



Contents of This Paper

Available Tools	2
The Solution.....	2
A Closer Look	2
Accessing Folders.....	3
Who's Authorizing Users.....	4
Tracking Key Files	5
Tracking the Last User of a File	5
Matching People to Data.....	6
Varonis for Auditing.....	7
Conclusion	7
About Varonis	7

Accelerating Audits with Automation: Understanding Who's Accessing Your Unstructured Data

Your Challenge

Many organizations have to respond to the queries of internal or external auditors and demonstrate that access to their unstructured data is being properly controlled. Questions such as the following from auditors are not uncommon:

- How do you know who can access this folder with financial/customer/sensitive data in it?
- Who authorized a user to have access permission to a file and how?
- If a key file was deleted, how would you know it happened, or who did it?
- Who were the last people to access a critical folder, and what did they do?
- How do you make sure that the right people have access to your data?

The urgency and frequency of such questions may vary, but one constant is that finding answers is time consuming and challenging.

If your organization still spends hours trying to get answers to seemingly simple questions about file access settings and activity, you are not alone. Today's IT managers are challenged to find a consistent way to quickly account for the activities of users and other IT personnel when it comes to unstructured data access.

Accelerating Audits with Automation: Understanding Who's Accessing Your Unstructured Data

Available Tools

Most people facing these questions quickly learn that the available tools are lacking. The Windows Event Viewer is insufficient to provide the level of detail needed. File server access logs provide too much data, get large quickly, and really slow servers down. Analytics and configuration management products deliver some relief in parsing logs, but you still end up spending hours trying to answer simple questions about access settings and activity. These tools just give you a better way to search for the answers, but not the answers themselves. In the end, you need lots of time to use these tools, as well as a pair of expert eyes.

The Solution

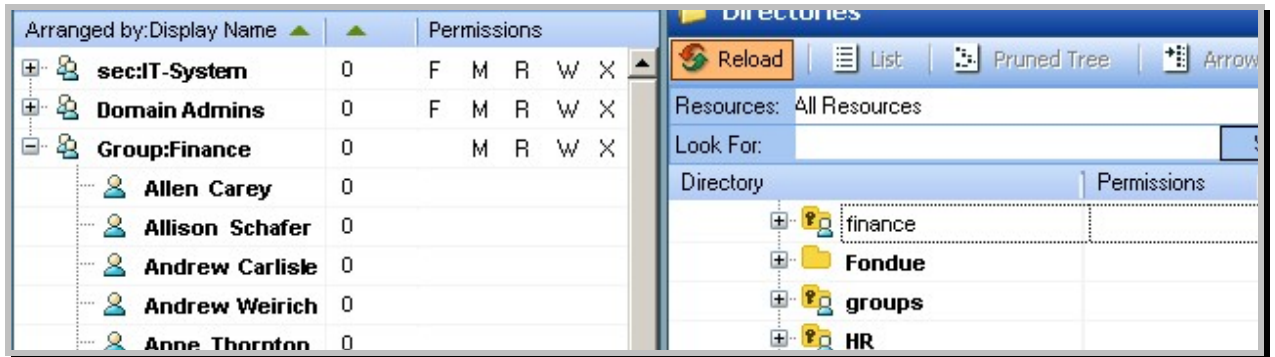
Varonis DatAdvantage and DataPrivilege provide immediate answers to these questions – and more – through an intuitive graphical interface and reports. Our solutions anticipate your questions, and put the answers – not just log data – at your fingertips. Our patent pending technology quickly finds all access events and correlates each with user and user group information. The result is answers to your exact questions about who is accessing data and how they are using it. This information is collected without impacting space or performance on your file servers, and is presented in a straightforward user interface and through configurable reports.

A Closer Look

The following sections show how Varonis solutions present the information you need for auditing, access control and data governance of your unstructured data.

How do you know who can access this folder with financial/customer/sensitive data in it?

