Barracuda

Steps to Secure Your Journey to the Public Cloud: Challenges, Misconceptions and Opportunities of Shared Responsibility

White Paper

Introduction

Organisations all over EMEA are waking up to the transformative possibilities offered by public cloud computing deployments. The drive for greater IT efficiency, business agility, and productivity has become an increasingly urgent one—especially since those businesses that tap the cloud effectively begin to pull ahead of their rivals. Yet, anecdotal evidence and quantitative surveys tell us that security is still a major barrier to greater cloud adoption.

From the WannaCry ransomware epidemic, to revelations of catastrophic data breaches at Yahoo, to the devastating cyberattacks against the Democratic National Committee, the past year has been a cautionary tale for IT security bosses everywhere. These incidents (and many like it) remind us of the scale and breadth of online threats facing organisations, whatever their size or sector.

That's why Barracuda Networks decided to find out more, with this in-depth look at the state of the public cloud across EMEA – how extensively it's used, for what purposes, and where the key security challenges lie.

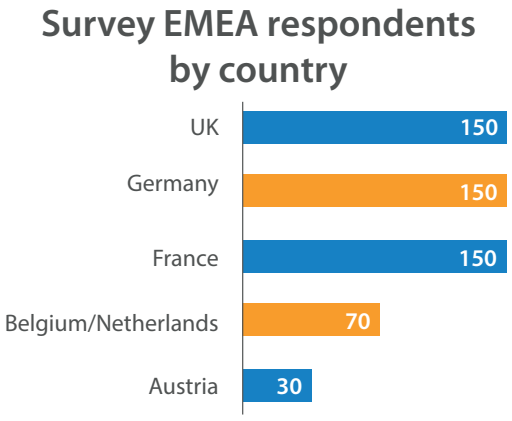
We found that interest in the public cloud continues to grow, with 20% of responding organisations' annual IT budgets currently being spent on cloud deployments. They're using services provided by several vendors and for a variety of reasons, including the storage of sensitive data. However, with 60% of firms having already been hit by a cyberattack and an additional 26% expecting one in the future, security concerns understandably loom large. Less than half (45%) of respondents believe that their public cloud IaaS provider completely offers strong protection when it comes to accessing cloud applications.

As the report reveals, there's a concerning lack of understanding of the Shared Responsibility Model, a key requirement of most IaaS providers, which states that cloud customers must provide much of the security themselves. This needs to change if organisations are to create the secure foundation on which public cloud success and business growth must be based.

The bottom line is that organisations are continuing to invest in public cloud projects, but they need a trusted vendor-neutral partner to help them navigate the choppy waters of cybersecurity if they want to minimise risk in the process. With sweeping new European data protection regulations landing in May 2018, no organisation can afford to ignore security today.

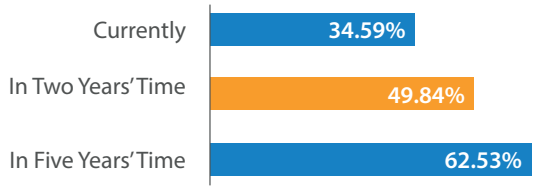
Demographics

Barracuda Networks commissioned Vanson Bourne to interview 550 IT decision makers from organisations across EMEA using a public cloud Infrastructure as a Service (IaaS). The study is part of a global report that analysed the results of 1,300 interviews with IT leaders worldwide. The demographic breakdown can be seen below.



