Unlocking the Public Cloud

Benefits, Strategies, Challenges, and Solutions

White Paper

Introduction

There is no doubt that public clouds are transforming businesses and organizations at nearly every level. Of course, not every organization is there – yet. But those who are, now have the ability to offer great insight to companies considering how to adopt and leverage public clouds, or help guide future strategies for those already there.

A year ago, we conducted research that highlighted our understanding of how the cloud became mainstream. This year, we dug deeper across a larger pool of cloud users to find out what they are doing, the challenges they face, and how those challenges are being solved.

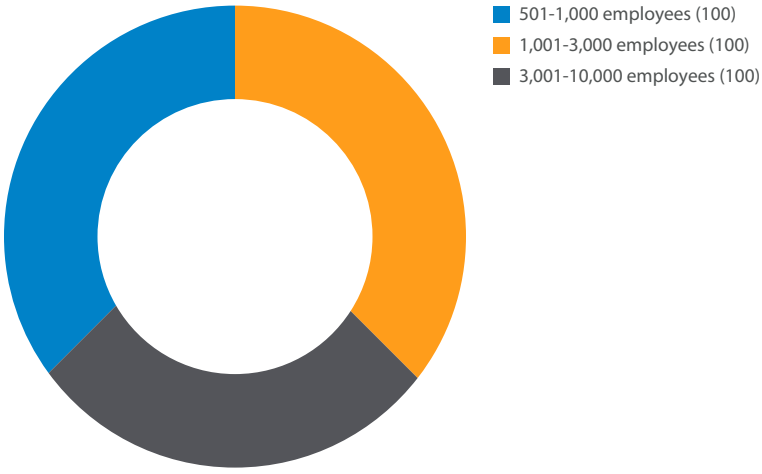
We found that interest in the public cloud continues to grow: On average, respondents' have over 40% of their infrastructure in the public cloud, and it appears that this number will increase to 75% in five years. They use services provided by a number of vendors for a variety of reasons, including storage of sensitive data. However, with approximately 50% of firms affected by a cyberattack and another one-third expecting one in the future, security remains a key concern. Only 57% feel their cloud infrastructure is totally secure.

The report also illustrates a disconnect between what organizations think they understand about cloud security and the real responsibilities that cloud providers bear. This is reflected in other findings, including how more experienced organizations in the cloud are enhancing security and fixing infrastructure gaps in order to become less prone to attacks; they are also doubling-down on leveraging public clouds.

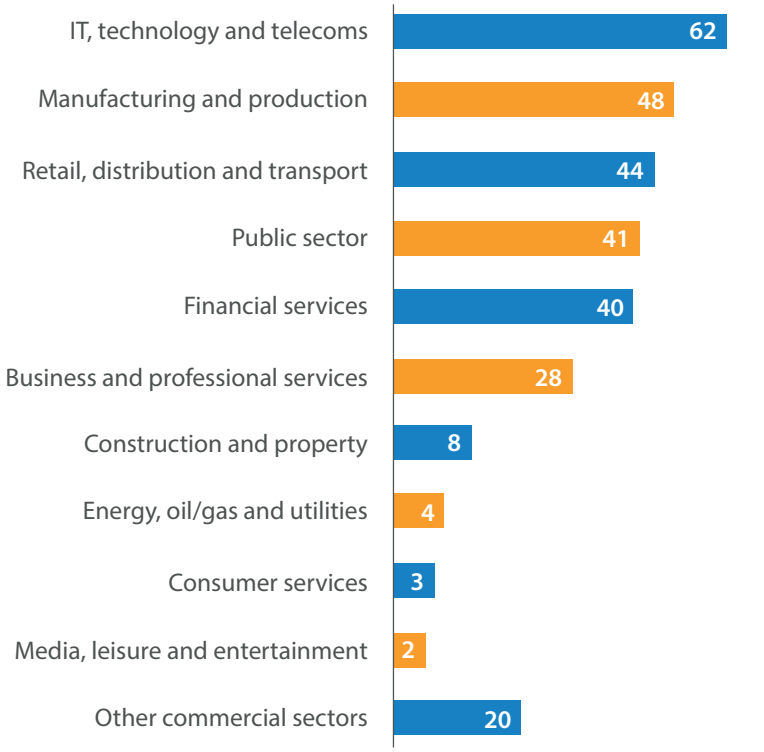
Demographics

Barracuda Networks commissioned Vanson Bourne to interview 300 IT decision makers from organizations across the US using public cloud Infrastructure as a Service (IaaS), widely dispersed across small, medium, and large-sized organizations. The study was part of a global report that analyzed the results of 1,300 interviews with IT leaders worldwide.

