

# Staying Ahead of the Hacker Curve

## Turn-key Web Application Security Solution

Website Testing / Vulnerability Scanning (Cenzic) & Web Application Firewall (Citrix)

# Detecting Flaws & Protecting Websites before Hacker Exploitation

## Integration Overview

The Cenzic / Citrix integration best protects websites against hacker attacks by detecting and then protecting them against a broad range of threats. Cenzic's web testing (vulnerability scanning) solutions combined with the Citrix's web application firewall is a powerful combination that prevents breaches and secures websites for both on-premise and cloud-based application deployments. The integration provides a "1-2 punch" against website hackers, as Cenzic identifies the website weaknesses and Citrix blocks against them until the flaws can be fixed.

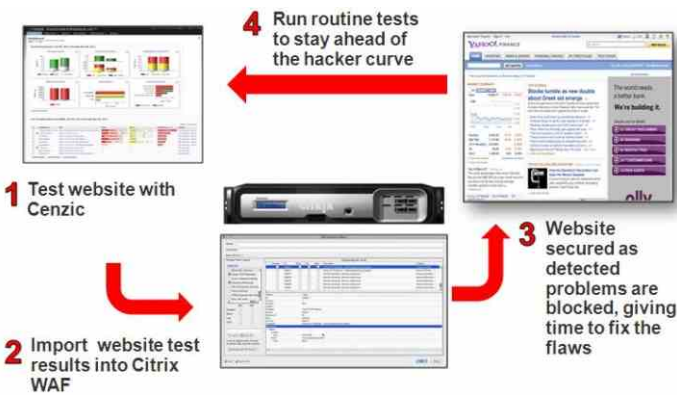


Figure 1: The Cenzic / Citrix integration.

The technologies together provide a "1-2 punch" against website hackers.

- 1 Websites are tested for security flaws using Cenzic products
- 2 Results are imported into the Citrix WAF
- 3 The Citrix WAF then blocks against those detected flaws until they can be fixed
- 4 Users routinely run website security tests to ensure they are staying ahead of the hacker curve

## Why Web Application Security is Important

Hackers are unrelenting. Whether it's politically motivated attacks from rogue states, or financially motivated attacks, there is a continuous stream of new security threats. Many of these attacks have been successful in causing major damage. Senior IT and security managers at small and large enterprises, hosting providers, managed security service providers (MSSP), cloud computing companies and government agencies have a huge challenge in addressing various security issues to protect their web infrastructure.

With approximately 75% of all Internet attacks targeting web applications, it's critical for companies to be prepared to defend their information assets diligently. This is becoming even more important, and more challenging, as these applications are developed and deployed within cloud environments.

While various network security technologies have succeeded in protecting the network layer, hackers can easily circumvent these security measures by attacking the web application layer. For example, it is straightforward to inject damaging attacks through commonly-used HTML forms and fields that can be manipulated by all application users, but it is not detected by either network firewalls or intrusion protection systems (IPS).

## What are the main contributors to web application vulnerabilities?

Firstly, most application developers have not been trained to consider security implications when developing applications. Secondly, even developers who have been trained are typically under pressure to release new functionality against an ever-narrowing development schedule. Even when they have the 'luxury' to test security, most don't have the right tools to discover vulnerabilities in the application.

For many businesses and government agencies, web application security carries even more significance due to the sensitive nature of the information used within the application.

Many web applications have direct connectivity with one or more databases containing private customer and company-specific intellectual property. It is this direct connection to information databases that make web applications a rich target for hackers.

Threats against web applications are often devised specifically for a target application, making threat identification by network-level security devices impossible. Relying on network security solutions leaves web applications exposed to a myriad of known attacks and zero-day exploits. Web application owners must figure out how to quickly discover security holes and develop an effective remediation plan - before significant damage occurs.

## Integration Details: Deploying Cenzic & Citrix

Utilizing Cenzic website security testing information with the Citrix WAF is a fully validated and straightforward process. Initially Cenzic Hailstorm or Cenzic ClickToSecure products perform an automatic security scan to identify any weaknesses within the tested Website applications. The user then receives a detailed vulnerability report to initiate remedial action. The detected vulnerabilities are exported from the Cenzic product to the Citrix NetScaler Application Firewall module via an XML file. After receiving the website security flaw information, Citrix's WAF automatically generates policy settings to protect the website and bind the Application Firewall profile within minutes. No additional configuration or learning is needed.

## Why Cenzic?

Website security is all about risk management. You need to know how many websites / web pages you have, where they are, which ones have been tested, what security flaws exist, how to prioritize those flaws and, finally, how to monitor on-going changes.

Cenzic provides answers to all these questions. With an easy-to-use interface, security teams can quickly run assessments on websites to find the security flaws that hackers most often exploit. The dashboard and reports provide decision support information at your fingertips so you can start acting on the results immediately.

