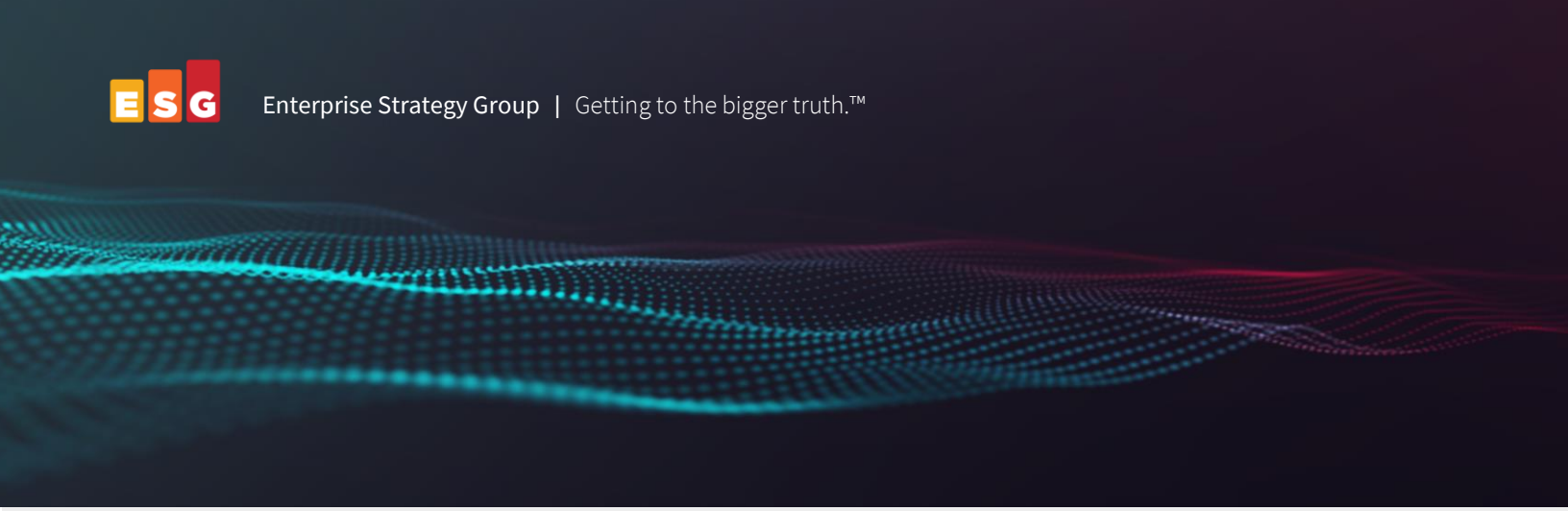


ESG WHITE PAPER

Attaining IT Transformation and Business Resiliency with Dell Technologies

Deploying Proven and Modern Data Protection Strategies Is Key to Accomplishing IT Transformation and Achieving Business Resiliency

By Christophe Bertrand, ESG Senior Analyst
and Monya Keane, ESG Senior Research Analyst

