ESG a division of TechTarget Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Simplifying and Modernizing Data Protection Solutions

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

ABSTRACT: Against a backdrop of intensified growth in data volumes and the growing complexity in IT architectures and increased cyber-threats, organizations must simplify the process and experience of modernized data protection. Protection of modern workloads, operational and cyber resilience, and simplified deployment and operation with a unified user experience should be the hallmarks of organizations' data protection frameworks. Organizations need to think long and hard about their strategies for protecting and securing data in an era when even a momentary lapse can result in major financial, operational, and brand reputation losses. Midsize organizations are particularly vulnerable since they share common challenges with their larger counterparts but often lack the resources necessary to combat data protection threats or have a dedicated data protection team. Organizations should consider integrated hardware/software appliances that reduce data protection complexity, increase operational resilience, and protect modern workloads.

Introduction

All organizations have long understood that the more they rely on digital data, the more risk they face. That risk takes many forms: financial, operational, customer relationship, legal, regulatory, and more, and the price tag of those risks can be staggering.

The sources of risk are also well understood: Human error, infrastructure failure, and cyber-threats have always been present. More recently, new sources of risk that must be addressed by data protection methods and solutions have sprung up, including massive growth in data volumes, the potential of lost mobile devices, malicious insider attacks, and the growing prevalence of remote and hybrid work.

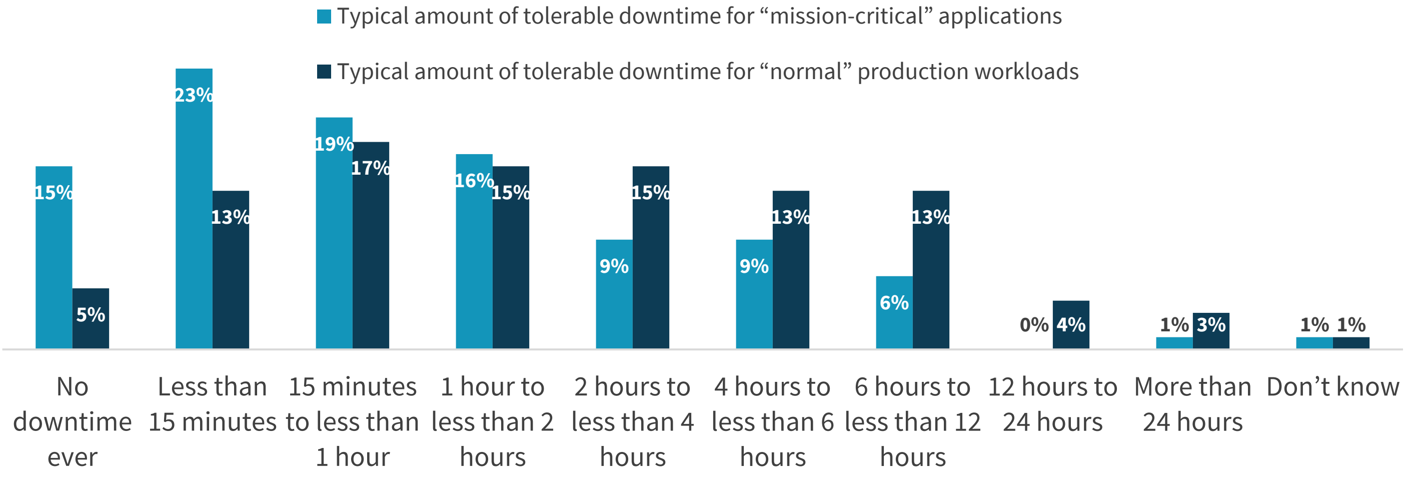
Today's data protection challenges are further exacerbated by the introduction of modern application workloads that often require hybrid architectures and frequent workload migration. Even the very nature of backup—a widely acknowledged core data protection function—has undergone huge transformation. Gone are the days when backups could be done incrementally at the end of a day when systems were normally unavailable for "maintenance" and when backup volumes were small enough to be done easily on streaming tape, mirrored hard drives, or removable media.

Data protection also has become more problematic due to the large and growing skills gap, both for IT overall and for specialized functions such as data protection and cybersecurity. Organizations no longer have the luxury of leveraging "PhDs in backup," if they ever had. Instead, many organizations rely on IT generalists to handle everything from backup and recovery management to sophisticated cybersecurity defenses. This is particularly acute in mid-sized organizations, most of which lack dedicated and experienced resources for data protection functions such as backup, recovery, archiving, data management, security, and more.

