

February 2020

Future shock: the cloud is the new network

Remove security barriers for
faster public cloud adoption

The digital transformation is underway. At the center of this profound change is the move to public cloud. But security concerns remain. This report delves into the impact of security roadblocks and how organizations can overcome them. »

Contents

- Introduction3
- Key findings4-5
- Perspective6-13
 - Public cloud: well established and integral to future success6
 - Firms are under attack, costing time and resources7
 - Security tops public cloud concerns8
 - Organizations are seeking third parties to help9
 - Secure connections to the cloud are important10
 - Web apps are often exposed11
 - Once the security roadblock is removed, growth can be unleashed12
 - Most would expect benefit from greater use of public cloud13
- Conclusion14
- About Barracuda15

Introduction

Across the globe, IT organizations are radically transforming how they deliver services to internal and external customers. At the center of this profound digital change is public cloud infrastructure — now seen as a prerequisite for innovation-driven growth. As a result, **Gartner predicts the market for public cloud services will grow at roughly three times the rate of the overall IT services market, topping \$331 billion by 2022.**

This is the engine room of the modern business, enabling companies to respond quickly to changing market demands and get closer to their customers with innovative applications and services — combining everything from AI and big data to cutting edge IoT systems. According to Oracle, by 2021 80% of all enterprise workloads will be in the cloud.

Yet security has been a perennial concern, even for those at the forefront of cloud adoption. We wanted to find out exactly how big an impact security roadblocks are having on investments, and ultimately on the value firms can derive from cloud deployments. This report covers not only the current threat landscape and challenges facing global organizations, but also where firms are looking for help to address their problems. In addition, we've been able to compare some of the findings to a similar study completed in 2017, to add useful historical context.

We found that while adoption rates for public cloud continue to grow, security continues to be a number one roadblock — understandable considering the volume and variety of threats organizations must face today. Many are choosing third-party security solutions as a result, claiming that if such efforts are successful, they could unlock tremendous business benefits.

Methodology

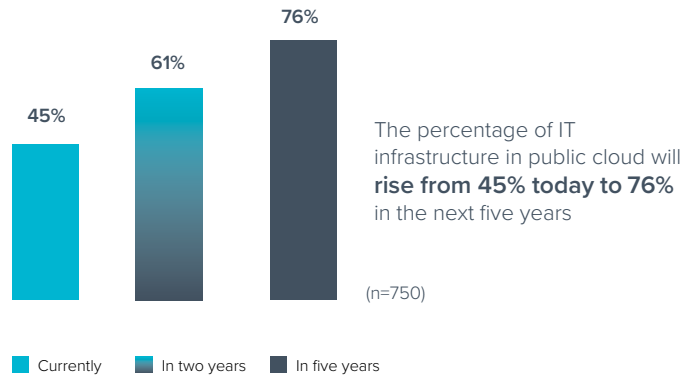
We commissioned independent market researcher Vanson Bourne to interview **750 IT decision makers** with responsibility for or knowledge of their organizations' cloud infrastructure. They came from organizations of all sizes and across a broad range of sectors, in **EMEA, APAC and the US.**

Key findings

FINDING #1

Organizations are moving infrastructure to public cloud.

Our findings make it clear that public cloud deployments are a key part of many organizations' IT strategies, and they will become even more important over the next five years. The average percentage of IT infrastructure running in the cloud stands at 45% today, rising to an estimated 76% in five years. Interestingly, in 2017 our survey respondents expected an even faster rate of growth in public cloud, predicting that by now 55% of their infrastructure would be in the public cloud, as opposed to the 45% as indicated in this survey.



FINDING #2

Security is the top concern restricting faster adoption of public cloud.

Our survey clearly indicates that the most important inhibitor to faster public cloud growth is security, with **70% of respondents saying that security concerns restrict their organizations' adoption of public cloud.** These security concerns include the security of public cloud infrastructure, the impact of cyber-attacks and the security of applications deployed in public cloud. It is not surprising that security concerns are top of mind with respondents, as **75% have already been targeted by a cyber-attack.**



Key findings

FINDING #3

Network integration is a major concern.

The second major set of concerns about public cloud adoption has to do with integration, **including integrating public cloud with legacy technologies, better integration with private cloud and enhanced integration with on-premises infrastructure.** A key factor here is the underlying network. For the public cloud to reach its full potential, the network needs to be seamlessly integrated into the cloud, including connections to branch and private cloud locations.



