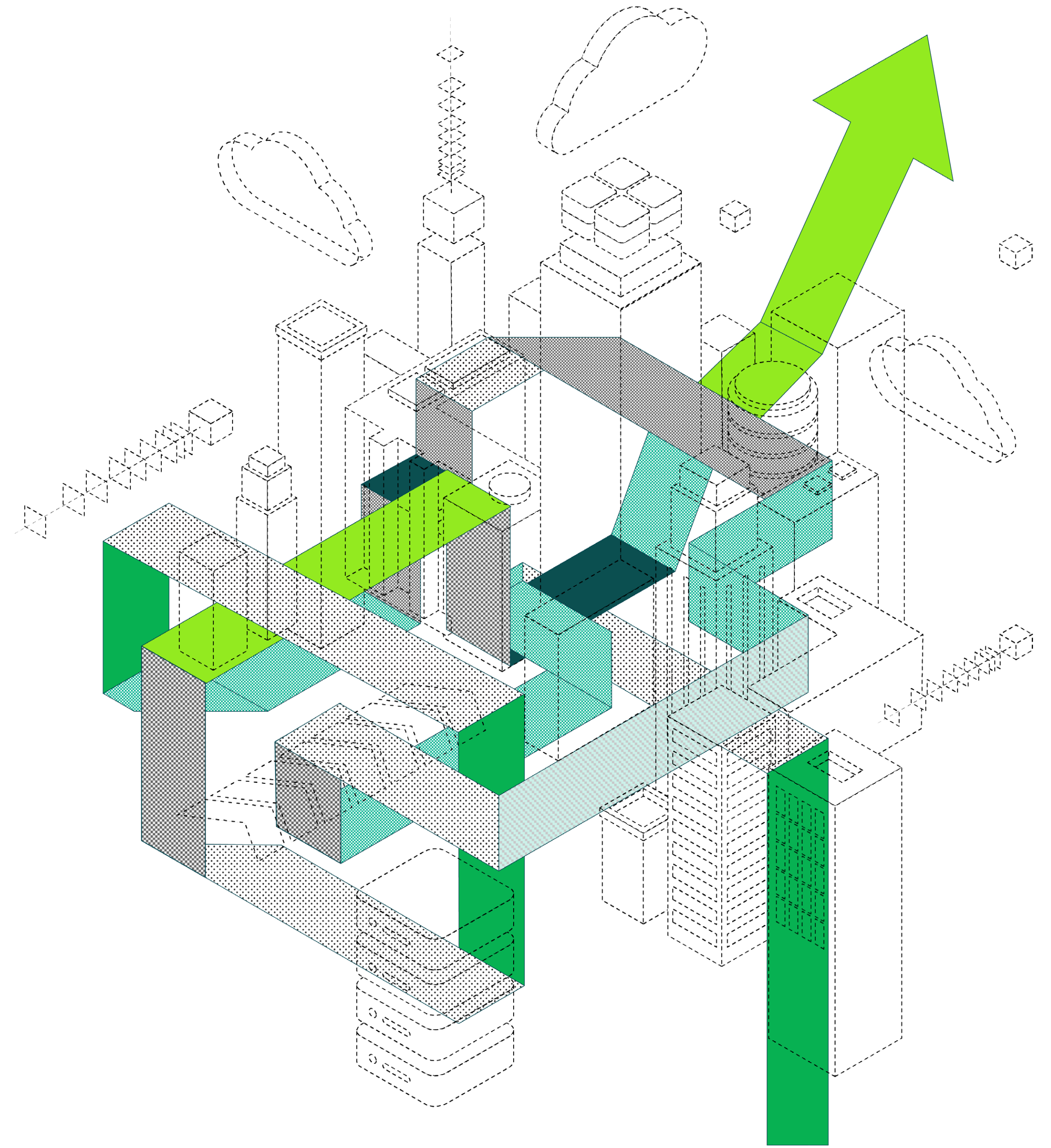


# 2021 Data Protection Report



veeam

# How the last year has affected IT, Digital Transformation, and data protection strategy ... in ways NEVER seen before

In **December 2020**, an independent research firm completed a survey of **3,000** enterprises across **28** countries on what their data protection challenges and goals were, regardless of what their current or future data protection vendor choices were.

The research project was commissioned by Veeam and helmed by two former industry analysts with a combined **60-years** of experience in the data protection industry. The results and insights from the survey, as well as Veeam's perspective, are both offered in this report.



**Dave Russell**

VP of Enterprise Strategy at Veeam  
Former VP, Distinguished Analyst,  
and lead author of the Magic  
Quadrant for Backup at Gartner  
**@BackupDave**



**Jason Buffington**

VP of Solutions Strategy at Veeam  
Former Principal Analyst for  
Data Protection at the Enterprise  
Strategy Group (ESG)  
**@JBuff**



# Contents

## 1.0

### INTRODUCTION

- 1.1 Key findings

## 2.0

### 2020 – A YEAR OF IT CHANGE

- 2.1 Expected IT challenges
- 2.2 Digital Transformation challenges
- 2.3 COVID-19 impact on Digital Transformation challenges
- 2.4 IT delivery strategy post COVID-19
- 2.5 Summary

## 3.0

### A NEW NEED FOR MODERN DATA PROTECTION

- 3.1 Data protection challenges
- 3.2 Data protection expectations vs. reality
- 3.3 The reality of data availability
- 3.4 Impacts of downtime
- 3.5 Today's modern data protection needs
- 3.6 Summary

## 4.0

### THE EFFECT OF CLOUD ON MODERN BACKUP

- 4.1 Cloud backup skyrockets
- 4.2 The future of DR is cloudy
- 4.3 Protecting SaaS (Software-as-a-Service)
- 4.4 Summary

## 5.0

### WHY CHANGE BACKUP SOLUTIONS IN 2021?

- 5.1 The drive for change
- 5.2 Outcomes when adopting modern data protection
- 5.3 Digital resiliency
- 5.4 Data accessibility and management
- 5.5 More than just backup – driving innovation

## 6.0

### CONCLUSION



## 1.0 Introduction

## 1.1 Key findings

## 1.0

# Introduction

Data protection, now more than ever, is providing peace of mind and ensuring business continuity. The world of data protection is wide and varying, across new technology and old, striving to support an ever-changing world of technology. This Data Protection Report looks into a recent global survey of **3,000** unbiased organizations to understand their approach toward data protection and management today. This includes how they expect to be prepared for the myriad IT challenges they face, including reacting to demand changes and interruptions in service, global influences (such as COVID-19), and more aspirational goals of IT modernization and Digital Transformation.

While organizations already have a diverse mix of physical servers (**29%**), virtual machines (**23%**), and cloud-hosted servers (**47%**), the amount of cloud-hosted workloads within hybrid-IT environments is expected to grow even faster over the next two years. This fast-paced shift shows that recent events such as the global pandemic have accelerated an already-strong movement towards a more cloud-friendly and multi-cloud ecosystem.

Company concerns seem to be consistent, with many thoughts going toward data and cloud availability, customer experience, and brand impact. However, this report shows that by modernizing data protection with easy-to-use and flexible solutions, businesses can significantly increase data protection and usability while also freeing many resources to focus further on their IT modernization and management efforts.

So, as you read this report, please keep your own IT challenges and goals in mind as you consider how you and your organization align with the **3,000** enterprises surveyed on modern data protection.

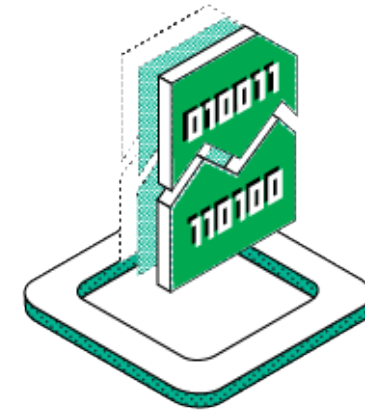


1.0 Introduction

1.1 Key findings

## 1.1

# Key findings



**11%**

**GROWTH IN ECONOMIC UNCERTAINTY**

Economic impact is driving organizations to think about their IT direction differently



**96%**

**OF ORGANIZATIONS WILL ACCELERATE CLOUD USAGE**

COVID significantly accelerated cloud adoption to ease on-prem management



**80%**

**OF ORGANIZATIONS NOW HAVE AN AVAILABILITY GAP**

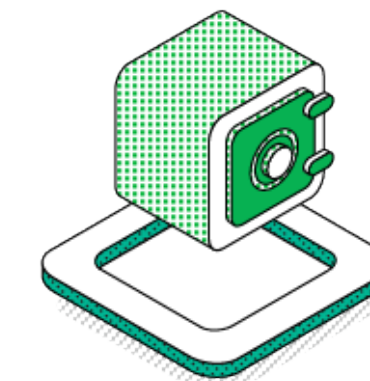
Faster modernization is increasing pressure on aging legacy systems



**58%**

**OF DATA CANNOT BE RECOVERED**

Failed backups and unverified restores means lost data and productivity



**#1**

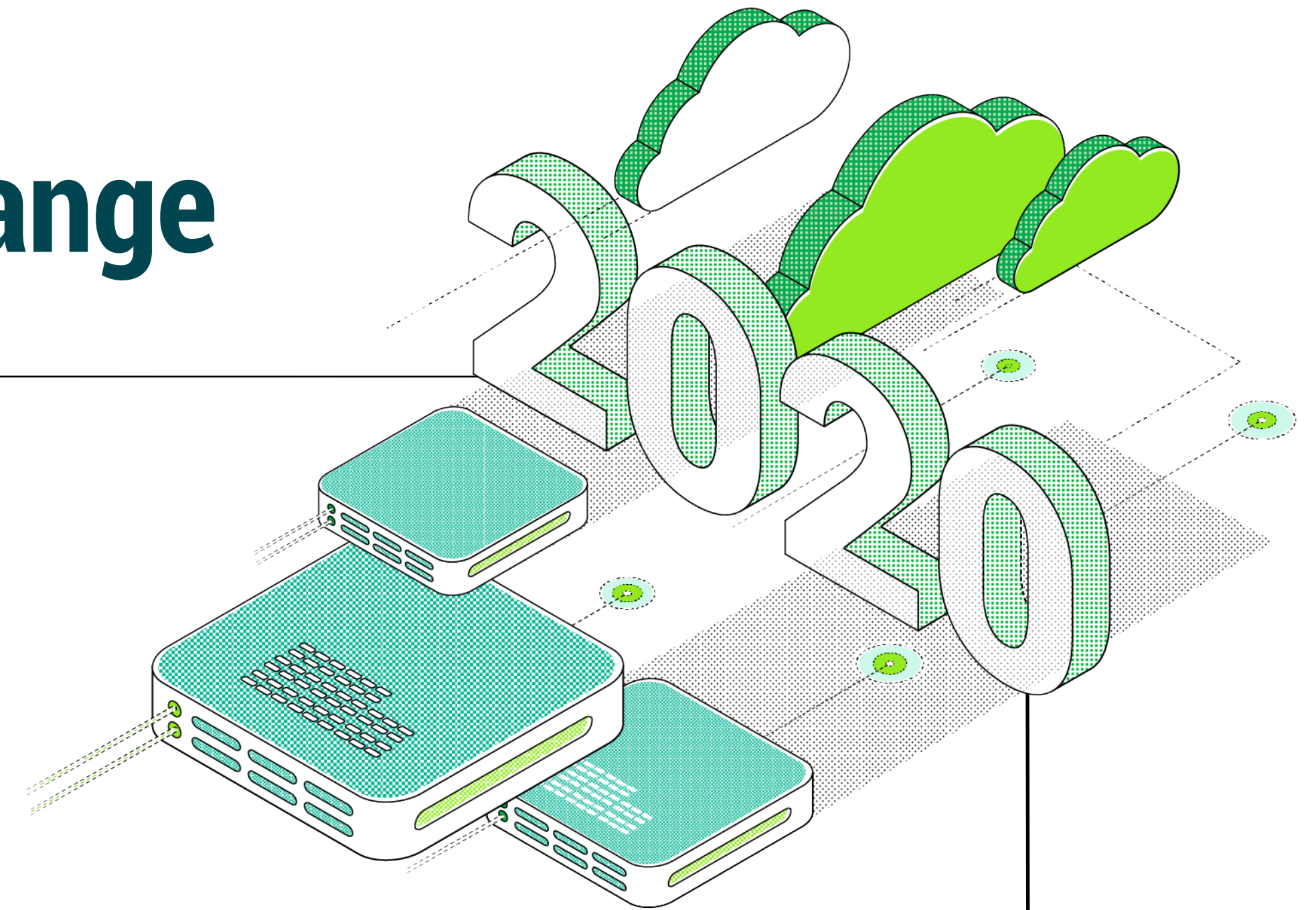
**DRIVER FOR CHANGE IS BACKUP RELIABILITY**

Organizations are looking for better reliability through modern protection

## 2.0 2020 – A year of IT change



2020 was unique for the world and created a new set of pressure for IT departments. Overnight, centralized IT organizations were catapulted into high-distributed networks, now supporting a highly-remote workforce. Budgets were tightened even more, strategic plans were slowed, and unfortunately, rampant ransomware was on the rise. This resulted in a new set of challenges and, in many cases, outcomes for IT plans through 2020 and beyond.





