FORESIGHT FACTORY

THE FUTURE OF MULTI-CLOUD

Five year expert predictions on how Multi-Cloud will shape business across EMEA

Contents

Executive Summary

Whoever controls the multi-cloud, controls the future.

The ability to keep pace with technological change and consumer demand will push many European, Middle Eastern, and African (EMEA) businesses to breaking point in the next five years. The multi-cloud is a huge opportunity to innovate and stay ahead of the curve. It also presents a new dimension of strategic challenge.

The Future of Multi-Cloud (FOMC) report is the first of its kind, providing exclusive new insight into how EMEA businesses will be revolutionised through innovative digital transformation. It combines exclusive expert input with proprietary data and research from Foresight Factory to chart the multi-cloud's evolution and impact in the next five years. In addition, the report explores how consumer data management is influencing multi-cloud rollout.

The rapid pace of technological progress is creating a multitude of options for the storage and transfer of information. Cloud storage was an enormous and cost-effective step forward for both enterprises and consumers. That was just the tip of the iceberg. The challenges and possibilities have irrevocably changed.

Using multiple public clouds is now a powerful, undeniable conduit for greater flexibility, innovation and regulatory compliance. The FOMC analyses how businesses have been using the multi-cloud to date, and how the technology will develop in the future. The report has been divided into five main sections:

- A new era of business innovation
- Unlocking unprecedented agility, efficiency, and cost savings
- Plugging the skills gap
- Safeguarding the future and building trust
- Coping with compliance and infrastructural complexity

A new era of business innovation

The multi-cloud is a game-changer for both business and consumers. It will pave the way for unprecedented innovation, bringing cloud architects, DevOps, NetOps and SecOps together to pioneer transformational services traditional infrastructures simply cannot deliver. Although challenges exist today related to cost, skills, legal constraints and legacy infrastructure configurations, the outlook over the next five years is bright. Technologies such as artificial intelligence (AI) and machine learning will be fundamental to driving higher levels of automation, removing significant obstructions to multi-cloud adoption. The era of cloud apprehension is almost over. Whilst some experts disagree on certain aspects of cloud development over the next five years, they agree that those still stalling on multi-cloud adoption could become increasingly irrelevant or even extinct.

Unlocking unprecedented agility, efficiency, and cost savings

Genuine profit-and-innovation yielding digital transformation can only happen at pace with fluidity and security. Complexity and cost are often trumpeted as impediments to a full multi-cloud embrace, but the tide is changing fast. Technological progress continues unchecked and corporate cloud literacy is becoming an operational prerequisite. In five years, upfront cost concerns will be less important. If harnessed with intelligence and foresight, the expansive opportunities afforded by the multi-cloud can only benefit bottom lines and earn customer trust through service excellence.

Plugging the skills gap

We live in a security conscious, app-powered multi-cloud world, and the demand for technologically appropriate, value-adding expertise is reaching fever pitch. It is time to explode the myth that the skills gap is an intractable problem and that cybersecurity and cloud computing are inaccessible career options. Predictable doomsayers and statistical regurgitations are obvious media staples. We need to highlight the kaleidoscopic potential of youth, promote industry diversity and deftly discuss how smart, context-driven and automated solutions can spark attractive new career opportunities, as well as free up existing workforces for more strategic and rewarding work.

Safeguarding the future and building trust

Attack surfaces are expanding at exponential rates. Cybercriminals are no longer tinkering hobbyists but instigators of a new “hacking economy” that can outpace businesses innovation. Organisations need to confront the security challenge head on without compromising quality of service. The ability to quickly develop and deploy scalable applications and services anywhere, on any platform, is vital to meet customer demand and remain competitive. Implementing a robust, future-proofed ecosystem of integrated security and cloud solutions will help to build end-to-end IT services that give key stakeholders greater context, control, and visibility into the threat landscape. It will also yield the confidence needed to remove the scourge and cost of complexity.

Coping with compliance and infrastructural complexity

The EU General Data Protection Regulation (GDPR) is the most comprehensive and far-reaching piece of legislation of its kind. However, it is not enough. Within five years we need a global standard for data protection. Without it, there will be chaos. The intricacies of regulating a borderless digital world is one of the biggest challenges facing governments worldwide. Swift collaborative action is needed. Meanwhile, businesses need to stay compliant with existing legislation, which is made ever more complex by cloud computing’s growing influence.

Acknowledgements

We are very grateful to F5 Networks for commissioning this report. We are also deeply appreciative of the time and expert contributions provided by the following:

Eric Marks
VP of Cloud Consulting,
CloudSpectator

Toni Prince
Managing Partner,
Cloud Advisors Group

David Linthicum
Chief Cloud Strategy Officer,
Deloitte Consulting

Roy Illsley
Principal Analyst,
Ovum

Mohammed Owais
CTO, Cazar

Colleen Foyn
Senior Project Manager Cloud Innovation,
BCX

Arthur Goldstuck
Managing Director,
World Wide Worx

Stephen Leece
Managing Director, CitiLogik

James Tomkins
Chief Architect, Met Office

Travis W. Rehl
Director of Product, CloudCheckr

Other Contributors:

George Eapen
CISO, General Electric MENAT

Simon Gosling
Futurist, Unruly

Firas Al-Hilu
IT Director of Global Healthcare Co

Frances Zelazny
Chief Strategy and Marketing Officer, Biocatch

Mubarik Hussain
Head of IT, Petroserv Ltd

Methodology

Foresight Factory conducted an extensive and in-depth research programme across EMEA, drawing on a range of research tools and methodologies.

The initial stage involved a wide-ranging EMEA-centric review of Foresight Factory's proprietary bank of over 100 trends. Underpinned by original research across 25 global markets, it yielded powerful insights into evolving technological and socio-economic changes likely to impact on multi-cloud environments.

The trend review was supplemented by an extensive literature review of publicly available research to ensure all current and relevant data was considered when shaping the report.

The outputs of both reviews were then combined to develop a discussion guide, which was used to conduct qualitative interviews with 15 leading cloud experts hailing from industry, regulatory bodies and digital start-ups.

The key insights and outputs of each stage of the research programme have been synthesised and applied throughout this report.

Introduction

Technological Turbulence

Technological transformation is happening in every industry. Interestingly, innovations developed in one field are sometimes applicable to another. For example, artificial intelligence (AI) with machine learning can be applied to defend against cyber-security threats, or for the programmatic management of automated tasks. In this febrile environment, businesses are under constant pressure to move fast and deliver innovative services without compromising user experiences or security. Gone are the days of using a single cloud provider. The age of the multi-cloud is now unavoidable.

Throughout this report we define the multi-cloud as managing resources across two different clouds or more, regardless of location (i.e. multiples of public and/or private cloud; a mix of on-premises and public cloud with integrated platforms), versus a hybrid cloud which is integrating a single public and private cloud. Amazon Web Services (AWS) and Microsoft Azure lead the way in terms of popularity as well as market share, followed by Google Cloud Platform (GCP), Oracle, IBM and HP.[1]

The Growing Desire for Multi-Cloud

The FOMC report firmly believes that businesses not using multi-cloud will be in the minority in the next five years.

We are already well on our way. According to RightScale's 2018 State of the Cloud Report, 81% of surveyed global enterprises currently have a multi-cloud strategy in place.[2]

"There will be some businesses that stick with one vendor, but the majority are definitely going to go on a multi-cloud journey," explains Roy Illsley, Principal Analyst at Ovum.

Arthur Goldstuck, Managing Director at World Wide Worx, concurs: "In today's business environment, it is impossible to stick to one platform, one provider, and one type of cloud," he says.

Some industries are already leading the multi-cloud field, according to David Linthicum, Chief Cloud Strategy Officer at Deloitte Consulting. "The biggest multi-cloud consumers right now are finance by a huge margin, retail and healthcare. That is a huge hunk of the economy."

In Cloudify/IOD's 2017 State of Enterprise MultiCloud Report[3], the most popular two-cloud combination was AWS and Azure, followed by AWS and OpenStack, and AWS and GCP. Cloudify believes the preference for AWS and Azure stems from a desire to avoid vendor lock-in. It was also noted that small and medium-sized businesses (SMBs) will typically look for a multi-cloud model, while larger organisations will go for a hybrid model or will choose multiple private clouds.

"Now, more than ever, the multi-cloud environment is the de facto pattern," says Eric Marks, VP of Cloud Strategy at Cloud Spectator. "With the uptake in cloud consumption, organisations are fearful of being locked in to a single global provider."

---

[1] InfoWorld, September 2017, David Linthicum Blog
[2] RightScale 2018 State of Enterprise Multi-Cloud Report
[3] Cloudify/IOD State of Enterprise MultiCloud Report, 2017

It is also an opportunity to tailor services and innovation.

"CIOs have realised that some clouds are more appropriate for certain workloads than others. It is not about going for a supplier anymore but more about picking the right place for the right reason," predicts Roy Illsley.

While a multi-cloud strategy can facilitate significant developments in security, flexibility and control it also presents significant challenges, including increased operational complexity, looming skill gaps, intensifying regulatory requirements and infrastructural obsolescence.

Internal IT's Wake-up Call

FOMC experts claim that one of multi-cloud's biggest impacts is likely to be cultural, particularly within IT departments across EMEA.

