FILECLOUD

ANNUAL ENTERPRISE CLOUD & DATA SECURITY REPORT

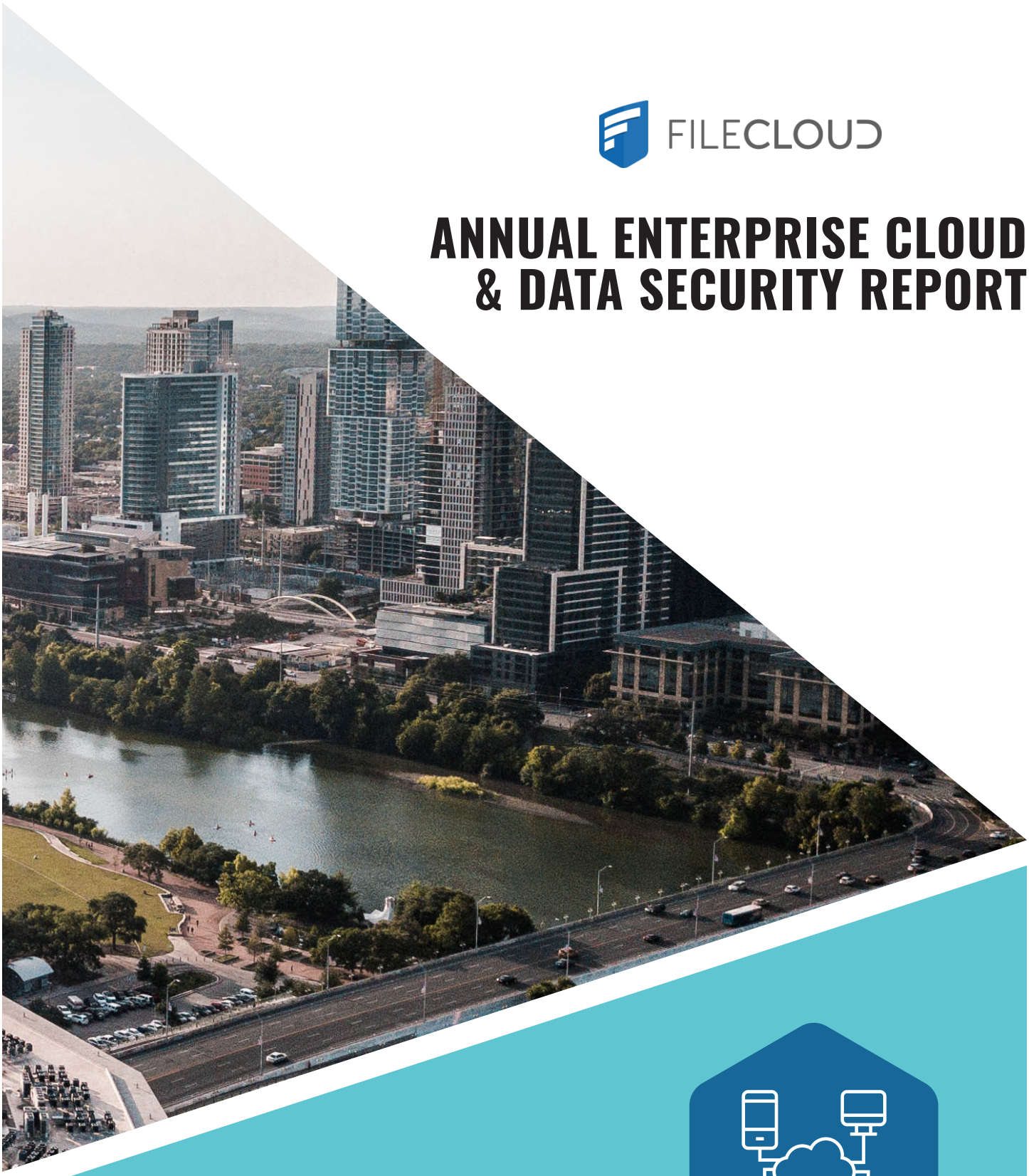


TABLE OF CONTENTS

INTRODUCTION

Recent revelations about the fragility of data security have challenged the way that many company leaders think about sharing information. From the EU's strict enforcement of Global Data Protection Regulations (GDPR) to breaking headlines on enterprise security breaches, there seems to be a new world order when it comes to protecting data.

At FileCloud, where we work with enterprises on private, public and hybrid cloud file sharing solutions, we are eager to help customers and analysts understand the ways in which the market is changing in response to these events and more. How will shifts in perceptions of data security affect the way that companies approach sharing and controlling data? Are these perceptions accurate, or are they influenced by misinformation? Perhaps most importantly, what does the future of enterprise data management look like?

To further examine the current thinking surrounding these issues and generate actionable market insights, we worked with Spiceworks to survey 150 enterprise representatives on their attitudes and approaches to enterprise data management.

Informed by the results of our survey, we can say with confidence that attitudes about enterprise data management are indeed undergoing a fundamental shift. Whereas enterprises once prioritized ease of sharing over all other factors, leaders are now more concerned about compliance, security and control.

