opentext™ | Cybersecurity

White Paper

File Dynamics and the Expanding Requirements of Data Management

An expanded emphasis on data growth, automation, compliance, security, and protection are all contributing to an evolving definition of network data management. To meet the dynamic demands of today's organizations, OpenText offers File Dynamics—an Identity- and Target-Driven policy approach to today's network data management challenges. With File Dynamics, you have the means to not only automatically provision, manage, and dispose of user and group storage, but to secure it from unauthorized access, and protect it from data loss or corruption from a ransomware attack.

Table of Contents

Introduction

"Data really powers everything we do.[1] It has been called the "raw material[2]" of business. That is why proper data management is so important. But the term "data management" is one that is continuously evolving.

Today, a variety of factors, including the overwhelming growth of data, compliance to data-specific industry and government regulations, the ramifications of unauthorized access to sensitive data, and the increasing incidents and sophistication of malware are causing organizations to make data management a bigger focus of their activities.

This greater emphasis on data management, along with its continued evolution, is the catalyst for the expanded data management services offered by NetIQ products by OpenText™. For example, the product that was once known as Storage Manager for Active Directory has now been renamed to File Dynamics to reflect the expanded data management services available in the product today—with even more data management services coming in the future.

Perhaps no area of data management has received more recent attention than data security. This includes threats both inside and outside the firewall, ranging from unauthorized access to files, to files corrupted through a ransomware attack.

Detailing Data Management Problems

Chances are, your organization has struggled with one or more of the following data management challenges:

- Automating data management tasks
- Enacting data management processing
- Data lifecycle management (also known as "data curation")
- Securing sensitive data from unauthorized access
- Protecting data from ransomware and other malware
- Quickly restoring backed up data

These tasks, along with many others—when performed manually or without adequate software tools—can quickly burden the resources of an IT department and prevent personnel from focusing on larger projects.

There are monetary costs for performing tasks manually that can add up to significant expenditures over time. An IDC report, for example, noted the findings from a 100,000+ combined student and faculty school district in Texas: "With students changing grades and often even schools every year, with students entering the school district and graduating, and with the movement of staff and faculty, the district ascertained that they were spending $5 to set up a new user and $2 per each change applied to the system.[3]"

Perhaps no area of data management, though, has received more recent attention than data security. This includes threats both inside and outside the firewall, ranging from unauthorized access to files to files corrupted through a ransomware attack.

1. Jeff Weiner, Chief Executive Officer, LinkedIn
2. Craig Mundie, Senior Advisor to the CEO, Microsoft
3. IDC, Novell Delivers a New Way of Intelligently Managing Organizations' File-Based information, #216013, Noemi Greyzdorf, January 2009

According to a 2021 report from the Herjavec Group, “In 2021, the average cost of recovery and ransom associated with a ransomware attack has been 2 times more than the 2020 average global ransom demand.”[4]

Introducing File Dynamics

For the data management challenges identified above, along with many others, we developed OpenText™ File Dynamics. File Dynamics provides extensive services to address the expanding requirements of network data management. Identity-Driven policies automate tasks that are traditionally done manually, resulting in cost savings and assurance that tasks are being performed properly. Target-Driven policies offer data migration, cleanup, workload capabilities, security from unauthorized access, and protection from data corruption and downtime.

Today, the technology in File Dynamics manages the data of millions of users and groups in hundreds of accounts across all industries.

Today, the technology in File Dynamics manages the data of millions of users and groups in hundreds of accounts across all industries.

How File Dynamics Works

By establishing both Identity-Driven policies and Target-Driven policies, you define how your data is provisioned, managed, and cleaned up, as well as how it is secured, protected, and recovered.

Figure 1. File Dynamics manages network-stored data using both Identity-Driven and Target-Driven policies.

4. State of Ransomware 2021 Q1–Q2, Herjavec Group, June 8, 2021

Identity-Driven Policies

Identity-Driven policies affect user and group objects that make up the Microsoft network operating system's directory service—Active Directory. A User Home Folder policy or a Group Collaborative policy specifies the settings for managing network storage areas for user and group objects respectively in Active Directory. For example, you could create a User Home Folder policy that was associated with the Human Resources organizational unit of your Active Directory forest. The settings within that policy would then apply to all user objects that reside in that organizational unit.

The settings within an Identity-Driven policy specify how user and group data is provisioned, how common management tasks are conducted, and how it is cleaned up.

The settings within an Identity-Driven policy specify how user and group data is provisioned, how common management tasks are conducted, and how it is cleaned up.

PROVISIONING

When a new user is added to an organizational unit or group that has an associated policy, File Dynamics automatically provisions user storage and enables access to collaborative storage areas, according to the settings in the policy.

