Top Ten Features of Epoch Data Protection Policies in File Dynamics

In addition to traditional backup systems and their vital role in today's data-centric organizations, implementing Epoch Data Protection policies in Micro Focus® File Dynamics allows organizations to maintain nearline protected archives of High-Value Target folders stored in the network file system. Security analysts recommend a multi-tier approach to provide more reliability with backups[1]. Epoch Data Protection policies in File Dynamics offer many unique features and benefits.

At many organizations, the assumption is that their backup system would be the logical means of restoring files corrupted in the event of a ransomware attack. However, the sophistication of recent attacks has many security experts recommending that you keep multiple backups[2] in various locations, with restrictive administrative and system access[3]. See how File Dynamics, with its Epoch Data Protection policies, addresses these recommendations in the features and benefits described below.

1. **Protects High-Value Targets.** Amid all of the potential petabytes of files on your network, some are absolutely vital and their loss or corruption would be catastrophic. Epoch Data Protection policies let you specify which network folders are "High-Value Targets" for archiving.

2. **Enables recovery of data after a ransomware attack.** Once you have deleted the ransomware culprit from your network, you can replace corrupted files from an Epoch. An Epoch is a representation of a High-Value Target's file system, permissions, and metadata at a point in time.

3. **Shortens data recovery times.** Rather than working with a busy and oftentimes short-handed IT staff, designated "data owners" can view an Epoch's contents and recover files. Locating files in an Epoch is much faster than doing so from a traditional backup system.

4. **Recovers data permissions.** Epochs not only include the files of a High-Value Target, but also the permissions, which a data owner can recover along with the files.

Along with safeguarding against ransomware attacks, there are other important reasons why an organization would want to protect their data through additional data archiving 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 existed at a particular point in time**

1 *Will your backups protect you against ransomware? Maria Korolov CSO Online, May 31, 2016*
2 *Ibid*
3 *Ransomware Damage Report: 2017 Edition, Herjavec Group, May 24, 2017*

"The single most effective deterrent to ransomware is to regularly back up and then verify your system."

ALEXANDER VOLYNKIN, JOSE MORALES, AND ANGELA HORNEMAN

Ransomware: Best Practices for Prevention and Response

May 31, 2017

Contact us at:
www.microfocus.com

5. **Archives data quickly.** Epoch Data Protection policies use an algorithm that archives High-Value Targets very quickly. The algorithm also determines which files have been modified since the last saved Epoch and only archives those modified files. Each saved Epoch, however, contains all files in the High-Value Target—not just the modified files.

6. **Easily check the integrity of archived data.** From the Data Owner Client, a data owner can quickly check the integrity of archived files in an Epoch at any time—something that is much more difficult to do using a traditional backup system.

7. **Perform single instance or repetitive archiving.** Once you set up your Epoch Data Protection policies, you can perform archives as often as you wish—from a single archive instance to a regularly scheduled archive.

8. **Granular view of data.** Viewing the contents of an Epoch is as intuitive and as detailed as viewing the contents of the file system using Windows Explorer. Rather than having to recover the entire contents of the Epoch, you can drill down within the file system and specify the files you want to recover.

9. **View a full document rendering before restoring.** This powerful feature lets you view the entire contents of a file from an Epoch to ensure that particular version of the file is the one you want to recover. There is no limitation to what can be viewed in the rendering. For example, if you want to see the text of a 200-page document, the rendering will include all 200 pages.

10. **Enables select personnel to recover data.** Once you have designated the data owner, they can recover files from the Epochs that you specify. For example, a data owner in the Legal division might be enabled to recover files from Epochs pertaining to High-Value Targets related to legal files, but not the Epochs related to the Sales department.