Varonis DatAdvantage provides a quick answer to this in two ways. If you need to know which users and groups have access to a folder, simply double click on the folder in the Work Area, and the users and groups with access to the folder are displayed along with corresponding permission levels. In the example screen below, you can see on the left which groups – and users – have access to the “finance” folder.



This information can also be generated in the DatAdvantage report, “User or Group Permissions on Directory.” Conversely, you may be called upon to identify what data a specific user or group can access. With Varonis DatAdvantage, you simply double click on the name of the user or group in the DatAdvantage “Work Area”. All the folders and files accessible to them appear highlighted in green, and their level of access (e.g., full, read, write, etc.) is shown, as is the source of access permission. In this example, clicking on the “Finance” group on the left results in all folders to the right where they access permissions to be highlighted in green.



This information can also be generated in the DatAdvantage report “Resource Permissions for User or Group.”

Varonis DataPrivilege also provides user and group access information for any managed directory, allowing data owners to verify at any time that the correct users and groups have access to their data.

Who authorized a user to have access permission to a file and how?

Varonis provides you this information in two ways. The first way is with Varonis DataPrivilege. With DataPrivilege, data owners themselves – rather than IT staff – are responsible for authorizing access to their data. When a user requests access via DataPrivilege’s web request form, the request is routed to the appropriate data owners. Owners approve or deny requests, specifying the level of access (e.g., read, write, etc.), an (optional) access expiration date, and the reason for granting or denying access. Every approval is logged in thorough detail, providing a record that can be used for auditing, generating reports or search queries.

In the example below we see three requests, two of which were approved. Each request includes information about when access was granted (or denied), by whom and why, making it easy to answer the questions of how a particular user got access and who gave it to them.

ID	Status	Date	Op. Type	Req. Type	Requested By	Requested For	Request On
1	Declined	September 7	Grant	Permission	FinUser	FinUser	...DP\NEW YORK\FINANCE\PAYROLL
3	Approved	September 7	Grant	Permission	FinUser	FinUser	...ORK\FINANCE\ACCOUNTS PAYABLE
5	Approved	September 7	Grant	Permission	FinUser	FinUser	...FINANCE\ACCOUNT RECEIVABLE

The second way Varonis answers this question is with Varonis DatAdvantage. DatAdvantage shows permissions as they are set in your environment, indicating where those permissions come from in the context of group membership or file system ACLs. This information is helpful, for example, in understanding if permissions were inherited from a global group, etc. In the example below, we see that Michael has access to the file “payments2K6.xls” because he inherited them as a member of the “Legal” group.

	Directory	Permissions	Explanations
Darren Parker	Corporate		
Fred Phelps	employment.dot		
Melissa Do...	Old Files (Kell...		
Michael Federle	payments2K6.xls	F M R W	(Inherited from "Legal")

Varonis DatAdvantage also provides a detailed audit trail for objects via its Object History. This information provides details about when changes were made to users and folder ACLs. These details can be helpful for both auditing and for performing a “roll back” to a previous state.

If a key file was deleted, how would you know it happened, or who did it?

Varonis DatAdvantage provides a complete audit trail of file and folder “delete” events in its Log Area. All events can be searched and sorted to pinpoint exactly who deleted a file on any monitored server, and when. Any search result can be exported immediately to Microsoft Excel with two mouse clicks. Here’s an example showing who deleted the file “Tax Withholding Clause.doc” at 10:34AM on April 2, 2006.

User Name	Operation	File Name	File Type	Event Count	First Time	Last Time	Directory
Operation: DELETE (1)							
User Name: Allen Weinheimer (1)							
Allen Weinheimer	DELETE	Tax Withholding Clause.doc	doc	1	4/2/2006 10:34:0...	4/2/2006 10:34:00 AM	ONTAP_ADMIN\$\vol\vol0\

DatAdvantage also provides this information in the “*Detailed Access Summary*” report. This report can be sent to the data owner on a scheduled basis for review, which can be especially helpful for sensitive files.

