White Paper

Five Considerations for Increasing the Availability of the Always-on Business

By Jason Buffington, Senior Analyst; and Monya Keane, Research Analyst

May 2014

This ESG White Paper was commissioned by Veeam and is distributed under license from ESG.

Contents

Executive Summary

"*How do we successfully back up a highly virtualized environment*?" That's no longer a new question, although IT organizations of all sizes continue to struggle with it.

- For example, terms have evolved from "*highly virtualized*" to "*modern data center*" because it really is inconceivable now to be both modern and predominantly physical. Yes, almost inevitably, physical servers will reside in most environments, but evolutions in IT are related squarely to highly virtualized platforms that are most often supported by advanced storage solutions and deployed across private, public or hybrid clouds.
- Similarly, we don't (or shouldn't) think in terms of "*backup.*" At a minimum, we should think "*data protection*" as the method, but the real goal is "*ensuring availability*" to data servers and services. Technology options and vision-centered mindsets have evolved. Backup is part of the story, but the focus truly is on ensuring availability through fast recovery and whatever other means are necessary to cost-effectively achieve an 'always on' data center.

Collectively, one should then ask "*What can be done to enhance the availability of an always-on datacenter*?"

So, while the terms have changed, one thing hasn't: Veeam as a technology leader and mindshare dominator in the discussion. In early 2014, ESG was contracted by Veeam to solicit the perspectives of 791 Veeam Backup & Replication customers. The effort centered on pinpointing why these users chose to deploy a data protection product to augment their data protection infrastructure. Why did they feel the need to supplement their legacy backup mechanisms with Veeam? The project explored the sentiments of these users toward Veeam, in contrast to their feelings about their earlier attempts to back up VMs in a growing IT infrastructure using other methods.

Introduction: New Needs Are Prompting New Technology Investments

Right now, quite a few IT organizations are on journeys toward creating and operating a *modern data center*—an IT infrastructure that is highly virtualized, leveraging multiple hypervisors across multiple hosts that are utilizing high-performing storage and networking underpinnings, including on premise and/or cloud-based infrastructures.

A contemporary data center might look like a large enterprise's traditional, raised-floor environment, or it might take the form of a couple of server racks tucked in a midsize company's back-room closet. Regardless of its actual size or number of servers, it can be cutting-edge modern. And because these modern infrastructures are so highly virtualized, they provide an IT organization with a number of benefits. For example:

- The organization can better utilize its existing IT resources (nice because no one has CapEx to spare).
- The whole environment is more manageable in general (also good because no one has OpEx to spare).
- Staff can do more with less (a circumstance everyone in IT strives for).
- Admins can "move around" platforms, applications, and other infrastructure elements much faster (and thus much more efficiently with potentially higher resiliency).

But with those benefits come challenges:

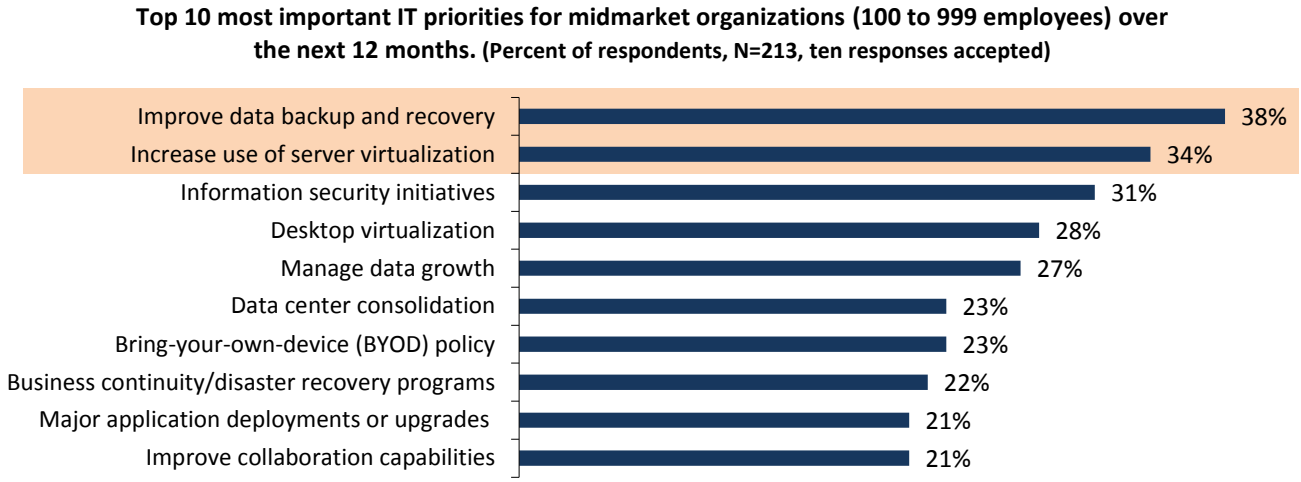
- Less tolerance to downtime due to dependency upon data.
- Lower tolerance for poor/legacy engineering due to the consolidation of many more key systems per actual hypervisor host and its pool of resources. CPU spikes and big, "lazy" backup windows are not acceptable.
- Huge increases in storage due to growing data sets, as well as VM sprawl in production. That growth results in the need for even more storage to back it all up, and then replicate it again for disaster preparedness.