2.1 Expected IT challenges

2.2 Digital Transformation challenges

2.3 COVID-19 impact on Digital Transformation challenges

2.4 IT delivery strategy post COVID-19

2.5 Summary

2.1

# Expected IT challenges

2020 was a roller coaster, and as such, changed the landscape of IT. Where in 2020, cyberthreats were the #1 challenge, now economic uncertainty (40%), meeting changing customer needs (32%), and skills shortage (32%) are trending higher.

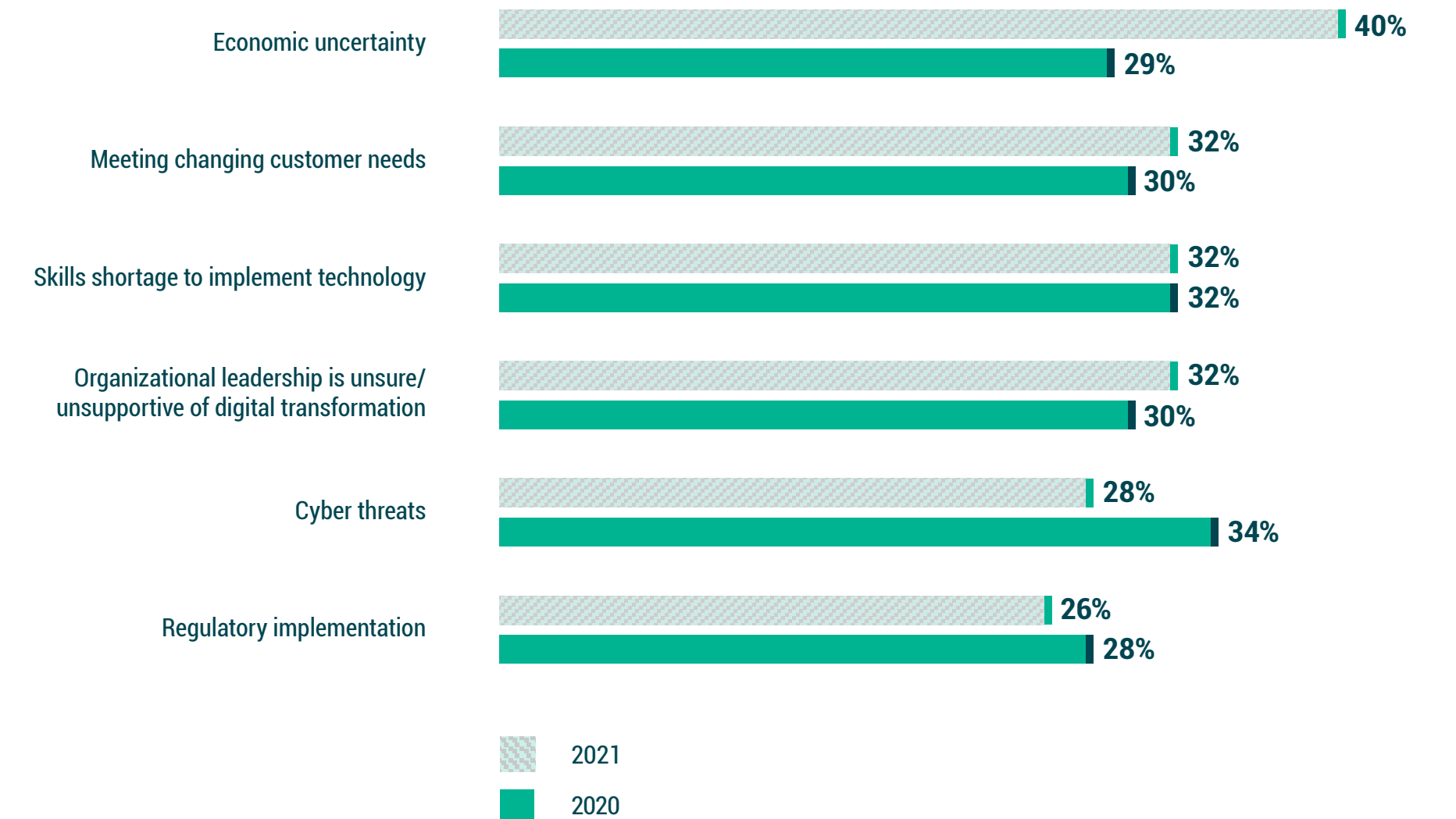
This does not mean the threat of malware is less (in fact it has increased through 2020). The data shows us that organizations are responding to the increased pressure of economic uncertainty, mainly as a direct effect of COVID. Customer needs and behaviors are also changing through this time, and as many organizations are now accelerating modern IT investment, this is putting pressure on skills availability.



Response to economic uncertainty is driving many new IT strategies



Which of the following do you believe will be a challenge in the next 12 months?





2.1 Expected IT challenges

2.2 Digital Transformation challenges

2.3 COVID-19 impact on Digital Transformation challenges

2.4 IT delivery strategy post COVID-19

2.5 Summary



Challenges due to legacy systems has risen year over year

## 2.2

# Digital Transformation challenges

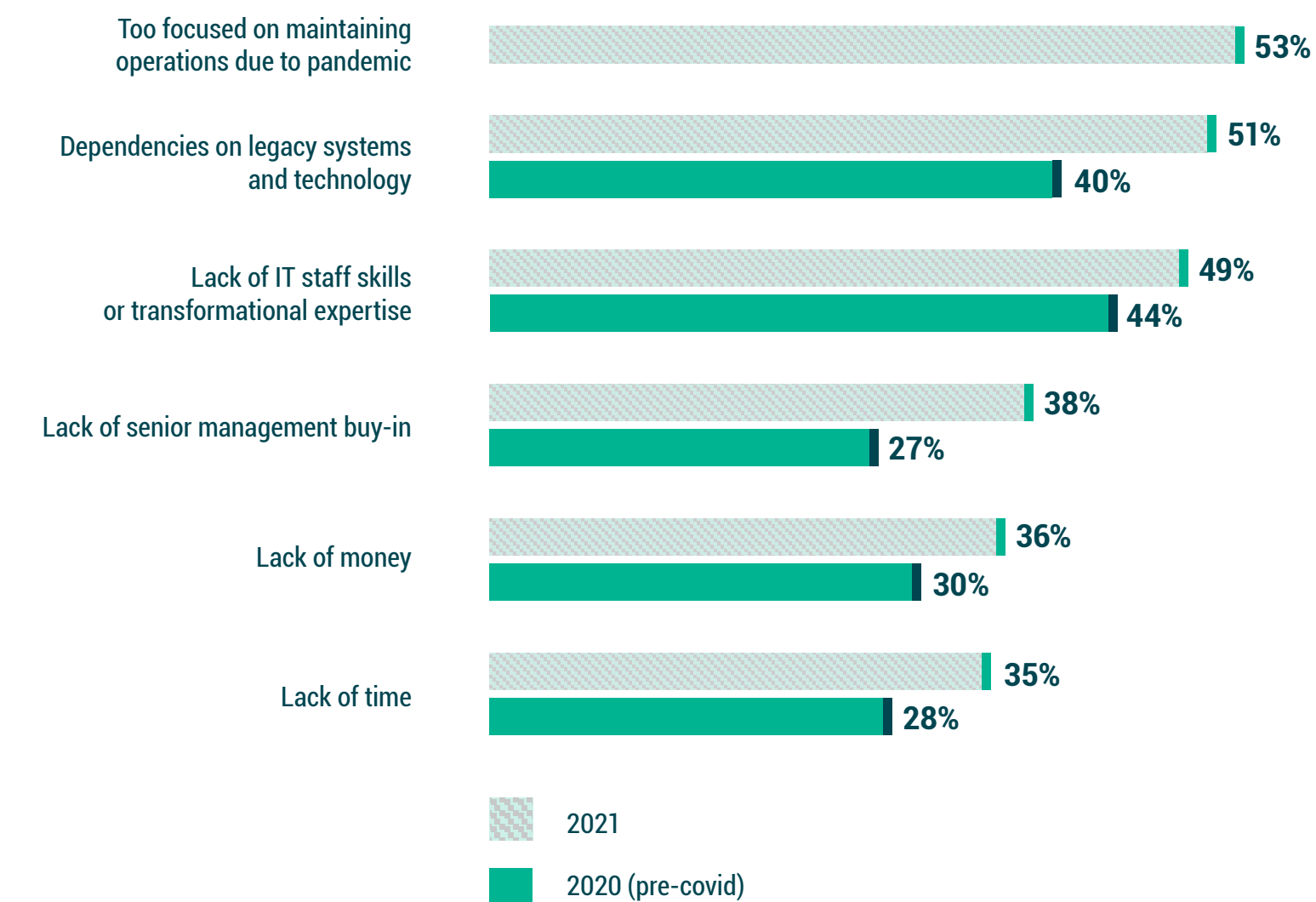
Digital Transformation provides many advantages. By modernizing business operations and processes, organizations can significantly impact customer service, cost reduction and employee tasks. More than **98%** of organizations are in the process or planning for Digital Transformation (up from **80%** in 2019), however, they are encountering some challenges.

The #1 challenge new to this report is being too focused on maintaining operations due to the pandemic (**53%**). This alone would have a significant impact on Digital Transformation goals. However, existing challenges remain. Dependency on legacy systems is rising quickly to the top (**51%**), compared to **40%** from 2019. That has significant impact on organizations' ability to modernize as quick as they desire due to a shortage in skill availability (**49%**) and lack of budget (**36%**).

As many organizations continue to maintain status quo, this is putting more dependencies on legacy systems and the skills to support them.



What, if anything, is preventing/did prevent your organization's ability to move forward with its digital transformation initiatives?