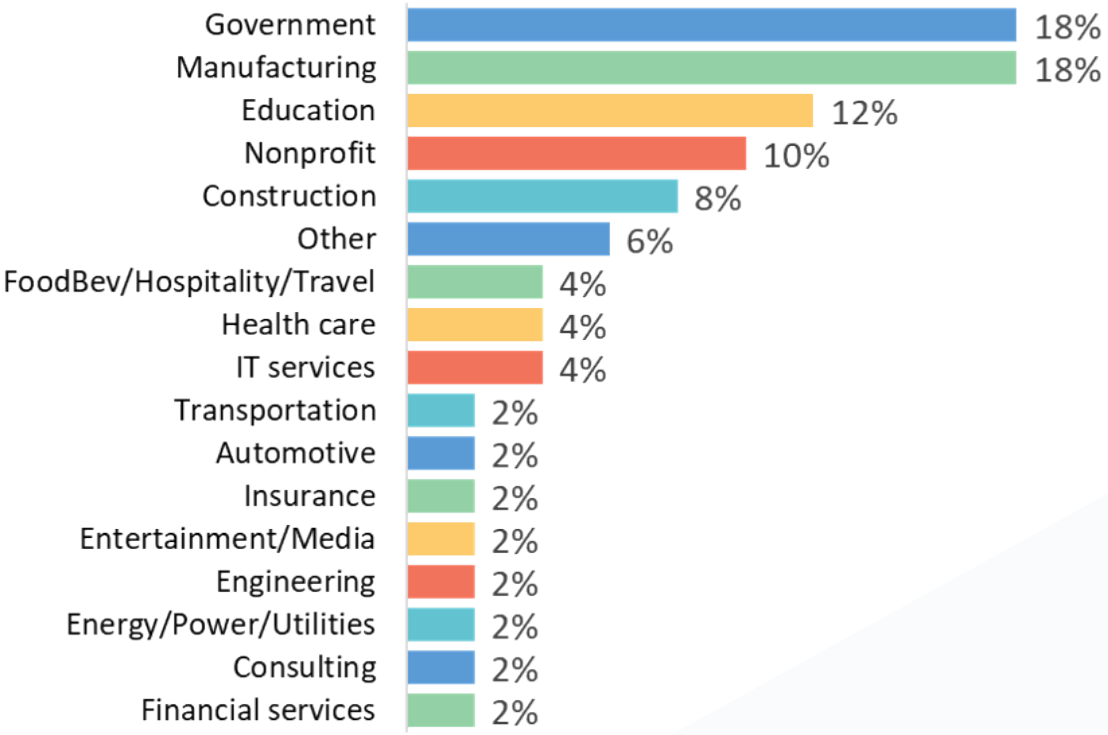
In practice, these concerns have forged a landscape where enterprises are increasingly moving away from a public cloud model in favor of a multi-cloud model. The multi-cloud model involves a mix of private, public and hybrid cloud infrastructure and services. As content is spread across it can become fragmented opening up the potential for data leaks, hacks and noncompliance issues. An enterprise data management solution not only supports the multi-cloud model but also needs to have strong security, audit and governance frameworks.

To meet these new challenges and assuage customers' fears, vendors are increasingly differentiating themselves on data control and security-related factors. Older solutions have to be discontinued to meet the growing demand for data control, which gives newer solutions such as FileCloud an opportunity to displace existing players.

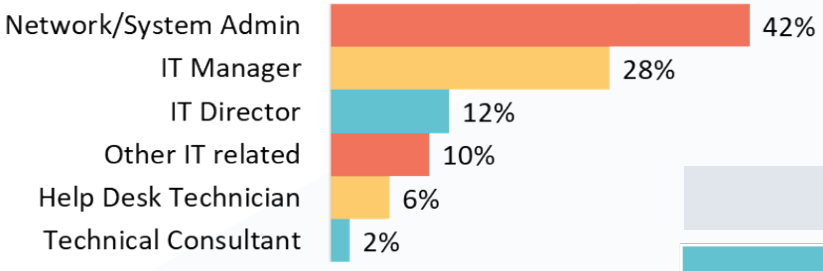
Cloud-agnostic solutions — those which provide a variety of options across public, private and hybrid clouds — are well-positioned to succeed in the current market environment. These solutions—as highlighted by our survey results—address the overarching enterprise goal of the moment: the ability to enable collaboration while simultaneously addressing data governance needs.

DEMOGRAPHICS

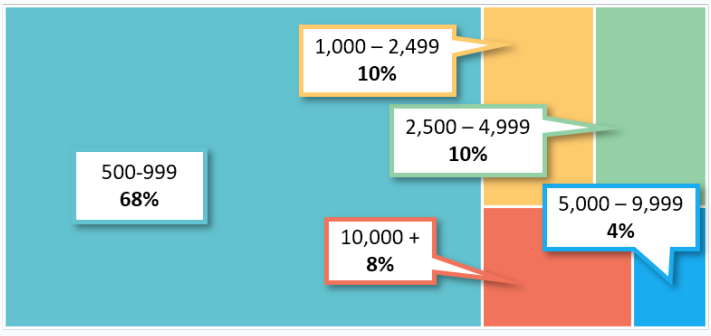
COMPANY INDUSTRY



TITLE OF RESPONDENTS



ORGANIZATION SIZE



KEY FINDINGS

64%

of businesses believe using personal sharing apps for storing and sharing office documents is the top threat for data security within an organization

