Enterprise Strategy Group | Getting to the bigger truth.™

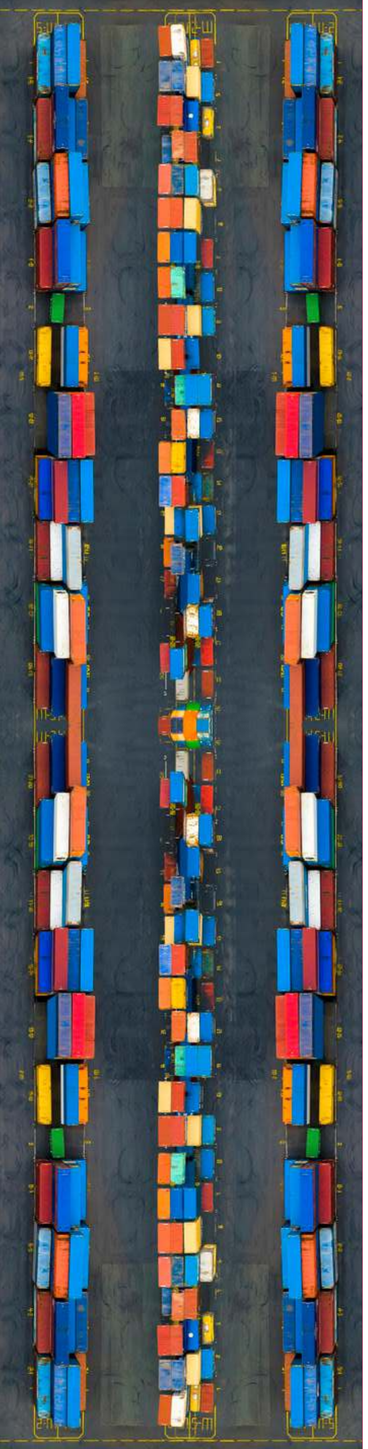
RESEARCH HIGHLIGHTS

Data Protection Trends and Strategies for Containers

Christophe Bertrand, ESG Senior Analyst

SEPTEMBER 2020

CONTENTS



Research Objectives

Container adoption is accelerating and so too is the requirement to properly protect container environments and the data in them. ESG research indicates that, so far, IT professionals are kicking the can down the road. While many recognize the growing importance of containers relative to other vital application platforms, confidence levels in the ability to protect containerized workloads are lagging. As was the case with other recent disruptive shifts in the IT landscape, including the VMware and cloud computing phenomena, newer data protection approaches are needed.

In order to gain insight into these trends, ESG surveyed 334 IT professionals at organizations in North America (US and Canada) personally responsible for or familiar with their organization's container-based application environment and strategy, including the associated data protection tools and processes. Respondents' organizations must have had or been planning to deploy a container-based application environment. This research aimed to understand the current state of end-users' application and container deployments, identify data management gaps, and highlight future expectations. Container backup methodologies will be explored to determine IT professionals' current practices and potential disconnects that may exist when protecting the Kubernetes/containers infrastructure at scale, providing additional insights into market dynamics and contrasts.

THIS STUDY SOUGHT TO:

Assess the level of adoption of containers and their associated backup and recovery processes, including deployment size.

Examine the buying intentions of IT teams regarding container infrastructure backup and recovery. Assess existing strategies and uncover expectations gaps.

Understand the existing challenges and drivers influencing container infrastructure backup, including technical hurdles spanning on-premises and cloud environments.

Gauge buyer preferences for deployment topologies, and better understand the criteria decision makers are prioritizing.

Back to Contents

Research Highlights

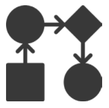
Containers adoption is in full acceleration and in position to become the go-to choice for production deployment in 24 months. Containers adoption is pervasive, with more than two-thirds of respondents already in production with these environments. Looking ahead to the next 24 months, the momentum continues, resulting in containers becoming the more widely used platform for production deployment, ahead of virtual machines.

Hybrid and multi-cloud strategies are intricately linked to containers deployments. Container technology is essentially hybrid with a majority of respondents reporting that their solutions will be deployed in a combination of cloud platforms and on-premises. More than three-quarters use cloud services as a container DR repository, with 47% identifying cloud as the sole destination for these secondary data copies.

There is a shared mandate beyond backup and recovery personas when it comes to the decision-making process for data protection of containers. Container backup and recovery is clearly a shared mandate in which backup and recovery personas are merely influencers, and more importantly, they do not own the container backup budget. While not owners of the budget, data protection teams still retain a significant influence in the technical decision process.

Hybrid and multi-cloud strategies complicate container backup, and the future looks to be split between incumbent backup and container-specific solutions. Hybrid cloud and multi-cloud environments present the most pressing challenges for IT professionals focused on managing backup/DR for containers. Currently, the vast majority of organizations report using their incumbent backup vendors to protect their container environment, but going forward, there is an expected shift toward purpose-built solutions.

There seems to be a big disconnect when it comes to container backup and recovery. It is apparent that many IT professionals may not be looking at the right metrics to help set business-appropriate SLAs for containers when it comes to data protection. Further demonstrating what appears to be a disconnect in terms of data protection, most IT professionals wrongly assume container-based applications can be backed up the same way individual applications are protected.



Still a lot of work left to align data recovery SLA expectations with reality. In this research, respondents were asked not only about their organizations' container application recovery time and point objectives, but also about the results. Overall, organizations reported success in terms of application recovery times, which were very much in line with expectations, but there is a significant discrepancy in terms of data recovery metrics.

Back to Contents

Containers adoption is in full acceleration and in position to become the go-to choice for production deployment in 24 months.

Container Adoption Is Full Speed Ahead and about to Become the Production Platform Of Choice

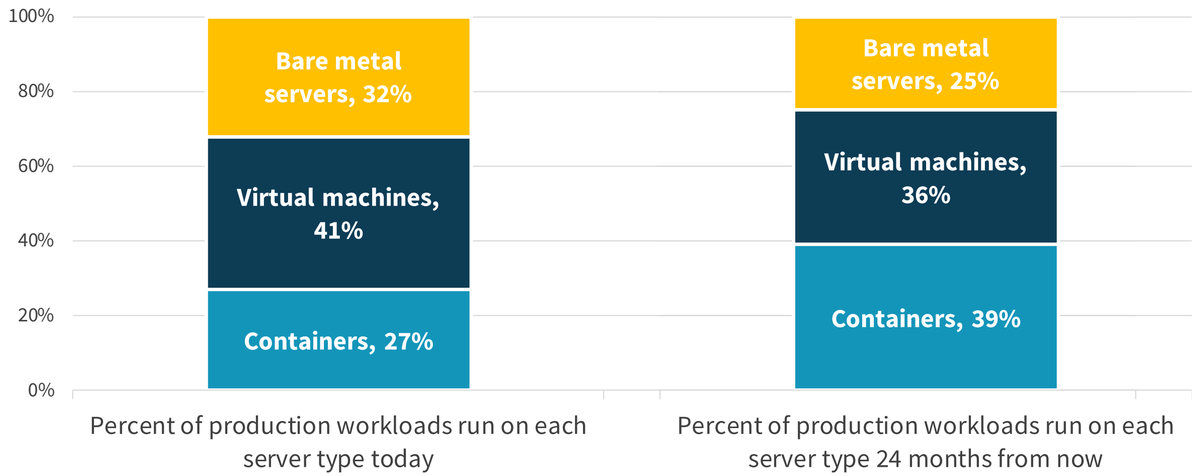
67%

currently use containers for production applications

Against a backdrop of accelerating digital transformation, it is not surprising that containers would be a popular technology to leverage on-premises and in the cloud. ESG's research shows that containers adoption is in full acceleration with more than two-thirds of respondents already in production with these environments. It should also be noted that the remainder actually use containers in test/dev environments exclusively but have plans to transition them to production environments in 12 months.

