

NEXPOSE

DEVELOPER'S STATEMENT: NeXpose, a PCI certified enterprise vulnerability management solution, accurately scans networks, databases, Web applications and other software to help organizations find IT security weaknesses and ensure policy and regulatory compliance.

Manufacturer	Rapid7
Contact details	www.rapid7.com/nexpose-vulnerability-assessment.htm

The NeXpose Security Appliance, developed by Rapid7, is an Enterprise level hardware solution and can be installed within a corporate network. Initial setup of the product is made easy by a well explained and easy to follow setup guide and the built-in LCD interface and the procedure is ideal for the company looking to expedite setup and begin securing their network against a wide array of vulnerabilities rapidly. The vulnerabilities being tested against on the simulated SMB network created by West Coast Labs engineers include weak interactive web applications, user-installed vulnerabilities such as games and personal software, and unpatched software by some of today's leading vendors.

Applying updates to the NeXpose Security Appliance is performed automatically, removing the chance of an Administrator forgetting and leaving the network open to attack. Successfully applied updates are displayed on the News area that can be accessed through a link at the top of every page. Each entry on the News section is listed by date and clicking on each entry gives the user access to a list of newly added vulnerability checks and performance upgrades.

After initial setup is complete, the device must be configured to provide a best-fit solution for the needs of each individual company. This is carried out via a web interface that can be accessed from a secure, non-standard port on the NeXpose appliance. The first step towards configuring NeXpose is the creation of users and groups, each of which can be assigned responsibility for the scanning of individual machines or for entire network areas.

Following on from user setup, groups of IP addresses (referred to as Sites) can be created from NeXpose's Home page. The user is asked to enter information such as the name and a brief description of the network, specific user account information, and any scheduling or alerting that is required. However it is in the actual scanning options that the true scalability of NeXpose is revealed. Due to the sheer amount of options, there are a significant number of different configurations available, and thus allow for the creation of potentially wide-ranging scans that can be customized to best-fit each area of a network.

Also included within NeXpose are a series of default scanning options called Profiles, which have been created through the close co-operation of Rapid7 and their existing customers. Even with the high volume of options available to the user, it only takes a very short amount of time



between the appliance being configured to the initiation of the first network scan, a key feature given the speed with which newly announced vulnerabilities can be exploited.

Throughout the network scan, the user is constantly kept aware of the scan progress via a real-time status screen. This screen is split into two windows, the first displaying information including the number of vulnerabilities being tested for and the number detected, a count of detected devices in the given IP range, and the amount of time remaining before the scan is complete. The second window breaks the above information down on a per machine basis and displays the IP address, Operating System, and number of vulnerabilities for each detected appliance.

Reports can be generated in a variety of common formats including PDF and HTML, and formatted differently depending on the intended recipient, ranging from an Executive Overview to the much more detailed Audit Report. The first provides an easy to understand yet thorough breakdown of the information gathered, while the Audit Report includes every detail of the scanned network including device names and addresses. Also included in the Audit Report is remediation advice for each detected vulnerability, saving an administrator or network team vital time otherwise taken up by researching how to defend their network. For those who wish to customize the information presented, NeXpose allows for the creation of user-defined reports.

THE VERDICT

With multiple configurations available and the ability to fit into a network running a number of different operating systems and services taken into account, Rapid7's NeXpose Security Appliance provides a very powerful security solution to any company looking for a more secure IT environment.



NeXpose from Rapid7 is Checkmark certified to the Premium level for Vulnerability Assessment.
www.check-mark.com