Of course, the harsh reality is that failing to adequately address operational resilience and IT complexity makes data protection more difficult, and the impact of service interruptions and downtime on the organization is even more onerous. Enterprise Strategy Group (ESG) research notes that organizations are heavily concerned with the impact of downtime, especially for mission-critical workloads. Respondents said that their organizations typically can only accept an average of 2 hours' downtime for mission-critical applications, and an average of just 4 hours for normal production applications. And the majority of respondents (57%) said their organizations can only tolerate less than 1 hour of downtime for mission-critical applications.[1]

Figure 1. One Hour Can Be a Long Time

What is the amount of downtime your organization can tolerate from servers running "mission-critical" applications/workloads before making the decision to "fail over/recover" to a BC/DR secondary site or service provider? What is the amount of downtime your organization can tolerate from servers running "normal" applications/workloads before making the decision to "fail over/recover" to a BC/DR secondary site or service provider? (Percent of respondents, N=378)



Source: ESG, a division of TechTarget, Inc.

ESG research also points out another source of complexity for data protection—the accelerating migration of mission-critical workloads to the cloud. 58% of those essential applications now are operated/run in some kind of cloud environment.[2] With all of these issues impacting an organization's ability to properly protect their data and ensure operational and cyber resiliency, it is no wonder 57% of organizations expect to spend more money on data protection in 2022 than they did in 2021.[3]

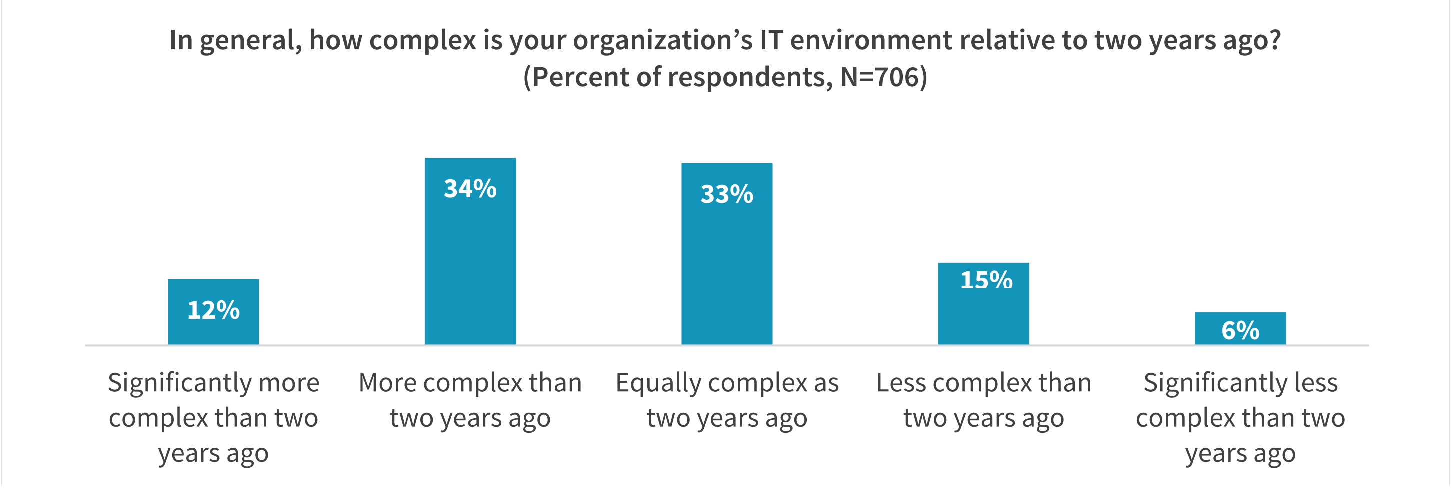
[1] Source: ESG Research Report, *Real-world SLAs and Availability Requirements*, October 2020.
[2] Ibid.
[3] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

Taking Complexity Out of Planning and Building a Modernized Data Protection Framework

Organizations looking to modernize their data protection strategies and solutions should understand and embrace the notion that, while each organization's priorities will be different, there are a number of common functions that are integral to achieving data protection goals.

A key issue that must be top-of-mind for those planning data recovery and business continuity is the imperative to reduce IT complexity. For instance, ESG research indicates that 46% of organizations believe IT is more complex than it was two years ago, compared with just 21% that believe it is less complex (see Figure 2).[4]

Figure 2. Nearly Half of Organizations Believe IT Is More Complex than Two Years Ago



Source: ESG, a division of TechTarget, Inc.

