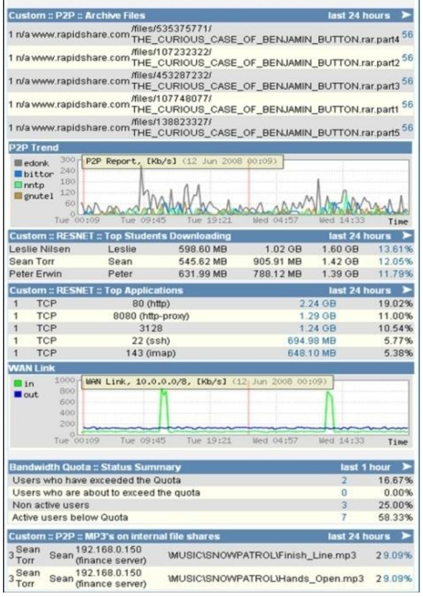
NETFORT
know your network

LANGuardian

NetFort LANGuardian SQL Server Database Monitor. Traffic-based monitoring of database activity – for audit and PCI compliance, troubleshooting, and data security.

> We found the NetFort LANGuardian very easy to deploy and configure and required minimal training. The integrated IDS and traffic analysis system ensures we always know what is going on in our network.
>
> – Jonathan Smith
> European Systems Manager
> Xilinx



Custom :: P2P :: Archive Files — last 24 hours ➤

1	n/a	www.rapidshare.com	/files/535375771/ THE_CURIOUS_CASE_OF_BENJAMIN_BUTTON.rar.part4	56
1	n/a	www.rapidshare.com	/files/107232322/ THE_CURIOUS_CASE_OF_BENJAMIN_BUTTON.rar.part2	56
1	n/a	www.rapidshare.com	/files/453287232/ THE_CURIOUS_CASE_OF_BENJAMIN_BUTTON.rar.part3	56
1	n/a	www.rapidshare.com	/files/107748077/ THE_CURIOUS_CASE_OF_BENJAMIN_BUTTON.rar.part1	56
1	n/a	www.rapidshare.com	/files/138823327/ THE_CURIOUS_CASE_OF_BENJAMIN_BUTTON.rar.part5	56

P2P Trend

Custom :: RESNET :: Top Students Downloading — last 24 hours ➤

Leslie Nilsen	Leslie	598.60 MB	1.02 GB	1.60 GB	13.61%
Sean Torr	Sean	545.62 MB	905.91 MB	1.42 GB	12.05%
Peter Erwin	Peter	631.99 MB	788.12 MB	1.39 GB	11.79%

Custom :: RESNET :: Top Applications — last 24 hours ➤

1	TCP	80 (http)	2.24 GB	19.02%
1	TCP	8080 (http-proxy)	1.29 GB	11.00%
1	TCP	3128	1.24 GB	10.54%
1	TCP	22 (ssh)	694.98 MB	5.77%
1	TCP	143 (imap)	648.10 MB	5.38%

WAN Link

Bandwidth Quota :: Status Summary — last 1 hour ➤

Users who have exceeded the Quota	2	16.67%
Users who are about to exceed the quota	0	0.00%
Non active users	3	25.00%
Active users below Quota	7	58.33%

Custom :: P2P :: MP3's on internal file shares — last 24 hours ➤

3	Sean Torr	Sean	192.168.0.150 (finance server)	\MUSIC\SNOWPATROL\Finish_Line.mp3	2	9.09%
3	Sean Torr	Sean	192.168.0.150 (finance server)	\MUSIC\SNOWPATROL\Hands_Open.mp3	2	9.09%

Monitor your SQL Server environment

SQL Server Database Monitor from NetFort Technologies is database activity monitoring software for your SQL Server databases. It monitors and records every access to your SQL Server databases, helping you to protect sensitive business data, secure your database infrastructure, detect fraudulent activity, and more easily meet your audit and compliance obligations.

You can do all of this with no impact on performance and without needing to redesign your databases or applications. And, with our Active Directory and Novell eDirectory integration, you can identify the actual users responsible for all database activity.

Security

All SQL Server activity is stored in the Event Repository, a proprietary database that is secure, hardened, tamper-proof, and completely independent of your SQL Server infrastructure. All database activity is time-stamped, providing a verifiable audit trail that you can use as part of your IT policy and compliance framework.

The Event Repository is independent of your SQL Server infrastructure, so you can configure your network to ensure that database administrators do not have access to the log data stored by SQL Server Database Monitor, and users who have access to the log data do not have access to your SQL Server databases. This enables you to implement separation of duties, a fundamental principle of IT security that is a key requirement for compliance with standards such as Payment Card Industry Data Security Standard (PCI-DSS) and Sarbanes-Oxley (SOX).
Because it observes all database traffic at the network level, SQL Server Database Monitor enables you to identify possible instances of fraudulent or unauthorized activity that would be difficult if not impossible to identify by monitoring databases individually using native logging:

- See when many different databases are accessed from a single client machine in a short time period – there could be an innocent explanation, but it could also be an indication that a user is trawling the database infrastructure for information to steal.
- Raise an alert when an application queries a database for many credit card numbers when it is designed to request only one at a time -- this could be an indication that the query has been subjected to a SQL injection attack.
- See which client machines are generating the most traffic to and from SQL Server databases, and drill down to identify which users, applications and databases are involved, as well as the SQL statements that are being applied.
- Ignore events originating from specific clients or destined for a specific server.

With SQL Server Database Monitor, you can access all of this information, and more, from a single browser-based user interface.

