

Micro Focus Data Protection for HPE ProLiant for Microsoft Azure Stack

JUNE 2018



Hybrid cloud is increasingly gaining popularity among enterprise IT buyers, as companies recognize and begin to validate its benefits. With a hybrid cloud, organizations can take advantage of the elasticity and agility of the public cloud, especially for new cloud-native apps, while continuing to run certain applications on premises. Users gain the choice of deploying new and existing workloads in the public cloud or the data center, wherever it makes the most sense, and the flexibility to migrate them as needed. A hybrid cloud significantly eases the transition to the cloud, enabling organizations to compete in the new cloud-driven world while preserving current IT investments. With these benefits in mind, well over 80% of organizations we recently surveyed are in the process of moving or planning a move to a hybrid cloud infrastructure.

In this brave new world, Microsoft Azure and Azure Stack are increasingly being adopted as the foundation for companies' hybrid cloud infrastructure. Microsoft Azure is a leading public cloud offering that, based on Taneja Group research, consistently ranks neck-in-neck with Amazon Web Services in enterprise adoption, with more than 50% of companies using or planning to use Azure within the next two years. Microsoft Azure Stack enables organizations to deliver Azure services from their own data center, and is delivered as an integrated hybrid cloud solution on HPE ProLiant servers. HPE ProLiant for Microsoft Azure Stack allows users to run Azure-consistent services on-premises to meet the key use cases of data sovereignty, security, and compliance; edge and disconnected applications; and high performance analytics, while providing a common developer experience. Together, Microsoft Azure and Azure Stack provide a natural and relatively frictionless path for Microsoft Windows customers to move to the cloud, along with support for new cloud-native tools and services that allow customers to fully take advantage of cloud agility and scalability.

As organizations move critical apps and data to the cloud, data protection quickly becomes a key requirement. But as buyers evaluate solutions, they often find that cloud providers' built-in backup tools lack the flexibility, breadth of coverage, app awareness and enterprise capabilities they have become accustomed to on premises. As a result, companies look to other vendors—often their on-premises providers—to meet their data protection needs. As we'll see, Micro Focus Data Protector offers a fully integrated, robust and comprehensive solution for backup and recovery on HPE ProLiant for Microsoft Azure Stack.

In this piece we'll further explore the need for data protection in a hybrid cloud environment, and examine the specific backup and recovery approaches that buyers are looking for, as revealed in our recent research. Then we'll briefly examine what makes Micro Focus Data Protector an ideal solution for protecting an organization's key information assets running on an HPE ProLiant for Microsoft Azure Stack hybrid cloud environment.

