White Paper

The Top Four Considerations When Selecting a Modern VM Protection, Recovery, and Availability Solution

Explaining the Trends that Continue to Drive Adoption of Virtualized IT and Virtualization-specific Protection

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

December 2016

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

Contents

Executive Summary

IT environments continue to evolve beyond physical servers. Today, many important production resources operate on virtual machines (VMs) running on multiple hypervisors, and more organizations have been moving their mission-critical business processes offsite to the cloud. As a result, the requirements for protecting organizational data, recovering it, and ensuring its availability also have changed.

ESG finds that:

- *Although not all servers are bound by a single service level agreement, SLAs should drive the search for the right data protection solution. An organization should adapt to the diverse uptime requirements of its workloads by incorporating a range of activities—including backups, snapshots, replication, and availability technologies—into its data protection strategy.*
- *Organizations need to be aware that whenever they modernize a modern, heterogeneous IT production environment, they must make corresponding enhancements to the protection environment as well. When commensurate protection modernization efforts do not occur, VM recovery failures will likely result.*
- *Organizations searching for a better protection, recovery, and availability solution should regard flexibility and agility as key differentiators. It is important for these organizations to take note of the agility with which a prospective solution accomplishes recoveries (i.e., if it is capable of application-consistent recovery, granular recovery, etc.) and the recovery platforms that the solution can leverage (i.e., recovery to another cloud or to a different hypervisor).*
- *The importance of good automation is growing dramatically. The greatest differentiator between "a backup tool" and "a virtualization-savvy data protection and availability solution" might be its ability to orchestrate and automate the recovery of a complex IT environment.*

Introduction

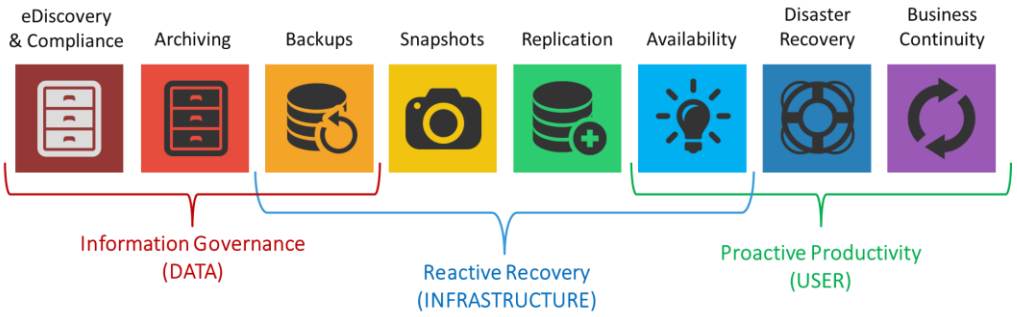
IT organizations exist to satisfy the needs of the businesses they support, but those needs are diverse. Fulfilling all of them can require a degree of IT heterogeneity beyond what many people would expect.

Therefore, in the past decade, IT transformation has become more aggressive—with efforts centered on expanding beyond traditional reliance on dedicated physical servers to embracing virtual machines. IT transformation efforts will most likely continue along this course. So, in a typical environment, we will continue to see:

- Some standalone **physical servers** still in use.
- A significant number of **virtualized servers** being used to host multiple virtual machines under various hypervisors.
- **Myriad cloud services** providing hosted infrastructure, hosted storage, software-as-a-service (SaaS), and similar services to complement the onsite physical servers and VMs.

In other words, considerable heterogeneity will remain evident. Each production platform listed above may need a separate availability and recoverability approach as well. The strategic spectrum of data protection tools and activities an IT organization might employ (see Figure 1) can be as diverse as the organization's production platforms themselves.

