VansonBourne

DELL Technologies

Global Data Protection Index – Cloud Environments

Dell Technologies

Key Findings 2020

1,000 IT decision makers were interviewed in November and December 2019

Organizations from a wide range of public and private sector industries

Organizations with 250+ employees

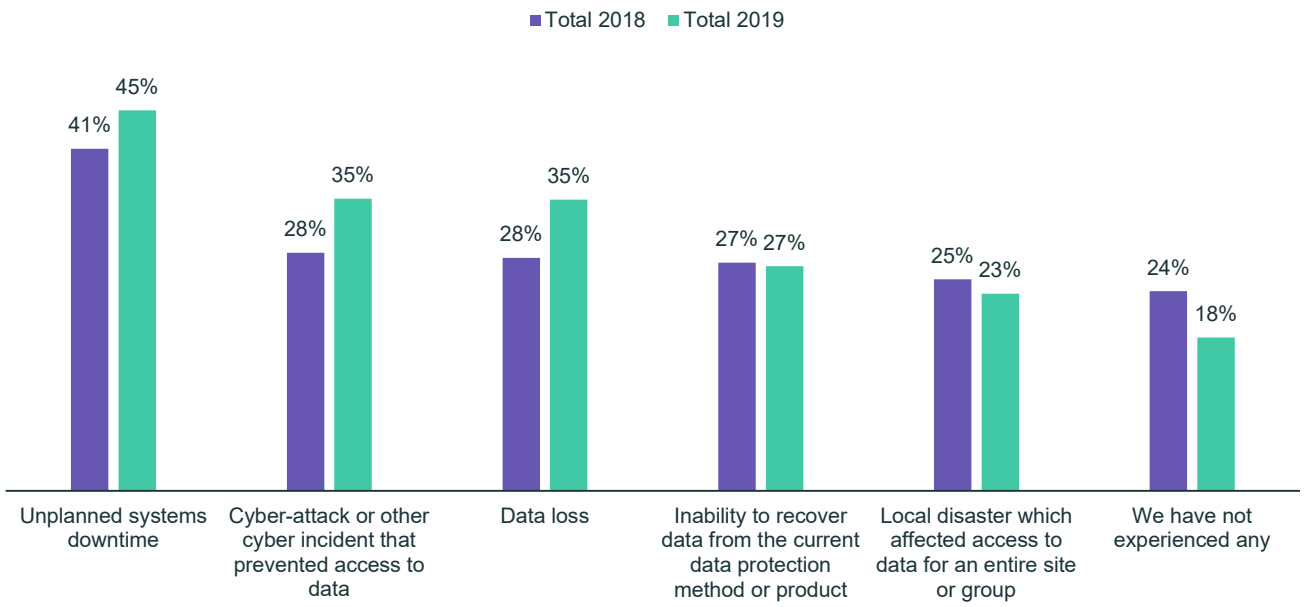
4 regions: Americas (200), EMEA (450), APJ (250), China (100)

Focus of key findings:

1. The rise of disruption
2. Hybrid cloud – the new normal
3. VMware data protection
4. Cloud data protection vulnerability
5. Data protection for newer technologies
6. Increased risk of using multiple data protection vendors

1. The rise of disruption

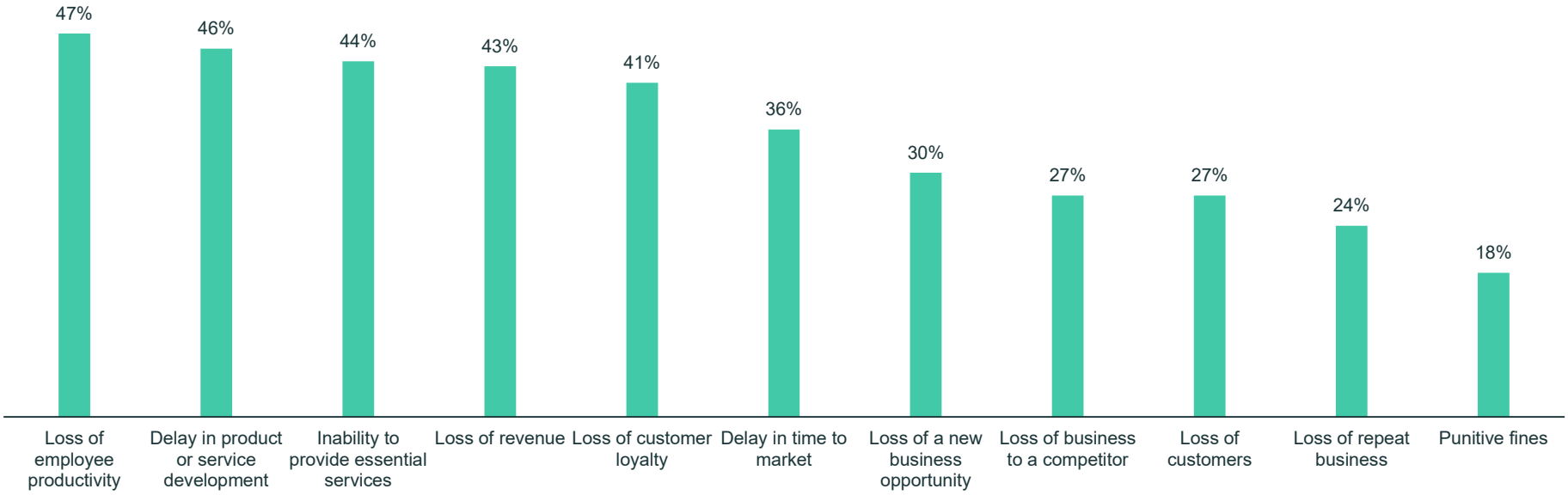
Disruptive events are on the rise, with even more organizations falling victim to one in 2019 compared to 2018