THE NEED FOR DATA PROTECTION FOR MICROSOFT AZURE STACK

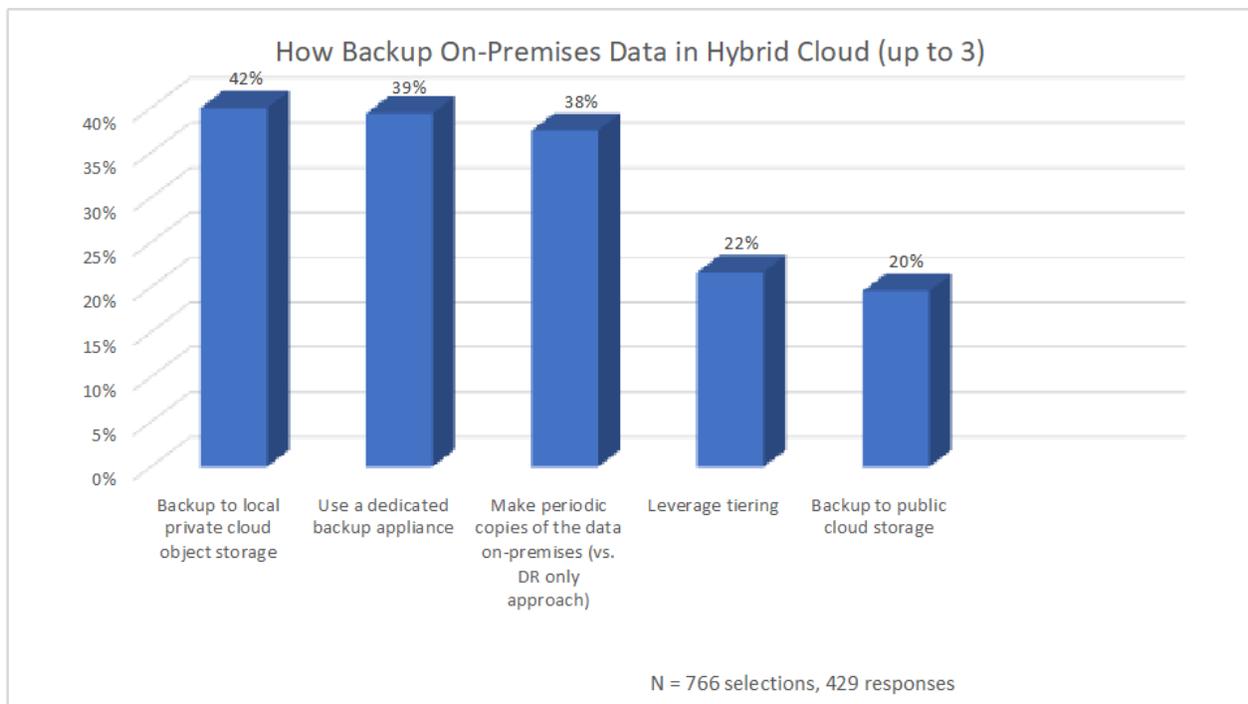
Data protection is rapidly becoming a key requirement and buyer focus in public and hybrid cloud environments. As you begin to move and deploy some of your critical apps and data in the cloud, you are also likely considering how best to protect those apps.

Based on our recent research findings, organizations are planning to move a growing number of apps of all types to a public and/or hybrid cloud, including cloud-architected and traditional on-prem apps, business critical and non-critical workloads; with some destined to be run as infrastructure-based solutions and others as software-as-a-service deployments. Not surprisingly, given the range and criticality of workloads being moved to the cloud, 95+% of companies running a hybrid cloud plan to back up data for their most important on-premises and cloud-based apps.

In our research, we learned that enterprises are looking for specific data protection capabilities in the hybrid cloud:

- **Flexibility:** The solution should support multiple backup approaches and topologies, agent or agentless, and offer backup on-prem or to the cloud. Figure 1 shows that no one or two backup options are dominant in buyers' plans.
- **Ability to use existing backup infrastructure and processes:** IT buyers prefer to continue to use familiar backup infrastructure and processes whenever possible, to avoid re-training and preserve existing data protection investments.
- **Adaptability to rapidly changing cloud environments:** Customers are looking to take advantage of an increasing number of hybrid cloud storage use cases, and as they do, will evolve their usage of backup methods over time.
- **App-specific backup, tailored to the needs of each application:** Our research showed that more than 80% of respondents prefer app consistency over crash consistency, assuming that it is not too difficult or costly to achieve.
- **Built-in monitoring and analytics:** It can be difficult for admins in a fast-moving hybrid cloud environment to assess how effectively they are meeting users' data protection needs. Practitioners need a simple means to stay on top of their backup and recovery activities, not just to avoid potential issues, but also to improve backup performance and ensure that service level agreements are met.
- **Meet data security and compliance requirements:** These are consistently listed as top requirements for workloads in a public or hybrid cloud.

Figure 1: How Backup On-Premises Data in Hybrid Cloud



SOURCE: TANEJA GROUP RESEARCH

Many customers assume the public cloud providers protect their data without any action required, but they generally do not. Snapshot and replication solutions or services are often available in the public cloud but do not meet buyers' key requirements outlined above. In particular, these technologies tend to be more DR oriented, and are not always tailored to the specific data protection needs of each app. As a consequence, snapshot and replication solutions cannot deliver app-consistent recovery, which a large majority of buyers are demanding in their cloud environments.

