ESG RESEARCH INSIGHTS PAPER

Why Data Protection Matters for Today's Multi-cloud Environments

A Research Study Exploring the Role of Optimized Data Protection Capabilities for Hybrid Cloud Success

By Christophe Bertrand, Senior Analyst

May 2020

Contents

Cloud Trends, Evolution, and Sprawl Yield a Changing Landscape for Data Protection

Cloud is gaining in adoption and popularity across many organizations today, reshaping traditional infrastructure. ESG research identified that 76% of organizations give public cloud as much or more consideration as on-premises infrastructure for new applications, which is a significant vote of confidence. As a matter of fact, 38% of organizations' data is expected to be cloud-resident within 24 months, while the number of public clouds in use is also expected to rise.
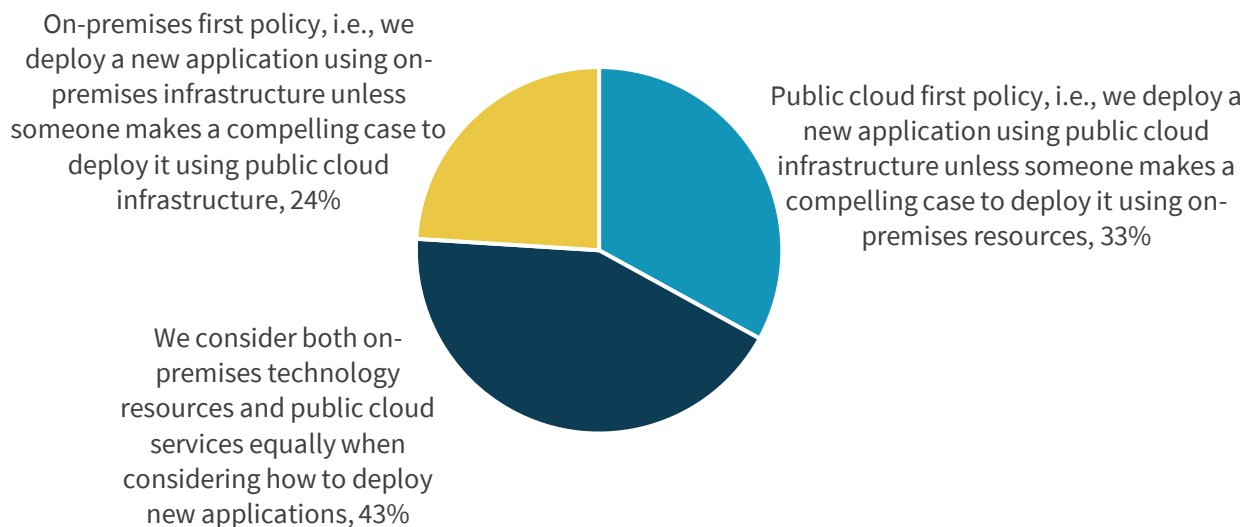
Users of cloud service providers (CSPs) do not put all their eggs in the same basket, with 82% utilizing multiple infrastructure CSPs today, while 86% expect to do so 3 years out. Specifically, the proportion using more than three CSPs is expected to double (31% versus 15%) in the same timeframe. Against this backdrop, it is not surprising that 73% of organizations report that using infrastructure in the public cloud (or multiple public clouds) in addition to on-premises infrastructure has added complexity to IT operations. Multi-cloud is happening, and it makes life more complex!

This means that many data-related processes, such as backup and recovery, need to adapt to this evolving hybrid (in which some workloads reside on-premises and others reside on public cloud infrastructure) and multi-cloud (in which workloads are hosted on a variety of public clouds) world. Data protection "follows" the workloads, a relationship borne out by ESG research: Organizations with more than 500 cloud-hosted VMs in their environment are more likely than those with 500 or less to utilize both Disaster Recovery-as-a-Service (DRaaS, 80% versus 57%) and cloud backup targets (82% versus 69%).[1] Said another way, as IaaS usage increases, so does an organization's propensity to use different protection solutions.

The other important consideration is maintaining coherent recovery point and time objectives (RPOs and RTOs) across what has become a very distributed infrastructure with different spans of control, security, and management. Data protection implementations must unify service levels across on-premises and cloud environments. There is therefore an opportunity to evolve current data protection architectural designs to embrace technologies that can handle your enterprise and cloud environments in a consistent manner.

Figure 1. Cloud or On-premises First?