Production means that certain service levels must be met in order to comply with the often-stringent demands of business, among which are data protection SLAs. Looking ahead to the next 24 months, the momentum continues, resulting in containers becoming the more widely used platform for production deployment, ahead of virtual machines. This is a significant and fundamental shift that, in turn, points to a domino effect of changes across IT.

APPROXIMATE PERCENTAGE BREAKDOWN OF THE PRODUCTION APPLICATIONS/WORKLOADS RUNNING ON EACH SERVER TYPE TODAY AND IN 24 MONTHS.

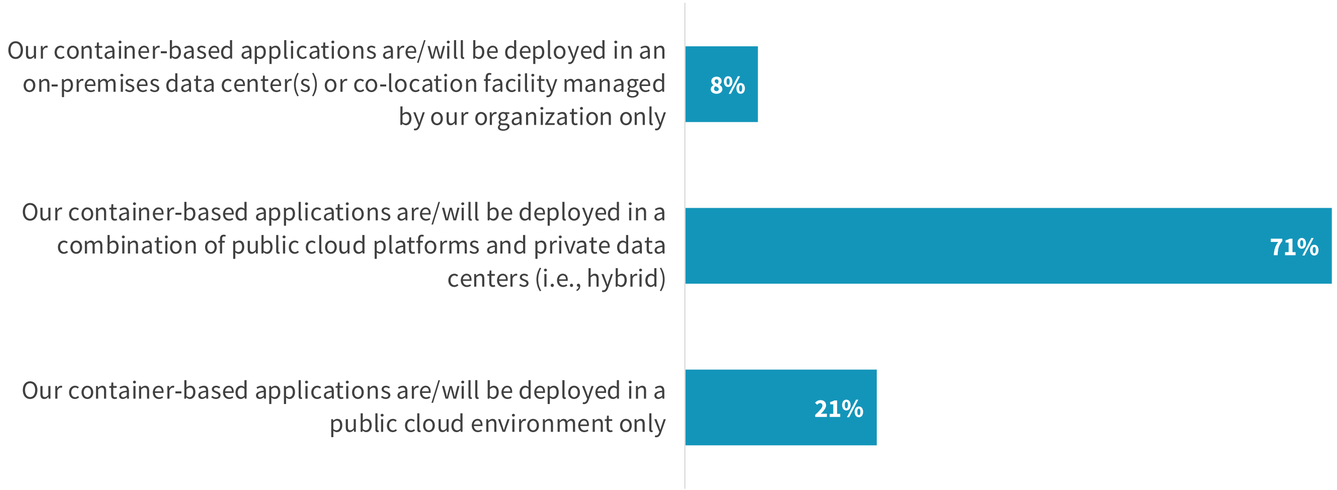


Back to Contents

Multi-cloud and Hybrid Are Vital to Containers Strategies

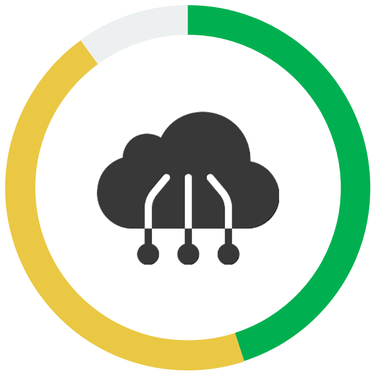
Containers can help fuel digital transformation efforts via faster, more nimble business application deployments that can quickly accommodate changing requirements and evolutions. In today's IT world, container technology is essentially hybrid, with a majority of respondents reporting that their solutions will be deployed in a combination of cloud platforms and on-premises. This multi-platform flexibility expectation directly impacts technology choices when it comes to container backup and recovery support for multi-cloud environments, making it an important or very important capability for 90% of respondents.

HOW CONTAINERS ARE BEING DEPLOYED/UTILIZED.



IMPORTANCE OF HAVING A CONTAINER BACKUP AND RECOVERY MANAGEMENT SOLUTION THAT WORKS ACROSS MULTIPLE DISPARATE PUBLIC CLOUD INFRASTRUCTURE SERVICES.

Container backup and recovery support for multi-cloud environments was rated as an important/very important capability for 90% of respondents.



45%

Very important, we plan to deploy across multiple disparate public cloud infrastructure service providers

45%

Important, we would prefer a multi-cloud management solution, but we can get by without it