Who were the last people to access a critical folder, and what did they do?

As is the case with deleted files, Varonis DatAdvantage tracks when an “open”, “create” or “rename/move” occurs. This makes determining who last accessed a specific file or folder, and how, as simple as selecting double clicking on the file name in the DatAdvantage Log Area. Here’s an example showing Melissa Cooley was the last person to access the file “Option Promises...” in the time frame under investigation.

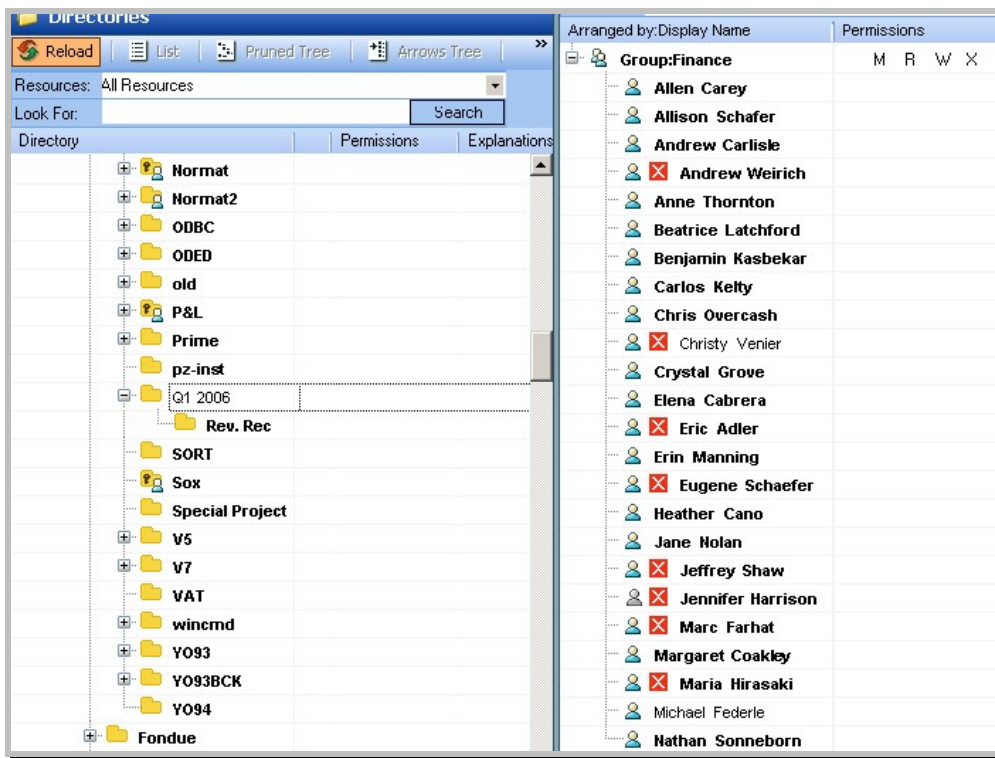
User Name	Operation	File Name	File Type	Event Count	First Time	Last Time	Directory
File Name: Option Promises Q1 2005.xls (15)							
Melissa Cooley	OPEN	Option Promises Q1 2005.xls	xls	1	4/3/2006 11:09:0...	4/3/2006 11:09:00 PM	ONTAP_ADMIN\$\
Alex Weinger	OPEN	Option Promises Q1 2005.xls	xls	3	4/3/2006 1:36:00...	4/3/2006 1:45:00 PM	ONTAP_ADMIN\$\
Alex Weinger	RENAME	Option Promises Q1 2005.xls	xls	1	4/3/2006 1:37:00...	4/3/2006 1:37:00 PM	ONTAP_ADMIN\$\
Melissa Cooley	OPEN	Option Promises Q1 2005.xls	xls	1	4/2/2006 11:09:0...	4/2/2006 11:09:00 PM	ONTAP_ADMIN\$\
Melissa Cooley	OPEN	Option Promises Q1 2005.xls	xls	1	4/2/2006 11:09:0...	4/2/2006 11:09:00 PM	ONTAP_ADMIN\$\
Melissa Cooley	OPEN	Option Promises Q1 2005.xls	xls	1	4/2/2006 11:09:0...	4/2/2006 11:09:00 PM	ONTAP_ADMIN\$\
Melissa Cooley	OPEN	Option Promises Q1 2005.xls	xls	1	4/2/2006 11:09:0...	4/2/2006 11:09:00 PM	ONTAP_ADMIN\$\
Alex Weinger	OPEN	Option Promises Q1 2005.xls	xls	11	4/2/2006 10:54:0...	4/2/2006 7:26:00 PM	ONTAP_ADMIN\$\
Alex Weinger	OPEN	Option Promises Q1 2005.xls	xls	11	4/2/2006 10:54:0...	4/2/2006 7:26:00 PM	ONTAP_ADMIN\$\
Alex Weinger	OPEN	Option Promises Q1 2005.xls	xls	11	4/2/2006 10:54:0...	4/2/2006 7:26:00 PM	ONTAP_ADMIN\$\
Alex Weinger	OPEN	Option Promises Q1 2005.xls	xls	11	4/2/2006 10:54:0...	4/2/2006 7:26:00 PM	ONTAP_ADMIN\$\
Alex Weinger	RENAME	Option Promises Q1 2005.xls	xls	10	4/2/2006 10:54:0...	4/2/2006 3:48:00 PM	ONTAP_ADMIN\$\
Alex Weinger	RENAME	Option Promises Q1 2005.xls	xls	10	4/2/2006 10:54:0...	4/2/2006 3:48:00 PM	ONTAP_ADMIN\$\
Alex Weinger	RENAME	Option Promises Q1 2005.xls	xls	10	4/2/2006 10:54:0...	4/2/2006 3:48:00 PM	ONTAP_ADMIN\$\
Alex Weinger	RENAME	Option Promises Q1 2005.xls	xls	10	4/2/2006 10:54:0...	4/2/2006 3:48:00 PM	ONTAP_ADMIN\$\

