



Leveraging Managed Services for Cloud, Mobile and Web Application Security



Table of Contents

Overview3
Application Security Vulnerabilities.....3
Application Vulnerability Testing Challenges3
Consequences of Forgoing Vulnerability Testing4
The Burden of Testing4
Problem Overview4
Historical Approach to Application Security Assessment.....5
The Solution: Managed Service Technology for Cloud, Mobile and Web Application Security ..5
Cenzic Managed Cloud.....5
About Cenzic6



Overview

Information security managers and directors are faced with the enormous responsibility of keeping Cloud, Mobile and Web applications secure from hackers. The ever-growing number of security threats and an increasing body of governmental regulations are overwhelming information security teams. With Cloud, Mobile and Web applications constantly evolving, finding vulnerabilities is a challenging, costly, and time-consuming undertaking. How can information security personnel protect sensitive data – and ultimately, the corporate reputation – without costly application security assessment outsourcing?

The solution is automated security assessment products that leverage stateful processing to comprehensively examine Cloud, Mobile and Web applications and reveal vulnerabilities in hours rather than weeks. These powerful solutions help information security teams quickly identify problems, regularly assess Cloud, Mobile and Web application security strength and ensure regulatory compliance.

Application Security Vulnerabilities

Cloud, Mobile and Web applications are growing in size and complexity. Despite their sophistication, these applications are designed to respond to simple HTTP requests. These requests can put applications and confidential information at risk as hackers can shield attacks with legal requests that pass through secured networks and intrusion detection systems. Once a malicious request interacts with a Cloud, Mobile or Web application, it can attack via vulnerabilities within the application. Some of the top Cloud, Mobile and Web application vulnerabilities include:

- Cross Site Request Forgery
- Ineffective Session Termination
- Session ID Identification
- Application Path Disclosure
- Un-validated input
- Broken access control
- Broken authentication and session management
- Cross-site scripting (XSS) flaws
- Buffer overflows
- Injection flaws
- Improper error handling
- Insecure storage
- Insecure configuration management

Cloud, Mobile and Web application security attacks are getting more and more prevalent. Whether it was the attack against Hannaford Brothers Supermarkets, TJ Maxx, Harvard servers or thousands of other sites, the news of application breaches keeps coming. The most recent Cross-Site Scripting (XSS) attack on the Obama Campaign site that redirected voters to Hillaryclinton.com highlights the problem of easily exploitable holes in most applications.

Application Vulnerability Testing Challenges

The consequences of failing to protect Cloud, Mobile and Web applications expose companies to information theft, unhappy customers and stiff penalties when organizations are not in compliance with regulatory requirements.

Even when companies do take steps to protect against Cloud, Mobile and Web application hacking, they often face overwhelming workloads or exorbitant security assessment outsourcing costs.



Consequences of Forgoing Vulnerability Testing

Loss of critical customer data and violations of government regulations are two of the largest consequences of bypassing application vulnerability testing.

Information Theft

Data theft takes many forms, including siphoning money from banks and financial institutions, exploiting e-commerce sites to conduct unauthorized transactions and accessing back-end databases with priceless stores of data. Information theft can force corporations to make financial restitutions and lead to customer loss.

Non-Compliance

Cloud and Web applications that are not in compliance with government regulations, such as Sarbanes-Oxley, GLBA, SB 1386 and HIPAA, can result in severe corporate penalties. With new regulations on the horizon, corporations need a way to assess and respond quickly to regulatory requirements.

The Burden of Testing

Performing regular security assessments on Cloud and Web applications, exposing vulnerabilities and quickly fixing them are complicated undertakings.

Staff Overload

Running internal security assessments on Cloud and Web applications is a time-consuming burden on internal information security staff. Skilled hackers have far outstripped the ability of information security staff to deal with them. Testing and securing these applications is more complex than network security. Just one Cloud or Web application may contain tens of thousands of lines of code and countless dynamic interactions between components, making finding security vulnerabilities an extremely daunting task.