41% want better integration
between public and private cloud

FINDING #4

A fully integrated, secure SD-WAN is the solution of choice.

Software Defined Wide Area Network (SD-WAN) appears to be the technology of choice for organizations keen to achieve a securely integrated network for their cloud deployments. **While only 23% of the respondents have already deployed SD-WAN, another 51% are either in the process of deploying or expect to deploy within the next 12 months.** Respondents are looking to SD-WAN solutions to resolve not only network issues but also security concerns, as SD-WAN is being used by more than half of those who have added security to their public cloud. Respondents realize that cloud provider native security solutions may not provide sufficient capabilities and are looking for third-party providers to help them overcome adoption barriers.



SD-WAN is in use by half
of those with public cloud security

PERSPECTIVE

Public cloud: well established and integral to future success.

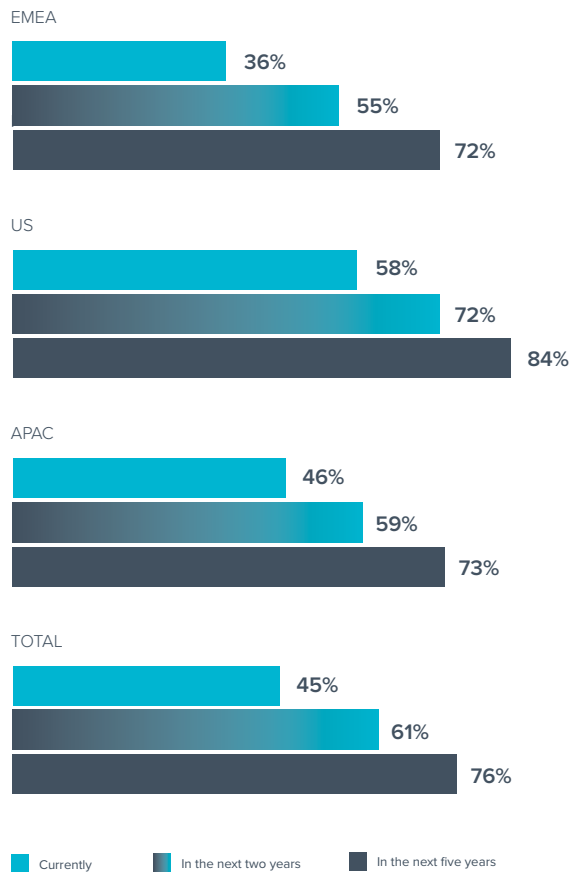
Public cloud deployments are a key part of many organizations' IT strategies, and they will become even more important over the coming five years. The average percentage of IT infrastructure running in the cloud stands at 45% today, rising to an estimated 76% in five years and even higher (84%) in the US. EMEA is further behind at just 36% today, but will reach around the same percentage as APAC in five years (72%).

Among the main uses of the cloud among global organizations today are data storage (81%), analytics (63%) and website/application hosting (61%). US companies are again leading the way in how they use the cloud, followed by those in APAC.

However, while there is more IT infrastructure running in the cloud today than there was three years ago (45% vs. 39%), there's not as much as respondents back then assumed there would be by 2019 (55%). It could be that security concerns have started to intensify over the intervening period, constraining investments and cloud growth.

What percentage of your organizations' infrastructure is running in the public cloud?

(n=750)



PERSPECTIVE

Firms are under attack, costing time and resources.

While organizations are investing heavily in public cloud infrastructure as a key IT and business enabler, this is happening against a backdrop of escalating cyber-threats.

Three-quarters of global respondents said their organization has been hit by an attack at least once, up from 56% in 2017.

Not only does this raise the prospect of data breaches and service outages, which can cause serious financial and reputational damage, but keeping hackers at bay is a constant drain on resources. On average, six hours per week are spent by staff managing and preventing security breaches, **and for nearly a third (29%) of organizations, security staff spend an entire day or more per week on such tasks.** This rises to 38% in APAC.



PERSPECTIVE

Security tops public cloud concerns.

Perhaps unsurprisingly given the scale of threats facing global firms, security issues top the list of IT leaders' concerns about their use of public cloud. Security of public cloud infrastructure (42%) comes first, followed by the impact of cyber-attacks (36%) and security of public cloud apps (33%). It's important to remember, however, that security is not the only public cloud challenge facing IT teams: integration with legacy tech (28%), regulatory compliance (28%), costs (24%), shadow IT (21%), and lack of in-house skills (19%) also loom large. A fifth (13%) of IT leaders say they are lacking an expert security partner to help them with public cloud deployments.