Performance

Because SQL Server Database Monitor generates its activity data from SQL Server network traffic, it has zero performance impact and it gives you a single point of access to the activity data for your entire database environment.

This is a significant improvement on the native logging and auditing utilities that come with SQL Server. The native utilities create log files on a per-server basis, making it difficult and time-consuming to monitor the log files for an environment with many SQL Server instances. Database performance is also affected when native logging is enabled.

SQL Server Database Monitor helps you to lower IT costs and increase operational efficiency by automating many database auditing and security tasks. You can configure it to automatically issue e-mail alerts or SNMP traps in real time when security policy violations occur. This feature is commonly used to notify an administrator when a SQL Server instance is accessed by a specified client.

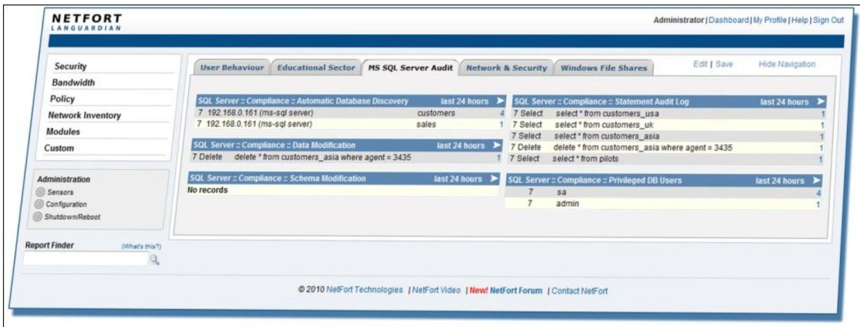
Compliance

Database activity monitoring is critically important for compliance with standards. The Sarbanes-Oxley Act (SOX) requires companies to apply strict internal controls to all systems that affect their ability to produce accurate financial reports, while the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations that process credit card transactions to prevent fraud by monitoring all access to cardholder data. SQL Server Database Monitor helps you to implement the internal controls and reporting systems that enable you to demonstrate compliance with these standards.

You can:

- Enforce segregation of duties
- Monitor high risk activity such as privileged user behavior, direct access to databases containing sensitive information, escalation of user privileges, and failed logins.
- Ensure that databases are queried and updated only through the appropriate applications.
- Generate alerts whenever an attempt is made to access a database directly or to circumvent SQL Server client application controls.

SQL Server Database Monitor implements an independent and secure audit trail that cannot be modified. Together with its detailed reporting and drilldown capabilities, this allows you to prove compliance with standards such as SOX and PCI-DSS.



SQL Server :: Compliance :: Automatic Database Discovery — last 24 hours

7 192.168.0.161 (ms-sql server) customers 4
7 192.168.0.161 (ms-sql server) sales 1

SQL Server :: Compliance :: Data Modification — last 24 hours

7 Delete delete * from customers_asia where agent = 3435 1

SQL Server :: Compliance :: Schema Modification — last 24 hours

No records

SQL Server :: Compliance :: Statement Audit Log — last 24 hours

7 Select select * from customers_usa 1
7 Select select * from customers_uk 1
7 Select select * from customers_asia 1
7 Delete delete * from customers_asia where agent = 3435 1
7 Select select * from pilots 1

SQL Server :: Compliance :: Privileged DB Users — last 24 hours

7 sa 4
7 admin 1

© 2010 NetFort Technologies | NetFort Video | New! NetFort Forum | Contact NetFort

Discovery

Knowing where data is located in your organization is critically important for risk management and compliance.
SQL Server Database Monitor helps you discover where important data is stored. You can create reports that list all databases on your network, see which users are accessing them, and what SQL statements they are applying. If a developer makes a copy of your customer database for testing purposes, or a new application begins interacting with your HR database, SQL Server Database Monitor will bring it to your attention. It will also notify you as new databases appear on the network.

How it works

SQL Server Database Monitor acts as an intrusion detection system (IDS) for your SQL Server databases. It records details of the user and application that accessed the database, the SQL statement used, and the database to which it applied. It works by monitoring the network traffic that passes through the SPAN or NetFlow port on your core network switch, using deep packet inspection (DPI) techniques to analyze the traffic and identify the SQL statements that users and applications are transmitting over network.

SQL Server Database Monitor is language-aware, enabling you to drill down to details of specific SQL operations and statements.

Supported SQL Server versions

SQL Server Database Monitor supports the following versions of SQL Server:

- SQL Server 7.5
- SQL Server 2000
- SQL Server 2005
- SQL Server 2008

Key benefits

The technical features of LANGuardian include:

- Secure and tamper-proof for audit and PCI compliance.
- Discover where important data is located.
- Troubleshoot performance problems.
- Identify potential fraud and unauthorized user activity.
- Receive immediate alerts to suspect activity.
- Get reports by e-mail at scheduled intervals.
- Active Directory integration allows you to pinpoint individual users.
- Create audit trails of access to sensitive databases and tables.

Try SQL Server Database Monitor

You can try LANGuardian on our online demo system:

https://demo.netfort.com

If you would like to try LANGuardian on your own network, you can download a free trial version from our website. The free trial is fully functional and last for 30 days from when you first use it. You can download it from our website:

http://www.sqlserverdatabasemonitor.com

Contact NetFort

UK Sales Office
27 Old Gloucester Street London
WC1N 3XX.

Web: www.netfort.com
Email: sales@netfort.com
Phone: (0207) 060 2850

© 2010 NetFort Technologies Limited. All rights reserved.