ESG SHOWCASE

Protecting Microsoft Azure with Backup and Recovery Solutions from Dell

Date: June 2022 **Author:** Christophe Bertrand, Practice Director and Senior Analyst

ABSTRACT: Public cloud and SaaS are top of mind for IT leaders as IT modernization continues to drive spending. However, the trend is running into headwinds as IT environment complexity, a shortage of critical IT skills, and the immediate need to combat cyber threats jeopardize data and disrupt innovation. A new breed of data protection built for multi-cloud, multi-workload environments promises to satisfy demanding cloud and on-premises SLAs and includes cyber protection and automation features to reduce complexity.

Market Landscape

Seventy-four percent of respondents to a recent ESG survey on the state of application infrastructure modernization trends across distributed cloud environments cited IT transformation as a top digital transformation initiative.[1] The maturity of digital transformation initiatives closely maps to the development of cloud-native applications and extensive use of DevOps and agile development, with cloud-native being synonymous with container architectures such as Kubernetes.

Almost all respondents (95%) indicated their organization uses public cloud services, and they expect the number of business applications running in the cloud to increase.[2] Currently, nearly one in five organizations report running more than 40% of their applications in the public cloud. This includes SaaS and custom applications.[3]

Although the cloud continues to be top of mind, organizations seek to balance public cloud and on-premises infrastructures and applications. While 44% of respondents indicated they had a cloud-first policy for new application deployment, nearly half (47%) said they consider both on-premises and public cloud equally.[4]

There is a significant overlap between growth in the cloud and the need for more effective cybersecurity. More than half of survey respondents identified strengthening cybersecurity (38%) and/or improving operational resiliency against cyber-attacks (28%) as top business initiatives driving technology investment in 2022. Cloud-specific cyber spending includes cloud application security (62%), data security (58%), and cloud infrastructure security (56%).[5]

The Challenge of Data Protection in a Multi-cloud, Multi-workload Environment

Application modernization and the broad adoption of container architectures and Kubernetes are increasing the number and variety of sites that IT must manage, both in the cloud and on-premises. The vast majority (86%) of organizations

[1] Source: ESG Research Report, *Application Infrastructure Modernization Trends Across Distributed Cloud Environments*, March 2022.
[2] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.
[3] Ibid.
[4] Ibid.
[5] Ibid.

leverage more than one provider for public cloud services.[6] The automated deployment, scaling, and management that Kubernetes brings to container-based applications undoubtedly contributes to the multi-cloud trend.

While Kubernetes applications offer benefits for modernizing or re-platforming applications, they also pose a growing data protection challenge. Three-quarters (75%) of IT professionals wrongly assume that these applications can be protected the same way as conventional applications.[7] This is a very dangerous assumption with ramifications for data protection SLAs. Over half of organizations (58%) rely on existing backup and recovery tools or storage-based snapshots for container data protection.[8] However, this traditional approach does not capture the full extent of a Kubernetes application and cannot guarantee recovery.