Number of employees in US respondents' organizations



Sector of US respondents' organizations



Key Findings

Public cloud adoption is growing at a rapid rate across industries

Respondents currently run 44% of their infrastructure in the public cloud, with intent to increase to 62% in two years and 76% in five years. Researchers found little discernible difference across vertical segments, with technology organizations understandably a few points above average, while public sector adopters leverage nearly 40% of their infrastructures in public clouds.

Different cloud providers have different strengths

On average, organizations are leveraging three different cloud infrastructures within their overall IT infrastructure. When asked which is the most utilized, Azure leads with 66%, AWS with 46%, and Google Cloud Platform with 36%. The majority of respondents (68%) employ multiple cloud providers because they believe different platforms have different strengths, while 52% feel security is increased through the use of more than one public cloud service provider.

Public clouds offer endless benefits

Ninety-nine percent of respondents report their organizations have seen benefits as a result of moving to the public cloud. While some companies saw 40-50% return on their investment—or even more than 50%—the majority of respondents experienced between 26% and 30% return within their first year of cloud deployments.

Security concerns still prevent widespread cloud adoption

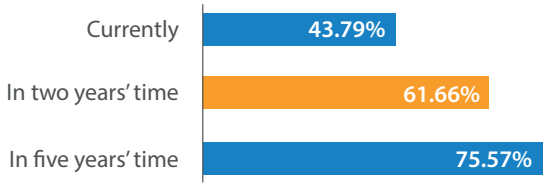
Seventy-four percent of respondents state that security concerns restrict their organizations' migration to the public cloud. In addition, about a quarter of respondents reported that they are concerned over the lack of an expert partner to work with for cloud security (26%), or have a lack of in-house skills to maintain the cloud (23%).

The Shared Responsibility Model is misunderstood
Although cloud vendors are only responsible for the security of their infrastructures under the shared responsibility model, 77% of respondents believe that public cloud service providers are responsible for securing customer data in the cloud, and 68% suggest public cloud providers are responsible for securing applications running on public clouds.

Organizations lack security measures for proper protection
Despite the lack of clarity around the shared responsibility model, 30% of organizations have not added additional security solutions to their public clouds. Additionally, of those who do have additional security measures in place, 95% of them see a need for added security outside their current scope.

Once in the Cloud, Adoption Soars

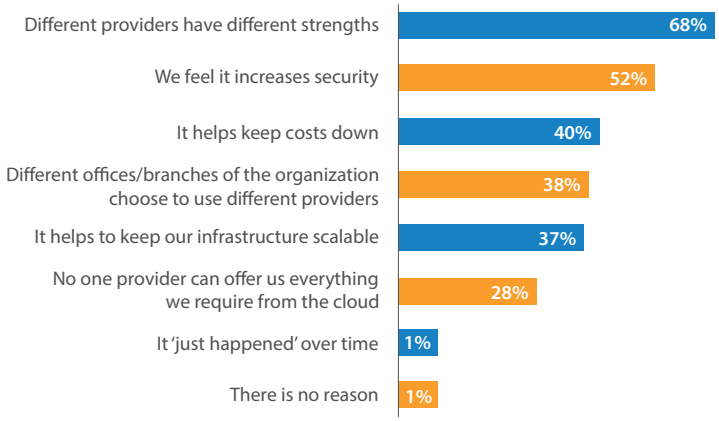
Percentage of organizations' infrastructure running in the public cloud



Organizations that have moved their infrastructure to the cloud continue to invest in cloud resources; in five years' time, their cloud footprints will nearly double. We also looked at different vertical segments across these respondents and found little discernible differences: Technology organizations were understandably a few points ahead of the average, but even public sector adopters have on average nearly 40% of their infrastructures already in public clouds.