Figure 1. The Spectrum of Data Protection



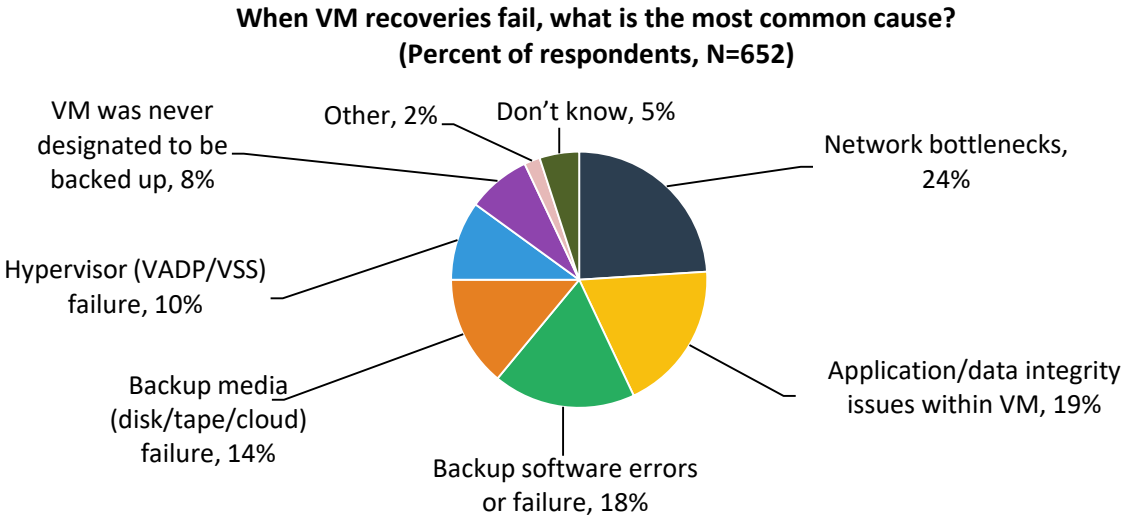
Source: Enterprise Strategy Group, 2016

Protecting a Diverse Infrastructure Can Be Complicated or Even Risky

With so much of a typical IT infrastructure operating in a virtualized manner these days, it is appropriate to examine the struggles that an IT organization can experience when protecting, recovering, and ensuring the availability of mission-critical platforms.

Usually, diverse SLAs will have been put into place across the diverse production platforms. Those diverse SLAs can only be addressed by equally varied methods of protection and recovery. As mentioned, whenever IT modernizes any aspect of a specific production platform, it must also modernize the associated protection and recoverability mechanisms safeguarding the platform's availability. When protection modernization efforts do not occur, the types of VM recovery failures shown in Figure 2[1] can arise.

Figure 2. Most Common Cause of VM Recovery Failures



Source: Enterprise Strategy Group, 2016

Virtualization Protection Makes Sense

Ensuring the recovery and availability of a highly virtualized environment certainly comes with challenges, including data recoverability, validating backup/recovery success, timely troubleshooting, predicting backup/restore times, identifying

[1] Source: ESG Research, *Protecting Highly Virtualized Environments*, expected to be published in January 2017.

factors causing bottlenecks or affecting backup performance, keeping pace as VM density grows, and closing gaps in protection.[2] But at least it is possible to codify the challenges according to two meta-trends:

- Recoverability of data—Today, everyone using modern technology should already be addressing this issue.
- Virtualization "savviness"—Finding an IT management technology that understands the dynamic, abstract nature of virtualized hosts, storage, and networks well enough to ensure they are protected and promptly recoverable.