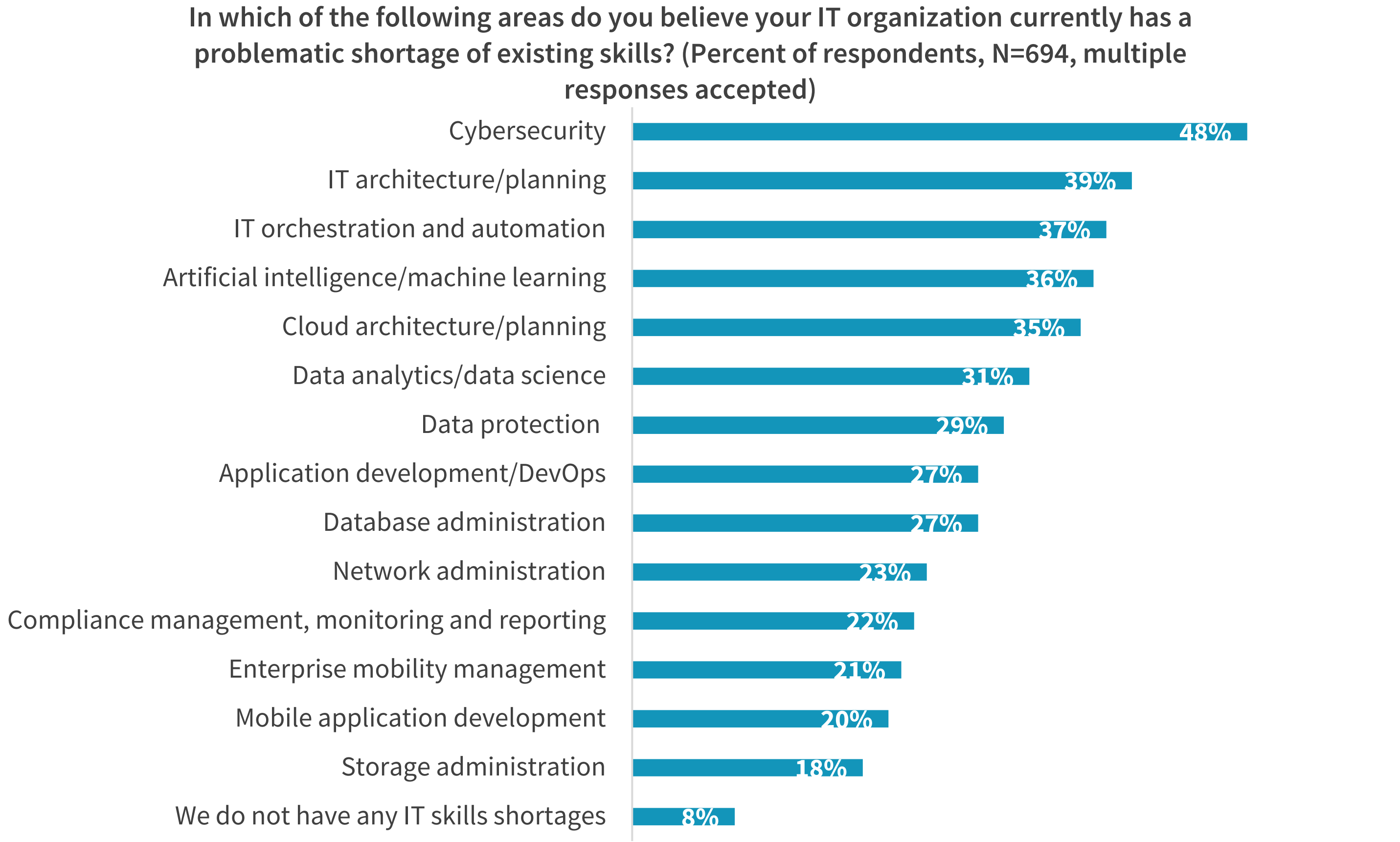
A Perfect Storm

The urgent need to improve cybersecurity is running into the transformation-driven increase in multi-cloud, multi-workload applications, creating a perfect storm of IT environmental complexity. When asked about the top drivers of complexity, organizations cite changes in the cybersecurity landscape (37%), higher volumes of data (35%), and applications leveraging new modern architecture (34%) as the main culprits.[9]

To make matters worse, the areas responsible for the growth in complexity also correspond closely to those suffering from a shortage of IT skills. More than half of respondents (54%) said their organization has a shortage of cloud/IT architecture skills, while nearly half (48%) indicated a shortage of cybersecurity skills, and 29% said they have a shortage of data protection skills (see Figure 2).[10]

[6] Source: ESG Research Report, *Application Infrastructure Modernization Trends Across Distributed Cloud Environments*, March 2022.
[7] Source: ESG Research Report, *Data Protection Trends and Strategies for Containers*, December 2020.
[8] Source: ESG Survey Results, *Data Protection Considerations for Containers,* December 2020.
[9] Source: ESG Complete Survey Results, *2022 Technology Spending intentions Survey*, November 2021.
[10] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

Figure 2. Cybersecurity and Cloud/IT Architecture Lead Skills Shortages



Source: ESG, a division of TechTarget, Inc.

For IT leaders, protecting complex IT environments from data loss and corruption, both conventional and cyber-related, requires solutions that were designed with the following in mind:

- Developed for multi-cloud, multi-workload containerized applications with automation to simplify data protection compliance in DevOps pipelines.
- Optimized for SaaS data protection.
- Able to provide advanced cyber protective measures with usability and automation assistance to minimize administrative overhead.
- Are easy to use and deploy.

Backup and Recovery Solutions for Microsoft Azure from Dell

Dell PowerProtect Data Manager is a unified platform for protecting a wide range of mission-critical enterprise workloads. This is a time-tested solution that includes extensions developed to protect multi-workload environments running on self-deployed Kubernetes clusters, Azure Kubernetes Service (AKS), and in-cloud Kubernetes as a Service (KaaS).