Whether it lives in a big glass house or on a small shelf, a modern data center is able to offer agility because it is enabled by virtualization. With that fact in mind, what must IT do to ensure the availability of those data center resources? A new kind of data center needs a new kind of data protection, the kind that can enable an "always-on business." Without good protection, even an otherwise modern data center will be incomplete, and the organization won't get the full benefit of its modernization investments.

What Are Your Goals and Priorities?

Adequate VM backup is nothing to get excited about. The process is too highly prioritized to settle for just "adequacy." Improving data backup and recovery and increasing the use of server virtualization both continue to be cited by many IT pros, especially those in midmarket organizations, as priorities for them this year (see Figure 1).[1] Even across both midsize *and* enterprise-scale companies, **increasing server virtualization** ties as the most-often stated priority this year, while **improving backup and recovery** is the third most-often cited priority overall.

Figure 1. Midmarket Organizations' Top IT Priorities for 2014



Source: Enterprise Strategy Group, 2014.

As mentioned, those two priorities—backup and recovery and server virtualization—are coupled tightly from an operational perspective. Midmarket organizations in particular struggle to keep up with protecting this kind of evolving, maturing infrastructure. They need *innovative* mechanisms. That is why virtualization-specific backup solutions such as Veeam's are prospering in the marketplace. They help IT to:

- Raise system availability by reducing downtime to near-zero.
- Protect increasing amounts of data.
- Access data and applications any time and from anywhere.

An investment in a modern data center is incomplete without an upgrade to its data protection capabilities.

> As Veeam's marketers like to put it, "*You cannot enable an always-on business with legacy backup*."
>
> Said differently, *if you are going to put all your eggs in one basket, it better be a highly available basket*.

It seems that IT organizations actually have suffered repeated bad experiences with the legacy solutions, especially regarding reliability. So, they have definitely begun taking protection-related considerations into account.

Five Considerations for Increasing the Availability of a Modern Data Center Through Better Protection

To achieve better overall availability, you need to have a comprehensive data protection solution. Most IT organizations already have some traditional or "unified" backup solution today—one that claims to back up VMs just as well as it backs up physical servers. But if that is the case, then why are so many IT departments buying a solution from a completely different backup vendor that only backs up virtual machines as part of ensuring their systems' availability?

[1] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.

To answer that question, ESG looked at its industry-wide research on virtualization-protection challenges, and then it compared those results with responses from 791 Veeam customers. The remainder of this paper sheds light on the five factors that appear to lead to a decision to introduce virtualization-specific data protection into a modern IT environment. Those factors center on:

- How *confident* you are in your backups and your ability to restore.
- The fact that your availability is largely based on how *fast* you can recover.
- How well you're *really* protected.
- Whether you'll be able to *see* whether you are protected or not.
- How else you can *avoid risk*.

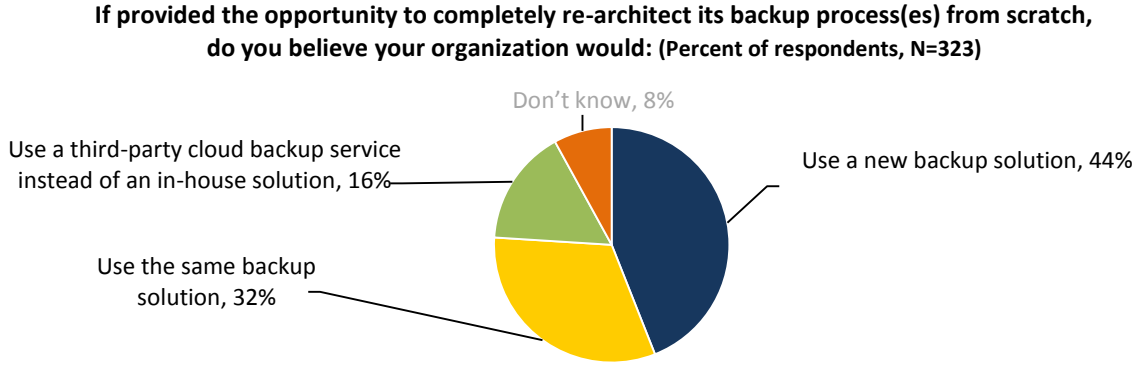
Each driving factor uncovered by the Veeam user survey is prefaced by existing ESG research on related market trends, with that data tying back to the experiences reported by the Veeam users.

CONSIDERATION ONE: How Confident Are You in Your Backups and Your Ability to Restore?

The reality is, many legacy unified backup solutions were slow to deliver comprehensive virtualization-protection capabilities. That situation led to new companies such as Veeam, which elected to solve the VM-protection problem directly. By the time VMware delivered robust backup APIs for its ecosystem, an innovation gap had arisen that, for many customers, still exists today.