When a new user is created in an Active Directory organizational unit, File Dynamics provisions network storage for the user according to the specifications of the policy that pertains to that organizational unit.

Based on what you specify in the policy, File Dynamics will:

- Provision the network home folder in a specified location on the network
- Establish access (based on group membership) to collaborative storage areas
- Provision a profile path
- Provision Remote Desktop Services (RDS) storage and profile paths
- Include any role-specific files in the provisioned storage locations
- Set all access permissions to the new storage areas

COMMON USER AND GROUP MANAGEMENT TASKS

The settings within the policy are also the means of automating or enacting regular, day-to-day network file system management tasks that most organizations tend to do manually. Common user and group storage management tasks include the ability to learn, through reports, how your storage is currently being managed and to make any needed adjustments.

These tasks include:

- Establishing and adjusting user disk quotas
- Automatically renaming a user home folder when a user object is renamed
- Managing folder attributes
- Providing a set of reports pertaining to your network storage content
- Grooming user home folders by removing files that meet certain conditions

- Moving user data when a user object is moved to a new organizational unit in Active Directory
- Load balancing data across servers
- Moving and copying data across servers

CLEANUP

Gartner began sounding the alarm about exponential data growth and the justifiable deletion of much of an organization's "dark data" in 2014 when the research organization identified a new "File Analysis" market segment.

Since that time, many organizations have begun developing defensible deletion strategies. A defensible deletion strategy is a comprehensive approach by the organization to reduce the storage costs and legal risks associated with the retention of electronically stored information (ESI). It is designed to address legal requirements for data retention, while at the same time eliminating ESI that no longer has any business value.

File Dynamics and its ability to automatically archive or dispose of data can be the means of helping organizations meet their defensible deletion objectives. Through policies, you can establish a set of rules for cleaning up data once a user object has been removed or disabled from Active Directory. This can greatly reduce the "orphan" files and folders that take up valuable disk space on an organization's servers.

File Dynamics and its ability to automatically archive or dispose of data, can be the means of helping organizations meet their defensible deletion objectives. Through policies, you can establish a set of rules for cleaning up data once a user object has been removed or disabled from Active Directory.

The aforementioned grooming capability can archive or delete files according to file extension, size, or when last accessed.

Storage cleanup includes disabling user access to files when a user becomes inactive in Active Directory and then either archiving or deleting the user's files.

Cleanup tasks include:

- Disabling network storage access when a user's account is disabled in Active Directory
- Archiving user home folder content
- Deleting storage

Target-Driven Policies

Target-Driven policies are associated directly with a network folder or share. Target-Driven polices provide unique management capabilities that are not offered with Identity-Driven policies. For example, the ability to move data from a network folder that is not a user or group folder, such as an application folder.

Target-Driven policies include the following:

- Data Location policies
- Content Control policies
- Security Notification policies

- Lockdown policies
- Fencing policies
- Workload policies
- Epoch Data Protection policies

DATA LOCATION POLICIES

These policies are the means of copying folders and their contents to a target folder. There is an option to remove the files from the source location after they have been copied. For example, if you were doing a server consolidation or moving data from a server to a NAS device (or vice versa), you could easily do so using Data Location policies.

CONTENT CONTROL POLICIES

Similar to Identity-Driven file grooming, Target-Driven Content Control policies remove files according to file type, age, size, last accessed date, and more. From any file path, you can either vault files to a new location or delete the files altogether. For example, you could use this feature to easily delete temporary files and in the process, make much more disk space available on your storage devices.

SECURITY NOTIFICATION POLICIES

Security Notification policies enable administrators to be notified of any changes in access permissions to network folders. These changes in permissions include a user being given a new or updated permission to a specific folder, or a user being granted access permissions to a folder by being added to a group.

Access permission updates are determined by the Phoenix Agent through a scheduled scan. Notifications are sent to administrators via email.

LOCKDOWN POLICIES

Sensitive data should be accessible on a “need to know” basis, meaning that only a limited set of individuals, based on their roles, should have access to this sensitive data. Furthermore, data owners—those most familiar with the sensitivity of the data and who should have access to it—should be empowered to be the ultimate decision makers.

Once you have established the proper access permissions for a high-value target, you can establish the archetype of access permissions for the high-value target that will be strictly enforced through a Lockdown policy. When unauthorized access permission changes are made to the high-value target, the new permissions are removed and the original permissions are restored.

FENCING POLICIES

There might be some high-value targets on which you might not want to place the same level of restrictions as a Security Lockdown policy but might nevertheless want to secure the access to only authorized users or roles.

Sensitive data should be accessible on a “need to know” basis, meaning that only a limited set of individuals, based on their roles, should have access to this sensitive data. Furthermore, data owners—those most familiar with the sensitivity of the data and who should have access to it—should be empowered to be the ultimate decision makers.