ESG research points out that, while protecting applications and data is obviously at the top of the list of data protection priorities, issues such as data recoverability and ensuring multicloud protection are important, as well.[5]

ESG research also highlights cloud-based data protection functionality as an important and efficient way for organizations to extend their traditional on-prem-based backup/recovery/restore infrastructure capabilities.[6]

Therefore, a modern data protection strategy should include a combination of important traits. These include:

- Simplification of deployment in what has become a hybrid infrastructure. Organizations just don't have the resources to assemble a "puzzle," and they need data protection solutions that work right out of the box.
- Ease of use across a variety of topologies and environments, in the context of growing data volumes and an increasing reliance on unstructured data.
- Support for key mission-critical workloads and platforms to deliver against data protection service-level agreements and the ability to limit business risk and impact should a data loss event occur, including in the context of cyber-attacks.

[4] Ibid.
[5] Ibid.
[6] Source: ESG Research Report, *Real-world SLAs and Availability Requirements*, October 2020.

- The need to leverage cloud technology for enhanced disaster recovery beyond the data center, in particular modern software as a service (SaaS) management options.
- Multiple ways to "consume" the technology in a flexible fashion, including type of deployment, payment/budgeting models, and ongoing support and service-level agreements.

Dell's Newest Data Protection Solution: PowerProtect Data Manager Appliance

Since data protection has taken on an even more strategic importance for all organizations, it is imperative that decision makers focus on selecting not only the best tools and services, but also the best technology partner that can help protect all their digital assets well into the future. Organizations should identify and work with technology partners that have an extensive array of solutions that can be utilized in numerous architectures and that have a track record of high-quality service and support.

That's where leveraging an architecture partner like Intel is also key. As organizations strategically invest in modernization of their data centers and servers, Intel architecture-based platforms can help in achieving the performance and reliability modern IT needs from compute, to network, to memory, and to accelerator technologies.

Dell Technologies has long been a leading supplier of infrastructure solutions and has extensive experience helping organizations plan, deploy, and manage their infrastructure for optimal data protection. Dell offers a number of options for data protection, including software-only solutions that can be deployed on premises or in the cloud; purpose-built appliances in both physical and virtual formats; integrated appliances, for either on-premises infrastructure or in leading cloud platforms such as Amazon Web Services, Microsoft Azure, or Google Cloud; or as a SaaS-based cloud solution.

Dell PowerProtect Data Manager Appliance is an integrated data protection solution representing a simple and flexible way to experience Dell PowerProtect Data Manager software functionality. It is aimed at midsize organizations that have enterprise-class data protection challenges but need a less-expensive, lower-capacity solution.

The appliance was engineered to align with the most significant requirements for modernized data protection:

- It is modern and relies on a software-defined architecture protection of existing and newer workloads.
- It has reliable, scalable security for both operational and cyber resilience.
- It is designed with simplicity in mind for easy deployment and usage, delivering a unified user experience in management, self-service backup and recovery, centralized governance, and role-based access control.