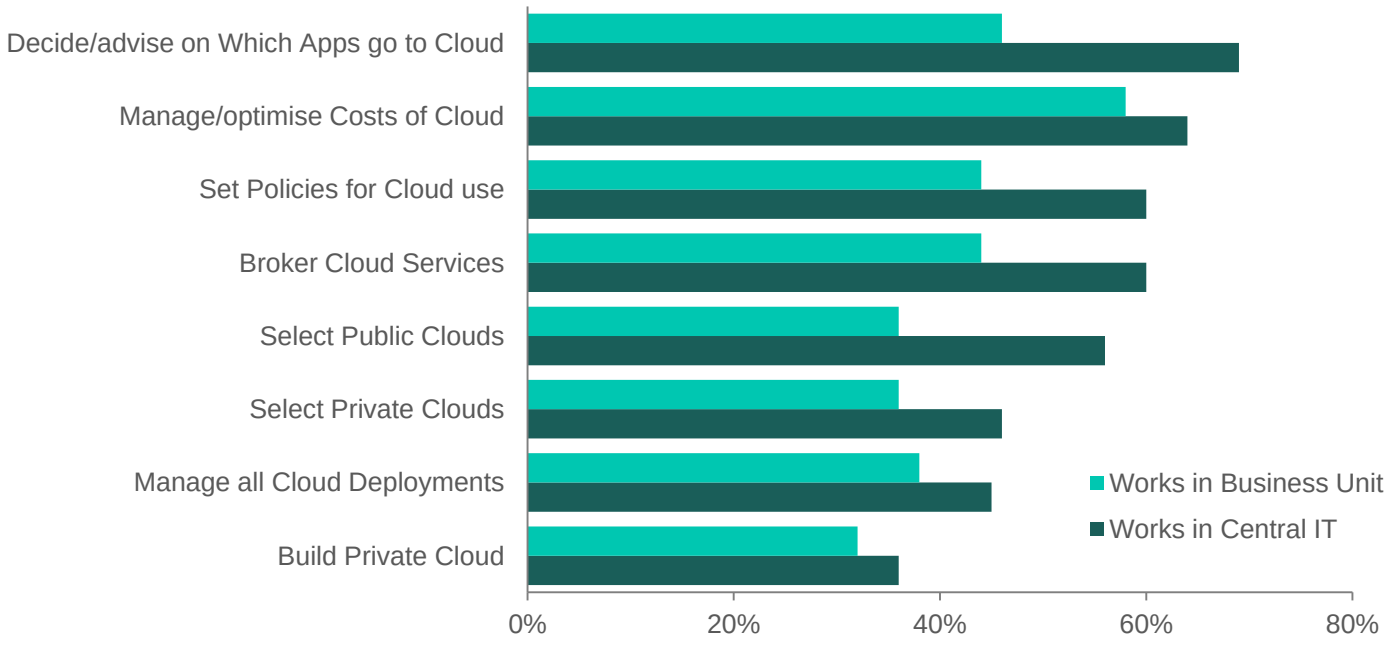
"The multi-cloud ramp up is one of the ultimate wake-up calls in internal IT to get their act together," says Eric Marks. "I think that one of the biggest transformative changes that it brings to an enterprise is the realisation of what a high performing IT organisation is and how it compares to what they have. Most of them are finding their IT organisations are sadly underperforming."

A vivid case in point for disrupting the IT status quo is the way hyperscale providers such as AWS, Azure and GCP have revolutionised ease of adoption. "There are now outsourced options where I can put a whole data centre in place within five minutes," Eric Marks explains. "I don't really need an IT organisation that needs a month to prepare some servers for my business project."

Chart 1 highlights the difference between central IT's view of their role and the view of the business units they support[4]. Interestingly, the process of selecting which public cloud(s) to use has the most divergent views. Central IT believes the selection of public clouds is more integral to their role than the business units envision.

[4] RightScale 2018 State of the Cloud Report

Chart 1: Enterprise Views of Role for Central IT, 2018



RightScale 2018 State of the Cloud Report

Consumer Power

Consumers are already extremely active in the multi-cloud space through extensive use of free services like Google Drive and Dropbox, and their relentless appetite for rapid, convenient and secure connectivity shows no signs of slowing. The Cisco Global Cloud Index estimates that consumer workloads and compute instances account for 27% of total usage, up from 24% in 2016. Video streaming and social networking are major contributors to this ongoing rise. Meanwhile, enterprise workloads and compute instances will fall slightly from 76% in 2016 to 73% in 2021.[5]

David Linthicum is bullish on continued consumer use and multi-cloud influence. "I think we are going to have retail clouds," he says. "The list goes on in terms of consumer-friendly clouds with their user-friendly interfaces. We are not necessarily going to find consumers leveraging S3 buckets or storage systems on Azure, but consumer-centric, SaaS-focused offerings will continue to grow at a significant rate."

Another notable aspect of the consumer multi-cloud world is the idea of serial arbitrage. "What's going to happen is kind of a parallel multi-cloud arbitrage model based on price and price performance – metrics like that," says Eric Marks.

[5] Cisco Global Cloud Index

Market Maturity and Shifting Definitions

There are major differences in multi-cloud adoption maturity and even debate about existing leadership positions. For example, David Linthicum claims that “Europe has a tendency to be much more multi-cloud than the United States.” On the other hand, Roy Illsley believes that North America leads the way, followed closely by the UK. “I think that countries like Germany are probably 3-6 months behind the UK, and France is probably another 3 months behind that,” he says, “then you’re looking at the Benelux countries and the Nordics.”

While maturity varies, the FOMC experts were unanimous in their belief that multi-cloud is a powerful and growing influence. However, precise figures on exact uptake are hard to find. This is partly due to inconsistent definitions.

“If you ask 10 people if a certain workload is a cloud workload, you would probably get 10 different answers. There are so many different definitions,” Roy Illsley explains.

A new era of business innovation

Fundamentally, most cloud service providers do the same thing: they host workloads for enterprises and consumers. Historically, cost has been the primary differentiator. That is changing. Today, it is more about what the cloud can enable rather than upfront expense concerns. Businesses are also more accustomed to the technology and are looking at factors ranging from serverless capabilities to regional data centre differences before choosing a cloud vendor.

Constant Change

Rapid technological innovation and hyperscale providers' deep pockets mean that change could well be multi-cloud's only constant.

"Given the pace of change and innovation, you're relying on leaders such as Amazon and Microsoft to really make the running in terms of the development of new features and to drive the maturity of new serverless capabilities," suggests James Tomkins, Chief Architect at the Met Office.

The pace of change is accelerating both in terms of software and hardware. According to RightScale's 2018 State of the Cloud report, machine learning is the most popular public cloud service in terms of future interest. 23% of respondents plan to use it, and another 23% are experimenting with the technology today.[6]

Microsoft's focus on machine learning has led it to invest in new server technologies, and the company has matched its innovation pace with enterprises' fluid and fast-changing needs.[7] Two years ago Microsoft had 32 core servers with 512GB Ram. Today, it runs 144 core servers with 4TB RAM. Its next generation assets will be even more powerful, supporting 50Gb networks and extremely low latency.

The necessity for hardware to keep up with the demands of both consumers and enterprises is also apparent in fields such as the Internet of Things (IoT) and edge computing. By 2019, IDC predicts that 45% of IoT-created data will be stored, processed, analysed, and acted upon close to, or at the edge of, the network.[8]

"People are really recognising the importance of being able to leverage computing resources on the edge to do more," said Scott Guthrie, Executive VP of the Microsoft Cloud + AI group, in a 2018 media interview.

"If you have a drone doing visual inspection of bridges looking for cracks, the amount of video that drone creates is enormous, and trying to upload it to the internet using 3G or 4G or even 5G is pretty bandwidth-intensive. The ability to have an Azure Stack instance on the truck where the engineer is doing video processing, doing AI on the edge, makes a tremendous difference as to whether that solution could work or not."[9]

---

[6] RightScale 2018 State of the Cloud Report
[7] Data Center Knowledge, As workloads Change, 'Scale Up' Augments 'Scale Out' in Cloud Data Centers. Mary Branscombe, May 2018
[8] November 2015, IDC FutureScape predictions.
[9] Microsoft Unveils AI Stack for On-Premises Data Centers and Edge Computing Sites, Mary Branscombe, May 2018

Either way, usage demands will be massive for both consumers and enterprises. Consumers, in particular, are increasingly using video content. Netflix users alone consumed more than one billion hours of video content per week in 2017. Meanwhile, almost five billion videos are watched on YouTube every day. In an average month, 8 out of 10 18-49 year-olds will watch YouTube-hosted content.[10]

At the same time, the development of new software and hardware features has created an unprecedented innovation arms race in the cloud. "Amazon is adding ten servers into the cloud pretty much every week, and that is going to be ongoing for the next five to ten years. The same applies to Azure," says David Linthicum.

Growth on this scale is, above all, reflective of the growing the needs of cloud service users. It is important to innovate both proactively and reactively.

"AWS sees the sheer scale of roll out of new services as a massive advantage," says Arthur Goldstuck. "It also means that if you go looking, the chances are you are going to find something pretty close to what you want." The constant update of dozens of new services means that enterprises will often choose the providers driving innovation. In May 2018 alone, Azure released 51 updates and patches.

Dealing with Vendor Lock-in

Vendor lock-in is a major concern for enterprises that value flexibility, and a major conundrum when weighing up the pros and cons of multi-cloud.

Some companies will commit to one platform if it means they can access innovative new services more easily. "For us, most of the innovation was happening on Azure, and by definition platform-as-a-service leaves you locked into one vendor" says Mohammed Owais, CTO at Cazar.

47% of industry influencers surveyed by Logic Monitor see vendor lock-in as one the biggest challenges for organisations dealing with the public cloud today.[11] Meanwhile, 20% of enterprises in the 2017 Cloudify/IOD State of Enterprise Multi-Cloud report stated that interoperability and no lock-in was the most important feature.

Specialised Offerings

Even with the scale of innovation from the major cloud service providers (CSP), there is still a need for technological diversity. Specialisation and the provision of specific vertical innovations may not be in the spotlight as often as the big hypervisors, but they are important factors in a multi-cloud world. "You are going to see more regional clouds provided by telcos to deliver specialist services to specific areas. Sometimes a local cloud is much more important than having something that is generic," says Roy Illsley.

According to the 2017 Cloudify/IOD State of Enterprise Multi-Cloud report, Software Defined Networking and Network Function Virtualisation (SDN/NFV) are the most critical emerging technologies for the telecommunications, defence and space industries. Containers are much more important for the software, networking and IT services industries. The CSPs that can integrate all these new technologies for specific industry verticals are becoming increasingly valuable.

---

[10] https://media.netflix.com/en/press-releases/2017-on-netflix-a-year-in-bingeing
https://www.youtube.com/yt/about/press/
[11] Cloud Vision 2020, The Future of the Cloud, Logic Monitor 2018

Examples of specialist companies able constructively mesh into the multi-cloud mix include Navantis, a Canadian vendor that uses Microsoft tools to help companies with application modernisation and integration. It also specifically specialises in Canadian regulation.