2.1 Expected IT challenges

2.2 Digital Transformation challenges

2.3 COVID-19 impact on Digital Transformation challenges

2.4 IT delivery strategy post COVID-19

2.5 Summary



50% of organizations in 2020 increased their DX efforts

## 2.3

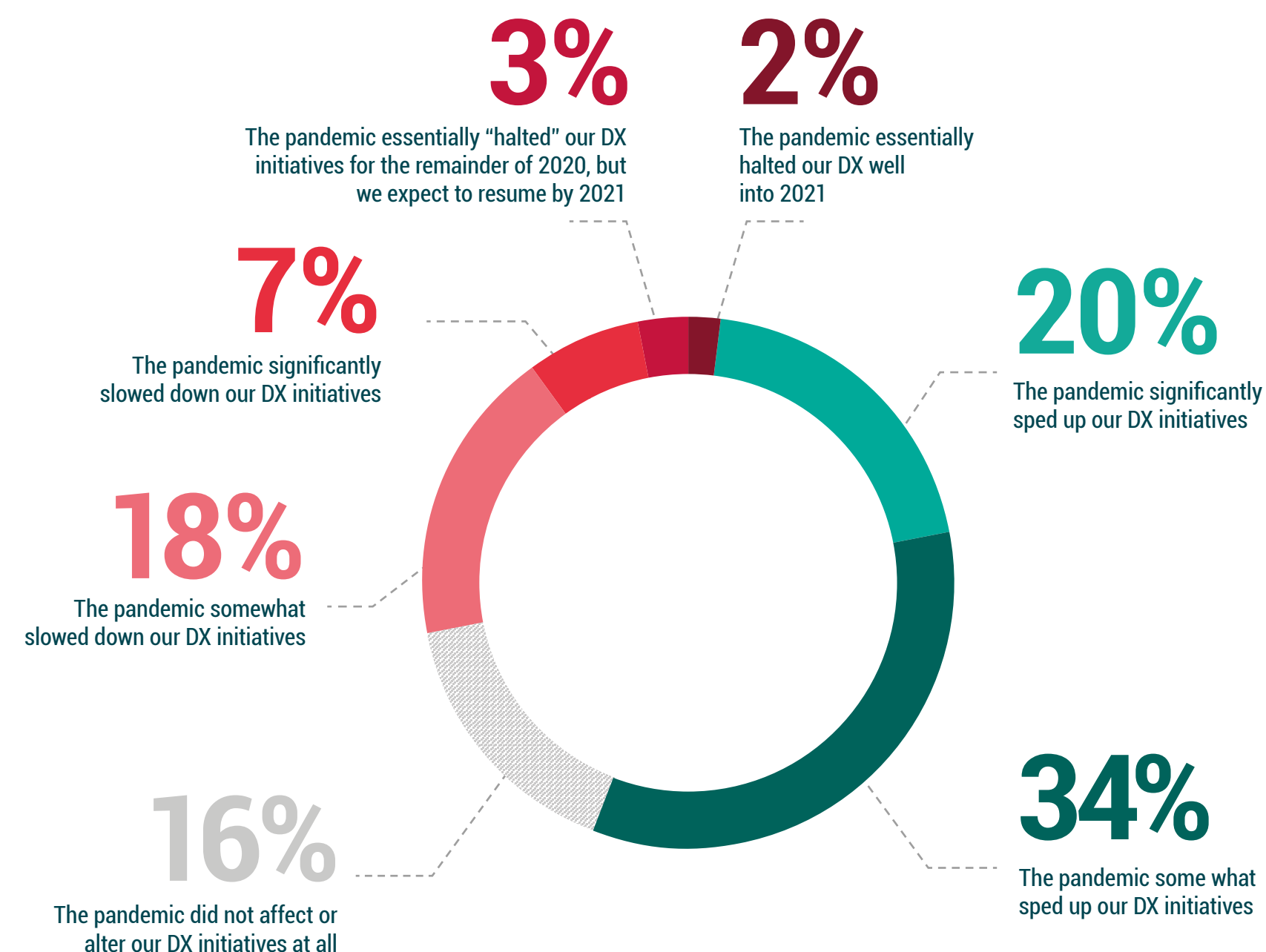
# COVID-19 impact on Digital Transformation challenges

COVID-19 also had an extraordinary effect on Digital Transformation (DX) efforts. In many cases, you would expect DX plans to slow down due to the reallocation of efforts, and in **30%** of organizations, that is precisely what happened. But there was also a massive increase in DX speed. Over **50%** of organizations accelerated their DX initiatives.

This shows two distinct Digital Transformation outcomes directly related to COVID-19. Organizations with mature DX plans accelerated their investments, focusing on rapid changes to business practices and the usage of cloud to assist. However, for those companies that had less mature efforts, they tended to pause to focus on sustainability.



To what extent did the global COVID-19 pandemic affect/alter your Digital Transformation (DX) initiatives?





- 2.1 Expected IT challenges
- 2.2 Digital Transformation challenges
- 2.3 COVID-19 impact on Digital Transformation challenges
- 2.4 IT delivery strategy post COVID-19**
- 2.5 Summary



96% of organizations are now driving faster cloud efforts due to COVID-19

## 2.4

# IT delivery strategy post COVID-19

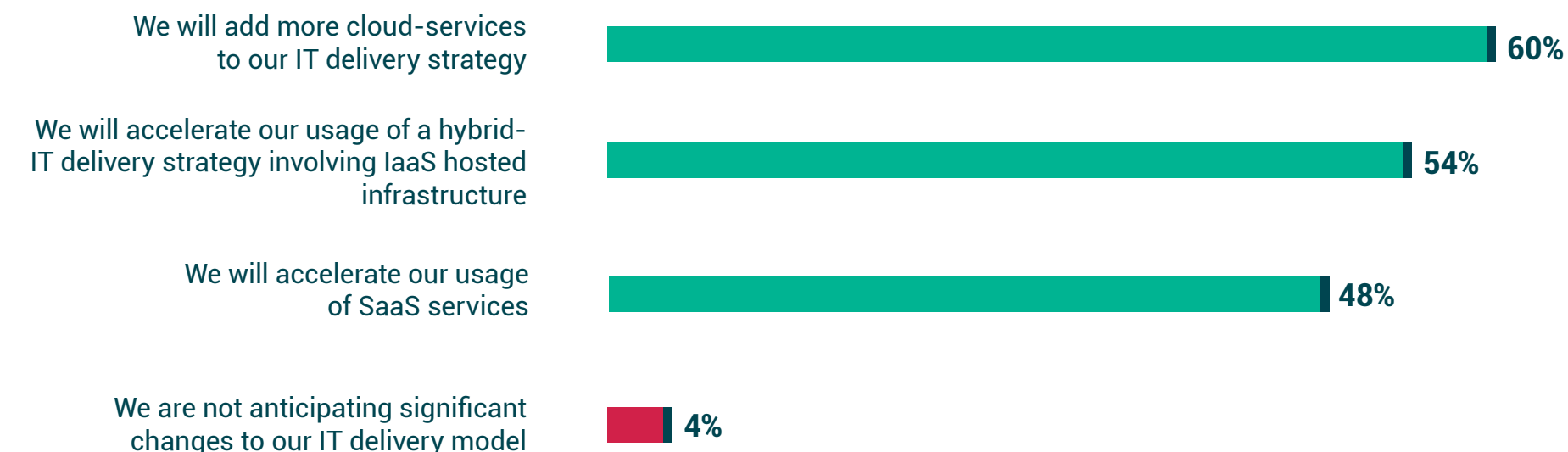
What will 2021 bring to IT strategy? The results show a massive investment change in IT delivery. In fact, only **4%** of organizations surveyed were not anticipating any significant changes in 2021.

In the first months of the pandemic, **91%** of organizations increased their usage of cloud services (**31%** significantly). This came as a result of remote workers using SaaS-based collaboration services, and the increased challenge for IT to maintain on-prem physical operations. This trend will continue through 2021, with the majority of organizations planning to add more cloud services and cloud usage to IT delivery strategy.

This shift must be highly considered when examining resources such as data protection and management. With the large shift to cloud-based IT strategy data, support systems like backup and DR must be modernized in parallel.



Looking ahead past the global COVID-19 pandemic and into 2021, how would you characterize your organization's expected IT delivery strategy?





- 2.1 Expected IT challenges
- 2.2 Digital Transformation challenges
- 2.3 COVID-19 impact on Digital Transformation challenges
- 2.4 IT delivery strategy post COVID-19
- 2.5 **Summary**

## 2.5

# Summary

The continued goals of Digital Transformation continue to ring true even today. Organizations still see massive value in modernizing their services, driving faster and more efficient practices. Most enterprises have already started their journey into Digital Transformation and show positive results. In fact, these same enterprises plan to continue their journey to extend those results.

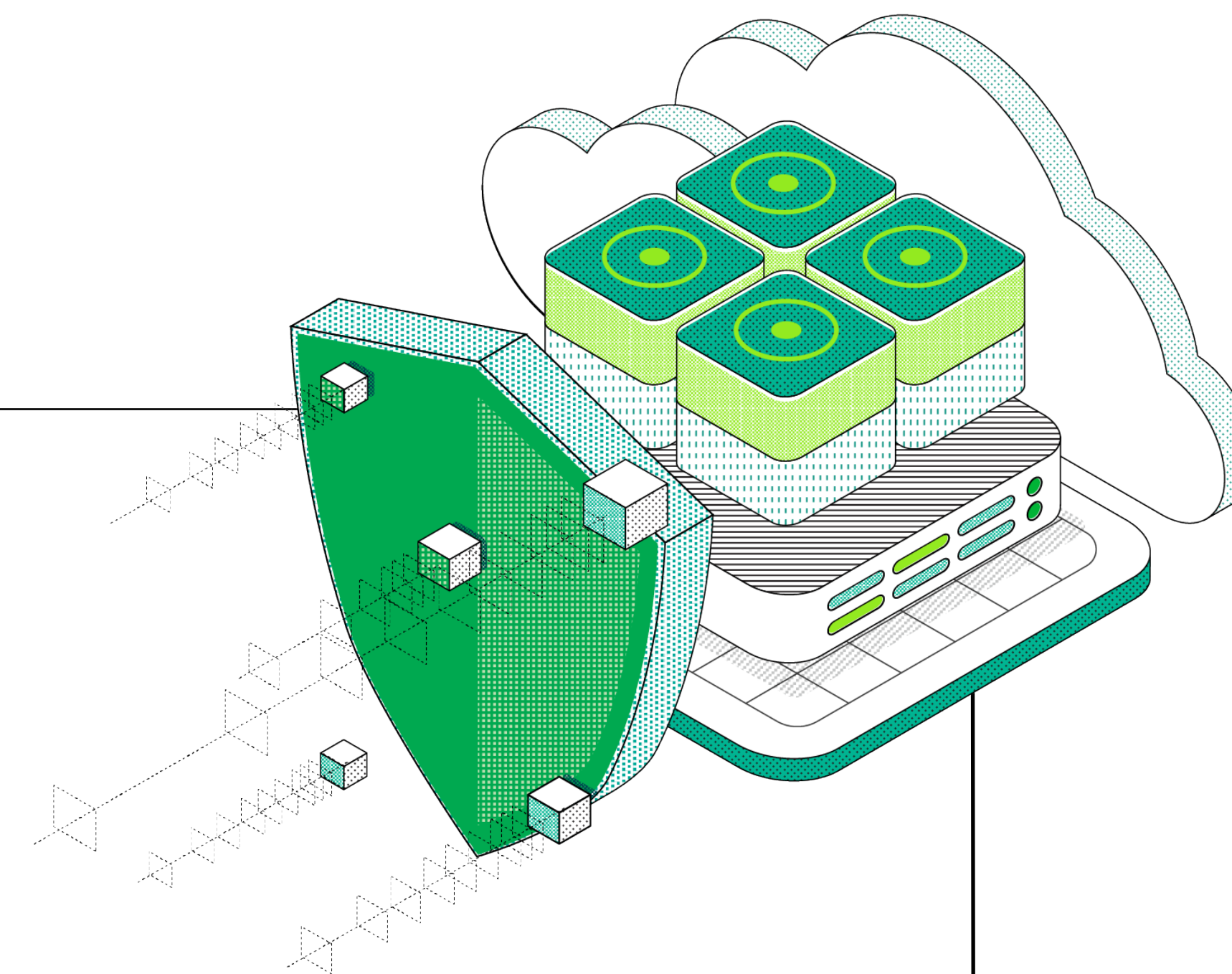
2020 did not change this direction, and in many cases, accelerated the goals. Many organizations saw the value of more modern platforms and services and the immediate returns to the business they can provide. However, with the modernization of core services, many companies are still leaving their data protection behind, which can have a vastly negative impact.



