# Policy-Driven Management:
## Simplify, Automate VM Data Protection

**How well protected is the data in your virtual machines? In today's rapidly changing IT environment, many IT professionals have a difficult time answering that question. The combination of VM sprawl and a proliferation of data protection strategies—all managed by multiple teams—leaves ample opportunity for data protection to simply fall through the cracks.**

This paper looks at the issues that impede the protection of data for all VMs and highlights storage policy-based management solutions that can both simplify the overall management burden and ensure that every VM's data is protected from instantiation to deletion.

## The data protection struggle

The use of server virtualization continues to grow at a strong pace, with the global virtualization market expected to reach more than $9 billion by 2026.[1] In today's data centers—whether on premises or in the cloud—server sprawl has been replaced by VM sprawl as VMs spin up to meet the demand for new, modern applications that impel businesses of all kinds forward. If "there's an app for that,"

[1] "Server Virtualization Market Size and Forecast," Verified Market Research, March 2020

TechTarget | Custom Media

DELL Technologies

there's also a VM for that, as organizations increasingly see the value of isolating applications in VMs, rely on cloud-based VMs for an increasing amount of their IT needs, and even deploy containers on VMs for greater agility and deployment flexibility in today's hybrid IT environments.

This VM sprawl has introduced another type of uncontrolled growth: tool sprawl. That happens when different entities within an organization increasingly utilize unique tool sets to create, manage, protect and secure the VMs that power their departments and the applications they support. In large part, this is because protection of a VM's data is performed separately from VM management tools. There is little or no integration between VM data protection and other VM lifecycle products, so VMs can be instantiated, run and taken down without data protection, often with no one realizing the number and scale of unprotected VMs across the organization.

When it comes to VM data protection, you can't protect what you don't know about, as the old adage goes, and there is a disconnect at the center of VM data protection. Storage or backup administrators often are not informed when new VMs are created, and so they rely on a set of discovery tools that will hopefully uncover all the new VMs so they can initiate protection protocols for them. It is this lack of coordination between development and operations teams and the backup admins that creates opportunities for data protection for a wide range of VMs to simply fall through the cracks. Consequently, these unprotected VMs, caused by a lack of integrated VM protection, can lead to workflows being put at risk for data loss.

## When VMs are unprotected

When VMs are created without a data protection strategy, storage and backup admins down the line are forced to use large nets to "catch" those newly instantiated VMs, and only then can they begin to create a data protection plan for them. However, this is a manual approach that can go only so far. As the scope and number of VMs continue to grow, it becomes increasingly difficult to ensure that every VM is in fact discovered and its data protected from loss or failure.

At enterprise scale, even the best laid plans for protecting VM data after the fact will have gaping holes in the nets used to catch new VMs and protect them after creation.

## Business impacts are far ranging

What are the risks if every VM instance is not properly protected and its data secured?

- Should data become lost or unrecoverable, downtime could result, leading to lost productivity, as workarounds must be created to compensate for the loss.
- Efficiencies are lost as employees are forced to turn from business-focused, customer-facing tasks to the unpleasant chore of re-creating business-critical data sets.
- Regulatory and governance penalties for data loss can skyrocket in today's alphabet soup of regulations,

including PCI, HIPAA and GDPR. GDPR, in particular, can be financially burdensome, with penalties running into hundreds of million dollars for a single loss.[2]

- Finally, in today's era of instant gratification, a downed application or function can lead customers to abandon a supplier for its competitor in a flash. Thus, there is a cycle of loss—first of the application availability, then of goodwill and finally of customers—all stemming from a VM's unprotected data.

## What enterprises want

When evaluating a VM data protection solution, it is important to keep in mind some key factors for a successful implementation. First, a VM data protection strategy must simplify the overall management burden for storage and virtual infrastructure (VI) admins as well as for the VM creators. There must be assurances that protection of VMs will occur automatically, ideally via policies that define the data protection to ensure that important data sets will be secured.

Critical to success is the ability to have data protection already defined when VMs are created, eliminating the need for a separate data protection process. Furthermore, the solution should offer simple data protection monitoring that extends throughout the entire VM lifecycle, from instantiation to retirement.

Ideally, self-service tools should also be available for VM owners and VI, storage and backup admins to perform ad hoc backups if and when needed. Finally, to further simplify data protection for VMs, the ideal platform will include all of the above integrated right into vSphere—all in one policy-driven tool.

## Introducing policy-driven storage by Dell EMC PowerProtect Data Manager

Working closely with VMware, Dell Technologies crafted a solution that provides for all these demands: Dell EMC PowerProtect Data Manager. By taking the guesswork out of VM data protection, Data Manager offers native vSphere integration of Data Manager policies with VMware storage policies.

Now, thanks to the tight vSphere integration of vCenter and Data Manager, VI, storage and backup admins as well as VM owners can choose a storage policy that will be applied to every VM automatically when it is instantiated—with no intervention needed. Data Manager also includes powerful monitoring tools to ensure compliance and governance mandates are being met and to ensure that desired protection is in place. Should a loss occur, Data Manager applies a persistent, continuous policy association even after VM recovery to ensure smooth, uninterrupted operations.

The result is the simplification of VM infrastructure, with integration of VM data protection from inception. In this manner, data protection is no longer an afterthought but a part of the VM lifecycle, whether the VMs reside on premises, in the cloud or in a hybrid environment.

## Why Dell EMC PowerProtect Data Manager?

Thanks to the long relationship between Dell and VMware, Data Manager is a tightly integrated, highly tuned joint offering. It leverages Dell's decades-long data protection expertise, enabling organizations to offload all the complexity while maintaining the richness of offering that Dell's partners and customers have come to expect.

This "best of both worlds" solution—proven and modern—is the only VM data protection solution that vSphere users will ever need, with set-and-forget automation that ensures confidence that protection will always be there when needed.

## Next steps

**Visit Dell Technologies at www.DellTechnologies.com/DataProtection to learn more about Dell EMC PowerProtect Data Manager.**

[2] "GDPR: The 6 Biggest Fines Enforced by Regulators So Far," Secure Privacy, Jan. 20, 2020