Solely adopting clouds from either specialist or generalist providers, however, could pose a problem when it comes to fully optimising operations. "You should have at least two hyperscale providers and maybe one speciality provider," advises Eric Marks. "This way you can have competition at the hyperscale level combined with the specialist services of the smaller provider. The smaller provider's prices could also influence the others."

Having multiple cloud service providers means also enterprises can quickly migrate workloads based on their needs at any given time.

The FOMC experts agree that specialist clouds running in concert with the large CSPs are likely to accelerate multi-cloud adoption in the next five years. Businesses are becoming more technologically savvy and specific with their requirements. This is forcing the bigger service providers to adapt while also opening up significant opportunities for those that can fill in the gaps and innovate.

Regional Differences

There are notable differences in regional cloud uptake across EMEA. For example, while AWS dominates US and European markets, it has virtually no presence in Africa. This leads to opportunities for other players to step in. A recent report by World Wide Worx highlighted that 50% of Nigerian enterprises use Azure, followed by 49% in South Africa and 37% in Kenya. GCP was used by between 25-29% of businesses in the same three countries. Oracle is used by 10% in Kenya, 8% in South African and 6% in Nigeria. IBM is used by 8% of business in Kenya, despite having virtually no presence elsewhere in the region. AWS claims a mere 2% share of uptake across all surveyed territories.[12]

The familiarity enterprises have with some providers may lead them to be less confident about switching to an unknown provider, even one as globally dominant as AWS.

Innovation in the Future

Dashboards that can be used to monitor multiple cloud services while also providing granular information will be the most common addition to IT professionals' tool-kits over the next five years. The FOMC experts agree that dashboards and the abstraction of a single layer are big short term necessities.

Simple management dashboards are already available, but the incorporation of new technology will be vital. Looking ahead, abstraction that can reach throughout the whole stack, integrating cloud services, containers and serverless functions will become standard.

"One of the most disruptive developments, and one that will evolve over the next five years is the serverless paradigm," says James Tomkins.

"Basically, it's moving you towards configuration, including smaller amounts of code, more manageable cost profiles. In addition, if you're deploying things at that level, then your scope for interacting in more lightweight ways with those public cloud environments makes multi-cloud environments perhaps more tenable."

---

[12] Cloud in Africa 2018, by World Wide Worx, for F5 Networks.

Serverless growth has been well documented by RightScale's 2018 State of the Cloud report, showing a 75% increase in just one year[13].

Top Growing Cloud Services, 2017-2018

Place	Service	Growth Rate	2017 Use	2018 Use
#1	**Serverless**	**75%**	**12%**	**21%**
#2	Container-as-a-service	36%	14%	19%
#3	DBaaS SQL	26%	35%	44%
#4	DBaaS NoSQL	22%	23%	28%
#5	DRaaS	21%	14%	17%

RightScale 2018 State of the Cloud Report

A large proportion of respondents to the RightScale 2018 State of the Cloud report are using configuration tools, with 34% implementing CI/CD in the cloud. 36% of respondents were using Ansible, with 21% planning to use the service in the future. This represents over 70% usage growth in a single year. Meanwhile, Terraform, a configuration tool released only in April 2018, is already being used by 20% of respondents, with another 17% planning to use it.[14]

"I think that the market is certainly right for companies that can help you orchestrate deployment, and the big push I am seeing now, and it certainly gives me hope for multi-cloud, is the maturity of the CI/CD providers," says Mohammed Owais. "So, the continuous integration and continuous delivery providers have now kind of taken on the role of tackling actual deployment of your application code or your services, wherever they reside."

As workload types change, so too does the need to orchestrate or manage them. Logic Monitor's Cloudvision 2020 report shows that 27% of IT professionals surveyed believe that 95% of workloads will be run in the cloud in five years. 44% of respondents to the 2017 Cloudify/IOD State of Enterprise Multi-Cloud report claimed that production workloads are the highest priority for orchestration today. 41% of respondents said that Cloud Management Platforms (CMPs) were the tools that they were using to do this. Inevitably, workloads will change in the future, influenced by factors such as the need to process data generated from IoT and other nascent technologies.[15]

The abstraction of the various layers and constant adaptation to new services does, however, impact on flexibility and cost. While enterprises want to be flexible, it can be difficult when tools that manage different cloud services and containers are hard to find. In addition, maintaining multiple cloud service providers can also be costly, depending on the size of a workload.

[13] RightScale 2018 State of the Cloud Report
[14] RightScale 2018 State of the Cloud Report
[15] Cloudify/IOD State of Enterprise MultiCloud Report, 2017

Implications: A New Era of Business Innovation

Implications for Enterprises:

- The need for differentiation and complex service delivery requirements will fuel further rapid technological innovation. Today, CSPs are adapting to customer demands, proactively creating new services and modules, as well as enabling start-ups and small and medium businesses (SMBs) to implement new strategies or develop new ways of launching products.

- Innovation is also the biggest implication for enterprises. Cloud options are significantly expanding and management and configuration tools that can combine the best services from multiple providers are becoming more sophisticated.

- Embracing the multi-cloud could also increase vulnerability. New services that are not properly understood or implemented could soon result in exploits, hacks, bugs and a host of other unforeseen problems.

- Over the coming decade, AI orchestration will lead to the gradual takeover of tasks and functions. AI and new orchestration capabilities will allow enterprises to automate many processes that would otherwise take up valuable time, freeing up IT teams for other tasks.

- New serverless architectures will fuel enterprises to cut down on time-to-market and simplify processes. It could also enable provider agnosticism and make it easier to benefit from the multi-cloud.

Implications for the Consumer:

- Few consumers will focus on the technical intricacies of the multi-cloud, but they will notice service drop-offs, inflexibility or security issues. At the same time, consumer data appetites are growing exponentially. All of this is likely to have a big influence on how businesses engage with and deploy cloud services, making multi-cloud scenarios more desirable over time and driving greater innovation.

- CSP specialisation will have a major impact on consumer multi-cloud usage. New CSPs that rapidly and securely enable the launch of custom applications and modification of stored objects will become more prominent.

- In the next five years, consumers will adopt interfaces that will utilise more multi-cloud systems for storage, including iCloud, Google Drive, etc.

- Consumers will be able to build and develop their own apps with unprecedented convenience and sophistication. The growing popularity of services like Scratch – a free object-oriented software development kit – is already on the rise and the evolution of the multi-cloud will push this even further.

Outlook: The Multi-Cloud Roadmap to Business Success

Innovation and specialisation will allow enterprises to find the best tools for their specific needs. Upfront cost will diminish as a deployment impediment over time. As a result, enterprises will be able to seamlessly grow in an optimal direction and become increasingly able to independently innovate and deliver new services. Technologies set to drive this transition include serverless architectures, and AI-powered orchestration layers and configuration tools to aid data-driven decision-making. Fear of vendor lock-in is expected to continue as a key justification for multi-cloud investments.

Unlocking Unprecedented Agility, Efficiency, and Cost Savings

With a multi-cloud strategy, enterprises can assign workloads to public clouds that are best suited for specific tasks, including speed, agility and security. Typically, cost is a barrier for many enterprises looking to use multiple cloud providers, though that short-term mindset is starting to change as more use-cases come to light. One of the ways that enterprises are increasing multi-cloud flexibility is through the adoption of open source, using resources such as Kubernetes or OpenStack. However, some experts strike a cautionary note and believe open source's popularity is on the wane.

Companies Must be Flexible

Vendor lock-in can prevent enterprises from being as flexible as they would like. This includes concerns of missing out on new features from other CSPs or the lack of a failsafe.

"The whole process of digitalisation demands that you have the ability to seamlessly move between different forms of cloud, whether it is on-premises or off-premises or in the private or public cloud," says Goldstuck.

Companies must be flexible, and the ability to fluidly move between different providers as needs dictate is becoming essential.

Comparison tools can give companies the ability to plan their multi-cloud strategy before committing to a provider mix. A diversity of consumption models can also enable focused trials and experimentation before committing to a service provider. For example, a user can pull down their containers or cloud storage and halt use of a service at any time. While dashboards are becoming more readily available, the ability to seamlessly switch between cloud services is already practised in some enterprises. In this instance, using a layer of abstraction could preserve flexibility while cutting down both financial and time costs.

Multi-Cloud Arbitrage

IDC reports that over 42% of European organisations cite managing and controlling cost as their most pressing multi-cloud data management priority. This rises to 51% among larger enterprises.[16]

Managing the costs of extant cloud services is another key issue for enterprises. According to RightScale's 2018 State of the Cloud Report, 64% of enterprise central IT respondents said that they viewed managing and optimising the costs of the cloud as central to their role (an increase of 9% since 2017).[17]

---

[16] IDC, Multi-cloud readiness among European Organisations in 2018, May 2018
[17] RightScale 2018 State of the Cloud Report

Inefficiency is also an issue. On average, respondents estimated that 30% of their cloud spend was wasted. RightScale also measured an additional 5% of waste. Costs can soon mount: 43% of respondents claimed to spend over $50,000 a month on their public cloud provision.[18]

Consolidation of spending and understanding your existing technology landscape is of paramount importance for enterprises. RightScale reports that 58% of respondents believe cloud saving optimisation is the number one priority in 2018.

Getting the right provider mix in place calls for rigorous analysis and clarity of purpose. Brand loyalty should not curtail action. If a service provider is fit for purpose, it should be considered. "The availability of choice will allow people to cherry-pick where they will get the best bang for their buck for a specific service," says Toni Prince, Managing Partner, Cloud Advisors Group.

The FOMC experts call for more enterprise support to get it right. This could come in the form of a dashboard or management platform that flags instances of waste. Ultimately, upfront costs are less important if enterprises alight on their optimal cloud configuration and remain customer-centric.

"With a multi-cloud dashboard, it becomes possible to mix, match and combine the best options," says Goldstuck. "Once you have more of that dashboard approach, and once you have greater commoditisation and the prices come down further, you will see an explosion in start-ups leveraging multi-cloud's benefits."

Where Next for Open Source?

Open source software is freely available and can be distributed and modified. It can play an important role in the multi-cloud space, though some FOMC experts disagree on the details.

