

Rapid7 NeXpose Vulnerability Assessment

Rapid7

DEVELOPER'S STATEMENT

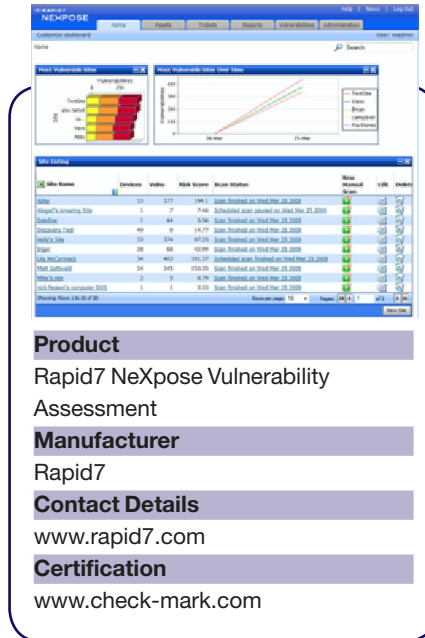
Rapid7 NeXpose helps securities professionals reduce their attack surface by providing actionable insights into the real threats from vulnerabilities across their entire IT infrastructure.

Rapid7's NeXpose Vulnerability Assessment appliance, tested here against the Vulnerability Assessment Checkmark, is the company's flagship product, offering enterprise-level unified vulnerability management, risk assessment and policy compliance reporting.

The primary goal of Rapid7's comprehensive approach to vulnerability detection with NeXpose, is the emphasis on both flexibility and ease of use, while the core function of the product is to audit operating systems, servers, network devices, databases and web applications for known or potential vulnerability threats.

These central abilities are complemented by other key features, including scan result accuracy, asset grouping with access control, risk analysis, report customization, automatic updates, automated ticketing, and remediation workflow.

Installation and setup of the appliance is a simple, fast and seamless task that is well documented from start to finish. Device management is accomplished via an SSL



Product

Rapid7 NeXpose Vulnerability Assessment

Manufacturer

Rapid7

Contact Details

www.rapid7.com

Certification

www.check-mark.com

encrypted web page using a non-standard service port to access the main console.

This facilitates easy navigation to the main sections of Site Creation, Assets, Ticketing, Reports, Vulnerabilities and Administration. Scan tasks are fully customizable, enabling an organization to define and specify assets and segments within their network.

In order to get scans underway, the administrator should enter specifications for IP address scanning by range or host, scan severity, alerts and

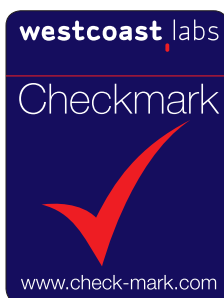
administrative login credentials (if available). This approach is recommended as it provides access to more in-depth information about installed applications on the endpoints.

There are multiple predefined scan templates to choose from and the administrator has the flexibility to create their own. Existing templates cover a wide range of scenarios and include full/normal audit, denial-of-service, penetration testing and database testing.

Scans may be undertaken by one of three distinct scan engines – default, local, or the Rapid 7 Hosted Scan Engine. A series of alerts notifies when a scan has completed or when vulnerabilities have been discovered. Usefully, these can be distributed to the administrator either by syslog, email or SNMP alert.

If accurate reporting is a major factor, then NeXpose will not disappoint. Reports generated include clear, accurate and easily interpreted data in a variety of formats. Several report templates are available and, once again the administrator has the flexibility to create a custom report template of their own.

Reports can be set to record information individually by host or for the entire site, and scheduled to run at a given date and time and sent to specific users if required.



WEST COAST LABS VERDICT

With its flexibility of customization and automated scheduling of scans, combined with the clear, concise and accurate provision of information, Rapid7's NeXpose Vulnerability Assessment appliance has proven why it would be a valued addition to an organization's range of protection.

CHECKMARK CERTIFICATION

Test results from our network gives credence to Rapid7's commitment to reliability and accurate vulnerability detection rating having achieved a Premium level Vulnerability Assessment Checkmark certification.

www.check-mark.com