Are they just using one cloud? The answer is surprising because, on average, organizations leverage three different cloud infrastructures within their overall IT infrastructure. When asked which is the most utilized, we found Azure leads the pack with 66%, AWS with 46%, and Google Cloud Platform with 36%. The reasons for using multiple cloud providers gave more insight into this:

Why do those organizations using more than one public cloud service provider, do so? Asked to those who use more than one (197)



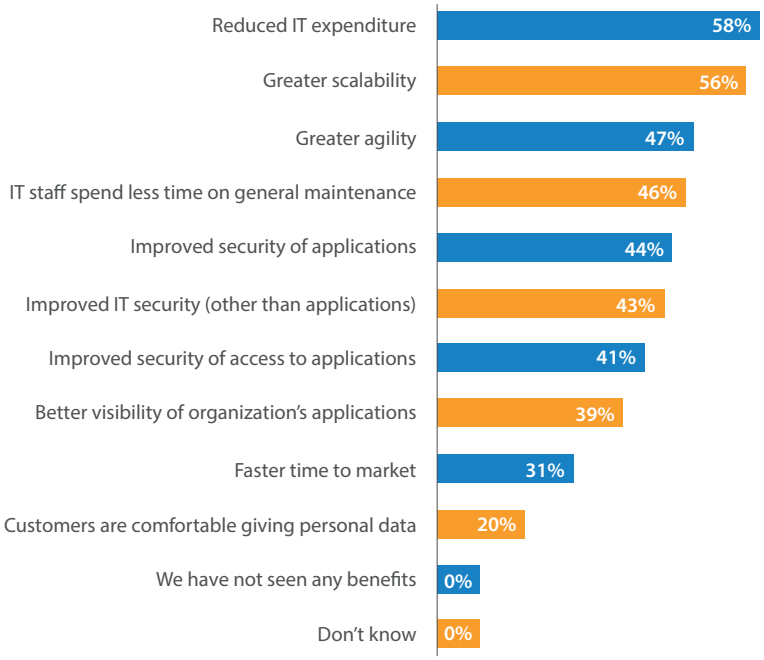
The majority of respondents believe that different providers have unique strengths, and are leveraging these cloud providers accordingly. Today, Azure is a dominant player in Info/Sec and IT data centers, whereas AWS has a more significant presence in Dev/Ops. Respondents also believe that leveraging multiple public cloud providers increases security.

However, continuing to use multiple providers will complicate the cloud landscape; further on, we discuss how companies are addressing security issues by mostly leveraging third-party solutions. With multiple infrastructures becoming commonplace, organizations will soon need to look at third parties that can operate inside multiple infrastructures—or their overall IT landscape complexity will grow dramatically, decreasing some of the cloud's most obvious benefits.

Benefits to Using Public Clouds

Virtually all organizations are gaining benefits from the cloud with 99% stating that they are seeing multiple benefits: The majority reported reduced IT expenditures and greater scalability. Greater agility, less time spent by IT on maintenance, and improved security (both for applications and for infrastructure) are essentially tied at around 45% of all respondents.

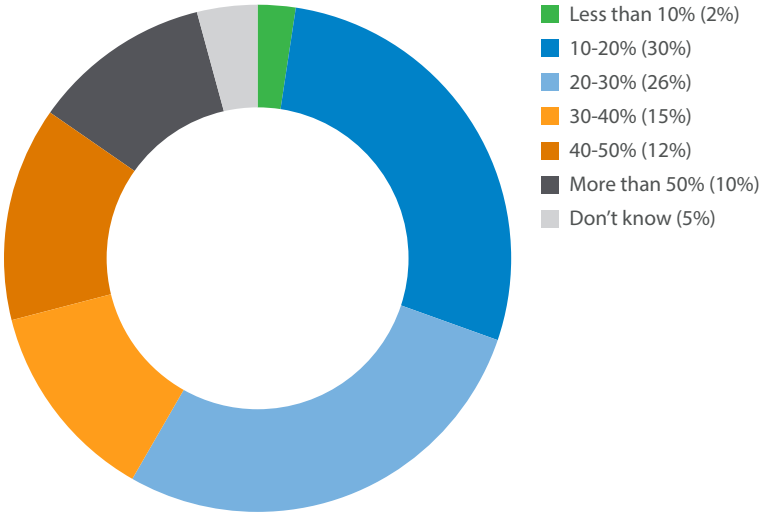
What benefits have organizations seen from using public cloud?