Which of the following best describes the approach your organization takes when it comes to new application deployments? (Percent of respondents, N=1,257)

On-premises first policy, i.e., we deploy a new application using on-premises infrastructure unless someone makes a compelling case to deploy it using public cloud infrastructure, 24%

Public cloud first policy, i.e., we deploy a new application using public cloud infrastructure unless someone makes a compelling case to deploy it using on-premises resources, 33%

We consider both on-premises technology resources and public cloud services equally when considering how to deploy new applications, 43%

Source: Enterprise Strategy Group

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

Many data protection solution decisions will hinge on where workloads reside, and end-users favor flexibility of workload placement: 83% of organizations make achieving workload placement flexibility—or the ability to run workloads on whatever cloud they want, on- or off-premises—a top-5 priority among all technology initiatives. This means that the data protection mechanisms will need to demonstrate the same level of flexibility to deliver on the backup and recovery mandates and service levels.

While there is enthusiasm for multi-cloud environments, respondents **generally give the functionality advantage to on-premises environments.** This is particularly true of security and manageability capabilities. As a proof point, 77% of surveyed organizations have repatriated a cloud-resident mission-critical workload (in other words, a high-priority application or set of applications that the business relies on) for a variety of technical and operational reasons.

The following examples were reported by organizations that had deployed specific applications in the cloud (not all users in the study):

- 27% pulled back supply chain management applications.

- 25% pulled back customer relationship management applications.

- 24% pulled back enterprise resource planning applications.

Even among emergent workloads, the percentages were largely consistent:
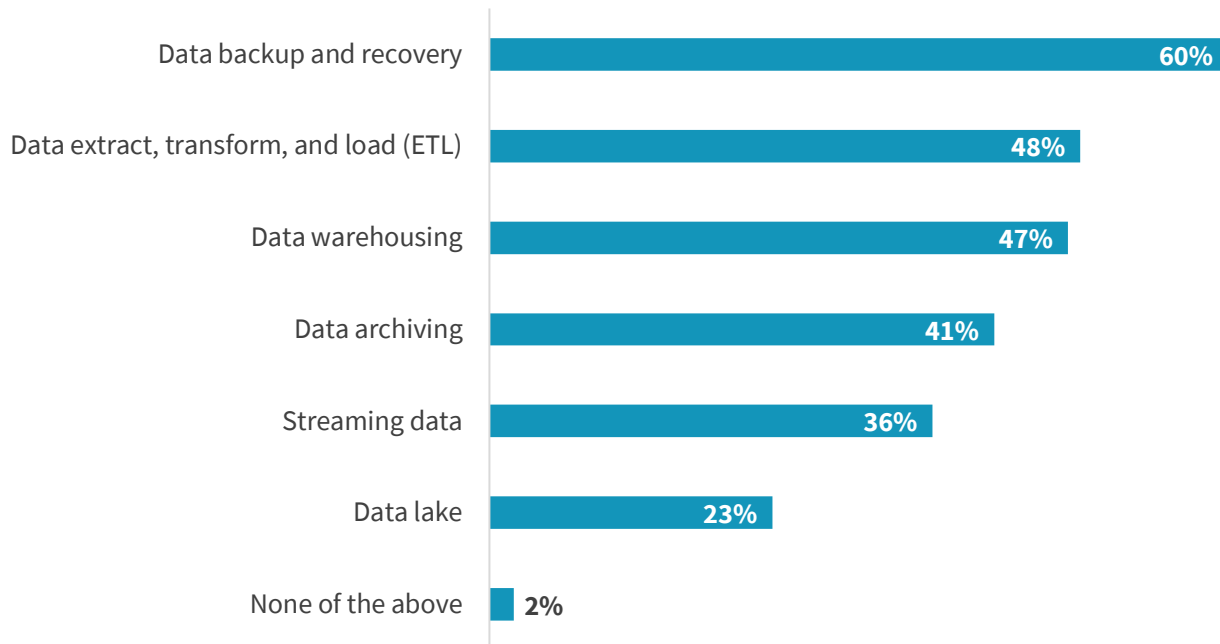
- 25% pulled back a machine learning workload.

- 24% pulled back their data lake environments.

- 23% pulled back big data analytics workloads.

- 21% pulled back deep learning workloads.

Difficulty in implementing security measures, excessive or unpredictable costs, technology and scalability issues, and data backup and recovery, closely followed by archiving, are the main reasons respondents provided for repatriating workloads. Whatever the reason for repatriation of a specific application, as mentioned, the backup and recovery processes "follow" the workload, in this case, back on-premises.

Respondents most often cite data protection as one of the most mission-critical data management workloads for their organization. Many internal stakeholders may have expectations that data protection happens by default, which of course is not the case for the many reasons we have highlighted. This, however, constitutes a mandate for IT professionals and business stakeholders to discuss the role and service levels that are needed for specific business functions or applications, which in turn informs the optimal solution to deploy.