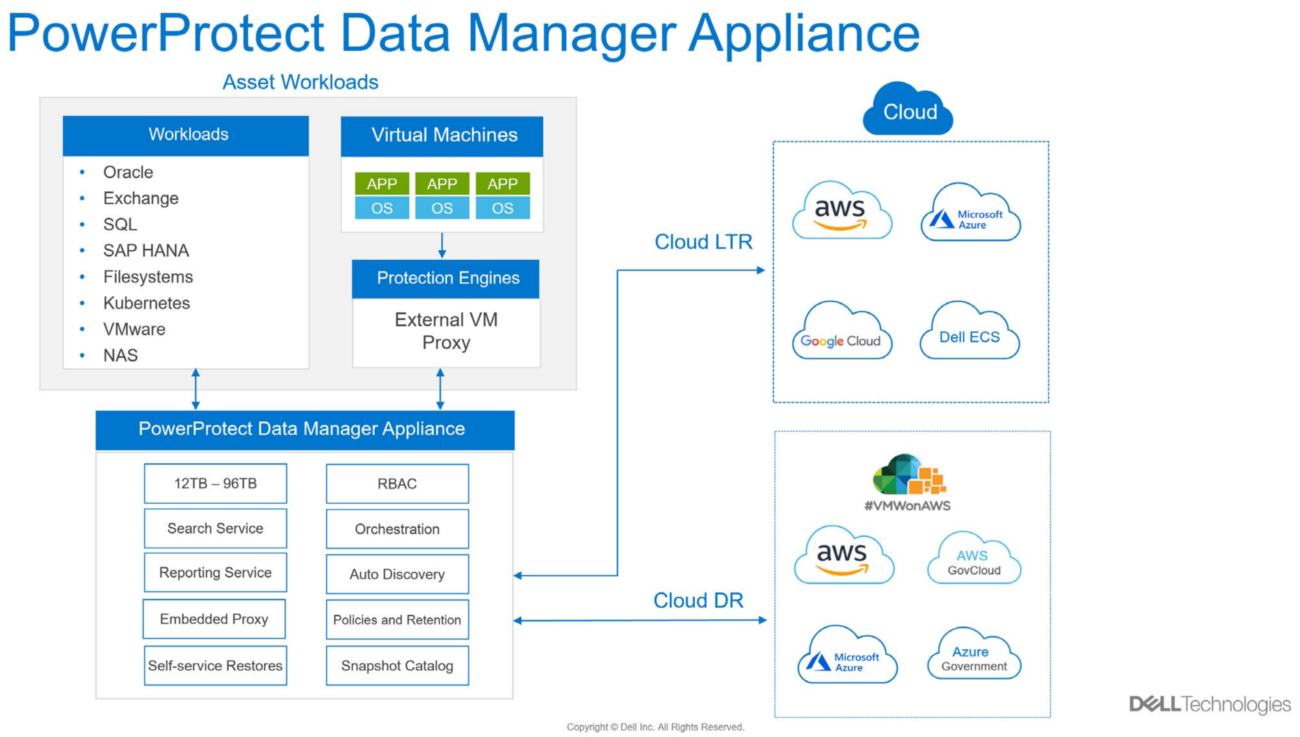
Dell PowerProtect Data Manager Appliance is based on scale-up architecture to ensure data protection can keep up with organizations' inevitable growth in data volumes. It also supports cloud-native workloads that are becoming more important in mid-range enterprises, such as Kubernetes, SAP HANA, and VMware environments, as well as essential enterprise applications such as Oracle, Exchange, SQL, and Linux/Unix file systems.

Other important data protection features include:

- Transparent Snapshots ensures availability of VMs at scale for near-zero impact to VMs or VM resources.
- Instant Access/Instant Restore of VMs with minimal operational disruptions, allowing VMs to boot and run directly on the appliance and restore back to the primary location when ready.

- Single sign-on to the appliance with role-based access control, without compromising security.
- Simplified management, monitoring, and reporting.

Figure 3. PowerProtect Data Manager Appliance



PowerProtect Data Manager Appliance

Asset Workloads

Workloads
- Oracle
- Exchange
- SQL
- SAP HANA
- Filesystems
- Kubernetes
- VMware
- NAS

Virtual Machines

APP APP APP
OS OS OS

Protection Engines

External VM Proxy

PowerProtect Data Manager Appliance

12TB – 96TB
Search Service
Reporting Service
Embedded Proxy
Self-service Restores

RBAC
Orchestration
Auto Discovery
Policies and Retention
Snapshot Catalog

Cloud LTR

Cloud DR

Cloud

aws
Microsoft Azure
Google Cloud
Dell ECS

#VMWonAWS
aws
AWS GovCloud
Microsoft Azure
Azure Government

Copyright © Dell Inc. All Rights Reserved.

DELL Technologies

Source: Dell Technologies

The Bigger Truth

The data protection challenges associated with sustained, rapid, and ceaseless data growth, combined with growing IT complexity, are expanding faster than most organizations can keep up. Organizations are craving a simpler approach to data protection in order to overcome the many innate challenges they face. All organizations—but especially fast-growing midsize entities—need a powerful, yet simple and affordable set of data protection options.

The core of a modernized data protection framework must be built around three key principles:

- Modern (flexibility achieved with a software-defined architecture, which enhances flexibility and ease of use and deployment for end-users while also providing a future-proof investment as workloads and capabilities evolve over time).
- Secure (fortifying the organization with operational and cyber resilience).
- Simple (supporting a unified user experience to juggle the need for reduced user friction and increased protection and resilience).

Dell is a leading player in the data protection market segment, offering a wide array of solutions designed to meet the individual needs of different types of organizations. Dell PowerProtect Data Manager Appliance simplifies the experience of adopting modern data protection with an integrated solution that is easy to deploy and simple to configure. The appliance uses Dell PowerProtect Data Manager software to provide a modern software-defined architecture, secure operational and cyber resilience, and a simple, unified user management experience. Organizations looking to modernize their data protection infrastructure should consider evaluating the Dell PowerProtect Data Manager Appliance.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

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