Data Management in a Multi-Cloud World:

Finance and Insurance Edition

Data Management in a Multi-Cloud World

Executive Summary

It may historically have only served as a simple extension to data storage for organisations, but cloud technology now brings with it endless potential in terms of the functionality it can offer to modern businesses.

As such, cloud utilisation is on the up across all industries, with finance and insurance no exception.

However, this growing implementation of cloud is not without its challenges, especially in the context of a post-pandemic world and one of the most highly regulated industries in existence – finance and insurance.

Many organisations are simply not performing well enough in terms of their data backups, visibility and scalability in this context. The current flaws are avoidable and this avoidance can be achieved while also consolidating vendors and simplifying the overall data management and data protection infrastructure. However, failure to improve in these areas could leave organisations vulnerable to consequences including regulatory breaches, business disruption or financial consequences.

This report focuses on a recent quantitative research study conducted with UK and Ireland IT decision makers (ITDMs). It explores how finance and insurance organisations are approaching cloud adoption, where the key challenges and apprehensions exist, and how organisations can look to overcome these challenges through making improvements to their approaches to data management and data protection.

Data Management in a Multi-Cloud World
Key findings

Click on a key finding to read more

48%

of data in surveyed ITDMs' organisations is stored or managed in the public cloud at present, expected to rise to 78% in five years' time, on average

62%

of respondents say that, thinking since COVID-19, moving more apps/data to the cloud is a top three priority for their organisation

68%

identify at least one application or data source that their organisation is unlikely to move to public cloud – security concerns (84%) are the most likely reason for this

52% indicate that risk of non-compliance with regulations is one of the greatest challenges facing the finance and insurance industries in terms of cloud-based deployments

89% agree that legislation and regulation makes data management more challenging

In the context of data backups, only a minority of surveyed ITDMs state that their organisation already has infrastructure that enables: storing backups across different locations (22%), being able to backup all workloads equally effectively (21%), automatic discovery of workloads and creation of backups (16%) and having a consolidated on-premises and cloud solution (13%)

15%

of respondents' organisations have full visibility with regards to regulatory requirements in relation to unstructured data

87%

highlight that scaling cloud backups and disaster recovery as cloud deployment grows could be easier, while 70% agree that an inability to scale cloud deployments effectively will hold organisations back

83%

utilise multiple different vendors or solutions in unison within their data protection infrastructure

<< Key findings

Cloud adoption is on the rise in finance and insurance organisations

As most organisations will know, the growing use of cloud is not expected to slow any time soon. Surveyed UK and Ireland IT decision makers from finance and insurance organisations estimate that approaching half (48%) of the data in their organisation is stored or managed in the public cloud at present, on average, and this figure is expected to rise quite considerably to 78% in five years' time. Considering the vast quantities of data that modern organisations will be managing, this represents a huge cloud undertaking. In addition, as organisations are increasingly working across multiple cloud deployments, their management and protection of this data becomes ever more complex.

The COVID-19 pandemic has only further accelerated organisations' drive towards cloud adoption. When thinking prior to the pandemic, half (50%) of respondents identified moving more apps and data to the cloud as being one of their organisation's top three business priorities. Yet thinking since COVID-19 commenced, over three in five (62%) place it in the top three.