82%

Have **suffered from a disruptive event (e.g. downtime or data loss)** in the last 12 months, compared to **76%** in 2018

Looking beyond the financial damage, disruption also results in a wide range of other consequences for organizations



There is also a considerable lack of confidence in a number of crucial areas relating to the data protection that organizations currently have in place

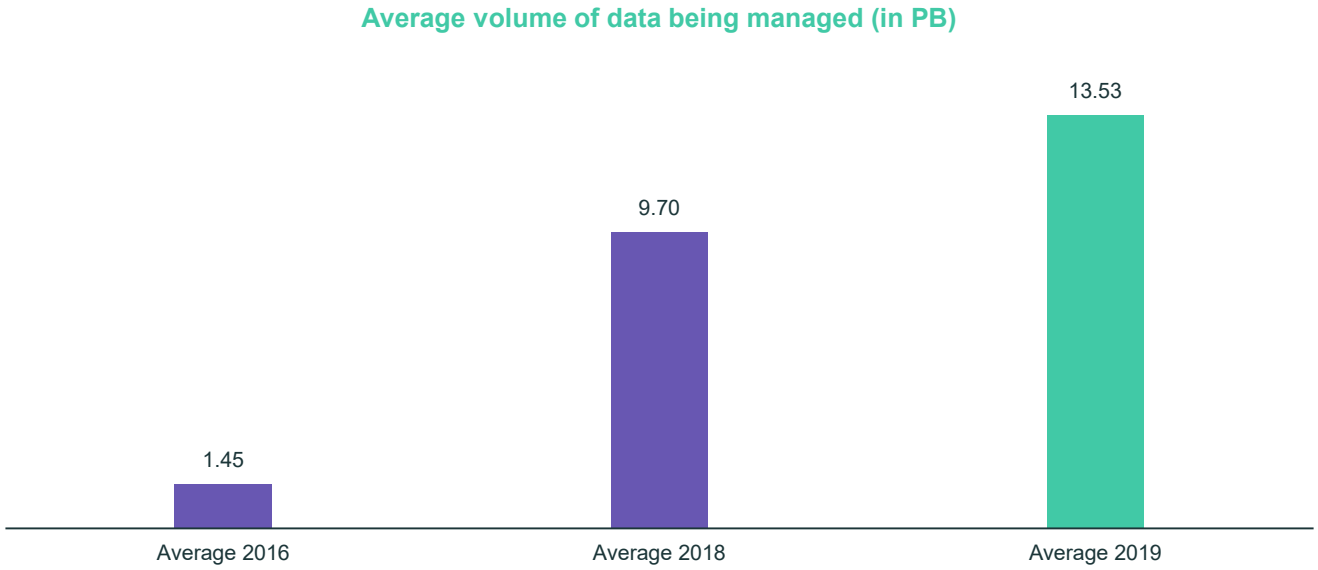
There is a lack of confidence in terms of…

…reliably **recovering all business-critical data** in the event of a cyberattack	**…fully recovering systems/data from all platforms** in the event of a data loss incident	**…compliance with regional data governance regulations**	**…meeting backup and recovery service level objectives**
69%	64%	62%	62%

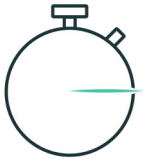
Meanwhile, there is widespread concern that more disruption will be experienced over the next 12 months

The majority (68%) of respondents are concerned that their organization **will experience a disruptive event in the next 12 months** (such as unplanned systems downtime)

Further adding to the challenge of disruption is the growing amount of data that organizations are managing – between 2018 and 2019, data volumes have increased by 39%

