

CONTENTS OF THIS WHITE PAPER

Overview	1
Why Review Entitlements?	2
Entitlement Review Challenges	2
A New Approach to Entitlement Reviews	3
A Project Plan for Entitlement Reviews	4
Phase 1: Risk Mitigation	5
Phase 2: Entitlement Optimization	10
Phase 3: Continuous Improvement	12
Conclusion	16
About Varonis	16

Entitlement Reviews: A Practitioner's Guide

OVERVIEW

For many organizations, conducting Entitlement Reviews is time consuming, error prone, and mostly manual. Complicating matters is the challenge of identifying the business owners of data – the very people who can help make critical decisions about entitlements.

Using Varonis DatAdvantage will dramatically streamline your Entitlement Review process by automatically and continually updating entitlement information, and providing visibility into data ownership. This expedites the whole effort, and makes it manageable and repeatable.

This document delivers a step-by-step process that your organization can follow to ensure that you know who owns each data set and who should have access to that data. This Entitlement Review process allows organizations with DatAdvantage to operationalize Entitlement Reviews and ensure access to their unstructured data is based on business needs.

WHY REVIEW ENTITLEMENTS?

In nearly every organization today, access to unstructured data is broken. Data is accessible by far too many people who have no business need to access the data. This is due primarily to the dynamic nature of business – with new project teams constantly forming, and job roles and responsibilities always changing – combined with the challenges of managing data access permissions, which usually end up being inherited rather than explicitly assigned based on business need.

By adopting a consistent, methodical practice of Entitlement Review – discovering and reducing excess permissions to unstructured data – IT organizations can transform this permissions landscape into one that keeps pace with personnel and data changes. Performing Entitlement Reviews with Varonis DatAdvantage reduces the time required to complete a Review, provides continually updated information, and, as a result, improves the ongoing accuracy of the access permissions to your unstructured data.

ENTITLEMENT REVIEW CHALLENGES

Historically, Entitlement Reviews have been a reactive, mostly manual process to ensure and/or demonstrate that users have appropriate access to shared data. For many organizations, the Entitlement Review goes something like this:

- The IT organization is tasked with conducting an Entitlement Review as the result of a periodic compliance audit, lost or deleted data, an access control breach, etc.
- An IT manager compiles a large spreadsheet showing which users have access to each folder, and then sends the spreadsheet to data owners for review.
- Data owners review the spreadsheet, marking the names of people that can have their access revoked, and then send the spreadsheet back to IT for implementation.

The challenges with this approach are many. First, because a project run this way can take weeks or months to complete, most organizations opt to perform these reviews only once a year. Obviously, changes within organizations rapidly outstrip the validity of a yearly Entitlement Review. Second, even after all this work, it is difficult to ensure the accuracy of the reviews because they are so manual. They depend on the accuracy of the spreadsheets, the diligence and accuracy of the data owners when reviewing the spreadsheets, and the accuracy of IT when implementing the changes. Finally, many organizations cannot identify the true business owner for a given set of data.

A NEW APPROACH TO ENTITLEMENT REVIEWS

DatAdvantage dramatically streamlines the Entitlement Review process by automatically and continually updating entitlement information, and providing visibility into data ownership. This not only simplifies the Entitlement Review process, but ensures it's up to date, accurate and has the desired business impact.

A New Approach to Entitlement Reviews

Identifies Data Owners

DatAdvantage simplifies the identification of data owners by analyzing data usage. Simply double click on any data set in the Statistics Area, and a complete activity report will appear including a list of active users, activity dates, and active directories. While the most active users may not always be the data owners, they often work for the data owner, or at least know who the data owner is.

Makes Permissions Recommendations

Based on analysis of actual data use over a period of just several weeks, DatAdvantage continuously monitors and automatically recommends which users should be removed from having access to data. DatAdvantage administrators can enact these recommendations in the live environment with a mouse click, or test and visualize their impact in a sand box prior to implementing. These recommendations are based on observed usage patterns, and in just 4 to 6 weeks are better than 99% accurate.