PowerProtect Data Manager provides enterprise-grade protection for Microsoft Azure Cloud workloads without the need to manage additional infrastructure. The solution supports end-to-end cyber resiliency and offers the same data protection functionality in the cloud and on-premises. Hybrid and multi-cloud data protection use cases include:

- Backup to the cloud.
- Backup of workloads in the cloud.
- Disaster recovery to the cloud.
- Long-term retention to the cloud with migration from on-premises to the cloud and back.

In addition, PowerProtect Cloud Snapshot Manager, a SaaS component of Data Manager, simplifies the protection of critical workloads in the public cloud by leveraging the underlying snapshot technology provided by Azure. A powerful tag-based policy engine with REST API enables automated protection of workloads for seamless backup and disaster recovery at cloud scale. These capabilities free DevOps to treat infrastructure as code.

PowerProtect Data Manager and PowerProtect DD Virtual Edition increase cloud efficiencies by combining data deduplication with Microsoft Azure Blob Storage, offering significantly lower cloud-compute, networking, and storage costs.[11]

Cyber Recovery for Microsoft Azure

PowerProtect Cyber Recovery for Azure offers multiple layers of protection to provide resilience against cyber-attacks and insider threats. It moves critical data away from the attack surface, physically and logically isolating it from access within Azure via a secure, automated operational air gap. The solution enables the recovery of critical data from the vault after a cyber-attack or for recovery testing procedures, allowing an organization to recover its data back to the corporate data center, to an alternate, or to a new VNET or clean environment within Azure.

Data Protection for Microsoft 365

Organizations need to employ cloud-based data protection solutions that offer predictable and controllable costs without adding complexity. Dell APEX Backup Services is a cloud-based data protection solution that offers unlimited on-demand scaling for continual protection of rapidly growing data volumes. The solution deploys easily and provides an intuitive web-based experience that extends centralized visibility and management across workloads and users.

Dell and Microsoft Azure

Available in the Azure marketplace, Dell and Azure cyber-resilient, multi-cloud data protection solutions simplify IT, lower costs, and reduce risk so that IT organizations can spend less time on infrastructure care and feeding and more time on application modernization. These solutions simplify IT by automating the protection of VMs, Kubernetes containers, and SaaS workloads.

By delivering solutions that are up to 75% more cost-effective than the competition,[12] Dell data protection offerings combined with Azure Blob storage give organizations a more efficient and sustainable way to scale workloads and data in the cloud.

And, through cloud-integrated cyber-resiliency capabilities, Dell and Azure help reduce risk from ransomware and cyber-attacks so IT has the confidence to recover critical data anywhere workloads reside.

[11] Source: ESG Economic Validation, *Understanding the Economics of In-cloud Data Protection: A Dell EMC Data Protection Solution Designed with Cost Optimization in Mind*, September 2021.
[12] Ibid.

The Bigger Truth

In today's increasingly complex hybrid multi-cloud, multi-workload environments, where on-premises is just another site, data protection vendors have a responsibility to craft their solutions as straightforward and uniform to deploy and manage as possible. Avoiding additional IT complexity is a must. Dell PowerProtect Data Manager achieves this with a unified platform for protecting a wide range of enterprise workloads, including self-deployed Kubernetes, Azure Kubernetes Service (AKS), and Kubernetes as a Service (KaaS).

Responsibility for data protection in these new multi-workload environments is increasingly a shared mandate,[13] involving IT operations teams, backup administrators, DevOps teams, and others. Dell PowerProtect Data Manager incorporates Kubernetes-specific data protection functionality and includes automation features that enable DevOps to integrate backup and recovery into their pipelines. Policy-based tagging lets developers treat the backup infrastructure as another element in their stack and is a powerful way to achieve reliable cloud-scale data protection compliance for new application workloads.

Ransomware has become a significant business continuity threat, and organizations must take whatever steps they can to protect critical business and operational data. Dell PowerProtect Cyber Recovery addresses this problem with a digital vault and air-gapped isolation, giving organizations the possibility of recovering data should ransomware attackers strike.

IT professionals should consider evaluating Dell's offerings for a number of reasons, including improved cybersecurity, reduced IT complexity, more reliable backup, and improved recovery. These are also the top benefits of cloud-based data protection cited by ESG survey respondents.[14] Based on these findings, Dell PowerProtect Data Manager, PowerProtect Cyber Recovery, and PowerProtect DD Virtual Edition are more than capable of providing these benefits.

a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com ✉ contact@esg-global.com ☎ 508.482.0188

[13] Source: ESG Research Report, *Data Protection Trends and Strategies for Containers*, December 2020.
[14] Source: ESG Research Report, *The Evolution of Data Protection Cloud Strategies*, May 2021.