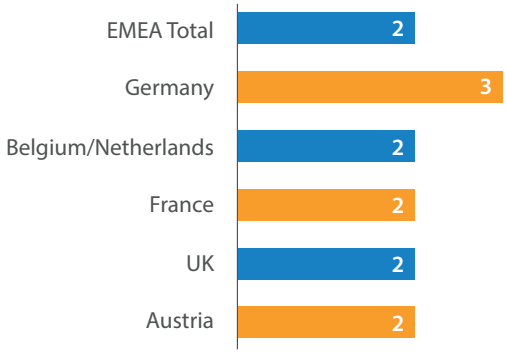
Public Cloud Adoption Continues to Soar

Percentage of organisations' infrastructure running in the public cloud



What is clear from the outset is that organisations across EMEA are investing heavily in public cloud projects. Respondents claimed nearly 35% of their infrastructure is currently in the public cloud, and predicted this will rise to half in two years' time and then to more than three-fifths (62%) in five years. Those in the UK currently have the lowest proportion of their IT in the cloud (29%) while those in Belgium and the Netherlands are most enthusiastic (41%)

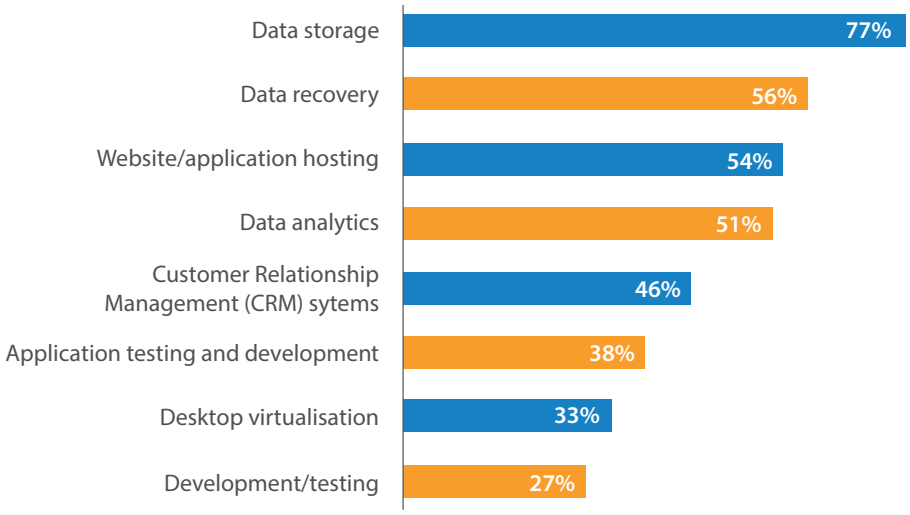
Average number of public cloud service providers respondents' organisations are currently using, split by respondent country



The average number of cloud providers used across the region is two (rising to three in Germany). Why are firms seeking to invest in multiple public cloud platforms? A combination of factors, but mainly because they think different players have different strengths (55%), and that it will increase security (44%) and help keep costs down (40%).

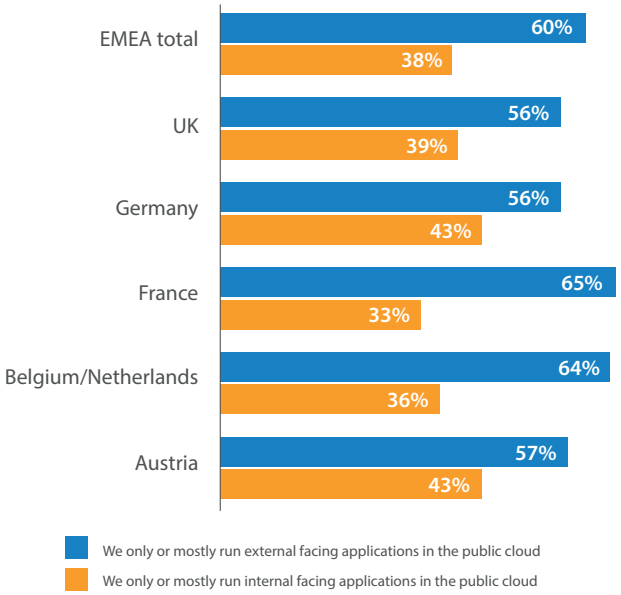
Given that organisations even in five years' time will be running hybrid environments delivered by multiple providers, it becomes increasingly important for them to partner with vendor agnostic third-party security and other players in order to extract the maximum value from projects.