## 3.0 A new need for modern data protection



With the rapid adoption of modern platforms such as hybrid cloud and SaaS growing (currently growing 15% YoY), many organizations continue to struggle with their data protection strategy. Legacy backup can't succeed with modern applications, stretch across the cloud successfully, or defend against cyberthreats. The goals and focus of those aging platforms are now becoming a costly risk to many organizations. Organizations need a modern data protection platform to match their evolving data protection needs. Being unified across clouds, hybrid, and on-premises can back up and restore legacy VMs while also protecting cloud-native, container-based applications. With a solution that can protect and recover from ransomware, that data accessibility can become a strategic asset to the organization.





3.1 Data protection challenges

- 3.2 Data protection expectations vs. reality
- 3.3 The reality of data availability
- 3.4 Impacts of downtime
- 3.5 Today's modern data protection needs
- 3.6 Summary

3.1

# Data protection challenges

The increased focus on modern and cloud-based services have a major impact on data protection trends for IT delivery practices. Inadequate backup or failure to meet SLAs topped the data protection challenges for 2021 at **40%** (up from **31%** in 2019), beating out all other metrics. As systems are aggressively turning to cloud and modern services, backup failure rates due to legacy systems are increasing, raising the pressure on IT to resolve.

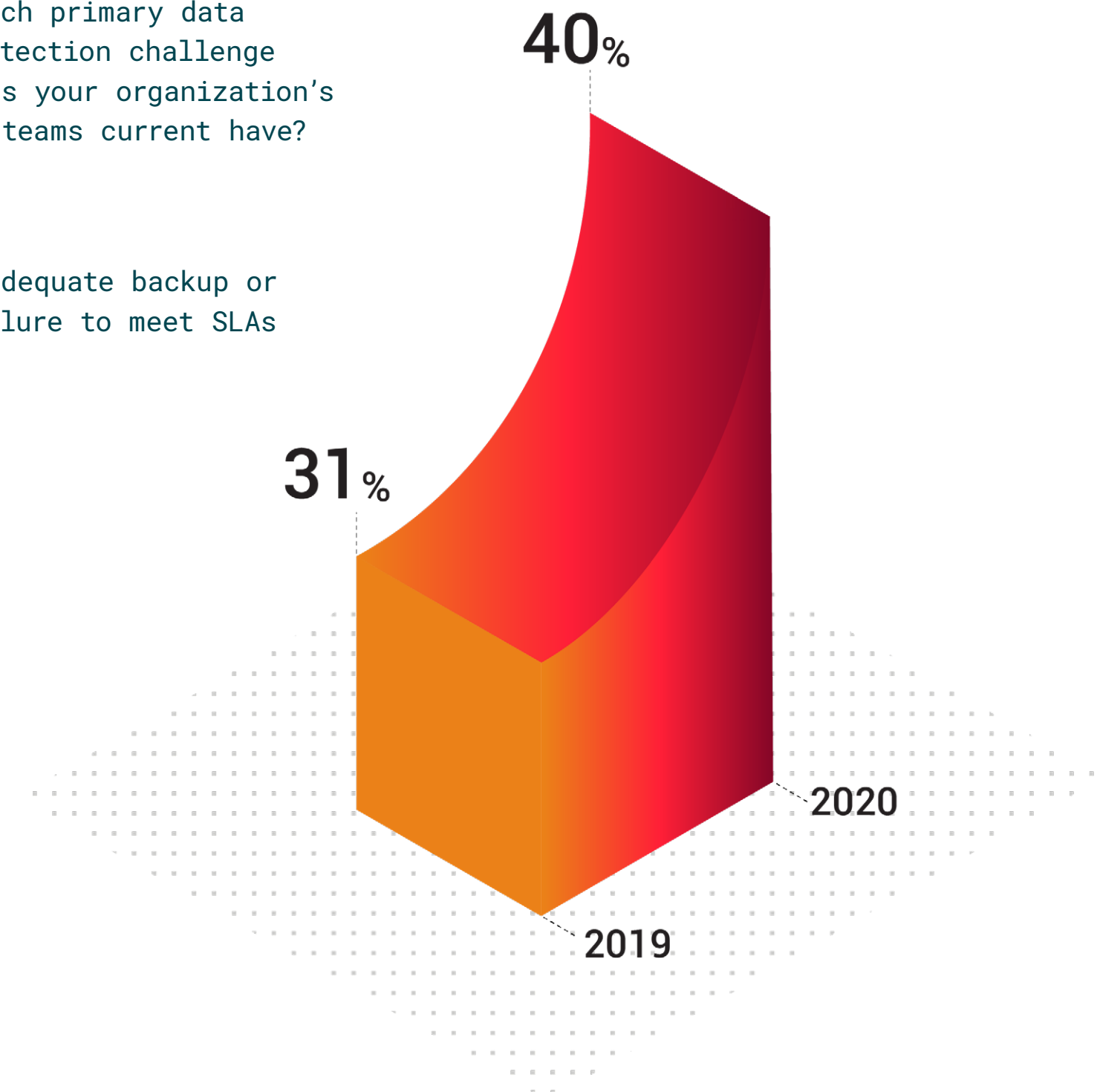


40% of respondents want their backup's to improve



Which primary data protection challenge does your organization's IT teams current have?

Inadequate backup or failure to meet SLAs





3.1 Data protection challenges

3.2 Data protection expectations vs. reality

3.3 The reality of data availability

3.4 Impacts of downtime

3.5 Today's modern data protection needs

3.6 Summary

## 3.2

# Data protection expectations vs. reality

Face it. There is always a gap between our expectations and reality in literally everything we do. And data availability and recovery are not exceptions. IT management will expect data to be safe and should not be lost under any circumstance and can be recovered without impact. However, in reality, the results can be quite different.

- Eighty percent of all organizations recognize that they have an **“Availability Gap”** between how fast they can recover applications versus how fast they need applications to be recovered.
- **Protection Gap:** Seventy-six percent of those same organizations said they have a gap between how frequently data is backed up versus how much data they can afford to lose.

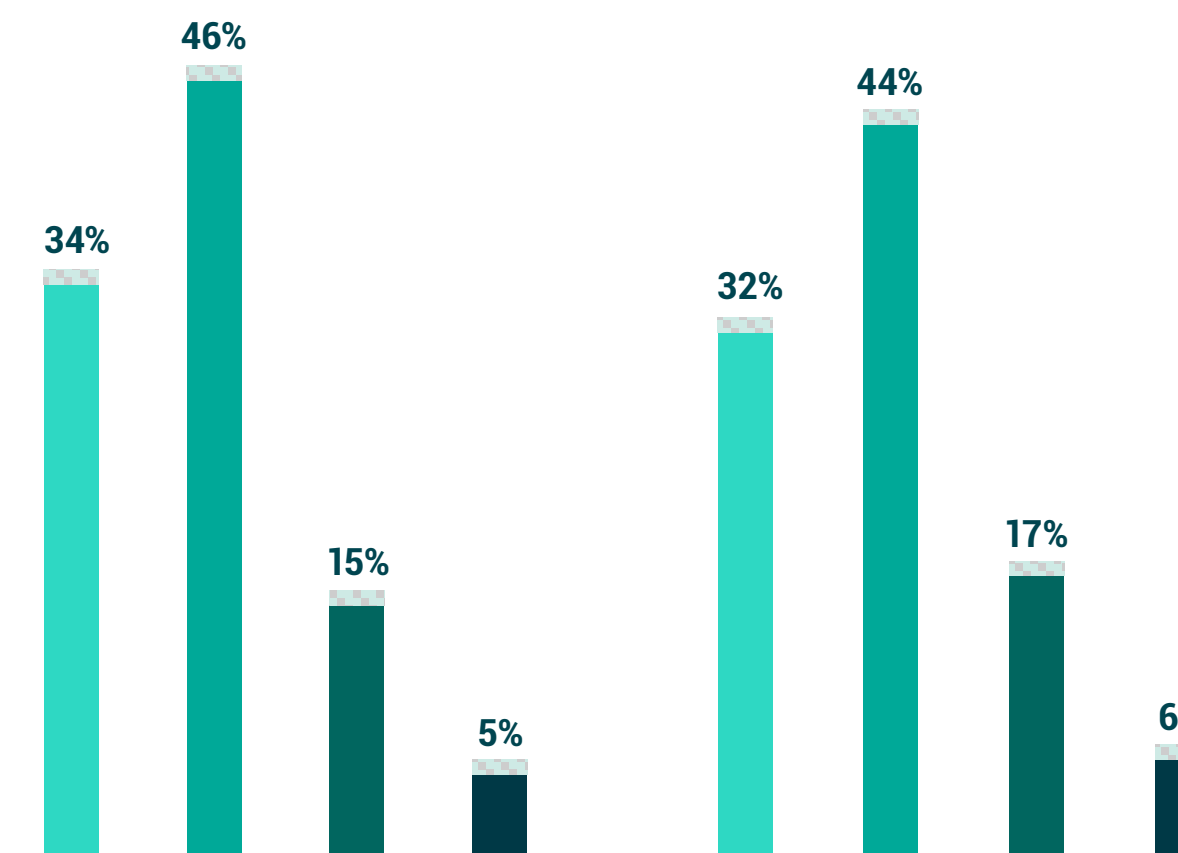
Many organizations clearly need to address the business need and the ability to meet that expectation with reliable data protection.



80% of organizations have a reality gap in their data protection



Do you have a «Reality Gap» between the Business and IT?



My organization has a gap between how fast we can recover applications versus how fast we need applications to be recovered and our users productive

My organization has a gap between how frequently our data is backed-up versus how much data that we can afford to lose after an outage

- Strongly Agree
- Agree
- Disagree
- Strongly Disagree



3.1 Data protection challenges

3.2 Data protection expectations vs. reality

3.3 The reality of data availability

3.4 Impacts of downtime

3.5 Today's modern data protection needs

3.6 Summary

### 3.3

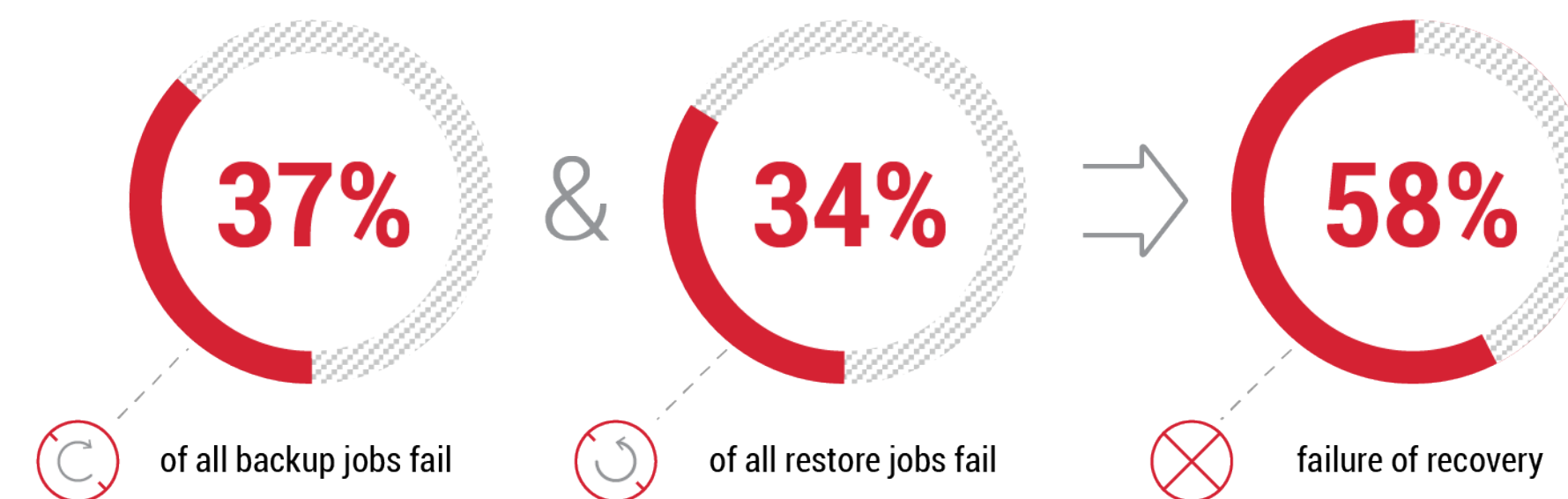
# The reality of data availability

Availability due to dependency on legacy systems and operations is still a critical factor in many organizations, but so is the lack of core functionality to provide backup and recovery capabilities.