Figure 2. Data Backup and Recovery Top the List of Mission-critical Data Management Workloads

Which of the following data management workloads would you classify as the most mission-critical at your organization? (Percent of respondents, N=1,257, three responses accepted)
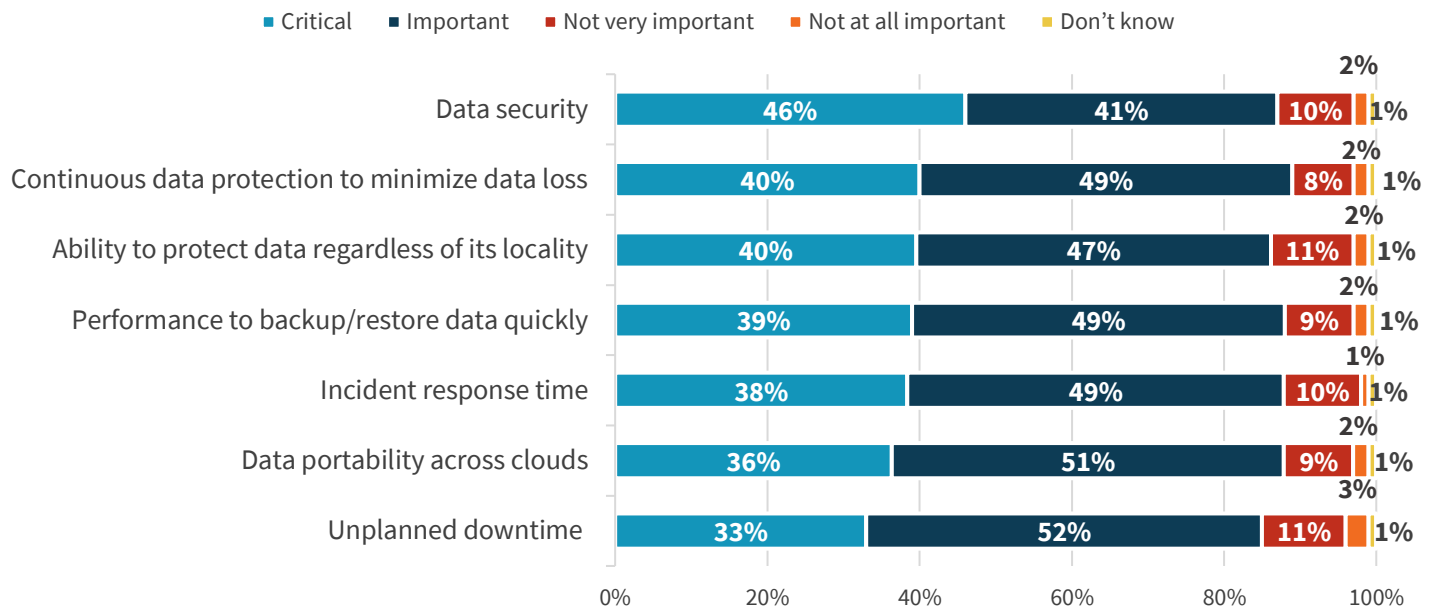
Workload	Percent
Data backup and recovery	60%
Data extract, transform, and load (ETL)	48%
Data warehousing	47%
Data archiving	41%
Streaming data	36%
Data lake	23%
None of the above	2%

Source: Enterprise Strategy Group

Data Protection as a Critical Factor for Hybrid Cloud Success

While 89% of IT professionals feel that continuous data protection is critical to hybrid cloud success, 87% feel the same about data security and the ability to protect data regardless of location. This means that the solution they deploy must offer the type of agility and functionality that spans multiple locations, on-premises or in the cloud, and topologies that can follow the workloads. Not surprisingly, data security is of prime concern to organizations ESG surveyed, as is the ability to mitigate data loss, or achieve low RPOs.

Figure 3. On-premises Protection Matters for Success in Hybrid Cloud

How important do you believe each of the following on-premises data protection environment characteristics are to achieving an effective hybrid cloud environment? (Percent of respondents, N=1,257)

■ Critical   ■ Important   ■ Not very important   ■ Not at all important   ■ Don't know

Characteristic	Critical	Important	Not very important	Not at all important	Don't know
Data security	46%	41%	10%	2%	1%
Continuous data protection to minimize data loss	40%	49%	8%	2%	1%
Ability to protect data regardless of its locality	40%	47%	11%	2%	1%
Performance to backup/restore data quickly	39%	49%	9%	2%	1%
Incident response time	38%	49%	10%	1%	1%
Data portability across clouds	36%	51%	9%	2%	1%
Unplanned downtime	33%	52%	11%	3%	1%

Source: Enterprise Strategy Group

Benefits from Optimized Data Protection for Multi-Cloud Environments

Data protection has evolved through the years and seen many innovations and technology iterations. While we do not intend to provide an exhaustive list in this paper, based on research and domain expertise, ESG generally defines "optimized" data protection as having the ability to perform backup and advanced, feature-rich recovery of data on-premises and in the cloud (cloud as a target or as a source), including SaaS. This includes the ability to protect physical and virtual environments as well as applications running on container infrastructure and optimizing storage consumption with deduplication. Optimized data protection solutions are designed to be easy to use yet offer advanced management and reporting capabilities and can be run as services. Optimized data protection is evolving to become intelligent data management.

