

NORMAN®

NetworkProtection appliance series

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 VLAN's
- Optional blocking of MSN and BitTorrents



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



NORMAN DNA MATCHING is a proactive technology and method for identifying the viral profile of all kinds of malicious programs, by recognizing inherited or reused programming codes in new malware.



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

Norman Network Protection, a comprehensive, high-performance security appliance that helps organizations to effectively protect critical IT infrastructure against cyber crime.

There is little doubt that organizations today must protect their networks from malicious threats to their corporate and customer data. With more information moving in and out of networks from a variety of sources, the risk of infection from malicious software (malware) is high. It is not just the threats themselves that are dangerous. Many users are exposing confidential and sensitive information, which heightens the risk of compromising systems by not taking proper precautions.



These threats can pose large problems for network administrators and updating and maintaining security solutions should never be neglected!

Ease of deployment

Since anti-malware scanning is performed over the wire, there is no need for any advanced configuration. The appliance is transparent and there is no need for any IP configuration other than enabling access to the appliance from the web-based console.

Enhanced Security

Looking for malware where no other solution is able to! Thousands of malicious files are using network protocols to get deeper into your network. With NNP, for the first time, you are able to prevent spreading on frequently used network protocols like RPC, CIFS and SMB in addition to the traditional internet protocols.

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.

Prevention

When the NNP appliance 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.

Jens Roed Andersen, Chief Information Security Officer at Arla:



"What was especially interesting for Arla Foods was that the system could be implemented without requiring major changes to the existing equipment."

PRODUCT DETAILS

Available as hardware and software based solutions.

Highly scalable hardware platform.

Runs on Linux.

Multithreaded application with multi-CPU support.

Norman Scanner Engine with Norman SandBox® and Norman DNA Matching Inside.



“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.”



Network Products Guide, the industry’s leading publication on information technologies and solutions, has named Norman Network Protection a winner of the 2009 Best Products and Services Award.



Transparency

NNP operates on Layer 2 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 NNP is instantly protecting your network.

Norman SandBox®

Being proactive is the only way to stay secure. With Normans SandBox® technology targeted at attacks and never previously seen malware will be detected. The Norman SandBox® Technology is a virtual environment where programs may perform in safe surroundings without interfering with the real processes.

Features & Benefits

- Eliminates high cost for configuration and maintenance
- Realtime scanning of network traffic with Minimal Latency Session Shadowing®
- Realtime analysis of unknown malware via Norman SandBox® logs
- Automatic Outbreak Prevention and Damage control with malware source detection and isolation
- Supports full scan of multiple protocols: FTP, HTTP, SMTP, POP3, RPC, TFTP, IRC and CIFS/SMB
- Multi-tiered traffic blocking or exclusion based on IP-address, MAC-address or VLAN ID
- Option to block MSN traffic and BitTorrents protocol
- Command Line Interface management available
- Automatic and transparent scan engine and signature update via Internet
- Integration with SNMP-based management tools
- Malware notifications by SNMP or SMTP (Email)
- Centralized management available with Norman Endpoint Manager. See separate product sheet for details

	NNP-R210-75	NNP-R210-250	NNP-R610-500
Nodes protected	75	250	500
Processor	Intel Xeon X3450 Processor (2.66GHz, 8M Cache, Turbo, HT) 1 S	Intel Xeon X3450 Processor (2.66GHz, 8M Cache, Turbo, HT) 1 S	Intel Xeon X5550 Processor (2.66GHz, 8M Cache, 6.40 GT/s QPI, Turbo, HT), 1333MHz Max Memory
RAM	4GB Memory (2x2GB Dual Rank UDIMMs) 1333MHz 1 S	4GB Memory (2x2GB Dual Rank UDIMMs) 1333MHz 1 S	6GB Memory for 1 CPU (3x2GB Dual Rank UDIMMs) 1333MHz
Hard drive	250GB SATA	250GB SATA	2x73GB SAS 10k 2.5" HD Hot Plug. Raid 1.
Network Cards	4x10/100/1000MB/s Ethernet	4x10/100/1000MB/s Ethernet	4x10/100/1000MB/s Ethernet
Options			
Processor			Intel Xeon X5550 Processor (2.66GHz, 8M Cache, 6.40 GT/s QPI, Turbo, HT), 1333MHz Max Memory
Network Card	Silicom bypass server dual port adapter for failover option	Silicom bypass server dual port adapter for failover option	Silicom bypass server dual port adapter for failover option
Power Supply			Redundant Power Supply



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.