On average, **23%** of servers had at least one expected outage in the last **12** months (with **36%** of organizations stating up to **50%** of their servers had at least one outage). As such, the integrity of backup becomes critical. You need to be able to ensure confidence that the backup is successful and can be used for recovery.

The research showed that a whopping **37%** of backups ended up with errors or could not complete in their allocated backup window. The research also showed that one-third (**34%**) of all restorations are also failing to restore within the expected SLA. Those are some scary figures, which mean more than half the time, organizations won't be able to restore their servers due to either failed backups or failed restores.\*

While there may be many factors relating to this including environment complexity, lack of capability with legacy solutions and IT skills, the adoption of modern data protection and process will have an instant positive effect.



\* 63% successful backups TIMES 66% successful restores EQUALS a 42% success rate



- 3.1 Data protection challenges
- 3.2 Data protection expectations vs. reality
- 3.3 The reality of data availability
- 3.4 Impacts of downtime**
- 3.5 Today's modern data protection needs
- 3.6 Summary

## 3.4

# Impacts of downtime

Downtime doesn't inconvenience just a few internal people. It can have vast and damaging effects on the organization. In 2020, the average downtime for an outage was **79** minutes, and with the cost of downtime now averaging **\$84,650** US per hour, there can be a significant financial impact.

However, the impact cannot be measured solely in costs per hour. There are many other potential downsides to outages. According to our respondents, there are three core impacts of downtime. External impact, including loss of customer confidence and damage to the brand, internal impacts such as employee morale and diversion of resources, and the third, litigation and regulation, which can have a significant effect on company valuation.

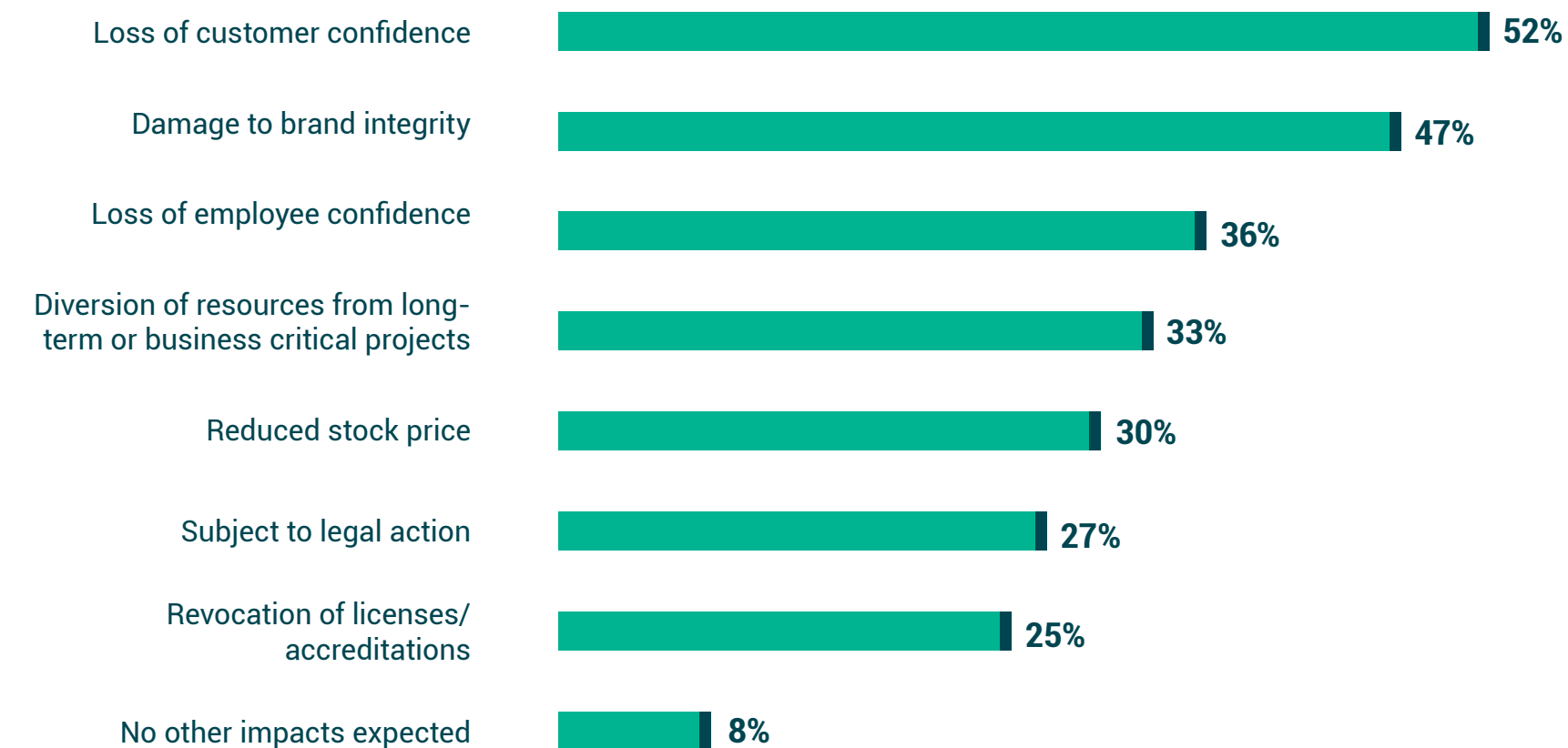
Downtime has more impacts across the organization than just the cost per hour.



Average downtime costs **\$85K** US per hour



What impacts could your organization experience from application downtime?







- 3.1 Data protection challenges
- 3.2 Data protection expectations vs. reality
- 3.3 The reality of data availability
- 3.4 Impacts of downtime
- 3.5 Today's modern data protection needs**
- 3.6 Summary

## 3.5

# Today's modern data protection needs

The need for modern data protection is more pressing than ever. With the acceleration of cloud and modern delivery practices and the reality of backup and restoration issues with legacy backup, modern data protection is essential. But what is it, according to the organizations really needing it?

According to the **3,000** global organizations who took part in the research, integrated data protection and security (**35%**), cloud workload portability (**36%**), and the ability to do disaster recovery via a cloud service (DRaaS) (**38%**) top the list.

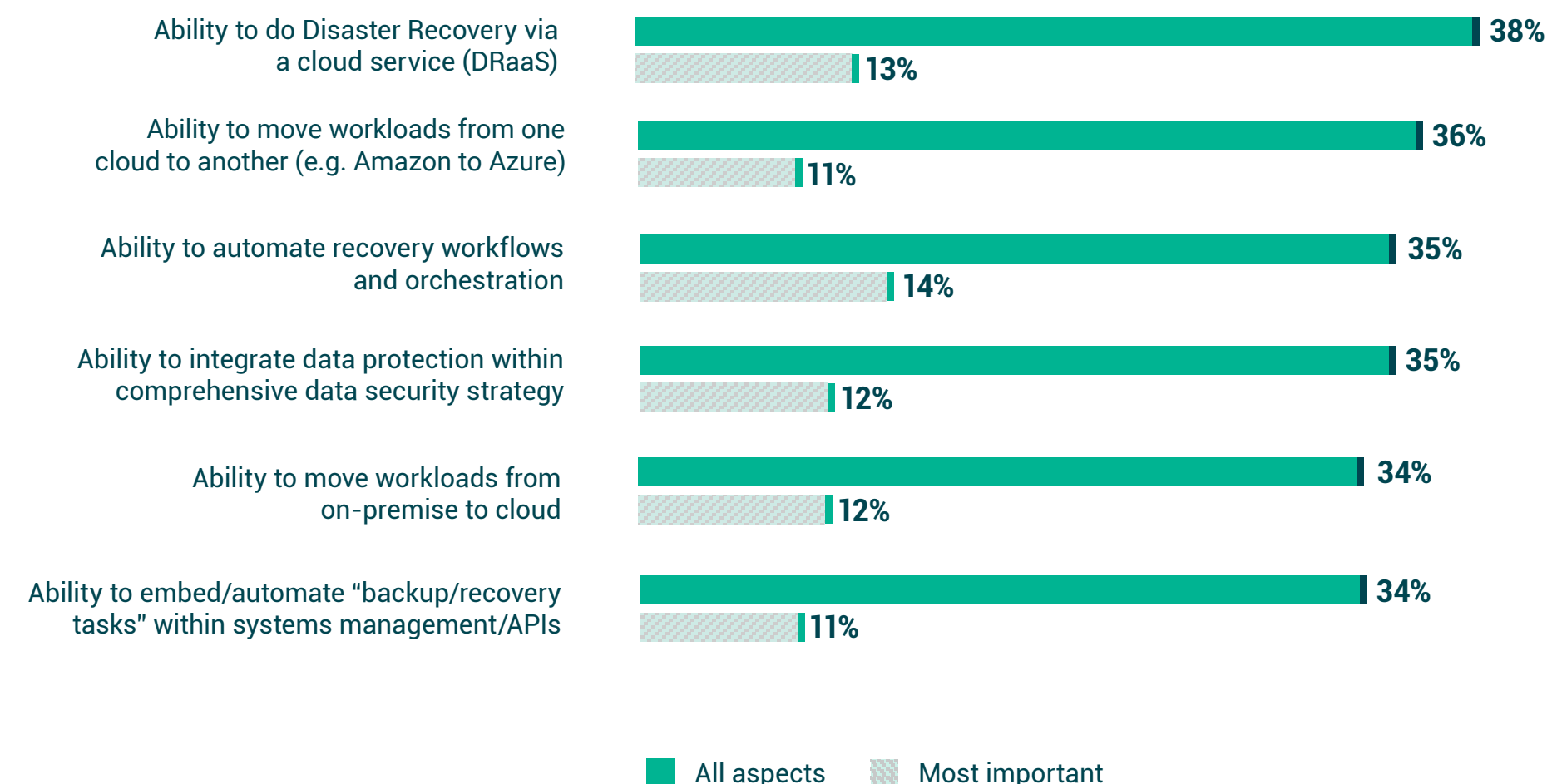
Collectively, the research shows that modern data protection needs to support the vast diversity of organizations' IT platforms (cloud, SaaS, virtual, physical), make data safe, accessible and usable for purposes such as DevOps and analytics, and ultimately enable consistent and unified data protection.



DRaaS is helping companies adopt cloud faster



Which would you consider to be defining aspects of a "modern" or "innovative" data management or data protection solution for your organization? Which is most important?