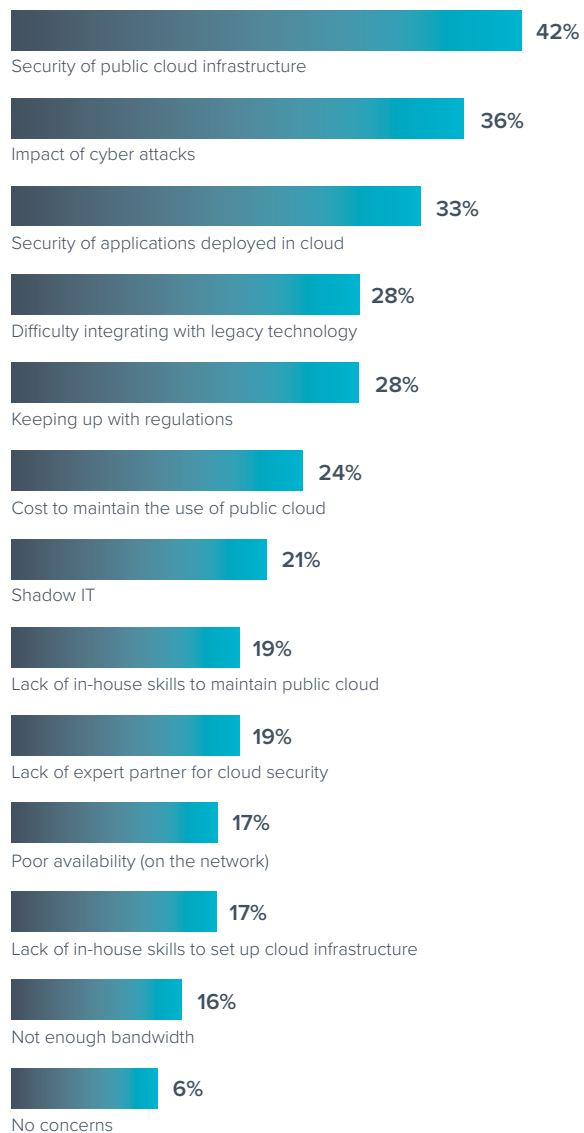
The top threats they see to public cloud infrastructure cover a broad sweep, from sophisticated hackers (45%) and application vulnerabilities (40%) to phishing (38%) and exposed corporate networks (37%). Organizations clearly need security partners that can address such concerns with industry leading, multi-layered product sets.

Not only is security a number one current public cloud concern, but it's also the main factor preventing greater adoption (51%), way more than costs (38%) and compliance (28%) in second and third place.

This is not a recent development. The same number of respondents (70%) in 2017 and 2020 claimed they are heavily or partly restricting public cloud adoption due to security concerns.

What are your top concerns for using a public cloud infrastructure?

(n=750)