Storing and managing data in the public cloud

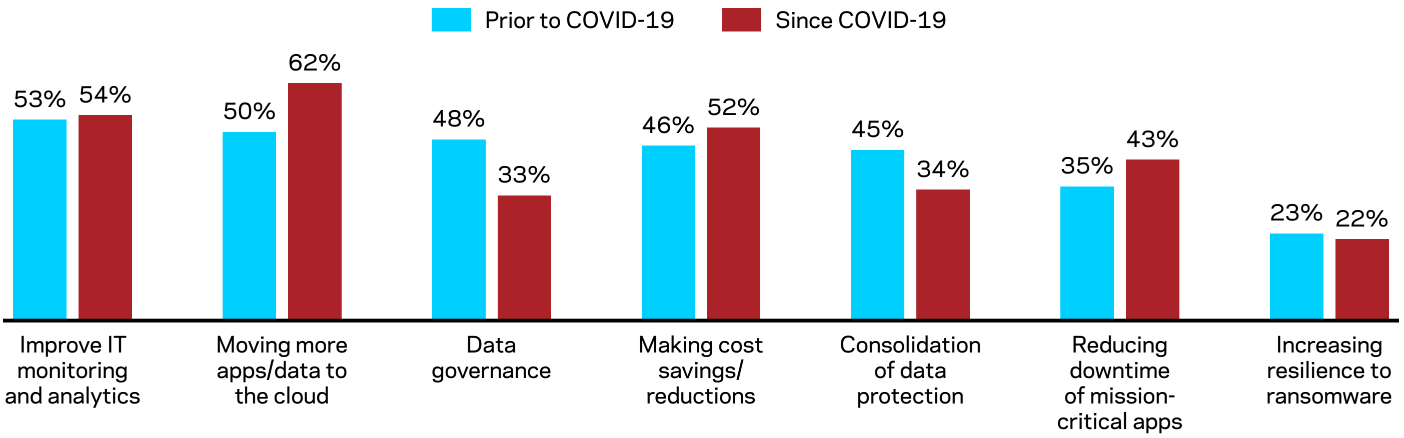
On average:

48.46%
at present

66.45%
in 3 years' time

78.48%
in 5 years' time

Organisations' top three priorities prior to and since COVID-19



Showing the proportion of respondents that place the above in the top three priorities for their organisation when thinking prior to COVID-19 and since COVID-19 [100]

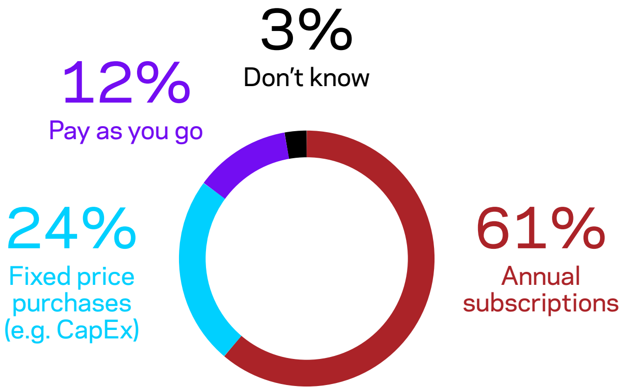
Meanwhile, COVID-19 has also resulted in organisations having to concentrate on cost reductions even more closely than normal. Making cost savings was, without question, extremely important before COVID-19, but since the pandemic commenced, and with a deep recession set to engulf the UK for what could be a considerable amount of time, this is now of paramount importance.

Over half (52%) place cost reductions in the top three business priorities for their organisation since COVID-19, yet this will no doubt be a key consideration for all organisations at present. Adding to this, approaching two thirds (63%) consider economic pressures in the wake of the COVID-19 pandemic to be among the greatest threats to their organisation's industry in the next five years.

This could in part explain why under a quarter (24%) now point to fixed price purchases (e.g. CapEx) as their preferred finance/payment option when procuring data management and data protection, compared to over three fifths (61%) preferring an annual subscription type approach. The added flexibility that this can bring holds a great deal of value to organisations, particularly at present.

Organisations are simultaneously needing to trim their financial outlay, while also needing to move full steam ahead with further implementation and utilisation of cloud-based deployments in order to remain agile and operational enough during the pandemic and its aftermath. It's a balancing act, but one which organisations must navigate while also often having ongoing doubts related to cloud.

Preferred finance/payment options for procuring data management and data protection solutions