## Cenzic helps users:

- Run website vulnerability assessments (i.e. tests)
- Provide actionable report information with remediation tips
- Help prioritize website flaws based on a quantitative metric
- Identify risks in various business units and/or specific websites

Cenzic offers on-premise and cloud-based solutions for ultimate flexibility in product choice. Cenzic ClickToSecure Cloud is a cloud offering where users access the technology to test Websites for basic hacker attacks and get actionable results all within their own Web portal. And Cenzic Hailstorm is an on-premise software suite that provides robust testing of websites where the user downloads, installs, and performs the scans all on their own.

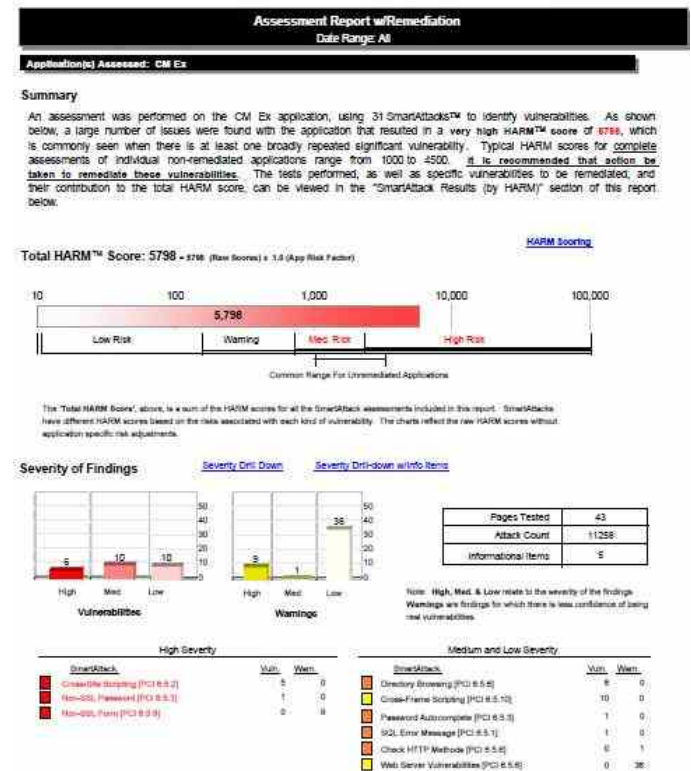


Figure 2: Cenzic website security flaw (vulnerability) report  
Figure 2 is an example of a typical Cenzic web vulnerability scanning report (first page). Cenzic reports provide an assessment summary of your Website's security flaws, easy-to-read severity charts, a prioritized listing of your vulnerabilities, findings on how your website meets compliance requirements, security flaw details and directions on how to fix them.

## Why Citrix?

With Citrix NetScaler Application Firewall, Citrix Systems delivers the industry's most comprehensive and fastest Web Application Firewall product line, with throughput rates supported from 500Mbps to over 12Gbps. Leveraging NetScaler's advanced nCore technology that powers the world's largest data centers, the NetScaler Application

Citrix NetScaler Application Firewall helps organizations address security challenges by:

- Providing the advantages of a positive security model to secure against attacks that are hard to protect with constant signature updates and using an adaptive learning engine to discover aspects of application to generate human-readable policy recommendations