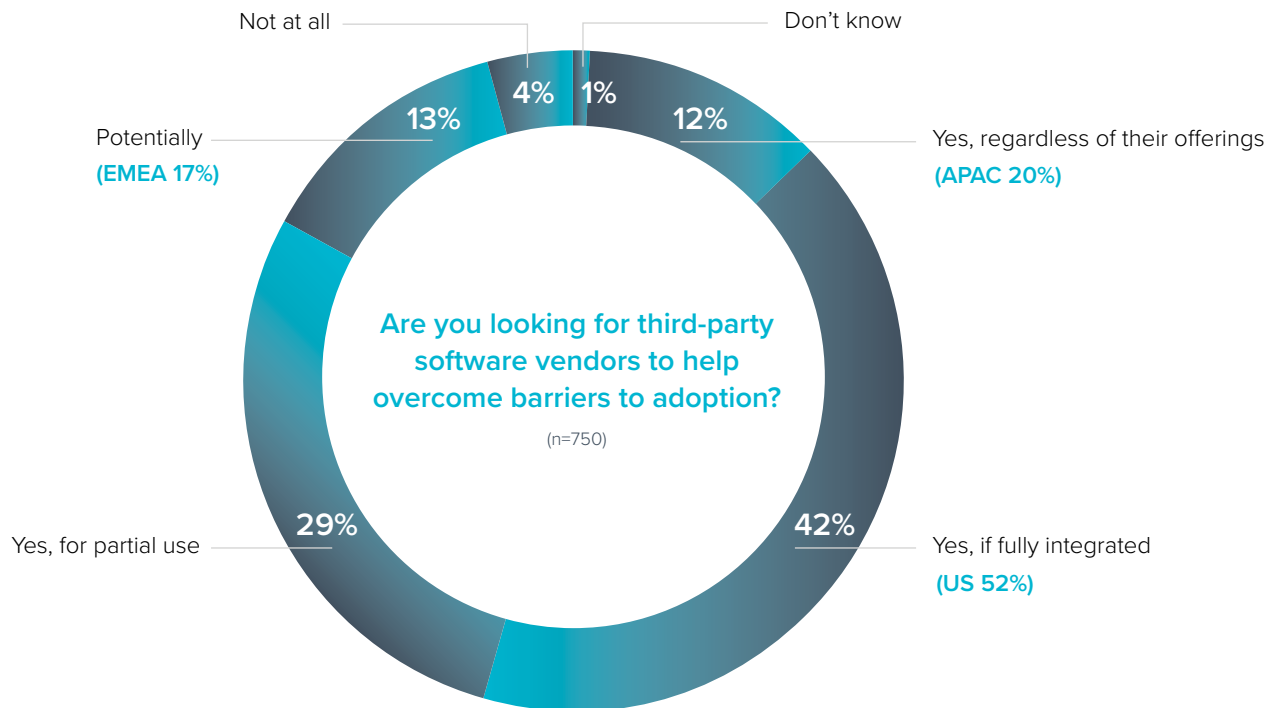


PERSPECTIVE

Organizations are seeking out third parties to help.

Although factors like improved staff training and regulatory guidance are important, **more secure cloud solutions (55%) and responsive threat detection (41%) are the elements which respondents believe would do most to address cloud adoption barriers.** This is especially true in APAC, where 62% cited more secure solutions.

95% of global respondents said they are looking to third-party providers to help them overcome adoption barriers. However, a sizeable minority (42%) will only do so if these providers offer full integration, highlighting the need for security providers to ensure their products fit seamlessly into the major cloud platforms.



PERSPECTIVE

Secure connections to the cloud are important.

Securing cloud networks and applications from external attacks must be a crucial part of any organizations' cyber-risk management strategy, as must protections to guard against insider human error and misconfiguration. But our research proved that connections to the public cloud are also a key consideration.

SD-WAN connections offer organizations the ability to manage security policies and bandwidth at the push of a button from a centralized location. This virtualized solution also adds network monitoring and traffic prioritization, and because it routes traffic over the internet, is cheaper than legacy MPLS. That's why **56% of global organizations have deployed or are in the process of deploying SD-WAN and a further 18% will do so in the next 12 months.**

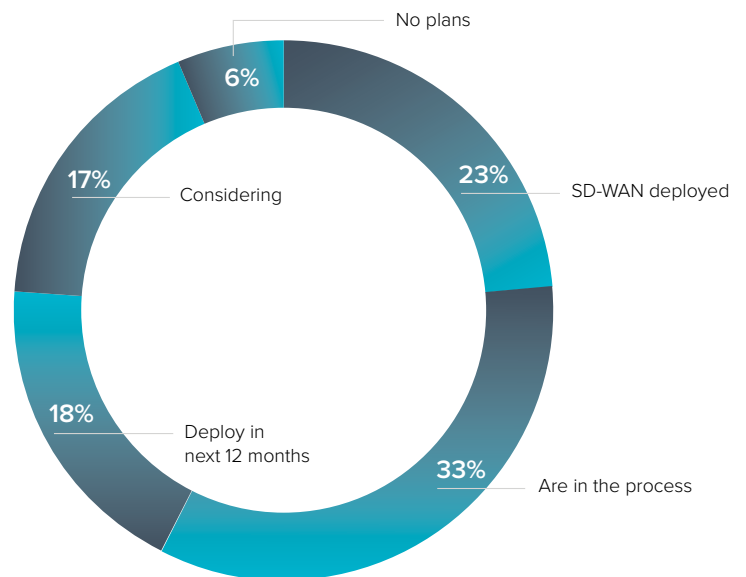
However, it also appears as if organizations are achieving less with SD-WAN than a couple of years ago, in areas such as network flexibility, connectivity and security. It could be that a lack of in-house resources and skills is hampering projects, or perhaps that IT buyers have chosen the wrong solutions. There are various models via which firms can deploy SD-WAN, but some add unnecessary extra cost and complexity, and may not offer the best possible threat protection.

