



NetFort LANGuardian introduces Microsoft™ FileShare Monitor for Total User Behaviour Visibility

In today's business world, an accessible IT infrastructure is necessary to ensure all company departments, co-workers and user groups can work in harmony to strategically align and optimize business functionality and efficiency. The focal point of this accessibility is the capacity to share vital data across different business functions and departments which requires granting permissions to a variety of users across a network to access, read from and write to files.

However, the risks attached to enabling users in this fashion can be damaging, leaving the network susceptible to activity that may cause data leakage or loss of confidential information. Quite often, the most damaging activity on a network is carried out by the user mistakenly, rather than maliciously. In order to enable organisations to safeguard file servers against susceptibility, NetFort Technologies pioneer product LANGuardian now incorporates the Microsoft™ File ShareMonitor module offering unprecedented visibility into user activity across file shares.



HOW DOES MICROSOFT™ FILE SHAREMONITOR WORK?

LANGuardian spans the network and captures traffic using deep packet inspection (DPI) technology to extract data from the Microsoft™ Server Message Block (a client-server, request-response protocol). To this end, all network traffic is mirrored and inspected and events relating to files and shares activity are delivered directly to an event database for real-time reporting.



ACTIVITY REPORTING FROM THE MICROSOFT™ FILE SHAREMONITOR MODULE

Users (clients) with allocated network permissions can access, read, write, copy, delete, create, rename or move network files and map network drives. Despite most users best intentions, these actions may sometimes wreak havoc within an organisations IT infrastructure.

When an incident occurs that impacts the day-to-day functioning of the business, Microsoft™ network file activity reports are readily available in real time in the newly created Application Decoders subsection of LANGuardians robust real-time reporting mechanism. Reporting can be tailored to suit an organisations desired data parameters and level of detail, allowing department heads and managers flexibility to achieve the exact outcome they want, when they want.



HOW DOES LANGUARDIANS MICROSOFT™ FILE SHAREMONITOR PROTECT YOUR VALUABLE NETWORK ASSETS



Unexpected losses of data may occur at any time, be it an employee losing a laptop that contains critical data or a removable data storage device that disappears from the company premises.

- LANGuardians Microsoft™ File ShareMonitor module enables a comprehensive audit trail on all file shares, saving time and money on troubleshooting.

- If business critical or sensitive files are tampered with, deleted or moved to a

removable storage device or laptop, the Microsoft™ File ShareMonitor reporting modules' spectrum of visibility answers in detail all of the questions relating to the event. Who performed the action on the file? What events were performed on the shared file? Where on the network this occurred? When exactly did the event occur?

- Leverage existing IT infrastructure investment through capacity management. Areas on the network that are subject to resource abuse or are, for inexplicable reasons, creating a drain on bandwidth are reviewed, enabling corrective action to take place and cutting costs of investing further in IT.

- Microsoft™ File ShareMonitor module enables total traceability and accountability within an organisation.



A VIEW OF NETWORK ACTIVITY REPORTS

The following are examples of the Network Activity reporting methods available through Microsoft™ File ShareMonitor Module;

■ Search by Filename

Generates a list of all files accessed over the network using Microsoft SMB protocol, ranked by number of accesses. Filter by filename (supports regular expression: e.g .xls\$) or access type (map, read, write, delete, rename). Drilldown to show a ranked list of files accesses, classified by client system.

Search by Filename (last 1 hour)				
Fred Dandy	\TECHNICAL_DOCUMENTS\Product_Specific	10	27.03	
Jill Dawson	\DOWNLOADS\Christmas_jnk->Christmas.exe	1	2.70	
Jill Dawson	\DOWNLOADS\Christmas_jnk	1	2.70	
Claire Ryan	\MUSIC\SNOWPATROL\Finish_Line.mp3	1	2.70	
Claire Ryan	\MUSIC\SNOWPATROL\Open_Your_Eyes.mp3	1	2.70	

Top Users (last 1 hour)						
Fred Dandy	Fred	Security Department	20.94 MB	26.85 MB	47.78 MB	14.3
Danny Noland	Danny	Customer Support	21.37 MB	23.48 MB	44.85 MB	13.1
Leslie Nilsen	Leslie	Sales Department	20.54 MB	22.07 MB	42.61 MB	13.1
Karen Clark	Karen	Testing Department	18.35 MB	18.97 MB	37.32 MB	11.1

■ Top MS Servers (by Events)

Generates a list of all systems serving files over the network using Microsoft SMB protocol, ranked by number of file access events. Filter by sensor, server, client and file action (map, read, write etc). Drilldown to a ranked list of files served, classified by client system, or drilldown to Sessions report.

Example of Top MS Servers (by Events) Report

S	Server	TOTAL	PERCENT
3	192.168.0.150 (finance server)	22	59.46
3	192.168.0.160 (file server)	15	40.54

■ Top MS Clients (by Events)

Generates a list of all systems accessing files over the network using Microsoft SMB protocol, ranked by number of file access events. Filter by sensor, server, client and file action (map, read, write etc). Drilldown to a ranked list of files served, classified by client system, or drilldown to Sessions report.

■ Top MS Servers (by Bandwidth)

Generates a list of all systems serving files over the network using Microsoft SMB protocol, ranked by bandwidth consumed. Filter by sensor, server and client. Drilldown to a ranked list of files served, classified by client system, or drilldown to Sessions report. Output is similar to Top MS Servers (by Events) as shown above.