Respondents noted that better security underscores the fact that the cloud can be made even more secure than on-premises environments — but that protection is not automatic.
When asked about returns on cloud expenditures, the majority of companies experience a fairly rapid return on their investments in cloud infrastructure, including services and any third-party solutions added to their cloud infrastructures.

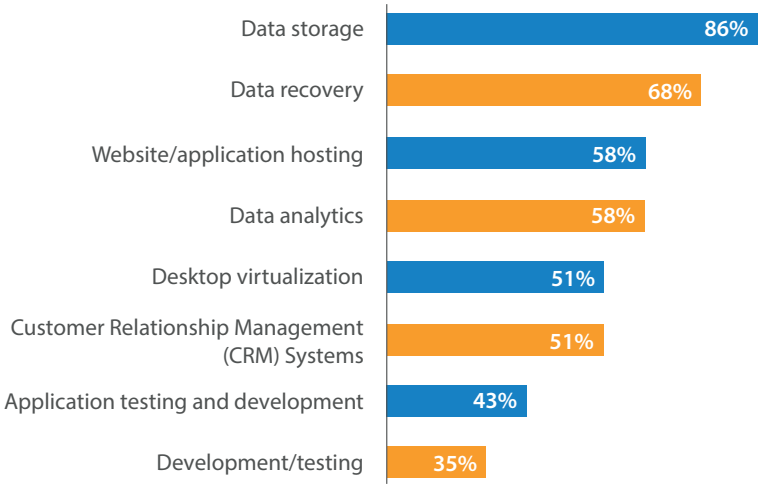
While some organizations saw 40-50% return on their investment, or even more than 50%, the majority of respondents experienced between 26% and 30% return within their first year of cloud deployments. The average ROI is 28.99%.

What positive ROI have organizations seen from using public cloud?



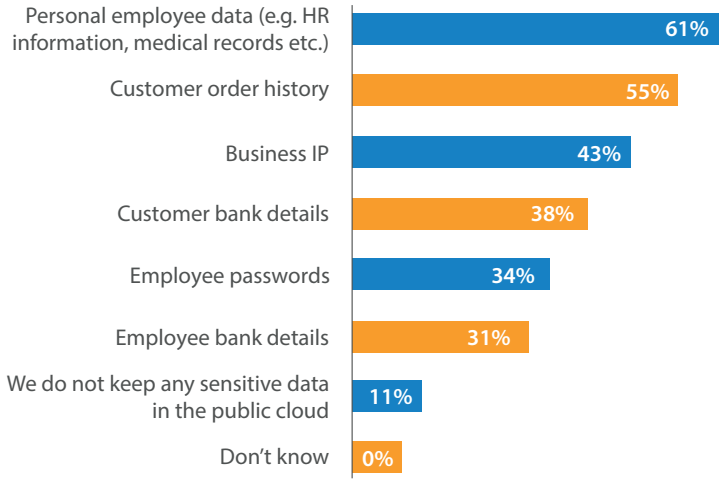
We also asked how organizations leverage clouds, and what kinds of data they put in public clouds. The responses illustrate that organizations are figuring out public clouds and are learning to navigate security and other concerns.

How do organizations leverage public cloud?



Organizations leverage public clouds for a variety of purposes: The top use is data storage and recovery, followed by website or application hosting. Some organizations use the cloud for data analytics, while others turn to it for desktop virtualization and relationship management systems. Over 40% use the cloud for application testing and development, and over a third for pure development and testing.