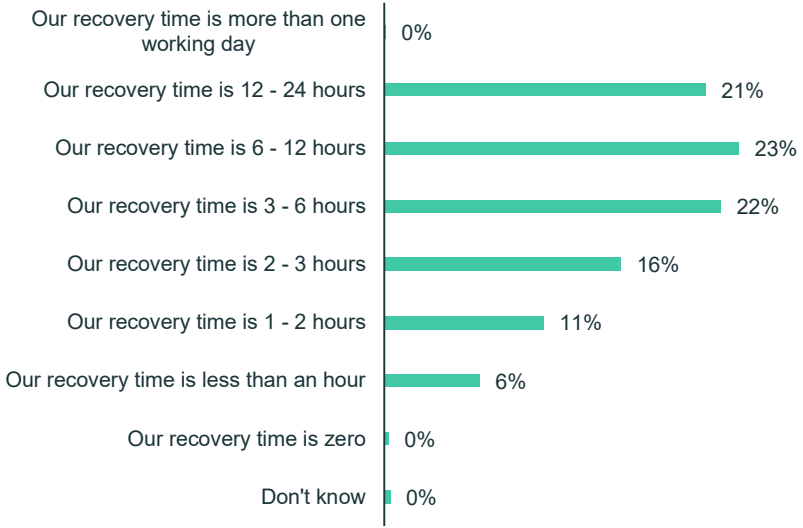


Unexpected downtime to critical applications can take significant time to recover from too – 8 hours on average in 2019



8 hours is the average recovery time should an unexpected event cause downtime to critical applications

(2018 = 7 hrs, 2016 = 7 hrs)



The cost of downtime is also on the up in organizations. Between 2018 and 2019 this increased by 54%, on average

Estimated total cost of downtime in the last 12 months (in USD)

$526,845
In 2018

$810,018
In 2019

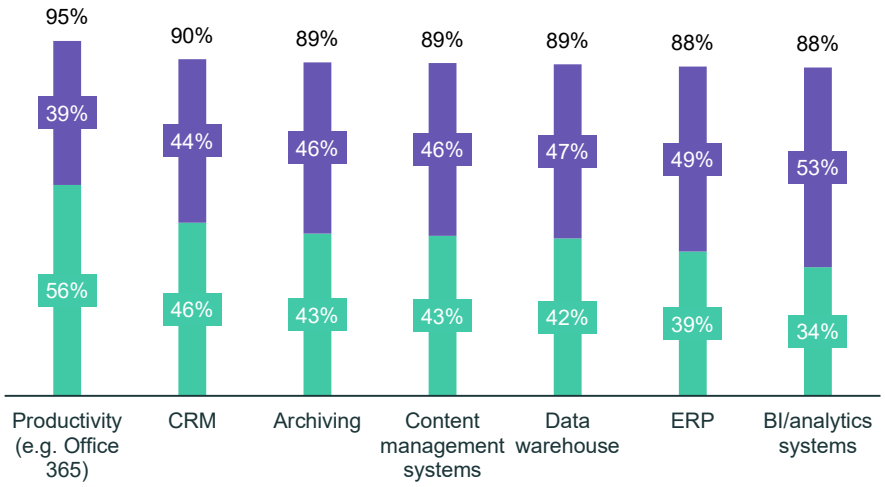
54%

Increase in the **average cost of downtime** between 2018 and 2019

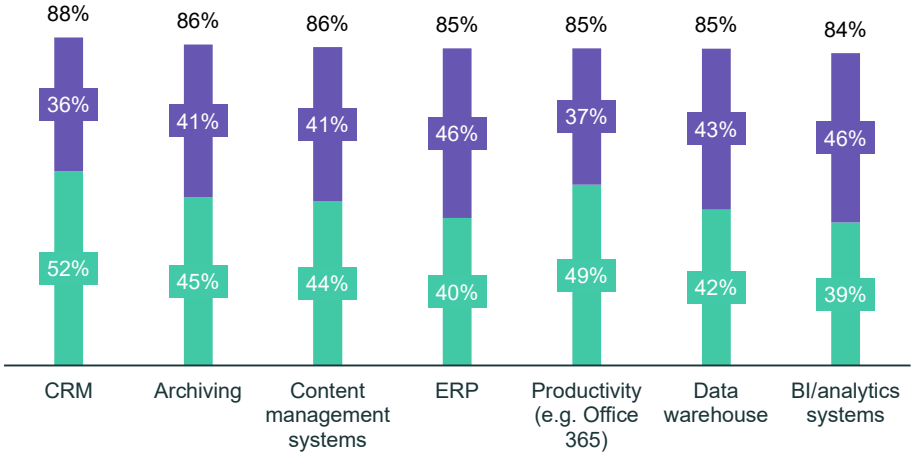
2. Hybrid cloud – the new normal

Most organizations are deploying mission-critical workloads into both public and private clouds