Based on our research insights, Microsoft hybrid cloud users have a need for a simple and comprehensive data protection solution, with the flexibility to address the backup and recovery needs for a range of different applications, and the built-in monitoring and analytics capabilities to ensure that backup service-level commitments can be met. As we'll see in the next section, Micro Focus Data Protector stands out as a solution that can meet these needs in an HPE Azure Stack environment.

MICRO FOCUS DATA PROTECTION FOR HPE PROLIANT FOR MICROSOFT AZURE STACK

As hybrid cloud infrastructure becomes commonplace, on-premises backup solutions must uniquely adapt to support these new environments. Our research has shown hybrid cloud installations will initially be an additive solution to already existing on-premises traditional infrastructure. For data protection, it means that enterprises will have to decide if it makes sense to absorb hybrid cloud backup and recovery into an existing solution or look for an entirely new solution. We believe that most Azure Stack customers will likely integrate hybrid cloud backup into their existing backup infrastructure. Therefore, the HPE solution combined with Micro Focus Data Protector provides an ideal data protection solution due to the broad compatibility and unique value-added integrations these companies have brought together with their respective hardware and software capabilities. In this section, we briefly outline how best to backup an HPE ProLiant for Microsoft Azure Stack environment using Micro Focus Data Protector software. A companion product called Micro Focus Backup Navigator provides IT staff with a global-wide interactive dashboard that enables analytical insight and adaptive intelligence to maintain backup and recovery operation SLA compliance.

Understanding Azure Stack's architectural impact on Backup

HPE ProLiant for Microsoft Azure Stack is a pre-tested, factory-integrated hybrid cloud solution, providing a development, management, and security experience consistent with Azure Public Cloud (see Figure 2). HPE Azure Stack delivers Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) on HPE hardware in your data center. It runs Azure compatible services on-premises to meet security, compliance, cost, and performance requirements. The HPE solution is a scale-out hyper-converged architecture primarily made up of 4-16 DL380 ProLiant nodes. Microsoft includes Infrastructure Backup Service, a solution for backing up the Azure Stack management and configuration environment. With Azure Stack, you can replicate data back to an Azure public cloud as a disaster recovery option using Azure Site Recovery, but the DR offering does not offer advanced data protection techniques such as backup lifecycle management, single item recovery, advanced app integration or many other data protection features that enterprises are accustomed to using. However, for data protection

Figure 2: HPE ProLiant for Microsoft Azure Stack Infrastructure Overview

Solution Components

- 1 Rack
- 2 TOR Switches
- 1 OOB Switch
- 1 DL360 Management Server (OOB Server)
- 4-16 DL380 Servers (Azure Stack Nodes)
- OneView /IRS

Factory Build

- Standard Factory Build
- Rack, Stack, Cable
- Load Firmware & Software
- Factory system test and verification

Onsite Installation by Pointnext

- Standard HW installation
- Connect to customer network
- Install Microsoft Azure Stack
- Integrate with Azure AD
- Verification
- Hand off to customer



SOURCE: HPE

of the customer's content, Microsoft recommends purchasing either Microsoft branded Azure Backup services or using third-party backup solutions such as Micro Focus Data Protector. For enterprise-class backup capabilities, many customers will require more than the native solutions Microsoft provides. Microsoft focuses optional native backup offerings at homogenous Microsoft environments.