Taking a broader perspective on cloud, successful cloud strategies, in part, can be defined as having strong hybrid cloud capabilities: The ability to choose between public cloud and private cloud technologies according to workload and business needs, not arbitrary outside factors.

IT must deliver services more quickly in a cloud-centric world, but also economically. Optimized data protection technologies help IT organizations achieve those goals. By allowing organizations to protect data wherever it resides, with confidence, organizations can roll out new cloud services (whether on- or off-premises) quickly, knowing that the protection mechanisms behind those services have them covered. Indicative of this, when ESG asked respondents what percentage of cloud projects are completed behind, on, and ahead of

Organizations with optimized data protection environments reported completing 57% more of their projects ahead of schedule

schedule, those with optimized data protection environments reported completing 57% more of their projects ahead of schedule (33% versus 21%).

Organizations with optimized data protection environments reported completing 59% more of their projects under budget
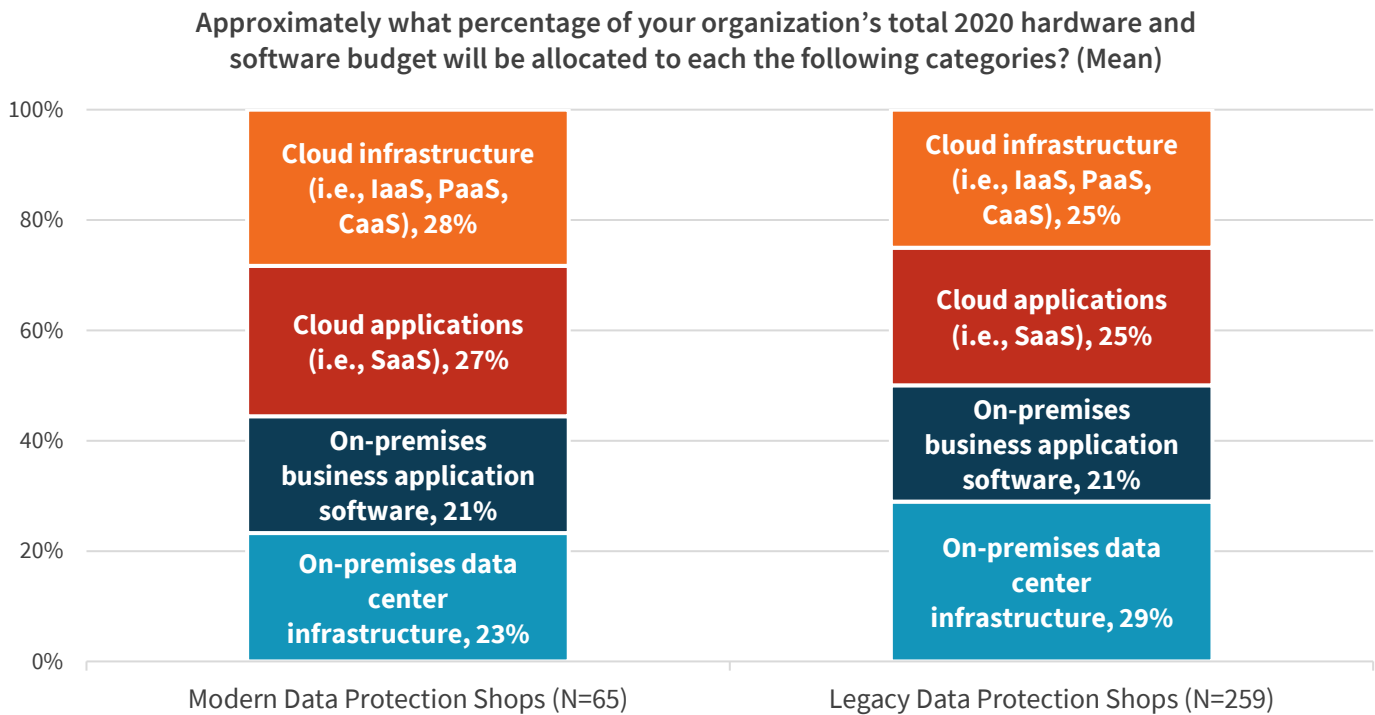
A big part of any cloud project's cost is manpower. The time of developers, IT architects, security architects, and data protection specialists is expensive, so getting projects done faster also means getting them done more cost effectively. When ESG asked respondents what percentage of cloud projects are completed under, on, and over budget, those with optimized data protection environments reported completing 59% more of their projects under budget (27% versus 17%).

