Solution Flyer

IT Operations Management

Safeguard Mission-Critical Applications with Data Protector

Micro Focus® Data Protector optimizes the backup and recovery of mission-critical applications, reducing interruptions to business operations.

Data Protector at a Glance:

- **Application-Aware:**
  Uses application programming interfaces (APIs) and deep integrations with underlying storage to speed up and improve the reliability of backup and recovery
- **Optimized for Hybrid Computing:**
  Streamlines backup and recovery on public cloud platforms
- **Uses Hardware Acceleration:**
  Takes advantage of storage hardware, enabling instant recovery, deduplication, and other time- and money-saving capabilities in both physical and virtual environments
- **Automates Analysis:**
  Analyzes and optimizes backup and recovery performance

Mission-Critical Applications Need a Strong Safety Net

IT departments may be risking application outages by using backup software not designed to meet strict service level agreements (SLAs). This can occur when backup software is sufficient for basic tasks, but not for backing up systems that require 100 percent uptime, such as those used to record customer orders, billing applications, and payrolls. If the backup software does not use dedicated application integration agents, it can't ensure data consistency or support applications running in high availability mode.

Companies with large amounts of data and complex, hybrid IT environments are particularly at risk of backup and recovery processes slowing down their operations. Some organizations try to overcome this challenge by using multiple backup solutions, each one designed to back up a different application. This approach can solve some application integration challenges, but not infrastructure integration problems. It's also harder to manage multiple backup applications, particularly when they don't use a consistent method of operating and reporting.

Having multiple backup applications also makes it harder to diagnose problems—the last thing an IT department needs when it's under pressure to bring a mission-critical system back online.

A Better Way to Protect Critical Data

A more effective way of protecting mission-critical applications is to use an enterprise-class backup and recovery solution that can scale extensively and integrate deeply with an organization's entire IT environment.

Micro Focus Data Protector uses this strategy. It is a backup and recovery solution designed to work efficiently with critical applications such as Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server, Oracle Server, SAP HANA, IBM Db2, and MySQL. It does this by using backup APIs (such as SAP BackInt, Oracle RMAN, or Microsoft VSS) or file system agents for integrating with Windows, Linux, and Unix, including mission-critical HP-UX environments. It also interfaces with storage hardware from Hewlett Packard Enterprise (HPE), Dell EMC, NetApp, Hitachi, Oracle, and other vendors.

Data Protector protects mission-critical applications across hybrid IT environments. It integrates with VMware vSphere and Microsoft Hyper-V, eliminating the need for separate solutions for virtual environments. Companies can also use it to store data using public cloud services such as Microsoft Azure, and those from Amazon Web Services, and Ceph and Scality storage systems.

Another feature that sets Data Protector apart from competing products is its predictive analytics engine. The solution monitors and

analyzes backup processes and provides exhaustive reports, including real-time reports about whether backups are meeting SLAs. This improves IT departments' visibility of backup and recovery operations and their ability to optimize them.

How Data Protector Safeguards Mission-Critical Applications

Speeds Up Backup and Restoration

Application awareness allows Data Protector to back up and recover applications running in complex high performance configurations. For example, it supports Oracle Real Application Clusters and Oracle's Automatic Storage Management feature for high-performance databases. Organizations can also use it to protect applications running in availability groups, maximizing uptime of applications such as SQL Server.

Companies that regularly turn on thousands of additional virtual servers to handle customer orders, or to process large production jobs, will also benefit from Data Protector. Application awareness allows it to back up these systems quickly and reliably.

Data Protector also takes advantage of an organization's storage hardware to speed up backup and recovery. For example, a company can use the software's hardware-assisted snapshot capability to back up a mission-critical SAP database to a storage array, so it can then recover the database instantly.

Organizations can use Data Protector to quickly recover entire systems in the event of a catastrophic failure, instead of setting up separate software for this task. This feature is called Enhanced Automated Disaster Recovery, or Bare-Metal Recovery, and it works by including disaster recovery images with backups—this eliminates the need for extra work to create disaster recovery images.

Data Protector can also back up data as often as every few minutes, increasing the amount of data it protects. Granular Recovery Extensions allow application owners to recover this data themselves, speeding up the recovery process.

Streamlines Data Replication

Companies with multiple sites can also benefit from the solution. Rather than backing up data to tape and then sending it via courier to a remote archive location, Data Protector makes it easier to replicate backups across the network. Its federated deduplication capability works with systems, such as HPE StoreOnce Catalyst and Dell EMC Data Domain to transfer the data in a deduplicated state, reducing bandwidth requirements.

If a company loses its primary backup system, the Automatic Replication Synchronization feature makes it easier to recover replicated backups from a remote system. It does this by eliminating the need to manually set up a standby cell manager.

Minimizes Data Loss

Better visibility of backup and recovery processes also helps administrators to detect problems before they result in application outages and data loss. For example, Data Protector can alert IT teams about resource conflicts.

Because the solution integrates with the entire IT environment, it also gives IT administrators a better picture of whether they are meeting backup and restoration SLAs and how to fix problems. For example, a company might be taking longer than usual to back up a database at a site in the U.S., which could delay replication of the data to a site in Europe. Data Protector could alert administrators that the database isn't being backed up fast enough, before the problem affects the European site. It can also analyze the cause of the problem and recommend steps to resolve it.

Saves Employees Time and Reduces Costs

Data Protector saves IT department's time by providing them with a single interface to manage hosts, clients, licenses, and backup jobs. This is particularly useful for companies storing primary backups on disk-based appliances and archives on tape libraries, including multiple tape formats acquired during company mergers. Rather than using separate management tools, administrators can use Data Protector to manage backup and recovery from all the storage platforms.

Administrators can also use Data Protector's analytics capability to predict when they will run out of backup storage capacity, allowing them to reduce hardware costs by buying only the infrastructure they need. By streamlining the backup and recovery environment in this way, administrators can dramatically simplify the task of supporting mission-critical applications.

Learn more at
www.microfocus.com/dataprotector