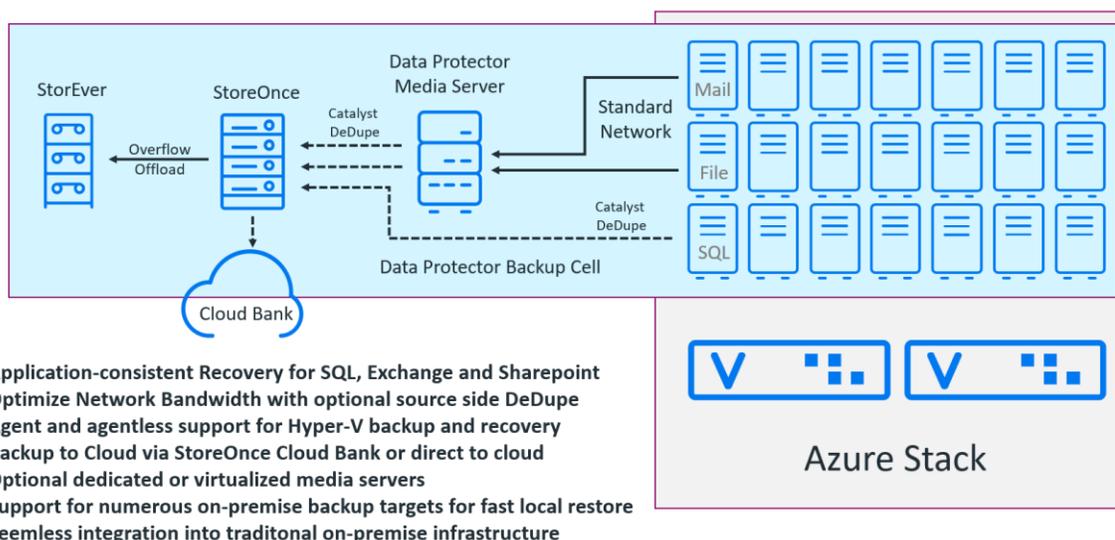
Azure Stack primary storage is provided using scale-out data services called Microsoft Storage Spaces Direct. Data protection solutions will need to be compliant with this type of storage and optimized for network-based backup since the applications and storage resources (including the backup process) share the total available IP bandwidth. The following attributes make up an ideal data protection solution for Azure Stack environments:

- **Efficient IP-based data movement:** Support for efficient use of IP bandwidth such as source-side deduplication, delta-based backups, snapshot integrated, etc.
- **Integration with existing backup solutions:** In most cases, Azure Stack will be incremental to existing on-premises infrastructure. Therefore, the solution should leverage existing backup software and hardware to minimize cost.
- **Optional backup to public cloud as well as on-premises:** Some customers will want to leverage the Azure public cloud as a backup target in addition to disaster recovery. However, on-premises backup targets will enable the fastest local restore time and may save cost if using existing hardware.
- **Advanced features for Microsoft environments:** The likely business applications for Azure Stack will be Microsoft centric. Therefore the backup environment should have advanced integrations into Microsoft SQL, Exchange, Hyper-V, etc.

HPE and Micro Focus Data Protector Solution

HPE and Micro Focus have engineered numerous advanced data protection options that work well in an Azure Stack environment. The goal of these solutions is to be flexible while seamlessly fitting into an existing backup environment, but also cloud-friendly to create a solution that can move ahead as enterprises transform into the future. In this paper, we will not go into the details of all the possible data protection features but will highlight the key aspects of an ideal solution for Azure Stack. Figure 3 is a basic diagram of how such a solution could come together.

Figure 3: Micro Focus Data Protector and HPE ProLiant for Microsoft Azure Stack Architecture



SOURCE: MICRO FOCUS

The following attributes make Micro Focus Data Protector with Backup Navigator an ideal solution for HPE ProLiant for Microsoft Azure Stack environments.