Fencing policies in File Dynamics lets you set limits on how access permissions may change over time. Using a set of ALLOW/DENY statements to define a "fence," the policy specifies Active Directory containers, users, or groups that might conceivably be given permissions to a high-value target in the future without an issue or should never be given rights in the future, as in restrictions specified in GDPR.

WORKLOAD POLICIES

Workload policies in File Dynamics provide the ability to handle work processes initiated from other applications. For example, reports generated in NetIQ File Reporter that specify the location of sensitive files can be imported into the Data Owner Client where a designated data owner can remediate the location of these sensitive files. This approach empowers organizations to provide automated network file system security remediation approved by a gatekeeper familiar with the files.

Workload policies specify source paths, along with the data owners who can access these paths.

EPOCH DATA PROTECTION POLICIES

As organizations deal with the increasingly devastating effects of ransomware, they are looking to solutions that provide data continuity. Data continuity is a term that includes the measures taken to safeguard the integrity and availability of critical data so that when an event takes place that either corrupts the data or disables access to it, restorative remediation can take place quickly and with minimal disruption.

You might logically conclude that the organization's backup system would take care of this; however, the sophistication of recent ransomware attacks has many security experts recommending that you keep multiple backups[5] in various locations, with restrictive administrative and system access.[6] Moreover, restoring data from traditional backup systems can be time-consuming, because it often requires IT administrators to sort through the contents of an entire system backup.

In addition to safeguarding against ransomware attacks, there are other reasons why an organization would want to protect data through additional data continuity measures. These include:

- Protecting data from inadvertent corruption, loss, or deletion
- Restoring the data to how it existed at a particular point in time

Similarly, organizations might need to protect and recover the permissions of high-value targets, including:

- Lost or destroyed permissions
- Inadvertently changed permissions
- Permissions as they previously existed at a particular point in time

Epoch Data Protection policies allow customers to maintain nearline standby views of high-value target folders stored in the network file system. Data owners can view and access the archive of the high-value target as it existed at a selected point in time. In essence, it is a "time machine" for the data and associated permissions on the high-value targets.

Epoch Data Protection policies allow customers to maintain nearline standby views of high-value target folders stored in the network file system. Data owners can view and access the archive of the high-value target as it existed at a selected point in time. In essence, it is a "time machine" for the data and associated permissions on the high-value targets.

5. Will your backups protect you against ransomware?, Maria KorolovCSO Online, May 31, 2016
6. Ransomware Damage Report: 2017 Edition, Herjavec Group, May 24, 2017

archive of the high-value target as it existed at a selected point in time. In essence, it is a "time machine" for the data and associated permissions on the high-value targets.

Archived files are located in a "Collection" of "Epochs." An Epoch consists of the directory structure and associated metadata at a point in time. The Collection is stored in a nearline repository called a "File Store." Epochs are saved to the File Store through a proxy, with no direct user access to the Collection. This creates a quarantined repository on the network so that it cannot be compromised by users.

Recovering a file from the File Store is a multi-step process. Using the Data Owner Client, the data owner first opens an Epoch and can then see its contents, including the option of opening a "View" of an individual file. The View is not the actual file, but a complete rendering of the file. Upon determining which files to recover, the data owner then makes a recovery request for those files. The Data Owner Client authenticates to the Engine and the Engine then delegates the recovery to the Phoenix Agent, which recovers the files to either the location where the file existed previously or to a location of the data owner's choosing.

UNIQUE BENEFITS

When it comes to data continuity, the data protection offered in File Dynamics offers many enhancements in addition to vital backup systems.

First, the Epoch Data Protection interface is easy to use and administer. Using either a wizard or a console, you can locate a file you want to recover. Locating and selecting files is similar to locating files in the Windows Explorer interface. Administrators that have worked with the complex user interfaces of other backup systems will find the Epoch Data Protection interface very intuitive.

