

NORMAN Network Protection

Securing your Enterprise Content Management

Norman Network Protection is a software solution designed to protect your communication infrastructure against malware like viruses, spyware, worms and trojans. This allows organizations to continue high-performance network operations with complete transparency and without any regard to potential malicious infections.



KEY FEATURES

- Deployable anywhere in the network
- Independent of the network infrastructure
- Protects both servers and clients
- Transparent to all entities in the network
- Requires no network adaptation
- Fit for small or larger networks
- Unmatched protocol scanning capabilities: FTP, HTTP, SMTP, POP3, RPC, TFTP, IRC and CIFS/SMB
- Supports unlimited number of VLANs

By simply connecting the Norman Network Protection machine to your network, you can protect the entire infrastructure from the Internet, or protect business critical areas of your network from being infected by malicious code. When the NNP detects a malicious file in transfer on your network, it actively terminates the file transfer and blocks the specific network path to prevent other users or systems from accessing the same file.

Some key benefits

Latency - not a problem

Traditional proxy solutions have several drawbacks. The most important consequence is the latency in data traffic created by the proxy itself. A proxy holds back the entire stream of files, while NNP avoids this problem by only holding back the necessary data needed to perform a malware scan.

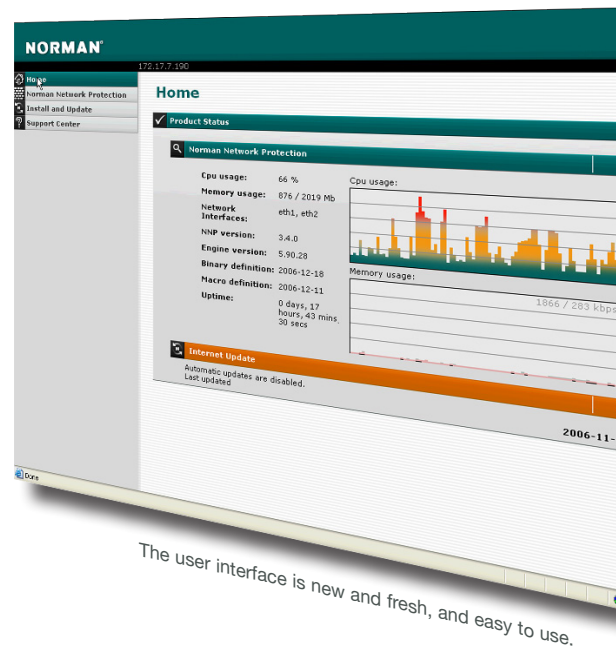
Database consistency

Norman Network Protection scans files before they are saved on the database server therefore it eliminates risk of database inconsistency and increase database uptime by reducing maintenance time.

NNP operates at the packet layer in the network, and is transparent to the IP traffic. No IP reconfiguration of your network is needed; just add an address for the administration interface and the NNP is instantly protecting your network.

Norman Network Protection gives you real time statistics and reports, presenting detected and blocked malware, system statistics and network statistics. The NNP's message handling system can send you incident emails and/or report to an operations center by SNMP-traps.

NNP is a fully transparent malware scanner that can be supplied as a software package or as an appliance. It can be installed easily at any point on the company network, such as the input and output of a database application. Proactive components like the behavior-based Norman SandBox® reduce the risk of infection from unknown malware. The SandBox also has a "DNA matching" feature which makes use of the fact that malware that is discovered is rarely entirely new. NNP scans protocols that are susceptible to malware in real-time. Documents are scanned during both upload and download.



The user interface is new and fresh, and easy to use.



PROACTIVE ANTIVIRUS

Norman Network Protection includes Norman SandBox® - a revolutionary way to detect new and unknown malware in a proactive way.



NORMAN DNA MATCHING

A new proactive technology and method for identifying the viral profile of all kinds of malicious programs.

NORMAN EXPLOIT DETECTION

This is a technology for detecting malware exploiting vulnerabilities in widely used document types like, OLE2 (Office documents), MDB (Access), WMF (Windows Media File), JPEG (pictures), RIFF (Windows media meta-format) and SWF (Flash).





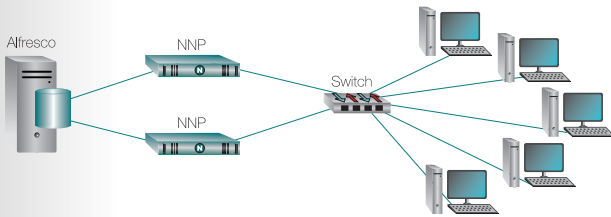
Reference case: Bauer AG and Norman

Bauer AG chooses Norman security solution

Special care and attention needs to go into the choice of virus protection software for database-based applications. Neither local virus protection nor purely signature-based scanners are considered ideal. Therefore, Bauer AG opted for the Norman Network Protection malware scanner to protect Alfresco, their new ECM solution.

Mechanical and civil engineering group Bauer AG develops and builds special mining machines and undertakes demanding projects all over the world in underground mining, bridge-building, sewage system construction and the restoration of historical structures. The group's 8,000 employees need to be able to access the information and data they need wherever they are in the world. To achieve this Bauer uses Alfresco, an open source enterprise content management solution.

Alfresco runs on three ECM servers at Bauer. Two are used in the production network and have two network cards each for redundancy reasons. The third server is part of a test network used to evaluate scenarios.



Occasionally, malicious code for which there is no signature may "slip through the net", resulting in an infected file being saved in the ECM system. Unfortunately, normal server-based virus scanners as used on file servers cannot be used on most ECM systems, including Alfresco. This is because the ECM systems save files in a structure where file index and files are separated. This could not be handled from a classical virus scanner. If a virus scanner were to be used in this way, deleting or moving the server files would result in an inconsistent system, as the ECM system would be unaware of the changes. Saving of the

malicious software would certainly be inhibited, if it were recognized at all, but in the worst case scenario the entire system would be destroyed, requiring a laborious rebuild.

Scanning before upload

Bauer AG wanted to avoid having any viruses on the server. The obvious choice was malware protection that could be installed on the company network as a tool to scan every instance of access to the ECM server. Files should be scanned during upload and download, but not while they are being stored in the file system, so that another virus scanner installed locally on the server would not be necessary. In addition to the traditional, signature-based scanner, part of the solution had to come from proactive security components. "Using only signature-based anti-malware solutions just doesn't cut it anymore when you consider that thousands of new viruses are popping up every day" explained Roland Bauer, IT Manager at Bauer AG. "We have sites all over the world – we could easily be one of the first companies to be attacked by a new virus". Bauer also has fairly clear ideas about which protocols they want to scan. Apart from HTTP, which is used to store files in the file system via the web and WebDAV, other files need to be scanned that are saved using normal network access. CIFS is the usual protocol for this.

"The installation costs were minimal because no modifications needed to be made to existing network components and no changes had to be made to network, proxy or gateway settings," explained Mr. Bauer. We also looked out for any potential latencies during scanning, as they are known to be a particular problem for proxies. NNP's Minimal Latency Session Shadowing feature did not disappoint.

The success of the trial period led to a unanimous decision to go ahead with the purchase of NNP. Mr. Bauer summed up the company's experience with Norman Network Protection in the following words: „The wide range of protocols scanned by Norman Network Protection and the fact that the system is proactive in dealing with virus threats means we have the right spectrum of functionality to effectively protect our ECM solution.“



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.