How do organisations leverage public cloud?



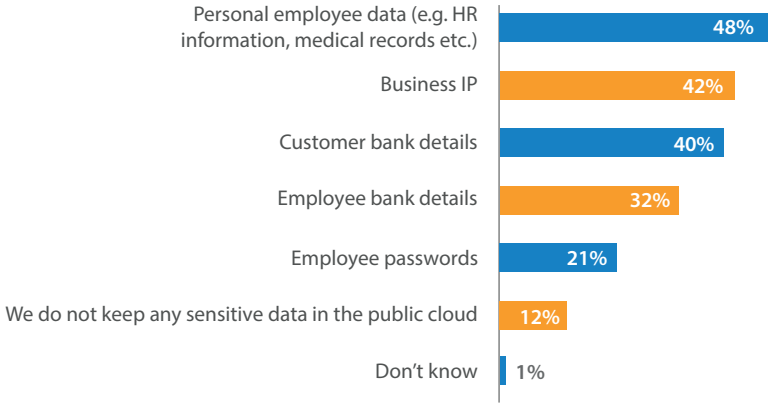
What are most organisations using the cloud for? A variety of purposes, but most popular is data storage (77%) and data recovery (56%), followed by web and app hosting (54%), data analytics (51%), and CRM systems (46%).

Do organisations use public cloud for internal-facing or external-facing applications? Split by respondent country



Three in five organisations said they mainly run external applications in the public cloud, although a sizeable minority (38%) across EMEA said they ran internal-facing apps. Respondents in France were the most likely (65%) to run external applications in the public cloud, while those in Germany (43%) and Austria (43%) were most likely to use it for internal apps.

What type of sensitive data does your organisation store in the public cloud? Asked to those who use public cloud for data storage (425)

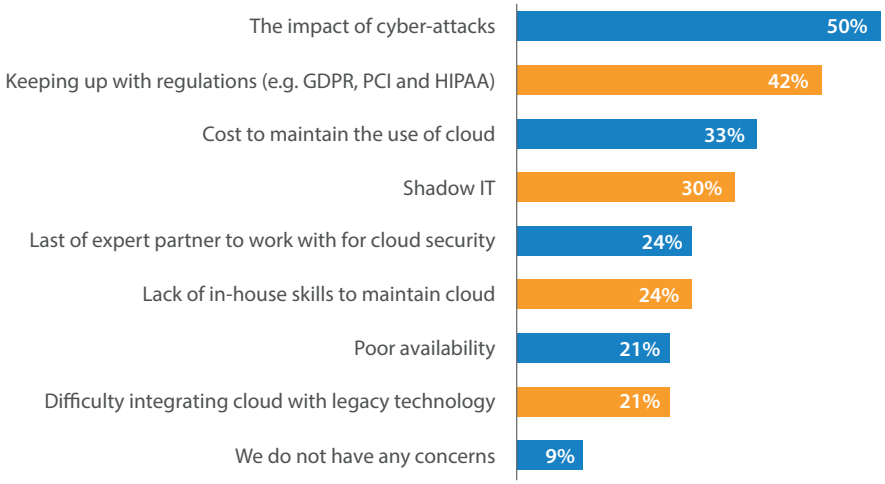


The question is, are these apps potentially exposing sensitive data? Organisations are certainly storing sensitive data in the public cloud, such as employee information (48%), business IP (42%) and customer bank details (40%). Austrian organisations were most likely to store customer bank data in the public cloud (61%) with UK respondents being the most risk averse (33%).

The upcoming EU General Data Protection Regulation (GDPR) will raise the stakes when it comes to securing sensitive customer data when it finally comes into force on 25 May 2018. Apart from mandating 72-hour breach disclosures, it will levy fines of up to 4% of global annual turnover, or €20m (whichever is higher) for serious infractions. This makes it clear that the need to ensure cloud data is properly protected is crucial.

