

CONTENTS OF THIS WHITE PAPER

Introduction.....	1
Revolutionizing Permissions Management with Automation	2
Identifying the Data Which Needs Reviewing	2
Align Data with Security Groups	2
Identify Data Owners	3
Providing Actionable Data	3
Executing the Decisions	3
Auditing the Process.....	3
Summary	4
Contact Us.....	4

Revolutionize Your Permissions Management

INTRODUCTION

Information resources, like folders on file servers, are protected by access control lists containing security groups. Users are gathered into these groups according to department, role, function or organizational need. If users are put into only the appropriate groups, and these groups are inserted into only the correct access control lists, then only the right users will have access to the data in that folder.

What happens in practice, however, is that many IT departments face significant challenges keeping the right users in the right groups and mapping the right groups to the right folders. As users move through an organization—changing roles, joining cross-functional teams, etc.—they require access to more and more data. The access control lists used to protect data often don't accurately reflect the needs of the organization—users have access to more than they need, increasing the likelihood of data loss, misuse and theft. IT doesn't have the ability to effectively reduce access without impacting organizational activity.

Who should actually be making access control decisions? IT has the ability to manage security groups and change access control lists, but technology administrators should not be burdened with deciding who has access to organizational data. Data access rights are an organizational decision, and need to be made by those with appropriate knowledge and authority to do so—those with the organizational context to make the right decisions about access to data. As requirements change, access rights should change with them. For example, when a user changes his role, that user should probably no longer have access to data resources that they no longer need. Additionally, new users often have their access rights “cloned” or duplicated from others—if the original user had too much access, so too does the new user.

In order to make sure that access rights, or entitlements, accurately reflect organizational need, they need to be reviewed on a regular basis. This process is often called an “entitlement review,” “re-certification” or “attestation.”

REVOLUTIONIZING PERMISSIONS MANAGEMENT WITH AUTOMATION

It is no longer possible for organizations to effectively review access without automation. In order to perform entitlement reviews, the organization must know—at a minimum—what data and which security groups require review, which groups grant access to what data, who is the owner or steward for each data set, and who has access to each data set and is in each group. These “must know” requirements take so much time to meet that IT cannot hope to provide this information to the organization in a timely, recurring manner for the data they have, much less keep up with data that is growing at 50% per year (Source: Gartner).

What’s needed is an automated entitlement review process that shifts the way IT works, and the way the organization thinks about data management and protection. IT will stop playing the intermediary between the data and the data owners, reduce its manual workload, and improve security at the same time. Automation will programmatically identify the resources that need to be reviewed, align security groups with data sets, identify data owners, route required access information—and actionable intelligence—to those owners, execute their decisions, and provide auditable evidence that the process is being followed.

Effective entitlement reviews will:

- Be generated automatically, taking information from access control lists and user and group repositories
- Be provided to data owners automatically
- Be functional and user-friendly, providing only information that’s needed to accurately perform a review
- Provide intelligence to help owners make proper decisions about access
- Automatically commit desired changes (so that IT doesn’t have to do it)

Identifying the Data Which Needs Reviewing

The highest level folders in a data repository where a non-IT user or group has write or read access, or “demarcation points,” need to be identified automatically. If the organization has access, that folder’s access needs to be reviewed by someone designated by the organization—a data owner or steward.

Align Data with Security Groups

When access to data is controlled by security groups, it’s critical that the groups themselves are properly aligned with the data sets they’re meant to protect. A group should give access to the data sets that are required while not granting access to anything else. This requires complete visibility into who can access a data set, and which data sets can be accessed by which groups. If the groups do not align with data, they need to be adjusted or new groups need to be created. Automation is required to provide this visibility, and to programmatically create new groups and re-permission the data sets if necessary.

varonis® Access Statistics						
Access Path	User Name	Date	SAM Account Name	File Server	Event Count	Event Count on Subdirs
C:\HR					8	810
	Root-Domain\Ann Perrino				0	41
	Root-Domain\Don Penisson				8	721
	Root-Domain\Erica Caffrey				0	48
C:\HR-Private					0	174
	Root-Domain\Alex Weinger				0	156
	Root-Domain\Frances Weidenfeller				0	4
	Root-Domain\Melissa Cooley				0	14
C:\Human Resources					0	185
	Root-Domain\Alex Weinger				0	59
	Root-Domain\Denise Walters				0	6
	Root-Domain\Frances Weidenfeller				0	120

