ESG SHOWCASE

Innovative Protection for Cloud-native Environments

Date: August 2022 **Author:** Christophe Bertrand, Practice Director

ABSTRACT: Cloud-native applications are becoming widespread, as more organizations look to leverage their agility, efficiency, and alignment with DevOps models. However, protecting these apps and their data requires functionality typically missing from legacy data protection offerings. Dell Technologies' hybrid multi-cloud data protection solutions, available from Google Cloud Marketplace, deliver cloud-native protection for on-premises and Google Cloud workloads to simplify IT, reduce risks, and lower costs.

Market Landscape: Cloud-native Data Protection Demands New Approaches

Data protection is vital, but organizations that are increasingly dependent on cloud-native applications and services may find that legacy data protection solutions and processes come up short. Those older solutions weren't designed to protect microservices-based containerized applications. Their design paradigm was "one application means one data set."

A large disconnect exists between people's beliefs about protecting cloud-native data and reality. ESG found that 75% of survey respondents believe container-based applications can be backed up the same way that individual applications are.[1] They can't be. That misconception results in unwelcome surprises for a lot of IT organizations.

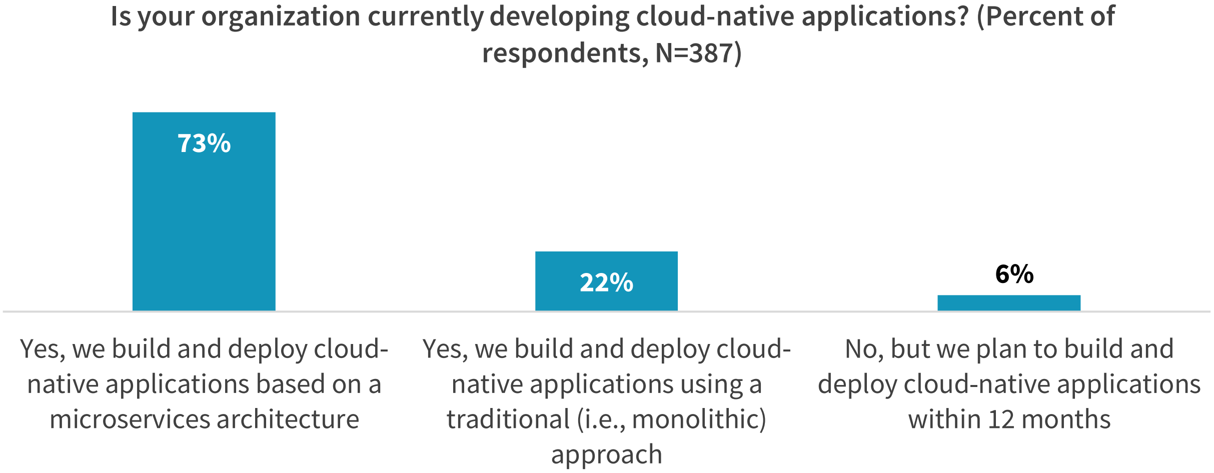
Legacy data protection is meant for static, monolithic applications, and it generally focuses on capturing data volumes. Containerized applications, though, are dynamic. That means the data protection solution must capture both the volumes and associated metadata. Notably, 73% of ESG survey respondents are already developing and deploying cloud-native applications based on a microservices architecture (see Figure 1).[2]

Unfortunately, many of those IT professionals may be unsure which container infrastructure components need protection. Remember, containerized applications are dynamic. They undergo regular, frequent changes that require protection of more than simply data. It is necessary to protect the applications cohesively as well. Effective protection demands backup of both data volumes and metadata. This is a fundamentally new process that differs markedly from what was used to protect static, monolithic legacy apps.

[1] Source: ESG Research Report, *Data Protection Trends and Strategies for Containers*, December 2020.

[2] Source: ESG Research Report, *Cloud-native Applications*, May 2022.

Figure 1. Deployment Trends for Developing and Deploying Cloud-native Applications



Source: ESG, a division of TechTarget, Inc.