Investments to optimize data protection appear to pay off in reduced future-facing on-premises infrastructure spending. "Legacy" data protection shops are allocating 26% more budget to modernizing on-prem infrastructure (29% versus 23%). Based on previous ESG research, the average enterprise's annual IT budget is approximately US$167M.[2] The opportunity to reallocate 6% of the IT budget (or just over US$10M for the average enterprise) to more strategic projects can have a very big impact.

One way to look at this data as an end-user is to consider that if you have a solid, optimized data protection environment, you do not have to throw money at updating or upgrading it. The environment is also less time-consuming to manage. That is all part of why we see these organizations having to allocate 6% less of their budget to on-prem infrastructure.

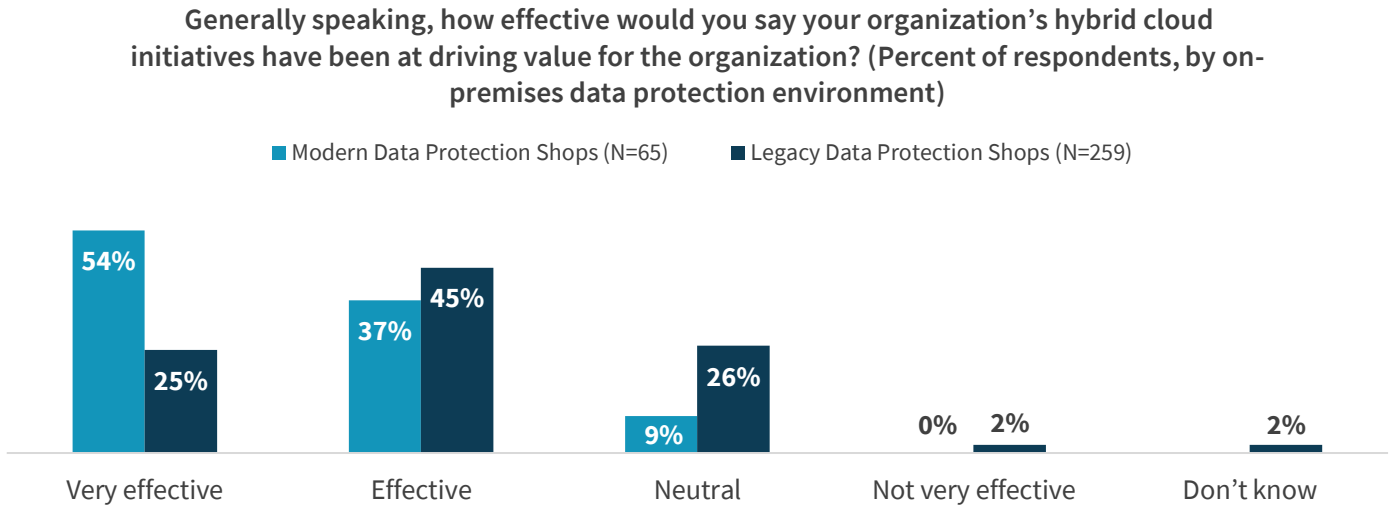**Figure 4. On-premises Infrastructure Spending Efficiencies**

Approximately what percentage of your organization's total 2020 hardware and software budget will be allocated to each the following categories? (Mean)

Modern Data Protection Shops (N=65):
- Cloud infrastructure (i.e., IaaS, PaaS, CaaS), 28%
- Cloud applications (i.e., SaaS), 27%
- On-premises business application software, 21%
- On-premises data center infrastructure, 23%

Legacy Data Protection Shops (N=259):
- Cloud infrastructure (i.e., IaaS, PaaS, CaaS), 25%
- Cloud applications (i.e., SaaS), 25%
- On-premises business application software, 21%
- On-premises data center infrastructure, 29%

Source: Enterprise Strategy Group

Data protection "touches" everything in IT by virtue of its mission and its data-centricity. It seems logical that having an optimized data protection solution by design or as an adjustment to the evolving infrastructure helps with operational

---

[2] Source: ESG Master Survey Results, 2020 Technology Spending Intentions Survey, January 2020.

