

USE CASE EXAMPLE FOR DATADVANTAGE FOR WINDOWS

Fixing Permissions

You can use DatAdvantage to fix permissions by working with data owners for strategic input, and by using the DatAdvantage modeling environment to test changes before implementing them in the production environment. You can provide data owners with information about who has access to their data so that they can review that intelligence and verify who has a legitimate business need for access. DatAdvantage reports will show data owners who has access to their data, who is actually accessing the data, where sensitive data is located, and whose access should be revoked. These reports can be generated on an ad-hoc basis or scheduled so that they are delivered to data owners regularly.

The Varonis modeling environment provides the ability to back-test and changes against the historical access record. For example, to reduce access to a data, you may want to create a new group of users that represents a subset of those who have access today. You can test that plan by making the change within the DatAdvantage simulation environment and then testing it against historical access patterns. If no errors emerge (e.g., users with actual access needs who would have been blocked) you can feel confident with your change and implement it in the production environment. Alternatively, you allow the change to remain in the simulation environment as new access events are collected, which will ensure the changes perform as desired against current access patterns.

Auditing

Varonis DatAdvantage can help you demonstrate to auditors that access to your unstructured data is properly controlled. You can use DatAdvantage to verify and report on who has potential access as well as who is actually accessing your data.

Potential Access

If you need to know which users and groups have access to a folder, you can simply double click on the folder in the DatAdvantage user interface and the users and groups with access to the folder are displayed along with corresponding permission levels. This information can also be generated via a DatAdvantage report, which can be delivered via email, posted to a server, etc.

Alternatively, if you need to identify which data a specific user or group can access, simply double click on the name of the user or group in the DatAdvantage user interface and all the folders and files accessible to them are highlighted, and their level of access (e.g., full, read, write, etc.) is shown, as is the source of access permission. You can instantly see whether those permissions are inherited or assigned directly. This information can also be generated via a report.

Actual Access

In addition to providing insight into potential access, Varonis DatAdvantage provides a detailed audit trail of each and every actual data access (i.e., create, open, write, delete, rename and permissions changes). Permission change details can be helpful for both auditing and for performing a “roll back” to a previous state.

All access events can be searched and sorted to pinpoint exactly who accessed a file on any monitored server, and when. Again, all of this information is available directly and interactively in the user interface and via reports.

Identify Data Owners

Varonis DatAdvantage for Windows identifies data owners and data users for unstructured Windows and NAS data. DatAdvantage shows a sorted ranking of the data users. Those users who most frequently access the data are typically the data owners or, as the chief consumers of the data, can quickly identify the data owners. Armed with the names of these people, administrators can quickly establish the business context and value of the data, and craft appropriate data protection policies. DatAdvantage for Windows does this through comprehensive data access auditing that has no performance impact on Windows file servers or NAS devices