VERITAS

Truth in Cloud 2019 Report

1,645 cloud architects reveal their challenges and successes in dealing with backup and data protection.

Introduction

Cloud data management today: the truth

In today's data-driven enterprise, good enough is not good enough. Given the increasing complexity of IT systems and commanding expectations from end users, enterprises and government and regulatory bodies, many organizations are desperate to identify how to effectively manage mounting data. And today, IT complexity is often a reflection of necessarily dynamic hybrid and multi-cloud solutions—a benefit to a business versus an impediment to functionality.

As cloud-based capabilities have improved, businesses are moving more data and workloads to the cloud and taking advantage of cloud-hosted solutions, making multifaceted data management and protection more important than ever before.

Answering how/when/where/why data is protected—and who protects it

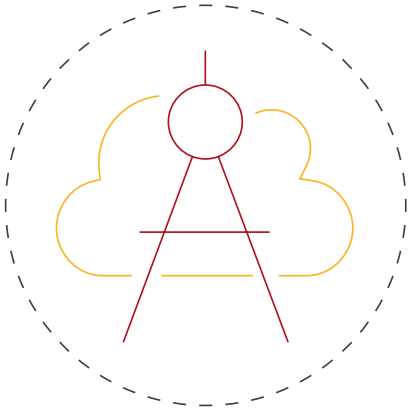
IT teams must be certain applications and data are recoverable in case of data corruption, human error, natural disaster and even ransomware—a single failure can cost a business enormously. Due to the rising responsibilities of today's cloud architects and administrators, with many expected to oversee data protection for their organizations, it's paramount to understand how they perceive the landscape and address their backup and recovery concerns.

The 2019 Truth in Cloud report highlights IT concerns in striking clarity

Cascade Insights asked 1,645 cloud architects and administrators across 15 countries to share their assumptions and insights on backup infrastructure as well as their ideas about the future of cloud data protection.

Among the key findings by Cascade Insights:

- A large portion of cloud architects and administrators believe the cloud provider is responsible for backing up cloud-based data.
- Often IT teams expect adopted hosted cloud solutions to deliver the same results as on-premises solutions.
- Cloud architects and administrators often prefer a comprehensive, single toolset beyond what the cloud provides; they are seeking simple backup and recovery for on-premises and cross-cloud workloads.
- Finally, they want a data protection solution capable of managing a range of workloads—in the cloud and beyond.