efficiency beyond just data protection. Our research highlights that 91% of IT organizations with optimized data protection environments actually report that they are effective at driving value with hybrid cloud initiatives (see Figure 5). When data protection needs are met, and also seamlessly and fully integrated across environments, it not only makes IT a hero but also frees up critical time that can be spent elsewhere, running the business and driving new initiatives.
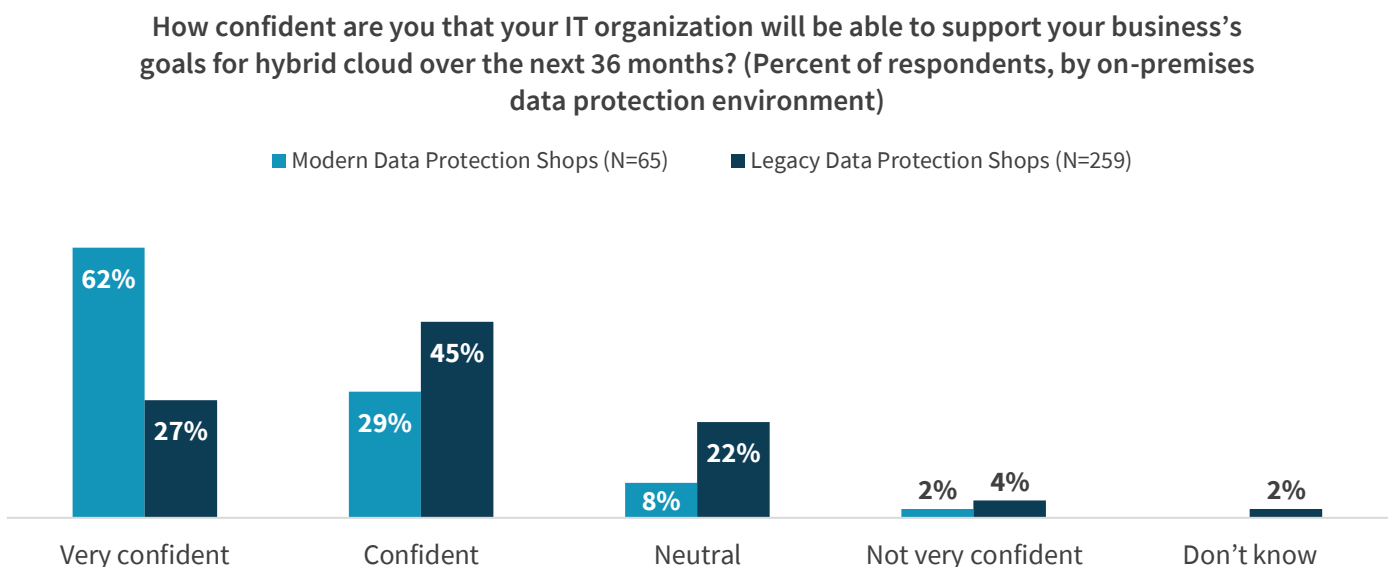
Figure 5. Hybrid Cloud Initiatives Are More Effective with Modern Storage

Generally speaking, how effective would you say your organization's hybrid cloud initiatives have been at driving value for the organization? (Percent of respondents, by on-premises data protection environment)

■ Modern Data Protection Shops (N=65)   ■ Legacy Data Protection Shops (N=259)

	Very effective	Effective	Neutral	Not very effective	Don't know
Modern	54%	37%	9%	0%	
Legacy	25%	45%	26%	2%	2%

Source: Enterprise Strategy Group

In addition, previous success in achieving hybrid cloud goals thanks to optimized data protection translates to an overall higher level of confidence in a business's ability to accomplish its hybrid cloud goals in the future (see Figure 6). Three-fifths (62%) of organizations with optimized data protection environments are very confident in their ability to support hybrid cloud goals over the next three years, 2.3 times the frequency of legacy data protection shops (see Figure 7). Also, IT organizations at modern data protection shops are 48% more likely than their legacy counterparts to be viewed as competitive differentiators by the c-suite (40% versus 27%).

Figure 6. Confidence in IT to Support Business Goals for Hybrid Cloud

How confident are you that your IT organization will be able to support your business's goals for hybrid cloud over the next 36 months? (Percent of respondents, by on-premises data protection environment)

■ Modern Data Protection Shops (N=65)   ■ Legacy Data Protection Shops (N=259)

	Very confident	Confident	Neutral	Not very confident	Don't know
Modern	62%	29%	8%	2%	
Legacy	27%	45%	22%	4%	2%

Source: Enterprise Strategy Group

The Bigger Truth

Optimized data protection infrastructures set the tone for success in hybrid cloud environments, and influence business, financial, and technical success beyond just data protection. Improving and optimizing data protection technologies is a key step in setting an organization up for successful hybrid cloud initiatives.

Data protection is a great learning ground for IT as it encompasses a variety of IT disciplines and must deliver against RPOs and RTOs that can be stringent in order to support the business and the many applications it relies on. The best practices and skills derived from this effort can be applied to many other projects.

This results in improved abilities to succeed in hybrid cloud environments while increasing executive-level confidence. This "virtuous circle" can also be identified in other areas. It is interesting to note that compared with organizations with legacy data protection infrastructure, those with optimized data protection infrastructure also report positive outcomes on cloud projects in general terms, and higher value from their hybrid cloud initiatives.