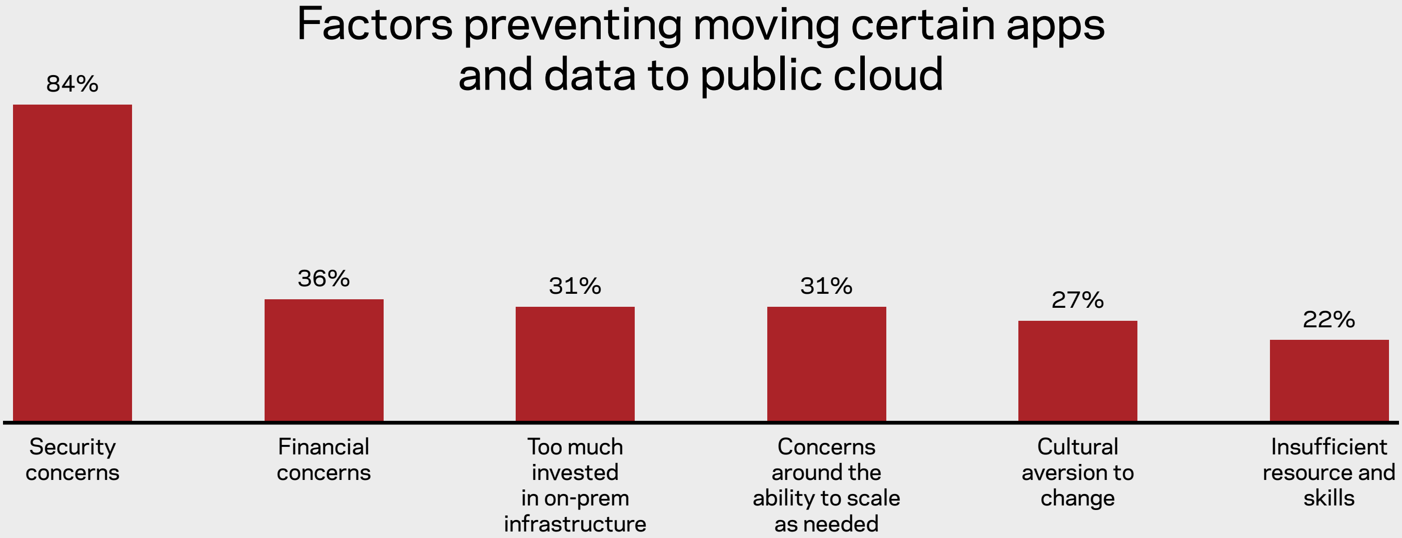
Which of the following finance/payment options would be most preferable for your organisation in terms of procuring data management and data protection solutions? [100]

<< Key findings

Apprehensions around cloud-based deployments

Despite considerable shifts towards greater cloud-centricity in finance and insurance organisations, there are still lingering apprehensions, with around seven in ten (68%) respondents highlighting at least one application or data source that their organisation would be reluctant to move to public cloud.

The standout factor preventing respondents' organisations from moving those certain applications or data sources to public cloud is security concerns, with the vast majority (84%) citing this as a worry, likely with the protection of their valuable data in mind.



Factors preventing moving certain apps and data to public cloud

What factors prevent your organisation from moving certain applications and data sources to public cloud? [67] Asked to respondents whose organisation would be unlikely to move certain applications or data sources to public cloud

This further builds on the considerable task facing UK and Ireland organisations right now. They must be running extremely lean costs and they have to be moving more applications and data sources to cloud-based deployments in order to maintain operations in the wake of COVID-19 and beyond. Yet, at the same time, they must be doing so without introducing any additional security risk.

The cost implications of failing to ensure effective management and protection of data, in a cloud context or otherwise, could be colossal, and this piles a huge amount of pressure on organisations in terms of their data protection choices.

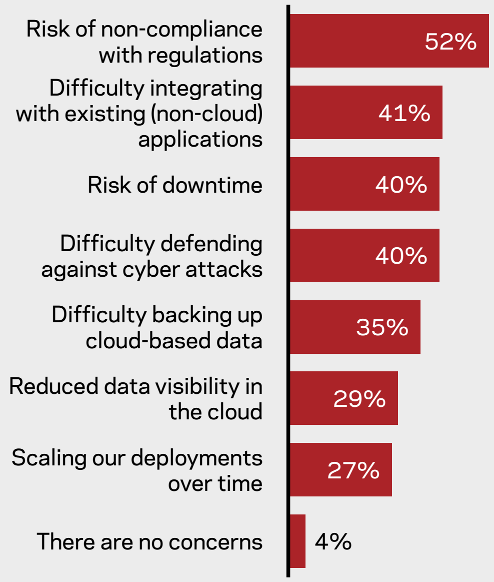
The highly regulated world of finance and insurance

In the wider context of the finance and insurance industry, a series of additional challenges confront organisations when it comes to increased cloud adoption, with regulations being front and centre within this. Almost all (96%) respondents point to at least one concern that relates to cloud-based deployments, with over half (52%) indicating that risk of non-compliance with regulations is one of the greatest challenges facing this specific industry.