3.1 Data protection challenges

3.2 Data protection  
expectations vs. reality

3.3 The reality of data  
availability

3.4 Impacts of downtime

3.5 Today's modern data  
protection needs

3.6 **Summary**

## 3.6

# Summary



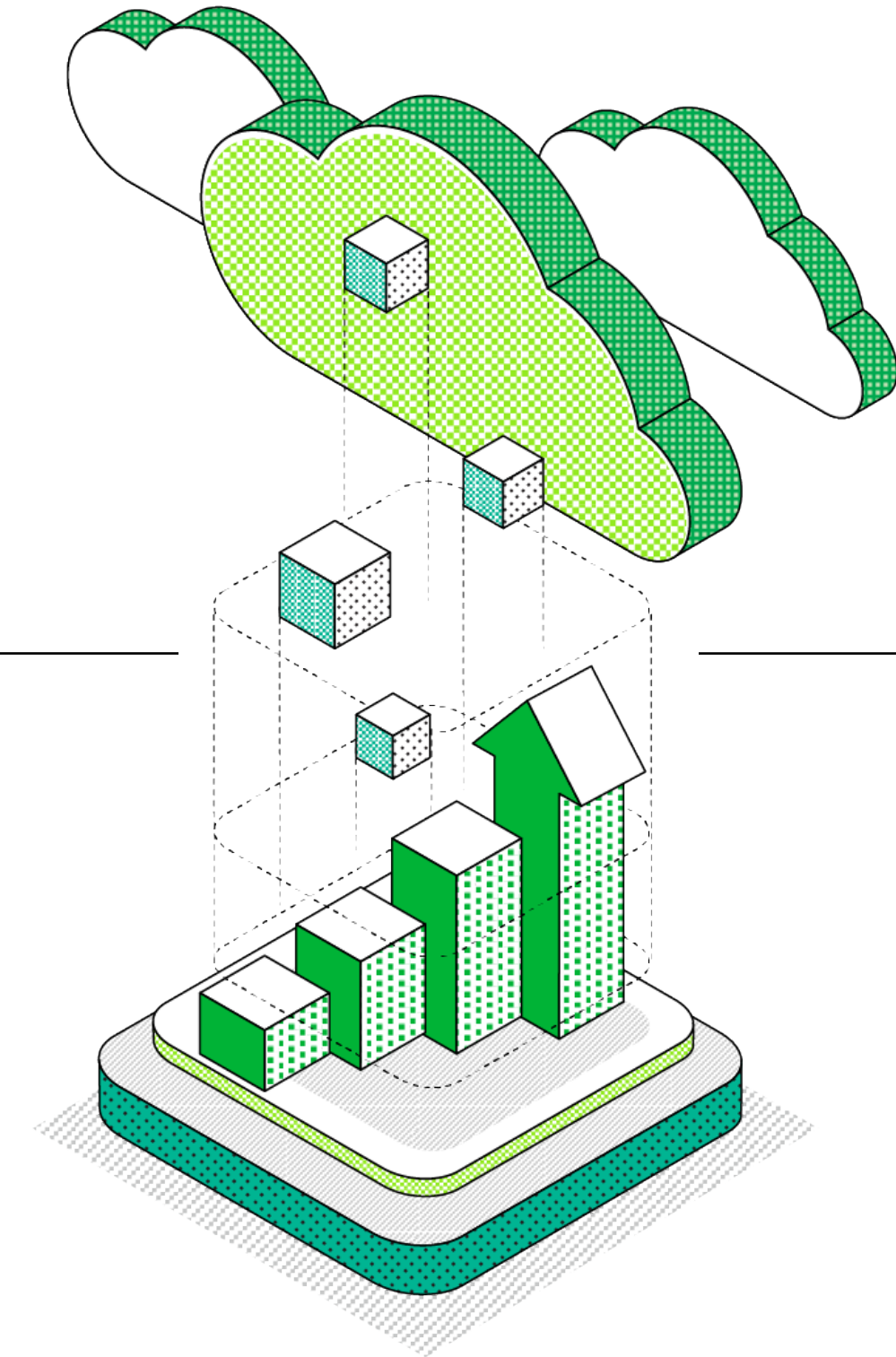
Data protection challenges are on the rise as organizations aggressively adopt modern services and new applications. They are putting pressure on legacy systems and the desire for more comprehensive data protection services. The laser focus on business continuity in 2020 has made backup and recovery SLAs mighty visible and greater weight in the organization's overall IT health.

Unfortunately, many organizations are still struggling to get legacy backup to continue to work. As systems become more advanced and complex, the pressure on aging data protection is starting to show. Organizations are desiring more from their backup than just backup. There is a strong need for standardized data protection for all data across all environments.

# 4.0 The effect of cloud on modern backup



Cloud is having a significant impact on modern backup. With the growth of cloud adoption and the advancement of cloud-based IT services strategy, the same effect is happening within modern data protection. To get a better idea of how companies plan to keep their data protection up to date, they were asked to describe their current backup environments and what they intend their environments to be like in 2023.





4.1 Cloud backup skyrockets

4.2 The future of DR is cloudy

4.3 Protecting SaaS (Software-as-a-Service)

4.4 Summary

4.1

# Cloud backup skyrockets

As organizations modernize their IT services, we also see steady growth in cloud-based data protection. The results also show growth of BaaS (Backup-protection-as-a-Service), with an **11%** estimated increase through 2021 alone, and still trending up after this. In comparison, self-managed backup using native services will stagnate, with an average of **1%** increase per year. The startling result here is the massive decline of on-prem tool usage, expected to be down over **50%** from current actuals within two years.

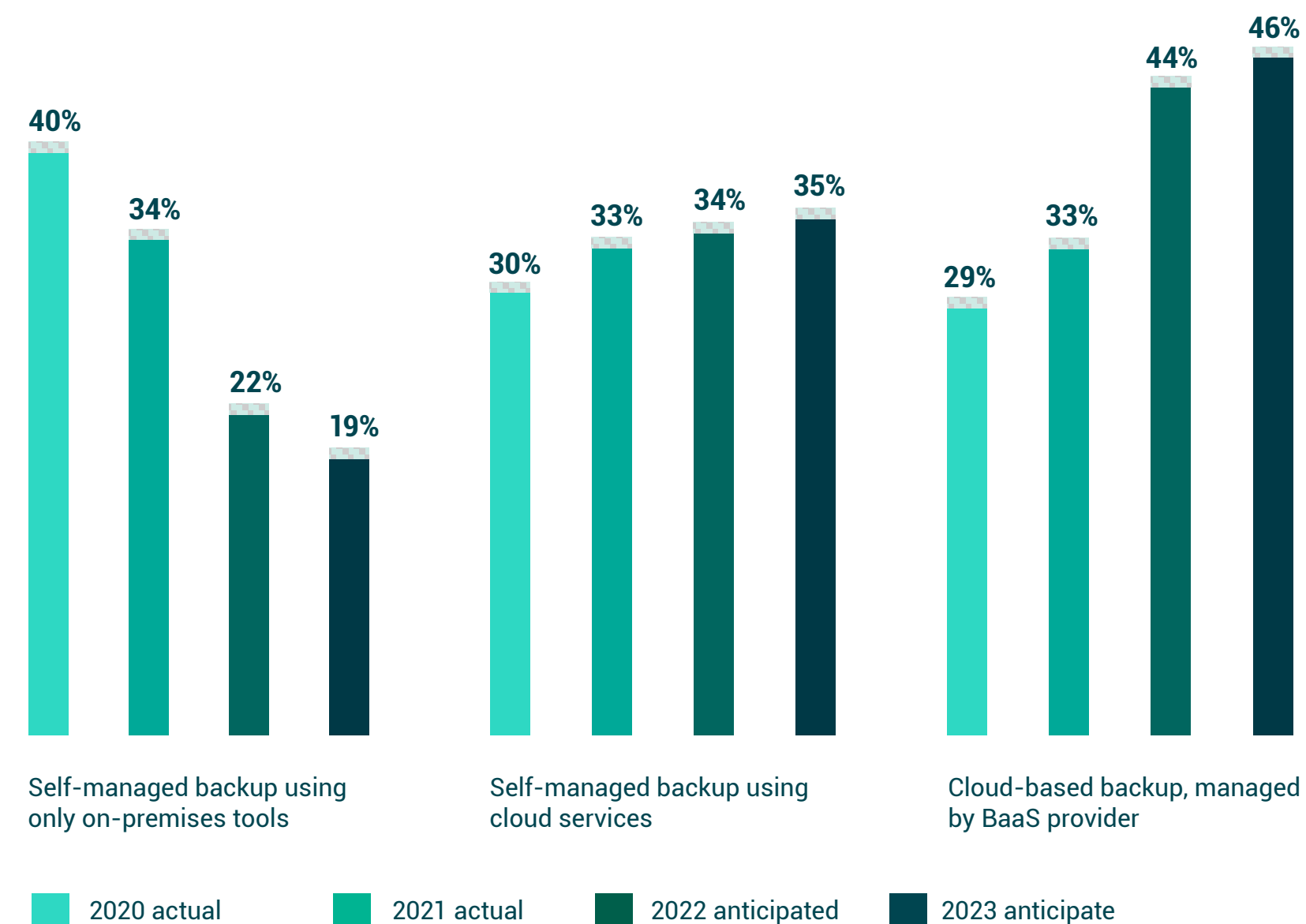
The effect of modernizing IT strategy can not be ignored, and as organizations adopt cloud-native approaches faster, it becomes increasingly apparent that they'll need to update their data protection platforms to support them.



81% of backup will be cloud based in the next two years



Approximately what percentage of your organization's production data is protected by each of the following mechanisms? Thinking ahead two years, which of the following do you anticipate being your organization's primary method of backing up data?





4.1 Cloud backup skyrockets

4.2 The future of DR is cloudy

4.3 Protecting SaaS (Software-as-a-Service)

4.4 Summary

## 4.2

# The future of DR is cloudy

Disaster recovery comes in many flavors but primarily focuses on where the will data reside (and DR “fail over” to) – with the predominant choices of DR locations being either self-managed on-prem (between two data centers) and DRaaS (cloud-based Disaster Recovery as a Service). As organizations modernize their data protection platforms, DR approaches are changing alongside.

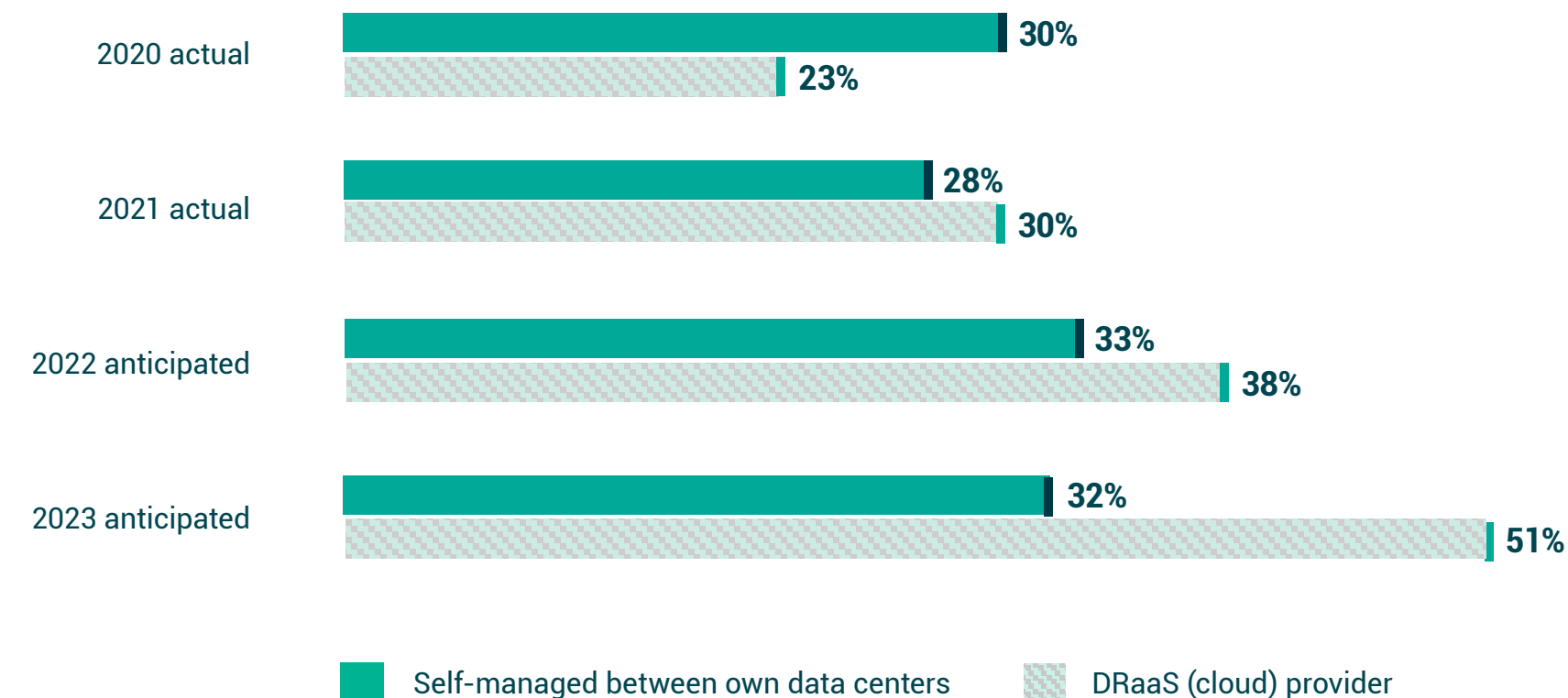
Typically, DR follows backup modernization trends, being tightly tied to the platforms, which remains the case here. With the growth of cloud-based modern data protection, the results also show a massive swing of **28%** through 2023 to DRaaS first approaches. The future of DR is indeed cloudy.