June 2020

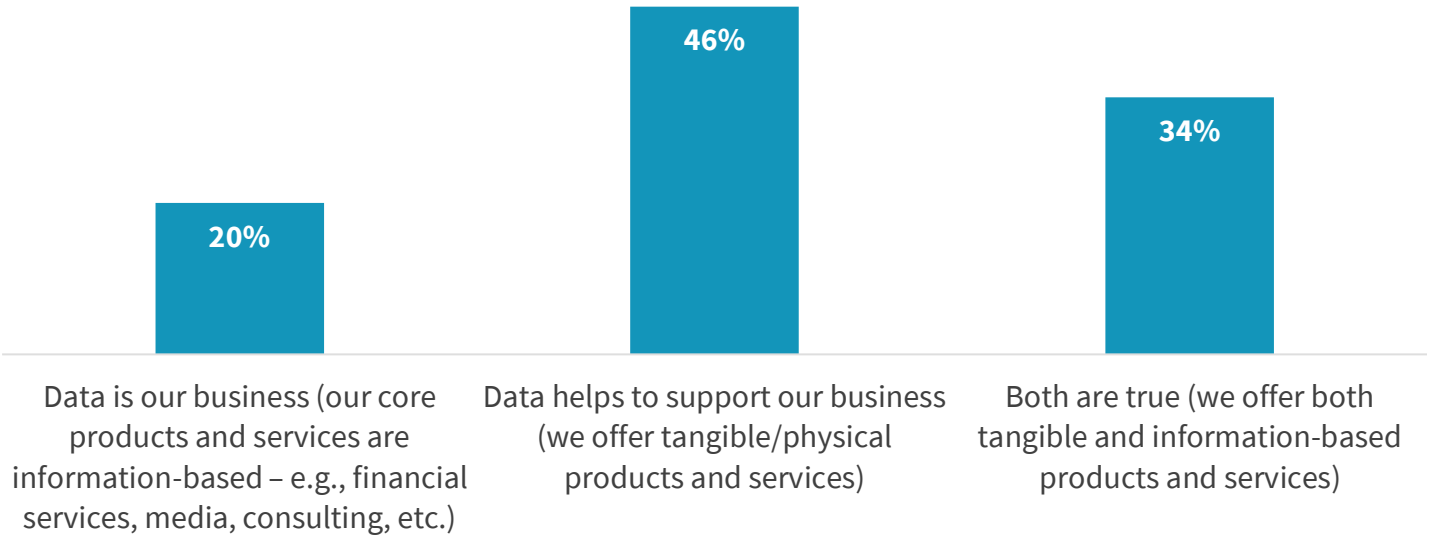
This ESG White Paper was commissioned by Dell Technologies
and is distributed under license from ESG.

Contents

Market Landscape: IT Resiliency in the Balance

Major IT trends are playing out, creating complexity for organizations that are at varying levels of maturity in their IT transformation efforts. To be successful today, most organizations need to establish a resilient IT infrastructure, leveraging systems that can anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises. That's because in many cases, the business is being driven partly or wholly by data (see Figure 1).[1] And in large part, the necessary degree of IT resiliency, resulting in either business success or failure, centers on deploying the right data protection technology.

Figure 1. Data Is at the Heart of Business



Source: Enterprise Strategy Group

Data Is the Business

Protecting data, the heart of many businesses, is vital to success. According to ESG survey research, 52% of IT decision makers expect that their organizations will develop and offer new data-centric products and services in the next two years.[2] Those projects will add complexity to their IT environments. But the most-reported reason that organizations' IT environments are becoming more complex is that they are struggling with higher data volumes.[3]

Data Protection, Disaster Recovery, and the Cloud

Organizations need to evolve with the changing business landscape. As major IT trends play out, the success or failure of an organization will depend on how resilient the organization is. Resilience is the key to deriving the long-lasting benefits of an organization through sustainable practice. Business leaders need to rethink how the enterprise creates value today and that will result from leveraging those high data volumes to make better-informed and faster decisions. Operational efficiency remains the most common objective for pursuing IT transformation, closely followed by gaining the ability to provide a better, more differentiated customer experience.[4] Better operational efficiency actually can benefit the customer

[1] Source: ESG Master Survey Results, *The Evolution from Data Backup to Data Intelligence*, January 2020.
[2] ibid.
[3] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[4] ibid.

experience. Specifically, when the operational efficiency of backup and recovery and BC/DR is improved, it means the IT group can focus more on projects and programs that will enhance customers' experience.