82%

of company admins think employees are the weakest link when it comes to data security

1 in 2 companies say they will NOT move mission critical workloads to a public cloud environment

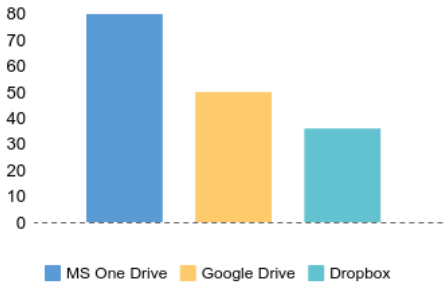
1 in 4 admins think some party other than the company has access to their data on the cloud

Top 3 Factors when Selecting a Cloud Provider

- Reliability — 68%
- Total Cost of Ownership — 50%
- Data Ownership & Privacy — 54%

- **8%** Only 8% of admins believe they are fully GDPR compliant
- **64%** 64% of admins say GDPR does not affect their company
- **38%** 38% of admins have no idea when their organization is expected to be fully compliant with GDPR

Expect to Use in Near Future



Using or Likely to Use

STATE OF THE CLOUD

Even in the Cloud Era, Businesses Don't Fully Trust the Cloud

Even as businesses continue to shift parts of their operations to the cloud, many companies harbor serious reservations about the cloud's reliability, privacy and cost. These reservations prevent enterprises from embracing the public cloud as their primary hosting and storage method; 58% of enterprises utilize the public cloud, yet a full 42% continue to use the private cloud, often as part of a hybrid model that allows them to access both public and private cloud hosting. Some companies even shun the cloud completely, with 30% choosing to self-host.

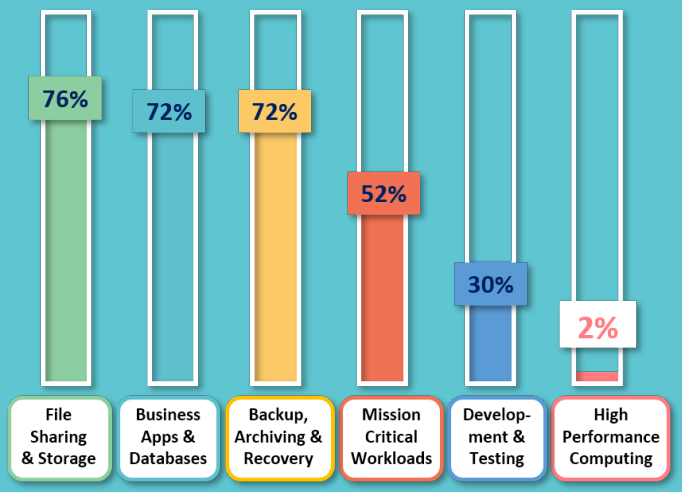
The distrust of the cloud often causes companies to separate their data and files into different tranches; only the most innocuous files will go into the public cloud, and more critical information will be stored on the private cloud or on the company's own servers. Half of all companies included in the survey said that they do not put mission-critical workloads on a cloud environment at all, citing reliability concerns. Additionally, 70% of development happens in non-cloud environments with no near-term plans to move to the cloud, indicating concerns over the security of source code.

Even putting privacy and security aside, many companies reject the cloud due to a simpler concern: cost. Less than 10% of companies are interested in moving their high-performance computing needs to the cloud, which would come at a high cost.

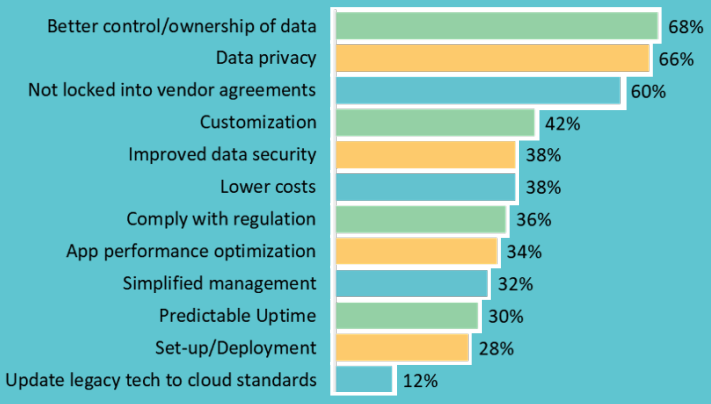
This may be changing in the near future, however, as 68% of companies expect their organization's IT budget for cloud infrastructure and services to increase in 2019.

As more companies increase budgets and explore cloud hosting options while simultaneously harboring fundamental concerns, providers should pay attention to companies' top reasons for selecting a cloud provider: reliability (68%), data ownership and privacy (54%) and cost of ownership (50%). A provider that can successfully address companies' major concerns about the cloud will be a very successful provider indeed.