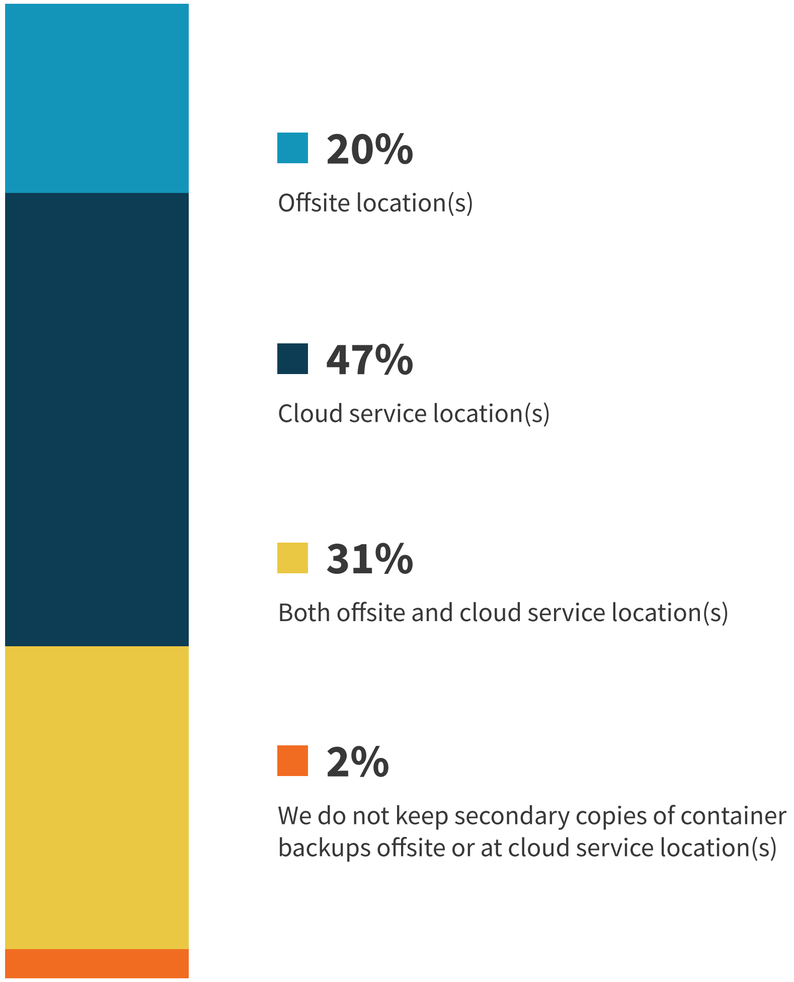
Back to Contents

Cloud Is Key For Container Disaster Recovery Copies

In addition to the fact that hybrid and multi-cloud strategies are intricately linked to containers deployments, it should be noted that cloud is considered a key topology for container disaster recovery secondary copies. Indeed, more than three-quarters use cloud as a container DR repository, with 47% identifying cloud as the sole destination for these secondary data copies.

More than three-quarters use cloud as a container DR repository with 47% identifying cloud as the **sole destination** for these secondary data copies.

LOCATION OF SECONDARY COPIES OF CONTAINER BACKUPS KEPT FOR DR PURPOSES.



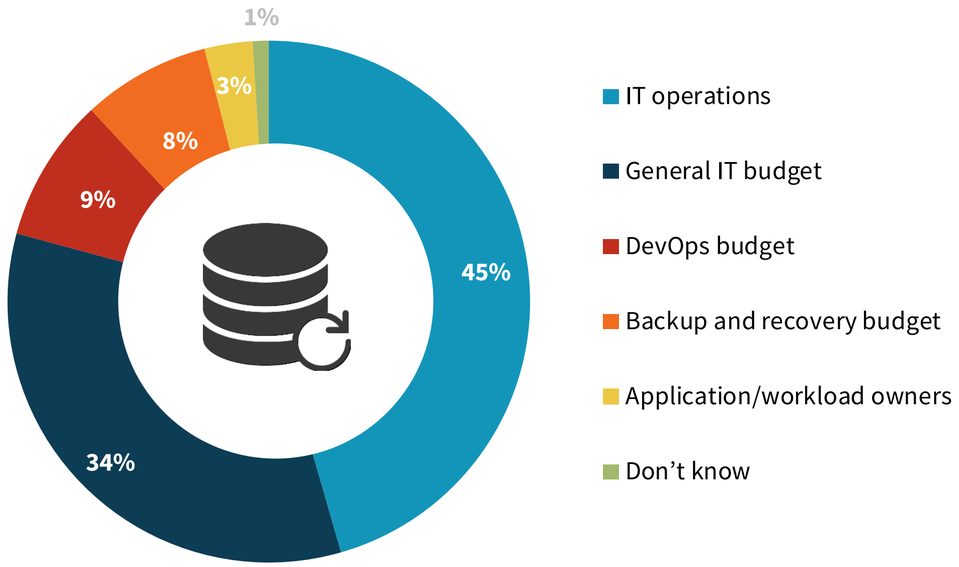
Back to Contents

There is a shared mandate beyond backup and recovery personas when it comes to the decision-making process for data protection of containers.

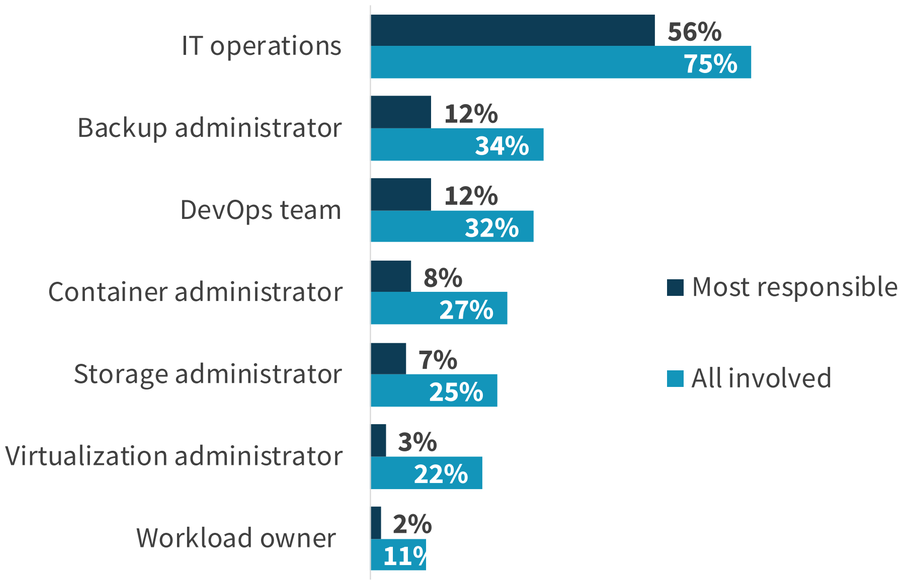
IT Operations Runs the Container Backup and Recovery Show

As is often the case in the space of backup and recovery, multiple stakeholders influence decisions, such as the workload owners, the business/functional leaders, and IT leadership tasked with mandates to support key service-level metrics. Container backup and recovery is clearly a shared mandate in which backup and recovery personas are merely influencers, and more importantly, they do not own the container backup budget. In turn, this means additional groups are playing a role in the decision-making process for data protection of containers. It can be an opportunity for IT, DevOps, and backup stakeholders to create a balanced approach to define and enable successful data protection SLAs for the container infrastructure. It also comes with a risk, as there can be significant differences in priorities and understanding of the technology and data protection processes across diverse IT subgroups.

GROUP RESPONSIBLE FOR FUNDING THE BACKUP AND RECOVERY BUDGET FOR APPLICATION CONTAINERS.



GROUPS RESPONSIBLE FOR MANAGING THE BACKUP AND RECOVERY OF CONTAINER-BASED ENVIRONMENT.