This stance is further reinforced by around nine in ten (89%) respondents agreeing that legislation and regulation makes data management more challenging for their organisation. In fact, for 19%, data management is considered far more challenging. In the context of highly regulated industries in particular, this is a worrying thought. One misstep in terms of regulatory compliance could bring with it a sizeable financial hit.

As an example, consider subject access requests (SARs) since the introduction of GDPR in 2018. An overwhelming majority (98%) of respondents' organisations have a formalised process for managing SARs, but for 86% this process is at least partially manual. It's therefore no real surprise to see almost all (95%) respondents admitting that their organisation could improve its approach to managing and processing these. For enterprise organisations, the amount of time and resource that may be being spent on fulfilling these kind of regulatory requests – SARs and otherwise – is considerable. In all likelihood, it's time and resource that could be being spent much more effectively elsewhere in the organisation.

Challenges to cloud deployment



In the context of your industry, which of the following do you see as being the greatest challenges/concerns that exist in relation to cloud-based deployments? [100]

95%

of respondents admit that their organisation could improve its approach to managing and processing subject access requests (SARs)

As far as areas where there is room for improvement in terms of managing and processing SARs, respondents are most likely to place speed (84%), scalability (76%), and visibility throughout the process (74%) in their top five. It begs the question: would better data management infrastructure enable organisations to deal with regulatory requirements more effectively with these key drivers in mind?

Organisations do not have a choice around whether they comply with regulations, and the punitive fines if they do not do so can be crippling for a business. It's therefore highly important that they employ processes and solutions that make their data management as effective as possible, even in cloud environments.

Areas of improvement for managing and processing subject access requests (SARs)

84%
Speed

76%
Scalability

74%
Visibility

74%
Tracking

69%
Compliance

What in particular would be most valuable to your organisation if it could be improved in terms of managing and processing subject access requests (SARs)? Combination of responses ranked first, second, third, fourth and fifth [95]. Asked to respondents who believe their organisation could improve its approach to managing and processing subject access requests (SARs)

<< Key findings

Areas for improvement within data management and data protection

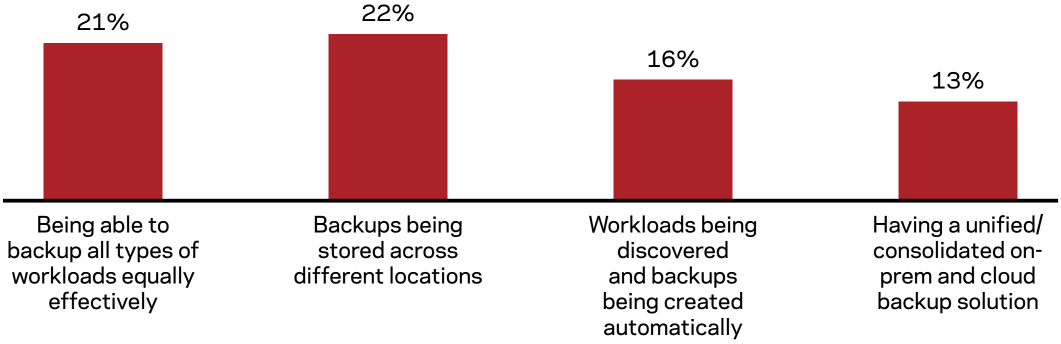
So where else are improvements needed? Which areas within data management and data protection are organisations tending to fall short of the necessary standards?

Data backups

One crucial area with notable room for improvement is data backups. The majority highlight it as either very important or absolutely essential that their organisation is able to: backup all workload types equally effectively (88%), store backups across different locations (85%), automate backup creation (79%) and have a consolidated backup solution across on-premises and cloud (76%).

However, concerningly, only a small proportion of surveyed ITDMs believe that their organisation's existing infrastructure – across any number of vendors and solutions that they may utilise in combination – already fully enables this. For example, only 21% say that their existing infrastructure enables all workload types to be backed up equally effectively. For the rest, at least some degree of improvement is required.

"No improvements needed - our current infrastructure already enables this"



Showing the proportion of respondents that believe their organisation does not need to improve and can already achieve the above with their existing data backup infrastructure [100]

Areas considered essential or very important for data backups:

88%
Being able to backup all types of workloads equally effectively

85%
Backups being stored across different locations

79%
Workloads being discovered and backups being created automatically

76%
Having a unified/ consolidated on-prem and cloud backup solution

In addition, when looking at critical cloud-based workloads, approaches to backups are subpar in many organisations. Over a third (36%) state that their cloud provider manages these backups, without any intervention required. However, this quite possibly means that a big assumption is being made – do these organisations know for sure that these backups are being managed suitably? The reality is that in many cases, cloud providers may not be backing up workloads that run on their platform – this is something that organisations ought to be wary of.