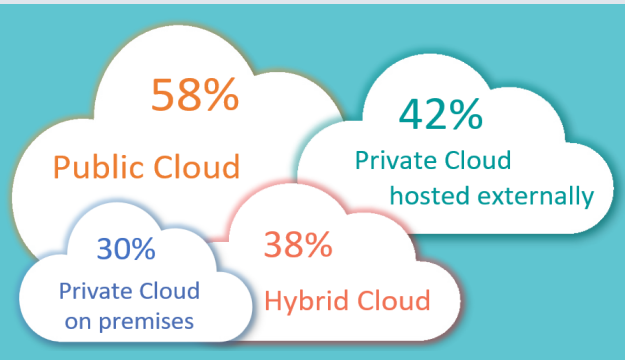
TYPES OF WORKLOADS HOSTED IN PUBLIC CLOUD



BENEFITS OF SELF-HOSTING VS USING THE CLOUD



CLOUD ENVIRONMENTS IN USE OR UNDER CONSIDERATION



STATE OF THE CLOUD PROVIDERS

Among IT Professionals, Microsoft Azure Wins Big Versus AWS in the Cloud

In the current market environment, cloud computing is essentially a duopoly dominated by Microsoft Azure and Amazon Web Services (AWS), with Google Cloud in a distant third. A full 74% of enterprises are using or likely to use Azure within the next 12 months, while only 40% are likely to use AWS in the next 12 months. Less than 18% of businesses are using or planning to use Google Cloud as their primary cloud provider.

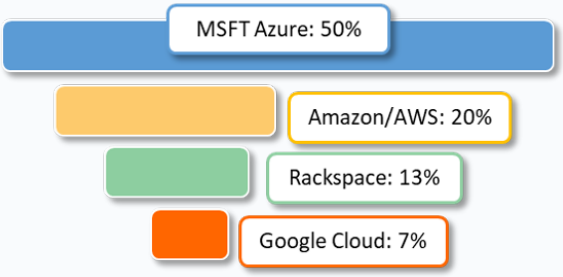
IT professionals, who often heavily influence the decision, believe that each of these top three providers are credible, ranking them all highly on the top three reasons for selecting a cloud provider: reliability, cost of ownership, and data ownership and privacy.

With similar rankings on these major characteristics for all three of the most common providers, it appears that Microsoft Azure's top position is primarily due to familiarity and compliance experience. Another reason that AWS and Google Cloud may lag behind is due to business conflicts of interest.

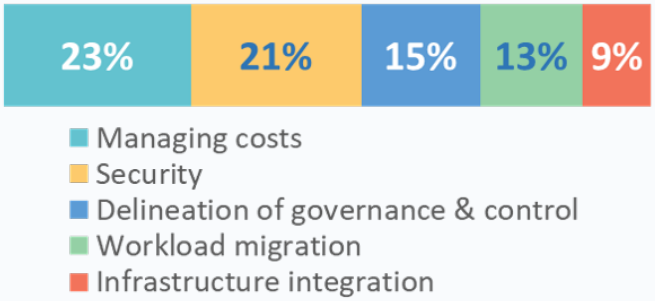
In spite of the high rankings, selecting a new provider can come with many challenges. When implementing a cloud provider, 23% of IT professionals name managing costs as their biggest challenge, followed by security (21%) and delineation of government and control (15%).

The main struggle with cost issues may be that managers expect that switching to cloud will immediately and substantially reduce costs, placing significant pressures on IT professionals to show results. Concerns about data government and control are likely exacerbated by the fact that the cloud is controlled by just a few large players, posing a competitive threat to enterprises.

TOP PRIMARY PROVIDERS OF CLOUD SERVICES



TOP 5 CHALLENGES OF IMPLEMENTING A CLOUD SERVICE PROVIDER



STATE OF DATA SECURITY AND OWNERSHIP

Enterprises Don't Fully Understand Data Ownership in the Cloud

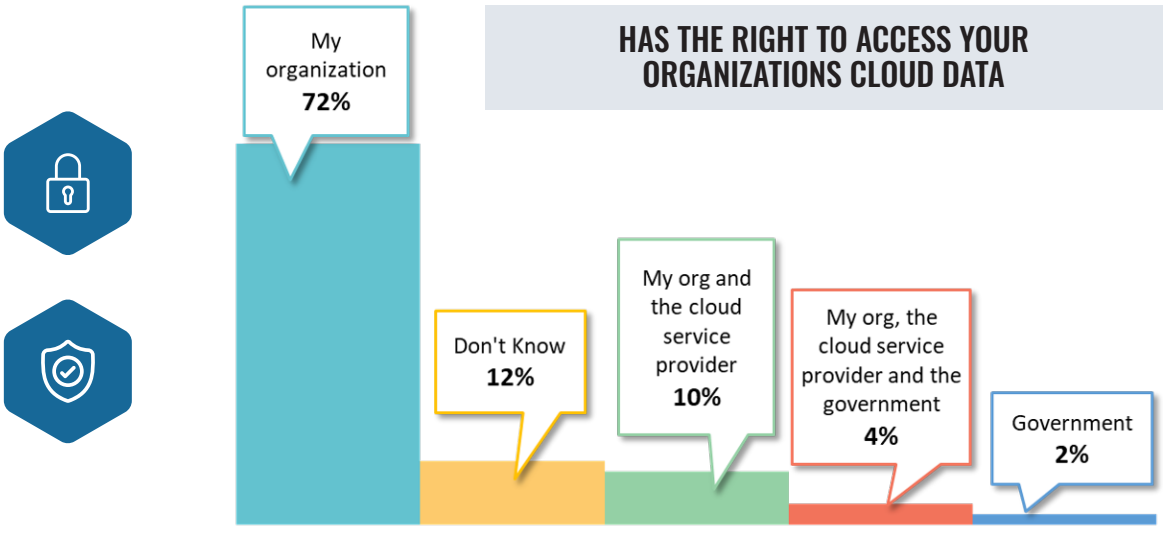
With data security and ownership consistently named as a reason that companies forego cloud computing, the topic warrants deeper investigation about the root causes for these concerns. Our survey results confirm that many commonly cited worries are actually rooted in misconceptions or a lack of understanding about who has the right to access enterprise data on the cloud.