Public cloud

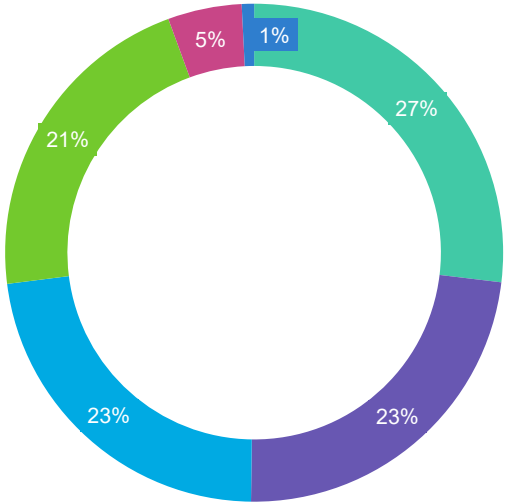


Private cloud



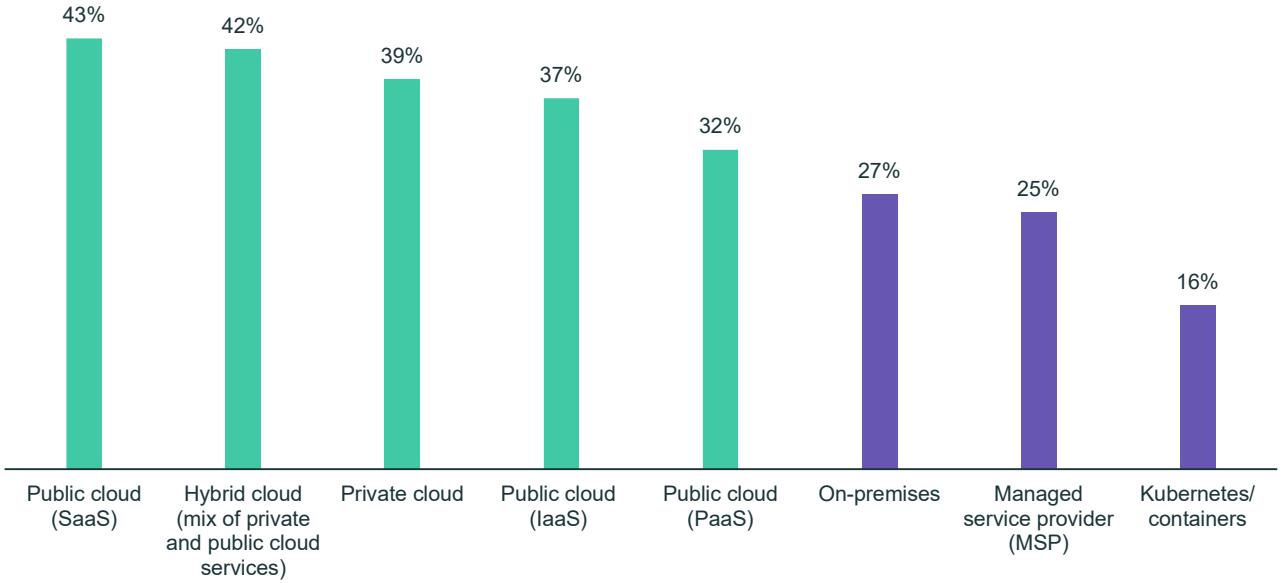
3. VMware data protection

For many, the hybrid cloud approach for application deployments will be based on VMware infrastructure. However, there is no clear standout in terms of how organizations are protecting VMware workloads in the cloud



4. Cloud data protection vulnerability

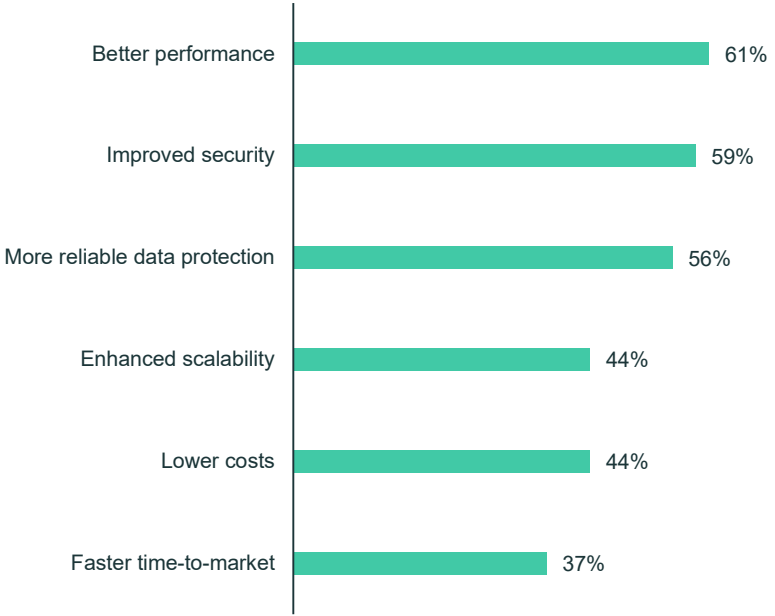
When deploying new applications, most organizations favour a cloud-based deployment model



94%

Choose **cloud deployments** (public, private and/or hybrid) for new applications

The decision to use public cloud when deploying new business applications is driven by a range of important business benefits



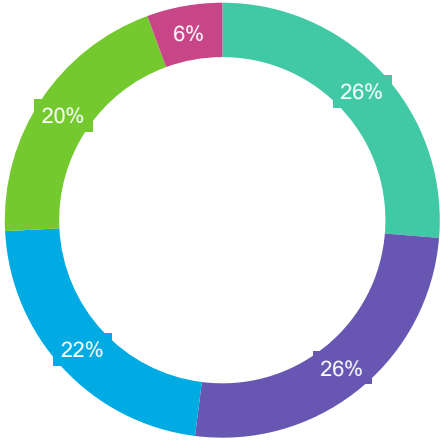
56%

Say the decision to use public cloud when deploying new business applications is driven by **more reliable data protection**