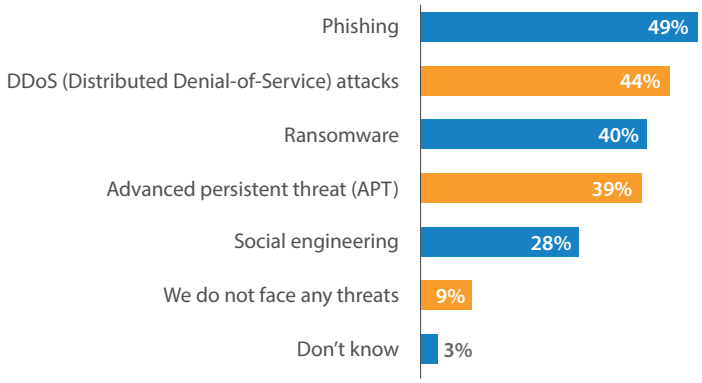
Security: A Shared Responsibility

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



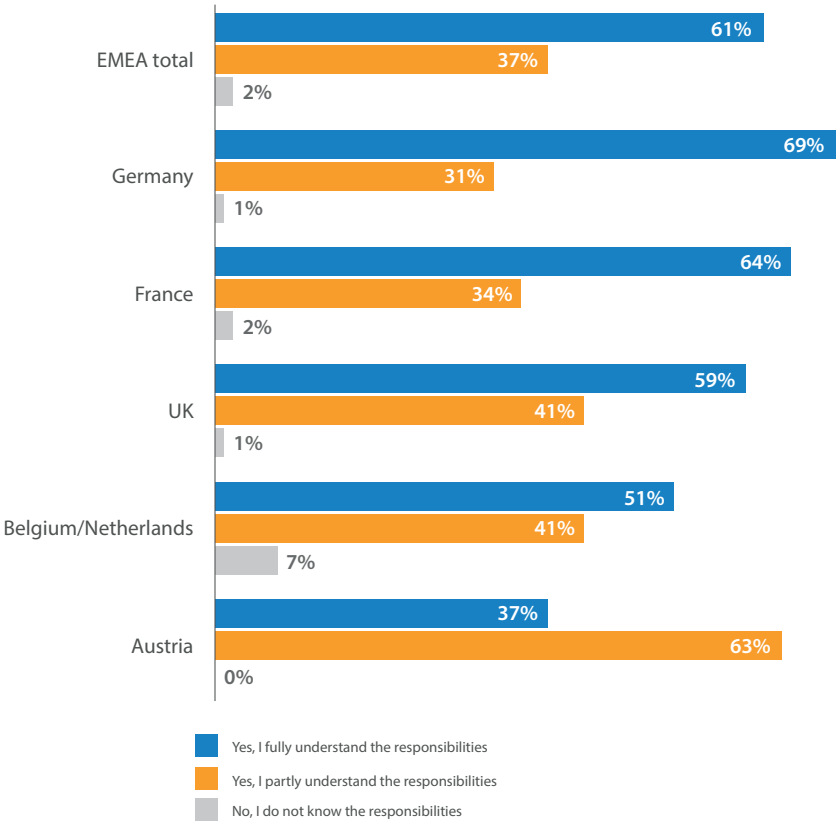
EMEA IT leaders are worried about the security implications of using the public cloud. In fact, "the impact of cyberattacks" came out as their top cloud concern (50%). That's perhaps unsurprising given that 60% said they've already been hit by a cyberattack, while 26% believe it will happen in the future. Organisations in Austria (73%) and Belgium/Netherlands (70%) have been hit the most, with those in France (55%) the least targeted.

What are the threats to organisations' public cloud infrastructure?



IT leaders seem to be most concerned about the threats posed by phishing (49%), DDoS (44%), ransomware (40%), and APTs (39%). This highlights just how broad a sweep of potential threats organisations need to protect against when considering public cloud security. A comprehensive defence-in-depth approach would seem the best way to mitigate cyber-related risk in this area.

