opentext™

Data Sheet

Data Protector for Cloud Workloads

OpenText Data Protector for Cloud Workloads is an enterprise grade backup and disaster recovery solution for corporate environments running modern IT workloads. Providing comprehensive backup for Microsoft 365, containers, and multiple hypervisors, to a diverse set of Cloud storage backup targets.

Product Highlights

An enterprise class, data centric backup and disaster recovery solution, Data Protector for Cloud Workloads (DP4CW) addresses the challenges of complexity, scalability and data security for modern IT workloads. Today's advanced IT environments are increasingly adopting newer technologies and migrating traditional applications and operations into hypervisors and onto the cloud. With a wide selection of cloud providers, hypervisors and containers now available Data Protector for Cloud Workloads supports the flexibility of deployments that modern companies want in order to meet operational goals while improving cost control and functional choice. It protects the use and migration to Microsoft 365 online which is increasingly being adopted for critical business operations. Built-in security protects backup data from unauthorized access and reporting dashboards give a clear insight to operational efficiency.

Data Protector for Cloud Workloads operates as a stand-alone solution, or it can be combined with Data Protector Premium through the integrated backup provider. This creates a comprehensive backup solution for the most complex environment allowing full use of storage infrastructure and platforms including physical, virtual, cloud, and tape. Implemented as a simple to understand and deploy capacity-based model, it is available with a perpetual or subscription license.

Key Benefits

Microsoft 365 Data Protection

Whether you are already using Microsoft 365 or considering migrating your environment onto it you need to ensure secure backup protection for your application data. While Microsoft will protect and backup the applications, they do not provide an enterprise quality backup solution for your data, so its protection falls to you. Data Protector for Cloud Workloads provides a high performance backup and recovery solution for the Microsoft 365 applications, including Exchange online, SharePoint online, Teams, and OneDrive for Business.

Protection for Your Hypervisor of Choice

There are many hypervisors available, and each offers different benefits for different applications and environments. Delivering backup protection across a wide range of hypervisors allows flexibility of solution to best meet your business demands. Extensive hypervisor backup support ensures your business is not hindered or compromised by a lack of backup protection.

Quick View

- Microsoft 365 data protection
- Container backup
- Wide range of hypervisor backup supports flexibility, operational efficiency, and cost saving
- Extensive cloud storage provider backup targets
- Role Based Access Control for user authorization
- Snapshot management and snapshot consistent technology
- File-level restore using mountable backups
- Recovery plans for automated DR
- Data encryption for file system backup destination
- Secondary backup destination
- Full and incremental backups
- Immutable backup to protect backup data from being encrypted by ransomware
- Open (REST) API for 3rd party software integration
- Simplified capacity licensing—perpetual and subscription

Modern Workloads

Containers, virtual machines, and applications are protected whether in the cloud or on-premises. Providing an agentless backup solution with snapshot management, Data Protector for Cloud Workloads is a fully inclusive solution that is simple to implement.

Backup Security

Ransomware and cyber-attacks are an increasing threat. Security is enhanced with Data Protector for Cloud Workloads by offering encryption to protect from data theft. Access management is enabled using Role Based Access Control, allowing access privileges to be set for individuals and groups.

Extended Environment Integration

Data Protector for Cloud Workloads seamless connects with Data Protector Premium to provide comprehensive backup capabilities across a full heterogeneous environment. By using the backup provider connection to Data Protector all the capabilities of Data Protector Premium can be utilized for backups. Expand the range of backup targets to include traditional storage infrastructure as well as tape backup. Tape backup is one of the key backup targets to ensure ransomware protection by isolating backups from all cyber-attacks.

Secondary Site Backup

Backup can be directed to a primary backup location and to a secondary backup location to store data in more than one location for added security or test purposes.

Key Features

Modern workloads demand a new level of data protection to address their specific needs. OpenText Data Protector for Cloud Workloads (DP4CW) provides a stable, agentless backup and snapshot-management solution for virtual machines, containers, storage providers, and applications working on-premises and in the cloud. DP4CW supports multiple backup destinations for convenient data storage planning including local filesystem or an NFS/CIFS share, or object storage (cloud providers), extending the already extensive backup capabilities of Data Protector.