In general, data protection spending for both cloud-based and on-premises workloads will go up—51% of respondents to an ESG research survey said they expect their organization to increase overall 2020 data protection spending relative to 2019. (It was one of the six most cited technologies for 2020 spending increase.) It's not surprising, then, that improving backup and recovery is the most commonly reported data center modernization investment priority for this year, cited by 30% of respondents. Similarly, BC/DR (mentioned by 19% of respondents) is a business initiative cited as an IT spending driver.[5]

Data protection processes need to "follow the data" and adequately protect IaaS and SaaS data residing in the cloud. Surveyed IT managers reported that 52% of VMs deployed in their organizations reside in the cloud, with the remaining 48% working on-premises. ESG also expects annual VM growth rates to be higher in the cloud than on-premises over the next 24 months.[6] With a highly mixed environment of virtualized workloads on-premises and the cloud, and the increasing amount of VMs being deployed, efficient and automated data protection that is highly integrated within the VM management environment is necessary to achieve efficiencies and scale to support the business.

The Shortcomings of Protecting VM Data

Tools for backing up and recovering virtualized data have been on the market for many years, yet most organizations surveyed by ESG still estimate that nearly 25% of their VM backup and restore jobs fail. Those recovery failures come at a cost, sometimes leading to significant negative operational efficiency and business impacts. The biggest negative impacts include productivity loss (43% of surveyed organizations experienced in the last 12 months), data loss (cited by 39%), revenue loss (31%), damage to brand integrity (29%), and loss of employee confidence (28%).[7]

Cybersecurity and Data Protection

As has been the case for several years, improving cybersecurity continues to be the business initiative survey respondents said would drive the most overall technology spending in their organizations over the next 12 months (cited by 40%). It makes sense: A combined 29% of the respondents also reported that their organizations are experiencing ransomware attacks on either a daily or a weekly basis.[8]

That situation is made worse by the fact that cybersecurity tops the list of IT skill shortages across all disciplines. Because not enough cyber experts are available to recruit, many organizations are instead investing in technologies to improve/increase cyber resiliency and protect critical data and applications from ransomware and other cyberattacks. Data protection and cybersecurity go hand in hand in that they both depend on a resilient IT infrastructure. The challenge is that there is a lack of cybersecurity skills/resources in the market, and the tools available are predominantly focused on endpoints and applications (e.g., WAF and firewall). Losing an endpoint is bad, but it's nothing compared with losing mission-critical data. Businesses must protect the data as the last line of defense, with an air-gapped core component as a major element of any cyber resiliency plan.

[5] ibid.
[6] Source: ESG Research Insight Paper, *Data Protection Trends in Virtual Environments*, February 2020.
[7] ibid.
[8] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

Three Waves for Modern Data Protection

The three "universal" IT resilience-related challenges are:

- Cloud data protection.
- VMware data protection.
- Cyber recovery.

All of those challenges are intertwined. IT transformation enables business transformation, but at the heart of business transformation is data. Resiliency—especially in an evolving landscape—is the fundamental objective organizations must achieve. And with the right data protection technologies, it *is* largely possible to achieve.

Multi-Cloud Data Protection

IT is now established in a multi-cloud world, with many organizations either using or considering using more than one off-premises cloud repository to store and protect secondary data. Multiple use cases exist—protecting on-premises data in the cloud, protecting data already in the cloud, leveraging the cloud for backup and disaster recovery as a service, etc. Over the past three years, ESG has observed significant growth in those use cases and expects the growth trend to accelerate,[9] despite the possible risks and potentially high hidden costs related to relying upon a third-party-operated cloud to store and protect an organization's most critical data.

These days—to truly protect business-critical data from hackers, insider threats, natural disasters, or human error—the protection solution must be able to span multiple cloud services. That is, it must protect the whole workload ecosystem across on-premises, public cloud, multi-cloud, and hybrid cloud environments.

In addition to migration/mobility to store, protect, replicate, and move data to and between cloud providers, other essential capabilities include:

- Advanced integration with VMware environments.
- Effective cloud tiering, which identifies infrequently used data and automatically moves that data to lower-cost object storage in the cloud.
- Intelligent data management to allow the organization to maximize the value of its data assets by leveraging secondary data for DevOps, analytics, and DR testing.
- Operational efficiency features.
- Efficient, verifiable disaster recovery features.
- The ability to ensure compliance with corporate/regulatory requirements while maintaining optimized operations.
- Simple deployment and easy day-to-day management by automating common backup and recovery tasks.
- Global scalability to protect any workload across any cloud.