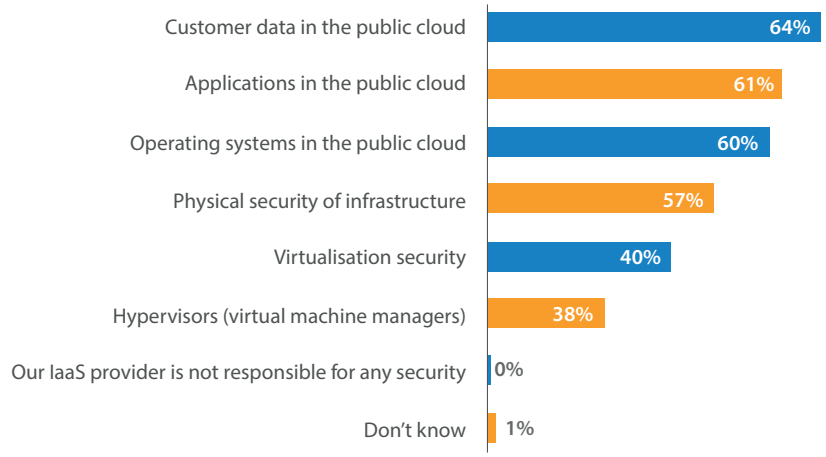
Do organisations understand who owns security responsibilities in the cloud? Split by respondent country



A key challenge remains: The cloud's Shared Responsibility Model. Most major providers espouse this model, where broadly speaking, they secure basic infrastructure components like compute, storage, database and networking, as well as the physical site. However, it is the customer's obligation to secure their data, apps, OS and other software elements running in the cloud. AWS has a clear explanation of its model here, while Microsoft's is here and Google's here.

Unfortunately, however, our research revealed a disconnect between the requirements of the major IaaS cloud providers and IT leader understanding. Just 61% across EMEA claimed to fully understand their responsibilities in this area – a figure rising to 69% in Germany and dropping to 51% in Belgium/Netherlands.

What do organisations believe public cloud service providers are responsible to secure?



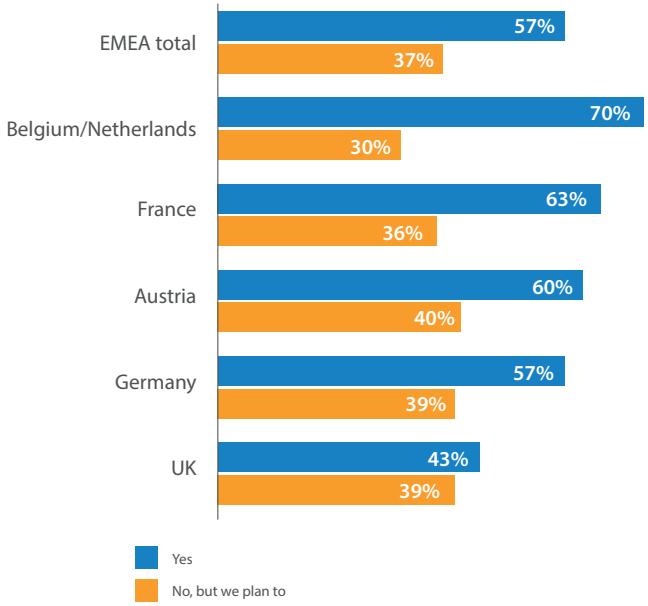
However, even this figure may overestimate the level of comprehension of shared security. Some 64% claimed it is the cloud provider's responsibility to secure data in the cloud, while 61% said the same about applications and 60% about operating systems. There's a dangerous gap between perception and reality here that could be leaving countless organisations across the region exposed to online threats. The lack of clarity regarding organisations' versus IaaS providers' cloud security responsibilities creates grey areas that IT decision makers must address if they want to keep key data and systems secure.

