Top 10 features of OpenText Data Protector for ransomware recovery

A scalable backup solution for hybrid IT, protecting unstructured data, critical apps, OS, and virtual environments

Many organizations rely on backup systems to restore files after ransomware attacks. Due to sophisticated attacks, experts recommend multiple backups in various locations with restrictive access, following the 3-2-1 rule. OpenText™ Data Protector addresses these recommendations with its features and benefits.

1 **High-value target protection**
Amid all the potential petabytes of files in your environment, some are vital and their loss or corruption would be catastrophic. OpenText Data Protector can set different RPO and RTO targets depending on application value.

2 **Instant recovery via native application integrations**
OpenText Data Protector provides backup support across the enterprise and ensures business continuity with a rapid recovery after data loss or system interruptions. (Read more about how OpenText Data Protector protects OpenText™ Documentum™ Content Management.)

3 **Improved application performance and data availability with advanced recovery options**
Application-aware automated snapshot management allows IT staff to set snapshots on an hourly basis, minimizing the amount of data loss if ransomware strikes.

> “One of the big Data Protector advantages is the native application integration for all our clients’ database systems, SAP being the key one. We provide online backup capabilities without negatively impacting the source systems, so performance remains at the same level while the backup is performed, a crucial feature for our clients.”

Alexander Förster
Chief Technology Security Officer, Coca-Cola FEMSA

Read the full case study ›

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 cost.

5 **Secure backups**
OpenText Data Protector has a built-in security model to protect backups. An enterprise-level backup and recovery solution, it has several methods of protecting backup data, such as encrypting backups during storage and while they are being transferred.

6 **Backup to cloud**
With native integration to 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. Additional cloud backup options are available with the OpenText 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 that is isolated from the regular system environment, preventing malicious code from infecting the systems and data.

8 **The power of OpenText**
OpenText Data Protector integrates with many OpenText products, including 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 **Advanced analytics provide operational insights**
The OpenText Intelligence BI 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 predict future needs.

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

Learn more about OpenText Data Protector for ransomeware recovery ›