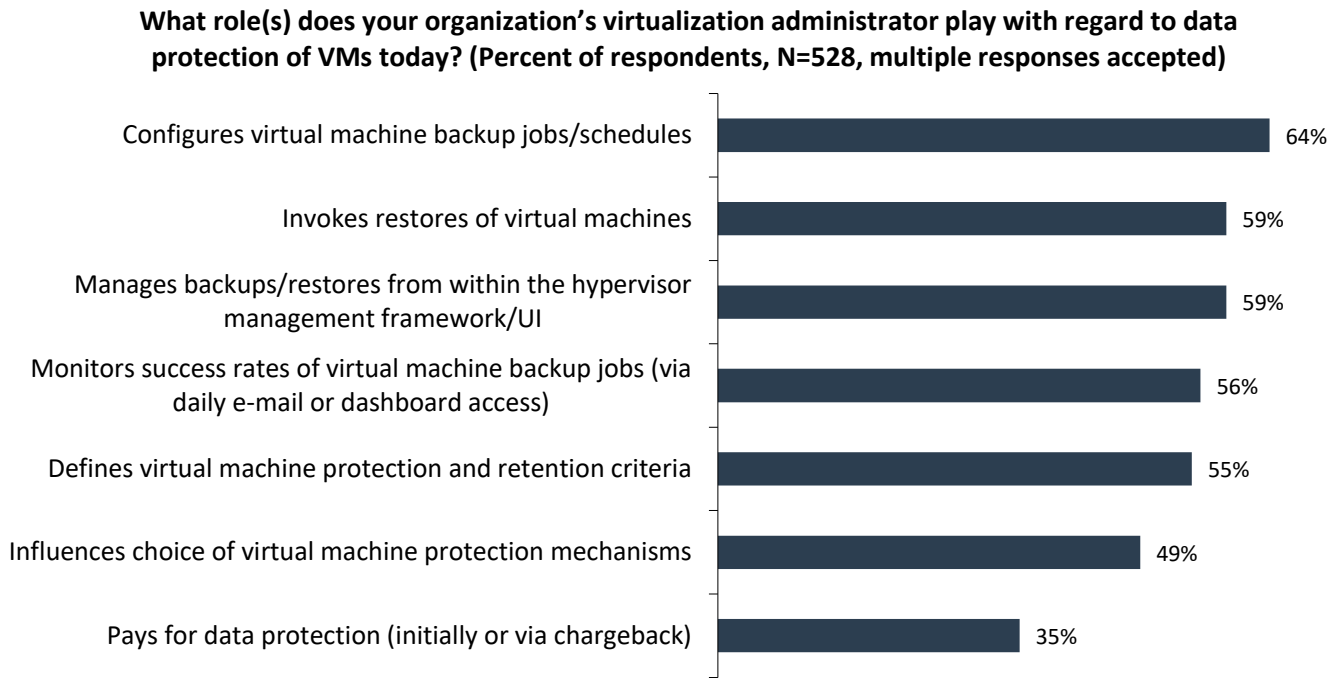
Of course, most organizations have two or more hypervisors to manage, which adds even more complexity to the availability-assurance challenge.

Nor is diversity in the underlying infrastructure (hosts, storage, and hypervisors) the only challenge. The roles of people in regard to choosing and using backup tools for virtual environments are evolving, too—moving away from all-encompassing backup administrators, toward IT Operations team members and virtualization administrators.

vAdmins Are Now Protecting Themselves

What role does your vAdmin play? The answer may surprise you. Your organization may employ virtualization-specific administrators or IT Ops administrators with experience in managing sophisticated, heterogeneous environments. The result is that traditional backup administrators are now being usurped to some degree by more virtualization-capable team members intent on ensuring the protection and recoverability of their own workloads. People other than backup admins now handle quite a few protection, recovery, and availability responsibilities (see Figure 3).[3]

Figure 3. Roles of vAdmins in Protecting VMs (North American and Asia-Pacific Markets)



Source: Enterprise Strategy Group, 2016

Notably, IT Operations professionals also seem to be adding backup tasks to the list of functions they provide for all servers across a heterogeneous environment (along with provisioning, monitoring, patching, and more). IT Ops admins appear to enjoy a tremendous amount of influence at this point, at least among the organizations surveyed by ESG.

[2] ibid.
[3] ibid.

For example, 53% of respondents reported that their IT Ops groups are making the final decision about how virtual machines will be protected/recovered, with 23% reporting that their vAdmins (or a similar role) own that responsibility, and 21% reporting that their backup admins decide.[4]

What to Look for in Modern VM Protection, VM Recovery, and VM Availability

Data protection vendors have long used phrases such as, "It's not about backup; it's about recovery." But many of them still fall short when it comes to ensuring the most desirable business outcome of all: ***The assured availability of business systems***.

