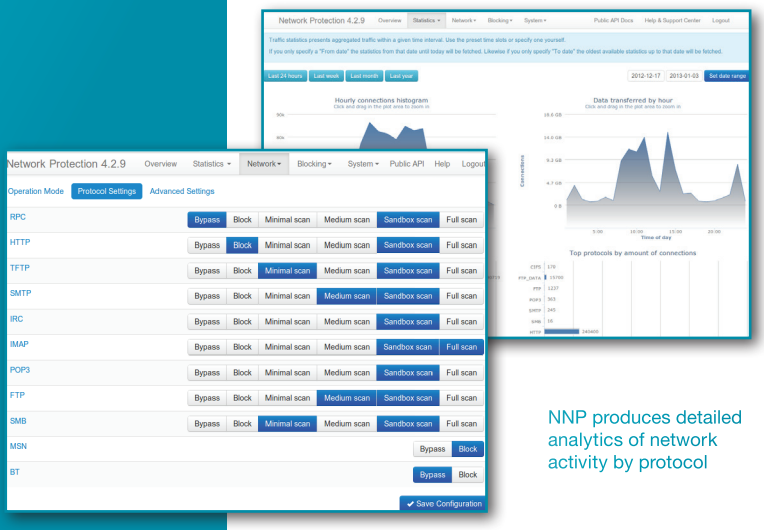
Network Protection

high performance security appliance

IN THIS PRODUCT SHEET:

Highly scalable and simple to deploy, NNP exposes threats by rapidly scanning multiple protocols on the wire – including email attachments - using signatures and sandboxing to automatically detect and block malicious traffic.



NNP produces detailed analytics of network activity by protocol

- *Scan and block malware across multiple protocols*
- *Fine-tune scan settings to implement your security policies*
- *Use as an incoming mail proxy to scan email attachments for malicious behavior*

NEW

- *Now with Norman Scanner Engine 7 (NSE7)*
  - *Fastest, highest performance scanning engine*
  - *New file detection capabilities*
  - *Integrated Norman Sandbox®*
  - *Smaller update files*
  - *Rapid response platform*

KEY BENEFITS

Turnkey Solution: Self-contained anti-malware appliance with everything you need to protect networks against malware.

Comprehensive Protection: Extensive list of protocols scanned and file types supported, since malware takes many forms and many paths.

High Performance: Ultra-fast high throughput scanning up to 6Gbps nominal traffic on 10Gbps interfaces.

Malware Prevention: When 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.

Configurable Scanning: Balance speed vs. depth of inspection by choosing to Bypass, Block, Minimal Scan, Medium Scan, or Full Scan for each protocol. In addition, Norman SandBox scan is always on, providing powerful detection capabilities.

High Availability: Supports multiple fail-over options for high-availability networks, enabling organizations to survive system or application failures with no discernible interruption to business-critical applications.

Low Latency: Traditional proxy solutions typically involve latency in data traffic by holding back a stream of files, while NNP avoids this problem by only holding back the necessary data needed to perform a malware scan.

Flexible Deployment: Deploy in-line as malware prevention or out-of-band to monitor and alert when malware is detected. Use as standalone network protection or in conjunction with Norman Malware Analyzer G2 (MAG2).

URL blocking: Prohibits access to unwanted web sites, preventing user exposure to threats and inappropriate content.

Transparent: Operates transparent to IP traffic on Layer 2 with no network IP reconfiguration – ready to use out of the box.

Enhanced Security: Detects deep malware intrusions that other solutions miss, preventing spreading on traditional Internet protocols and common network protocols including Windows File Sharing.

Comprehensive Malware Defense with Norman Network Protection and MAG2.

When Norman Network Protection (NNP) is deployed with the Malware Analyzer G2 (MAG2), the interception and discovery of malicious files in your network is easy. NNP collects files on the wire, detects known malware and delivers payloads from unknown threats to MAG2 for deep malware analysis. Once analysis is completed in MAG2, security teams have actionable intelligence to remediate the damage from the malware. In addition, MAG2 provides NNP with detection criteria for the malware so that future attacks can be blocked.

PRODUCT FEATURES

General:

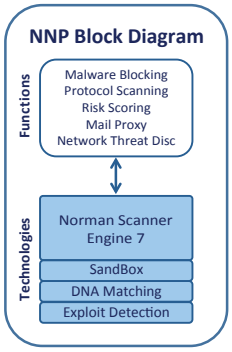
- Deployable anywhere in the network
- Highly scalable platform
- Mirror port / SPAN port support
- Supports network cards up to 10Gbps with scanning up to 6Gbps
- Supports up to 4,096 VLANs
- High availability solution and built-in redundancy with failover NIC
- Remote API for configuration, status, and reporting information, including batch configuration of multiple NNPs
- High availability solution and built-in redundancy with failover NIC
- Mail proxy to scan and block / quarantine / forward suspicious inbound email prior to delivery

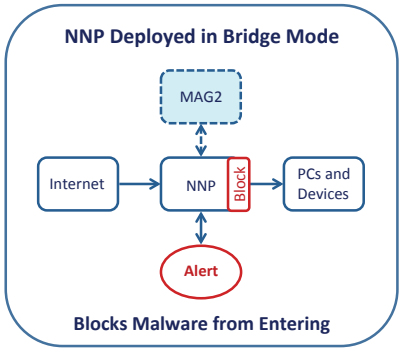
Malware Scanning:

- Real-time malware scanning of network traffic
- Extensive files scanning support now includes Windows x64 (PE32+), Apple binaries (Mach-O), and .NET binaries
- Remote application programming interface (API)
- Malware source detection and isolation
- Automatic scan engine and signature update

Additional Features:

- Optional blocking of MSN traffic and BitTorrent protocol
- Customizable content / URL blocking
- Multi-tiered traffic blocking or exclusion based on IP-address, MAC-address or VLAN ID
- Powerful integration and workflow support with remote API alerting via SMTP/mail, remote syslog, and SNMP





Deploy NNP in-line or out-of-band, standalone or in conjunction with Norman's MAG2

Unmatched protocol scanning capabilities include:

- HTTP
- SMTP
- POP3
- IMAP4
- RPC
- FTP
- TFTP
- IRC file transfers
- Windows file sharing (CIFS/SMB/SMB2)
- Block MSN and BitTorrent protocols

NORMAN AS

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.

Norman ASA
P.O. Box 43
N-1324 Lysaker, Norway
Tel: +47-67-10-97-00
Fax: +47-67-58-99-40
norman@norman.no

Norman Data Defense
1855 1st Avenue, Suite 201
San Diego, CA 92101 USA
1-888-GO-NORMAN

Norman SandBox® US Patent Number 7,356,736