In addition to challenges tied to protecting cloud-native apps, another danger to critical data comes in the form of persistent cyber-attacks. For example, ESG research shows that 30% of organizations experience ransomware attacks on at least a weekly basis, and 87% of respondents are concerned that their backups could become infected or corrupted.[3] Clearly, those organizations need new tools and processes to protect cloud-native data and applications effectively.

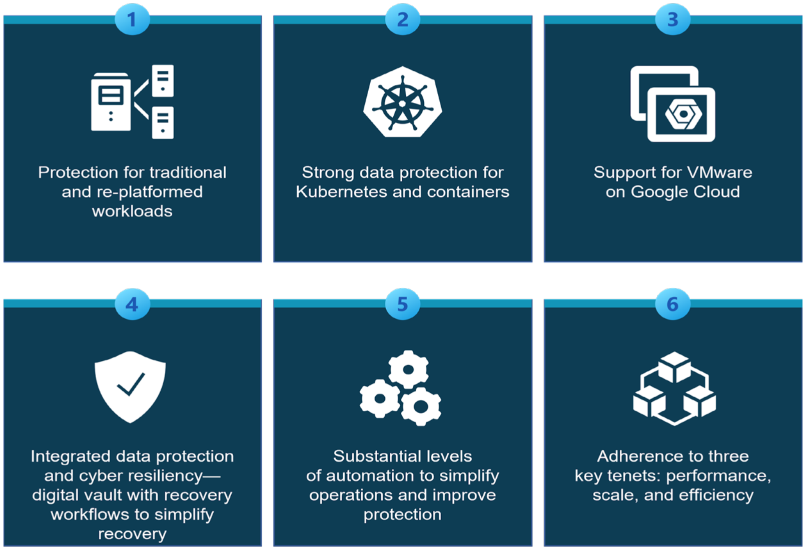
For Cloud-native Applications: A Purpose-built Google Cloud Data Protection Solution from Dell

Considering the current challenges, it is fortunate that Dell Technologies and Google have been working together to create next-generation data protection solutions for cloud-native apps. Google is a leader in cloud-native technologies and microservices, and Dell is a leading provider of cyber-resilient, multi-cloud data protection solutions that simplify and automate the protection of VMs, containers, cloud-native apps, and SaaS workloads. Their combined offerings provide many features and capabilities (see Figure 2) to meet the protection-related demands of both traditional and cloud-native workloads, with components that include:

- Integrated support for VMware workloads through Google Cloud VMware engine and Dell PowerProtect Data Manager to ensure protection of VMware virtual machines and VMware Tanzu Kubernetes containers.
- Features that support the unique needs of cloud-native protection, with support for Google Anthos and all the major distributions of Kubernetes.
- The use of Google Cloud object storage to deliver increased data protection efficiencies.
- Integrated cloud snapshot management to simplify management of Google cloud storage snapshots.
- SaaS workload protection, including Google Workspace, M365, and Salesforce.com, to ensure vital SaaS data is protected and recoverable.
- A cyber-recovery offering using an isolated digital vault in Google Cloud to protect mission-critical data from ransomware attacks and similar cyber-threats.

[3] Source: ESG Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022.

Figure 2. Six Essential Capabilities for Google Cloud Data Protection from Dell Technologies


1
Protection for traditional and re-platformed workloads
2
Strong data protection for Kubernetes and containers
3
Support for VMware on Google Cloud
4
Integrated data protection and cyber resiliency—digital vault with recovery workflows to simplify recovery
5
Substantial levels of automation to simplify operations and improve protection
6
Adherence to three key tenets: performance, scale, and efficiency

Source: ESG, a division of TechTarget, Inc.

Those capabilities are only the beginning. The technology will keep evolving to accommodate an environment marked by constant data growth, IT skill-set scarcity, and frequent launches of new data-centric services. The future will see additional, deeper integration between cloud services and data protection solutions, with more automation to simplify daily operational tasks performed by overburdened IT staff.