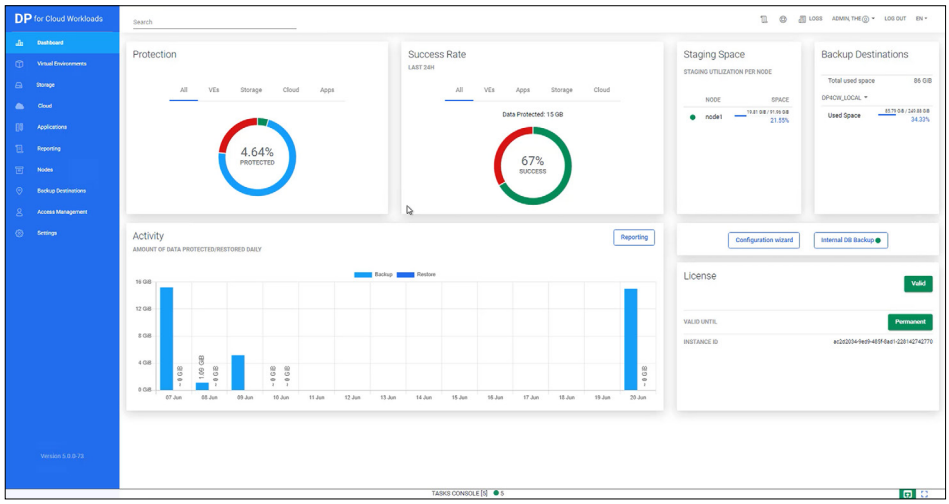

Figure 1. Data Protector for Cloud Workloads Dashboard

Microsoft 365 Data Protection

Online applications offer many advantages, but they only provide minimal data backup support. Data Protector for Cloud Workloads' backup capabilities are extensive, offering many usable features on a scalable architecture.

- Restore to cloud or to local systems.
- Automatic synchronization of users.
- Cross-account migration of files/mails.
- Quick search and find.
- Exchange Online: emails, contacts, calendar, and events
- SharePoint Online: Sites
- OneDrive for Business: Files
- Teams: Teams chats, 1on1 chats, Teams document libraries and sites.

Hypervisor Integrations

A wide range of hypervisors are supported to extend protection for virtual machines beyond Hyper-V and VMware.

- Full and incremental backup protection for KVM, Oracle VM, AWS EC2, Nutanix, and Citrix Hypervisor.
- File level restore with AWS EC2 and Citrix XEN, and including mountable backups for KVM, and Oracle VM.
- Depending on hypervisor, capabilities also include application consistent snapshots, option to exclude specific volumes, changed block tracking (CBT), LVM thin-pool support

OpenStack and OpenShift

This scripted solution enables VM Workloads in AWS EC2 to be snapshotted first then replicated into AWS S3 storage. This offers the advantage that backup data is separated from live data, and it is then possible to make use of Data Protector scheduling, reporting, and monitoring for your hybrid-IT approach.

- OpenShift backup of metadata and data in persistent volumes
- Automatic pause of running deployments for consistent backup.
- Option to exclude specific persistent volumes.

- OpenStack backup of instance metadata and data in QCOW2 volumes.
- Full and incremental backup—Option to exclude specific volumes and restore individual files.
- Disk attachment backup strategy using Cinder.

Container Backup

Backup support is provided for Kubernetes, Proxmox and OpenShift. DP4CW provides agentless full and incremental consistent backup.

Role Based Access Control

RBAC supports administrator role as well as being able to create groups and offers full role management. Groups allows multiple users to be assigned to multiple roles. LDAP is supported and LDAP accounts are automatically assigned to the Operators group when first created.

Automated Recovery Plans

Recovery plans enable the automated recovery of multiple VMs. Different recovery plans can be implemented:

- On demand for disaster recovery will restore multiple VMs
- Scheduled recovery implements periodic testing of restore.

Restore testing is a critical aspect of any backup solution to ensure correct operation of the solution.

Learn more at

DP4CW Product Overview Page

DP4CW Technical Documentation

DP4CW Trial Download

www.microfocus.com/opentext

** Full product technical documentation is available here:* **www.microfocus.com/documentation/data-protector/clouds/DP4CW.pdf**

Software Requirements

Operating System Support:

- RedHat Enterprise Linux, version 8.x Minimal install (Basic functionality)

Or

- CentOS, version 8.x and Stream Minimal install (Basic functionality)

Data Protector for Cloud Workloads Server:

- MariaDB 10.4 (installed from the official MariaDB repository)

Hardware Requirements

All-in-one installation (DP4CW Server and Node on the same machine)

Minimum requirements (Physical or virtual server):

- CPUs: 4 cores
- RAM: 8GB
- Disk 1: 20GB for Operating System, and Data Protector for Cloud Workloads installation
- Disk 2: 200GB–1TB for backup staging (can be skipped if configured to stage directly on external backup destination)

Separated model installation (DP4CW Server and Node on separate machines)

Data Protector for Cloud Workloads Server (Physical or virtual) minimum requirements:

- CPUs: 2 cores
- RAM: 6GB
- Disk 1: 20GB for Operating System, and Data Protector for Cloud Workloads installation
- Disk 2: 200GB–1TB for backup

Data Protector for Cloud Workloads Node (Physical or virtual) minimum requirements:

- CPUs: 2 cores
- RAM: 4GB
- Disk 1: 20GB for Operating System, and Data Protector for Cloud Workloads installation
- Disk 2: 200GB–1TB for backup staging (can be skipped if configured to stage directly on external backup destination)

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™