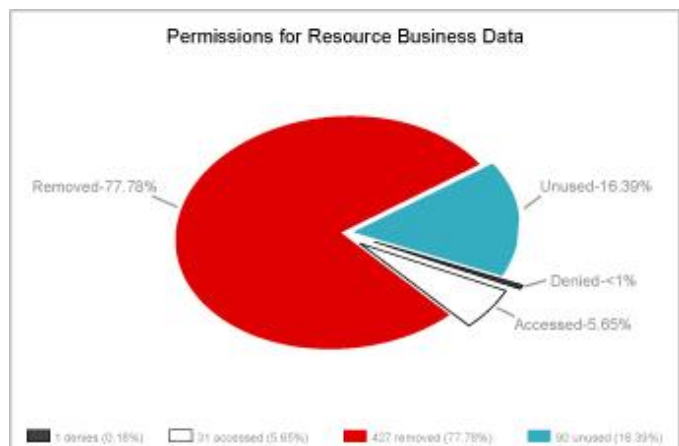
Provides Continuously Updated Information

As business conditions change, DatAdvantage keeps pace. If, for example, a user changes jobs or their project ends, and they no longer access a certain set of data, DatAdvantage will observe this behavior and recommend revoking the user's access permission. DatAdvantage can even send data owners the new permissions recommendations on a scheduled basis for their review and approval.

Monitors Global Group Access

To aid in the identification of users who have inherited access entitlement through global groups (Everyone, Domain Users, etc), DatAdvantage can identify and report on folders where Global Groups are explicitly named in the ACL. A report showing the presence of global groups can be automatically sent to IT staff or compliance groups so that they can decide whether to remove global group ACLs. DatAdvantage also identifies those users who are currently accessing a data set through a global group, so that their access is not impeded by any remediation.

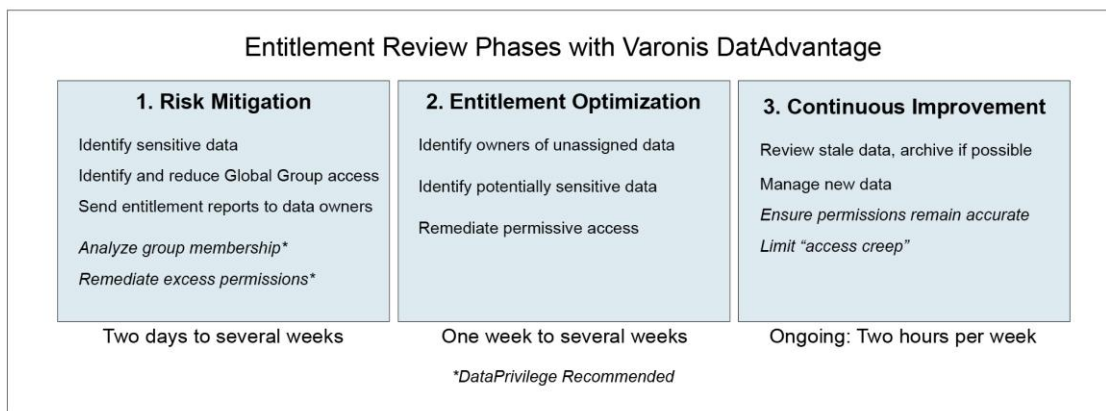
The Varonis DatAdvantage chart, right, highlights a situation in which data is overly accessible: Nearly 80% of the permissions to access data are "oversubscriptions" that should be revoked. This is a very common scenario for businesses, and DatAdvantage can help. DatAdvantage not only provides visibility, but it delivers the tools you need to resolve the situation without disrupting business.



A PROJECT PLAN FOR ENTITLEMENT REVIEWS

The remainder of this document presents a project plan for implementing an Entitlement Review process with DatAdvantage. Following the project plan will maximize the effectiveness of DatAdvantage in helping you with your Entitlement Reviews. The plan includes the following phases:

1. Risk Mitigation: Review and correct critical business data entitlements
2. Entitlement Optimization: Review and correct additional data entitlements
3. Continuous Improvement: Address stale data and maintain accurate entitlements



The Entitlement Review process using Varonis DatAdvantage – and, where appropriate, DataPrivilege – is shown graphically above. Each box represents one of the three phases in the process and includes the major steps to be completed in that phase. Timeframes on the bottom are examples, and will vary depending upon the overall volume of data and number of data owners in your organization.