Combining that fact with the unrest felt by other groups within IT, and it is easy to see how the "status quo" became insufficient for many (see Figure 2).[2]

Figure 2. Customer Willingness to Change Backup Solutions "from Scratch"

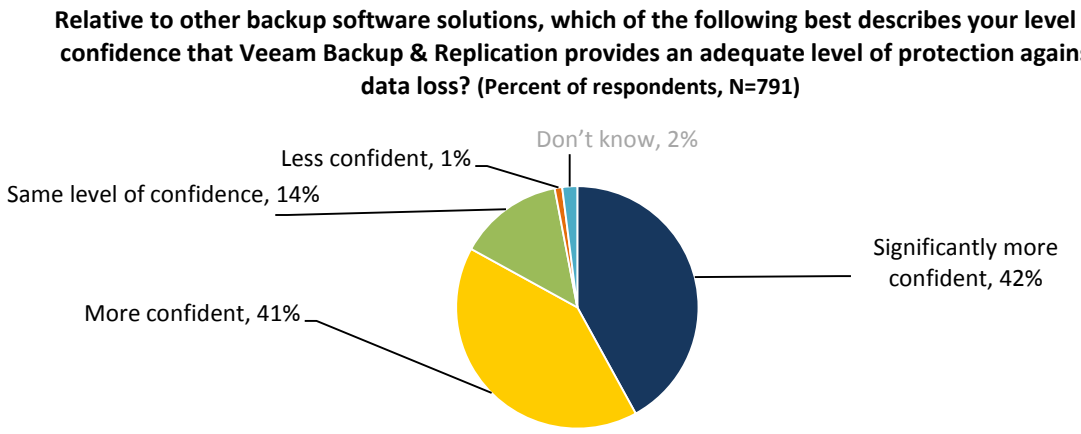


Source: Enterprise Strategy Group, 2014.

If you can't even *trust* your backup solution, its other bells and whistles won't matter. Notably, a combined 83% of the 791 Veeam users surveyed told ESG they were either more confident or significantly more confident now than they'd been with their previous backup solution (see Figure 3),[3] a fact that most likely manifests itself in higher IT satisfaction and improved systems' availability.

[2] Source: ESG Research Report, *Trends in Data Protection Modernization*, August 2012.
[3] Source: Custom research conducted by ESG for Veeam, February 2014.

Figure 3. Confidence Level Using Veeam Backup and Replication to Protect Against Data Loss

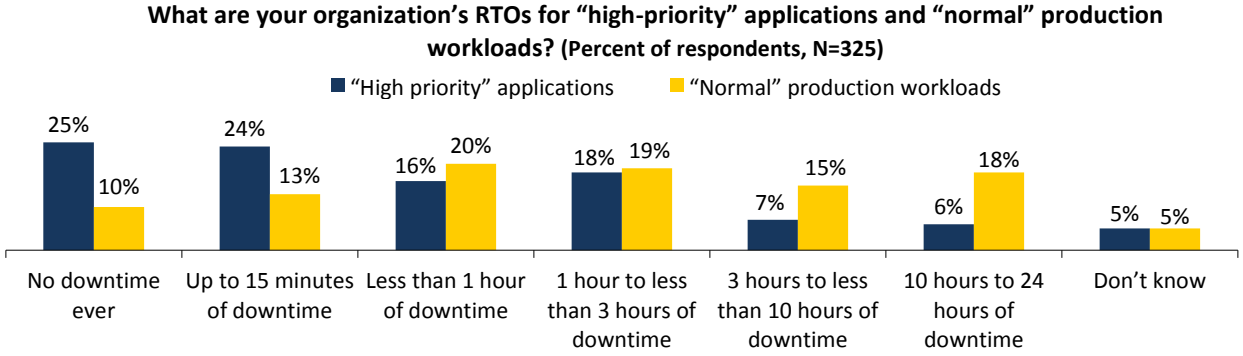


Source: Enterprise Strategy Group, 2014.

CONSIDERATION TWO: Your Availability Is Largely Based on "*How Fast You Can Recover*"

IT administrators not only need to trust their backup solution, they also need to consider what it does for them and the workloads/services being protected. Many say that one key to ensuring the availability of modern data center systems' availability is VM *recovery*; and they aren't wrong. ESG research shows that a combined 83% of high-priority tier-1 applications have a downtime-tolerance window of just three hours or less. Even a combined 62% of so-called "normal" (non-mission-critical) apps have that same brief downtime-tolerance window (see Figure 4).[4]

Figure 4. Downtime Tolerance for Tier-1 and Normal Applications



Source: Enterprise Strategy Group, 2014.

