ESG SHOWCASE

Simplifying VMware Multi-Cloud with VMware Cloud Foundation on Dell VxRail and Dell PowerProtect Data Protection

Date: February 2022 **Authors:** Paul Nashawaty, Senior Analyst; and Christophe Bertrand, Practice Director

ABSTRACT: When it comes to transforming IT with a multi-cloud approach, organizations must think about more than ease of use and deployment. They must also ensure that both the platform and its workloads are adequately protected against data loss and cyber-exposure. This becomes more necessary at scale and across traditional and modern workloads, whether data is on-premises, at the edge, or in the cloud. That's where the all-in-one solution from Dell Technologies comes in: It is a highly integrated solution that combines VMware Cloud Foundation (VCF) on Dell VxRail Hyperconverged Infrastructure (HCI), commonly referred to as VCF on VxRail with Dell PowerProtect Data Protection.

Market Landscape

Data Protection Is Key

IT organizations have very low tolerance for data unavailability. ESG research shows that 15% of organizations tolerate no downtime at all for their mission-critical applications, while another 42% say that their mission-critical applications must be back online in less than one hour. In addition, RPOs are very stringent, with 15% aiming for no mission-critical data loss at all.[1]

Downtime is not just a technical issue; it is a business problem. In fact, downtime has significant economic, operational, and legal impacts. For example, one in five survey respondents cite the diversion of IT resources from other business-critical projects as the potential downtime impact that concerns them most.[2]

… Against a Backdrop of Increased Cyber Risk

Recent research from ESG shows that almost two-thirds (63%) of organizations surveyed reported attempted ransomware attacks in the past 12 months, with 36% reporting ongoing, frequent attempts on a monthly basis or more frequently. Nearly half (48%) of all respondents reported being the victim of a successful ransomware attack.[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.

It should therefore be no surprise that 82% of organizations are more concerned about ransomware today than they were two years ago, and 67% of them are escalating the conversation to the executive level. This is happening in the context of severe skills shortages, with 48% of organizations reporting a shortage of cybersecurity skills.[4]

Ransomware resilience includes deploying a variety of technologies and processes, among which is the ability to recover from a last good known copy or backup. Implementing data-recoverability capabilities for cyber-resilience is top of mind for IT decision makers, with 47% indicating that it is one of the areas of data protection in which they expect to make the most significant investments over the next 12 to 18 months. And when it comes to the infrastructure, 79% of organizations use substantial edge deployments.[5]

Figure 1. Key Data Points

Source: Enterprise Strategy Group, Inc.

The large threat landscape, coupled with the software-defined nature of the platform under discussion (VCF on VxRail), means that it is even more critical for organizations to protect both the workloads *and* the platform.

Picking the Right Infrastructure Deployment Model Will Help

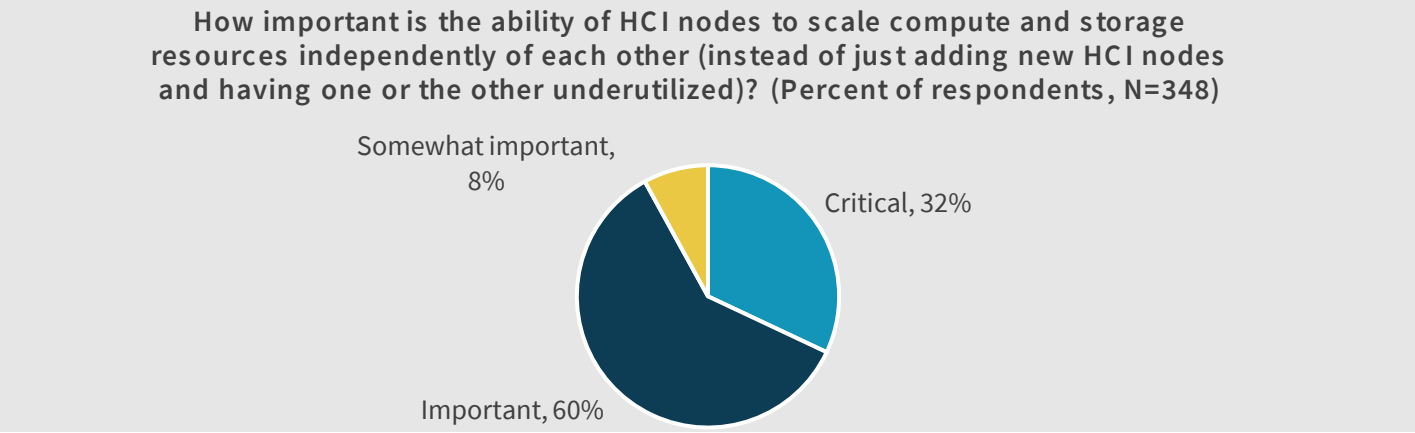
When considering the right infrastructure, organizations should consider simplifying and controlling data and costs by simplifying and optimizing hardware and software deployments. Infrastructure would include compute, memory, storage, network, virtualization, software, integration, and lifecycle stack.

And when considering these components, it is equally important to understand the importance of scale. VCF on VxRail takes advantage of the unique VxRail HCI System Software to extend native VMware capabilities, simplifying and automating infrastructure and cloud management into a single curated system. VxRail also supports multi-dimensional scale with the ability to add compute and storage independently to support different workloads. VxRail is the only jointly engineered system with deep VMware Cloud Foundation integration, meaning both the hyperconverged infrastructure layer and VMware cloud software stack are managed as a turnkey hybrid cloud experience.