Many companies simply aren't sure how the cloud works; one in four administrators think that a party other than the company has access to their data on the cloud, and 12% of enterprises admitted outright that they have no idea who has the right to access their organization's cloud data. Additionally, the differences between public cloud, private cloud, and hybrid cloud computing often aren't clear to decision-makers.

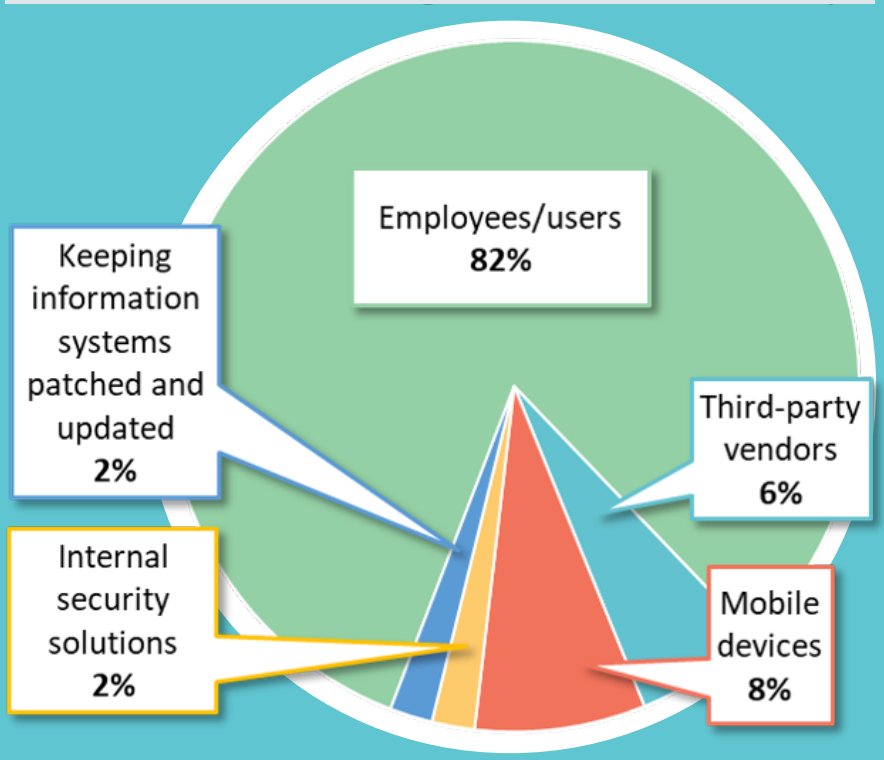
While an incomplete understanding of the cloud may exacerbate security concerns, even the most cloud-savvy IT administrators share some of the same worries. That's largely because while office IT experts may understand the cloud, their fellow employees may not; 82% of enterprises believe that their own employees are the "weakest link" to their organization's data security.

In fact, concerns about employees unintentionally exposing data is the number one fear of IT administrators, with 74% of respondents saying that it is something they worry about. Comparatively, only 68% of IT administrators said they are concerned about hacking via a password breach and only 8% were concerned about government spying or corporate espionage.

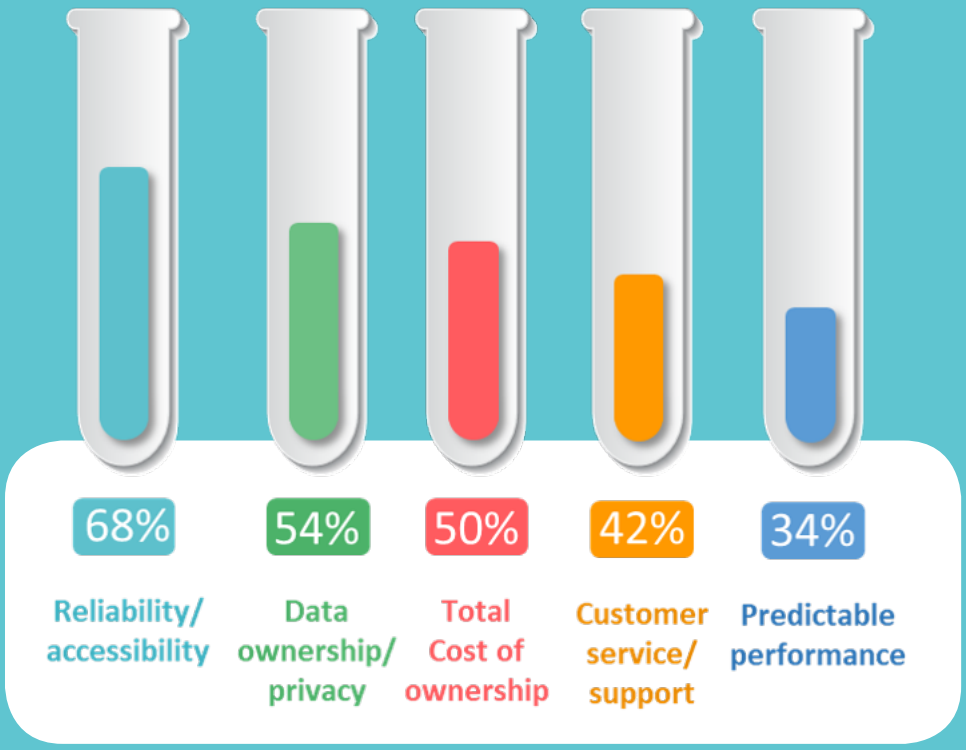
Those concerns are understandably troubling, as leaking customer data can cause severe business damage. The harmful effects of a customer data leak are so powerful that 38% of companies said that protecting customers' personal data is even more important than protecting financial data and employee records.



