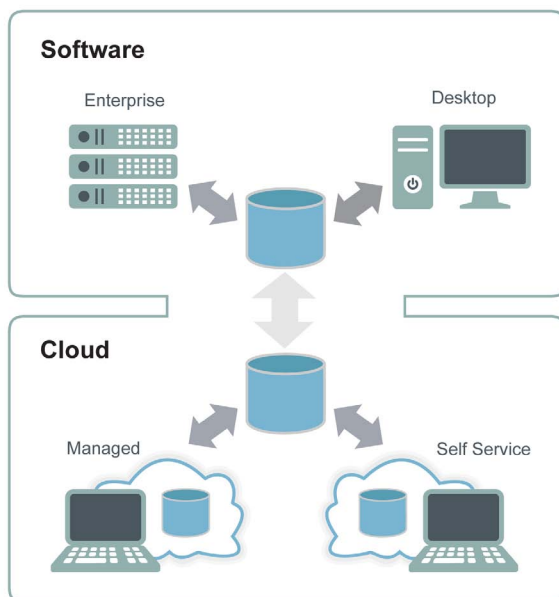
Cenzic’s Hailstorm technology goes beyond a static / signature-based approach by emulating a true hacker with a behavioral-based approach that maintains the state of the application while attacking the application at the browser level. By using a browser to attack applications at the web level, Cenzic finds all critical vulnerabilities including application logic tests such as session hijacking, strong passwords, privacy policy validation, etc. as well as all the core vulnerabilities like XSS, Buffer Overflow, SQL Disclosure, and others. And, only Cenzic Hailstorm can test for vulnerabilities across all types of applications including commercial and proprietary applications, Web infrastructure and all stages of a Web application. This non-signature based technology has made Cenzic solutions the most accurate in the industry, yielding few false positives and finding more “real” vulnerabilities.

Cenzic’s Attack Arsenal: SmartAttack® Library

Cenzic SmartAttacks are automated attacks that simulate a hacker trying to compromise or cripple an application. These attacks are termed “smart” because their objective is to find vulnerabilities rather than to compromise the application. Cenzic Hailstorm’s vulnerability discovery is driven by the SmartAttack® library, which encapsulates best practices to test application attack resistance and validate conformance to regulatory and internal security compliance.

Cenzic’s Measurement of Risk: HARM® Score

Also, incorporated into the Cenzic Hailstorm technology is its scoring system called HARM (Hailstorm Application Risk Metric). It is a quantitative score for the risk associated with a Cloud, Mobile or Web application. The score is based on how easy the vulnerability is to exploit and how damage can be done if a breach occurs. Because HARM the scores of multiple applications can be compared it helps to determine a priority list of which application needs to be remediated first. Another benefit is that you can compare the HARM score for a single application across a time period to show IT professionals they are improving their security posture. If the application scored 10,000 three months ago and scores 5,000 today, IT professionals can be confident in knowing they are moving in the right direction.



Cenzic Hailstorm’s Unified Architecture

Cenzic Hailstorm Technology

Cenzic Hailstorm’s technology architecture is the common framework for both our software and managed service offerings.



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.