Notably, ESG research has identified that independent scaling of necessary resources in the HCI cluster is important or critical for 92% of IT organizations (see Figure 2).[6]

[4] Source: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.
[5] Ibid.
[6] Source: ESG Survey Results, *Hyperconverged Infrastructure 2.0*, October 2021.

Figure 2. Scaling HCI Compute and Storage Resources



Source: Enterprise Strategy Group, Inc.

In essence, driving transformation using a modern hybrid cloud platform will eliminate IT silos on-premises and in the cloud. HCI platforms and clusters will interact from the core to the edge. In an ESG research survey, 23% of respondents indicated that they are running 100 to 500 edge locations, with 30% indicating that they expected to be managing 500 to 1,000 edge locations 24 months from now.[7]

Platform automation between components in the infrastructure and the business requirements governing it are dependent on the application delivery process. Many parts of the organization are impacted and will benefit from automation between components. A good example is the DevOps team that constantly seeks more performance and quality and needs the right infrastructure to do so. According to ESG research, 38% of respondents indicated they employ DevOps extensively.[8] This includes, to some extent, the automation of the CI/CD pipeline.

Dell Delivers on the Need for a Simple and Fast Path to a Protected VMware Multi-Cloud

Backup and recovery success is not always a guarantee, resulting in significant impact to business-critical applications. Alternative technologies have proven to be limited when met with scale or rapidly growing environments. Organizations report that on average they can only successfully backup and restore 77% of on-premises VMs (meaning backups are complete without errors and VMs and associated data can be restored).[9]

Protecting applications and workloads with a traditional approach often requires multiple vendors, resulting in risk, cost, and operational complexity (in turn generating more manual processes). The net result is fewer recovery points, slower backups and recoveries, missed key SLAs, and, therefore, heightened business and cyber-recovery risk.

Organizations, therefore, need a modern and integrated approach, one that focuses on hybrid multi-cloud and may include containerized workloads such as VMware Tanzu, while providing significant levels of automation to protect the platform itself and its associated workloads. This is especially necessary in the context of cyber-resilience and adequate preparation for cyber-recovery.

This is where the Dell approach stands apart with its complete PowerProtect data protection portfolio, which was designed to be a comprehensive and unified solution to run and protect traditional and modern workloads. It is a "one-stop shop"

[7] Source: ESG Survey Results, *Hyperconverged Infrastructure 2.0*, October 2021.
[8] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.
[9] Source: ESG Research Insights Paper commissioned by Dell Technologies, *Data Protection Trends in Virtual Environments*, February 2020.

for multi-cloud data protection of VMware environments, with deep VMware integration, certification, high performance, and automation at scale. All this is in support of multi-cloud solutions from VMware.

However, robust protection of all applications, both traditional (VM-based) and modern (containerized workloads), is not enough. Robust data protection today also means protecting the platform itself. To provide the solution, Dell teams have worked in conjunction with VMware to ensure the platform protection is robust, yet simple. In the context of the Dell and VMware offerings, this specifically includes the VxRail Manager components and VMware Cloud Foundation components. This platform protection is coupled with workload protection integration that provides simplified self-service data protection and administration through VMware native interfaces. In turn, this enables VM administrators to take charge of their data protection needs, even leveraging automated runbooks for multi-cloud/hybrid recoveries when needed.

A good recent example of innovation for backing up VMs at scale that deserves special attention is the use of Transparent Snapshots, available with PowerProtect Data Manager. Dell Technologies recently introduced this new snapshot technology to specifically help protect workloads, with simplicity and performance as the design point. The solution is automatically placed on new ESX hosts without any additional work. The solution does not require a reboot or use of maintenance mode on ESX. As VMs are added and need to be protected, Dell Technologies makes sure deployment occurs. It has a near-zero impact on VMs and ESX overhead alike, without using proxies. In other words, data is backed up without business disruption with minimal production impact. Dell claims that Transparent Snapshots delivers up to 5x faster backups and 5x reduction in VM latency compared with traditional VM backup methods.

Simplifying VM backups allows workloads that previously were not backed up often, or ever, because of potential business disruption to be backed up regularly. And, in turn, it enables more recovery points, which can be critical for cyber-recovery.

The Bigger Truth

As IT complexity and data volumes continue to grow from core to edge, IT leaders must consider new ways of simplifying deployments of their infrastructure while building resilience in, not only for the workloads, but also for the infrastructure itself. The complexity of multi-vendor IT "infrastructure puzzles" has become untenable.

This is becoming an even more pressing need, as ransomware threats are rampant. In this new era of cyber-resilience challenges, the new norm should be to deploy integrated and more operationally efficient infrastructure with built-in resilience.

The new reality is that organizations need to protect critical infrastructure configuration and should consider it a best cyber-resilience practice. What good is data that can't run on anything? If you don't protect the key components that make the software-defined infrastructure work, you can't restore your workloads successfully!

In the context of the integrated Dell and VMware solution, each VCF on VxRail deployment is essentially a fully protected cloud platform component. Operationally, having a highly integrated cloud platform with data protection that is also highly integrated with VMware simplifies deployment, eliminates management complexity, and reduces costs, creating a simple and fast path to a protected multi-/distributed cloud.

At the end of the day, a simple rule of thumb for IT professionals deploying infrastructure is to remember that "if you can't protect it, you can't deploy it!" The Dell solution allows customers to run *and* protect traditional and modern workloads wherever they live—without the need to source infrastructure components from multiple vendors. It should be on every IT professional's shortlist of solutions to consider.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188