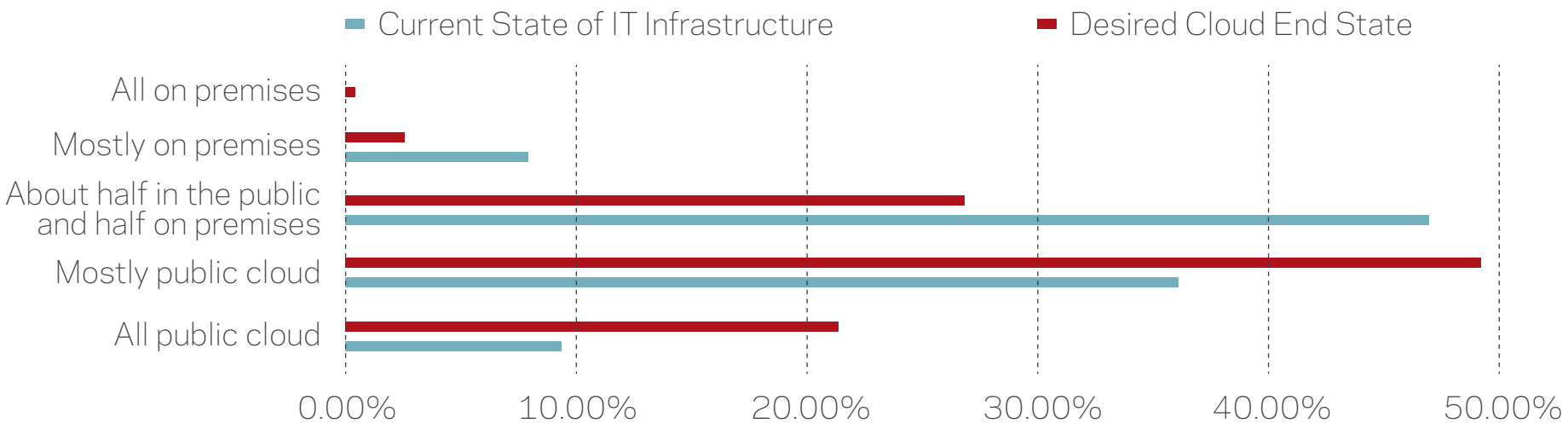


Figure 1. Over three-quarters of those surveyed want to run most or all their applications on public cloud infrastructures.

Aligning best practices to progress

Nearly 50 percent of cloud architects report almost half of their organization's infrastructure is in the cloud, with 77 percent sharing their desired end state is running most or all applications on public cloud infrastructure. And currently, nearly 50 percent of businesses are using third-party applications to back up cloud-based data (see Figure 1).

Although cloud innovation is evidently everywhere, many organizations are struggling to define best practices in data protection to accommodate the cloud. In fact, when asked about cloud backup and recovery, 34 percent of cloud architects and administrators said they believed cloud backup was the cloud provider's responsibility, with only 29 percent identifying backup as the responsibility of their organization; among this group, most preferred to outsource backup to a third-party vendor.

This finding points to a meaningful misconception: 84 percent of cloud architects and administrators believe cloud data is backed up by the cloud provider; despite the prevalence of cloud services among today's enterprises, a majority of those responsible for maintaining cloud-based data remain uncertain of who is liable for its integrity and recovery (see Figure 2).

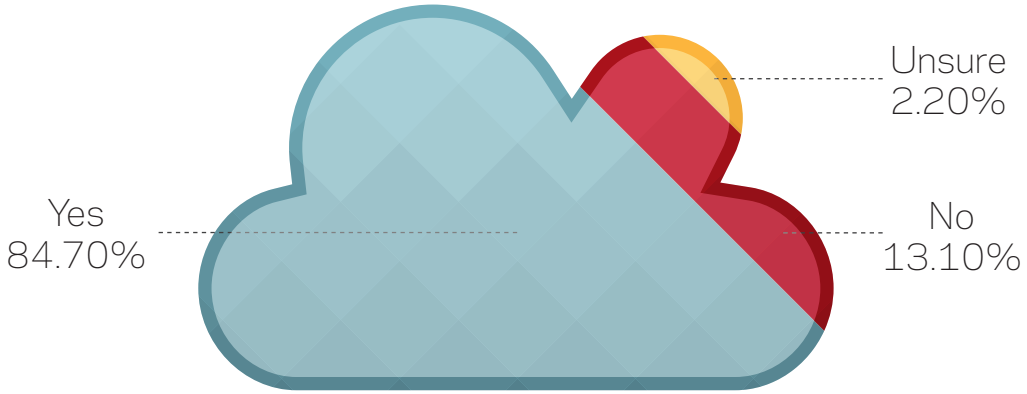


Figure 2. When asked who is responsible for backing up cloud data, most respondents think it's the cloud provider (but they're wrong).

Your data is your responsibility in the cloud

Cloud technologies are not infallible, nor are cloud architects or administrators. There will be downtime, and if downtime occurs when data is not protected, it will be lost—full stop. For most organizations, the loss of business-critical data is not an option, which is why clarity about data protection is so important. It's the responsibility of your organization to safeguard its data from the threat of potential downtime, not the cloud provider's alone.

This concern is implied in respondents' replies, with 46 percent of cloud architects and administrators noting they would like to use the same backup solution for on-premises and cloud-based workloads, though few currently do (see Figure 3). They seemingly appreciate the importance of implementing a proven, robust data protection solution, although they remain reliant on cloud-native options.