What type of sensitive data does your organization store in the public cloud? Asked to thos who use public cloud for data storage (257)



Organizations also store sensitive data in the cloud. While employee records and personnel data are among the top sensitive items being stored, organizations are storing business IP in public clouds. Bank details, both for customers and for employees, are included in the sensitive data being stored by organizations in the public cloud.

The responses about sensitive data illustrate a level of trust in cloud security, yet in some ways it's at odds with organizations' overall views on security and risks, which we'll examine next.

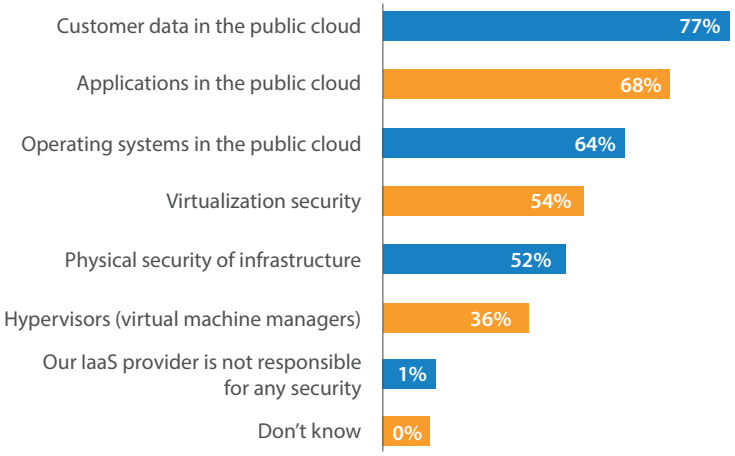
Security: Only Partly Understood

The Shared Security Model is standard across all cloud platforms. It states that while the cloud vendor will ensure the security of its infrastructure, organizations are responsible for the security surrounding what they put into the cloud. More than four in five (84%) respondents reported that they fully understand the public cloud security responsibilities of both their organization and IaaS provider, and an additional 15% cited that they partly understand public cloud responsibilities.

However, when asked what cloud vendors are responsible for securing, the responses clearly indicate that the Shared Security Model is not fully understood. More than 75% of respondents felt public cloud service providers are responsible for securing customer data in the cloud, and some 68% felt public cloud providers are responsible for securing applications running on their clouds.

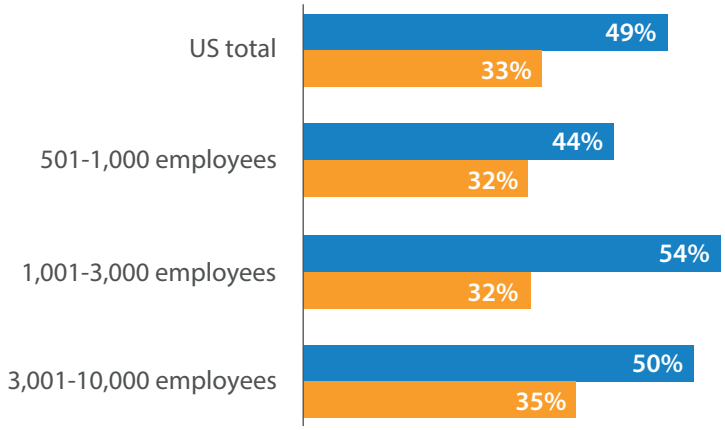
However, when asked more directly about security, around three quarters (74%) of those interviewed state that security concerns restrict their organization's migration to the public cloud. In addition, the vast majority (89%) of respondents believe that there are threats to their organization's public cloud infrastructure for securing applications in the public cloud.

What do organizations believe that public cloud service providers have a responsibility to secure? Asked to those who have an understanding of cloud security responsibilities (296)



Over nine in ten surveyed IT decision makers (92%) state that they have concerns over their organization's use of public cloud, with the most likely (58%) being the impact of cyberattacks. In addition, around a quarter of respondents report that they are concerned over the lack of an expert partner to work with for cloud security (26%), or have a lack of in-house skills to maintain the cloud (23%).

What benefits have organizations seen from using public cloud?