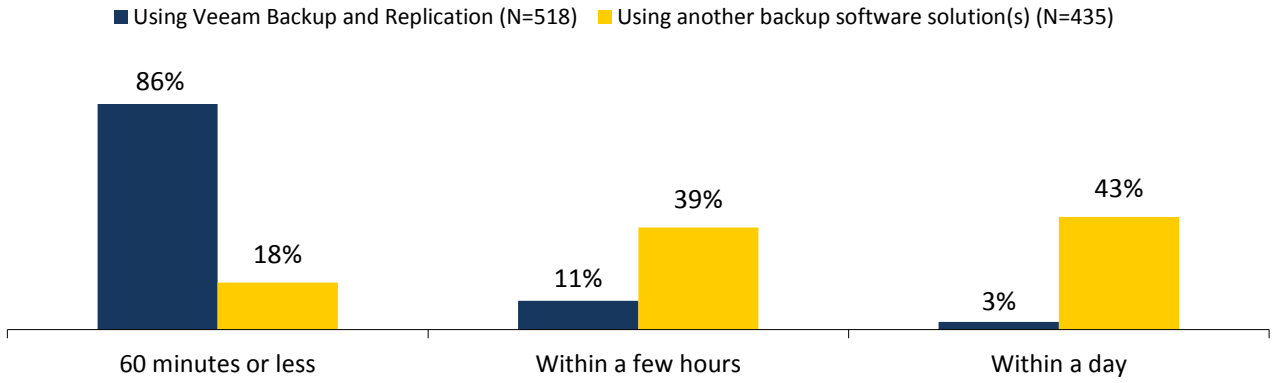
System availability is *the* measure of IT effectiveness today. Regardless of whether the workplace looks like a huge multinational enterprise or a smaller/midmarket firm, the productivity of everyone—IT staff and end-users alike—is utterly dependent on *access* to their data.

One question that ESG asked Veeam customers concerned how fast they could recover their VMs—using Veeam compared with using backup products they'd deployed prior to or in conjunction with Veeam. The difference in speed was almost "night and day" (see Figure 5).[5]

[4] Source: ESG Research Report, *Trends for Protecting Highly Virtualized and Private Cloud Environments*, June 2013.
[5] Source: Custom research conducted by ESG for Veeam, February 2014.

Figure 5. Ability to Resume VM with Veeam Software Solutions Relative to Other Data Protection Vendors/Products

In a scenario involving a virtual machine outage, how quickly—on average—has your organization been able to resume functionality (i.e., get the failed VM back up and running) as part of recovering through Veeam Backup and Replication compared to other backup software solutions? (Percent of respondents)



Source: Enterprise Strategy Group, 2014.

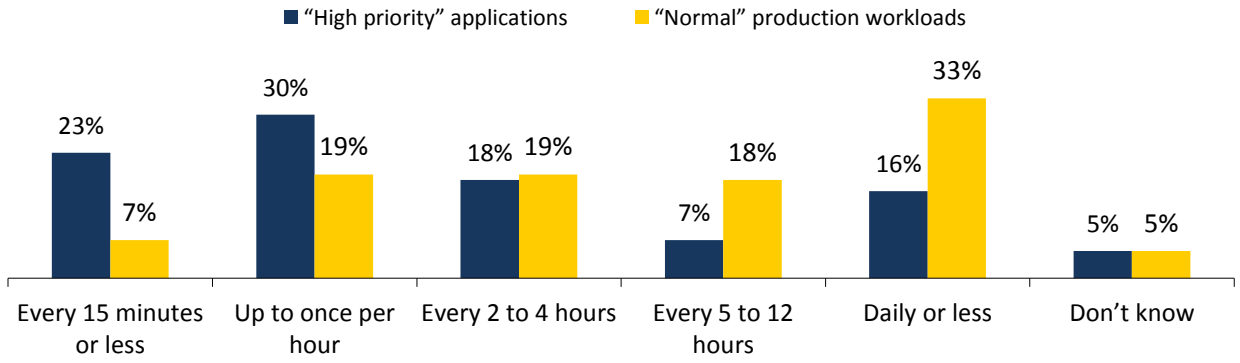
On average, the Veeam users surveyed reported being able to recover a VM in less than an hour. In contrast, when using backup products other than Veeam, their reported recovery timeframes ranged from "a few hours" to "within a day." Also notable beyond the Instant VM Recovery feature is Veeam's integration with storage-array snapshots, providing yet another availability-increasing capability to recover systems quickly.

CONSIDERATION THREE: How Well Are You Protected?

When IT people think of service level agreements (SLAs) related to data protection, one important requirement that often comes to mind is an assured return-point objective (RPO). No one can afford to lose lots of data. Frequent backups to help ensure adherence to already-established RPOs are vitally important (see Figure 6).[6]

Figure 6. Frequency of Making Backup Copies for High-priority Applications and Normal Production Workloads

Please indicate the frequency with which your organization makes backup copies for "high-priority" applications and "normal" production workloads in order to meet its RPOs for each. (Percent of respondents, N=325)



Source: Enterprise Strategy Group, 2014.

[6] Source: ESG Research Report, *Trends for Protecting Highly Virtualized and Private Cloud Environments*, June 2013.

Ensuring a highly-available infrastructure includes not only a fast recovery (RTO) capability, but also protecting against data loss (RPO). Of course, meeting an RPO does involve more than leveraging good backup software: Achieving it must also take into account the speed of the relevant storage arrays, the bandwidth of the network pipes, even the speed at which the backup administrators react when the need arises.