It's a gamble they could be taking, and if these assumptions are unfounded, it is certainly not the cloud service provider that would be held to account by regulatory bodies or frustrated customers should the worst happen and the company needs to restore lost data.

Organisations must ensure that their backup capabilities are comprehensive, automated, and usable across on-premises and cloud-based deployments alike in order to effectively cover them for any eventuality where a fast recovery is required.

Visibility

Data visibility is another critical element within effective data management, particularly in the context of such a highly regulated industry. Yet among surveyed ITDMs from finance and insurance organisations, only a minority (15%) claim that their existing tools and processes give them full visibility when thinking of unstructured data. For the rest, visibility is at least somewhat lacking, and this simply isn't good enough. Whether there are gaping holes or relatively small gaps in visibility, organisations could be opening the door to further risk of falling short of regulatory compliance.

Only 15%

believe that their organisation has full visibility with regards to compliance and regulatory requirements of their unstructured data

Organisations should improve their data management so that they have the all-encompassing data visibility that is needed to ensure that they remain fully compliant with regulations. This is something that will be made far easier through consolidation of data management and data protection vendors.

Scalability

Elsewhere, and more concerningly in the context of growing cloud deployments, scalability of backups and disaster recovery is a clear issue for many. While the majority (96%) of respondents say that scaling cloud backups and disaster recovery is possible for their organisation, 87% highlight that the process could be easier. In an ideal world, organisations would be able to scale up and down freely in accordance with changing use of cloud deployments, without fear of this hindering their data protection, but seemingly that is not always the case at present.

80%
believe that scaling their data protection/management solutions is a big challenge for the next five years

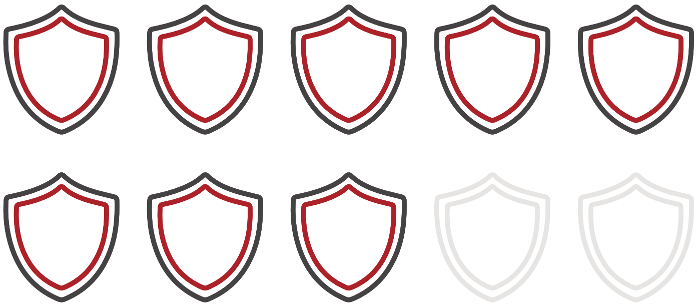
70%
agree that an inability to scale cloud deployments effectively will hold organisations back

Building on this, eight in ten (80%) surveyed ITDMs acknowledge that scaling data protection and data management is set to be a great challenge for them in the next five years. Considering the growth in organisations' cloud deployments and the growth in the volume of data that organisations are managing in general, this is hardly a surprise. Meanwhile, the majority (70%) also agree that an inability to scale cloud deployments effectively is something that will hold organisations back. In the wake of COVID-19, where a competitive disadvantage could be catastrophic for any organisation, this should be avoided at all costs.

Organisations must ensure that they are utilising a data protection and management solution which is not inhibited when it is time to scale operations up or down, so that they can embrace growing volumes of data and growing cloud utilisation rather than see this as a challenge.

Using multiple vendors

Likely to be a key contributor to the struggles facing organisations is the fact that over four in five (83%) utilise multiple different vendors or solutions in unison within their data protection infrastructure. In reality, this approach can bring with it a whole host of additional challenges and complexities.