[9] Source: ESG Master Survey Results, *Data Protection Cloud Strategies*, June 2019.

VMware Data Protection

Even though IT organizations are very comfortable with virtualization technology overall, the rapid growth of VM environments can present a challenge if the organization does not have a comprehensive data protection strategy. Right now, organizations are in dire need of modern VM data protection to ensure the protection and security of critical data assets that are likely hosted on VMs both on-premises and in the cloud.

The smart approach is to simplify IT with tightly integrated VMware hybrid cloud solutions that deliver a common data protection experience on-premises and in the cloud. This integration with VMware delivers self-service data protection with easy data management and automated backups to accelerate IT transformation. Deep technical integration with VMware is needed to truly deliver on hybrid cloud DR and data protection solutions. Orchestration and automation are vital given the growing number of VMs and their distributed nature. Having a consistent solution across on-premises and the cloud provides operational efficiency. Having a large ecosystem of channel and managed service provider partnerships to supplement internal teams will help, too.

Additionally, a requirement to meet the needs of cloud-native solutions and the applications that support them is quickly becoming the new normal. From an economic point of view, cloud-native technologies enable the true value of cloud by allowing applications to scale and evolve in much shorter timelines. This scalability creates new opportunities for the business in terms of revenue growth, efficiency improvements, and better customer experience. Protecting these cloud-native environments must be central to the conversation.

Cyber Recovery

Cyber recovery often involves deploying disaster recovery methodologies, but cyber recovery and DR are very different processes. The processes for modern cyberattack remediation can involve establishing workflow automation to protect and isolate critical data, identify suspicious activity, and accelerate recovery to quickly resume normal business operations. That activity is also sometimes referred to as isolated recovery—such solutions protect copies of critical data within a dedicated digital vault, ideally via an operational air gap (physical isolation from the network).

Isolated recovery capabilities are crucial to creating a secure infrastructure that increases cyber resilience and safeguards critical data, especially as a trend has arisen with recent cyberattacks that encrypt and/or destroy primary backups both on-premises and in the cloud.

Downtime-avoidance efforts are obviously important—the FBI says cybercrime cost American businesses and individuals $3.5 billion in 2019.[10]

Given that we are living in the "data era," ransomware and other cyberattacks are not going away any time soon. In fact, their scope, scale, and frequency continue to increase, especially with a sudden growth of a remote workforce. That's why modernizing and transforming IT must involve deploying intelligent, automated cyber recovery analytics. Today's landscape of rapidly changing threats and massive data volumes makes it practically obligatory for organizations to use adaptive analytics, machine learning, and forensic tools to detect, diagnose, and accelerate recovery. Intelligent tools (AI/ML in the vault to scan and analyze data), along with automated protection and recovery workflows, will alleviate the burden of managing, protecting, and recovering known-good versions of ever-growing data repositories so that business can resume in the event of a cyberattack.

[10] Source: Federal Bureau of Investigation Internet Crime Complaint Center, *2019 Internet Crime Report*, February 2020.

The Bigger Truth

The three universal pillars of IT resiliency—cloud data protection, VM protection, and protection against cyber threats—all offer potential for an IT organization to:

- Improve operational efficiency.
- Reduce business risk.
- Increase the value of data, making it usable for DevOps, DR testing, and business analysis.

Mechanisms and solutions able to accomplish those goals already exist today. Thus, not only can organizations achieve great IT resiliency, but they won't have to reinvent the wheel. It is far better to adapt and improve existing IT investments—to develop the necessary skill sets by leveraging intelligent and innovative solutions as a replacement for experts who are in short supply. Protecting the business begins with protecting the data.

For organizations to succeed as data grows (with multi-cloud, VM sprawl, and cyber risks becoming more sophisticated), the organization will need a trusted partner such as Dell Technologies, with a rich portfolio of solutions, ecosystem partnerships, and integrations that result in even higher efficiency and resilience to maintain critical processes and the IT systems that support them.

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