- **Application-consistent Recovery:** Micro Focus supports application-consistent backup and restore for many mission-critical applications, including popular Microsoft Exchange, SQL Server, and SharePoint application environments. Not only are backups consistent, but the solution also supports granular recovery of individual items. Snapshot and replication-based backup schemes are typically crash consistent and are cumbersome to use when restoring individual items from a backup.
- **Network Bandwidth Optimization:** Micro Focus Data Protector when combined with HPE StoreOnce provides options to minimize network bandwidth, such as through the use of source-side deduplication or by placing media servers directly in the Azure Stack environment. Since Azure Stack is a scale-out HCI architecture, this enables the backup administrator to balance network usage versus CPU usage to optimize the system overall. Micro Focus Backup Navigator can monitor the overall backup process to help ensure SLA compliance. If not compliant, then Backup Navigator allows backup jobs to be easily reconfigured to ensure the optimal use of system resources.
- **Optional Backup to the Cloud:** Micro Focus supports backing up directly to AWS and Azure public clouds, for those that want to add an Azure Stack with a minimal hardware footprint. Also, Micro Focus supports backing up to the cloud by using HPE Cloud Bank Storage. HPE Cloud Bank Storage is a feature of HPE StoreOnce systems that delivers highly efficient, economic and reliable data transfer to your on-premises and off-premises cloud. Another key benefit of combining StoreOnce deduplication and cloud storage is that you can achieve very fast local restores while also saving longer term backups into the cloud cost effectively.
- **Heterogenous Flexibility:** Micro Focus Data Protector has a rich history of supporting multiple enterprise backup environments. By seamlessly fitting into an Azure Stack environment, Micro Focus Data Protector enables Azure Stack to fit into an existing customer's backup infrastructure. This allows Azure Stack customers to benefit from other infrastructure already on-premises, such as backup appliances, media servers, and even tape-based systems.
- **Enterprise-wide monitoring and analytics:** Micro Focus Backup Navigator provides an interactive dashboard that gives analytical insight and adaptive intelligence to maintain backup and recovery operations. IT staff can immediately identify inefficiencies within the backup operations and the unbalanced use of backup resources and uncover failures before they are exposed in the recovery process. With adaptive intelligence, the highest priority backup jobs are ensured completion within given service level agreements.

TANEJA GROUP OPINION

The hybrid cloud transformation is real and accelerating across the IT industry, and we believe it will soon become the most popular on-premises infrastructure approach. This transformation demands that data protection solutions quickly adapt and protect the data in a way enterprise customers are accustomed to. Microsoft Azure Stack promises to be a very popular hybrid cloud approach with many customers. However, we believe that there will be many types of hybrid clouds, and existing infrastructure on-premises will remain in place for some time into the future. Therefore, we would recommend solutions that are flexible enough to handle existing IT infrastructure but also architected to transform into the new environments. We believe Micro Focus Data Protector is a solution that works well in today's environment and is constantly evolving and improving to work well in a hybrid cloud future. Micro Focus Data Protector is a highly modular, scalable solution, which is a perfect complement to the micro-services architectures of the future.

Micro Focus and HPE are working together on numerous cloud-ready data protection solutions as we have highlighted in this Solution Brief. We expect this strategic partnership to remain strong in the

future as both companies focus on hybrid cloud solutions. New regulations such as GDPR will dictate that meeting data security and compliance requirements are not only critical issues for businesses today, but also as new requirements crop up in the future. We believe that solutions that are flexible and can adapt to new requirements quickly will be the ones that thrive in the new hybrid cloud world. Both HPE and Micro Focus are well positioned to help businesses seamlessly transform from a legacy environment to the hybrid cloud future.

NOTICE: The information and product recommendations made by Taneja Group are based upon public information and sources and may also include personal opinions both of Taneja Group and others, all of which we believe to be accurate and reliable. However, as market conditions change and not within our control, the information and recommendations are made without warranty of any kind. All product names used and mentioned herein are the trademarks of their respective owners. Taneja Group, Inc. assumes no responsibility or liability for any damages whatsoever (including incidental, consequential or otherwise), caused by your use of, or reliance upon, the information and recommendations presented herein, nor for any inadvertent errors that may appear in this document.