

Vulnerability assessment tools are getting better and better as appliances become the platform du jour, reports Peter Stephenson.

This month we looked at vulnerability assessment and penetration test tools. The leading difference between last year's tests and this year's is that this year we saw more hybrid products that offered both vulnerability scanning and penetration testing. We also reviewed a passive scanner for

the first time and saw a lot more attention to meeting regulatory requirements, especially in the payment card industry.

We had a nice bunch of products that included appliances and software-only. We had one product that is strictly a penetration testing tool and, as we had some other

products that included vulnerability assessment and penetration testing, this forced us to break the group up into three sub-groups: vulnerability assessment, penetration testing and hybrid (both).

In general, we were impressed with their utility, ease of use and comprehensive reporting.

Rapid7 NeXpose



Vendor Rapid7 LLC
Price \$25,000 for 1 class C license, plus \$2,000-\$4,000 for the appliance
Contact www.rapid7.com

Rapid7 NeXpose is, generally, an impressive appliance. Although it is a hybrid (vulnerability scanner and penetration test tool), the pen

tool is used specifically to validate vulnerabilities and is not intended to be used alone.

This is typical of the way an attacker would attempt to penetrate a target.

Set-up is plug and play, and the product can use DHCP if the network supports it. Set-up begins using the LCD display on the appliance and, after setting

addresses, further management and configuration is through a normal web browser.

The user interface is clean and reporting is robust. NeXpose sports an easy to use, well-organized dashboard and, like most of the products we looked at, it supports a wide range of compliance reporting including PCI.

The device begins by scanning the network to discover devices for testing. Once it completes its scans, it performs automatic penetration testing in an attempt to exploit the vulnerabilities found. This greatly limits false positives. It does, however, lower performance. NeXpose found just over 80 percent of our vulnerabilities.

This appliance has some added capabilities we found impressive. For example, it performs trouble ticketing and makes recommendations for risk reduction based on the vulnerabilities it finds.

Documentation is comprehensive, clear and well-organized and the product comes with a quick-start guide that takes you through set-up. Phone support is available during working hours at no cost and for additional cost there is an

extended 24/7 plan available. Upgrades to the signature set are free and available every three days. The website is full of support tools, such as FAQs, documentation briefs and other useful documents.

At between \$2,000 and \$4,000 for the appliance, plus \$25,000 for a class C license, NeXpose is not cheap. But it delivers a lot of bang for the buck and we rate it our Best Buy in the hybrid class.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★☆
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★☆
OVERALL RATING	★★★★★
Strengths Compliance reporting, quick, easy deployment, additional vulnerability management features.	
Weaknesses Can become pricey in large networks.	
Verdict We award this product our Best Buy in the hybrid class for its strong use of penetration as a vulnerability validation tool and its ease of use and management.	



Compliance reporting, quick, easy deployment, additional vulnerability management features.

Peter Stephenson

Rapid7 LLC
 545 Boylston Street, Boston, MA 02116
 Toll free: 866 7 RAPID 7
 Phone: 617.247.1717 • Fax: 617.507.6488
 www.rapid7.com