For those running workloads in multiple cloud environments, there is not a clear “go to” in terms of protection

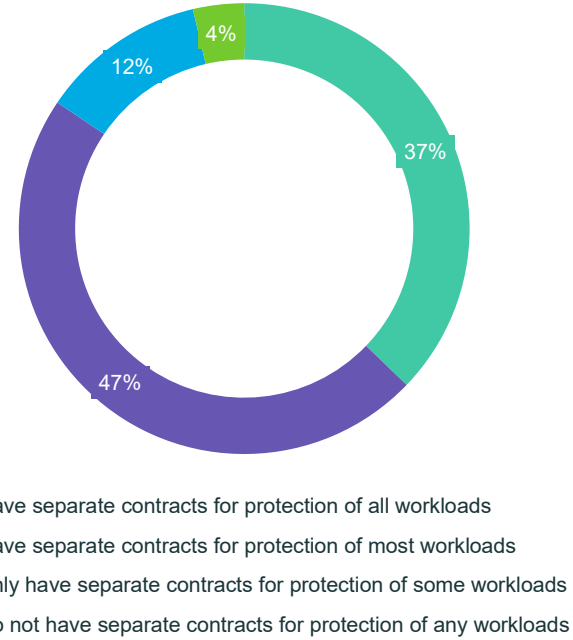
20%

Believe that **responsibility for protecting workloads running in multiple clouds sits with the cloud service providers** themselves



- Our current backup solution allows us to protect workloads running in multiple clouds
- We use multiple backup tools to protect workloads running in multiple clouds
- We plan to upgrade our data protection solution to enable the backup of workloads across multiple clouds
- Each cloud service provider is responsible for protecting our workloads
- We are not running workloads in multiple cloud environments

However, most of those that say their cloud service provider protects their cloud-based workloads do not actually have separate contracts for protection of all workloads

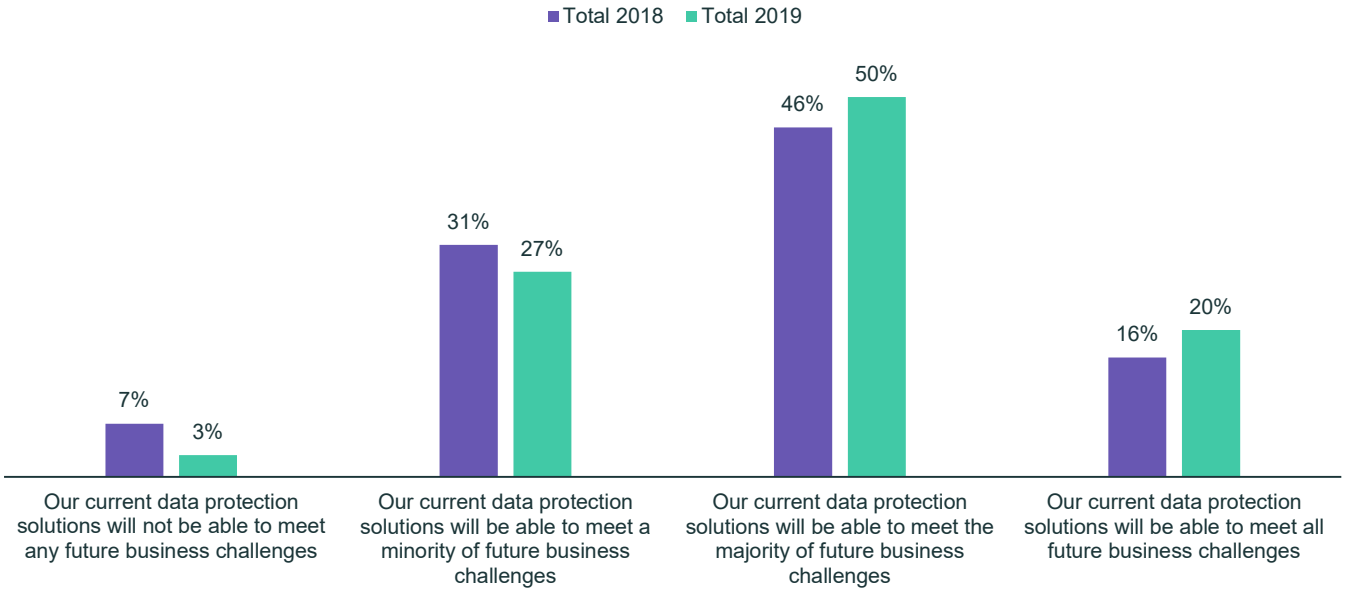


63%

Say that their organization **does not have a separate contract** with its cloud service provider(s) for **protection of all workloads**