Most respondents to our survey (52%) said their preference was to acquire SD-WAN via a cloud provider. The reason, it seems, is a perception that this is the easiest method via which to adopt the technology (45%). Yet this could be down to a lack of awareness of the full range of options available on the market. In fact, unified, easy-to-deploy solutions from proven cybersecurity vendors may provide a better alternative.

A single solution combining advanced security and SD-WAN in one appliance at each gateway edge works best for those that want enhanced application performance, network flexibility and agility combined with industry leading security.

Are you planning to deploy SD-WAN?

(n=750)



PERSPECTIVE

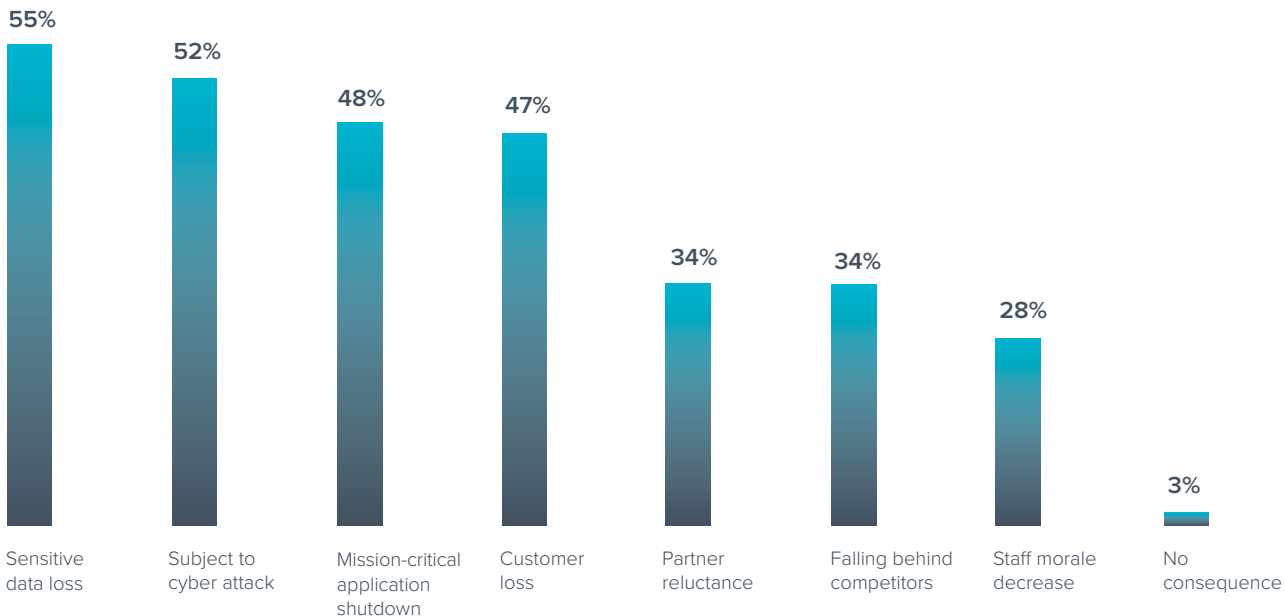
Web apps are often exposed.

Another crucial area of the public cloud that requires scrutiny is the security of web applications. Although they're a business-critical tool for delivering optimized experiences to customers and enhancing employee productivity, they're also prone to containing serious vulnerabilities and can be a leading cause of data breaches.

Respondents to our survey acknowledge this: they admit that the consequences of poor app security range **from critical**

What would you expect the consequence to be for organizations with poor application quality?

(n=750)



data theft (55%) and successful cyber-attacks (52%) to application shutdowns (48%) and lost customers (47%).

Most also agree that they need protection for apps that can be accessed by external users, as well as those that involve commerce or PII, or can be accessed via mobile devices.

Yet over a third (35%) of global IT leaders admit that their web applications are not fully protected, rising to 42% in EMEA. Why aren't they doing more? Perhaps they haven't been able to find the right security partners, especially if they're looking to public cloud platforms to offer protection.