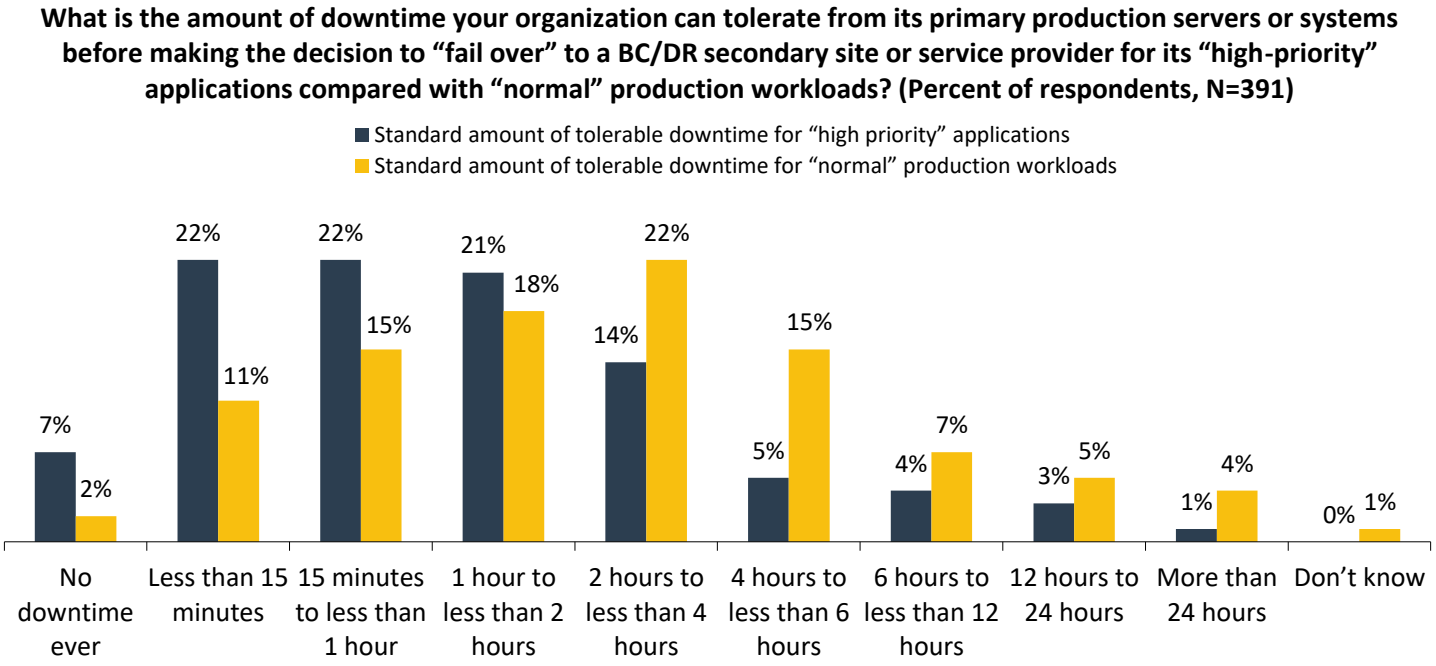
An IT organization can help itself win that race to zero downtime by endeavoring to use a range of techniques that avoid outages and data loss—in other words, techniques that will help it meet the recovery point objectives (RPOs) and recovery time objectives (RTOs) for servers.

Eventually, as the organization gets closer to that zero-downtime point, it will want to pivot from a philosophical mindset of reactive recovery to one of proactive availability. The ultimate business-level outcome—achieving higher operational productivity and greater profitability—is the main motivation.

SLAs Should Drive the Search for a Solution

Obviously, not all servers are bound by a single service level agreement. Required uptime is based in large part on the business unit that a given workload supports—or more precisely, on the importance of the work being done by that unit. This fact bolsters ESG's recommendation that IT organizations should be leveraging as many colors of the data protection spectrum (see Figure 1) as necessary to accommodate different servers' varying uptime needs (see Figure 4).[5]

Figure 4. Amount of Downtime Organizations Can Tolerate for Primary Production Systems Before Failing Over to BC/DR Site: High-priority vs. Normal Workloads



Source: Enterprise Strategy Group, 2016

[4] ibid.

[5] Source: ESG Research Report, *The Evolving Business Continuity and Disaster Recovery Landscape*, February 2016.

As a way to meet SLAs, ESG does *not* unilaterally recommend the use of multiple vendors across the data protection spectrum. An IT organization should simply focus on seeking out data protection technologies (coming from the same or a different vendor) suited to supporting a heterogeneous, hybrid IT environment.

Most IT groups already seem to realize that this approach is the right one. For example, ESG found that only 11% of the organizations it surveyed are not supplementing their VM backups with snapshots and/or replication.[6] Similar attention to protection diversity appears to be prevalent with physical servers and cloud-based services, too.

Only 11% of organizations surveyed by ESG do not supplement their VM backups with snapshots, replication, or both.

