8MAN

LOGGA:
MONITORING YOUR CRITICAL DATA IN FILE SERVER AND ACTIVE DIRECTORY

In the current business environment, there is a growing need for organisations to provide seamless and transparent information sharing amongst employees. However this is often at odds with complex regulatory and privacy requirements that mean systems need to be in place to prevent data breaches and unauthorised access to information. With 8MAN Logga, organisations can quickly and easily monitor critical and sensitive data access and manipulation, thereby allowing information sharing while ensuring data integrity and security. FS-Logga monitors Windows and NetApp file servers, while AD Logga documents all changes of objects within Active Directory.

8MAN Logga tracks and generates automated reports on all user activities on specified directories, folders and files to meet security and compliance requirements. Tasks that traditionally required countless man hours to complete, can now be accomplished with just a few clicks. Organisations can find out who has accessed which files when and what specific actions were performed. Any unauthorised access, alteration or deletion is instantly recorded and reported. This is essential when investigating suspected data breaches and for meeting information compliance requirements.

ADVANTAGES:

SEGREGATION OF DUTIES

Proprietary information is business sensitive data which gives companies a competitive advantage. Therefore, the access to this data has to be secured and limited to a need-to-know basis.

With Logga, acces rights permissions and duties are clearly visible, helping you safeguard sensitive information

LOGGA SUPPORTS

NTFS Windows Server, NetApp Server and Active Directory.

REPORT 1

Track access
Identify all activities on specific files, folders or directories – who created, read or edited the information.

REPORT 2

What specific changes have taken place?
Detect if permissions have been altered without authorisation.

REPORT 3

Unauthorised access?
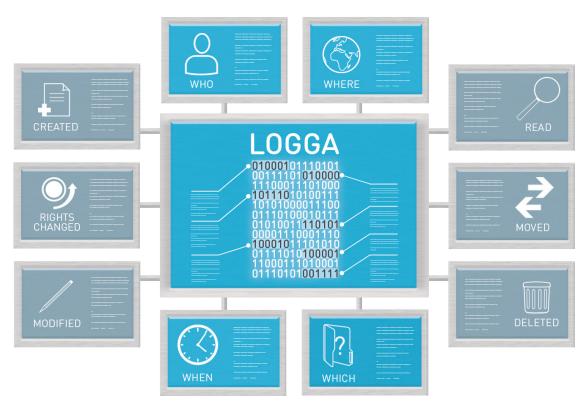Detailed reports provide documented proof of any attempted and unauthorised access.

LOGGA - THE DATA MASTERMIND

Changes in business operations and processes are inevitable - triggered by growth, new technologies and/or external factors. These changes have direct implications on the administration rights within an organisation. With 8MAN Logga organisations can document whether the current administration rights are appropriate for the changing strategy and operations. Employees can then be provided with the information access they need to meet their business goals and objectives.

CREATED

WHO

WHERE

READ

RIGHTS CHANGED

LOGGA

01000101110101
00111101010000
11100011101000
101110101001111
10101000011100
01110100010111
0101001111010101
00001110001110
100010111101010
0111101010100001
11000111010001
01110101001111

MOVED

MODIFIED

WHEN

WHICH

DELETED

TARGETED TRACKING AND REPORTING

Each and every, folder and directory requests can be recorded. However, a significant amount of valuable storage space can easily be access-consumed if the system is not making intelligent selections of which information assets to track and record. With 8MAN Logga, organisations can easily select only those files, folders and directories that need to be monitored for compliance and security purposes. Through this smart selection, 8MAN Logga saves time, resources and storage space.

Company data can broadly be divided into three categories: critical, sensitive and general information. Around 80% of the data a company holds on its servers is not business critical or sensitive in nature. Organisations need an intelligent logging system to ensure only critical and sensitive data access requests and actions are recorded.

The Data Owner concept from 8MAN assists in identifying this remaining data, which is client sensitive or mission critical information with direct impact on a company's health. 8MAN Logga only tracks changes made to this data by continually monitoring for unauthorised access and actions.

Only with 8MAN Logga can unauthorised access to sensitive and critical information tracked and automatically reported upon, providing documented audit trails and timely alerts.