



DATA ROVER™



Throwing light on Dark Data

...and securing your assets

Introduction

... taking important decisions on managing business and personal data can only be done when you have precise and detailed information.

Data Rover™ is the solution for managing and securing user-generated-data on any File System. At **Data Rover** we give you state-of-the-art technology to explore uncharted data territories. **Data Rover™** is your vehicle to help you uncover the junk and examine valuable, and probably delicate, data information on your “planet”, or in the cloud! With this knowledge and our expertise you have the power to decide and do...

Let us help you by discovering and taking full control over what you have... or, didn't know you had! Let us also help you identify hidden threats within your organization and then define preventive measures against further vulnerability. Let us show you on how to keep an eye on user behavioral patterns.

Probing into data content and security

Data Rover™ bridges the gap between user data and content management, data security and infrastructure. One really powerful dynamic solution for your business.

Data Rover™ is an advanced corporate storage management and user data management solution, allowing administrators, directors, heads of department managers and corporate users to get a full understanding on the files that are stored in their shares and corporate filers. With **Data Rover™** the administrator decides what information should go to which set of people within the organization and what they can, or could do, with the information provided. With **Data Rover™** the objective is to get insight and total control over your user data and the “dark data” residing in your organization.

Data Rover™ is your *vehicle* to:

- Understand what data you have, where it is..., and who and when has had access to it...
- Apply intelligent and advanced data management policies...
- Control and track user generated data and content...
- Achieve regulatory Compliance (GDPR, SOX..)
- Help enforce a “least privilege” model
- Discover and fix insecure file access rules...
- Backtrack and identify and prevent data leakage and abnormal user behaviour...
- Screen the data that you allow into your organisation and report back to those responsible or accountable...
- Distinguish and classify data types for legal compliance, governance, age, redundancy...
- Highlight the dark areas of your Business Data *and take action*...
- ... ultimately the objective is to be proud of your company and your work!

Data Rover™ - the probe has landed!

Data Rover™ is the vehicle we started building the year the infamous Martian rover Curiosity landed on Mars. Our **Data Rover™**, like all rovers, has a scientific mission to accomplish. Go over the terrain, collect the data, and determine if the environment we are in is safe and hospitable.

Data Rover™ delivers the answers to all those questions and actively prevents recurrence. Not only will you be in control but you will also save substantially, starting from your resource management to being able to invest



far better in optimizing your security and business development. With our solution we guarantee you will gain Knowledge and Power! Let us help you.

To be on the leading edge you need to be aware and in control...

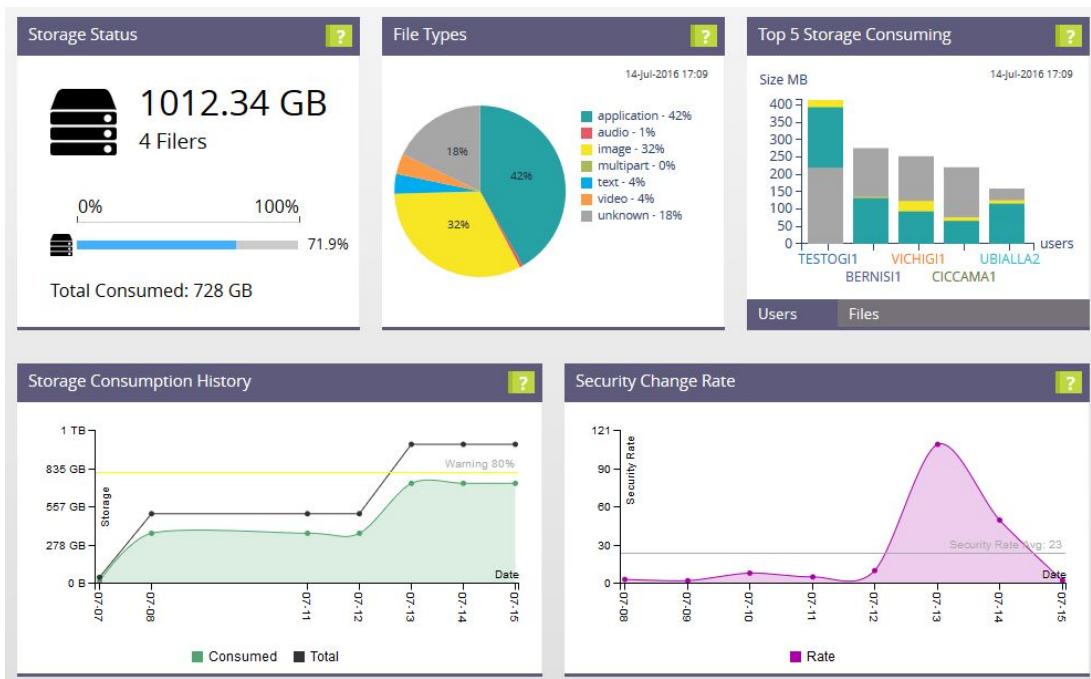
Dark Data is operational data that is not being used or shouldn't be there. Consulting and market research company Gartner Inc. describes dark data as "information assets that organizations collect, process and store in the course of their regular business activity, but generally fail to use for other purposes".