The first phase of the plan will help you Review your sensitive business data first. As you do this, you'll learn the basic steps of reviewing and cleaning up entitlements for any data set:

- Identify the data set
- Identify the data owners
- Clean up excessive permissions due to Global Groups
- Data owner review of permissions
- Revoke remaining excess permissions

As you perform these steps, you'll see how DatAdvantage simplifies and automates much of the process. In the second phase, you will apply what you learned from first phase to additional unstructured data in your environment. Finally, in the third phase, you'll learn which processes you can put in place to ensure Entitlement Reviews are an ongoing and straightforward business practice

PHASE 1: RISK MITIGATION

Using DatAdvantage, you may want to target from four to six weeks to complete this phase. That will provide enough time for DatAdvantage to collect data usage information that will be helpful in Phase 2: Entitlement Optimization. Phase 1: Risk Mitigation consists of the following steps:

1. Identify sensitive data
2. Identify and limit global group access
3. Send entitlement reports to data owners
4. Analyze group membership
5. Remediate excess permissions

1. Identify Sensitive Data

We are going to begin our Entitlement Review by focusing on the most sensitive unstructured data in your organization. You may already know which data sets are the most sensitive because you've been tasked to help protect them. For many organizations, this is data belonging to regulated or other key business functions such as Finance, Human Resources, Legal, Research & Development, etc. As part of the Entitlement Review, you will want to keep a list of this sensitive data, as well as some details about it. It is a good idea to keep track of this information in a spreadsheet or some other organized form so that you can refer to it. If you do not already have a list, you can use the spreadsheet named "Entitlement Review Worksheet" that accompanies this document as a starting point.

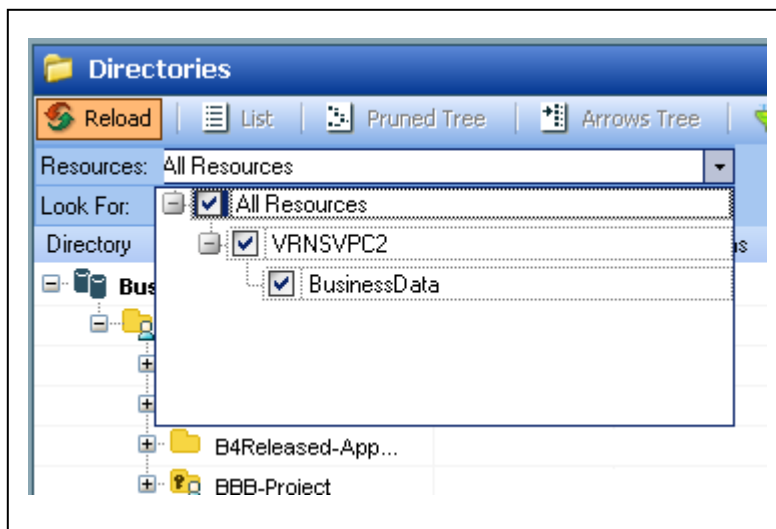
In Phase 1: Risk Mitigation, we are going to focus on data which you know is sensitive and for which you already know the owner – because you've already been tasked with protecting it. In Phase 2: Entitlement Optimization, we will show you how to identify data owners and additional data which may also be sensitive.

If you are not explicitly aware of what data is sensitive in your organization, you will need to work with the Business or Functional units in your company to identify their sensitive data.

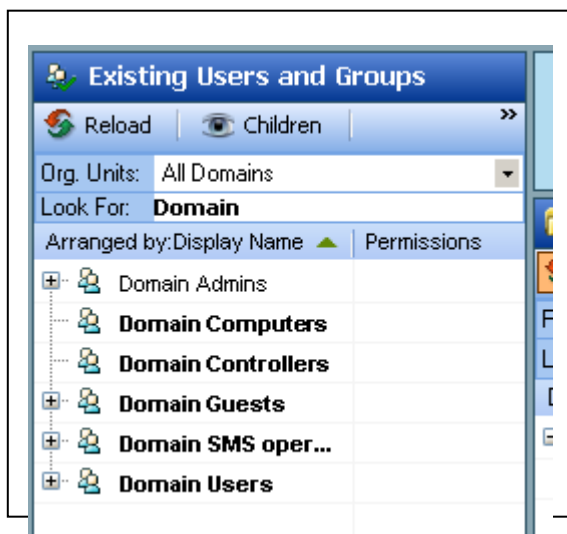
2. Identify and Limit Global Group Access

