data rover
Your data, your success.

Software Product Description

Advanced User Data and Security Management for any Data-Driven Organisation

> *A single solution for infrastructure and security managers to seamlessly manage two worlds.*

DATA ROVER LTD
Bexhill o/s, E. Sussex, UK | info@data-rover.com | Tel. +44 208 089.0006

It allows data users to explore, manage, process and protect their data effectively and efficiently, by simultaneously addressing the two primary needs related to the use of data: Cyber Security and Data Management.

Data Rover is used in business environments where the management and protection of information and IT infrastructure are critical to business success. Data Rover is extremely powerful in contexts where the storage infrastructure is complex, or when there are numerous users having different levels of permissions to access data. The software is designed for companies that need to ensure compliance with personal (private personnel) data protection regulations and provides detailed analysis of data access permissions.

Data Rover gives you vital information that allows you to make strategic and educated decisions so you can both safeguard, exploit and safely share your data assets while also giving you far greater insight on the efficiency of your resources.

What is Data Rover's technical objective?

Data Rover plays a key role in business asset protection and corporate data management policy definition.

Among its key features the application provides invaluable information in analysing access privileges to files and folders on corporate storage devices. It allows you to analyse the effective permissions of the users, i.e. the real ones. The software helps you identify and distinguish valuable assets from junk information that become unnecessary ballast and an unjustified cost to the company. Data Rover bridges IT security and data management, offering information that is difficult and overly time-consuming to obtain manually or through the use of multiple system tools simultaneously. Data Rover enhances and helps storage infrastructure management operations and allows you to identify security flaws or wastage of resources quickly and precisely. Ultimately Data Rover substantially reduces the company's carbon footprint resulting in overall significant savings.

Data Rover has been designed to respond to on-premise heterogeneous storage environments, and/or those companies preparing to transition to the Cloud, or are in a hybrid configuration.

Who is it used by?

Those who directly benefit from the use of Data Rover are IT personnel, i.e. those who are responsible for managing IT infrastructures and their security. Data Rover helps these professionals identify and remediate

security issues and wasted resources on the organisation's storage devices. Data Rover also provides the business and staff with an environment to safely transfer and exchange data in and out of the organisation.

It is mainly aimed at Chief Technical Officers (CTOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and Data Protection Officers (DPOs), but also to IT managers, system engineers and business managers.

Data Rover is also beneficial to company employees who generate and work data continuously as they are delivered valuable information that identifies situations that require attention. This aspect of Data Rover is crucial in making the user aware and involved in data management.

The solution is applicable in practically all business verticals: healthcare, finance, industry, law enforcement, public sector, and can be used in companies of any size, from the SMEs upwards.

Data Rover Features

Data Analytics

Gives one a complete and detailed on-demand view of the access privileges to the files and folders present across the entire company's storage devices and presents it as if it were a single device. Through the effective permissions display function one can select a user or group and precisely see which files and folders they have access to and with what level of privilege. The function allows you to select a specific file or folder and display the complete list of all users and groups who have the possibility of working on the specified resource and presents the effective privileges available to the various people. Thus you can determine who can E.g., access, modify or delete specific information and so be able to identify eventual security flaws or unauthorised access issues.

The permissions are graphically represented and are easily recognisable thanks to a recurring colour scheme. In addition to the common table-view you can navigate within the files and folders using our dynamic “Security Tree” diagram: the branches of the Tree take on different colours to represent the privilege levels held by the user and follow the same colour scheme of the permissions standardised by Data Rover.

Data Rover's "Point-In-Time" feature provides a historical view of data and permissions within an organisation. It allows users to check and analyse the status applied to data accessibility (effective permissions). Data Rover users can go back and forth in time in order to pinpoint the historical changes and investigate any discrepancies or security issues that may have occurred. The Point-In-Time feature is a powerful tool for ensuring data security and compliance are ratified throughout an organisation's data lifecycle.

Explore Storage Tree

In most modern enterprises, having multiple storage devices for storing data is common practice. However, this distribution across different devices and types can make data management and analysis complicated, especially considering that each device can have its own file system structure and set of access permissions. To address this Data Rover gathers each device and applies a single browser interface.