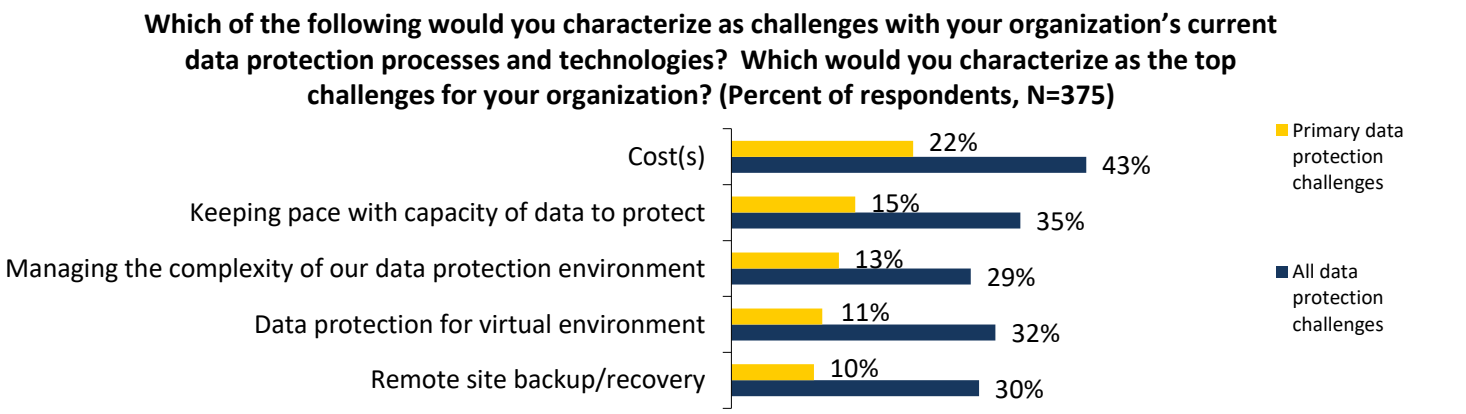
Be Clear and Aligned About the Challenges the Organization Is Trying to Solve

Finding a VM availability solution should mean more than evolving from "legacy protection" to "new availability." Your SLAs and the requirements of your business will help you uncover what you're *really* solving for.

It is very important to achieve alignment between senior leadership (who are mindful of the business in general), and IT implementers (who are tasked with service delivery). However, those groups are often disconnected in their visions of what needs to be modernized or strategically transformed.

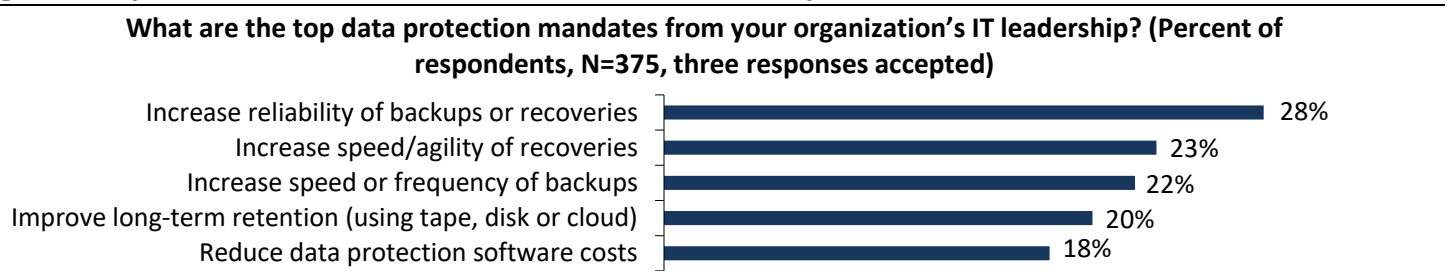
Figure 5[7] describes the five most common protection challenges that IT implementers must focus their attention on. In contrast, Figure 6[8] shows the five most common protection outcomes IT executives surveyed by ESG expect those implementers to enact. The implementers' actual challenges are clearly unaligned with the executives' mandates.

Figure 5. Top Five Data Protection Challenges for IT Implementers



Source: Enterprise Strategy Group, 2016

Figure 6. Top Five Data Protection Mandates from IT Leadership



Source: Enterprise Strategy Group, 2016

[6] Source: ESG Research, *Protecting Highly Virtualized Environments*, expected to be published in January 2017.
[7] Source: ESG Research Report, *2015 Trends in Data Protection Modernization*, September 2015.
[8] ibid.

