

NetworkProtection v4 for Collaboration Servers

IN THIS PRODUCTSHEET:

- » The challenge
- » The solution
- » Key features
- » ROI

The challenge

Special care and attention needs to go into the choice of antivirus software for database-based applications. Neither local antivirus nor purely signature-based antivirus scanners are considered ideal. Local antivirus software may be risky and can create discrepancy between the actual file system and the databases if files are quarantined at the file system level only. Also considering that local antivirus signature file are getting larger, and with multiple updates daily, will affect the performance on busy collaboration systems while scanning for malware.

The solution

Norman Network Protection for Collaboration Server does not affect the server performance because its install at the front of the collaboration server farm. This makes customers able to continue high performance network and server operations with complete transparency without any potential malicious infections neither any disrupted databases.

Key features

- » Prevent disrupted collaboration databases
- » Protect against malware infected documents
- » Prevent distribution of malware
- » Real time statistics and reports
- » No latency
- » Easy to install
- » Support for 10Gb/s networks

Easy install and operation: The solution is independent of network topology and other networking units. It provides value from the second it is installed in the network. Norman Network Protection protects collaboration servers as Microsoft SharePoint and Alfresco systems against malware and includes a powerful management and reporting tool to provide efficient status and reports on the malware situation.

Norman Network Protection Collaboration Server is a fully transparent malware gateway and 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 behaviour-based Norman SandBox® reduce the risk of infection from unknown malware. This simulates a computer, including its environment, in which unknown files are allowed to execute their commands unhindered. All activities of those files are monitored and evaluated and the file and path are disabled if necessary.

Norman Network Protection Collaboration Server scans those protocols that are susceptible to malware, including HTTP, FTP, SMTP, POP3, RPC, TFTP, IRC and Windows file sharing. Documents are scanned during both upload and download.



Microsoft SharePoint



Gartner

According to Gartner, "Collaborative workspaces provide an easy mechanism for file and content sharing, which also facilitates malware propagation."¹ The results include infected systems and lost or stolen information.

1 Gartner Research. Security Considerations and Best Practices for Securing SharePoint. February 2009.



Bauer use Alfresco ECM solution.

"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 Enterprise Content Management system."

Roland Bauer, Head of IT at Bauer AG

In-line communication: By simply connecting the Norman Network Protection Collaboration Server in-line into 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 like viruses, spyware, trojans and worms.

Latency - no problem: Traditional security gateways use proxy solutions and these 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, something Norman Network Protection Collaboration Server avoids by being transparent to the traffic. NNP lets the data pass through, only holding back the necessary data needed to perform a malware scan.

Automatic block of infected data: When Norman Network Protection Collaboration Server 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 infected data.

Deployment: Norman Network Protection Collaboration Server operates on 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 Norman Network Protection is instantly protecting your network.

Reporting: Norman Network Protection Collaboration Server gives you real time statistics and reports, presenting detected and blocked malware, system statistics and network statistics. The Norman Network Protection message handling system can send you incident emails and report to an operations center by using SNMP.

ROI

The solution is independent of network topology and other networking units. It provides value from the second it is installed in the network. Norman Network Protection Collaboration Server protects against viruses, worms, trojans, spyware, and other malware and includes a powerful management and reporting tool to provide efficient status and reports on the malware situation in the network. Unknown files are allowed to execute their commands unhindered, and all activities of those files are monitored and evaluated and the file and path are disabled if necessary.

Check www.norman.com/nnp for the latest updates



NORMAN SANDBOX®

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



NORMAN DNA MATCHING

is a proactive method for identifying the viral profile of all kinds of malicious programs.



NORMAN EXPLOIT DETECTION

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



"Providing such simple and unproblematic malware protection, along with an excellent, again very straightforward control system, makes this an extremely user-friendly weapon in the fight against malware problems in business networks, as well as a powerful one. We look forward to investigating a wider range of appliances to see how they match up to this impressive effort from Norman."



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.

NORMAN®



www.norman.com

Norman SandBox® US Patent Number 7,356,736