"Open source is getting more popular, not less, and more components are offered in this format," says Eric Marks. "It's becoming more and more viable. You are soon going to have a full IT stack that is entirely built from open source components."

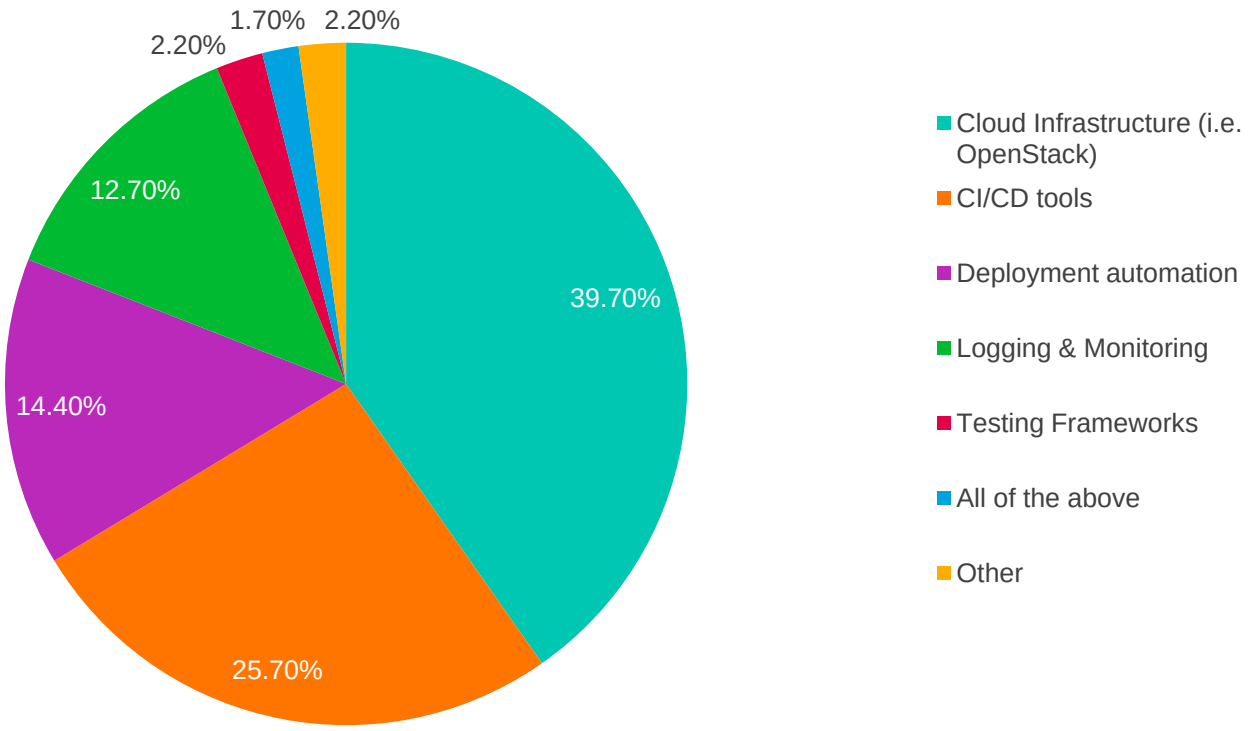
Importantly, open source software can help bridge existing interoperability gaps.

"People will use the right cloud for the right reason, and they'll be looking for an orchestration layer to mitigate the challenges with integration and cross-cloud working," says Roy Illsley.

David Linthicum is less optimistic. "We still have a significant shift away from open source," he says. "For example, we are coming to the demise of OpenStack, and we are not seeing players in terms of management consoles and open source backing public cloud platforms. Those seem to be being pushed aside right now."

[18] RightScale 2018 State of the Cloud Report

Chart 2: Open source tools evaluated during the last year



Source: Cloudify/IOD State of Enterprise MultiCloud, 2017

Chart 2 shows the open source tools evaluated by global enterprises in 2017. It highlights how a plethora of open source tools have emerged to offer alternatives to standardised premium solutions. Open source infrastructure was the most popular and is likely influenced by cost considerations. Interestingly, less than 2% evaluated "all of the above" choices, showing that, while many enterprises may want to use open source components, they tend to want them for specific, potentially gap-filling tasks or to save on avoidable costs.

With sectors adopting technology at different rates, open source uptake will remain variable due to security policies and varying commercial objectives.

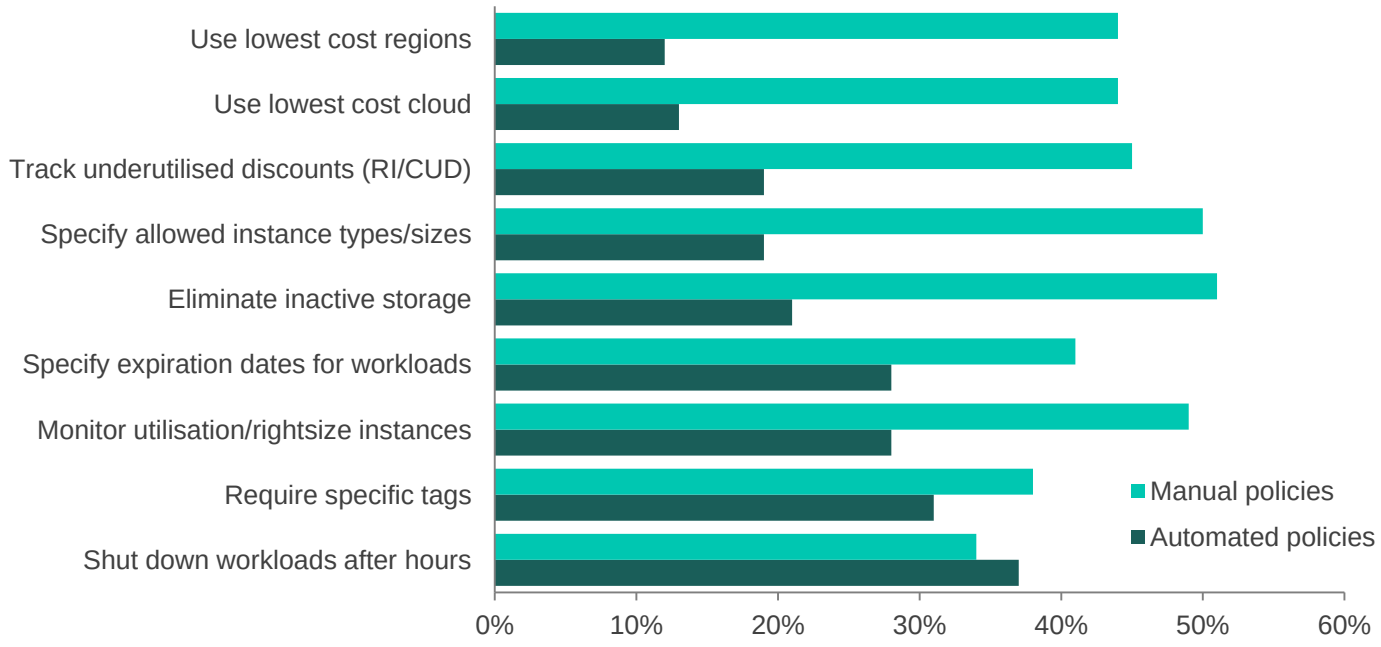
"We don't use open source at all," explains Colleen Foyn, Senior Project Manager Cloud Innovation, BCX. "If it's not supported our clients won't even look at it. Companies like WalMart are very strict on PCR compliance, so open source makes me a bit nervous. We would rather go with paid software that we know is secure."

Billing – One among Many Complexities

21% of respondents in the RightScale 2018 State of the Cloud Report stated that managing cloud spend was a "significant challenge", with 55% saying that it was "somewhat of a challenge". This changes slightly by company size, with 80% of enterprises claiming that managing cloud spend was a challenge, compared to only 72% of SMBs. Chart 3 shows how companies are optimising cloud cost, and for which processes they are using automated or manual policies[19]:

[19] RightScale 2018 State of the Cloud Report

Chart 3: How Companies are Optimising Cloud Cost



Source: RightScale 2018 State of the Cloud Report

Billing complexities can drive enterprises away from multi-cloud. Tools such as dashboards can help give DevOps and other IT professionals the visibility needed to maintain control.

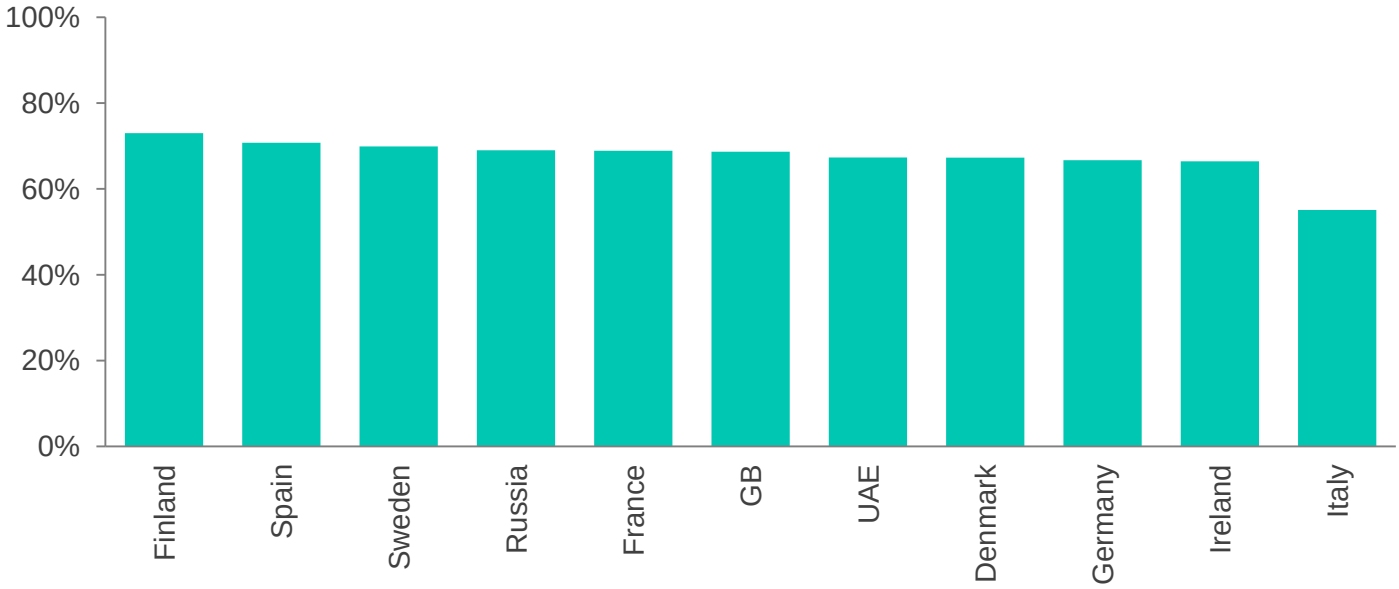
Challenges

Flexibility and cost are two of the main motivations for enterprises using cloud services today. A strong multi-cloud strategy can only emerge if constructed with a coherent aim and full visibility of any potentially derailing variables.