*Report generated on 4/9/2009 9:09:47 AM

Identify Data Owners

Once the containers and security groups that need to be managed (and be regularly reviewed) are identified, the appropriate organizational representatives need to be involved in the entitlement review process. The most efficient method to identify a data owner is to analyze access activity to see which users are most actively accessing data sets, and combine this information with other metadata, such as the Department Name or Managed By fields in Active Directory. Automation should provide this information, reducing by an order of magnitude the time required to accurately identify a data owner.

Providing Actionable Data

Providing a long list of users to each data owner is ineffective. Dozens, or even hundreds of users may have access to a data set or belong to their groups, and data owners may be asked to review many data sets and many groups. Data owners need a short list of users to pay attention to—those that should probably be removed based on sophisticated analysis and users whose access the owner has not previously approved.

Executing the Decisions

Once a data owner has made the decision to revoke access, automation should execute those decisions so that IT does not need to manually effect the changes. For IT, each group or access control list change takes time, requires administrative credentials, and introduces an opportunity for error.

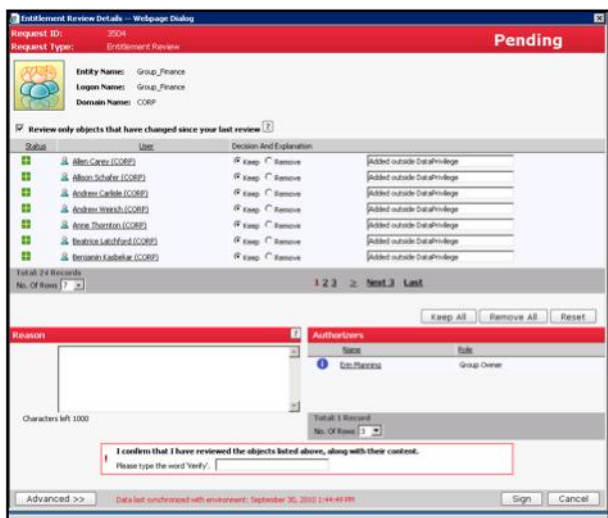
Auditing the Process

Not only does the process need to be automated, there must be evidence that the process is being followed, and controls to identify when it is not being followed. An automated solution will be completely auditable and reportable, so that there is a record of every entitlement review and every access decision that is made.

SUMMARY

Using Varonis® DatAdvantage® and DataPrivilege®, organizations can implement an automated entitlement review process that meets all of these goals far more efficiently than through manual methods. DatAdvantage provides complete visibility into the permissions of an organization’s unstructured and semi-structured data: who can access data, who is accessing data, and actionable intelligence on who should have access. With DataPrivilege, data and group owners are provided regular, automatic entitlement reviews. Owners are given all of the relevant information about their resources, including intelligent recommendations made by DatAdvantage on where access can be reduced without impacting organizational activity. Once submitted, changes can be committed to file and directory servers automatically.

With Varonis, IT can automate antiquated, manual processes that are inefficient and ineffective, and keep pace with growing data sets, and the growing numbers of containers and groups. Automated entitlement reviews using Varonis are more accurate while reducing the burden on IT and eliminating errors which can affect the organization. The entire review process is audited, so IT administrators, compliance officers, and management are able to report on the health of the review process, ensuring that policies are not only implemented, but verified. With proper intelligence, workflow and automation, Varonis helps IT meet the challenges posed by explosive data growth, ensuring proper management and protection of critical data resources—now and in the future.



CONTACT US

Worldwide Headquarters
 499 7th Avenue, 23rd Floor, South Tower
 New York, NY 10018
 Phone: 877-292-8767
sales@varonis.com

WORLDWIDE HEADQUARTERS

499 7th Ave., 23rd Floor, South Tower
 New York, NY 10018
 Phone: 877-292-8767
sales@varonis.com

EUROPE, MIDDLE EAST AND AFRICA

1 Northumberland Ave., Trafalgar Square
 London, United Kingdom WC2N 5BW
 Phone: +44-0-800-756-9784
sales-europe@varonis.com