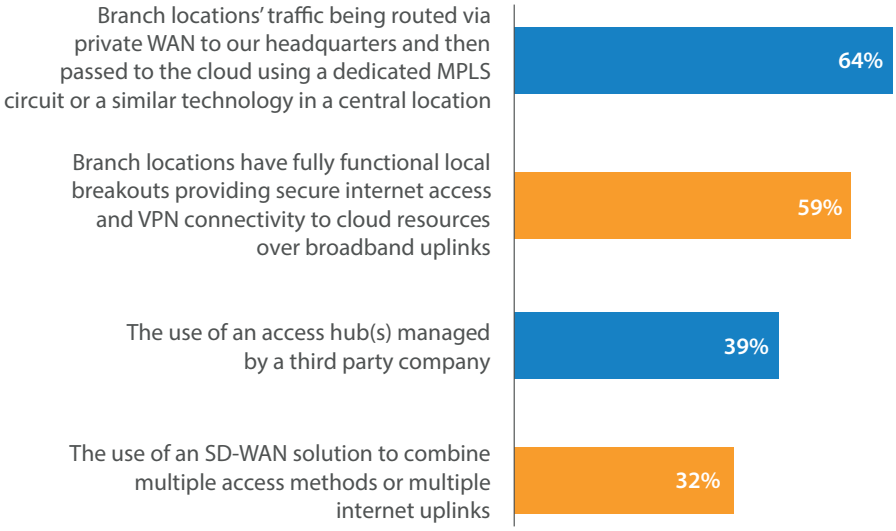


If organizations haven't been targeted yet by a cyberattack, a large majority feel such an attack is imminent. It doesn't matter whether organizations are large or small, the perceived risk is nearly identical. And while larger organizations tend to report already having been attacked, small organizations are also being attacked. Eighty-eight percent of the organizations who have suffered a cyberattack reported that the attack had measurable negative impacts on their operations. Loss of faith in the public cloud is the most consistent impact, but over 25% of impacted organizations faced either regulatory or compensatory fines as the result of a cyberattack.

Overcoming Security Challenges

It's very clear from the results of this survey that despite security concerns and the real threat of attacks, organizations continue to leverage the cloud and grow their cloud infrastructures. Two thirds (67%) of respondents say that their organizations have already added some additional security solutions to their public cloud to protect it during access. Additionally, 30% cite that they have not yet, but plan to do so in the future.

Which of the following security solutions have organizations added to their public cloud? Asked to those who have added additional security (200)

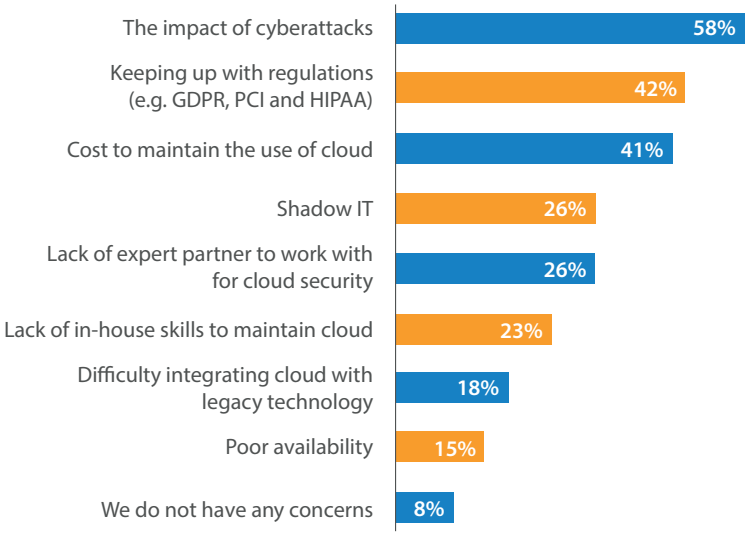


When we asked what organizations are doing, two strategies emerged. The most prevalent strategy involved routing traffic to and through a central firewall or other security measures, and then rerouting traffic back out. The second strategy is to provide branch locations with fully functional local breakouts using distributed firewalls or a similar security routine for all internet traffic and access.