5. Data protection for newer technologies

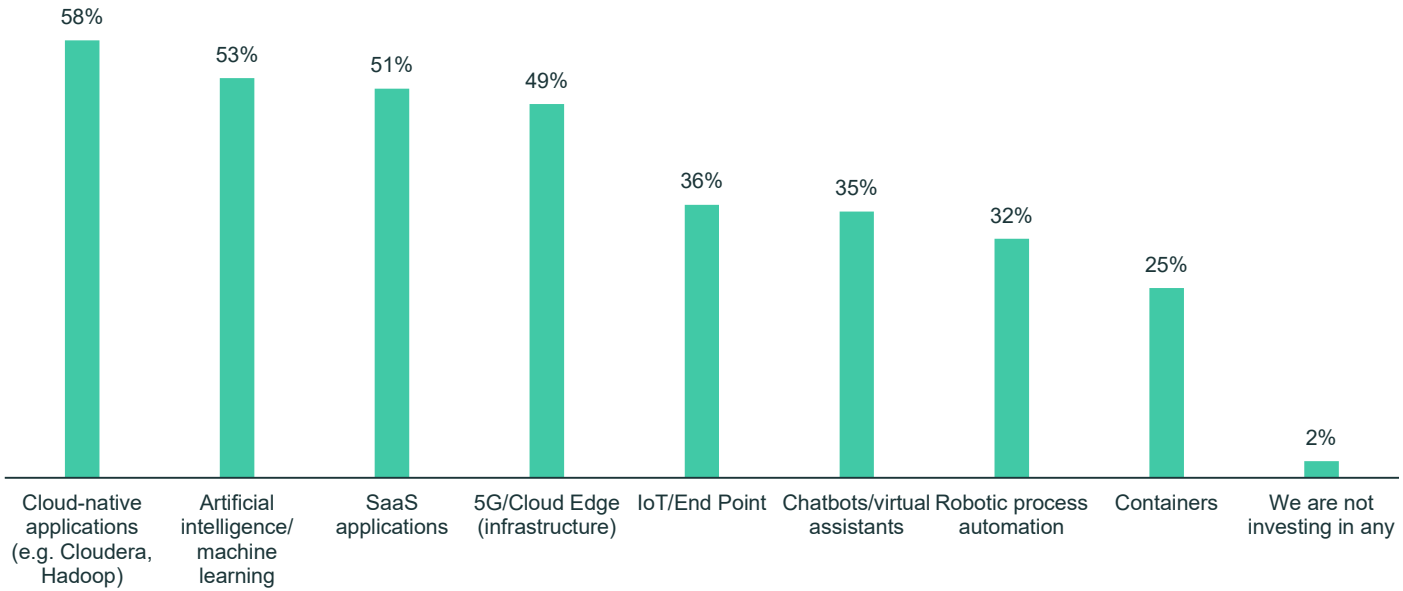
For the vast majority of organizations, their current data protection solution(s) will not be sufficient for meeting all future business challenges



80%

Say that their organization's existing data protection solution(s) **will not be able to meet all future business challenges**

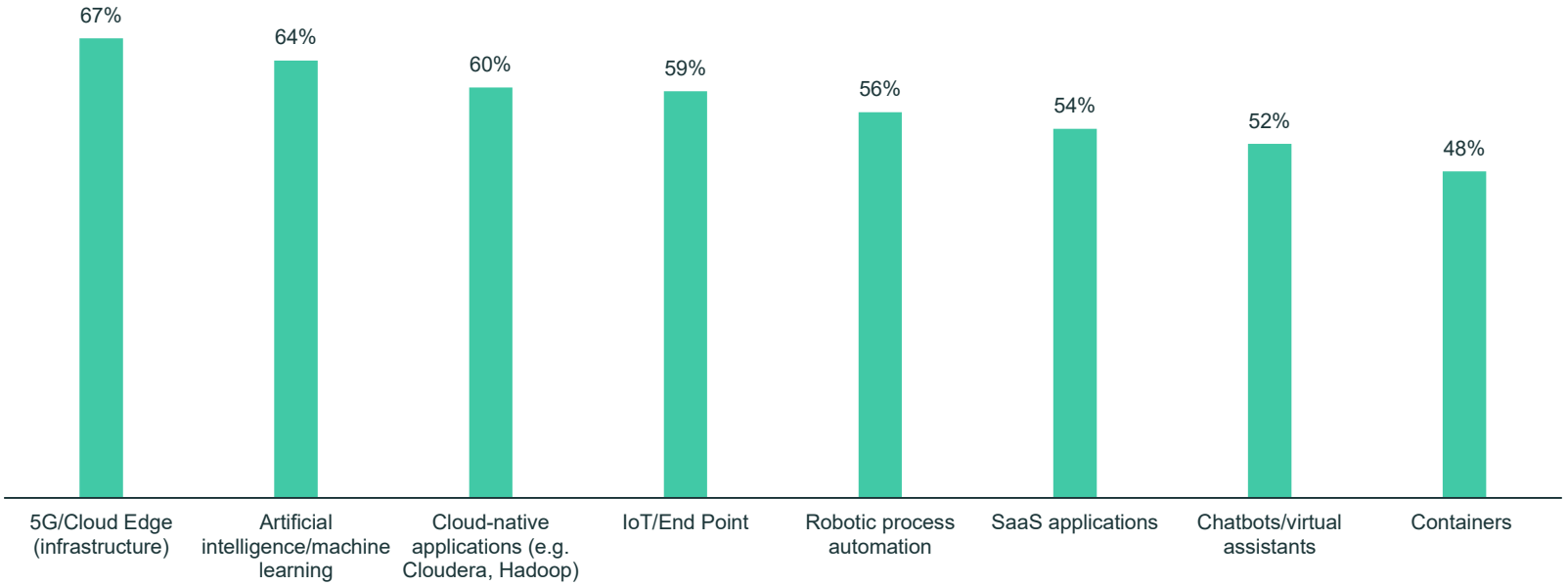
Almost all organizations are making at least some investment into newer or emerging technologies