WEAKEST LINK IN ORGANIZATION'S DATA SECURITY



TOP 5 FACTORS IN EVALUATING CLOUD SERVICE PROVIDERS



STATE OF FILE SHARING AND COLLABORATION

Consumerization of IT is Backfiring — Companies are Concerned About Security and Data Fragmentation

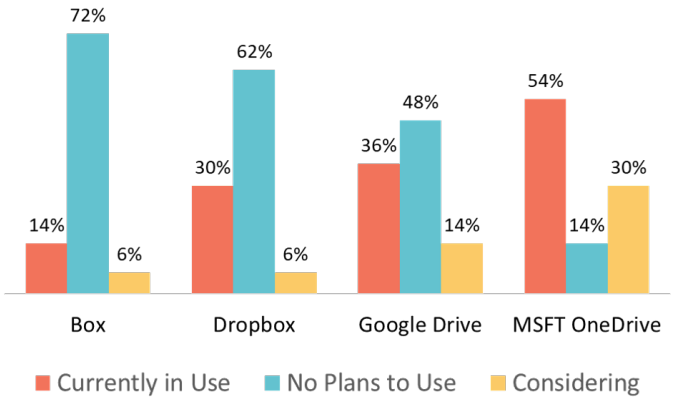
Thanks to personal cloud sharing and storing apps, cloud computing is a familiar concept to consumers worldwide. That has been a blessing and a curse for enterprises concerned about data security. While employees' familiarity with the concept of file sharing makes adoption easier, their strong existing preferences for familiar consumer-facing apps can derail efforts to stick to a sole enterprise-facing provider. It is difficult to prevent employees from storing office documents on their personal Dropbox, OneDrive or Google Drive, and 64% of businesses believe that using personal sharing apps for office documents is the top threat to data security.

The consumerization of IT is the cause of another headache for enterprise IT administrators: data fragmentation. If employees use consumer-facing cloud options instead of the company's official sole provider, they stray from the goal of unifying data into one cloud source. According to our survey, 58% of administrators believe that their employees use storage, syncing and sharing apps beyond their sole provider. Additionally, employees will often save multiple versions of the same document across different locations, and 38% of IT administrators say that cloud-based file sharing applications lead to confusion over different versions of documents.

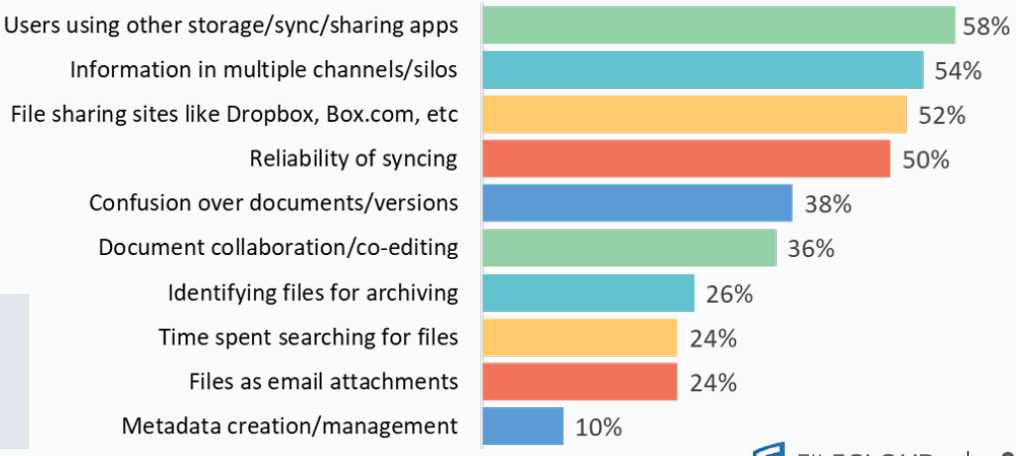
Even with concerns about consumer file sharing apps, however, many large companies still plan to utilize them; 84% of enterprises said they expect to use Microsoft Onedrive in the near future, 50% said they expect to use Google Drive, and 36% will use Dropbox. For many of these companies, convenience is king.

