

Norman Network Protection



PRODUCT REVIEW PRODUCT REVIEW PRODUCT REV

The latest security appliance from Norman Data Defence Systems is dramatically different from most solutions, as not only does it focus exclusively on viruses and malware, but it offers a greater range of deployment choices. Rather than just target gateway duties, the new Norman Network Protection (NNP) appliance can play many roles, as it's designed to sit between any two networks, scan traffic passing between them, and weed out malicious content.

Deployed as a low-profile Dell PowerEdge rack server, the NNP is equipped with a dual-port Gigabit card which it uses to sit directly in the flow of traffic, allowing it to transparently monitor all network activity. No client configuration is required as it doesn't act as a proxy, and by scanning data packets at the data link layer it is completely invisible; system users won't even know it's in the background.

It offers three scanning methods with standard signature based detection first on the list. Next up is Norman's DNA Matching feature, which offers good zero-day protection from new threats. Much malicious code has many similarities, and the NNP inspects the code as it passes through it - and if it finds inherited or reused code it considers it as malware, and blocks it.

Norman's SandBox makes the NNP virtually

unique and it creates these in protected memory whenever malicious code is detected. The Norman SandBox emulates a Windows system and this includes the system BIOS, Windows registry, hard disk boot sectors, file systems and even a video card. The code is fooled into thinking it is in a real system and is allowed to run so that the NNP can see what it is up to. If the code makes any attempts to look for other systems - as many viruses would do during their infection process - then the NNP creates more SandBoxes on demand.

We found installation a cakewalk as we placed the NNP mid-stream in between two network segments and accessed it remotely via its dedicated management network port. The dual-port card doesn't require any IP addresses, so no network configuration is necessary. The simple web browser interface runs through a quick start wizard where you pick and choose from a range of protocols including HTTP, FTP, POP3, SMTP, FTP, SMB and CIFS and decide on the scanning procedures for each one.

The toughest scanning method activates the SandBox feature and will also check inside archived files. You can switch either of these off individually for each protocol or go for a minimum scan which uses neither. You can also block access to web sites deemed to be harbouring malicious content for periods ranging from a number of days, weeks or

months. Facilities are provided for creating lists of IP addresses, MAC addresses and VLANs where traffic from these sources will be blocked from passing through the NNP or excluded from the scanning process.

To test the NNP we started by attempting to copy files infected with genuine viruses across systems on each subnet. From the initiating user's perspective, nothing untoward happens as the copy appears to complete. However, looking on the recipient system we could see the test files were either blocked completely by the NNP, or were of zero byte sizes and consequently unusable. Alerting facilities are provided as you can have the NNP issue email alerts and SNMP traps when suspect content or web sites are blocked.

The NNP clearly has a number of advantages over traditional gateway security devices as it can be deployed across a much wider range of network scenarios. Installation doesn't get any easier, it is transparent in operation and the Norman SandBox technology provides a very strong security barrier. **NC**

Product: Norman Network Protection
Supplier: Norman Data Defence Systems (UK) Ltd

Tel: 08707 448044

Web site: www.norman.com

Price: A one year licences for up to 250 users is £3,495 excluding VAT