98%

Are investing in at least one **newer/emerging technology**

Around half or more of those using each of the technologies listed are struggling to find suitable data protection for them



Despite their obvious value, emerging technologies are widely recognized as introducing additional challenges and concerns

52%

Consider **lack of data protection for newer technologies** to be one of the top five data protection challenges facing their organization

71%

Agree that **emerging technologies create more complexity** when it comes to data protection

61%

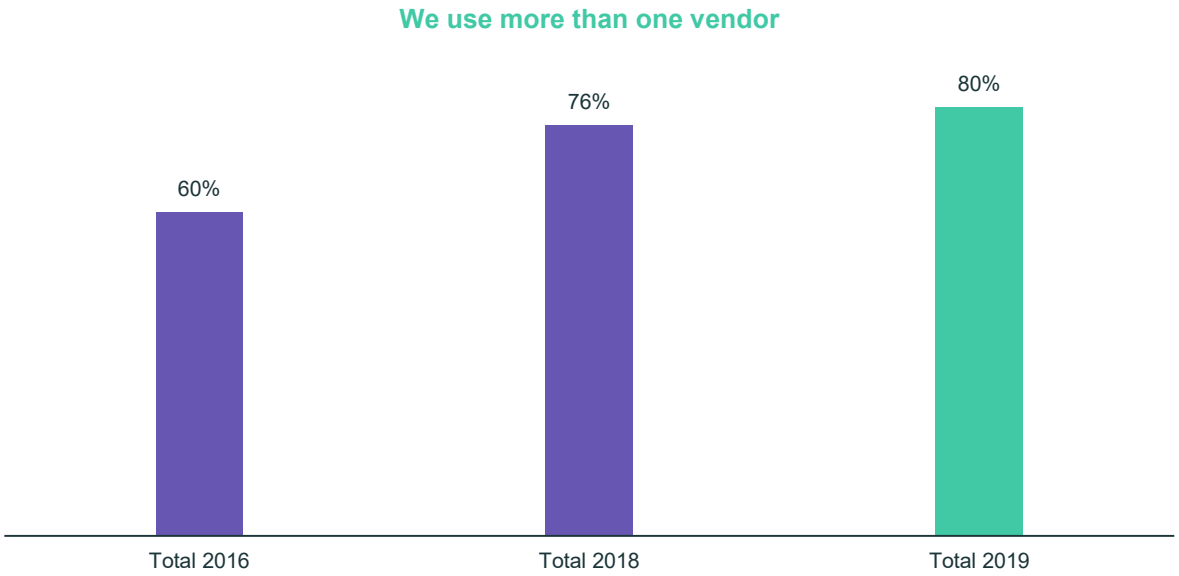
Agree that **emerging technologies pose a risk** to data protection