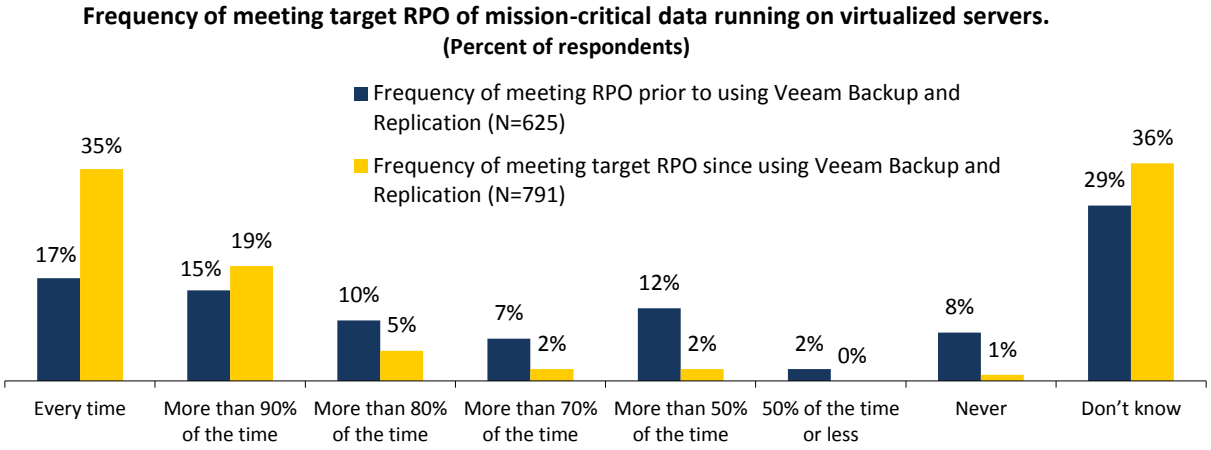
But if you have a higher-performing data protection solution that *also* is less obtrusive, (e.g., designed for modern data centers) then you tend to back up your data more often—thus ensuring that less of it might be lost. By optimizing the data protection process, one can increase the frequency of protection. That step enables IT to evolve beyond "just backup" to more continuous data protection and disaster preparedness.

Veeam Backup & Replication is architected exclusively for virtualized environments. It is therefore designed to be very good at taking advantage of the plumbing inside a hypervisor to "back up less" and complete each backup job more efficiently while protecting production VMs and hosts from performance penalties.

Because the software is engineered for efficiency in highly virtualized environments, its customers appear to be backing up their data more frequently (see Figure 7),[7] with the result, in theory, that they would experience less lost data if a downtime situation actually were to occur – as another step towards increasing data center overall availability.

BY OPTIMIZING the data protection process, one can increase the frequency of protection. That step enables IT to evolve beyond "just backup" to more continuous data protection and ultimately, better disaster preparedness.

Figure 7. Frequency of Meeting Target RPO of Mission-critical Data Running on Virtualized Servers



Source: Enterprise Strategy Group, 2014.

CONSIDERATION FOUR: How Can You See Whether You Are Protected or Not?

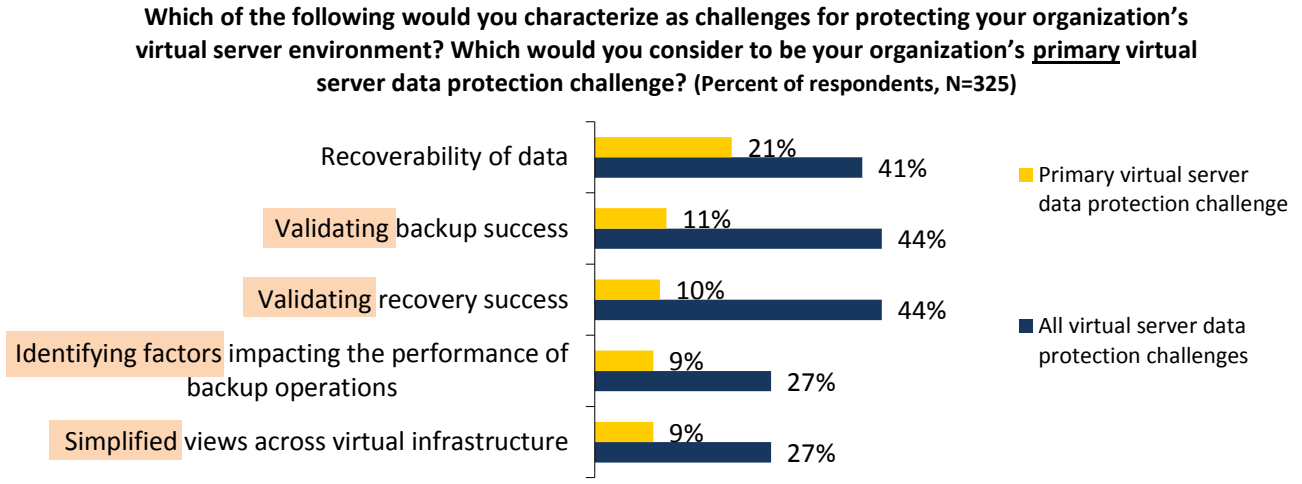
Although the convergence of dense computing systems, high-performance storage arrays and virtualization boosts agility and consolidates resources, it has the potential to make data protection both easier *and* more challenging:

- **It makes protection easier** because, with many servers encapsulated inside one physical shell, it's easy to copy a virtual hard disk to a different machine and just turn everything back on (certainly easier than disconnecting a physical machine, pulling it from a rack, shipping it elsewhere, then plugging it back in).
- **It makes protection more challenging** because virtualization adds abstraction. You can't "touch" a production VM's wiring interconnects to a backup server. Everything is abstracted within a software-defined network, software-defined storage, software-defined data center, etc. Thus, you are forced to identify after the fact which host, in which cluster, running which shared data store, across which SDN the data was moving before it was backed up to storage. Clearly, it would be a struggle to use a physical-only backup tool to figure out what is going right (or wrong) in that kind of virtualized environment.

[7] Source: Custom research conducted by ESG for Veeam, February 2014.

As Figure 8 shows, many of the virtual protection challenges that IT professionals experience relate to poor visibility.[8]

Figure 8. Top Five Challenges in Protecting an Organization's Virtual Server Environment

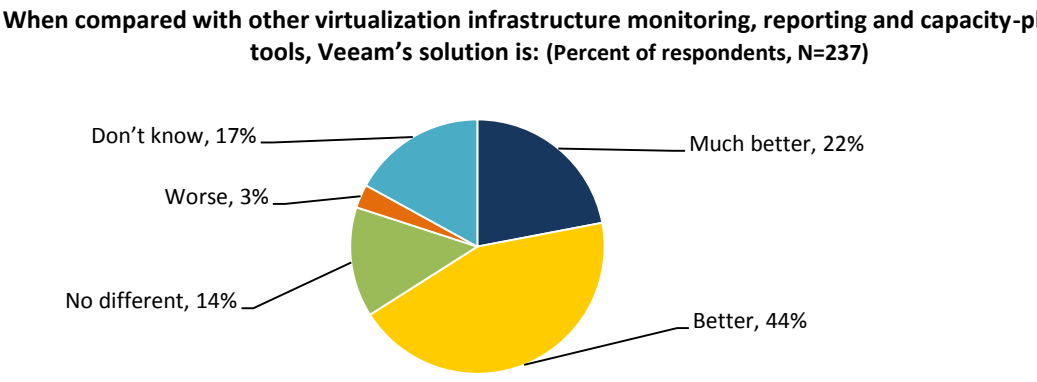


Source: Enterprise Strategy Group, 2014.

If "visibility" is a challenge in ensuring the availability of the modern data center, then the solution is better "monitoring and manageability," particularly because a broad set of administrators and secondary stakeholders have vested interests in how well the data center is protected.

Virtualization is the "platform" that underpins the modern data center. Your data protection strategy should enable both virtualization admins and application owners to be parties to the process of monitoring it. As Figure 9 shows,[9] Veeam customers indicate they are happier with the various application-related support tools provided in the Veeam protection toolkit (in this case, via the Veeam ONE management tool) than they were with products they were using before Veeam.

Figure 9. Respondents Rate Veeam ONE Compared with Other Tools



Source: Enterprise Strategy Group, 2014.

It is notable that Veeam's visibility solutions can be appreciated not only in the Veeam ONE management platform, but also in Veeam's Management Packs (MPs) for Microsoft System Center (for its backup solution as well as the hypervisors themselves) and within the Veeam Backup & Replication console itself.

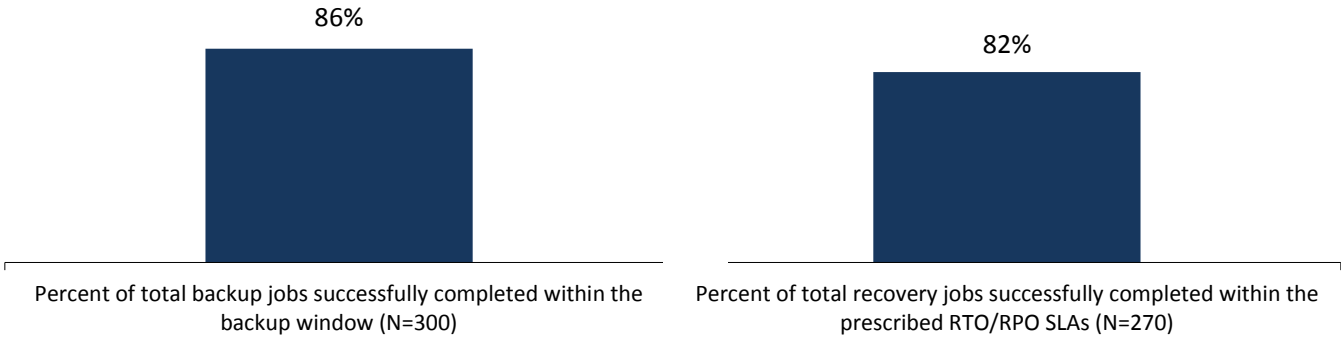
[8] Source: ESG Research Report, *Trends for Protecting Highly Virtualized and Private Cloud Environments*, June 2013.
[9] Source: Custom research conducted by ESG for Veeam, February 2014.