It's important to understand and limit which data in your organization is accessible by Global Groups (e.g., Everyone, Domain Users, Users, Authenticated users, Domain Guests, Guests). Using these groups to set permissions can lead to access that is too liberal because membership in these groups generally does not align to business data access needs. This step in the Entitlement Review process identifies which Global Groups have access to your sensitive data and helps you limit that.

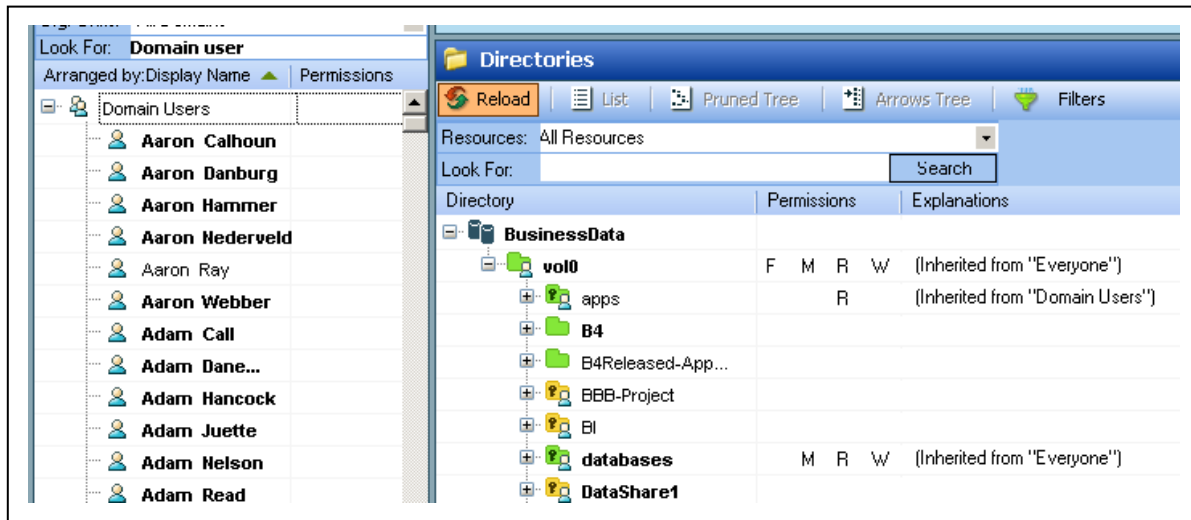
We'll begin by using the Work Area of DatAdvantage. In the Work Area, make sure that the servers with sensitive data are active resources, as illustrated in the following screen capture.



Next, in the Users and Groups pane, type in the first few letters of one of the Global Groups (e.g., "Domain" in the example below) so that the Group name appears.



Now, double click on the specified group, and any folders where the Global Group has access will turn green. This indicates that the Global Group has access to these folders. In the example below, you can see where the "Domain Users" have access.



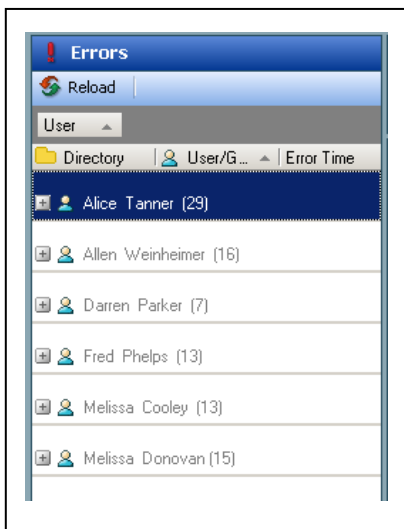
Now that you know where the Global Group has access, you can target those green folders with sensitive data, and revoke access for this Group.