As a result, the FOMC experts expect to see the emergence of price comparison and switching services for cloud. Initially, these will require user input, but automation could soon take over for greater speed and accuracy. As indicated in chart 4, people are already receptive to this type of service.[20] There is significant potential for radical change. Both CSPs and enterprises would be able to devote much more time to other more strategic tasks. Automation-focused tools also have powerful waste-saving properties.

[20] Source: Foresight Factory │ Base: 370-3212 online respondents per country aged 16-64 , 2017 August

Chart 4: EMEA Interest in automatic switching services, 2017 | "How interested would you be in the following services?" A service which automatically switched your household utility supplier so that you always got the cheapest tariffs



Source: Foresight Factory Research | Base: 370-3212 online respondents per country aged 16-64, 2017 August

Implications: Unlocking Unprecedented Agility, Efficiency, and Cost Savings

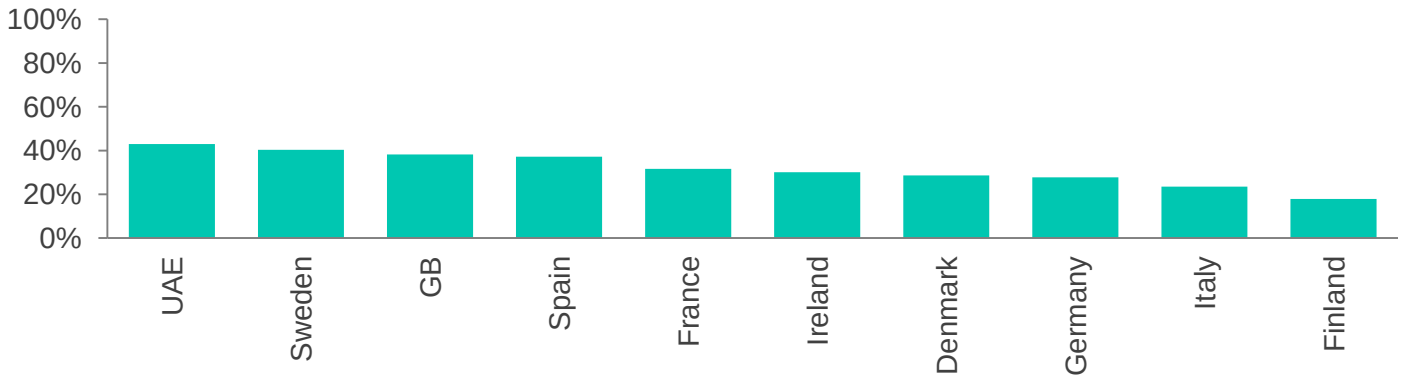
Implications for Enterprises:

- Using the right mix of services is an important consideration. Enterprises will have to make difficult choices between increasing flexibility and cost or stay with one cloud provider and keep costs and complexity more manageable.
- If the forecast of open source decline becomes more prominent, businesses may be cautious to adopt OpenStack or similar services, for fear of fewer patches and less support. If open source growth forecasts are more positive, businesses will be more confident using the technology to maintain more of their IT stack.
- Increasingly, enterprises need the technological wherewithal to decide which cloud service distribution mode to use based on their own specific circumstances.
- A multi-cloud strategy will necessitate a dashboard for monitoring spend as well as waste. Some services such as Cloudability already offer this and more sophisticated solutions are on the horizon. This will include services that automatically identify waste and re-allocate resources in real time.
- AI will become increasingly pervasive as businesses look for every competitive advantage, particularly in terms of optimising efficiency.

Implications for Consumers:

- The potential demise of open source would have far reaching ramifications for consumers, though many use the free versions of the storage tools that Google, or Amazon provide.
- Significantly, consumers that are using open source software to start a small business or develop software as a hobby may be constrained if costs become prohibitive.
- If open source declines in popularity consumer-oriented tools will become more difficult to obtain. Consequently, consumers already unfamiliar with the cloud could lose confidence in the technology.
- The ability to easily switch between different cloud storage services will be increasingly important for consumers who regularly switch between brands. Consumers will demand that this process becomes seamless, without the need for local storage.
- There is a growing trend for brand agnosticism. Consumers want to use the services that suit them at a specific time. Cloud services will be treated similarly to financial services or telecoms providers. Consumers want freedom of choice and flexibility (particularly in terms of avoiding vendor lock-in).
- New payment options will emerge as consumers come to better understand the intrinsic value of their data. Such shifts in public attitudes point towards a possible future where consumers pay for cloud services with their personal data.

Chart 5: Evidence of brand agnosticism across EMEA, 2017 | "How strongly do you agree or disagree with the following statements?" I regularly switch between different financial products/providers to make sure I am getting the best rates | 2017



Source: Foresight Factory Research | Base: 392-3433 online respondents per country aged 16-64, 2017 August

Outlook: Removing the Cost Barrier

Using the right combination of cloud services will not only ensure flexibility but also provide redundancies in the case of errors or server failure. The latter can be the difference between services working or critical failure.[21] As ever, cost is a potential roadblock. However, tools are emerging to ensure waste is cut from the onset, and the long-term gains of an innovation-fuelling multi-cloud strategy are becoming increasingly apparent.

[21] https://virtualizationreview.com/articles/2018/03/05/aws-outage.aspx

Plugging the Skills Gap

Adopting a multi-cloud strategy is necessary for many businesses for flexibility reasons but the added complexity of monitoring multiple cloud services, as well as containers, APIs and other processes can be daunting. Standardisation of processes across multiple cloud services can thus be a major inhibitor to multi-cloud. There is also a knowledge and skills gap to contend with. Available workforces are simply not keeping pace with technological developments and business requirements. Siloing of existing knowledge or lack of collaboration within businesses may further exacerbate multi-cloud apprehension and unfamiliarity.

Enterprises Have a Critical Knowledge Gap

Many IT professionals lack both general and specific knowledge as it relates to multi-cloud. For instance, they may not know about how to efficiently use new services (i.e. serverless architectures), or how to integrate or orchestrate multiple processes to work in tandem.

A move to a multi-cloud strategy brings significant challenges and enterprises need to ensure they understand the nuances of these before they invest too heavily.

Multi-cloud management was cited as the 4th biggest challenge for enterprises according to the 2017 Cloudify/IOD State of Enterprise MultiCloud report (13% of surveyed IT professionals). This is seen as almost as important as more traditional cloud management concerns such as app deployment or automated scaling and was deemed even more important than cost analysis.[22]

Not sharing information across teams can also deny businesses access to new and potentially game-changing technologies. Cloudify and IOD's 2017 State of Enterprise MultiCloud report also found that the speed of technological adoption was far greater in non-siloed organisations. 74% of non-siloed organisations took six months or less to adopt new technology (30% would adopt it in weeks), versus 58% of siloed organisations taking over six months to adopt new tech.[23]

It is vital for all the relevant parts of a business to understand any cloud strategy in use. Any knowledge gaps can result in severe security or compliance issues. It can also lead to problems with Shadow IT whereby certain individuals begin using another cloud provider without the knowledge of the rest of the organisation.

Learning Multiple Skillsets a Major Challenge for Businesses

Most of the FOMC experts claimed that there was little difference in the skills required to use multiple clouds.

"I think someone trained on Azure or AWS is going to be able to make the transition fairly easily and understand the language and the environment," says Goldstuck.

---

[22] Cloudify/IOD State of Enterprise MultiCloud Report, 2017
[23] Cloudify/IOD State of Enterprise MultiCloud Report, 2017

According to the Cloudify/IOD 2017 State of Enterprise MultiCloud report, the three biggest hindrances to the adoption of new technology are people and politics (32%), skillsets (22%) and company culture (21%). These make up 75% of the hindrances to new technology adoption and highlights the necessity to properly disseminate of information within a company. Building skillsets is arguably the trickiest to overcome. Training or hiring can be an enormous effort for enterprises, and even deciding on which skills are necessary can be difficult.

Andy Jassy, CEO of AWS, echoes this point. "Learning multiple platforms is a pain," he said during a recent media interview. "Trying to make the shift from on-premises to the cloud is hard enough, and learning multiple cloud platforms is an added, unnecessary layer of complexity."[24]

The cumulative result of all this uncertainty is that some enterprises will not move to the multi-cloud in the near future.

Enterprises Can't Keep up with Multi-Cloud Strategy

The multi-cloud approach can scale relative to the size of the enterprise, but the ability to keep track of the myriad services and upgrades pushed out by major CSPs can be overwhelming.

"If you know Amazon has 500-1000 services that you're interested in and Google has 200 services and Azure has 500 services, and if you're adding all three of those clouds, then you have to manage the use of those services amongst the systems in your portfolio," says David Linthicum. "The ability to do abstraction, governance, and federated security that goes beyond the major cloud providers is key, and obviously that adds much more risk, much more expense, and much more complexity."

Enabling IT to broker multiple cloud services is an important initiative for 32% of respondents in RightScale's 2018 State of the Cloud report[25]. This shows that there may be miscommunication between IT operators who see the necessity of developing a multi-cloud strategy, and those that are restricting it. Once again this can impact innovation and agility. Clearly, it is necessary to have standardised knowledge and goals throughout an organisation.