Data Rover with its Storage Tree feature allows you to view the entire file system structure of each storage device as if it were one large storage system. IT administrators can easily navigate through all the folders present in each storage device and analyse them easily.

Using Storage Tree, Data Rover users can initiate specific analyses on each of the storage devices by activating the advanced Data Analytics features. IT administrators gain insight over the data stored without having to spend hours manually searching and analysing the files and folders one by one. Human error is eliminated.

Dark Data and Data Screening

"Dark data" is junk data. Totally unnecessary, useless rubbish that accumulates over time and constitutes an unjustified cost to the company. 100% of companies suffer from this problem. This data is present in various forms, e.g.; unused or obsolete files, duplicate/triplicate documents, data belonging to users who no longer work in the company, or file types that are either banned or non-pertinent to the company etc.

Data accumulated over time contributes not just to increased occupied storage, but excess management time, backup space and time, power, and even legal costs that bare no added value to the company but quite the contrary. Identifying and removing this "dark data" improves the efficiency and security of your storage infrastructure, freeing up space and resources for more important data and reducing the risk of data loss or security breaches .

Data Rover offers precise information for the identification of each specific Dark Data type and provides statistical information allowing you to evaluate the impact this data has on the infrastructures and therefore to understand the gravity of the situation and take action on the offenders.

Through the Data Screening feature one configures periodic house-keeping routines based on Dark Data reports. These reports group the junk data of each owner, manager, stakeholder and notifies them via email. The user is updated regularly on their personal storage usage so they can self-manage and contribute in keeping the storage systems clean and efficient. Involving the user and stakeholders renders the organisation much more data content aware,

Security Reports

Data Rover generates specific security reports that deliver extremely precise and detailed analysis on the effective permissions applied to files and folders, privileges that can be potentially incorrect and/or dangerous to the information security. Examples of reports are:

"Full Control"

This permission grants the user the ability to perform any type of operation on the file or folder. This includes the right to read, modify, delete, and grant permissions to other users. E,g., if an unauthorised user acquires Full Control permission on a business critical folder, he/she could modify or delete files and compromise the work or security of the entire company. Another case could be where an attacker deletes/modifies files within the folder, or even moves them to another storage location, thus preventing the company from accessing that data anymore. A form of ransom.

"Change Permissions"

Allows the user to change the permissions assigned to users, on a file or folder. E.g., if an unauthorised user acquires the rights to change permissions on a folder then he/she could grant access to confidential data to other users, or even just to himself. If attackers were to obtain this permission, they could increase their access privileges or prevent other users from accessing a particular file or folder.

"Change Ownership"

Allows users to take ownership over a file or folder and thus acquire all related privileges. E.g,, if an attacker takes ownership over a folder containing sensitive data, he/she could gain total control over the folder and its contents and thus allow the person to do absolutely anything with that data.

"Delete"

Allows the user to delete a file or folder. E.g., if an attacker acquires rights to delete a business critical folder, he/she can delete files and affect the business continuity of the company.

These are just a few simple examples of how misconfigurations allow unauthorised users to compromise the security of the company and its data. Data Rover reports quickly identify these risk areas so you can take the appropriate security measures to protect your staff and your business.

File Auditing

Data Rover’s File Auditor essentially determines who did exactly what, from where and when.

Data Rover's file auditing system is an important and powerful tool for monitoring user and administrator activity on company shared folders and files on Windows based file servers. The system allows you to accurately track all the operations performed, such as the creation, modification or deletion of a file or folder, by whom and when. Furthermore, thanks to our IP address tracking Data Rover identifies the location from where the action was performed.

The use of the file auditing system is essential for the security of company data. If one suspects a user(s) has tampered with a file(s) the File Auditing system provides the complete information necessary to check that hypothesis. It can also be used to detect any abnormal user behaviour, such as repeated changes to sensitive files or folders in the organisation.

The information provided by Data Rover can be used to identify any violations of the company's data privacy policy and take the necessary measures to prevent future events from recurring. Access to and use of Data Rover's File Auditing is limited exclusively to authorised company personnel and follows the privacy and compliance regulations in vigour.

