

# Review of Norman Network Protection 4.0

February 2011

## Norman Network Protection Appliance Excels When Used In Layered Defense

Businesses looking to improve network security are often overwhelmed by the many choices available, including software solutions versus the new generation of security appliances. And businesses are focused on daily operations and the need to make financial targets in a tough economy. Network security is understood to be important, but realistically investment in security expense is minimized wherever possible.

In practice this often means that security administrators will install a cheap and servicable firewall as a network gateway and then use endpoint security as another line of defense at the desktop. Even using this defense-in-depth strategy means that all too often many malware streams still get through. At the desktop, the industry offers dozens of Endpoint Security options for additional defense.

Norman is offering a new, innovative solution address this malware defense dilemma. Anchored by the Norman Security Suite endpoint product line, Norman has been pioneering new technologies over the past several years. Most notable is the advanced SandBox technology in the company's anti-malware scanning technology. SandBox detects new malware at a high rate, making Norman's scanning engine popular in many 3rd party products.

Now Norman offers Network Protection, available as either an appliance or software. Detailed information can be found on Norman's website at [www.norman.com](http://www.norman.com) including registration

for a trial version, detailed product overview sheets and a full manual.

We reviewed the hardware appliance solution, installed on a Dell box, which included a quick-install guide. When we booted up the machine, we quickly saw a Norman splash screen, followed by a simple network configuration process. After the quick initial setup, the appliance rebooted, giving the user web browser access to the management console, which seemed smooth and stable.

The user is asked to choose specific protection scanning level settings for each network protocol and other options include URL blocking settings, configuration of the messages to display to users connection to malicious websites, and control of logging and email alert messaging. Email and SNMP options send alerts without requiring monitoring of the interface. The level of data, and where and how it is sent, can all be easily configured.

The Norman appliance may be placed at the gateway or between network segments. Two interfaces pass all data through, scanning the traffic streams in real time, blocking anything malicious. For this test, we put the machine between two subnets. The traffic between the subnets seemed completely unaffected by inserting the device. Upon looking at the management GUI, we could see throughput levels of the traffic being monitored and subsequent malware we attempted to pass through the device on various protocols was blocked



immediately. The interface gave us all the information we were looking for about network traffic, the system hardware, and malware blocked, all organized clearly and enhanced by visual tables and graphs.

Even when we put the device under heavy traffic loads, there was virtually no slowdown, with malicious files continually blocked, as opposed to behavior we observe on proxy based appliances, which require the full object to make a risk decision before passing it on to the destination system. The invisible no-latency technology Norman boasted gave us even smoother and quicker connectivity that we expected.

One of the most interesting features of the appliance is the SandBox detections. When malicious files are run through the SandBox, detailed behavior of the file is reported as it executed safely inside the Norman's simulated proactive "clone" environment. The report includes information about changes the malware would have made to the target file system and registry, as well as network behavior and other information.

Norman Network Protection's selling point is simple, affordable superior malware protection. NNP simply blocks malware passing through core protocols with minimal network

affects and administrative overhead. The plug-and-play abilities and ease of integration makes it flexible enough to be installed at any location in any network layout. As a bonus this product keeps the overheads low, barely impacting traffic flow. The addition of the proactive Sandbox with the traditional technology scanning adds an extra layer of defense against new and unknown threats.

NNP can be placed anywhere within a network and could be an important part of a network security strategy from the SMB to larger, more complex networks. In the SMB scenario, NNP will protect the whole business network from outside threats. In more complex networks, Norman Network Protection also secures email services, web servers and the FTP server.

As we have noted, many businesses with limited budgets place their most robust antimalware defense at the client level, with some kind of Endpoint Protection solution. Norman believes that NNP can significantly improve antimalware protection in this scenario, and has independent lab testing results to prove it.

In 2010 testing with NSS Labs, Inc., Norman announced that NNP improved network security up to 38% when used in conjunction with a range of leading endpoint protection solutions. The appliance is picking up malware threats the Endpoint software doesn't see. The point is that most security experts feel that one layer of security just isn't enough anymore. With a layer of defense at the gateway and another layer at the endpoint, users have a higher chance of defeating even the toughest malware threats.

We agree that a multilayered approach such as offered by the Norman Network Protection appliance and a standard industry endpoint solution offer a superior defense-in-depth strategy for the SMB and can provide a strong additional layer of protection against network threats which endpoint products alone may miss.

Keep in mind that we tested NNP between subnets. Typically malware appliances focus on stopping threats only at the gateway, but increasingly threats are being introduced by internal mobile devices, such as laptop PCs and USB devices connected innocently to LAN segments.



**NORMAN SANDBOX®**  
is a revolutionary way to detect new and unknown malware in a proactive way.



**NORMAN DNA MATCHING**  
is a proactive method for identifying the viral profile of all kinds of malicious programs.



**NORMAN EXPLOIT DETECTION**  
is a technology for detecting malware exploiting vulnerabilities in widely used document types.



**Pricing**

SMB NNP	R-210 Appliance w/next business day replacement service 1 yr: .....	\$2,995
SMB NNP	R-210 Appliance Annual Renewal: .....	\$1,797

**NNP Options available**

- Quad-Core Intel® Xeon® E5420 2x6MB Cache, 2.5GHz 1333MHz FSB
- Intel® PRO 1000VT Quad Port Gigabit Network Card, PCI-E
- 4Yr ProSupport for IT and Next Business Day On-Site Service
- 5Yr ProSupport for IT and Next Business Day On-Site Service
- Bypass Copper
- Bypass Fiber
- Redundant Power Supply - No Power Cord and No Rack Rails option

For more information about Norman security solutions and the new NNP 4.0, please go to [www.norman.com](http://www.norman.com)



Norman ASA is a world leading company within the field of data security, internet protection and analysis tools. Through its SandBox technology Norman offers a unique and proactive protection unlike any other competitor. While focusing on its proactive antivirus technology, the company has formed alliances which enable Norman to offer a complete range of data security services. Norman was established in 1984 and is headquartered in Norway with continental Europe, UK and US as its main markets.

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

Norman SandBox® US Patent Number 7,356,736

**NORMAN®**