If you discovered any global groups with access to sensitive data, you can now model what would happen if you revoked their access to this data, and you can do so without impacting your production environment. The Varonis DatAdvantage "what-if" sandbox environment lets you model changes before implementing them on your servers. Simply revoke access by this group, but do not commit the changes to your production environment.

Over a brief modeling period (we recommend six weeks), if any user accesses this data via their Global Group permissions, they will show up in the Errors pane, as well as in the Global Access Analysis report which displays the effects of permission removal on Global Access groups.

Removing Global Group Access without DatAdvantage

Removing Global Group access by simply deleting the Groups from folder ACLs can seriously hamper legitimate use. DatAdvantage delivers the groundbreaking ability to model these types of entitlement changes before making them in your production environment. This reveals which users of the Group actually need access, and let's you make the necessary entitlement changes without disrupting workflows.



If you have been running DatAdvantage in your environment for a long enough period (again, typically six weeks), you can look at the Errors pane or Global Access Analysis report now and immediately see the impact of removing the Global Group's access to the sensitive data. The access errors in the report and Error pane are based on modeling entitlement changes against historical access patterns. In the Errors pane at right, we can see six users whose access has been blocked because Global Group access was removed from a particular data set.

NOTE: Some organizations may wish to skip the modeling process for some data sets, and eliminate Global Group access immediately. This is a reasonable approach if you can identify users that should have access to the given data set with reasonable certainty. However, for data sets whose users cannot be easily identified, you will run the risk of cutting off warranted access.

You should now repeat the above process with all of the Global Groups for which you would like to reduce access.

3. Send Entitlement Reports to Data Owners

In this step, you should schedule reports for each owner of sensitive data (for instructions on scheduling reports, see the DatAdvantage User Guide). Two reports should be sent to data owners on a regularly scheduled basis: the "User or Group Permissions on Directory" report and the "Group Members" report. The first displays a list of groups and users with explicitly named access to the specified directories and files. Here is an example of the "User or Group Permissions on Directory" report for the "finance" folder.

User/Group Permissions On Directory

ACCESS PATH	DIRECTORY /FILE	DOMAIN NAME	OU NAME	USER/GROUP NAME	SAM ACCOUNT NAME	TYPE	RECOMMENDED SETTINGS
/vol/vol0/finance	Directory	VRNSDEMO	Users	Domain Admins	Domain Admins	Group	Unchanged
/vol/vol0/finance	Directory	VRNSDEMO	2. Distribution Group	Group:Finance	GroupFinance	Group	Unchanged
/vol/vol0/finance	Directory	VRNSDEMO	Group	sec:IT-System	sec_IT-System	Group	Unchanged

The second report lists members of the groups contained in the first report. In this example, we see a report for group "Finance", which has access to the "finance" folder. In addition to reporting on the current permissions, both reports contain DatAdvantage Recommendations on users whose permissions can be safely revoked without affecting their day-to-day activity.

Group Members

GROUP NAME	MEMBER NAME	SAM ACCOUNT NAME	RECOMMENDED SETTINGS
VRNSDEMO/Group:Finance	VRNSDEMO/Michael Federle	Michael Federle	Unchanged
VRNSDEMO/Group:Finance	VRNSDEMO/Marc Farhart	Marc Farhart	Removed
VRNSDEMO/Group:Finance	VRNSDEMO/Erin Manning	Erin Manning	Unchanged
VRNSDEMO/Group:Finance	VRNSDEMO/Andrew Carlisle	Andrew Carlisle	Unchanged
VRNSDEMO/Group:Finance	VRNSDEMO/Eric Adler	Eric Adler	Removed

You should now schedule reports for each data owner so that they can review the users and groups that have access to their sensitive data.

4. Analyze Membership

During their initial reviews of the reports you scheduled in the previous step, data owners should analyze the permissions and highlight changes they wish to make, recommendations they wish to follow, etc. Many organizations have a requirement that a data owner physically sign these documents; to accomplish this, data owners can simply print out the reports, make changes with a pen, sign them, and then hand them back to the IT department.

NOTE: If your organization requires a detailed audit trail for Entitlement Reviews and changes, you should consider using Varonis DataPrivilege (see sidebar on Page XX, in the Phase 3: Continuous Improvement). Entitlement provisioning with DataPrivilege includes an authorization audit trail and reporting.