Advanced Data Exchange and Tracking

Data Gate provides the company with an advanced data exchange and tracking system exclusively designed for the business guaranteeing both functionality and unprecedented security. The solution includes configurable data cleaning technology that automatically deletes the oldest files from the data share thus preventing storage wastage and potential data leakage. You can automate the “share life” period such that information is only made available to the recipient(s) for a given window of time so ensuring control that nothing is left lying around.

The system also features a storage/user quota management tool whereby staff work only with a set amount of disk space for a given period of time so as not to affect the resources allocated to others. It also offers an effective "data policy" definition system, which allows you to establish which types of files can be shared and to set limits on the size of the files to be exchanged.

Data Gate integrates seamlessly with the corporate Active Directory infrastructure, permitting you to define usage/user privileges directly through AD groups. This means you choose who can use Data Gate and with which level of authorisation by appropriately configuring Active Directory.

Among the most common use cases involves a sender within a "trusted" environment, such as the corporate environment (Intranet), and an external recipient in an untrusted public environment (Internet) needing to share, or work on, business documents. Thanks to Data Gate, these two subjects can exchange files in total safety.

The solution boasts a powerful internal auditing tool that allows you to trace all the actions performed within the Data Gate environment, ensuring the transparency, traceability, and life cycle of the information being exchanged.

Effective Permissions: what are they?

Data Rover's Effective Permissions module essentially determines who has acquired or been assigned the rights to do what and thus highlight what are the true capabilities of users that access, work and modify data stored on the company storage.

"Effective permissions" are the effective/real privileges that a user or group of users have on a particular file or folder in a computer storage system. These privileges are determined by several factors that evolve over time and are the union and combination of the permissions assigned to the user or group in the file system and may differ from those initially assigned due to inheritance, overlapping or nested permissions, or other factors. E.g.,a user might have "read" permissions on a folder due to group membership, but not have "write" permissions due to overlapping permissions assigned directly to the user. The "effective permissions" feature in Data Rover allows you to identify exactly the status of the true access rights for each user or group and thus simplifies the management of permissions and the protection of sensitive data. Through Data Rover, you can find potential security flaws or identify which users or groups have access to information they shouldn't have.

The extraction and analysis of detailed and accurate information on the Effective permissions is extraordinarily complex because it depends on numerous variables, such as the hierarchical structure of users and user groups, the permissions assigned to individual users and user groups, permissions inherited from parent folders and other factors that can influence the final result. Furthermore it may happen that access permissions to files and folders are assigned and changed over time, making the analysis even more intricate. The complexity further increases in a corporate environment, where there are many folders and files, and where access to resources might be managed by a large number of users and user groups. For these reasons, IT administrators will find it very difficult to keep control and maintain the security of corporate data without the help of specialised software tools. Here Data Rover excels in its ability to deliver super high-definition reports on the environment that pin-point exactly what is evolving within the organisation . Through the application of Data Rover one is able to attain total control over who can access what.

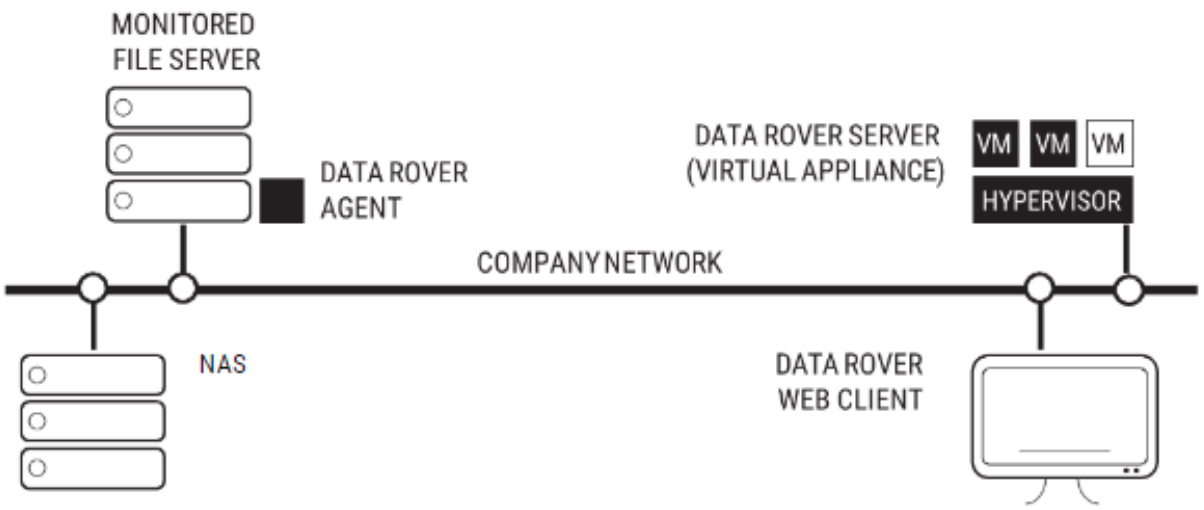
Data Rover infrastructure and components