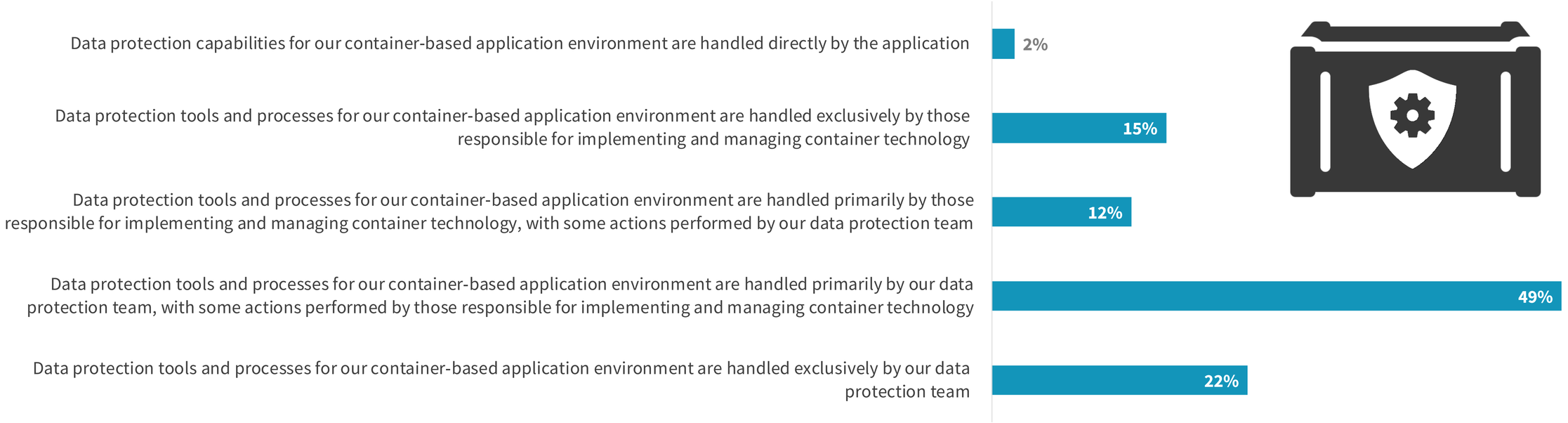


Back to Contents

Data Protection Responsibility Is Primarily a Shared Mandate

The tool selection process ownership provides a more precise picture of how organizations will approach their technology choices for container backup and recovery. While not owners of the budget, data protection teams still retain a significant influence in the technical decision process, but only in slightly more than one in five cases is it an exclusive decision ownership. For vendors and channel players, this highlights the fact that sales and marketing motions will require an adjustment in order to engage with a broader set of decision makers and influencers compared to traditional data protection efforts.

DATA PROTECTION STRATEGY FOR CONTAINER-BASED APPLICATION ENVIRONMENT.



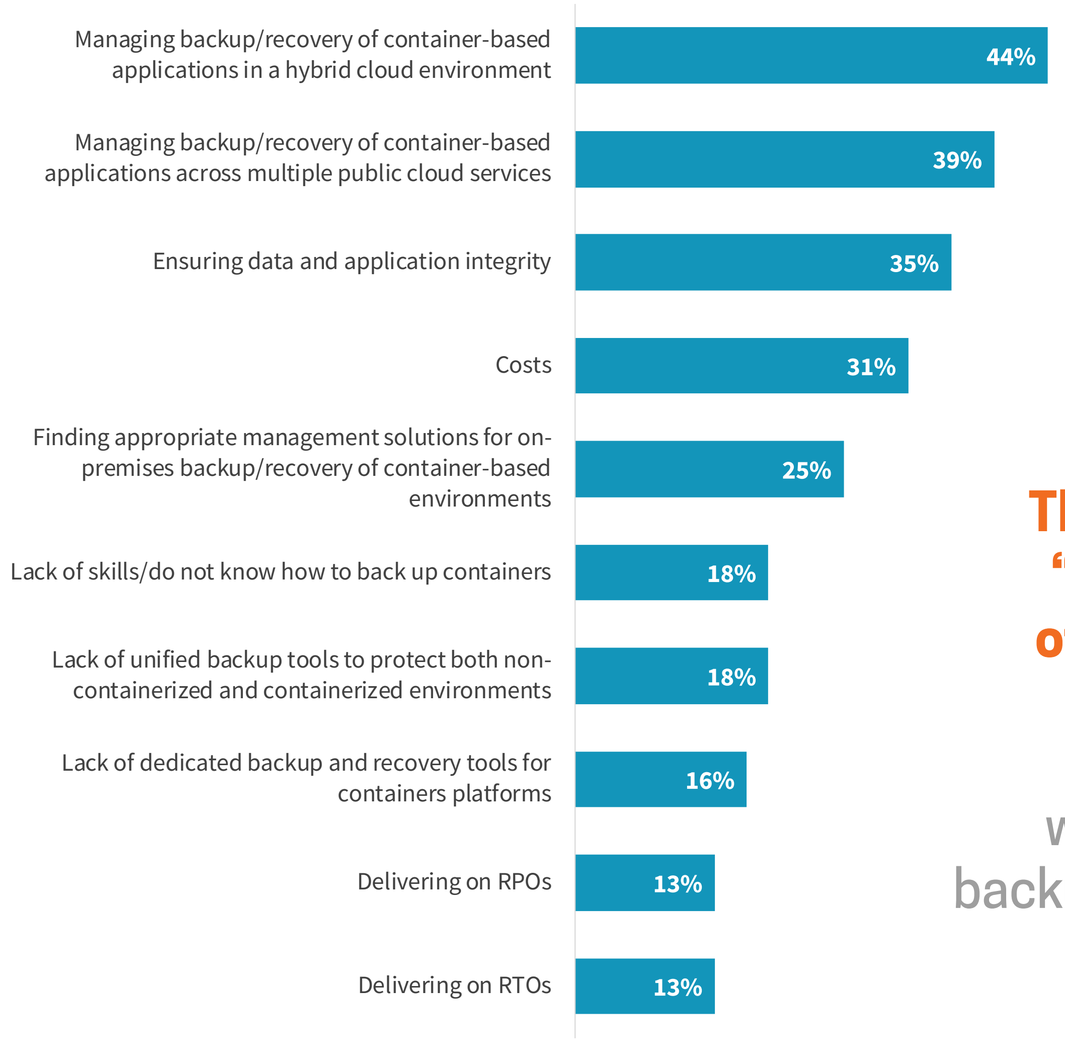
Back to Contents

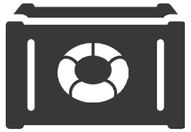
Hybrid and multi-cloud strategies complicate container backup, and the future looks to be split between incumbent backup and container-specific solutions.

Cloud Complexity and Data Integrity Are the Most Common Container Backup Impediments

When new technologies are deployed in production, challenges invariably come up as adoption grows wider and systems take on a more critical business role. There is a natural "domino effect" of deploying new technologies in production when it comes to backup and recovery. New technology means that backup and recovery solutions have to adjust to adequately protect the environment. This can mean re-architecting processes and solutions or supporting new environments and hybrid topologies. Hybrid cloud and multi-cloud environments present the most pressing challenges for IT professionals focused on managing backup/DR for containers. IT professionals are also struggling with ensuring data and application integrity, and delivering on SLAs, which represents a fundamental issue that must be fixed. The lack of container-specific backup tools is also often reported as a challenge and may be a reason for the aforementioned data and application integrity issues.

BIGGEST CHALLENGES RELATED TO MANAGING BACKUP/DISASTER RECOVERY FOR CONTAINER ENVIRONMENTS.





There is a natural "domino effect" of deploying new technologies in production when it comes to backup and recovery.