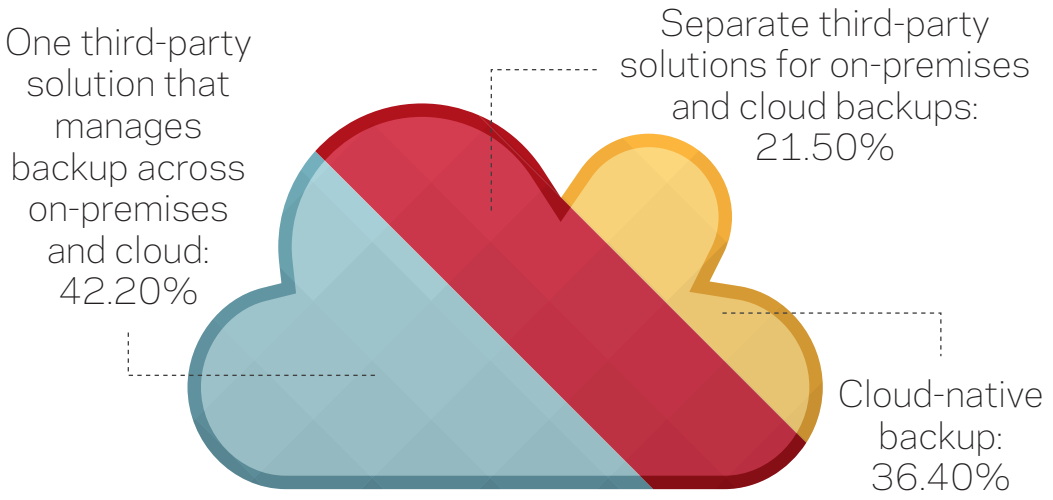


Figure 3. Most respondents use one or more third-party solutions to manage backups across on-premises and the cloud.

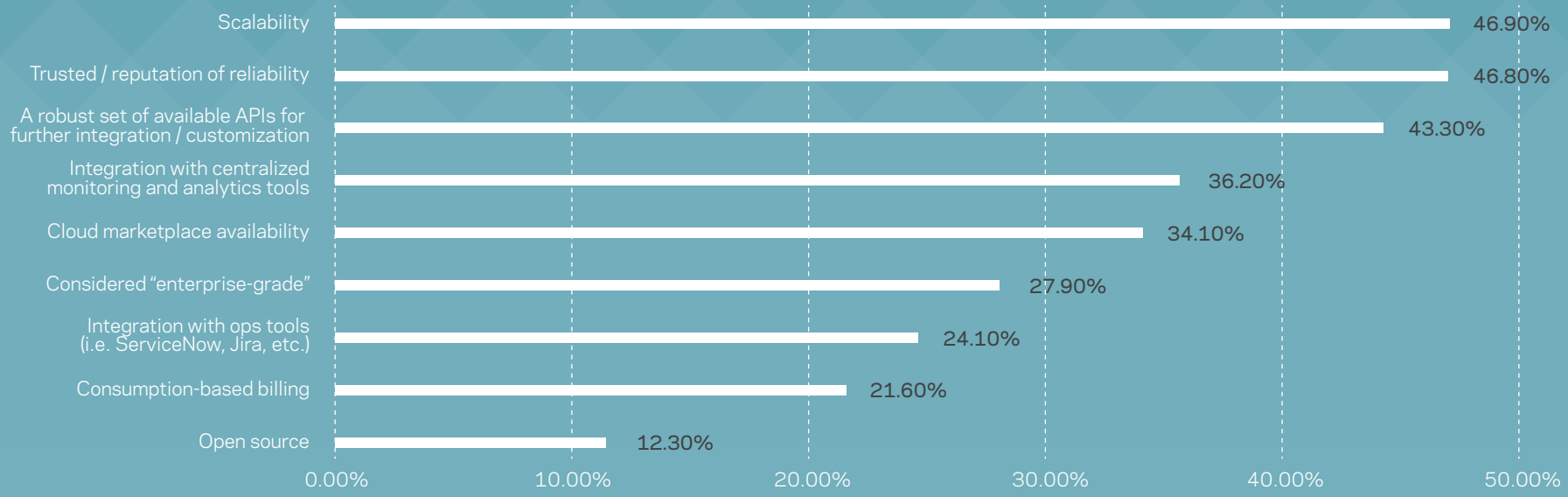


Figure 4. The most important criteria for a backup solution align with the overall advantages of the cloud.