62%

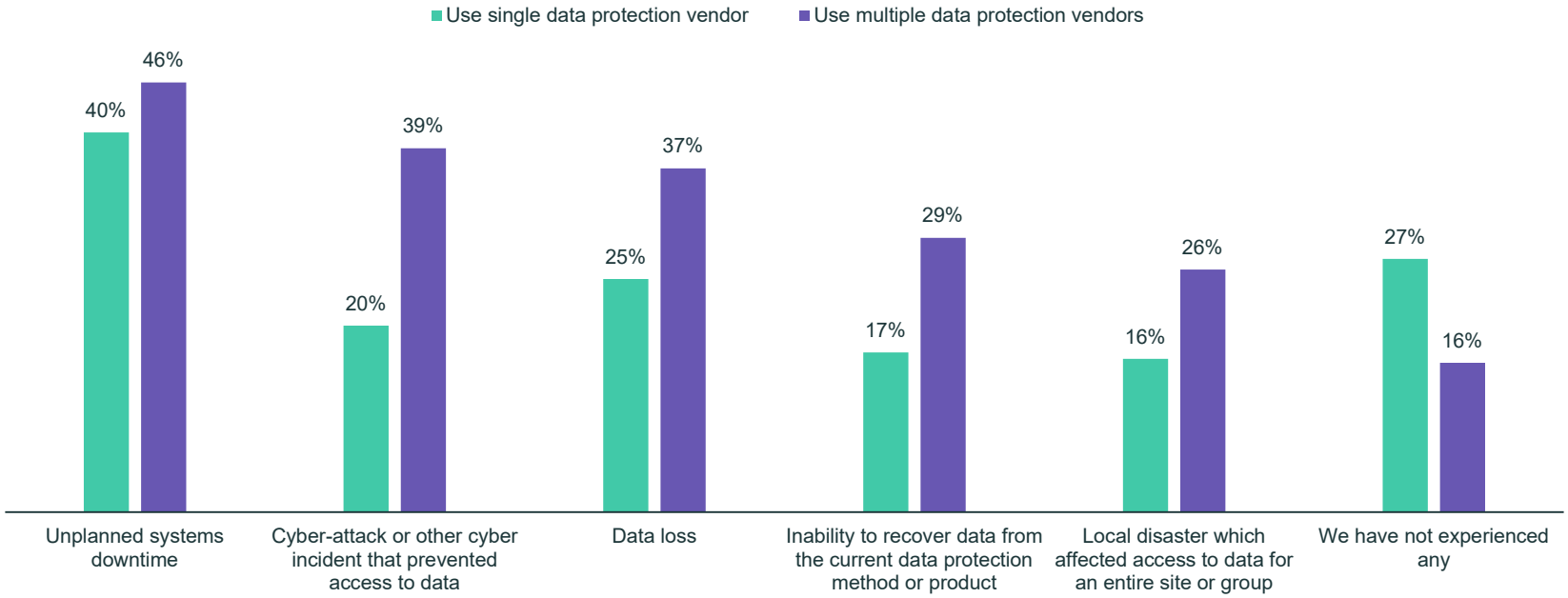
Agree that their organization's **existing data protection measures may not be sufficient to cope** with new and emerging technologies

6. Increased risk of using multiple data protection vendors

Organizations are increasingly using multiple data protection vendors for their data protection needs – in 2019, 80% of organizations are doing this



Those using multiple data protection vendors are more likely to report suffering from disruption over the last 12 months



For organizations that have experienced data loss in the last 12 months, the costs are typically nearly 5x higher for those using multiple vendors, on average

Estimated total cost of data loss in the last 12 months (in USD)

$1,090,436

Use multiple data protection vendors

$227,781

Use single data protection vendor

5x

Higher average **cost from data loss** experienced by those using multiple vendors

For those that have experienced unplanned downtime in the last 12 months, the costs are typically nearly 2x higher for those using multiple vendors, on average

Estimated total cost of downtime in the last 12 months (in USD)

$881,207

Use multiple data protection vendors

$473,512

Use single data protection vendor

2x

Higher **average cost from unplanned downtime** experienced by those using multiple vendors

Key Findings - In Summary (1/2)

The rise of disruption

- Disruptive events are on the rise, with even more organizations falling victim to one in 2019 compared to 2018
- Looking beyond the financial damage, disruption also results in a wide range of other consequences for organizations
- There is also a considerable lack of confidence in a number of crucial areas relating to the data protection that organizations currently have in place
- Meanwhile, there is widespread concern that more disruption will be experienced over the next 12 months
- Further adding to the challenge of disruption is the growing amount of data that organizations are managing – between 2018 and 2019, data volumes have increased by 39%
- Unexpected downtime to critical applications can take significant time to recover from too – 8 hours on average in 2019
- The cost of downtime is also on the up in organizations. Between 2018 and 2019 this increased by 54%

Hybrid cloud – the new normal

- Most organizations are deploying mission-critical workloads into both public and private clouds

VMware data protection

- For many, the hybrid cloud approach for application deployments will be based on VMware infrastructure. However, there is no clear standout in terms of how organizations are protecting VMware workloads in the cloud

Key Findings - In Summary (2/2)

Cloud data protection vulnerability

- When deploying new applications, most organizations favour a cloud-based deployment model
- The decision to use public cloud when deploying new business applications is driven by a range of important business benefits
- For those running workloads in multiple cloud environments, there is not a clear “go to” in terms of protection
- However, most of those that say their cloud service provider protects their cloud-based workloads do not actually have separate contracts for protection of all workloads

Data protection for newer technologies

- For the vast majority of organizations, their current data protection solution(s) will not be sufficient for meeting all future business challenges
- Almost all organizations are making at least some investment into newer or emerging technologies
- Around half or more of those using each of the technologies listed are struggling to find suitable data protection for them
- Despite their obvious value, emerging technologies are widely recognized as introducing additional challenges and concerns

Increased risk of using multiple data protection vendors

- Organizations are increasingly using multiple data protection vendors for their data protection needs – in 2019, 80% of organizations are doing this
- Those using multiple data protection vendors are more likely to report suffering from disruption over the last 12 months
- For organizations that have experienced data loss in the last 12 months, the costs are typically nearly 5x higher for those using multiple vendors, on average
- For those that have experienced unplanned downtime in the last 12 months, the costs are typically nearly 2x higher for those using multiple vendors, on average