



## RAPID7 NEXPOSE

### BENEFITS

#### Secures the complete Web application

Rapid7 NeXpose identifies vulnerabilities throughout the entire application, scanning the browser and server-side components for exposures that other Web application scanners do not find.

#### Scans Web 2.0 applications

Rapid7 NeXpose is the first vulnerability scanning solution that analyzes JavaScript, AJAX and Flash applications in testing, quality assurance, deployment and ongoing management.

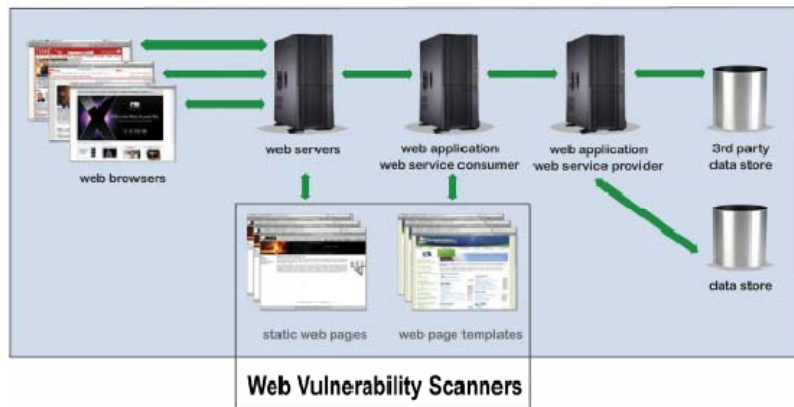
#### In-Depth Web Scanning

Scans web applications for known vulnerabilities, including SQL Injection and Cross-site scripting. Provides deeper scans through the Rapid7 browser emulation technology.

## Web Application Scanning

Web technologies have enabled the Internet to develop into an application platform, becoming the platform of choice for both internal and external corporate applications. Today the set of Web technologies and programs known as Web 2.0 is cultivating a social trend of new behaviors enabling real time communication and information sharing.

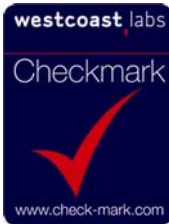
The popularity of Web applications have made them a choice target for hackers who attempt to corrupt data, crash hosts, gain access to the corporate network and steal valuable information. Because they exist as a conduit between external users and a company's internal databases, Web applications can be one of the biggest IT security risks. For Web sites that take credit cards, the risk transcends the corporation to individuals who conduct e-commerce on the Internet. Web applications need to be regularly audited and closely monitored for changes and improper usage.



## COMPLEXITY OF WEB APPLICATIONS

This diagram provides a simplified look at the many components involved in a Web application. In each area, there could be vulnerabilities that must be located and remediated to reduce the risk of attack. To effectively find and remediate vulnerabilities in Web applications, security administrators need reliable scanning solutions that dig deeper into the environment and provide a more complete and accurate picture of what security issues may be lurking inside of a Web application.

Most Web application scanners target the developer, enabling them to find security risks in their code during development. Once the application goes live, Web application scanners struggle to recognize and uncover vulnerabilities in new Web 2.0 functionality such as JavaScript, AJAX and Flash.



## FEATURES

### Browser Emulation Scanning Technology (BEST)

Scans client-side Web applications to find vulnerabilities in Web 2.0 technologies such as JavaScript, AJAX, and Flash.

### Web Application Pass-Through Scanning

Utilizes found vulnerabilities to scan and report on vulnerabilities that lie deep in the network, providing a more accurate and complete report on Web application exposures.

### Content Scanning

Scans applications for specific content such as credit card and social security numbers, ensuring personally identifiable information is not visible to hackers.

### Lone Star Bank

"NeXpose gives us a wider view of what's happening as it assesses all IT systems and devices across the organization, including Web applications, databases, firewalls, switches and routers. ... All of these can be scanned for vulnerabilities, a major reason we chose NeXpose."

### About Rapid7

Rapid7 is a leader in vulnerability management and compliance, delivering a single unified solution across an organization's entire infrastructure. Rapid7 NeXpose is the only solution that includes support for web applications, databases, operating systems, and network devices in a single system, giving direct, actionable visibility into the real threats to mitigate risk and remain compliant. For more information, visit [www.rapid7.com](http://www.rapid7.com).

WA DS 0109

## NEXPOSE VERSUS WEB SCANNERS

	Web Scanners	NeXpose
Browser-Based Scanning		√
Web Application Vulnerability Pass-Through		√
Database Scanning		√
Third Party Application and Database Scanning		√
Operating System Scanning		√
Command Execution	√	√
Parameter Injection	√	√
SQL Injection	√	√
Cross-Site Scripting	√	√
Directory Traversal	√	√
Abnormal Input	√	√
Parameter Overflow/ Buffer Overflow	√	√
Parameter Addition	√	√
Path Manipulation/Path Truncation	√	√
Character Encoding	√	√
MS-DOS 8.3 Short Filename	√	√
Character Stripping	√	√
Site Search	√	√
Application Mapping	√	√
Crawl	√	√
Automatic Form-Filling	√	√
SSL Support	√	√
Proxy Support	√	√
Client Certificate Support	√	√
State Management	√	√
Directory Enumeration	√	√
Web Server Assessment	√	√
HTTP Compliance	√	√
WebDAV Compliance	√	√
SSL Strength	√	√
Certificate Analysis	√	√
Content Investigation	√	√
Spam Gateway Detection	√	√
Client-Side Pricing	√	√
Sensitive Developer Comments	√	√
WebServer/Web Package Identification	√	√
Absolute Path Detection	√	√
Error Message Identification Permissions	√	√
Permissions Assessment	√	√
Known Attacks	√	√
Session Hijacking	√	√