File Dynamics

Automate network file system management tasks while securing your organization's most important files from unauthorized access or corruption from ransomware attacks through the power of policy-enacted data management. Identity-driven policies in NetIQ File Dynamics provision user and group storage, perform day-to-day management tasks, and clean up and dispose of storage content. Target-driven policies move files, clean up storage, and secure high-value targets, while providing data protection through secure nearline backup.

Product Overview

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, security, and assurance that tasks are being performed properly. Target-driven policies offer data migration and relocation, cleanup, security, and protection from data corruption and downtime through nearline storage backup of high-value targets, enabling quick recovery of files and their associated permissions.

Key Benefits

File Dynamics is engineered to alleviate the network file system management workload of administrators while helping them reach their regulatory compliance objectives. In so doing, File Dynamics offers the following benefits:

- **Lowers network data management costs.** File Dynamics lowers costs in a variety of ways:
  - First, it automates storage management tasks that are typically done manually. These include provisioning user and collaborative storage, setting rights, setting quota limits, migrating storage, redistributing storage, archiving storage, and cleaning up storage.
  - Second, through its ability to regularly clean up, archive and delete storage content, File Dynamics can lessen the need for deploying additional primary storage resources.
  - Third, by reducing the need for more storage resources, File Dynamics can provide resulting savings in power and cooling costs.
- **Addresses security compliance requirements.** Identity-driven policies enable you to establish role-specific access permissions so that only authorized users have access to certain files. In a security audit, for example, you can demonstrate that only members of the Human Resources department have access to confidential employee files.
- **Keeps Sensitive Data Secure.** A series of security-based Target-Driven policies let you protect high-value targets from unauthorized access. Notification policies notify you when access permissions have been updated. Fencing policies restrict access to certain users and groups, and Lockdown policies prevent new users from being granted access.
- **Data Protection.** Epoch Data Protection policies in File Dynamics allow you to maintain nearline archives of critical files located in high-value targets on your

Quick View

Engine Host
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Event Monitor Host
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

File System Agent Host
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Phoenix Agent Host
- Windows Server 2022
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Administrative Workstation Host
- Any platform where .NET 4.6.2 can run

network. If files on the network were to become corrupted or encrypted through a ransomware attack, designated data owners could quickly and easily recover protected, non-corrupted versions of the files from the last saved "Epoch" and replace the corrupted files.

- **Relocates data.** Workload policies provide the ability to import externally-generated files, such as security reports from NetIQ File Reporter, and then rectify the location of these files for optimization and regulatory compliance.

Key Features

- **User and collaborative storage management.** File Dynamics manages both user and collaborative storage. User storage includes a user home folder and any number of auxiliary storage folders. Collaborative storage can be a container or group storage folder where all members have access to the single folder, or a more organized folder where each user in the group is granted a personal folder within the container or group folder.
- **Policy-dictated actions.** Policies specify the data management actions to take as a result of an Active Directory event, selecting a Management Action option from the administrative interface, or a scheduled event. For example, a home folder policy applied to a particular organizational unit in Active Directory specifies how each user home folder is to be provisioned, including the folder's size, location, rights, attributes, unallowable file types, redistribution paths, vaulting paths, disposal procedures, and more.
- **Data security.** Multiple security policy types keep high-value targets secure through a number of automated actions including notifying data owners of changes in access permissions, specifying which users and groups can be granted access and those who cannot, along with locking down access to a specified set of users.
- **Data protection.** Epoch Data Protection policies are target-driven policies in File Dynamics that allow you to maintain nearline restricted access archives of high-value target folders stored in the network file system. Exclusive access permissions are limited to administrators known as data owners who can view and access the archive of the high-value target as it existed at a selected point in the past. In essence, it is a "time machine" for the data and associated permissions in the high-value targets. When necessary, data owners can quickly recover files that have become corrupted, such as through a ransomware attack.
- **Data migration and relocation.** File Dynamics automatically moves data in a number of ways:
  - When a user is moved from one Active Directory container to another.
  - Through a distribution setting in a policy.
  - By changing the target paths within a policy.
  - From an eDirectory to Active Directory environment or one Active Directory forest to another using the Cross-Empire Data Migration subsystem.
  - Through Workload policies where specific files can be moved from one location to another.