51% of all DR will be cloud based by 2023



Considering your organization’s business continuity and disaster recovery (BC/DR) strategy, is your secondary data stored within your own datacenters or at a cloud-provider? What do you anticipate doing in the next two years?





4.1 Cloud backup skyrockets

4.2 The future of DR is cloudy

4.3 Protecting SaaS (Software-as-a-Service)

4.4 Summary

### 4.3

# Protecting SaaS (Software-as-a-Service)

One of the most extensive SaaS solutions used today is Office 365. Typically, a vendor such as Microsoft provides a level of short-term or minimal-functioning data protection, such as a short-term “Recycle Bin,” but data that is not restored within that timeframe or long-term data archival are not part of the package. In these cases, third-party native backup solutions such as Veeam® Backup for Microsoft Office 365 are used, providing long-term data protection and archival services.

With the increase in the usage of solutions such as Office 365 and more companies now using this SaaS platform for critical corporate collaboration, the results also show the data protection approach’s maturation.

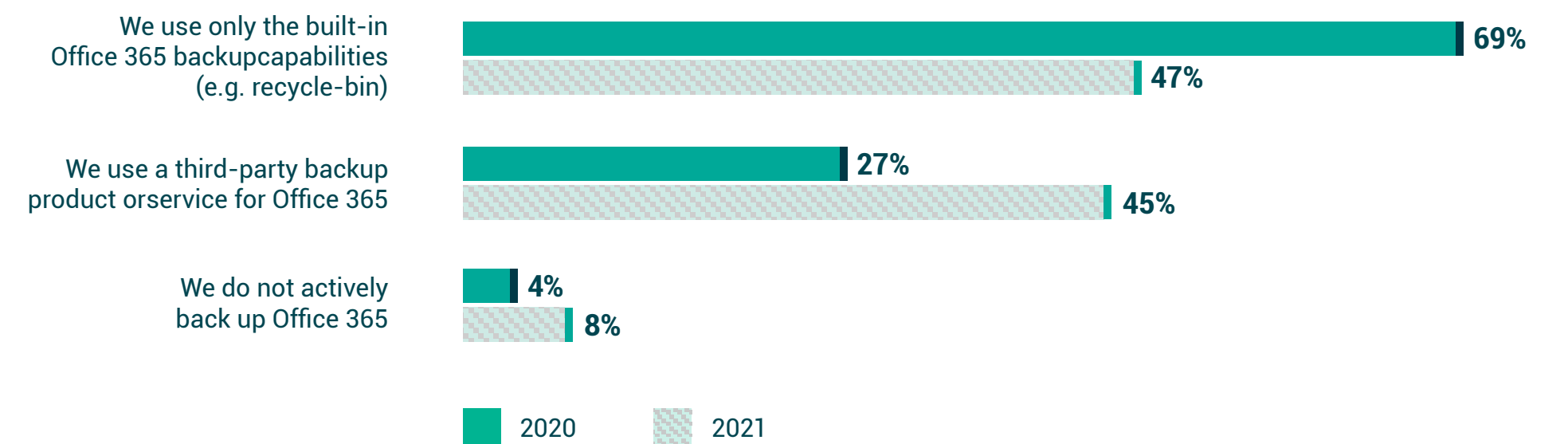
There was an **18%** growth in using a dedicated backup solution for Office 365 (such as Veeam Backup for Microsoft Office 365), with a **22%** drop in the reliance on the built-in office backup capabilities. This is to be expected as organizations are now using SaaS platforms as part of their core business, and understand the criticality of modern data protection in these environments.



Office 365 backup is almost doubling through 2021



How does your organization back up Office 365 data?





4.1 Cloud backup skyrockets

4.2 The future of DR is cloudy

4.3 Protecting SaaS (Software-as-a-Service)

4.4 Summary

## 4.4

# Summary

As IT services modernize and cloud adoption accelerates, organizations are looking more to cloud-native data protection solutions to manage their entire portfolio.

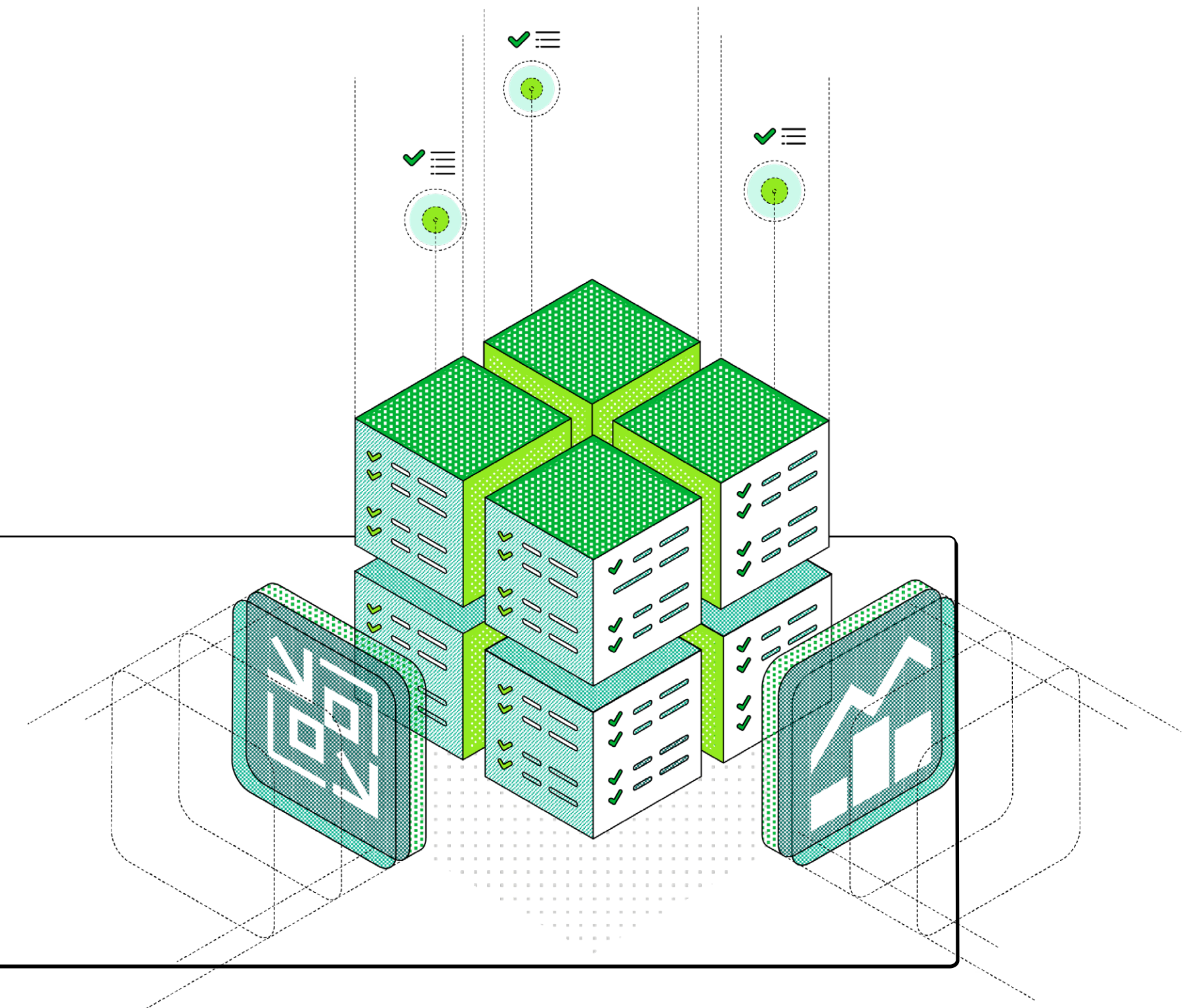
Organizations need to look for modern data protection solutions that have a cloud-first approach, that can manage all platforms centrally (in and out of the cloud) is workload focused (for greatest reach), and supports new directions in cloud-native investments, including Kubernetes.



# 5.0 Why change backup solutions in 2021?



The facts are clear; legacy data protection costs you time and money while putting your data at risk. It's holding you back from unleashing your data's full potential while ensuring its 100% protection and recovery.







5.1 The drive for change

5.2 Outcomes when adopting modern data protection

5.3 Digital resiliency

5.4 Data accessibility and management

5.5 More than just backup – driving innovation



Capabilities, cost, and complexity remain the top reasons for switching data protection solutions

## 5.1

# The drive for change

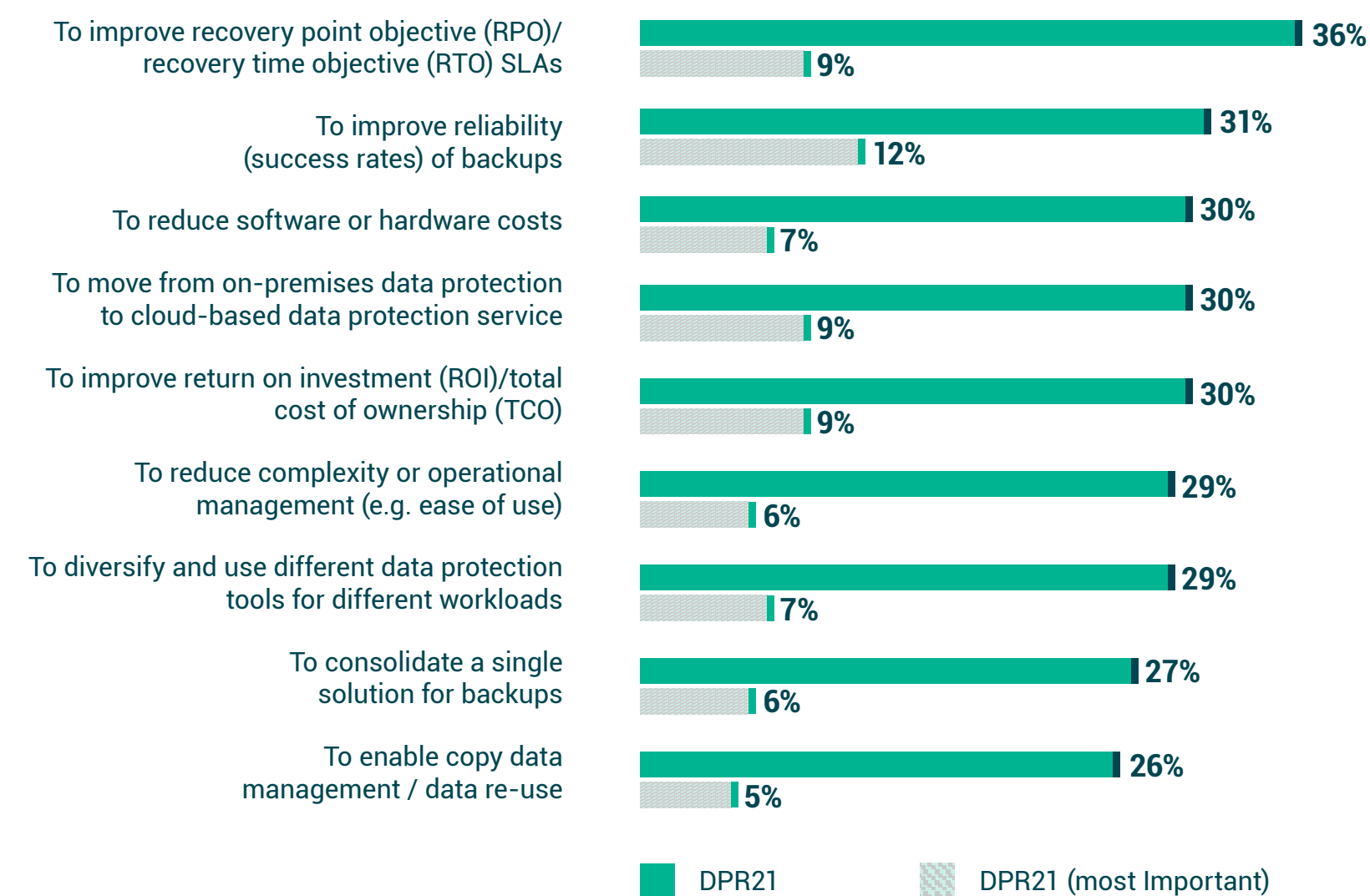
Many organizations are considering moving to a new modern data protection solution, but what are the main catalysts for change?