CONSIDERATION FIVE: How Else Can You Avoid Risk?

In 2012, ESG investigated organizations' backup and recovery success rates, finding that in the organizations surveyed, 86% of backups and only 82% of recoveries were completing successfully, on average (see Figure 10).[10] One could easily argue that one of seven backups failing and one of five recoveries not meeting SLAs is the definition of "*risky*."

Figure 10. Success Rates for Backup and Recovery Jobs

Please indicate your organization's approximate overall success rate for all backup jobs completed within backup windows, as well as for all recovery jobs completed within prescribed RTO/RPO SLAs. (Mean)



Source: Enterprise Strategy Group, 2014.

As long as auto-retry is available, the 86% success rate might be palatable from a *backup* perspective. But one out of five *recovery* jobs not meeting expectations is a much more ominous finding. If such a failure happens at the end of a three-, four-, or even eight-hour-long recovery attempt, a lot of time was just wasted: You accomplished nothing other than amassing even more downtime, along with the costs and pains that accompany it.

In contrast, Veeam customers cited a 95% success rate for backup jobs and a 96% RTO SLA attainment, both of which are made even more impressive considering they cited 73% backups and 77% recovery SLAs before using Veeam.

And although it is easy to state that better backups and more reliable restores reduce risk, Veeam goes further with its *Veeam Virtual Lab*, which provides an on-demand sandbox for pre-testing configurations, deployment scenarios, etc. for proactive risk mitigation as well.

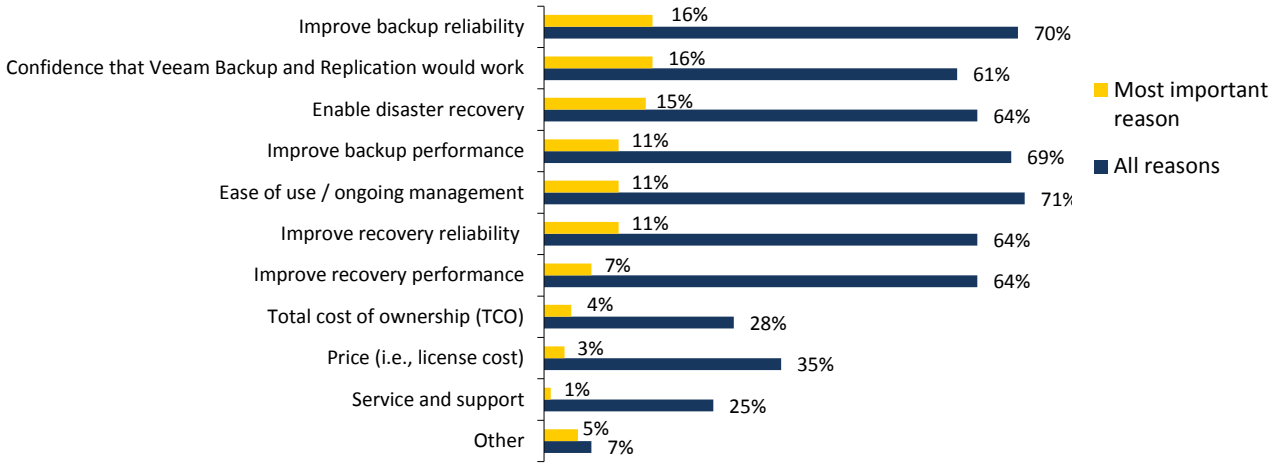
Why Veeam?

Each of the considerations above look at one aspect of modernizing data protection in order to increase the systems' availability of an "always-on" data center, which combine to reflect why Veeam customers choose to rely upon Veeam products (see Figure 11).[11]

[10] Source: ESG Research Report, *Trends in Data Protection Modernization*, August 2012.
[11] Source: Custom research conducted by ESG for Veeam, February 2014.

Figure 11. Why Organizations Decided to Implement Veeam Backup & Replication

To the best of your knowledge, why did your organization decide to implement Veeam Backup & Replication? What was the primary reason your organization implemented Veeam Backup & Replication? (Percent of respondents, N=791)