5. Remediate excess permissions

After data owners return the edited reports to you, you can use DatAdvantage to implement the permissions changes via DatAdvantage. All changes are logged for future reference in the DatAdvantage "Entity History" area.

NOTE: To simplify your Entitlement Review process, you may want to consider the following best practice which is employed by many DatAdvantage users:

If a data owner does not over-rule a DatAdvantage Recommendation within a set period of time, IT should commit the change in DatAdvantage.

For example, the entitlement reports from step 3 are scheduled to be sent to data owners once a month. If a data owner does not contact IT to “over-rule” a DatAdvantage Recommendation within one week, IT will implement the Recommendation through the DatAdvantage commit engine.

PHASE 2: ENTITLEMENT OPTIMIZATION

In Phase 1: Risk Mitigation, we performed an Entitlement Review for data your organization already designated as “sensitive”. In Phase 2: Entitlement Optimization, we will look at the other unstructured data in your environment. Assuming most of your data falls into this category, you will be spending more time in this Phase. However, if you spent several weeks conducting Phase 1: Risk Mitigation, you will be able to benefit in this phase from the analysis DatAdvantage has been performing, and this will help accelerate this phase for you. DatAdvantage collects data usage events and calculates usage statistics over time, watching which users access what data, and how, as well as how users’ access patterns relate to those of other users. This analysis will make it easier for you to identify data owners for this second phase of the Entitlement Review process.

This second phase consists of the following steps:

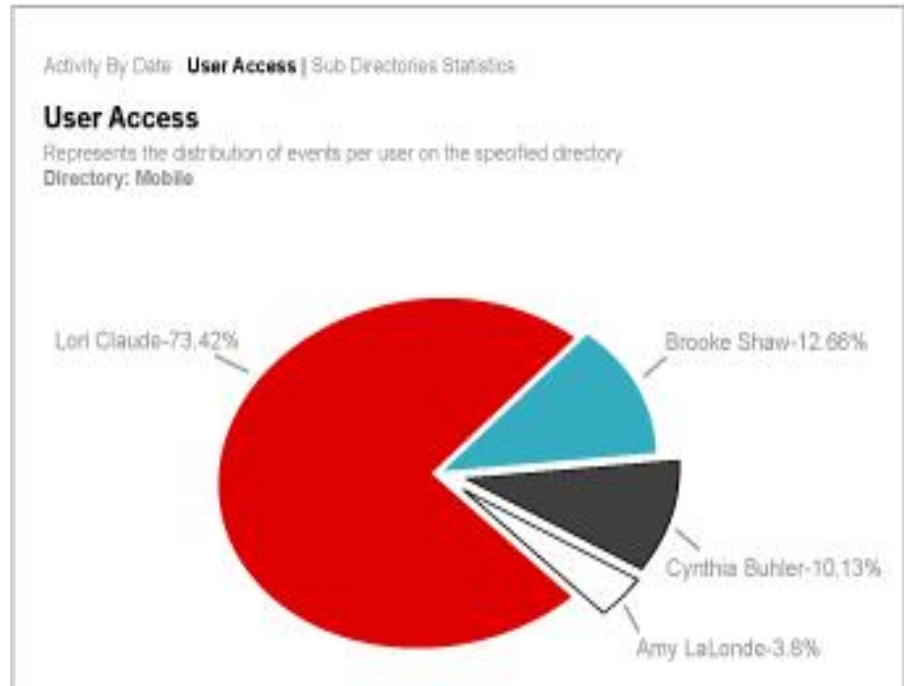
1. Identify owners of unassigned data
2. Identify potentially sensitive data
3. Remediate permissive access

1. Identify Owners of Unassigned Data

Most organizations have data sets for which owners have not been identified. After DatAdvantage has been running for just a few weeks, owner identification becomes a simple process. You can just double click on a folder in the Statistics Area of DatAdvantage, select “User Access” and look through the names that appear in the pie chart.

This is the list of names of the most active users of the data—and the data owner may very well be in this list. In the example to the right, “Lori Claude” appears to be either the data owner of the “Mobile” directory, or she is someone who may be able to tell us who the owner is.