Dark Security. Your file system contains critical business data and sensitive information that is the fruit of thousands of hours of work. A data theft, loss and corruption if left unprotected leads to downtime and service disruption. Downtime is extremely costly not just from the technical point of view but undoubtedly has a huge business impact. The only solution is to take control by protecting and administering the user's activities on the file systems.

Data Rover™ offers advanced easily-generated security reports to CISOs and CTOs.

True Effective Permissions. Are you absolutely sure that the information given to you by Microsoft® "Effective Permissions" represents the maximum allowed rights for a user or group? If your answer is NO, you should read further on and, instead of worrying, take action! By calculating the set ACLs at all levels, **Data Rover™** can easily tell you the exact and real Effective Permissions applied to a file or a folder. Do you already have an Auditing tool? Consider that auditing tools are just made to log activities, not to analyze them in different contexts. This means you won't be able to get the true Effective Permissions a user has on a file or folder, just to know that the user has accessed or removed a file.

Data Rover™ automates and actively does the process of security analysis and permission reporting. It provides a scalable and cost-effective way of managing network data resources across the organization.



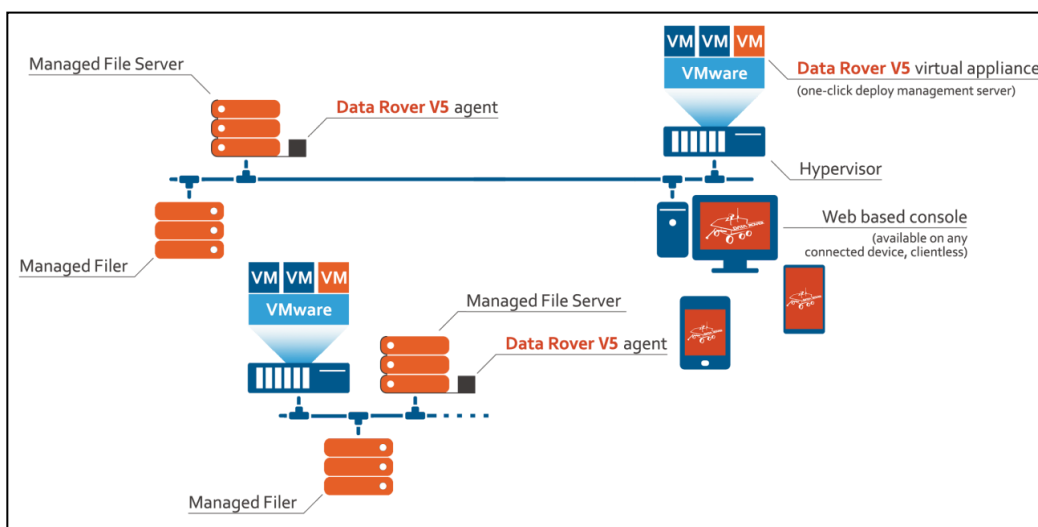
The Data Rover™ Dashboard gives you an immediate view of how users are working with corporate data within the monitored environment. The Security Change Rate chart lets you easily identify potential issues in the data security area.



Data Rover™ architecture and technical details

Data Rover™ architecture is mainly built on:

- An exclusively web-based console
- Well-supported web-based technologies
- Secure linux-powered virtual or physical appliance
- No direct access to the internal appliance components (including database)
- Multiple and strong volumes encryption
- Peer-to-peer smart-routing between Data Rover™ nodes (including agents)
- Super-simple architecture
- HTTPS-only communications



No more waiting on the phone for application support! With the brand new **Telemetry & Support Mode**, Data Rover™ Ground Control can automatically retrieve logs, diagnose and fix issues while your system keeps running. It's all silent and non-interruptive, just flip the switch to consent privacy-proof and fully encrypted remote support operations.