

White Paper: Managing Unstructured Data: 10 Key Requirements

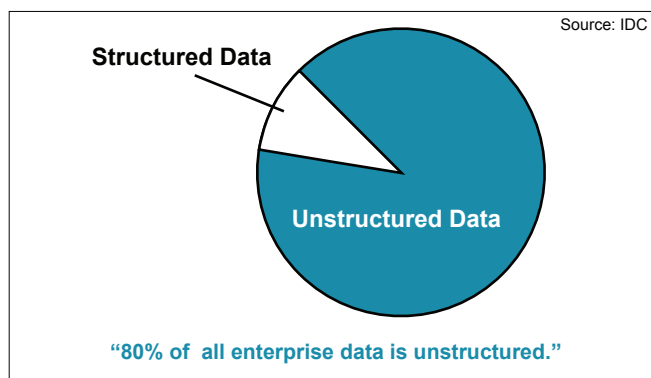


CONTENTS OF THIS WHITE PAPER

The Ten Key Requirements.....	2
Visibility.....	2
Control.....	2
Auditing.....	2
Security.....	3
Performance.....	3
Scale.....	3
Ease of Installation.....	3
Ease of Use.....	3
Ease of Integration.....	3
Low Total Cost Of Ownership.....	4
Conclusion.....	4
About Varonis.....	5

Managing Unstructured Data: 10 Key Requirements

un-structured data: Unstructured data refers to computerized information that does not have a data structure (i.e. exist within a database). Examples of “unstructured data” may include documents, presentations, spreadsheets, scanned images, multimedia files, etc.



The following are ten key requirements for any effort, system or technology whose purpose is to protect business data and specifically the documents, presentations, spreadsheets, scanned images, multimedia files, etc. that fill file servers and form any enterprise’s valued assets.

When considering which technology to implement to realize your data management objectives, it is important to gauge the effectiveness of the solution against the ten requirements of data protection. These requirements are: visibility, control, auditing, security, performance, scalability, ease of installation, ease of use, ease of integration and low total cost of ownership. Additionally, any system for controlling access to unstructured data has to provide sufficient automation to make the process continuous and accurate.

THE TEN KEY REQUIREMENTS

Visibility

Any solution for unstructured data management and control must provide a clear visual representation of the access settings to the data as they are currently defined in the existing network. This visual must show, in an aggregated and searchable fashion:

- All users including their group memberships, Active Directory attributes and data permissions
- All folders and sub folders within a file server as well as the Microsoft NTFS permissions to this folder for any user or user group who is part of the domain
- Filtered views that allow queries based on username, group name or folder/data name
- Automated updating of views to reflect changes or new data within Active Directory (i.e., user to group membership) as well as within the file server (i.e., new data, deleted data, renamed data)

Control

Any solution for unstructured data management must include all mechanisms to define, test, enact and reverse file and folder permissions. Specifically the system needs to provide:

- The means to “push” or commit changes to access permissions directly onto the file server. The mechanism should include an option to push changes explicitly with system administrator intervention or in an automated fashion via a scheduler.
- “What If” capabilities, otherwise known as a sandbox where changes to folder permissions can be carried out in a simulated fashion in order to determine what, if any, the impact to access will be. For instance, the system shall allow the revocation of an entire group’s permissions in a sandbox. The system should indicate clearly which legitimate users will be affected negatively and allow for mitigation of that condition prior to live push.

Auditing

A detailed audit must be provided for all aspects of data use. The presentation of the information should be easily comprehensible and searchable. Specifically, the audit record should include:

- All file touches for a given Active Directory user (i.e., open, delete, rename)
- All access by access type (i.e., open, delete, rename)
- All access activity by folder
- All access detail to sensitive folders
- All inactive users
- All inactive data sets
- All administrative changes including security configuration changes by administrators
- On-hand searchable audit record for a period of no less than 12 months
- The information listed above should be available as reports in different formats, and should be exportable
- The delivery of reports to subscribers should be automated and able to be scheduled.
- The audit information should be searchable with support for complex Boolean (e.g. “and”, “or”, etc.) search conditions.