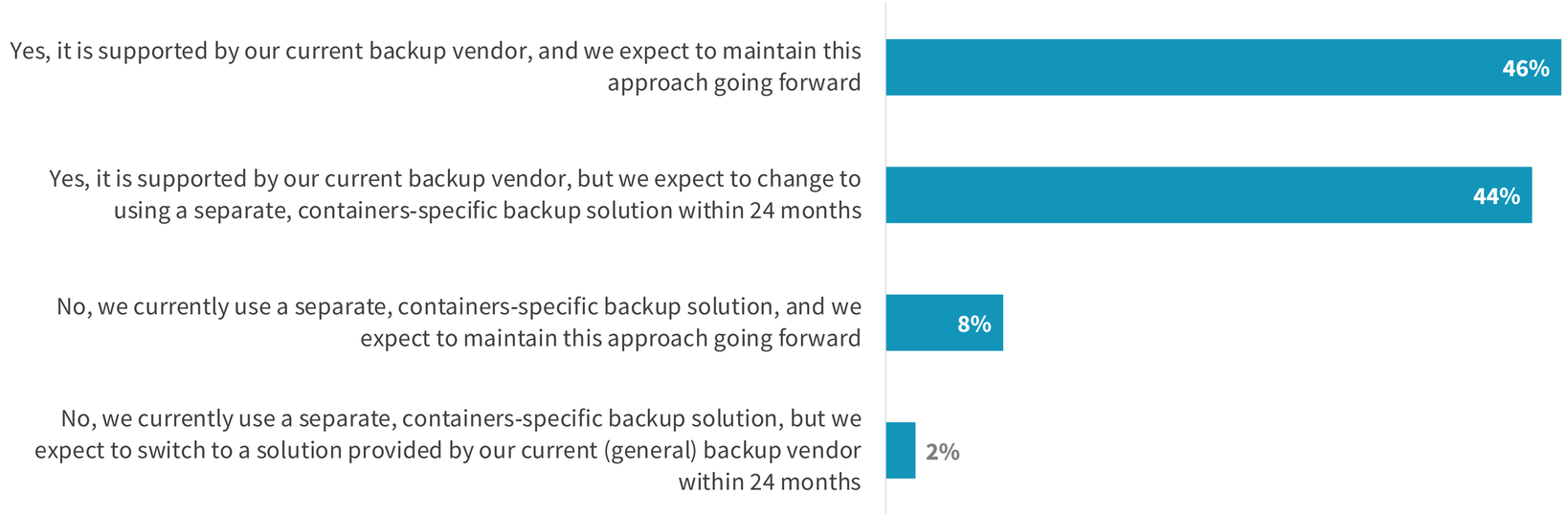
Back to Contents

While Most Currently Use Incumbent Backup Vendors, the Majority Expect to Switch to a Container-specific Solution

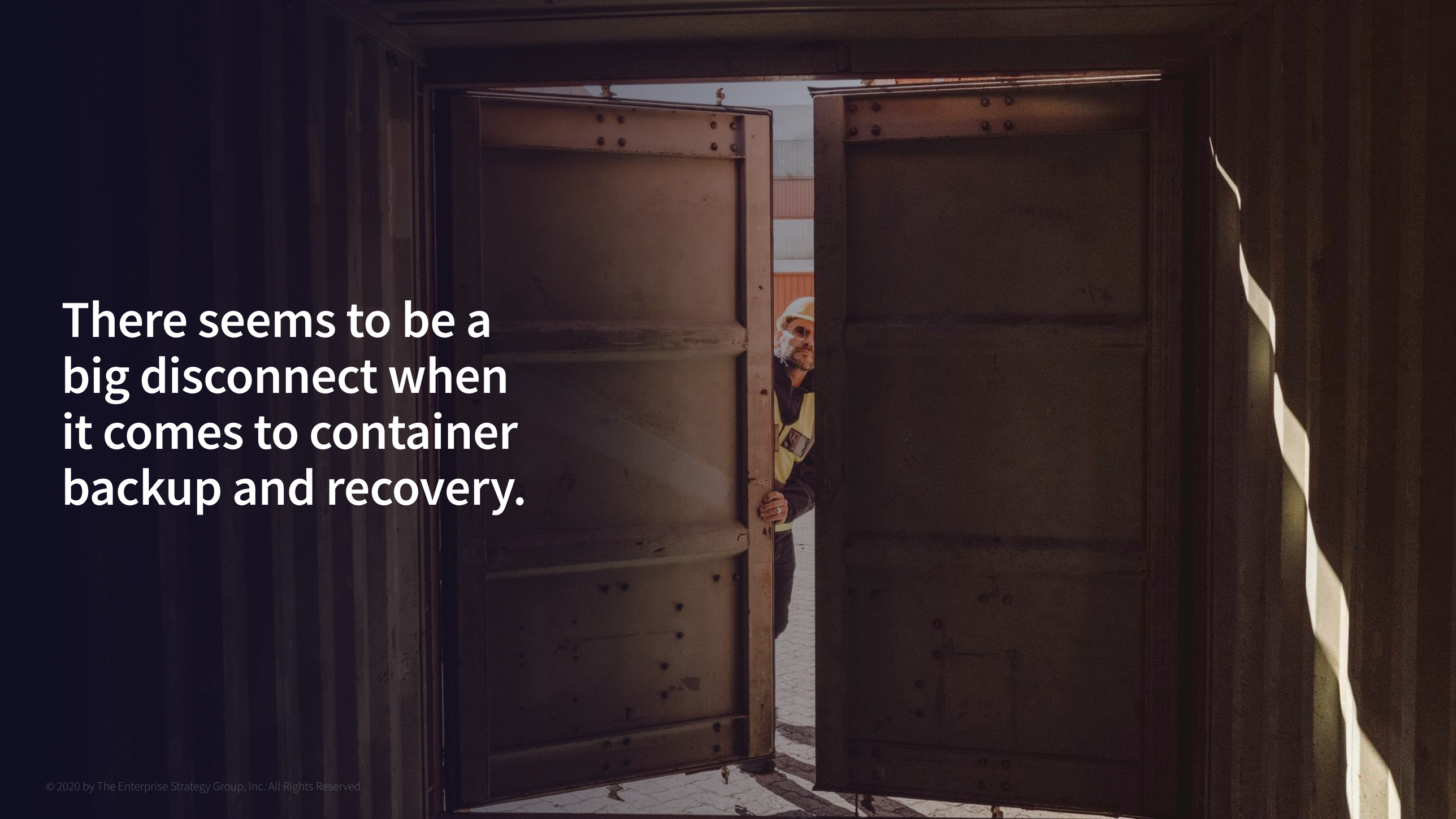
With the knowledge of the most common container backup challenges, including the ties to hybrid and multi-cloud environments, respondents were asked if their organization's container backup schema integrates with its current data protection environment. Currently, the vast majority of organizations report using their incumbent backup vendors to protect their container environment. However, going forward, there is an expected shift toward purpose-built solutions, with 52% planning to use container-specific backup technology.

There is an expected shift toward purpose-built solutions, with 52% planning to use container-specific backup technology.