A known need to go beyond minimal data protection

Although survey respondents express interest in cloud-native backups and snapshotting, for example, they realize real data management, like enacting data retention policies and multi-cloud backup orchestration, is preferably provided by third-party backup and recovery software. Notably, this group may be fearful of cloud lock-in, desiring to maintain the ability to move easily between cloud providers.

Increasing cloud adoption, increasing budgets for cloud data protection solutions

Despite evident concerns about cloud data management, most cloud architects and administrators say they're satisfied with their backup provider, noting the value of lightweight solutions allowing organized data management—regardless of its source—in the same catalog. They express interest in solutions that auto-discover new cloud resources and ensure they are protected, and they're willing to pay: A majority of cloud architects and administrators expect budgets for backup and recovery to substantially increase over the next three years, with the most common increase expected to be 15 percent (see Figure 6).

Several factors are driving increased budgets for data protection:

- Regulatory change, especially in the EU, is creating the demand to retain data for longer periods of time, ultimately impacting storage requirements.
- Mistrust of single backup providers is causing organizations to use multiple providers to reduce risk.
- Constant data growth requires solutions that can scale with increasing data.

As organizations become more heterogeneous, there are key areas of focus important to vendors:

- Provider support for products in the face of continual change because it demonstrates awareness of users' shifting interests and needs and the commitment to keep pace.
- API frameworks—a resource that is increasingly important as systems within organizations are interconnected.
- Flexibility because products must be able to handle changing workload requirements and maintain the same level of service.
- Confidence in meeting uptime targets—now, business continuity is a non-negotiable criterion for success.

Backup solution selection must play to cloud value propositions

To successfully address the interests and needs of today's cloud architects and administrators, third-party backup and recovery providers must be aligned with cloud value propositions, including:

- **Scalability**—One advantage of the cloud is scale—applications that are properly architected can handle an almost-unlimited load; IT teams want backup and recovery solutions that can handle scale easily, too.
- **Robust APIs**—All cloud management is possible through APIs—even on-premises management is being automated and integrated; IT teams want to be able to plug their backup and recovery solution into automation pipelines and DevOps applications.
- **Monitoring and analytics**—People want confirmation of their cloud workloads—to know backups are completed successfully and data is restored quickly and reliably.
- **Cloud marketplace availability**—Marketplaces are key resources to discover solutions that complement cloud provider offerings; architects and administrators are interested in resources to discover cloud-capable backup and recovery solutions.

Figure 5 outlines six ways third-party providers can add value in a cloud environment.

Everything is transactional in the cloud

Organizations are confined to the capabilities of the cloud provider, and they only provide a level of uptime they can confidently command. For a majority, 99.99 percent uptime is no longer sufficient—the bar is higher. In fact, 53 percent of cloud architects and administrators noted uptime targets of 99.99 percent or greater. To meet customers' expectations and remain competitive, companies providing cloud data management and protection solutions must reliably support today's high availability requirements.

53.3%
of cloud architects/ admins have uptime targets of 99.99% or greater.