Sixty-four percent of organizations that have added additional security solutions route their branch locations' traffic to headquarters, and then pass it to the cloud using a dedicated MPLS circuit in a central location. However, more than nine in ten (95%) respondents report that they see a need for additional security solutions to be added to their public cloud to protect it during access.

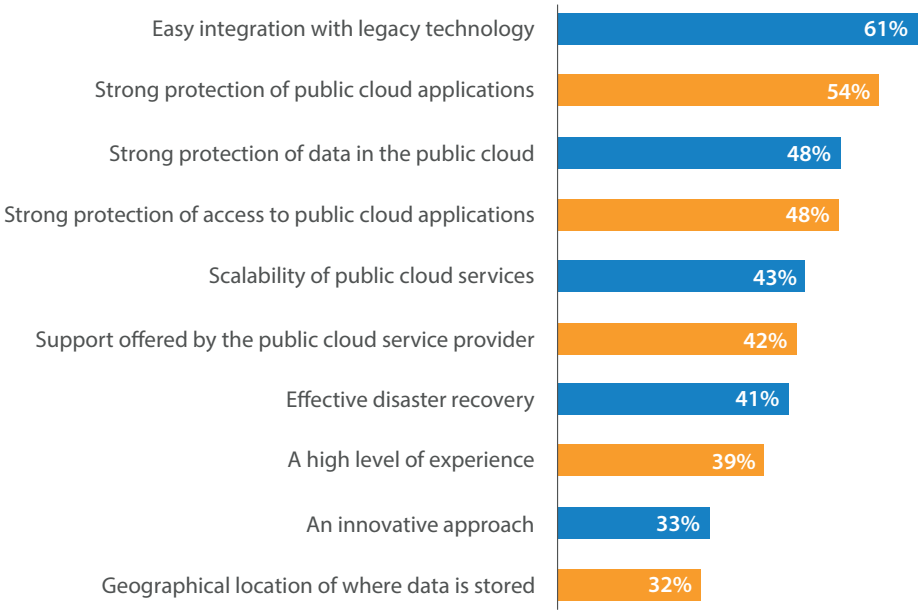
While organizations are investing in additional security to address perceived gaps in their cloud infrastructures, we found other concerns as well. Security dominates the discussion, but regulatory requirements and the cost to maintain cloud infrastructure were also raised as concerns. Over 25% of all organizations reported issues with either needing a shadow IT organization to shepherd their cloud infrastructure, or the lack of an expert partner to help bolster cloud security.

What are the concerns that organization have regarding the use of public cloud?



Conclusion

What are the ten most important drivers for choosing a public cloud service provider?



Despite the challenges, the overall benefits to leveraging cloud infrastructure is pushing organizations to accelerate their cloud adoptions. More than half of respondents report that easy integration with legacy technology (61%) and strong protection of applications in the public cloud (54%) are important drivers when choosing a public cloud IaaS provider to use in their organization, while around half (48%) said the same regarding strong protection of access to applications in the public cloud.

Scalability, support, and innovation are also reported as important drivers to cloud adoption. Organizations applauded the support they are offered from public cloud providers, and more and more are seeing the cloud as an effective means of disaster recovery.

For readers of this summary, a key takeaway is that security remains a key concern. The upside is that organizations can (and are) augmenting support with third-party providers. These solutions allow them to create infrastructures that are even more secure than those on-premises.

As cloud infrastructures evolve and organizations deploy more clouds, a corresponding challenge will be ensuring they have chosen third parties who provide cross-platform solutions and expertise. Additionally, it should not be forgotten that these organizations are coming from somewhere (i.e., on-premises infrastructures), and their chosen third parties need a strong understanding of hybrid deployments as well as pure cloud ones.

Protecting users, applications, and data for more than 150,000 organizations worldwide, Barracuda Networks has developed a global reputation as the go-to leader for powerful, easy-to-use, affordable IT solutions. The company's proven customer-centric business model focuses on delivering high value, subscription-based IT solutions for security and data protection. For additional information, please visit www.barracuda.com.

About Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide, and are delivered in appliance, virtual appliance, cloud, and hybrid configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com