

## USE CASE EXAMPLE FOR DATADVANTAGE FOR UNIX/LINUX

### *Identify Data Owners*

Varonis DatAdvantage for UNIX/Linux identifies data owners and data users for unstructured UNIX and Linux data. DatAdvantage for UNIX/Linux 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 UNIX/Linux does this through comprehensive data access auditing that has no performance impact on UNIX or Linux servers.

### *Auditing*

Varonis DatAdvantage for UNIX/Linux validates for auditors that access to your unstructured data is properly controlled. Use DatAdvantage for UNIX/Linux to verify and report on who has potential access as well as who is actually accessing your data.

DatAdvantage for UNIX/Linux shows all users and groups with access to a directory along with corresponding permission levels. You can also identify what data a user or group can access. This mapping between users and data is available in the DatAdvantage for UNIX/Linux user interface and via a reports.

In addition to providing insight into potential access, Varonis DatAdvantage for UNIX/Linux provides a detailed audit trail of each and every actual data access (i.e., create, open, write, delete, rename and permissions changes) by every user – all without impacting performance. All access events can be searched and sorted to pinpoint exactly who accessed a file on any monitored server, and when.

### *Fixing Permissions*

You can use DatAdvantage for UNIX/Linux to fix permissions by working with data owners for strategic input, and by using the DatAdvantage for UNIX/Linux 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 for UNIX/Linux 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 DatAdvantage for UNIX/Linux 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 for UNIX/Linux 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.