Topping the list is improved recovery point objective (RPO)/recovery time objective (RTO) SLAs (**36%**), followed by a reduction in costs (**30%**), and to improve reliability (success rates) of backups (**31%**). This continues to be a core theme for this year’s results – increasing the platform’s capability for backup success/recovery, while reducing overall IT spending.

One of the largest trends is the desire to change from capital expenditure (CapEx) to operational expenditure (OpEx) models (up from **20%** to **24%** this year), in line with the growing adoption of cloud-based services. Ultimately, the most important consideration remains to improve the reliability (success rates) of backups.



Which of the following would drive your organization to change its primary backup solution to a new solution or service? What is the most important consideration?





5.1 The drive for change

5.2 **Outcomes when adopting modern data protection**

5.3 Digital resiliency

5.4 Data accessibility and management

5.5 More than just backup – driving innovation

## 5.2

# Outcomes when adopting modern data protection

The 2021 Data Protection research provided much insight into trends and analysis, but what can you expect if you move to a modern data protection solution? Modern data protection can deliver new levels of confidence and operational excellence, ensuring your data is always protected and available, as well as many other economic and productivity benefits. Recently Veeam sponsored **IDC Research** to develop a white paper targeting outcomes. Some of those results, as with other research findings, are included below to showcase measurable results.



Learn more about  
 IDC Research, The Economic  
 Impact of Veeam Cloud Data  
 Management Platform, April 2020



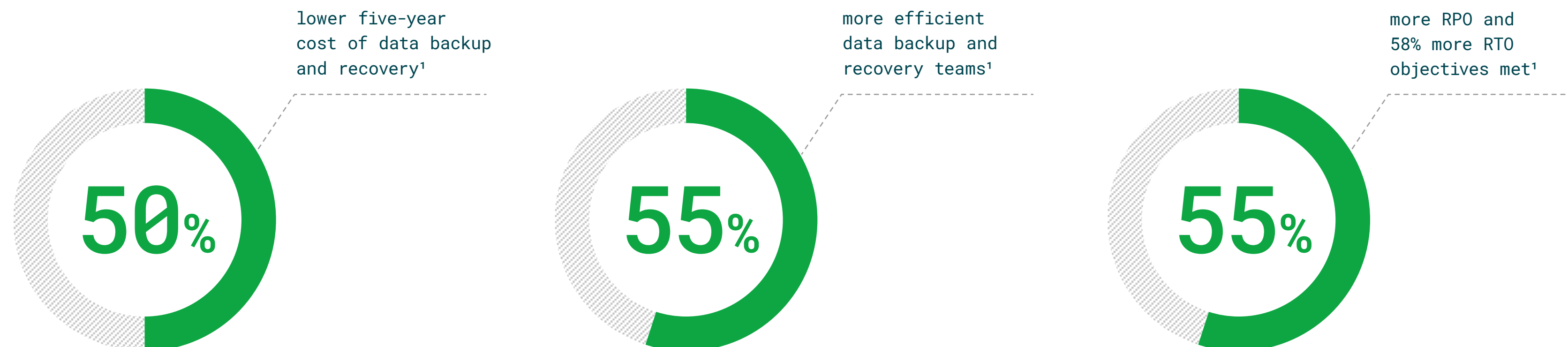
- 5.1 The drive for change
- 5.2 Outcomes when adopting modern data protection
- 5.3 Digital resiliency**
- 5.4 Data accessibility and management
- 5.5 More than just backup – driving innovation

## 5.3

# Digital resiliency

Digital resiliency is the outcome of the unified solution of unified data protection across all platforms (legacy and modern), combined with cost-effective and trusted backup and recovery. Reducing the vast overhead and cost of legacy data protection while providing reliable security against malware threats and ensuring organizational-wide data protection.

Organizations using Veeam Cloud Data Management Platform are experiencing significant cost savings (including **280%** 5-year return on investment<sup>1</sup>), increased RPO and RTO objectives, and more substantial ransomware protection and cost recovery. In fact, **95% of Veeam customers experienced little to no financial impact at all due to ransomware attacks<sup>2</sup>.**





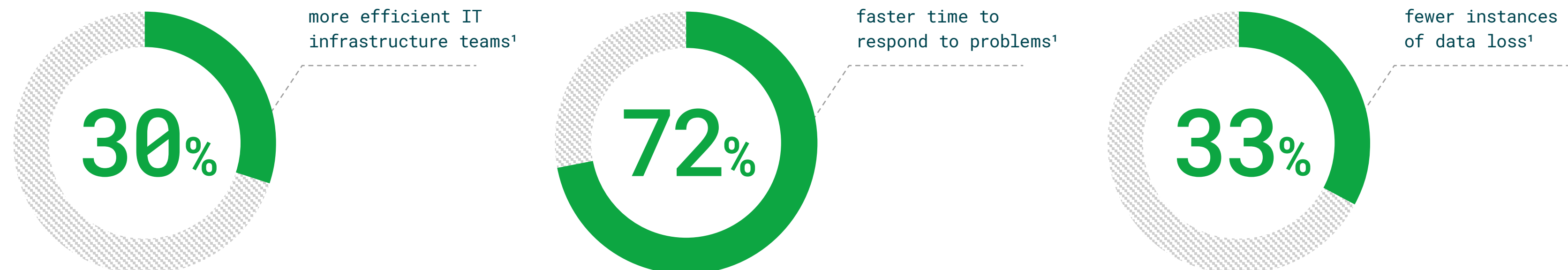
- 5.1 The drive for change
- 5.2 Outcomes when adopting modern data protection
- 5.3 Digital resiliency
- 5.4 Data accessibility and management**
- 5.5 More than just backup – driving innovation

## 5.4

# Data accessibility and management

Modern data management increases availability through automated and instant recovery, keeping data platforms healthy without manual intervention, and reducing compliance risks. Managing data without process reduces efficiency and can increase the time of recovery. Systems need automated processes to simplify management and recovery while reducing risk.

Well-managed data provides nearly perfect availability and uninterrupted accessibility, driving data trust and integrity. Organizations that have adopted a strong data management platform such as Veeam Cloud Data Management Platform experience an increased IT infrastructure team efficiency through fewer instances of data loss, and improved confidence in backup reliability leading to a **86%** reduced restoration time of business-critical workloads<sup>3</sup>.





- 5.1 The drive for change
- 5.2 Outcomes when adopting modern data protection
- 5.3 Digital resiliency
- 5.4 Data accessibility and management

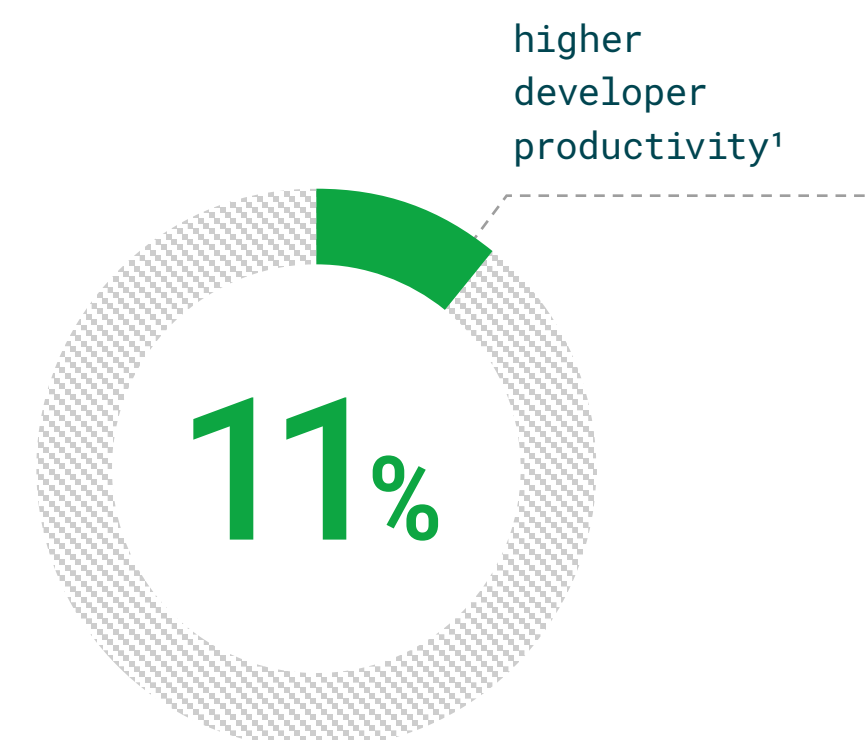
**5.5 More than just backup – driving innovation**

## 5.5

# More than just backup – driving innovation

Innovation accelerates when data is readily accessible. Legacy backup solutions can trap data, not allowing it to be re-used. Modern data management can help unleash this data, driving business goals faster. Backup can no longer be just backup. That powerful central repository of data needs to be used for more.

By re-using the trapped data in backups, organizations can drive business analysis, decision making, development, and richer customer experiences faster. Organizations doing this today experience higher developer productivity, a reduction in risk of audit and compliance failure, and less lost employee productive time due to data loss.





## 6.0 Conclusion

## 6.0

# Conclusion

With the rapid change of IT strategy and faster adoption of modern services, data protection is more than ever under pressure to be simple, flexible and reliable to support and grow the business. No longer can backup be enough; organizations are looking for more from their data protection systems. Lower costs, higher automation, and intelligence and data reuse, to name just a few.

With the accelerated adoption of cloud-based services, mainly from the COVID-19 impact, legacy data protection is having a negative effect on organizations' ability to keep critical data available. As organizations look to modernize their business practices, modern data protection must remain a key component of this plan.

<sup>1</sup> IDC Research, [The Economic Impact of Veeam Cloud Data Management Platform](#), April 2020

<sup>2</sup> Veeam Ransomware Customer Study, August 2018

<sup>3</sup> IDC Research, [Using Veeam to Ensure Data Availability and Retention in Multi-Cloud Environments](#), August 2020

<sup>4</sup> IDC Research, [IDC Race to Zero Survey 2018](#), October 2018

## Methodology

Veeam commissioned independent market research company Vanson Bourne to conduct a quantitative research study into data protection market trends, adoption and perceptions across enterprise organizations globally.

The research was carried out between September and October 2020, targeting **3,000** IT decision makers from over 40 countries using an unbiased qualitative and quantitative approach to ensure impartiality for the results.

## About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit [www.vansonbourne.com](http://www.vansonbourne.com).

## About Veeam

With more than a decade of innovation, Veeam continues to distinguish itself as the industry leader for backup and data protection. While we started our company focused on protecting virtualized workloads, our breadth of capabilities now spans physical infrastructures to public clouds like AWS, Azure and GCP, Kubernetes, and SaaS workloads.

Our complete data management platform extends beyond core backup and recovery with monitoring, disaster recovery, data mobility across cloud and data centers, security focusing on ransomware protection, and data reuse capabilities. These key components take backup to the next level. Veeam's platform growth has resulted in a leadership position in every top tier analyst ranking, peer review platform, and growth that far outpaces any leading vendor in the market.



Learn more about  
[Veeam Cloud Data Management™](#)



[veeam.com](https://www.veeam.com)