DOES CONTAINER BACKUP SCHEMA INTEGRATE WITH CURRENT DATA PROTECTION ENVIRONMENT?



Back to Contents



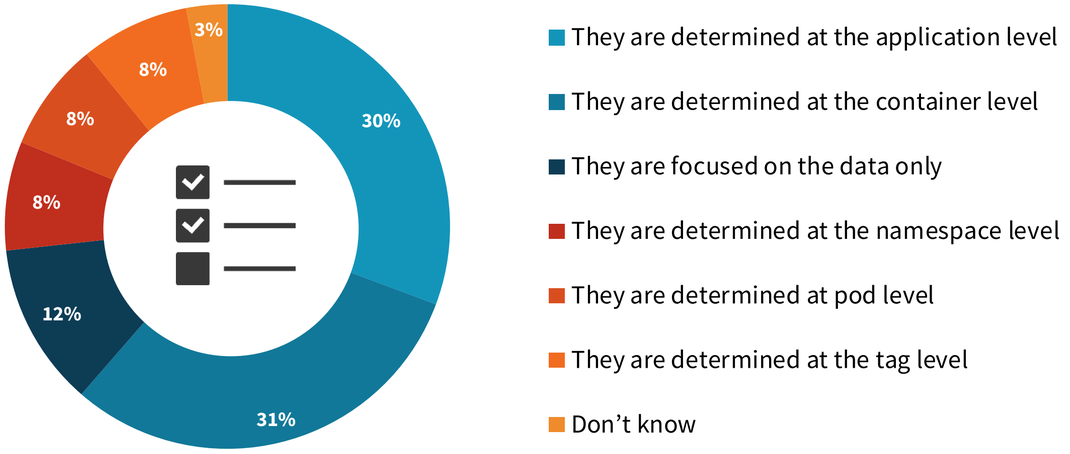
There seems to be a big disconnect when it comes to container backup and recovery.

No Clear Consensus on SLA Determination, Further Underscoring Container Backup Confusion

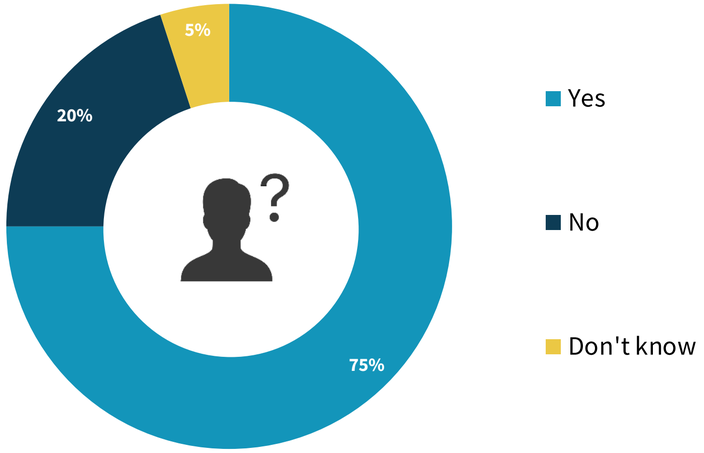
As containers continue their penetration of production environments, data protection SLAs become more critical: Downtime is costly and disruptive. Upon closer inspection, it is apparent that many IT professionals may not be looking at the right metrics to help set business-appropriate SLAs for containers when it comes to data protection. More than one-third take a restrictive view by only looking at data (12%), namespace (8%), pod-level (8%), and tag-level (8%) when they should be focused on application- or container-level data protection. This is because of the need to achieve coherent and complete data protection and therefore deliver on recoverability. In other words, backing up only data won't restore containers themselves.

Further demonstrating what appears to be a disconnect in terms of data protection, most IT professionals wrongly assume container-based applications can be backed up the same way individual applications are protected. It should be noted that this type of disconnect is also presenting itself in other areas of technology, for example with SaaS backup recently and virtual machines many years ago. Clearly, increased market education and improved messaging are needed.

HOW SLAS OF BACKUP AND RECOVERY FOR CONTAINER ENVIRONMENTS ARE DETERMINED.



CAN CONTAINER-BASED APPLICATIONS BE BACKED UP THE SAME WAY INDIVIDUAL APPLICATIONS ARE BACKED UP?