DatAdvantage also provides this information in the report labeled, “*Detailed Access Summary*.”

How do you make sure that the right people have access to your data?

Varonis DatAdvantage uses patent-pending technology to identify users who have permissions that they don't need – that is, more access rights than required to perform their jobs.

DatAdvantage identifies these users for any folder with a simple double click on the name of the folder in the Work Area. A red “X” appears next to those users that may be removed from Active Directory Groups on the folder's ACL, as well as any users or groups that may be removed from the ACL itself. In the example below, there are several users in the Finance group who do not need access to the “Q1 2006” folder to do their jobs – yet they have access. Varonis DatAdvantage recommends revoking their access, and provides a sophisticated “what if” environment to ensure you are comfortable with any changes before committing to them.



DatAdvantage also provides this data in the reports “Summary of Changes for Directory” and “Summary of Changes for User or Group.” These reports can dramatically speed up a permissions entitlement review by highlighting access that can be tightened without interfering with business processes.

Varonis For Auditing

Varonis DatAdvantage and Varonis DataPrivilege simplify auditing, making it easy to see, understand and report on user access to unstructured data. That's an important first step in meeting the demands of auditors and establishing proper data governance for your unstructured data. To learn more about what Varonis DatAdvantage and Varonis DataPrivilege can do for you, contact us for a free evaluation by phone at 877-292-8767, by email at sales@varonis.com, or on the web at www.varonis.com.

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 its, 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.

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, health care, 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.

Varonis Worldwide Headquarters

499 7th Ave., 23rd Floor
New York, NY 10018
Phone: 877-292-8767

www.varonis.com