Flyer
Security

Extending the Value of Your Identity Management System with File Dynamics

Your identity management system is invaluable. It helps to ensure regulatory compliance and appropriate application access, provide identity-based account provisioning, and promote complete account lifecycle management. And with the addition of Micro Focus® File Dynamics, it can do even more!

File Dynamics at a Glance:

- **Manages lifecycle of data based on identity and role:**
  As user or group accounts are created through your identity management system, File Dynamics simultaneously provisions the associated user and group storage areas.
- **Assigns proper access to network storage:**
  As your identity management system creates a new user or group, File Dynamics assigns or restricts access permissions to group or user storage.
- **Helps meet compliance objectives:**
  Security policies secure sensitive data through alerts and restrictions.

Identity Management Systems

You deployed your identity management system with the objective of ensuring that only authenticated users have access to the specific applications, systems, or IT environments to which they are authorized. The system provides automated control over user provisioning and the process of onboarding new users such as employees, partners, clients, and other stakeholders. Additional controls include the process of authorizing system permissions for existing users and the offboarding of users who are no longer authorized to access the organization's systems.

In short, your identity management system is an amazing tool for automating the process of providing users the right access to applications and systems they need to perform their jobs. With all of its capabilities, it might be hard to imagine that your identity management system can do much more—but it can.

Sensitive Information in Structured and Unstructured Data

Your identity management system helps to ensure appropriate access to applications, which can in turn enable and restrict access to sensitive information stored in databases. Known as "structured data," these data are a primary source of personal identifiable information (PII), health records, account numbers, passwords, and other confidential information that, when accessed by unauthorized individuals, can have potentially devastating consequences.

An equally vulnerable, but historically less emphasized data set, is "unstructured data." Unstructured data are the file-based data—the word processing, spreadsheets, media, virtual images, and other files that make up more than 80 percent of an organization's stored data. And like structured data, unstructured data can also contain sensitive information that needs to be protected. In some cases, it could be PII exported from structured data sources. But it's not just about PII—unstructured data can be the "crown jewels" of a company's data. Excel files might contain profit and loss data, Word files might include legal information, and PowerPoint files might include sales forecasts.

Automating Unstructured Data Management

File Dynamics is the means of extending the provisioning and access management capabilities of your identity management system from structured data to unstructured data. Through policies that you establish in File Dynamics, your identity management system can now automate the management and secure access of unstructured data located on your enterprise network.

In other words, as your identity management system automatically grants access to applications and systems based on identity and role, through File Dynamics, your identity management system can simultaneously provision group, project, or user network storage as well as establish or restrict access to network

With File Dynamics, you can extend the capabilities of your identity management system to oversee identity-based access management to include unstructured data.

Contact us at:
www.microfocus.com

Like what you read? Share it.

folders storing sensitive data, also known as "high-value targets."

Below are just a few examples of the capabilities of File Dynamics. In many ways, you are limited only by your imagination.

Provisioning Network Storage

File Dynamics enables you to create policies that trigger actions when events take place in Active Directory (AD). These actions include provisioning new network storage locations. For example, if an organization initiated a new project through the identity management system, an administrator would initiate the approval and workflow process that would create a group and specify the group members. At the same time, File Dynamics could create a network storage area according to the size, location, structure, and permissions specified in the policy.

Additionally, network storage locations can be provisioned for users according to their identity and role—with size, location, structure, permissions, and other settings based on the policy specifications.

Securing Access to Sensitive Data

File Dynamics can also automate the provisioning and governance of sensitive data tied to workflow and approval processes within your identity management system.

For example, an organization might need to provision folders for storing sensitive data for their customers. A request for a new folder that includes the customer name and user access requirements would be submitted for approval. The identity management system would then create two groups: one needing Read access and one needing Write access. As these groups are created in AD, File Dynamics can provision the new folder, assign permissions for each group, set the ownership, and establish a standardized folder structure.

To further assure that sensitive data is protected from unauthorized access, File Dynamics enables you to establish various security policies that secure data through alerts and restrictions. Security Notification policies notify you when access permissions on a high-value target have been changed. Lockdown policies prevent access permissions on a high-value target from being modified. And Fencing policies limit access for high-value targets to only authorized users and roles.