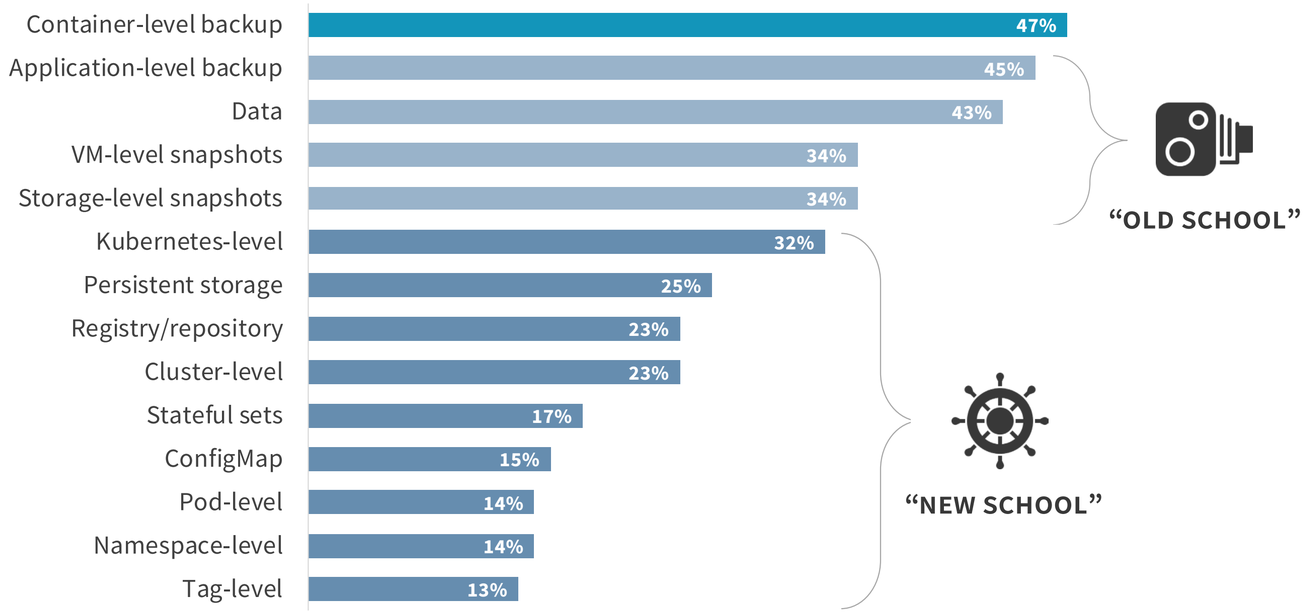


Back to Contents

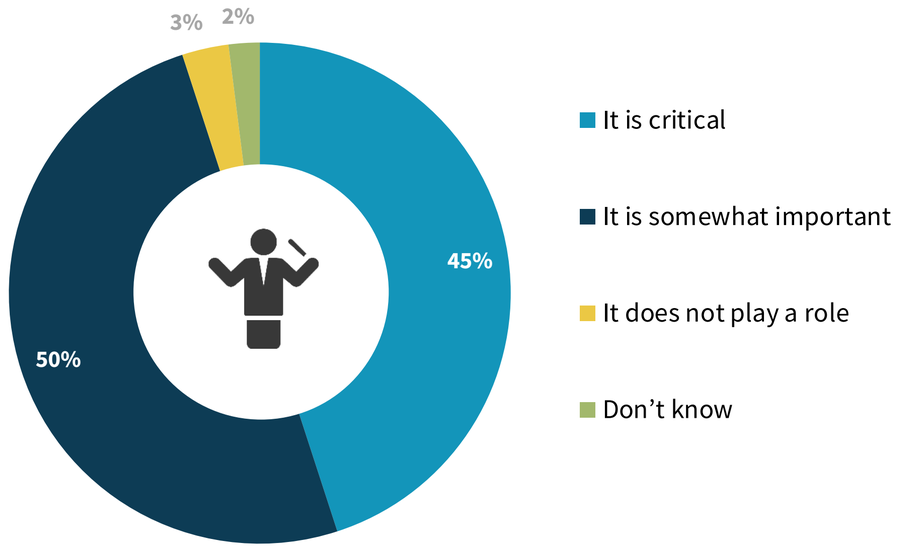
Double-clicking on Data Protection Components Vital to Container Backup

Additional insight on the more granular technical understanding of respondents confirms that there is a high degree of confusion in the market, which could lead to missed SLAs and data loss if the wrong approach is selected. This presents an opportunity for vendors to demonstrate thought leadership (for those that have a solution) and educate the market that the "old way" will not work and is actually risky. A specific emphasis on orchestration capabilities would be an additional area on which to focus as it is essential to successful backup and recovery of container environments. Indeed, while orchestration is critical, especially at scale, more than one out of two don't see it that way.

RESOURCES REQUIRED TO SUPPORT SUCCESSFUL AND CONSISTENT BACKUP AND RECOVERY OF CONTAINER ENVIRONMENTS.



ROLE OF ORCHESTRATION IN CONTAINER BACKUP AND RECOVERY.



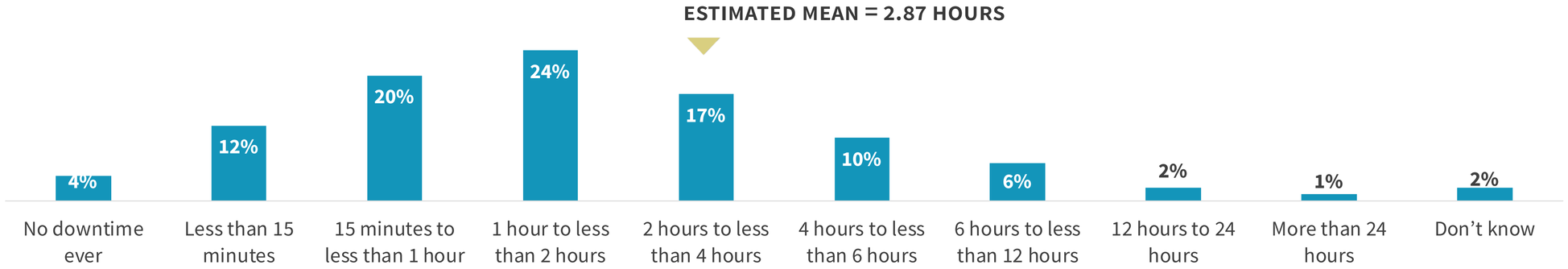
Back to Contents

Still a lot of work left to align data recovery SLA expectations with reality.

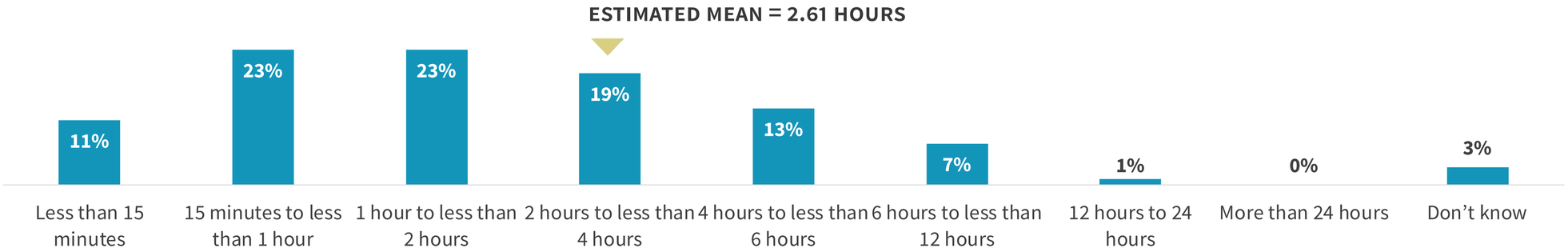
Recovery Time Actuals Are in Line With Expectations

Service level metrics for backup/DR are recovery time objective (RTO), which is how long an outage can last or how long to "get back on your feet," and recovery point objective (RPO), which assesses how much data can be lost and/or the point in time from which it can be recovered. These are typically expressed in hours and minutes to match the majority of business requirements. In this research, respondents were asked not only about these objectives but also about the results (how well they did against their RPOs and RTOs). This is referred to as the "actuals." Overall, organizations reported success in terms of application recovery times, which were very much in line with expectations.

AMOUNT OF DOWNTIME ORGANIZATIONS CAN TOLERATE FROM SERVERS RUNNING CONTAINER-BASED APPLICATIONS/WORKLOADS BEFORE MAKING THE DECISION TO "FAILOVER/RECOVER."



APPROXIMATE LENGTH OF TIME IT TYPICALLY TAKES TO RESUME CONTAINER-BASED APPLICATIONS.