Alternatively, you can identify the groups that the active users belong to with the “Parents” button in the Users and Groups pane. If one of the groups’ names turns out to be the name of a group within your company, then the data may belong to that organizational group, and the head of that group may be the data owner. In the example above, we can see which groups “Lori” belongs to, indicating potential data owners, if “Lori” herself is not the owner.



2. Identify potentially sensitive data

DatAdvantage helps you identify data that is potentially sensitive. In the Statistics Area of DatAdvantage, you can double click on a group of users in the Users and Groups pane, and all the directories that group collectively accesses will appear. You can apply this technique to identify sensitive data by using the names of data owners from Phase 1: Risk Mitigation, as well as key groups such as “finance”, “legal”, etc. These folders accessed by these users and groups are also candidates for adding to their sphere of ownership.

For example, double-click on the finance group. All folders that any member of the group has accessed will appear. You can then present a list of folders to the head of Finance, and say, “This data appears to belong to your group—do you agree?” If so, you can add this folder to the list of folders being managed by the Finance group.

In the example below, the group “DOK-DM” has been using data in the folder “Market”, making them candidates as owners.

Directories Accessed
Represents the number of events by the specified user on a directory (click a directory to view events for its subdirectory)
Group: Group:Dok-DM

Parent Directory: \\vol\vol0\Market

Directory	Events
apps - 1	In Sub Directories 0
Meetings - 0	In Sub Directories 2
Archive - 0	In Sub Directories 2
Dev - 0	In Sub Directories 4
Sales Tools - 0	In Sub Directories 8
Customer Program Management - 9	In Sub Directories 9
DOK Flash & Controllers - 20	In Sub Directories 0
Engineering - 0	In Sub Directories 48

3.

entitlement to this data:

1. Send entitlement reports to data owners
2. Analyze membership
3. Remediate excess permissions

PHASE 3: CONTINUOUS IMPROVEMENT

The third major phase of conducting your Entitlement Review involves establishing ongoing processes to address stale data and help you tackle other entitlement changes in your environment. Specifically, this phase includes:

1. Reviewing stale data, and archiving if possible
2. Managing new data
3. Ensuring permissions remain accurate
4. Limiting “access creep”

1. Reviewing Stale Data

DatAdvantage identifies directories that are no longer in use. Schedule the “Inactive Directories” report to run periodically, for example monthly. This report will help you identify data that has not been accessed for a given time period. If possible, restrict access to this data or archive it. Archiving this data will help reduce the risk of misuse or theft, and will also reduce storage costs.

2. Managing new data sets

As new data stores and hierarchies are created, you will need to include these in your Entitlement Review process. When a file server is added, or a business owner creates a new directory structure, you will need to identify data owners and review permissions.

3. Ensuring permissions remain accurate.

The steps for maintaining proper entitlements using DatAdvantage are presented below. Before we detail those, it is worth noting that the easiest ways to maintain data access entitlements is to connect the data users in your organization with the data owners directly. Varonis DataPrivilege is a solution that was created to do exactly that. It streamlines this portion of the Entitlement Review process and enables you, as an IT manager, to spend less time ensuring permissions remain accurate.

DataPrivilege – described in greater detail in the sidebar to the right – brings together data owners and users in a forum for communicating, authorizing and activating entitlements. This helps data owners by allowing them to control exactly who has access to their data, and under what conditions. It helps data users by accelerating the time it takes to get access to the data they need to do their jobs. And, it helps IT staff by freeing up more of their time to focus on other tasks. IT managers can still monitor and report on entitlement provisioning with DataPrivilege because it includes an authorization audit trail and reporting.

About Varonis DataPrivilege

Varonis DataPrivilege allows data owners to manage the authorization process themselves, without requiring IT staff to broker data access requests.

Users fill out a simple DataPrivilege web form to request access to a particular data set. The form includes fields to specify the type of access desired (read, modify, etc), an explanation for the request, and an optional field with an expiration date.

Data owners and their designated authorizers then receive these requests via email notification. They can choose to grant or deny the request, modify the type of access, and supply an expiration date. If the request is granted, DataPrivilege automatically makes the required changes to the appropriate ACL or group to grant permissions, and enforces revocation at the expiration date.

