Conducting file system access reviews using OpenText Identity Governance and OpenText File Reporter

Now OpenText Identity Governance lets you conduct access reviews and certifications on the sensitive unstructured data located on your network

At a glance

- OpenText File Reporter translates complex file system permissions into the OpenText Identity Governance permissions model.
- OpenText File Reporter permission scans are imported into the OpenText Identity Governance database for access reviews.
- Enables access reviews and certifications for specified network file system locations.
- Line-of-business manager can keep or remove access permissions in the OpenText Identity Governance interface.

Overview

Organizations storing sensitive personal data in application databases rely on OpenText™ Identity Governance to meet regulatory compliance through access reviews. Access reviews certify that authorized users have the correct access permissions and that unauthorized users do not have access. With regulations requiring the proper management of personally identifiable information (PII), potentially exorbitant fines can be a result of noncompliance.

These same organizations also store sensitive data in their network file systems and this data needs to be protected from unauthorized access as well. Yes, it could be files with PII, but it can also be legal documents, sales forecasts, financial information, and other strategic information.

And while unauthorized access might not necessarily result in fines, it can be devastating to the competitive viability of the organization.

OpenText Identity Governance and OpenText File Reporter work as an integrated solution for enabling you to conduct access reviews and certifications for network folders and shares storing sensitive unstructured data.

Target paths

Specifying the network file system locations for access review are done in OpenText File Reporter. You create a “target path” for each of the network locations that are to be reviewed.

Creating a target path such as *WNDWSSERV\ Departments\Finance*, for example, would enable a manager within OpenText Identity Governance to conduct an access review on the Finance network folder and all subfolders in that target path.

Target paths can be categorized so that each can be easily identified in OpenText Identity Governance. In the above example, a category assigned as Finance would be applicable. Each saved target path will be displayed in the OpenText Identity Governance interface as an individual review definition for access review.

Permissions scans and translations

As part of its reporting capabilities, OpenText File Reporter performs scans of the network file system. One of these types of scans is a permissions scan where OpenText File Reporter identifies the NTFS permissions that users are assigned to network folders storing sensitive and high-value data. NTFS permissions are complex, with an extensive set of permissions enabling the reading, writing, and management of data within the network folder.

To simplify complex NTFS permissions to permissions that a line-of-business manager conducting an access review can understand, File Reporter performs an “abstraction process” where it translates the NTFS permissions to corresponding generic file system access rights—specifically, Read, Write, and Change Permissions. These permissions are the same as those used in an application access review in OpenText Identity Governance, so that they will be familiar to the line-of-business manager conducting the access review.

If you prefer, you can have the abstraction process take place automatically when the permission scan is conducted. This makes it so that you can conduct an access review directly after a permissions scan.

Configuration and transmission

There is a minimal amount of initial configuration work in OpenText Identity Governance before you can conduct access reviews on the target paths. Once completed, you can transmit the scanned abstracted permissions from the OpenText File Reporter SQL database to the OpenText Identity Governance SQL database via the provided JavaScript Object Notation (JSON) collector in OpenText File Reporter.

OpenText Identity Governance and OpenText File Reporter work as an integrated solution for enabling you to conduct access reviews and certifications for network folders and shares storing sensitive unstructured data.

Conducting access reviews

Once the permission scans have been transmitted to the OpenText Identity Governance SQL database, the target paths are available for a designated user to conduct an access review. The ability to conduct access reviews are based on the identity and role of the user who has logged into OpenText Identity Governance. In other words, only authorized users such as an application owner or manager will be able to conduct access reviews for a specific target path.

Access reviews on target paths can be conducted using all of the capabilities of OpenText Identity Governance. For example, an access review can display access through display options such as “Group by user,” “Group by permission,” etc. Additionally, the manager or application owner conducting the access review can maintain or restrict access through the familiar “Keep” and “Remove” buttons.

Conclusion

Data needing protection from unauthorized access is not just the structured data storing PII in an application’s database, it’s also the financial, legal, sales, marketing, and other strategic data that distinguishes your organization competitively. OpenText Identity Governance, integrated with OpenText File Reporter, provides the ability to perform access reviews on network locations storing sensitive and high-value unstructured data, keep or remove access, and provide attestation that only authorized users have access to this sensitive and high-value data.

opentext™