opentext™

Top Reasons

Top Ten Features of Data Protector for Ransomware Recovery

OpenText Data Protector is an enterprise class, highly scalable backup and recovery software solution. Its deep integration with hardware storage providers provides a single backup and recovery solution for simple or complex hybrid-IT environments. It provides a complete protection for unstructured data, mission critical application, Operating Systems and virtualized environments.

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[1] in various locations, with restrictive administrative and system access[2], in other words, they`ve recommended to follow the 3-2-1 backup rule. See how OpenText™ Data Protector, with its functionalities, 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 environment, some of them are absolutely vital and their loss or corruption would be catastrophic. Data Protector could set different RPO and RTO targets depending on application value.

2. **Instant recovery via native application integrations.** Data Protector provides one of the most comprehensive mission critical applications protection for applications. This provides backup support across the enterprise and ensures business continuity with a rapid recovery after any data loss or system interruptions.

3. **Improve application performance and data availability with advanced recovery options.** Data Protector provides application aware automated snapshot management. IT staff could set snapshots on an hourly basis, minimizing the amount of data loss if ransomware strikes.

4. **Automated disaster recovery.** Automate DR with centralized bare metal recovery from or to physical and virtual systems from any existing file system or image. This option is enabled with a single click at no additional costs.

Data Protector saves IT administrator's time and ensures business continuity by providing a disaster recovery process that is built for modern enterprise IT environments. With Data Protector, administrators can:

- Quickly recover data and systems after a security breach, such as a ransomware attack.
- Reestablish operations at local and remote offices after natural disasters.
- Streamline IT management by using the same solution for backup and disaster recovery.
- Increase efficiency and business agility by recovering data to new systems with dissimilar hardware and hypervisors.
- Improve business continuity by ensuring up-to-date recovery images.
- Simplify disaster recovery using an interactive recovery wizard.

[1] *How to protect backups from ransomware, Maria Korolov, CSO Nov 2, 2020*

[2] *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

Connect with Us
OpenText CEO Mark Barrenechea’s blog

5. **Secure Backups.** Data Protector has adopted a secure approach to protect backups with a built-in security model. It is an enterprise-level backup and recovery solution with several methods of protecting backup data, such as encrypting backups during storage and while they are being transferred. In addition, Data Protector is Common Criteria certified[3].

6. **Backup to cloud.** Data Protector features native integration to the Amazon S3, Microsoft Azure, Scality, and Ceph cloud storage solutions. All data exchanged with or stored within these services is compressed and encrypted for efficiency and security. Extensive additional cloud backup options are available with the Data Protector for Cloud Workloads extension product.

7. **Tape Archive and Cyberattack Protection.** Tape backup provides security from ransomware attacks by backing up data onto a media type which is isolated from the regular system environment and so prevents malicious code from infecting the systems and data.

8. **The power of OpenText.** OpenText Data Protector integrates with many OpenText™ portfolio products including powerful automation tools to ensure businesses can maximize their productivity and simplify their environments. Automating routine tasks, such as regular maintenance, provisioning of resources, analytics and incident resolution may reduce operational costs and manual errors.

9. **Gain operational insights through advanced analytics.** The new reporting tool uses real-time intelligence derived from operational analytics to provide hindsight to resolve issues, insight to reflect the current process state and relationships, and foresight to enable prediction of future needs.

10. **Standardized protection.** Finally, Data Protector provides a unified and scalable architecture that enables centralized management across physical and virtualized environments, disparate OSs, and business applications from the core data center to remote sites. A single and comprehensive backup solution for heterogeneous hybrid IT environments.

Learn more at:
www.microfocus.com/dataprotector

www.microfocus.com/opentext

Download a free trial at:
www.microfocus.com/en-us/products/data-protector-backup-recovery-software/free-trial

[3] *NIAP web page*

opentext™