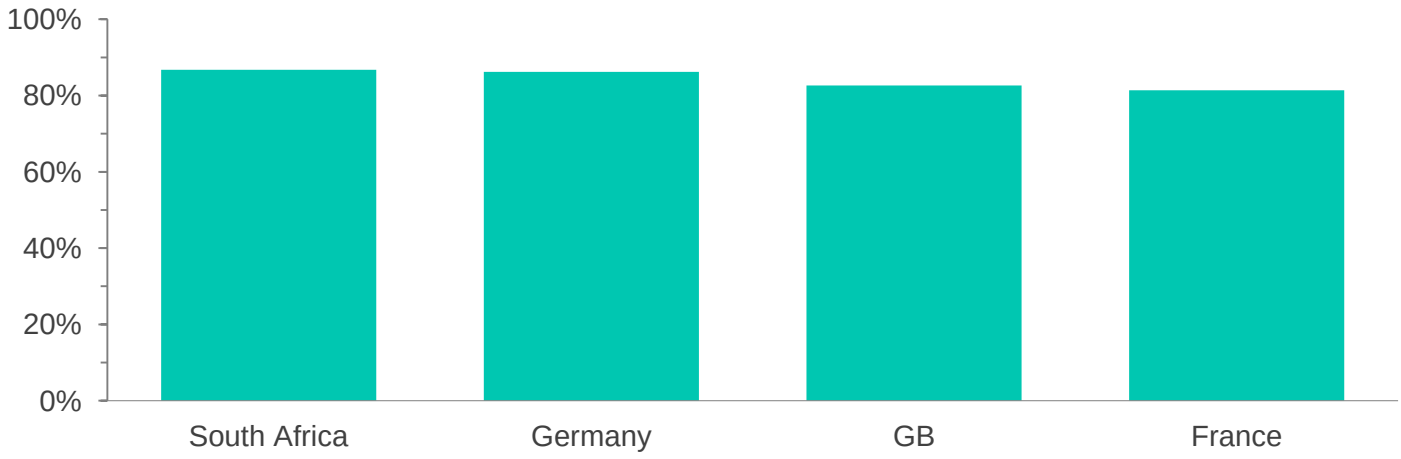
According to findings from 451 Research, there are regional differences to consider as well. Almost four out of five surveyed businesses in Western Europe claimed IT and security departments are best placed to understand digital transformation. In the Middle East and Africa, it was just over three in five.

451 Research found that legal teams lag behind in the understanding of digital transformation, which in the context of GDPR and other regulations could prove problematic. In Western Europe, just over half of legal departments claimed full understanding, dropping to below two in five for the Middle East and Africa.[26] The nature of moving to multi-cloud can have far-reaching implications. Making sure all teams adequately understand the details is vital to prevent inconsistencies and difficult situations. The good news is that workforces tend to be receptive to new technology and skillsets (see Chart 6).

---

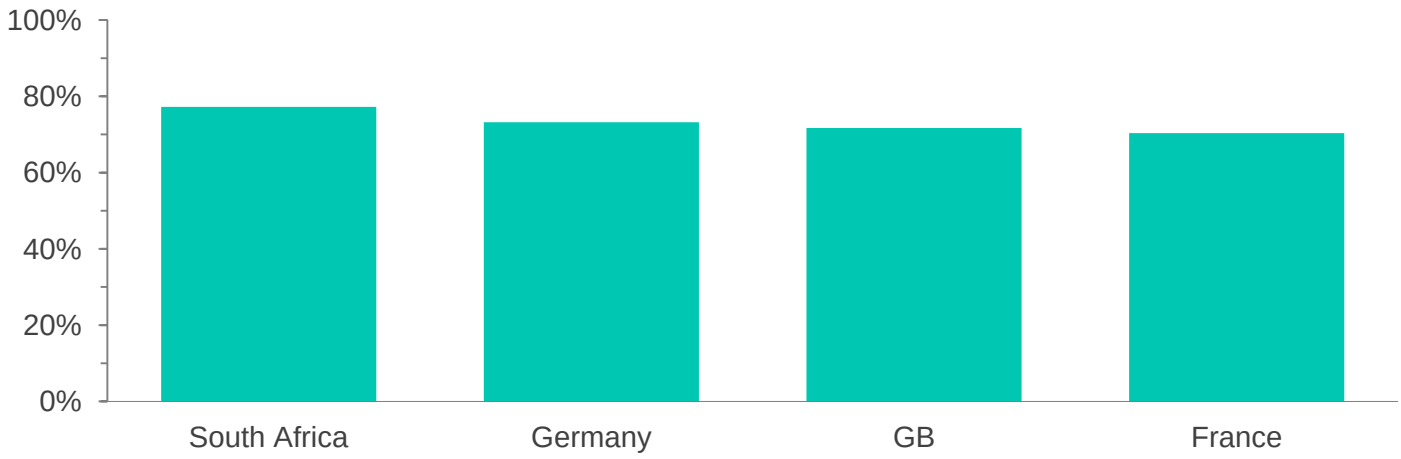
[24] Network World, April 27 2017, Brandon Butler, Senior Editor, Network World.
[25] RightScale 2018 State of the Cloud Report
[26] 451 Research

Chart 6: Needing to learn new skills, 2015 | "I will need to continue to learn new skills throughout my life to be successful in work" | % who agree or agree strongly



Source: Foresight Factory Research | Base: 1000 online respondents per country aged 16-25, 2015 November

Chart 7: Needing skills for employment, 2015 | "I am prepared to learn a whole new skill-set to get a job" | % who agree or agree strongly



Source: Foresight Factory Research | Base: 1000 online respondents per country aged 16-25, 2015 November

Organisations Need New Technology to Manage the Multi-Cloud

Multi-cloud management complexity means that businesses need new tools and processes to cope.

"We've got to find a way to collapse the technology monitoring landscape to a single, more simple view," warns Eric Marks.

Recent data from WinMagic's June 2018 survey of global IT decision makers backs this up. 63% of respondents claimed that the need for multiple management tools halted their multi-cloud strategies. A quarter of the respondents claimed that, because of compliance issues, they only work with a single cloud vendor.[27]

[27] WinMagic Survey, June 2018,

"You have to have some sort of a management, security and governance infrastructure to deal with the number of cloud-native services under your control," says David Linthicum.

The layer required to sit above the various cloud services would potentially also need to cover multiple types of monitoring, including compliance, security, management and billing. The number of aspects a dashboard needs to cover is impossible via a single pane of glass.

Management and Orchestration

Management and orchestration tools are available from vendors like VMware, Terraform and Ansible. However, cloud management platforms are by far the most popular. Cloudify and IOD's 2017 State of Enterprise Multi-Cloud survey found that 41% of respondents used a cloud management platform. It is notable that 29% used "other" orchestration and management tools, highlighting both the diversity and uncategorised complexity of currently available options.[28]

The difficulty of staying on top of cloud services increases steeply with the number of services an enterprise monitors. "If you've got lots of small services then monitoring becomes key," says Mohammed Owais. "From our experience, a dashboard definitely would have helped. If that meant that we had one vendor that was helping us with monitoring across multiple cloud providers, one that was helping us with deployment across multiple cloud providers and one that was potentially helping us with billing, or at least monitoring of the billing, that would have made things significantly easier. I can't imagine one company doing all three."

Does every Company Need a Dashboard?

"A dashboard is on the mind of every single IT director or CIO that you talk to," says Toni Prince.

While dashboards can significantly decrease the complexity of managing multi-cloud services, some argue that it could add another dimension of complexity. Future automation could mitigate this viewpoint, however.

"There needs to be an IT operations desk that gives you the operational view," says Eric Marks.

"It's a kind of two-layered single pane. The end-user view and then the operations view of what's really happening behind the scenes while consumers are using all these different cloud services, building apps, deploying them in to containers and so on. There needs to be that single view to basically aggregate all those APIs in."

Generally, a dashboard is necessary to implement control over various different processes, including utilisation management and potentially even historic utilisation analysis. More specifically, a dashboard is vital in the context of controlling security operations across multiple clouds.

Is One Dashboard Enough?

Managing security across multiple clouds can be difficult, especially with different protocols that are not interoperable with one another. As a result, a multi-dashboard solution may be required. "I need at least three or maybe four windows into my operational world," explains Eric Marks.

---

[28] Cloudify/IOD State of Enterprise MultiCloud Report, 2017

"I need API management tools to see what my APIs are doing. I need container management tools to look at what my containers are doing, and make sure that they get paired up and placed on the appropriate host. I also need my cloud management tools to manage the cloud services layer, and then I need the monitoring infrastructure for all the rest. The single pane of glass for the cloud is only one of multiple panes of glass that we need to manage this environment."

The need for multiple dashboards to drill down into specific operations such as security also raises questions about the elimination of potential vulnerabilities, including on-premises storage and cloud services.

"Automation is key, governance is key, third party security systems and identity access management is key. This is going to drive a lot of spending over the next five years," predicts David Linthicum.

Dashboards may Abstract away from the Native Platform

While a dashboard would be a welcome addition to a businesses' monitoring arsenal, some experts believe it could distract DevOps from the underlying technology and just create another new set of problems to grapple with. "Dashboards can only really abstract you away so much from the underlying platform. Ultimately, you still need to understand everything that lies behind that," ventures James Tomkins.

While a dashboard can provide information and oversight it could also add another layer of unwanted complexity. Furthermore, the desire to drill down into operations to look at native services may prevent some IT professionals from adopting more generalist dashboards.

Looking Ahead

As more enterprises adopt a multi-cloud strategy, complexity, at least for a period of time, will increase dramatically. This will be somewhat alleviated when dashboards and other tools become common, and orchestration and machine learning take over time consuming aspects of managing and standardising multiple clouds.

Although Amazon and Microsoft offer product training, there are few third party organisations that can help train IT teams to become "multi-cloud ready". Initiatives such as the Cloud Academy can teach users skills such as Azure, AWS and GCP, and there are expectations that the creators of dashboards will offer training services as well. This could help mitigate the knowledge and skills gap, as well as give the dashboard creators an opportunity to build client rapport.

One future-facing technological innovation flagged by many FOMC experts was the ability to have multiple dashboards for different levels of abstraction, including security, monitoring, compliance and containers. While dashboards exist in various forms, the ability to monitor containers or serverless apps across different cloud deployments is not yet possible.