Unfortunately, when IT implementers and IT executives are disconnected in this manner, the result can be neither group getting what it expected, and the organization suffering as a whole.

Flexibility and Agility Matter

Figure 6 revealed that senior IT executives' two most frequently cited aspirations for improving data protection relate in some way to recovery flexibility. It is possible to enhance flexibility and agility by:

- Leveraging diverse recovery capabilities—e.g., backups, plus snapshots, plus replicas.
- Creating a greater number of recovery points by performing backups more frequently, which also might allow the organization to mitigate ransomware threats and other problems.

Any organization trying to find a better protection, recovery, or availability solution should regard flexibility and agility as key differentiators.

In particular, it is helpful to identify the methods through which recovery could be accomplished and the platforms that the recovery can leverage. For example, can the solution protect physical servers but recover them into VMs? Can it recover a VMware VM onto a Hyper-V host or vice versa? Can it utilize cloud storage to ensure data survivability, and then recover that data to a new service provider or to new hosts in a different geography? Can it recover multiple VMs through a disaster recovery-as-a-service (DRaaS) offering?

The features that respondents surveyed by ESG say they want in a VM-protection solution include many capabilities that relate closely to flexibility and agility:[9]

- Ability to automatically detect and protect VMs
- "Instant" or rapid recovery of VMs directly from the backup server/appliance
- Application consistency within VMs
- Continuous or near-continuous data protection
- Ability to use cloud services for offsite protection
- Management of backups/recoveries from within hypervisor UI
- Granular recovery of files from within VM-based backups
- Integrated protection with storage snapshots
- Ability to use cloud services for BC/DR
- Integration with hardware-based deduplication arrays
- Ability to recover one hypervisor's VM into a different hypervisor
- Ability to protect infrastructure-as-a-service (IaaS)-hosted VMs
- Built-in software-based deduplication
- Ability to use tape for long-term retention of VM-centric data

Automation and Orchestration

VM protection sometimes unfolds "one server at a time." However, true availability *at an organizational level* is a bit more complex, with multiple applications across many servers having to reconstitute in a logical, well-orchestrated manner. Without proper orchestration, two types of recovery failures can occur:

[9] Source: ESG Research, *Protecting Highly Virtualized Environments*, expected to be published in January 2017.

- Prioritization-related failures—not all servers and their hosted applications are equal. Everything depends on how a workload relates to the business units and processes. So, simply highlighting a block of machines and restarting them may not satisfy the organization's recoverability and availability goals. Prioritization-related failures sometimes arise because the most knowledgeable operators are unavailable during the recovery effort. Therefore, the IT infrastructure recovery process should be documented ahead of time to help ensure availability.

- Interdependency failures—many business-critical or particularly complex applications are formed from multiple underlying server components (e.g., a web front-end connected through middleware to multiple databases). In this case, simply restarting the seven or so affected interdependent VMs probably won't actually restore full access to the application. Those seven VMs (plus the Active Directory authentication service) would need to be restarted *in a very specific order* to resume functionality. That's not achievable with legacy backup tools alone.

The greatest differentiator between "a backup tool" and "a virtualization-savvy data protection and availability solution" just might be the ability to orchestrate and automate the recoverability of a complex IT environment.

The Bigger Truth

Organizations in increasing numbers are recognizing that, moving forward, a few important facts of life will be influencing their data protection, recovery, and availability strategies. For example:

- Production environments will be increasingly heterogeneous, encompassing residual physical servers, virtualized machines running across multiple hypervisors, and cloud-based capabilities.

- In the "race to zero" for RPO and RTO, the smart thing to do will be to plan on combining the reliability of modern backup with the agility of snapshots and the survivability of replication.

- Agility, automation, and orchestration will only continue to grow in importance as must-have attributes.

As much as those trends will impact businesses and their survivability, another important fact of life is that it will be essential to achieve alignment between the executives who understand the business, and the various IT implementers and partners who lead strategic execution.

One way to bolster that alignment is for everyone to work together to identify and deploy an availability solution engineered specifically to support the virtual machines that run so many of today's business-critical platforms and workloads.

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