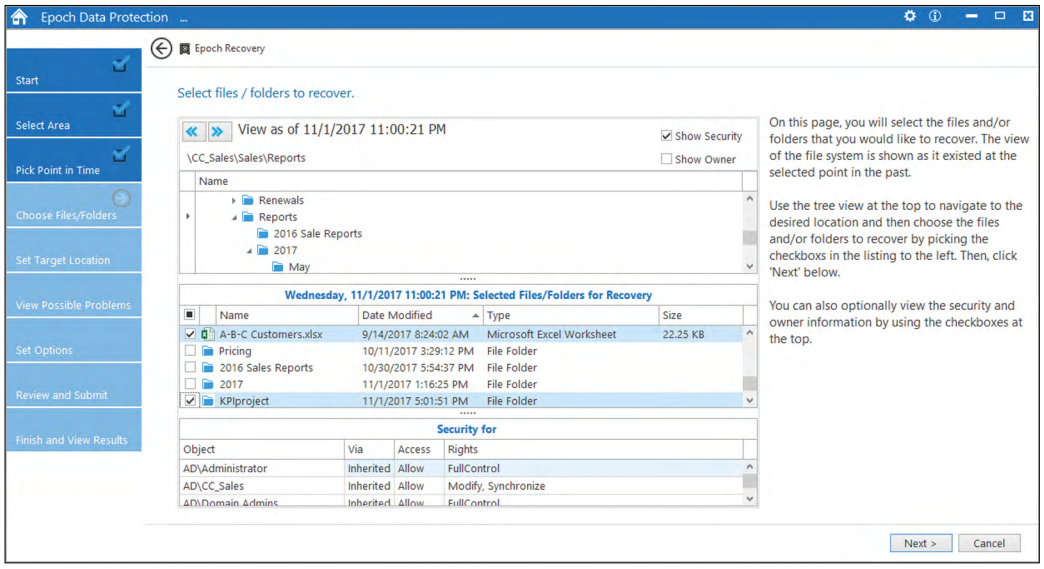

Figure 2. Epoch Protection Interface. In this example, a data owner is using a wizard to specify files for recovery.

Second, with File Dynamics you can designate specific data owners to be in charge of restoring data and permissions from high-value targets. This offloads the responsibility from overworked IT staff, and in the process enables a faster response and restoration time from the data owner—a critical factor in effective data continuity.

Third, Epoch Data Protection uses limited read/write access to backup locations—a remedy for diminishing the threat of ransomware. With restricted network access to the protected high-value targets, data and their permissions remain protected from ransomware and other malware threats.

Fourth, Epoch Data Protection enables you to back up high-value targets as frequently as you would like and permits the data owners to verify the integrity of the backups. According to the Software Engineering Institute at Carnegie Mellon University, "The single most effective deterrent to ransomware is to regularly back up and then verify your system."[7]

Fifth, the Epoch Data Protection repository is one more repository for your critical data. Security analysts recommend a multi-tier approach to provide more reliability with backups.[8]

Sixth, Epoch Data Protection policies archive files quickly, because only files that have been modified since the last saved Epoch are backed up. However, when you open the new (or any) saved Epoch, it will contain all of the archived files in the high-value target—not just the modified files.

Seventh, as you locate a file for recovery, you can view a complete rendering of the file to verify that the selected file is, indeed, the file you want to recover.

The File Dynamics Engine, in cooperation with the Agents, enact the Identity-Driven and Target-Driven policy actions.

Epoch Data Protection uses limited read/write access to backup locations—a remedy for diminishing the threat of ransomware. With restricted network access to the protected high-value targets, data and their permissions remain protected from ransomware and other malware threats.

Expanding Data Management Services

Data management requirements have changed dramatically since we introduced our first data management product—File System Factory—in 2003. Back then, the principal focus of the product was completing the account automation chain of identity management systems by automating the provisioning of network user storage locations in synchronization with the automated account provisioning provided by the identity management system. The product became an instant success—especially within organizations with a large number of user accounts.

Over time, the product name was changed to OpenText Storage Manager as capabilities were expanded to include features to solve other data management challenges—challenges that included addressing data growth, security, compliance requirements, data loss prevention, and more. And as data management continues to evolve and its requirements continue to expand, NetIQ is committed to continue to address those challenges.

7. Ransomware: Best Practices for Prevention and Response, Alexander Volynkin, Jose Morales, Angela Horneman, May 31, 2017
8. Will your backups protect you against ransomware? Maria KorolovCSO Online, May 31, 2016

With Identity-Driven policies providing automated user and collaborative data management, combined with Target-Driven policies that provide selected storage management and data protection, you have a data management system in File Dynamics that meets an extensive set of today's data management challenges.

And as data management requirements continue to evolve, so will File Dynamics. Development plans are now in place for even more Target-Driven management capabilities that will be introduced in future releases.

With Identity-Driven policies providing automated user and collaborative data management, combined with Target-Driven policies that provide selected storage management and data protection, you have a data management system in File Dynamics that meets an extensive set of today's data management challenges.

Conclusion

Identity- and Target-Driven policies in File Dynamics work together to manage an extensive set of data management tasks that will save you money, provide assurance that management tasks are being performed correctly, and give you confidence that files located on high-value targets are protected.

As network-stored data continues to grow, as regulations for data storage and access continue to become more stringent and complex, and as threats from malware continue to cause more and more devastation, the data management capabilities of File Dynamics are needed more than ever.

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.