Some of the larger providers are already moving towards offering a more specialised service. Microsoft, for example, is focusing on machine learning for Azure via the Microsoft Azure Machine Learning Studio and the consistent release of new machine learning tools. Amazon, on the other hand, is focusing on containerisation with their Elastic Container Service, wherein they have a set of tools to assist with the management of Docker. This specialisation could result in more granular dashboards within a single service, but it is unlikely that AWS and Azure will release tools that encourage the use of other platforms.

Implications: Plugging the Skills Gap

Implications for the Consumer

- Consumer cloud knowledge is very limited despite widespread use. This is unlikely to change in the short-term.
- Simplification is needed to inspire greater understanding, including rebranding products and focusing on the user-experience. Google excels here, positioning many of their products in an explicitly consumer-centric, accessible fashion. This style of presentation and functionality needs to be replicated by other enterprises

Implications for Enterprise

- Some businesses are more at risk than others when it comes to the skills gap. It will become increasingly important for businesses across EMEA to adequately map out existing gaps and understand how these can be addressed in both the short, medium and long term.
- Multi-cloud management can be difficult and often requires the use of third party tools. This presents new opportunities for ambitious and specialist cloud management providers capable of winning end users' trust.
- The monitoring of containers, APIs and serverless applications is rare. New services and technologies are constantly being developed, with a lag time for dashboard providers to integrate these and train relevant staff.
- Abstracting away from cloud and container tools can cause difficulty. It is important for IT professionals to fully understand the native platforms they are using and introduce abstraction.
- Recoding software to operate with different endpoints takes time and expertise, which some smaller organisations might not have. However, recoding software to operate with a dashboard that then itself links to different endpoints will be more successful.
- Multi-cloud will be the dominant strategy for most enterprises, but new methods will undoubtedly emerge. It is imperative that enterprises maintain a watchful eye on new innovations and train employees as appropriate.

Outlook: the Need for Speed for Development, Collaboration and Empowerment

The skills gap is a clear and present danger but one that needs to be faced head on. Now is the time to scale our skills and invest more in the next generation of industry experts.

Today's youngsters are technologically immersed in an unprecedented way. Their lives are shaped by data both in the way they learn and play. To ensure they become responsible, vigilant cybercitizens, it is crucial to integrate smarter security and cloud disciplines into the school curriculum and home life from the outset, whether for personal awareness or longer-term employment prospects.

Governments and academic institutions frequently tout the importance of STEM (science, technology, engineering, and mathematics) skills at school, but the acronym is arguably a letter shy. In today's digital society, perhaps we should re-consider STEMS by adding 'S for Security' to the education agenda. By bringing the subject into the daily programme, students will understand the issues and follow best practice to discern right from wrong. Tackling the problem early on also paves the way for improving the current problem of an insufficient number of IT specialists graduating from university.

There is also significant potential to actively encourage more women to pursue IT as a career. For example, the Global Information Security Workforce Study indicates only 7% are currently working in cybersecurity, but there is a growing appetite to change this issue.

Safeguarding the Future and Building Trust

Attack surfaces are expanding at a staggering pace with both cybercriminals and their tools becoming increasingly sophisticated and destructive. Managing multiple challenges in a multi-cloud world can undermine organisations' confidence to withstand a cyber-attack. The explosive proliferation of applications in the cloud has created a vast new playing field for cyber-criminals. Today, the fear of attack is constant.

Apps can now be deployed from anywhere, including data centres, private and public clouds, containers and SaaS platforms. The spread of multi-cloud architectures, if inadequately managed, can lead to application sprawl and overwhelming security complexity.

A Changing Landscape

The development of multi-cloud comes at a time when the cyber threat landscape is also in a state of flux, with new types of threat constantly emerging and spreading fast. While large CSPs provide significant security support to enterprises, gaps are still possible.

McAfee's 2018 Threat Predictions[29] details how the security landscape will undergo five major changes. These include the development of an arms race in machine learning; the growth of ransomware; the threats generated from the popularity of serverless apps; the surrendering of privacy and the exposure of children to online threats.

In the world of cyber-security, machine learning can yield a host of solutions to costly problems plaguing companies for decades. This includes detecting and implementing solutions for vulnerabilities, zero day exploits and other threats. Machine learning can also assist human operators in the assessment and quick resolution of threats. However, when used by attackers the technology can be used to detect vulnerabilities for exploit, and quickly react to security measures.

The multi-cloud brings a level of complexity that can lead companies to use third party dashboards and other services, many of which may have vulnerabilities. Furthermore, the necessity to standardise security across platforms can be difficult and time consuming. Security gaps may also appear when enterprises are unable to replicate the most secure policies across all cloud services.

Ransomware was one of 2017's biggest cybersecurity growth areas, according to Symantec's ISTR 23 report.[30] It has also been in the media headlines following a number of notable attacks, including WannaCry and Petya/NotPetya.

In the context of the multi-cloud, ransomware provides a similar threat to other attacks. However, the types of industry targeted are different.

---

[29] McAfee Labs 2018 Threat Predictions, November 2017
[30] Symantec ISTR 23

According to NTT Security[31], the biggest sector targeted by ransomware in 2017 was business and professional services (28% of attacks). Government was the next largest, showing that even state level security is sometimes insufficient.

With the multi-cloud, the added flexibility of having redundancies can give enterprises the opportunity to store sensitive data across multiple centres, ensuring that critical infrastructure can potentially be rebuilt if needed.

Serverless apps can “save time and reduce costs” while also exhibiting critical flaws.

PureSec found that one in five serverless apps have a critical security vulnerability that can be hijacked for malicious purposes.[32] These security flaws may be localised to the platform in use, whether it is Lambda or Azure’s serverless architecture. Consequently, there may be a need for bespoke flaw detection and amendment. A dashboard that standardises security across cloud services may not do so across serverless architectures or may not cover all the flaws that attackers have discovered.

Types of Threat

NTTSecurity outlines the origins and nature of the threats in the EMEA region, below:

Services and Attacks in EMEA, 2017

Top services used in attacks against EMEA	Top malware types from EMEA	Top regions attacking EMEA
File shares (45%)	Trojan/Dropper (67%)	United States (26%)
Websites (32%)	Virus/Worm (15%)	France (11%)
Remote Administration (17%)		United Kingdom (10%)

Source: NTTSecurity Global Threat Intelligence Report, 2017

Furthermore, NTTSecurity claims that 38% of all worldwide phishing attacks originate in the Netherlands, and 53% of worldwide phishing attacks come from EMEA.

Private versus Public

In a recent AWS survey, security improvement was the top response to the question, “what, if anything, could change in the public cloud that would make the private cloud redundant or unnecessary for you?”.[33] 61% of enterprises stated they would avoid running sensitive data workloads on public clouds.[34]

The opportunity for businesses now is to rethink where the priorities lie in today’s evolving IT landscape. This is where advanced security automation and orchestration systems come in to play, helping to streamline and standardise IT processes, reduce operating costs and improve time to market.

---

[31] NTTSecurity Global Threat Intelligence Report, 2017

[33] AWS Insider, Security, Vendor Lock-in top public cloud concerns, Gladys Rama, from Stratoscale Hybridge Cloud Survey

[34] AWS Insider, Security, Vendor Lock-in top public cloud concerns, Gladys Rama, from Stratoscale Hybridge Cloud Survey

Optimal operational automation needs to encompass the configuration, deployment, and scaling of applications and servers. Removing manual processes and using automated systems provides decision-makers with the ability to identify threats quicker, enabling application threat protection before it is too late. Furthermore, the ability to manage data protection from a single source, and to move data between public and private clouds, will allow businesses to achieve the agility they need to improve performance and meet evolving customer demands.

While private clouds are here to stay, much of the enterprise workloads are predicted to move to public clouds in the near future, often for security reasons. As a result, many enterprises are reluctant to depend on a single vendor.

"European organisations are more likely to leverage several clouds at the same time," says David Linthicum.

"They don't want to put all their eggs in one basket, and there is a sense of distrust in some of the American providers with some of the legal issues that have come up, such as the CLOUD Act."

The problems reach another order of magnitude when considering future cloud use cases, which are likely to include more complex interactions with critical infrastructure and life- and business-critical services.

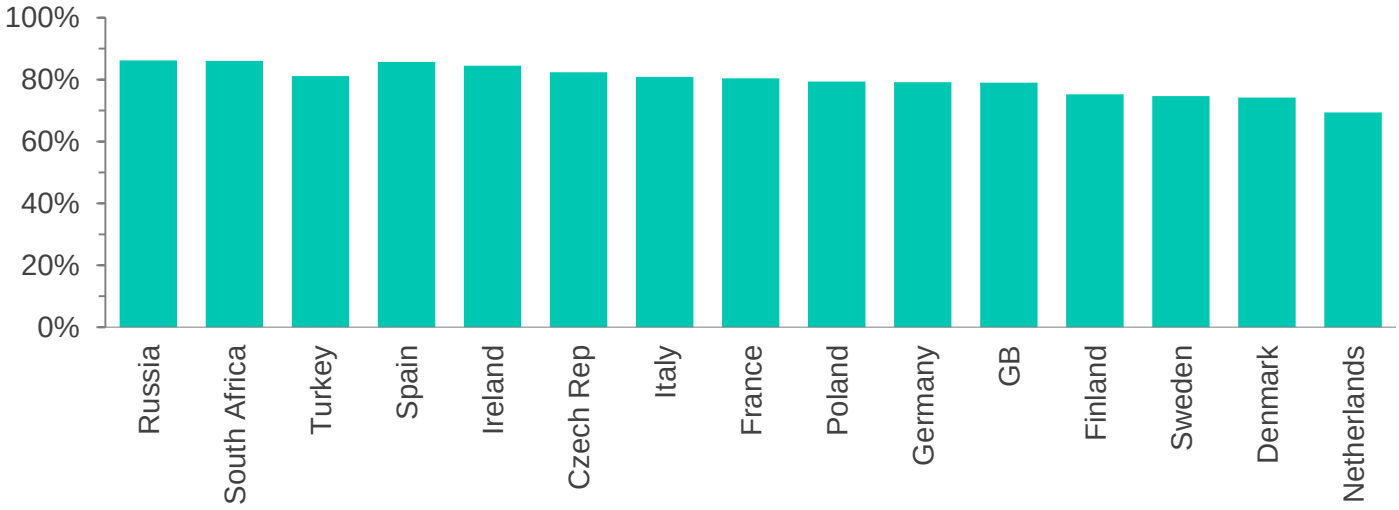
Consumer Capital

There is a growing consumer awareness about how personal data is stored and used. These concerns can impact the types of storage enterprises use, and the degree of security enterprises need to employ to ensure data theft scandals are minimised. While many data theft scandals do not tend to permanently hinder a company's ability to operate, they can be embarrassing, and can lead to calls for change.