It could also be a result of the fact that, although decisions surrounding public cloud solutions tend now to be made high up within IT — **at IT director (48%) and CIO (27%) level** — **just 2% of respondents said CISOs are the primary decision maker.**

PERSPECTIVE

Once the security roadblock is removed, growth can be unleashed.

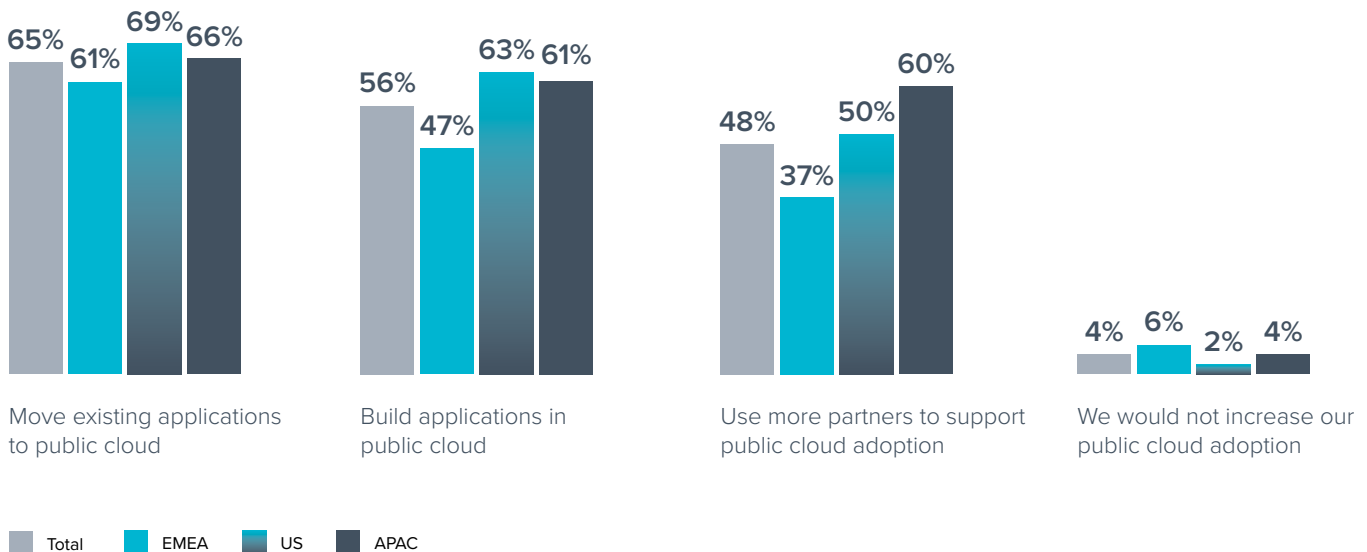
The value that organizations could generate increases once they remove the traditional blockers to public cloud adoption. An overwhelming number of respondents said they would **move more applications to the cloud (65%), build more applications in the cloud (56%) and use more partners to support cloud adoption (48%, rising to 60% in APAC).**

What's more, almost all expect to see benefits from greater use of the public cloud. **These are led by reduced IT expenditure (42%) and greater scalability (41%), but also include improved security (40%), greater agility (39%), and IT staff being able to focus on higher value tasks (38%).**

Given that security concerns were cited by over half of respondents as a barrier to cloud adoption, more than any other factor, it's clear that addressing such challenges is absolutely critical if organizations want to drive business success in the future.

How would you increase public cloud use if barriers to adoption were removed?

(n=696)