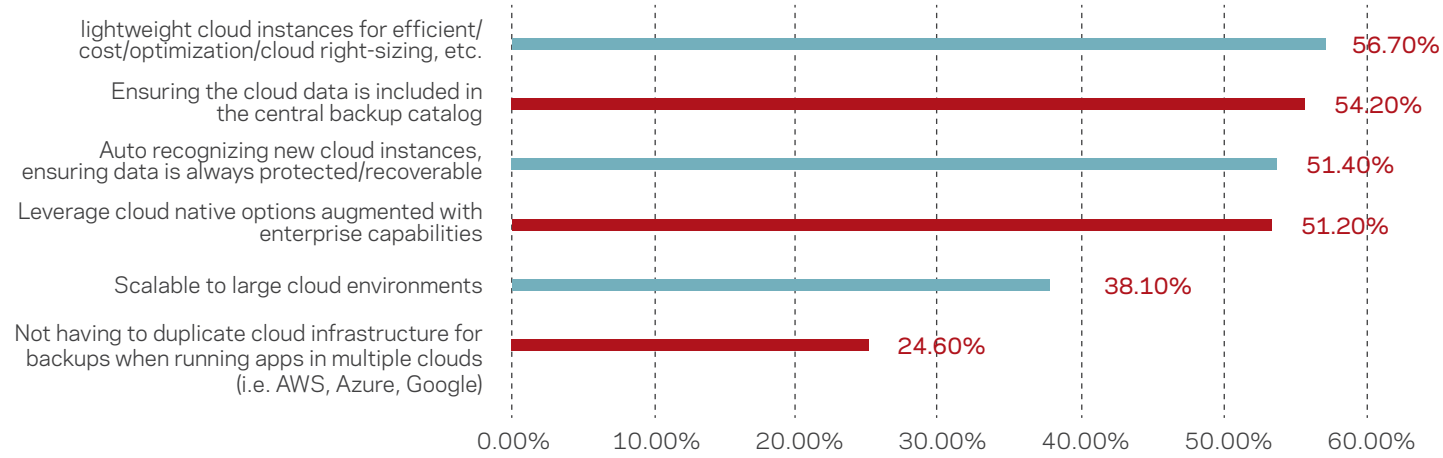


Figure 5. Six ways third-party providers can add value in cloud environments.

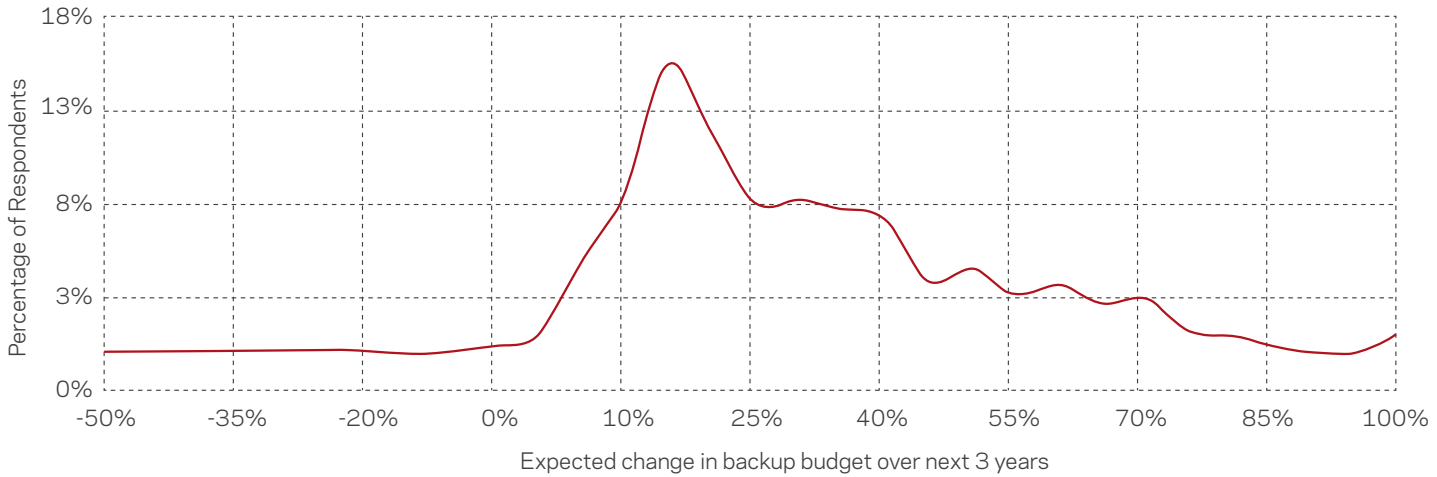


Figure 6. Most respondents expect their backup and recovery budgets to increase.

Several factors are driving increased budgets for data protection:

- Regulatory change, especially in the EU, is creating a push for retaining data for a longer period of time, creating a greater need for storage in response.
- Mistrust of single-backup providers is causing organizations to use multiple providers to reduce risk.
- Constant data growth at every company means a solution that can scale with the increasing data load is crucial.