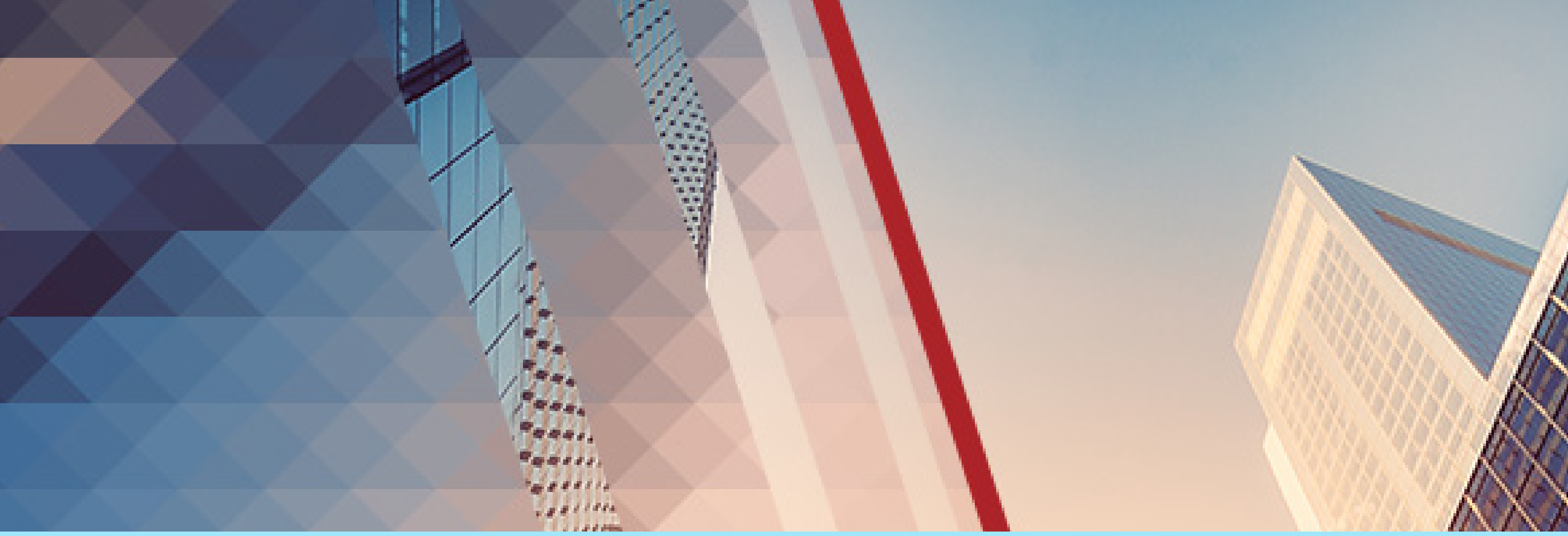


83%

are utilising multiple different vendors or solutions in unison within their data protection infrastructure

Comprehensive backing up of all data and workloads, complete data visibility, and fully scalable operations, both on-premises and in the cloud, are all inevitably going to be far more challenging for organisations which are trying to do this across a series of different vendors or solutions. Those that have a standardised approach in place for this will no doubt find it much more straightforward to find success in each of these areas individually and when considered in combination.

Organisations should therefore seek to work with a single data protection and data management vendor in order to achieve better results.



Conclusion

As cloud adoption is expected to continue rising in the coming years, something that the COVID-19 pandemic has seemingly accelerated, data protection and data management is only set to grow increasingly complex and challenging for finance and insurance organisations.

This is in addition to a series of already existing apprehensions among surveyed IT decision makers in relation to the cloud deployments of their organisations, primarily linked to security concerns and the extensive catalogue of regulations and legislation that relate to this industry.

Meanwhile, there are several important areas where considerable room for improvement exists at present in terms of data protection and data management in many organisations. Backup processes are often not automated or comprehensive enough, data visibility is not good enough, and scalability of data management as cloud deployments grow leaves a lot to be desired.

Within this, the majority of organisations are working with multiple vendors and solutions, something that is likely to be a key contributor to many of the more specific challenges being faced in the context of data management and data protection.

Organisations need to work with a single vendor for their management and protection of data. Doing so should help them to reduce workloads, mitigate complexity and improve confidence around resilience and reliability.

It's up to organisations to take positive steps towards consolidating and thereby improving their data management and data protection infrastructure – this will enable them to embrace cloud deployments without fear, rather than seeing it as a cause for alarm.

VERITAS™

ENTERPRISE DATA SERVICES

PLATFORM

AVAILABILITY

PROTECTION

INSIGHTS

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds. Learn more at http://www.veritas.com

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

METHODOLOGY

Veritas commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 100 UK and Ireland IT decision makers were interviewed in July and August 2020. Respondents were from **finance and insurance** organisations with at least 500 employees. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Copyright © 2020 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.