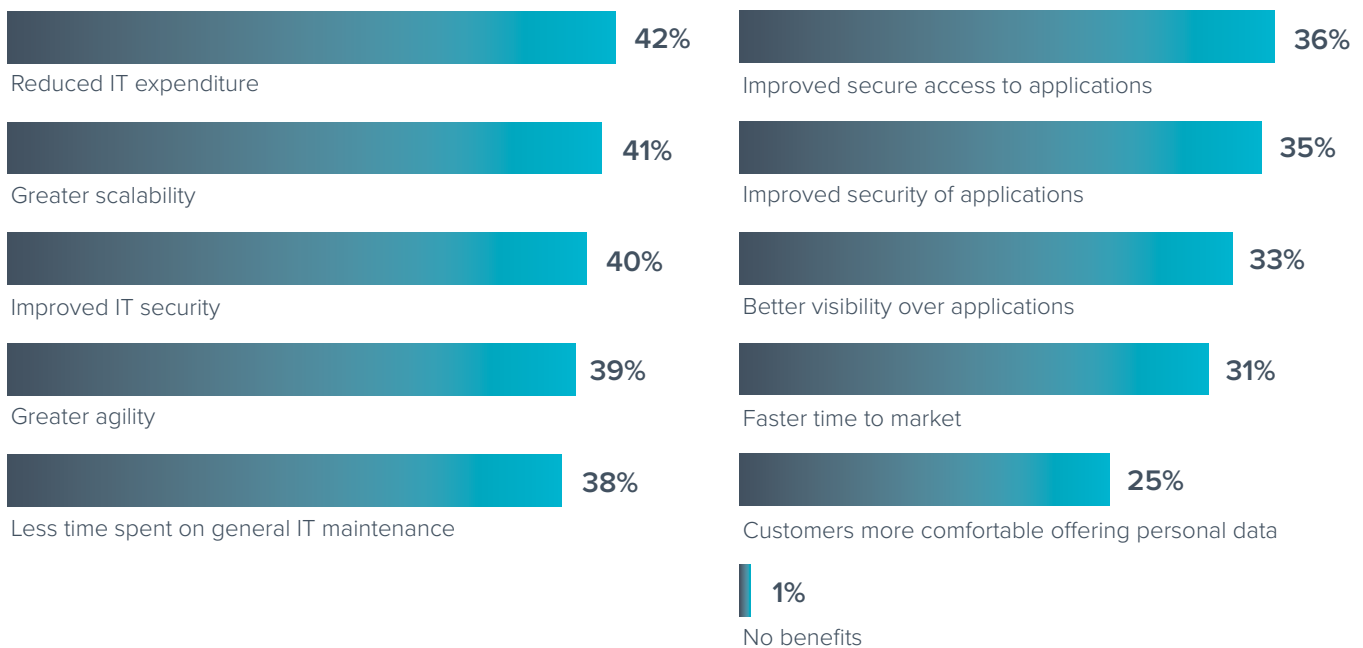
PERSPECTIVE

Most would expect benefit from greater use of public cloud.

Seeing these benefits would strengthen any organization and justifies the investment that could be required to ramp up public cloud adoption. Exploring the ability to reduce IT expenditure, increasing agility and visibility of applications is enough reason for the most senior members of an organization to take this prospect seriously.

What additional benefits would your organization expect to see if it made greater use of public cloud?

(n=750)



Conclusion

Public cloud deployments are a key part of most global organizations' IT strategies and will become even more central to their future success. As more IT infrastructure moves to public cloud, providers will offer more native network capabilities, and public cloud will expand to include more network functionality. Customers will benefit from the seamless integration of cloud native network services with cloud infrastructure, making cloud the backbone of modern distributed enterprise.

But cyber-attacks are a constant threat, costing organizations time and money to mitigate on a weekly basis.

These organizations are in no doubt what is the number one concern for current cloud deployments and the biggest roadblock to future investments: cybersecurity. We've observed this trend for several years, with most firms heavily or partly restricting public cloud adoption on such concerns since at least 2017. The vast majority of organizations are looking to third-party security vendors to help them tackle these challenges, but there are caveats.

They need their security vendors to offer advanced security and cloud connectivity tightly integrated with the major cloud platforms. They're also demanding simplicity and expertise from SD-WAN providers, to offer secure, easy-to-deploy, agile solutions. And many admit that they need particular help securing the web applications that often represent a major weakness in the IT infrastructure.

Further still, many organizations cite skills and regulatory compliance as major barriers to cloud adoption. That means they're looking not only for protection from external hacking threats, but also compliance orchestration and

posture management to tackle human error like cloud misconfigurations. Security vendors that can offer a complete package of cloud-generation firewalls, web application firewalls, SD-WAN deployments and automated security policy compliance will find themselves in strong demand.

Those organizations able to find a trusted security partner to deliver these capabilities and overcome their challenges will be in the fast lane to business growth and digital transformation success.

Organizations able to find a trusted security partner will be in the fast lane to business growth and digital transformation success.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-enabled, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them—in ways they may not even know they are at risk—so they can focus on taking their business to the next level.

Get more information at barracuda.com.