Security

A system for unstructured data governance needs to provide an automated means for the revocation of data permissions. Specifically the system should:

- Identify by name all users whose access to a given data set should be revoked
- Re-compute revocations as changes to Active Directory and file servers occur
- Provide the means to test the recommended revocations prior to enacting on the servers for enforcement
- Provide revocations with accuracy greater than 3 nines (99.9%)

Performance

Any proposed solution for unstructured data management should not impede the performance of file servers, the user access experience or business traffic flow. Specifically, the system should not require Windows auditing in order to deliver its core functionality for data control.

Scale

Because most organizations add additional file servers over time, and unstructured data can grow rapidly, the system has to provide room for growth. A data governance solution should be able to scale to accommodate unstructured data doubling in volume every 12 months.

Ease of Installation

A practical data protection solution cannot disrupt business operations or traffic flow. A solution should install quickly (e.g., within 5 business days), without the need for specialized professional services, and without assigning dedicated IT staff.

Ease of Use

A solution should not require specialized off-site training in order to operate. Any necessary training should be simple, and something the vendor can deliver themselves, on-site. Of course, the user interface should be intuitive.

Ease of Integration

Data protection solutions need to support a range of file servers and storage devices including Windows Server 2003 and network attached storage (NAS) from leading NAS vendors.

Low Total Cost of Ownership

A solution for data protection has to demonstrate quantifiable benefits in time and resource savings. Be sure to look for automation in the following areas, which are often the most manually intensive:

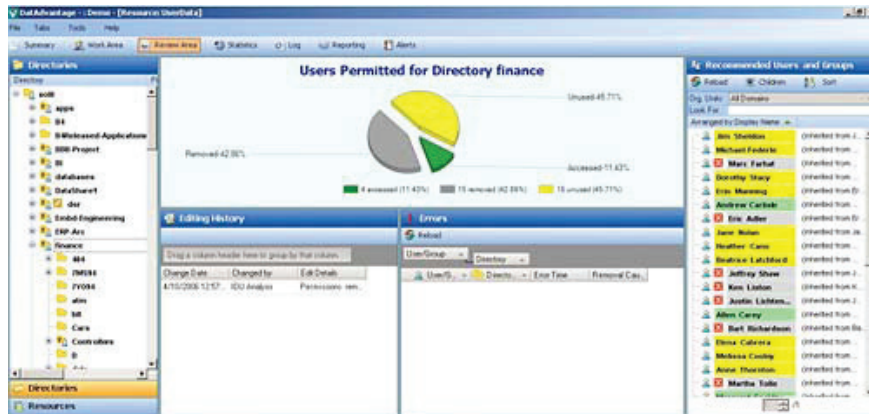
- Data permission revocations
- Data audit report generation
- Data entitlement review
- Stale data identification
- Data business owner identification
- Data migration

CONCLUSION

Varonis Systems is a software company unilaterally focused on data governance. Our software solutions deliver on the ten imperatives for protecting unstructured data by showing exactly who has access to it, how individuals are using their permissions and who should have their access revoked. And, Varonis dynamically adjusts as changes to either directories or file servers occur, so that access controls to shared data are always warranted and based on business needs. With Varonis in place, the fundamental step to data loss prevention is addressed: limiting what data makes its way to laptops, printers and USB drives. That way, efforts to further protect data via filtering, encryption, etc., can be focused on only those items that are valuable, sensitive and actively being accessed.

VARONIS® DATADVANTAGE®

With Varonis® DatAdvantage®, you can see individual users and the groups they are part of, drawn directly from your user repository. You can see every folder and file on your file servers. And with Varonis, you can now connect the two. With just a few clicks you can see what groups a user is part of and where their permissions came from.



Functions

- Visualizing the entire data access control environment
- Adaptively determining proper authorizations
- Identifying data business owners
- Auditing and reporting on all aspects of data use

Benefits

- Effective and scalable data access control
- Increased and consistent data protection
- Reduction in the cost and complexity of data control
- Comprehensive and granular auditing of data use

ABOUT VARONIS

Today Varonis is the foremost innovator and solution provider of comprehensive, actionable data governance solutions. The company’s installations span leading firms in financial services, healthcare, energy, manufacturing and technology worldwide. Based on patent-pending technology and a highly accurate analytics platform, Varonis solutions give organizations total visibility and control over their data, ensuring that only the right users have access to the right data at all times.