The Solution Components of Dell Cyber-resilient Data Protection for Google Cloud

The partnership between these two leading vendors to provide comprehensive data protection for traditional workloads and cloud-native apps alike is an outgrowth of their combined leadership in supporting cloud-native environments. Google engineers created Kubernetes. Google also provides GKE, a fully managed environment for cloud-native apps, and it continues to contribute to the open-source community. It has a best-in-class services organization to help with all aspects of cloud-native projects—enabling organizations to extend their VMware operations into the cloud while enjoying the same operational experience as they do on-premises with Google Cloud VMware Engine.

Similarly, Dell, an end-to-end IT solutions provider, provides integrated IT infrastructure and software-defined solutions and services that enable organizations to rapidly develop, deploy, protect, and secure cloud-native applications across hybrid, multi-cloud environments.

The enhanced data protection solution from Dell for Google Cloud fully protects the containers and microservices that are the foundation of cloud-native applications. As noted, it protects both data volumes and metadata, and it can protect dynamically changing apps. These capabilities supplement the protection it offers for the unique needs of microservices and Kubernetes environments. Furthermore, Dell data protection solutions for Google Cloud deliver increased automation, thereby providing better protection while placing fewer demands on busy administrators. Automation ensures more consistent, effective protection by eliminating human errors that can occur during data protection-related activities.

For example, Dell PowerProtect Data Manager is a unified platform for protecting a wide range of mission-critical enterprise workloads. The solution includes extensions developed to protect multi-workload environments running on self-deployed Kubernetes clusters. PowerProtect Data Manager provides enterprise-grade protection for Google Cloud workloads without the need to manage additional infrastructure. It supports hybrid and multi-cloud data protection use cases such as backup to the cloud, backup of workloads in the cloud, disaster recovery to the cloud, and long-term retention to the cloud with migration on-premises to the cloud and back.

Dell provides cyber-resiliency capabilities across multi-workload environments to help organizations maintain fully operational status after cyber-attacks. Another benefit stemming from the breadth of Dell's cloud data protection portfolio is the ability to protect SaaS workloads with APEX Backup Services. Using one solution across many different SaaS apps not only provides more consistent protection, but also reduces demands on IT staff.

Additionally, Dell Cloud Snapshot Manager has been enhanced to protect cloud-native applications. Now IT can use a single tool to discover, orchestrate, and automate the protection of Google Cloud workloads using tag-based policies. Cloud Snapshot Manager provides global visibility and control to deliver data protection across an entire cloud infrastructure.

Lastly, a noteworthy financial-related benefit is that organizations can acquire Dell cloud data protection solutions directly from the Google Cloud Marketplace. Moreover, these purchases can be made with pre-committed spend with Google Cloud, reducing that commitment while gaining a valuable solution. This approach both improves cost efficiency and simplifies purchasing.

The Bigger Truth

An inability to protect newer types of workloads such as containers and cloud-native applications reliably and consistently can weaken business resiliency and impede digital transformation efforts. The Dell solution for Google Cloud ensures that today's emerging cloud-native apps are protected, even giving the data owners (i.e., developers) the flexibility to protect their own workloads through self-service capabilities, APIs, and tagging, while IT operations staff retain an oversight role to ensure SLAs will be met.

Dell and Google are enterprise-class partners, offering a better way to protect cloud-native applications. Google delivers next-generation cloud-native services, components, and offerings that organizations are using to build these new apps:

- Dell cloud data protection solutions bring performance, scale, and efficiency to data protection for cloud-native apps and microservices environments.
- It is now possible to protect multiple workload types (VMs, containers, cloud-native apps, and SaaS) in the cloud leveraging Dell cloud data protection solutions.
- Dell cloud data protection solutions improve operational efficiency, resiliency, and scalability while reducing the total cost of ownership by up to 81%.[4]

Collectively, these are enhanced data protection offerings designed from the outset by Dell and Google to support the numerous unique protection demands of modern, cloud-native applications. Organizations already leveraging these partners' platforms or looking to improve their data protection and resiliency position by using them should investigate whether these Dell and Google solutions might provide substantial benefits to their business.

[4] Source: ESG Economic Validation commissioned by Dell Technologies, *Understanding the Economics of In-cloud Data Protection: A Dell Technologies Data Protection Solution Designed with Cost Optimization in Mind*, September 2021.

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