The future of IT is hybrid cloud topologies, and that's where we expect to see continuing innovation in the data protection space.

How Dell Technologies Can Help

This ESG Research Insights Paper was commissioned by Dell Technologies, VMware, and Intel Corporation, all of which are keenly focused on helping organizations achieve their cloud goals.

Together, Dell Technologies, VMware, and Intel Corporation are driving innovation and next-generation capabilities with the broadest portfolio of trusted infrastructure, cloud, and data protection solutions. This comprehensive portfolio of hardware, software, and services enables organizations to easily adopt transformative technologies to maximize performance, compete, and thrive in the new digital economy.

Dell EMC Data Protection solutions for the cloud, multi-cloud, and hybrid cloud help customers transform their data centers to enable greater operational efficiency, resiliency, and scalability throughout the entire cloud infrastructure. Additionally, Dell Technologies APEX delivers the industry's broadest end-to-end portfolio of consumption-based and as-a-Service solutions ideally suited for the way on-premises infrastructure and services are consumed in the on-demand economy.

To learn more about Dell EMC Data Protection Solutions for Cloud, start here.

# Appendix – Research Methodology and Respondent Demographics

To gather data for this report, ESG conducted a comprehensive online survey of IT decision makers from private- and public-sector organizations in 11 countries: US (33%), Canada (4%), UK (13%), France (9%), Germany (7%), Singapore (5%), Australia (5%), India (4%), Hong Kong (3%), Brazil (8%), and Mexico (8%). The survey was fielded between September 17, 2019 and October 12, 2019. To qualify for this survey, respondents were required to have influence in the purchase of cloud investments (public or private) at organizations utilizing public cloud infrastructure and operating modernized on-premises data center environments.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 1,257 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

The figures below detail the demographics of the respondent base: individual respondents' current job responsibilities, as well as respondent organizations' total number of employees and primary industry.
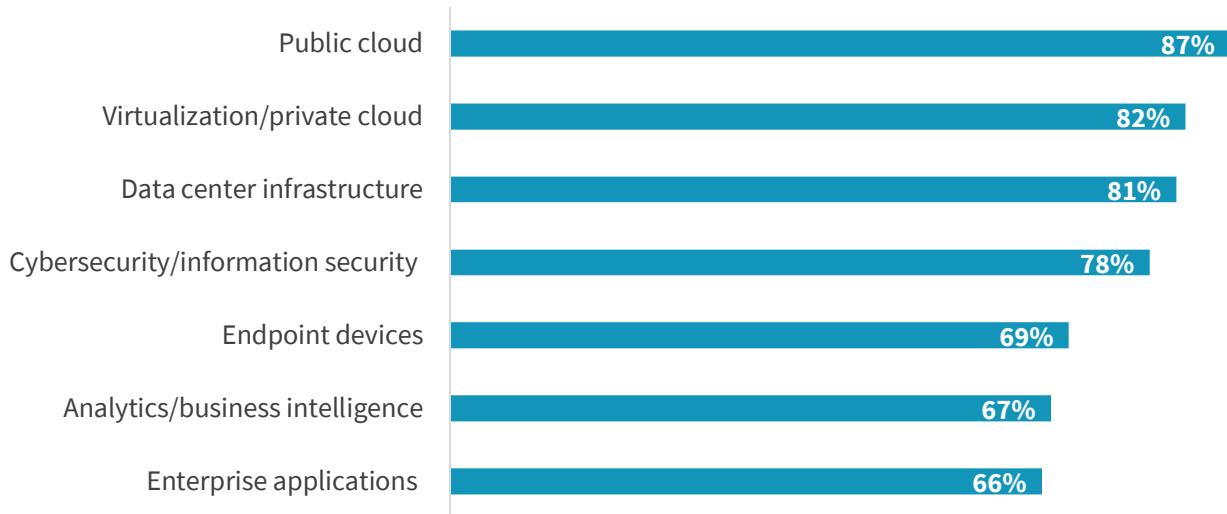
Figure 7. Survey Respondents, by Job Title/Level