Varonis DataPrivilege captures information about each request and response, building an audit trail from which reports can be generated.

By using DataPrivilege, entitlement reviews become embedded into an organization's daily workflow, becoming an end-to-end entitlement process.

To use DatAdvantage to help maintain permissions, you will need to spend time reviewing and acting on the data provided by DatAdvantage and the reports to which you have subscribed. Depending on your environment, you will need to spend time weekly or daily working with this information.

You should first commit entitlement changes based on data owner reviews and DatAdvantage Recommendations. For those Recommendations that have been approved, you can simply right click on the Recommendation in the "Recommended Users and Groups" pane and select "Commit..." from the menu, as illustrated in the menu to the right.

Once you select "Commit...", simply follow the dialog boxes that appear to commit the changes to your production environment.

You can also use DatAdvantage to make changes beyond the DatAdvantage Recommendations, such as permissions revocations or additions specified by data owners. To do this, simply right click on the user, group or folder to be modified and select the desired operation.

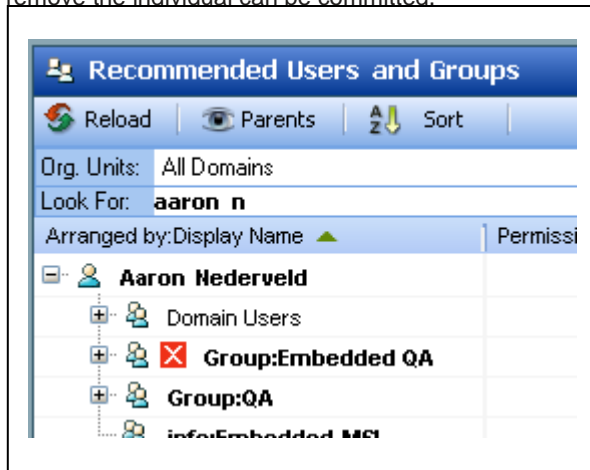


After committing entitlement changes, you should identify and clean up Global Groups that appear in ACLs. Schedule an "Explicit Permissions for User or Group" report to run weekly or monthly. This will detail folders where each Global Group has access, and the companion "Global Access Analysis" report displays the effects of permission removal on Global Access groups. Or, you can use the work area to quickly spot these folders after double clicking on a Global Group in the Existing Users and Groups pane. The same steps listed in Phase 1: Risk Mitigation, step 2 may be followed here.

4. Limiting "access creep"

Limiting access creep is another step where DataPrivilege can help, ensuring that data owners play a direct role in assigning and managing data access entitlements.

For organizations not using DataPrivilege, IT managers should review DatAdvantage Recommendations for users when a request is made to add a user to a group, or to add a user to an ACL. In the DatAdvantage Work Area, type the user's display name into the Recommended Users and Groups pane. Make sure the Parents button is showing (click the "Children" button to switch if necessary), and then click on the user to examine the groups of which that user is a member. You'll be able to see which groups are no longer used by this user, as indicated by the red X's (see the screen capture below). You should then review these groups with the user's manager to determine if the Varonis Recommendations to remove the individual can be committed.



CONCLUSION

Conducting Entitlement Reviews without DatAdvantage is a time consuming, error prone, and mostly manual process. This is compounded by the fact that many organizations cannot identify the true business owners for their data. Varonis DatAdvantage dramatically streamlines the Entitlement Review process by automatically and continually updating entitlement information, and providing visibility into data ownership. This not only simplifies the Entitlement Review process, but ensures it's up to date, accurate and has the desired business impact.

Following the Entitlement Review process outlined in this document allows organizations with DatAdvantage to operationalize Entitlement Reviews and ensure access to their unstructured data is based on business needs.

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.

WORLDWIDE HEADQUARTERS

1250 Broadway, 31st Floor
New York, NY 10001
Phone: 877-292-8767
sales@varonis.com

EUROPE, MIDDLE EAST AND AFRICA

55 Old Broad Street
London, United Kingdom EC2M 1RX
Phone: +44(0)20 3402 6044
sales-europe@varonis.com