Additionally, enforcing strict use of a sole enterprise-facing file sharing provider doesn't necessarily remove all obstacles from cloud computing. When using enterprise-facing file sharing solutions, enterprises reported challenges concerning the reliability of file synchronization and document conflicts. If widespread, these issues result in poor user experience, reduced productivity and data loss. These are precisely the opposite effects of the results enterprises hope for when they adopt cloud computing.

FILE SHARING & STORAGE USAGE - ALL



MAIN CHALLENGES OF USING CLOUD-BASED FILE SHARING & STORAGE APPLICATIONS



STATE OF GDPR COMPLIANCE

The Threat of a Significant GDPR Penalty Hasn't Swayed U.S. Companies to Invest in GDPR Compliance

As GDPR becomes a mainstay in the EU, other countries are exploring similar regulations of their own to address data privacy concerns. While the U.S. has yet to enact similar legislation, major industry players including Apple and Microsoft have already weighed in on the benefits of similar protections for their U.S. customers. California has signed the California Consumer Privacy Act, and other states may soon follow.

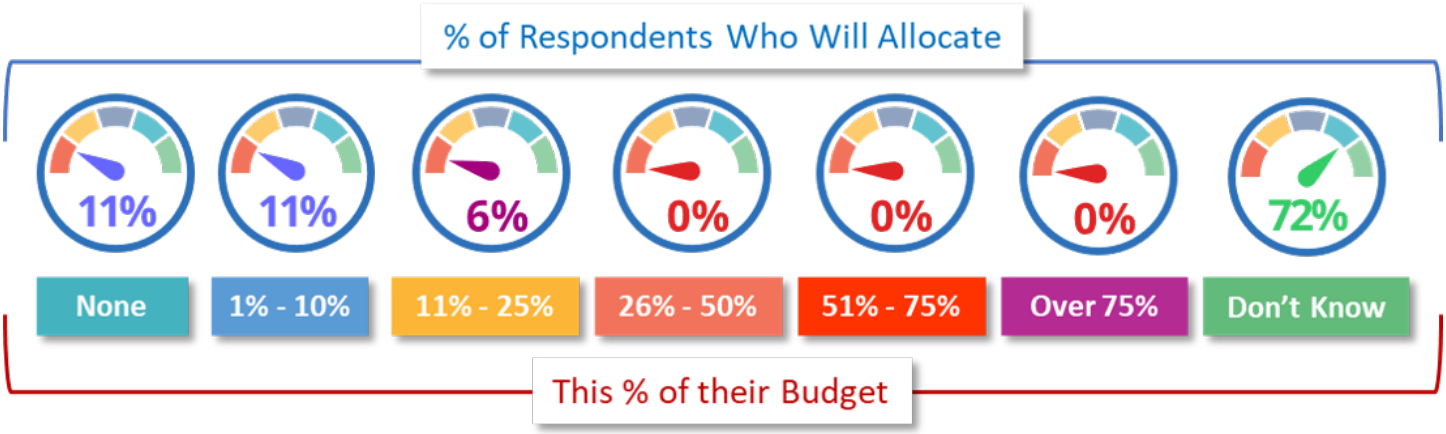
In spite of this increasing chatter and a sense of inevitability, our survey somewhat surprisingly shows that GDPR is not a pressing issue for most IT professionals in the U.S. Only 8% of IT administrators believe that they are currently fully GDPR compliant and over 60% believe GDPR doesn't affect them.

Many U.S. companies do not have clear plans to become compliant with GDPR in the future, either, with 38% of companies saying they have no idea when they expect their organization to become fully compliant. An additional 25% of the companies said they expect to be compliant by mid-2019 and 25% by the end of 2019.

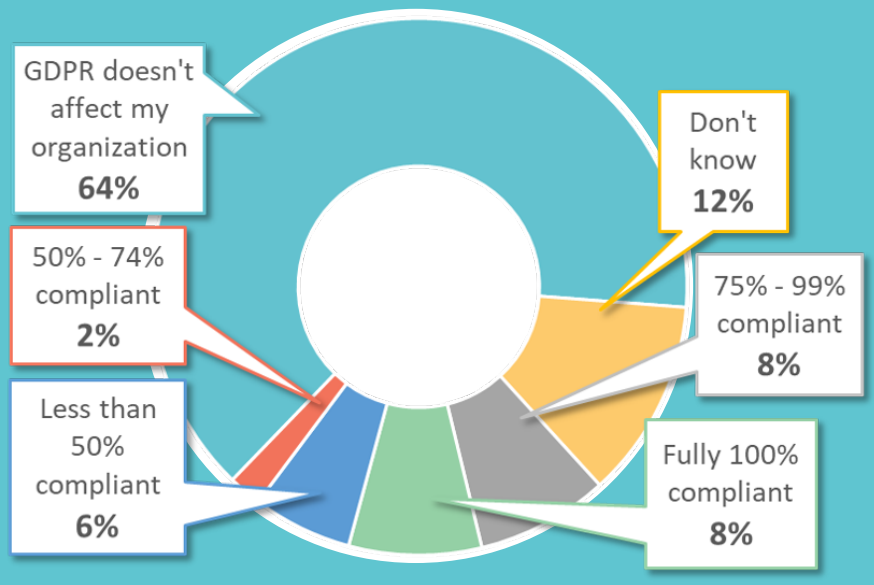
Even among the companies that do plan to meet GDPR requirements, plans often appear somewhat haphazard; just 50% of enterprises are documenting processes to prove compliance and 38% are educating end-users on security best practices. A lack of security policies and a lack of enforcement may expose companies to significant vulnerabilities regarding data protection.