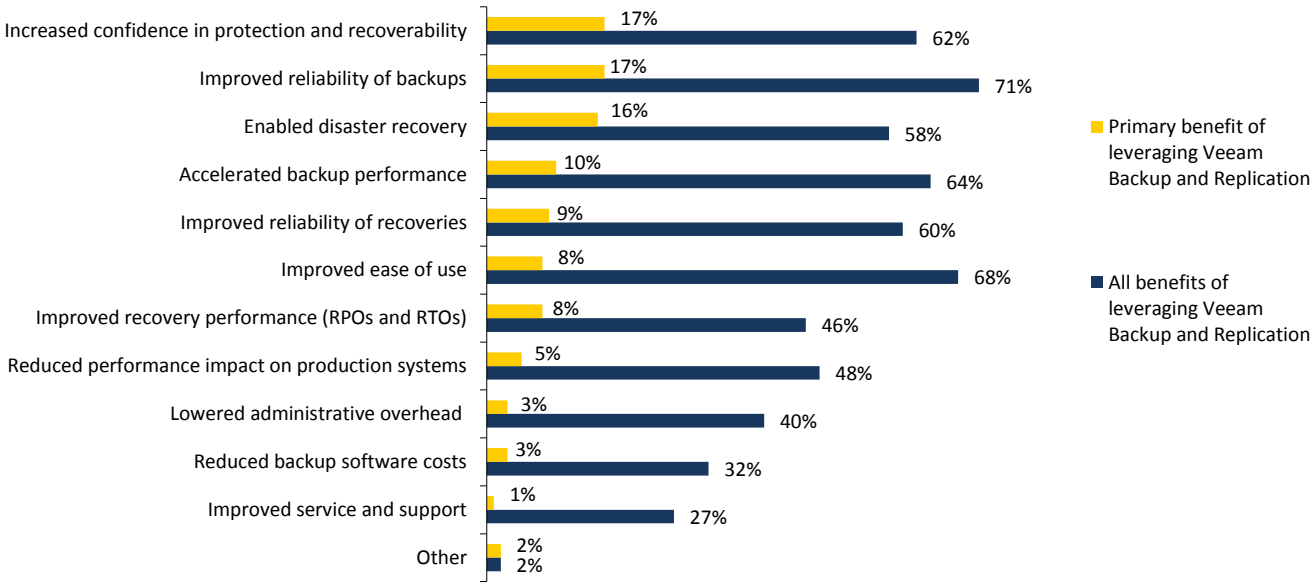


Source: Enterprise Strategy Group, 2014.

Again, availability by the users to their data and IT systems is the only measure that matters. And that availability assurance is not achievable if you can't restore your data. Following the respondents' initial selection, implementation, and subsequent use of the software, their increased confidence remained very prominent as a reported positive outcome. This heightened confidence is not surprising, considering that the respondents were also reporting that their actual recovery reliability levels did, in fact, rise (see Figure 12).[12]

Figure 12. Benefits Organizations Have Realized as a Result of Leveraging Veeam Backup & Replication

What benefits has your organization realized as the result of leveraging Veeam Backup & Replication to protect its virtual server environment? What is the primary benefit your organization has realized? (Percent of respondents, N=791)



Source: Enterprise Strategy Group, 2014.

[12] Ibid.

The Bigger Truth

A "modern data center" is virtualized, regardless of whether it extends physically across a large raised floor or is confined to a closet. In fact, that IT environment, including not only the VMs but the underlying compute resources and storage solutions could just as easily be in a hosted- or hybrid-cloud, or on-premises down the hall. Regardless of its physical characteristics, the modern data center has to be protected—reliably and rapidly—no matter what size it is.

When ESG surveyed Veeam customers on the topic of protecting their critical IT infrastructure, those customers reported the following in regard to:

- **How *confident* they are in their backups and ability to restore—**They felt an appreciably higher level of confidence in their Veeam solution than they did with whatever product(s) they had been using for VM backup before, including products that claim to be well-suited for unified physical/virtual backup solution.
- **Their availability being based largely on *how fast* they can recover—**They cited the solution's Instant VM Recovery feature as being significantly better than alternatives they'd previously used—in terms of both overall user experience and actual time needed to complete their recovery jobs—while also appreciating the application- and snapshot-enabled recovery capabilities.
- ***How well* they are really being protected—**They reported success in achieving their goal of increasing the percentage of backup jobs completed within their pre-established backup windows, as well as noticeable improvements to RTO and RPO. This assurance presumably comes not only from the engineering within Veeam's backup product itself in features such as SureBackup and SureReplica, but also through proactive testing through the Veeam Virtual Lab.
- ***Whether they can see* whether they are protected or not—**They gained significant visibility through Veeam Backup & Recovery's console, the Veeam management packs for System Center, its integration with vCenter, and the Veeam ONE management platform.
- **How else they are *able to avoid risk*—**They cited a 95% success rate for backup jobs and a 96% RTO SLA attainment, both of which are made even more impressive considering that they reported experiencing 73% backup SLAs and 77% recovery SLAs before using Veeam. And again, they could take advantage of Veeam Virtual Lab to assess planned configurations/deployment scenarios and mitigate risks proactively.

With such a high assurance of reliable, rapid VM recovery, and the resulting improved systems' availability that those data protection capabilities incur, it comes as no surprise to see a growing number of IT organizations relying on Veeam for protecting their modern data center.

Data protection cannot be an add-on or afterthought to designing a modern data center that is agile and highly available. Rather, as Veeam would say, it's a core requirement in enabling an 'always-on' business.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com