Data Rover's foundation version requires two components: the Appliance and the Agent, located in the Customer's on-premise infrastructure.

Description

The appliance is a virtual machine hosted on VMWare vSphere or Microsoft Hyper-V infrastructure. The Agent is software installed on a Microsoft Windows Server 2016 or higher machine which, through a user with authorised credentials, acquires information and data from the storage to be monitored (Windows storage of the NTFS type natively, however it is also capable of collecting information from shared folders via Windows SMB/CIFS protocol). The Agent takes care of retrieving and sending the data to the Appliance, where they are processed and made available for consultation by application users.

Data Rover interacts with the Customer's Active Directory infrastructure (Microsoft Active Directory schema version 69 or higher), from which it takes information on users, groups, domains, etc. to be able to cross-reference them with the data collected by the Agent and produce the various reports. Active Directory elements are scanned using the Agent or directly from the Virtual Appliance using the LDAP protocol.



In the diagram above, we see a typical Data Rover installation. The Data Rover server is located within the customer's virtual infrastructure. Monitoring of storage resources (File Server or NAS) takes place via Agents. The Agent can be installed natively on Windows-based file servers or on a support service machine to scan NAS devices.

Minimum Installation Requirements

DATA ROVER APPLIANCE 6.0.1:
Compatible with ESXi 6.5 and above
Processors: 2x2 vCPU (Core)
Memory: 8 GB RAM
Storage: 4 Virtual Disks (“Thin” format)
- OS Disk: 80 GB
- Disk Virtual memory (Swap): 16 GB
- Data Disk 1: 500 GB
- Data Disk 2: 600 GB

DATA ROVER AGENT:
Microsoft Windows Server 2016 or higher operating system
Microsoft .NET Framework 4.8
Windows Management Instrumentation (WMI) support enabled
Latest generation Quad-Core processor at least 2.5 GHz
Memory: 4 GB Ram
Disk space: 150 MB (install)
Disk space: 20 GB (data cache)

Execution of the "Data Rover Agent" service by user account:

1. a domain account user enabled for Active Directory queries (LDAP)
2. belonging to the administrators group on the local machine
3. granted at least read and access permissions to the file system branches to be monitored

The requirements indicated here are the starting point. The final sizing of the Data Rover appliance and configuration of the Agents depend on the characteristics and size of the infrastructure to be managed. Please refer to the product manual for detailed information.

Licensing

The Data Rover software requires a valid and unique customer licence key to use for each installation. If desired a single key may be configured to handle multiple sites. The key is entered during installation and periodically the client side key checks in through the network connection to the Data Rover Cloud. The License Server checks the operating parameters of the installation (parameters covered by the licence).

N.B.: Prolonged absence of connection to the License Server will prevent the extraction of information from the software until the link is restored. Note also that during the loss of contact, or even interrupted use, Data Rover sits in an active set-it-and-forget-it mode constantly collecting data.

DocID:T-SWPRDE-EN | Version:00010

data rover
Your data, your success.

+4402080089.0006

info@data-rover.com

www.data-rover.com