The laissez-faire attitudes of IT professionals appear to reflect those of upper management. The best way for management to demonstrate support for data privacy initiatives is to allocate appropriate funding, yet 72% of enterprises responding to our survey said that they have no idea how much of their IT budget will be allocated to GDPR. At least for the moment, it is apparent that management teams at most U.S. companies don't consider GDPR compliance a top priority.

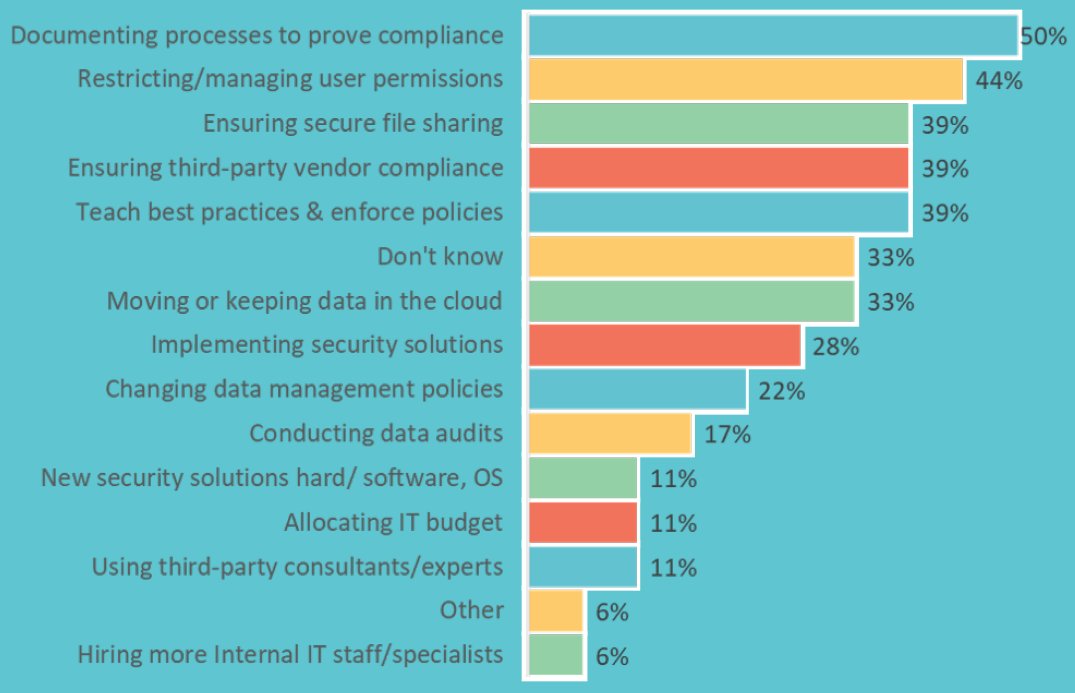
AMOUNT OF 2019 IT BUDGET TO BE ALLOCATED TO GDPR



PROGRESS TOWARD GDPR COMPLIANCE



ACTIONS UNDERWAY TO ACHIEVE GDPR COMPLIANCE



CONCLUSION

Cloud Adoption is a Work in Progress

While the cloud is gaining traction among enterprises, our study's findings indicate that removing barriers to increased adoption is still a work in progress. Enterprises often struggle with the learning curve of new technologies, and the cloud is no exception.

In order for cloud computing to truly reach its potential as a central source that can effectively store and protect data, enterprises must tackle critical security and compliance challenges related to end-user behavior. While changing behavior can be difficult, the realization that security threats can impact a company's bottom line should sufficiently incentivize companies to implement educational initiatives.

The first step to eliminating threats from end-user behavior is to establish clear security protocols and educate employees on how to follow them accordingly. Training should include information on general cloud security, best practices to control sensitive data, and the threat associated with using consumer-facing cloud tools outside of company protocols. Since employees are currently seen as the weakest link in data security, shoring up their knowledge and understanding can increase confidence in cloud computing.

To be effective, any education effort will require support not only from IT administrators, but also from top management. Managers should issue top-town directives and align incentives to ensure that there are real consequences for inappropriate end-user behavior.

Until then, it seems apparent that companies will opt for name brand recognition in order to balance their concerns about security and reliability. Companies will also find comfort in opting for a hybrid cloud model, which offers a high degree of control and choice and the ability to keep sensitive information on their own servers.

In spite of reservations, most companies do recognize the incredible potential of cloud-based environments to aggregate data into a central location while keeping that data safe. Against the backdrop of an expanding need for collaboration by an increasingly global workforce, businesses that can get their cloud strategy right will enjoy a comparative advantage over less cloud-savvy peers. Additionally, as data privacy legislation becomes the norm, those who already have a compliant cloud strategy stand to benefit.

With the right tools and the right procedures in place, enterprises can move beyond their distrust and embrace the cloud for its incredible possibilities.