Given these challenges, it makes sense to partner with a vendor agnostic security expert to advise on exactly which pieces of the IaaS puzzle is the customer's responsibility. In fact, on that list of top public cloud concerns, a quarter (24%) of EMEA IT leaders claimed they were worried that they lacked such a trusted partner to help secure their infrastructure.

Overcoming Security Challenges

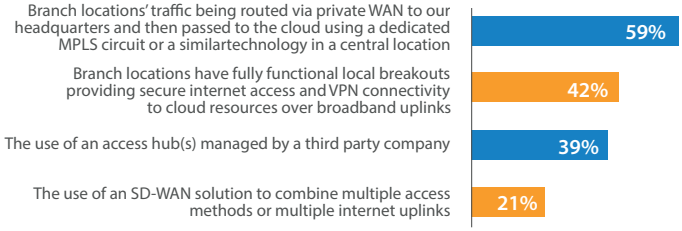
The report has shown us that EMEA organisations are storing sensitive information in the public cloud and are concerned about ongoing security, but have limited understanding of their responsibilities. This begs the question: What are IT leaders doing right now to mitigate cyber risk in the cloud?

Has your organisation added additional security solutions to its public cloud?



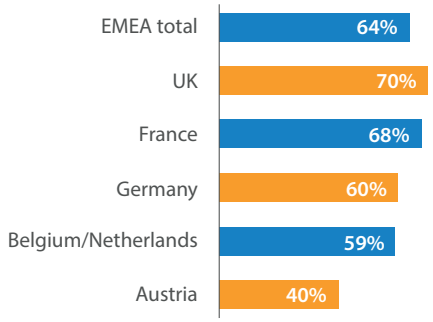
Over half (57%) of respondents claimed they've invested in additional security products to protect access to the public cloud, while a further third (37%) said they plan to in the future. Those in Belgium/Netherlands were most likely to have added security (70%), while UK organisations were least likely (43%).

Which of the following security solutions have organisations added to their public cloud?



A majority of organisations (59%) said they'd taken the initial step of routing all traffic through a centralised firewall, but a growing number (42%) said they were distributing security solutions across their infrastructure – and over a third (39%) were using a third-party provider to manage security.

Percentage of organisations where security has precluded their ability to migrate to public cloud, split by respondent country



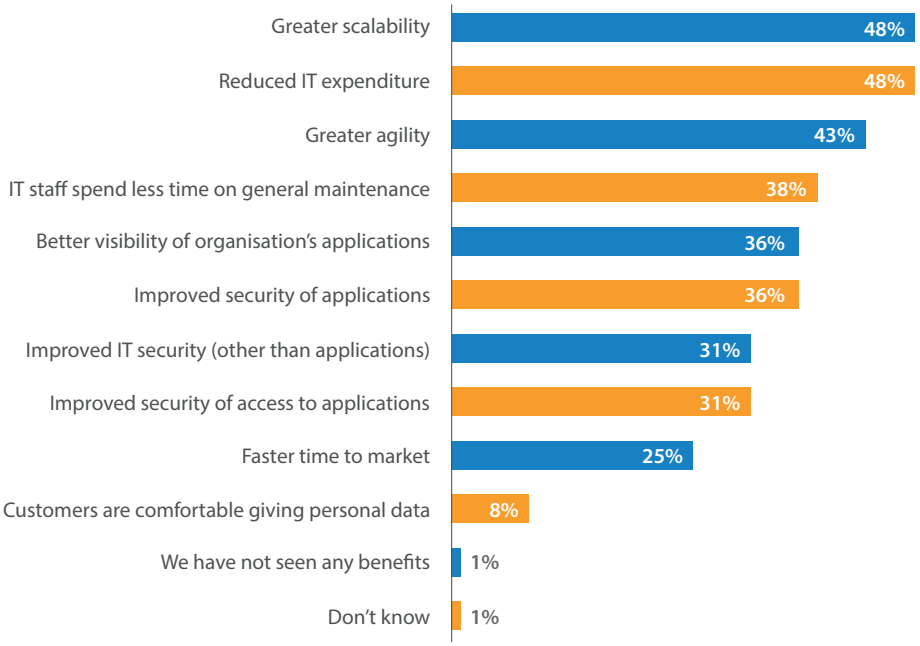
Unfortunately, despite extra investments in cybersecurity, concerns over threats to public IaaS clouds have actively restricted migration efforts for 64% of EMEA organisations. In the