Which of the following best describes your current job title/level? (Percent of respondents, N=1,257)
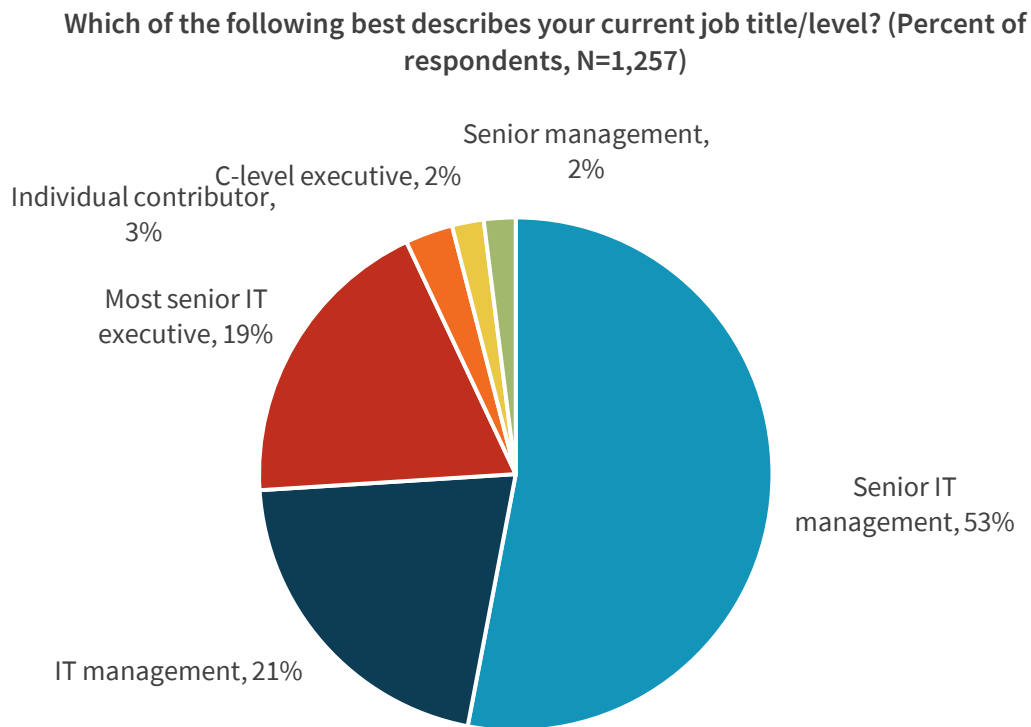
Source: Enterprise Strategy Group

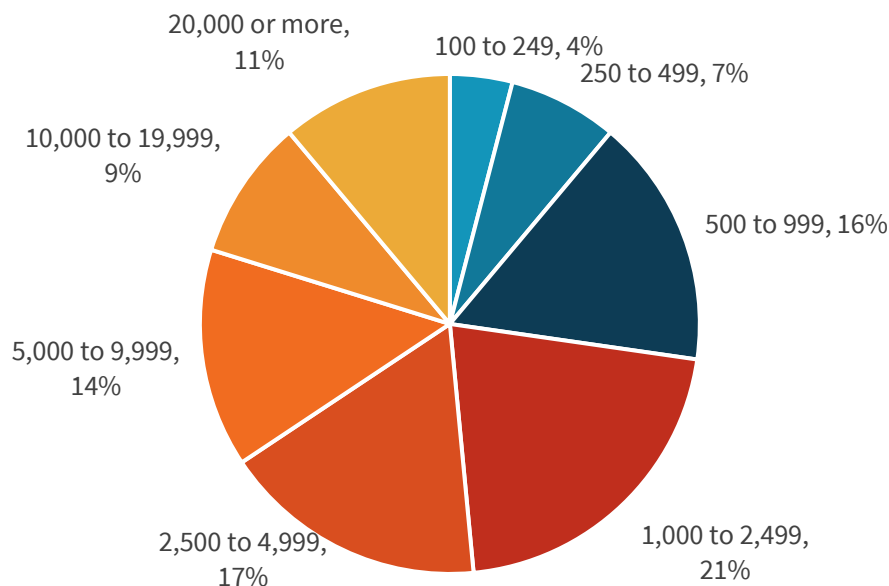**Figure 8. Survey Respondents, by IT Responsibility Areas**

In which of the following areas of IT do you have significant involvement in the purchase process for your company? (Percent of respondents, N=1,257, multiple responses accepted)

Public cloud	87%
Virtualization/private cloud	82%
Data center infrastructure	81%
Cybersecurity/information security	78%
Endpoint devices	69%
Analytics/business intelligence	67%
Enterprise applications	66%

Source: Enterprise Strategy Group

Figure 9. Survey Respondents, by Company Size (Number of Employees)

How many total employees does your organization have worldwide? (Percent of respondents, N=1,257)

- 100 to 249, 4%
- 250 to 499, 7%
- 500 to 999, 16%
- 1,000 to 2,499, 21%
- 2,500 to 4,999, 17%
- 5,000 to 9,999, 14%
- 10,000 to 19,999, 9%
- 20,000 or more, 11%

Source: Enterprise Strategy Group

Figure 10. Survey Respondents, by Industry

What is your organization's primary industry? (Percent of respondents, N=1,257)

- Other, 15%
- Technology, 26%
- Government, 2%
- Business services, 5%
- Communications & media, 7%
- Manufacturing, 17%
- Healthcare, 8%
- Retail/wholesale, 9%
- Financial, 11%

Source: Enterprise Strategy Group

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