Recoverability is key: Organizations want the ability to recover past cloud data

Cloud architects and administrators noted the desire to be able to recover data as far back as at least 10 years (see Figure 7), though currently only 13 percent are able to reach that goal. Increasing cloud usage points to a future where more data will need to be stored and cataloged and where "smart" data management policies will decide what data is kept across more on-premises (SSD and HDD) and cloud (object storage, long-term storage) storage tiers.

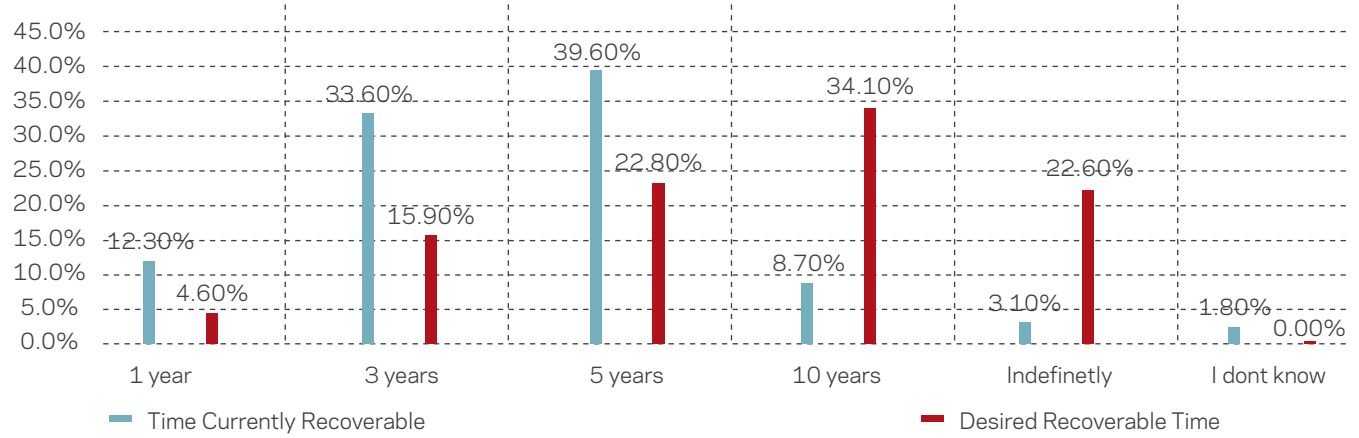


Figure 7. Although most respondents want to recover data at least 10 years old, only a small percentage are able to do so.

69%

of cloud architects and administrators expect to begin adopting or will have adopted some form of serverless computing

Serverless computing adoption on the rise

Over the next 12 months, 69 percent of cloud architects and administrators expect to begin adopting or will have adopted some form of serverless computing. Although these solutions tend to be stateless, the data created by them will need to be backed up. The data in these solutions will be stored in an increasing variety of databases (relational, NoSQL, time-series, graph) as well as disk and object storage. Backup and recovery solutions must keep up with the proliferation of cloud storage options even as new development paradigms like serverless computing take hold.

A strategy for better cloud data management

As these survey results demonstrate, notable change is occurring in data management as more enterprises move into the cloud. Organizations with a clear cloud data management strategy will likely see greater success in the long term because they'll be able to confidently meet the demands of our shared IT future—ensuring the integrity of data no matter where it resides.

The best next step for many organizations is the definition of a data management plan; they must identify the best practices and supporting solutions to manage their cloud-based data with attention to organizational plans to shift market approach and scale. Although a majority of respondents conveyed current satisfaction with their vendor, as managed services become the norm, many will seek backup and recovery solutions hosting richer, cross-environment capabilities.

SURVEY METHODOLOGY

Cascade Insights interviewed a total of 1,645 cloud architects and administrators in June and July, 2019 across the U.S., the U.K., France, Germany, Switzerland, the UAE, Canada, Mexico, Brazil, Australia, New Zealand, Singapore, China, Japan and the Republic of Korea.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at www.veritas.com or follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827 | veritas.com

For specific country offices and contact numbers, please visit our website.
veritas.com/company/contact

VERITAS

Copyright © 2019 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.

V0978 11/19