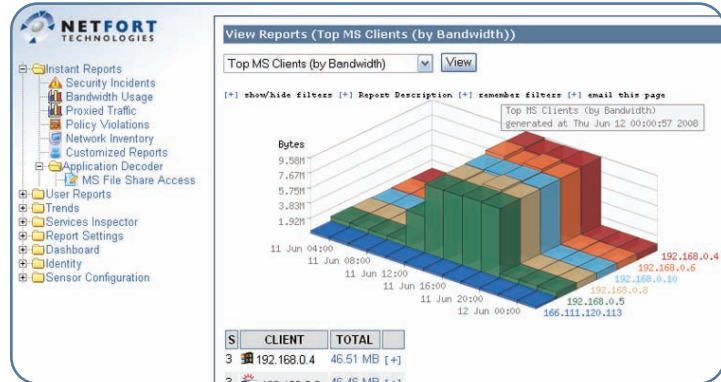


A VIEW OF NETWORK ACTIVITY REPORTS

■ Top MS Clients (by Bandwidth)

Generates a list of all systems accessing files over the network using Microsoft SMB protocol, ranked by bandwidth consumed. Filter by sensor, server and client. Drilldown to a ranked list of files served, classified by client system, or drilldown to Sessions report. Output is similar to Top MS Clients (by Events) as shown above.

Example of Top MS Clients by Bandwidth



■ User Search by Filename

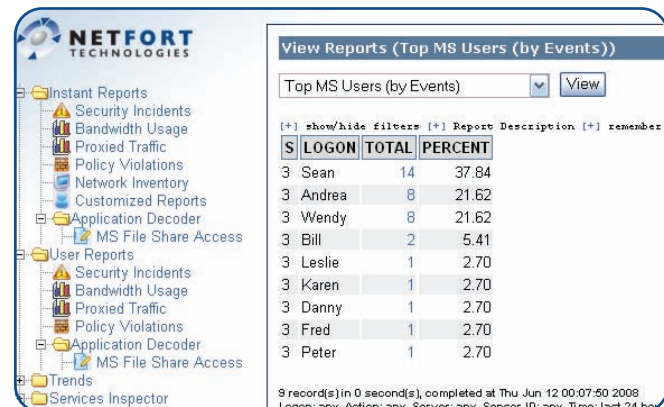
Generates a list of all files accessed over the network using Microsoft SMB protocol, ranked by number of accesses. Filter by user, filename (supports regular expression: e.g. *.xls\$) or access type (map, read, write, delete, rename). Drilldown to show a ranked list of files, classified by the user.

■ Top MS Servers (by Bandwidth)

Generates a list of all systems serving files over the network using Microsoft SMB protocol, ranked by number of file access events. Filter by sensor, server, user and file action (map, read, write etc). Drilldown to a ranked list of files served, classified by user, or drilldown to User Sessions report.

■ Top MS Users (by events)

Generates a list of all Users accessing files over the network using Microsoft SMB protocol, ranked by number of file access events. Filter by sensor, server, user and file action (map, read, write etc). Drilldown to a ranked list of files served, classified by user, or drilldown to Sessions report.



■ Top MS Servers (by User Bandwidth)

Generates a list of all systems serving files over the network using Microsoft SMB protocol, ranked by bandwidth consumed. Filter by sensor, server and user. Drilldown to a ranked list of files served, classified by user accessing files, or drilldown to Sessions report. Output is similar to Top MS Servers (by Events) as shown above)

■ Top MS Users (by Bandwidth)

Generates a list of all users accessing files over the network using Microsoft SMB protocol, ranked by bandwidth consumed. Filter by sensor, server and user. Drilldown to a ranked list of files served, classified by user, or drilldown to Sessions report.



HOW ARE OUR CUSTOMERS MAKING MICROSOFT™ FILE SHAREMONITOR WORK FROM THEM?

“We’ve found that the majority of our network performance issues are caused by network users. This is where LANGuardian plays a strong role in costs and time savings for us. We plug it in and begin troubleshooting immediately. Within minutes we can find the source of the issue.”

IT Manager, Leading European Mobile & Telephony Communications Provider

“Our organisation had major problems with network latency on certain parts of the network, affecting some of our branch offices and slowing down productivity among employees. We tried everything to find out what was causing the problem. We even went as far as hiring independent consultants to carry out some analysis work to detect the cause of the problem but to no avail. Finally, we decided to try LANGuardian. Using the File ShareMonitor component of LANGuardian, we discovered what the root of the problem was. This is the most cost effective and rapid piece of troubleshooting work we have ever done.”

Senior Network Consultant, Public Service Sector, Ireland

Corporate Headquarters

NetFort Technologies Unit 7
 IDA Innovation Centre
 Upper Newcastle
 Galway
 Ireland

T: +353 (0) 91 520 501
 F: +353 (0) 91 526 571
 E: sales@netforttechnologies.com

North American Regional Office

Netfort Technologies,
 280 Madison Avenue,
 #912 - 9th Floor,
 New York,
 NY 10016.

T: +1 646 924 0732
 F: +1 646 924 0778
 E: nasales@netforttechnologies.com

EMEA Regional Office

NetFort Technologies
 27 Old Gloucester Street
 London WC1N 3XX
 United Kingdom

T: +44 (0) 207 060 2850
 F: +44 (0) 207 060 2890
 E: emeasales@netforttechnologies.com

<http://www.netforttechnologies.com>