UK, the figure is the highest in the region, with 70% claiming they've pulled back from public cloud projects because of security concerns, while respondents in Austria (40%) appear to be the least concerned.

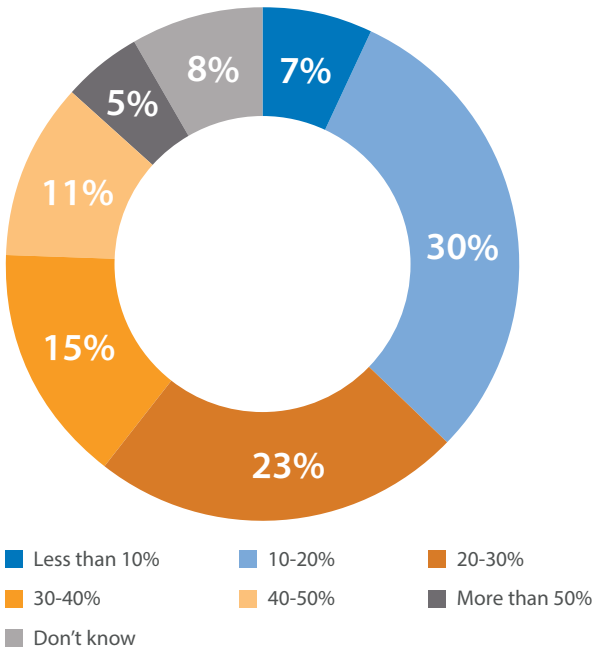
Conclusion

Despite the numerous challenges and the concerns of EMEA IT decision makers highlighted in this survey, the public cloud remains a hugely attractive prospect for many.

What benefits have organisations seen from using public cloud?



What positive ROI have organisations seen from using public cloud?



Nearly all (99%) respondents claimed their organisation has seen benefits as a result of moving to the public cloud, with just over half flagging greater scalability (48%) and reduced IT expenditure (48%) as major plusses, while 43% mentioned greater agility. On average, 26% of respondents reported a positive ROI by moving to the public cloud—this illustrates just why the cloud has become so popular.

Yet, with onerous EU compliance obligations coming next May, security needs to remain front of mind. EMEA IT leaders know this, and are investing in additional security to help protect their cloud deployments. But many are still confused over exactly what their responsibilities are when it comes to cloud security, and would benefit from the advice of a trusted third-party expert.

Become "Cloud Ready"

As a leading cloud security provider, Barracuda has already addressed many of the challenges and concerns that organisations raised in this survey. We have sought to address growing hybrid infrastructures by providing products that operate in similar fashion whether on-premises or in the cloud, and leverage all the innovations that cloud providers build into their infrastructures.

Barracuda remains out in front in regards to licensing options – for example, we were the first firewall to offer Bring Your Own License (BYOL), Pay as You Go(PAYG), and metered billing. Barracuda has also designed its solutions for a hybrid world: Our on-premises and cloud solutions can work seamlessly together to protect customers' data and applications, regardless of where it resides. Barracuda is a great choice for organisations that are just beginning their cloud journey or finding new ways to unlock the value of the public cloud.

To learn more about Barracuda's cloud security solutions, visit Barracuda's Cloud Ready web page. https://www.barracuda.com/programs/cloudready

About Barracuda Networks

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 deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda

Brunel House
Stephenson Road, Houndmills
Basingstoke RG21 6XR
United Kingdom

t: +44 (0) 1256 300 100
e: emeainfo@barracuda.com
w: barracuda.com