Exorbitant Costs

When companies do not adequately test and protect their Cloud and Web applications in-house, they must outsource the job to application assessment consultants. Because qualified consultants are rare and very expensive, testing complex these applications for vulnerabilities manually can be very costly and time consuming. Enterprises can easily spend millions of dollars each year on manual penetration testing that covers only a small fraction of their Cloud and Web applications. Even a smaller company can easily spend \$25,000 to \$50,000 to test an average-sized Web application a single time with no assured level of consistency.

Problem Overview

Cloud, Mobile and Web applications are proliferating and their availability present irresistible temptations to hackers. The applications contain vulnerabilities in a myriad of forms. For example, a common hacker attack is SQL injection, which involves altering the expected content submitted via a form by inserting unexpected text, such as logic altering SQL code, often resulting in unrestrained database access.

Challenges assessing Cloud, Mobile and Web application vulnerabilities include:

- **Application vulnerabilities are growing every month:** With 400+ new Cloud, Mobile and Web vulnerabilities discovered every month, the sheer volume of vulnerabilities outstrips information security professionals' ability to deal with them.
- **Applications are growing in complexity:** Cloud, Mobile and Web applications are rapidly growing in number and complexity, making it extremely difficult and costly to test and secure even a small percentage of a company's these critical applications.
- **Application security professionals are hard to find:** The majority of information security professionals do not understand the complexities of application security.



- **Existing staff are overloaded:** Because most security personnel are already overworked, Cloud, Mobile and Web application security is a low priority.
- **Cost:** Outsourcing Cloud, Mobile and Web application security assessment to outside consultants is extremely costly.

Historical Approach to Application Security Assessment

In the mid-1990s, network scanning tools and manual penetration testing made up the core of security assessment methods. It was not until the late 1990s that securing Web applications became a concern. Ethical hacking was the typical solution and involved in-house personnel or hired security consultants – often former hackers – who attempted to break application security methods. However, few businesses were focused on keeping their applications secure and no sophisticated tools existed to aid in the process. Instead, expert knowledge and experience was necessary.

Sensing an opportunity, the big consulting firms and boutique security consultancies began offering manual security assessment services using teams of experts. Although effective, they were very costly and often took weeks or months to perform their assessments. Many companies are still outsourcing application security assessments to external system integrators.

By 2000, application scanners entered the market and were able to scan Web applications for limited vulnerabilities such as buffer overflows. Although ambitious in their aim, these tools provided many false positive results, leaving companies with an enormous workload to locate actual vulnerabilities.

In 2004, the next generation in automated solutions, known as Stateful Assessment products, entered the market. Able to maintain the state of an application while testing, these solutions are able to emulate a hacker and assess security vulnerabilities at very high speeds, reducing false positives and the costs traditionally associated with manual assessments.

Although the Stateful assessment-based products are very effective in automating and providing accurate security assessment results, many companies are not able to take advantage of the technology due to lack of internal security expertise. These companies have traditionally either outsourced all of their application security assessments or have done very little proactive security assessments. As a result, they have few people with application security knowledge who are already overworked. These companies need a solution that uses a powerful technology without bringing it in house in the short term.

The Solution: Managed Service Technology for Cloud, Mobile and Web Application Security

A managed service solution that leverages a powerful technology platform allows companies to “jump start” their application security process without the overhead of installing software or hardware or dealing with implementation issues. This is particularly effective for companies, large and small with minimal in-house security expertise or resources.

The managed service allows companies to have the vendor run the assessment for them, get the results in a professional report, and start working on remediation through their development process. This approach is far more cost effective than manual security assessment and penetration testing and companies can eventually transfer it back in-house once they have built the expertise.

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.

- 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

Due to the unceasing onslaught of hackers’ employing new methods to access valuable data organizations, application security must be an ongoing effort. Effective application security is not a one-time event, but a discipline of testing and re-testing – continuously throughout an application’s lifecycle. Continuous testing is the only way to protect applications from the hundreds of new threats that come out every month. Cenzic Managed Cloud supports ongoing application testing – even when apps are in production.

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.