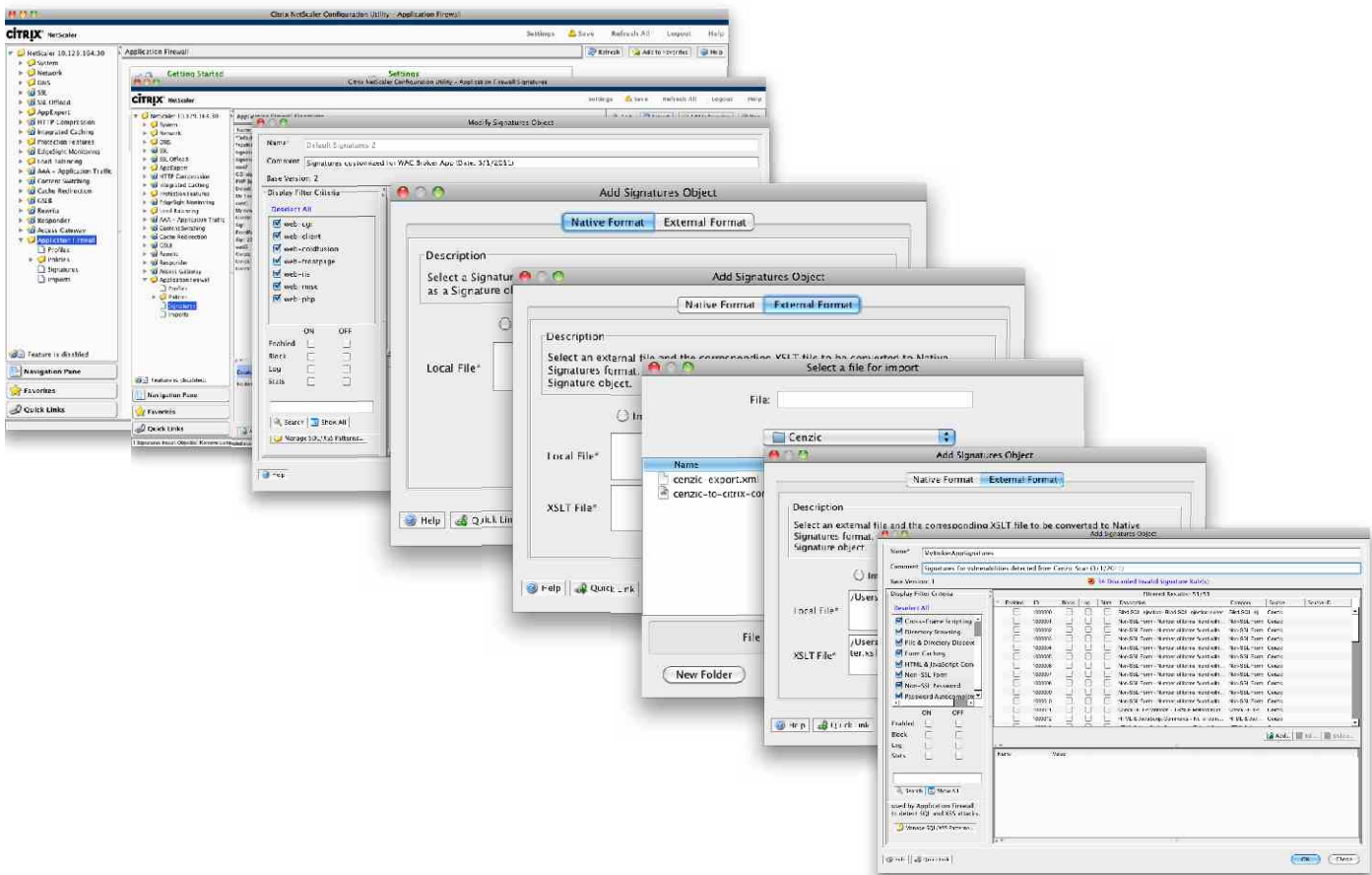


Figure 3: NetScaler Application Firewall

Firewall provides an ideal union of security, scalability and “pay-as-you-grow” performance.

The NetScaler Application Firewall is available as standalone hardware appliance, as well as a fully integrated module for NetScaler MPX hardware appliances and NetScaler VPX software-based virtual appliances.

- Conforming to privacy and data security mandates such as PCI/DSS by securing credit or debit card numbers, and administratively defined data objects to prevent inadvertent disclosure of sensitive application content
- Centralizing security for all Web applications and Web services to greatly simplify security management and to provide consistent security across all corporate, with complete separation of each application's security policies, controls, reporting details and log data

- Providing flexibility to adapt to changing business by enabling flexible, stepwise deployment of Web application,
- Protecting by using default and advanced profiles that includes authenticated access to sensitive data, and
- Enabling deployment flexibility with availability on multiple hardware and virtualized appliance platforms to meet the performance and availability requirements of any organization.

## About Cenzic

Cenzic provides software and SaaS security solutions to help organizations secure their websites against hacker attacks. Cenzic focuses on web application security, automating the

process of identifying security defects at the web application level where more than 75 percent of hacker attacks occur. Its dynamic, black box Web application testing is built on a non-signature-based technology that finds more “real” vulnerabilities as well as provides vulnerability management, risk management, and compliance for regulations and industry standards such as PCI or HIPAA. The Cenzic solution suite fits the needs of companies across all industries, from an entry-level, on-demand cloud solution (Cenzic ClickToSecure Cloud), to remote testing performed by Cenzic security experts (Cenzic ClickToSecure Managed), to a full enterprise software product (Cenzic Hailstorm Enterprise ARC) for managing security risks across the entire company. [www.cenzic.com](http://www.cenzic.com)



Worldwide Headquarters  
Citrix Systems Inc.  
851 West Cypress Creek Road  
Fort Lauderdale, FL 33309, USA  
T +1 800 393 1888  
T +1 954 267 3000

[www.citrix.com](http://www.citrix.com)

Americas  
Citrix Silicon Valley  
4988 Great America Parkway  
Santa Clara, CA 95054, USA  
T +1 408 790 8000

Europe  
Citrix Systems International GmbH  
Rheinweg 9  
8200 Schaffhausen, Switzerland  
T +41 52 635 7700

Asia Pacific  
Citrix Systems Hong Kong Ltd.  
Suite 3201, 32nd Floor  
One International Finance Centre  
1 Harbour View Street  
Central, Hong Kong  
T +852 2100 5000

Citrix Online Division  
6500 Hollister Avenue  
Goleta, CA 93117, USA  
T +1 805 690 6400



## About Citrix Ready

Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry leading alliances and partner eco-system, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at [www.citrixready.com/ready](http://www.citrixready.com/ready).