

Norman Endpoint Protection



Norman Endpoint Protection (NEP) software from Norman Data Defense Systems, aims to provide a complete security umbrella for laptops, desktops and servers, delivering some of the toughest anti-virus and anti-malware measures on the market. It operates a three-pronged attack by utilising Norman's SandBox, DNA matching, and exploit-detection technologies. Endpoint protection is provided by client software and this delivers the full force of Norman's scanning technologies. These are managed centrally from the Norman Endpoint Manager (NEM) console, and a closer look shows that the three technologies are quite unique.

The SandBox runs on each protected system as part of the client software. When malicious traffic is detected, it emulates a Windows system in protected memory and presents it to the code, complete with system BIOS, Windows registry, hard disk boot sectors, file systems and a video card. The code is allowed to run while the client software observes its actions. If the code exhibits worm-like behaviour by attempting to access other systems the client creates more sandboxes for it, and when it's satisfied it is malicious, blocks it.

DNA matching also provides zero-day protection by exploiting the fact that much of today's malicious code is created using freely available development kits, and so

has many similarities. It is a part of the client scanning processes and will, for example, cache web pages locally and scan their code. If it finds inherited or reused code, it considers it as malware and blocks it.

Last up is exploit detection and one of its attributes allows it to inspect certain files, looking for shellcode which could start a command shell, running other programs. A good example of this would be the recent spate of malicious PDF files that exploited vulnerabilities within Adobe Acrobat, attempting to run other programs.

We found deployment to be a pleasantly simple process. After loading the NEM console realms are created, which define logical groupings of networks and their endpoints. Within each realm you can have multiple groups and sub-groups, each being assigned a security policy which defines client configurations. Topology filters can be used so that NEP automatically places systems into predefined groups depending on criteria such as their name, or IP address.

For endpoint deployment you can push the client to groups, or create an MSI package. This is made easier as the NEM sniffs out all network systems and lists them ready for selection. We adopted the MSI route, deploying the client to a range of Windows XP, Server 2003 and Server 2008

systems in just minutes. We used a single policy which enabled client functions such as update intervals, on-access and email scanning, Internet protection and the SandBox; users were prevented from changing settings. From the NEM console we could easily see the status of our test clients as each had a colour coded icon beside it.

Using a batch of genuine viruses, our attempts to infect the test systems were all rebuffed. The console risk indicator immediately lit up with warnings and alarms. Assigning thresholds to events allows NEM to issue timely warnings and alerts via email, SMS, syslog and SNMP traps.

Some vendors have been unable to resist packing their security software suites with too many features, creating products that are very difficult to manage. Norman has avoided this by staying true to its roots and focusing clearly on malware. The end result is a security product that's good value, easily managed, and capable of delivering some of the toughest endpoint protection that is currently available. **NC**

Product: Norman Endpoint Protection
Supplier: Norman Data Defense Systems (UK) Ltd

Tel: 01908 847413

Web site: www.norman.com

Price: 100 users - £1,717 ex VAT