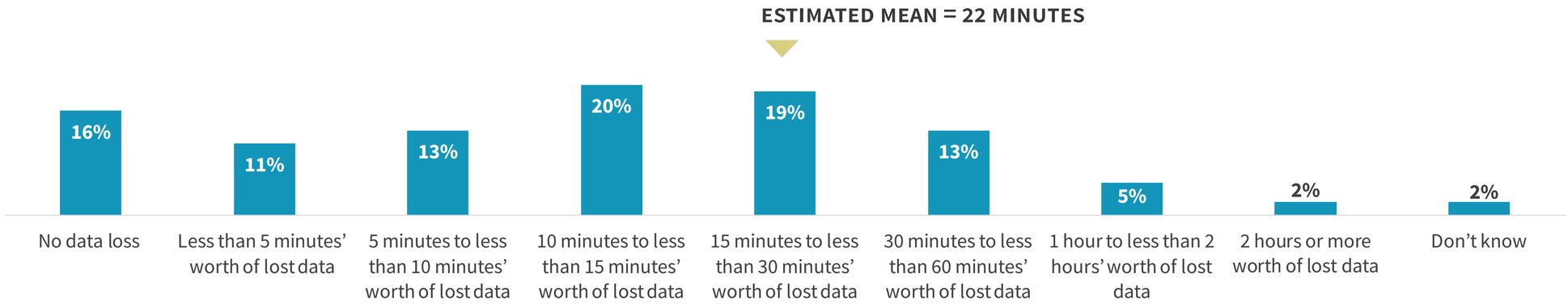


Back to Contents

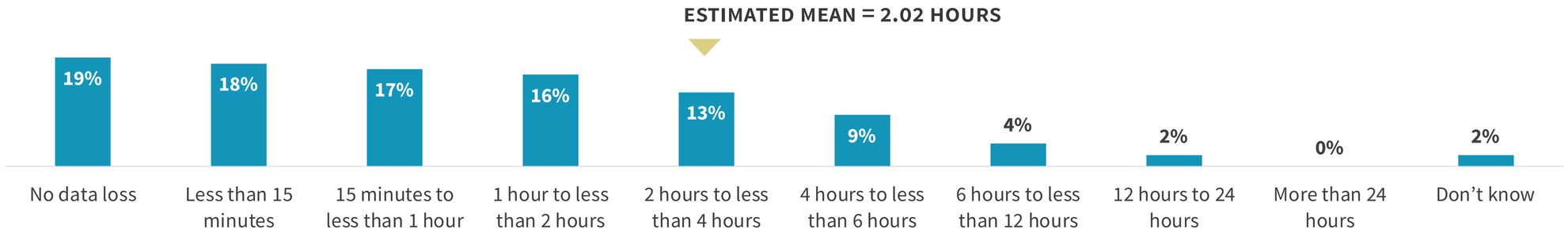
Recovery Point Actuals Reveal Big Container Backup Disconnect

However, the RTO-RTA alignment might suggest a false sense of security. The disconnect on container backup technology previously highlighted appeared more visibly in the recovery point metrics. While RPO is 22 minutes on average, the RPA (recovery point actual) was over 2 hours! This is a significant discrepancy. It is one thing to get the containers and applications back up and running, but it is another thing to get all the data back without losing any previous transactions. The ability to attain both objectives is what IT should deliver. There is lots of work left when it comes to RPOs of containerized applications, which should be a major consideration for further production-grade deployments for mission-critical applications on these platforms.

AMOUNT OF DATA ASSOCIATED WITH CONTAINER-BASED APPLICATIONS THAT CAN BE LOST WITHOUT SIGNIFICANT IMPACT TO THE BUSINESS.



APPROXIMATE AMOUNT OF DATA TYPICALLY LOST WHEN RESUMING CONTAINER-BASED APPLICATIONS.



Back to Contents

Zerto

Zerto helps customers accelerate IT transformation by reducing the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions with a single IT Resilience Platform, Zerto is changing the way disaster recovery, data protection and cloud are managed. With enterprise scale, Zerto's software platform delivers continuous availability for an always-on customer experience while simplifying workload mobility to protect, recover and move applications freely across hybrid and multi-clouds. Zerto is trusted globally by over 8,000 customers, works with more than 1,500 partners and is powering resiliency offerings for 450 managed services providers. Learn more at Zerto.com.

LEARN MORE

ABOUT ESG

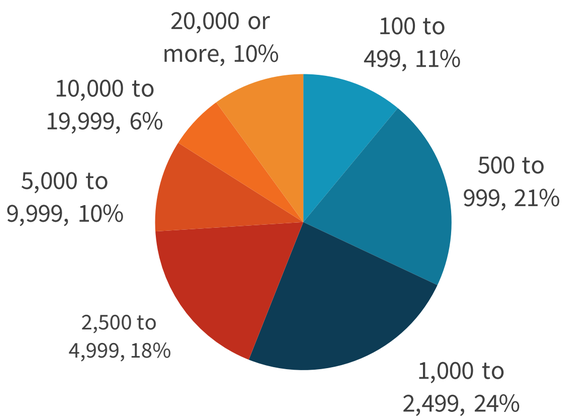
Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

Research Methodology

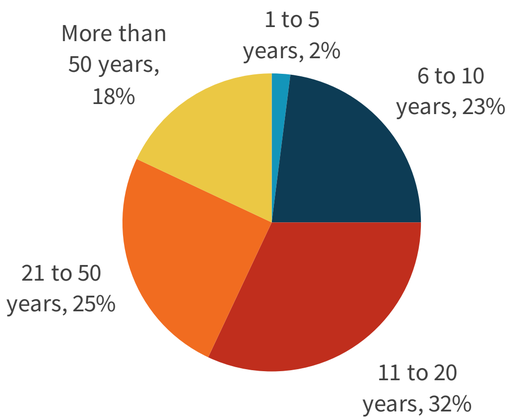
To gather data for this report, ESG conducted a comprehensive online survey of IT professionals from private- and public-sector organizations in North America (United States and Canada) between June 12, 2020 and June 24, 2020. To qualify for this survey, respondents were required to be IT professionals personally responsible for or familiar with their organization's container-based application environment and strategy, including the associated data protection tools and processes. Respondents' organizations must have had or been planning to deploy a container-based application environment. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 334 IT professionals.

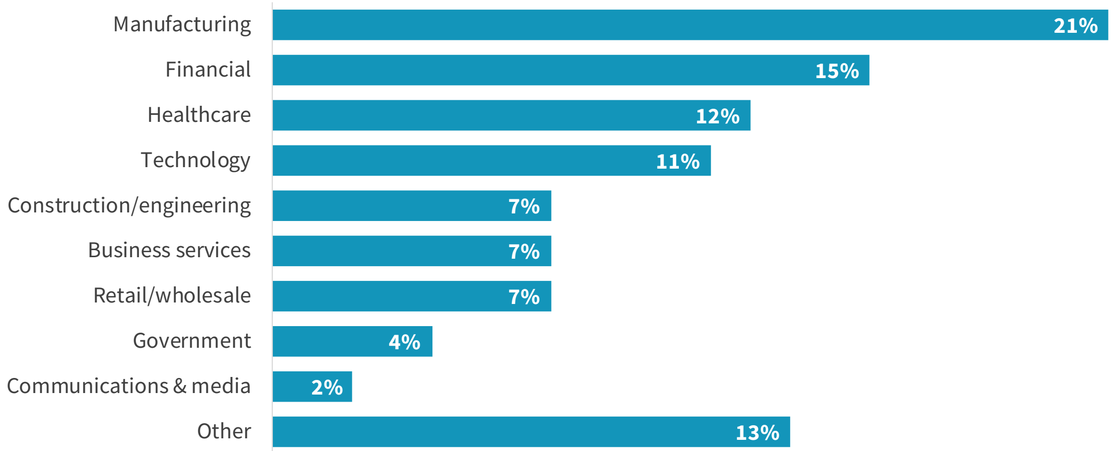
Respondents by Number of Employees



Respondents by Age of Company



Respondents by Industry



Back to Contents