This is especially true in the context of the EU GDPR. According to Foresight Factory research, 81% of consumers globally want more control over their personal information and the way it is stored, rising to 86% in parts of western Europe.[35]

[35] Source: FF Online Research │ Base: 1000-5000 online respondents per country aged 16-64 (S. Africa 16-54), 2016 February

Chart 8: EMEA Consumer demand for more control over personal information, 2016 | "How strongly do you agree or disagree with the following statements? I would like more control over the personal information I give companies and the way in which it is stored" | % who agree strongly or agree | 2016



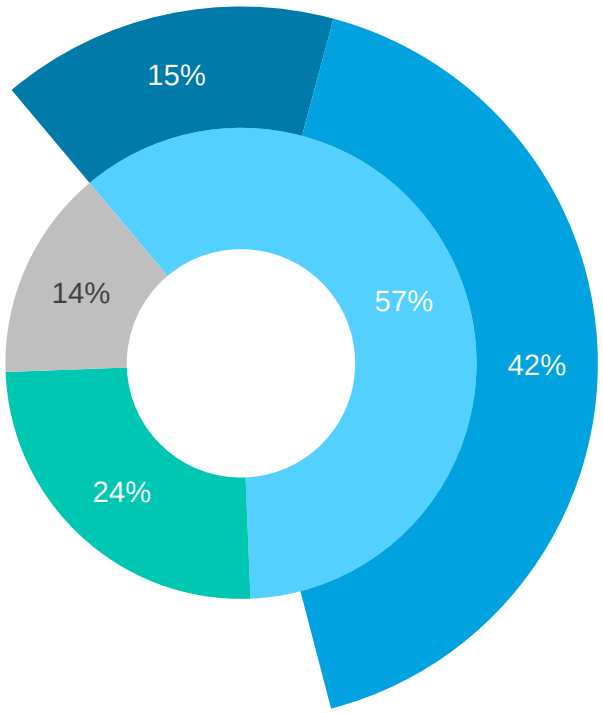
Source: Foresight Factory Research | Base: 1000-5000 online respondents per country aged 16-64 (S. Africa 16-54), 2016 February

Furthermore, the way consumers want to use data is nuanced, and may affect the ways it is stored.[36]

Chart 9: EMEA Consumer desires for how they want to trade personal information, 2016 | "For which reasons would you be happy to give permission to a company to use your personal data."

Private Preference
No explicit interest in data sharing with brands and minimal interest in data-led services or products covered by our research.

Function Favourers
No explicit data sharing with brands, but shows interest in data-led personalised products or services, so will likely share if the proposition is right and data used is obviously relevant



Discount Only
This group is happy to provide personal data to brands, but their only driver to share is to receive better and more relevant discounts from brands.

It's Personal
This group is explicitly willing to share data for a wider range of personalisation features, including tailored advice, discounts and improved product suggestions.

Source: Foresight Factory Research | Base: 1000-5000 online respondents per country aged 16+, 2016 February

[36] Source: FFonline Research | Base: 1000-5000 online respondents per country aged 16-64, 2016 February

Consumers want to use their data in different ways, including more functional benefits (i.e. discounts or simply keeping their data private). If consumers want different levels of access to their data, this could force enterprises to store it in different ways. For example critical private data could be kept on-premises, and the rest in a series of public clouds. Multi-cloud organisation also becomes critical here, as transferring consumer data between clouds grows in importance.

Consumer desire for more data storage transparency is intrinsically linked with trust. Both enterprises and consumers want to trust that those organisations storing their data are doing so effectively, safely and with minimal change of cost or process in the future. Scandals such as security breaches and data leaks are constantly changing trust-levels across industries.

Looking ahead

Adopting a multi-cloud route does not have to mean compromising security. With advanced security solutions, businesses can safely move their applications to any cloud model that works best for their strategy without geographic or infrastructural constraints. Consumer demands and industry competitiveness continue to make the cloud an essential option. The right deployment strategy makes it a viable and safe one.

The threat landscape is more sophisticated than ever due to volumetric attacks, malicious bots, and other tools targeting apps and sensitive data. Many traditional practices are no longer effective because they are too labour intensive and time inefficient to protect what really matters. This is where automation comes in to streamline and standardise IT processes, as well as remove human error. It also helps IT staff focus on other priorities, such as analytics and problem solving.

IT decision-makers want services that deliver, manage and protect applications in the cloud as they do in the data centre. Avoiding rudderless multi-cloud sprawls and simplifying the related complexities is vital to determine which workloads fit the right environments. This means considering the application delivery and security capabilities of each cloud provider, as well as the perennial issues pertaining to lack of visibility and control.

The rising value of data will also lead to changes in the security landscape. For example, consumer reaction to data breaches may change as their data gains tangible value.

Security – Implications for Enterprise

- The move to multi-cloud will lead to many enterprises needing a layer of security that can cover multiple cloud services, as well as extra services such as serverless applications. This will require training, as well as bespoke implementations.

- The perception that on-premises is more secure than public cloud is will become more confusing for enterprises. In practice, context will be a key determinant of security postures.

- Regulation and compliance may restrict enterprises' choices when it comes to which software to use and which formats are most attractive. Compliance teams and IT teams should work together continuously to perfect a security system whereby regulations and processes are up to date and keep pace with industry innovations.

- For developers, the multi-cloud offers flexibility, innovation and potential new problems with complexity. The security implications revolve around making sure that protocols and processes are standardised across clouds, and that any gaps are swiftly filled.

- Guarding against threats on a multi-cloud system could be more difficult than on a single cloud. Learning the skills to spot any unusual activity on multiple clouds will be key for enterprises in the future.
- Over the coming decade, biometrics will become the standard security process for all enterprises. Such developments will lessen the disparities between companies' security systems.

Security – Implications for the Consumer

- Consumers expect security but are not prepared to spend money or time on making sure that their data is secure. Brands will be the first to blame for any security breaches. Consumers want to do little more than remember their password (and many will use biometric security).
- Trust is a key part of the consumer security experience. Consumers may be distrustful of brands that have had high profile security breaches or who do not proactively communicate their security ethos and policy.
- Consumers will increasingly expect tailored, multi-faceted security solutions that are relevant to the type or importance of the data being stored. Businesses must avoid a one-size-fits-all security strategy when engaging consumers with multi-cloud services.
- Knowledge of security, and the cloud in general, is very limited among consumers. Consumers want to know that their data is "safe", accessible and not being viewed by unauthorised eyes. The actual way that data is secured may be overwhelming to consumers, so simplicity of language and communicate will be increasingly vital.
- Just like enterprises, consumers will store some vital information on the cloud and duplicate it on their local machines. Growing consumer demand for multiple failsafe mechanisms will be a significant driver for the uptake of both hybrid and multi-cloud services. Cloud service providers will increasingly have to make such best-practice behaviours mandatory. For example, enforcing the duplication of critical documents/files across multiple storage systems.

Outlook: Talent and Technology must go Hand in Hand to keep Businesses Safe

Security is an area that will only become more important with the continued development of the multi-cloud. While the larger cloud providers offer security services as part of their cloud provision, there are still gaps. This requires engaging third-party security that can operate across multiple clouds. Maintaining security skills across multiple clouds will become increasingly vital as many enterprises find themselves under-equipped to deal with the pressures of keeping pace with technological innovation. It is also essential to bridge the gap between the executive boardroom and those responsible for security decisions. Nevertheless, adopting a multi-cloud route does not have to mean compromising security. With advanced security solutions, businesses can safely move their applications to any cloud model that works best for their strategy without geographic or infrastructural constraints.

Coping with Compliance and Infrastructural Complexity

Inconsistent and shifting regulation can cause problems to both CSPs looking to open data centres in new locations, as well as enterprises seeking to expand internationally. The GDPR in Europe is posing new challenges to the way data is stored, whereas regulations in other parts of the world can be vague and potentially hard to comply with. A distrust of storing data in the United States, can also be a factor in how enterprises develop their multi-cloud strategy (as influenced by the CLOUD Act). Infrastructure variables can also be a major factor in multi-cloud uptake – especially in the context of the availability of data centres and the reliability of bandwidth. Europe is mostly well served by the major CSPs. Africa and the Middle East less so, leading to different cloud choices and different levels of multi-cloud adoption.

Complex Regional Differences in Adoption

"Every country has got very specific dynamics around the embrace of cloud. The phrase that we use is 'cloud is not a country'. The benefits are experienced very differently by different markets," says Arthur Goldstuck.

In the EU, the GDPR will play a large part in changing multi-cloud adoption, while different data sovereignty laws across Africa and the Middle East will also prove influential. The availability of data centres and other technologies also impact multi-cloud adoption. For example, Africa has very low AWS adoption rates due to infrastructural constraints.

Unregulated Multi-Cloud?

Regulation of the multi-cloud itself in the West can be difficult, but developments like the EU GDPR will still put pressure on enterprises to make adjustments.

"People are reticent to hand out data other than to trusted vendors and they will want a pretty encompassing GDPR compliant capability," says Stephen Leece, Managing Director of Citilogik.

On the other hand, the perception of regulation as an inhibitor still persists. In the Cloudify/IOD State of Enterprise MultiCloud Report, 20% of respondents cited processes and regulations as the biggest hindrance to new technology adoption.[37]

Data Sovereignty Concerns

Every country has different data sovereignty regulations that affect cloud adoption. For example, in Saudi Arabia the financial sector has to keep everything within the boundaries of the country, so they opt to use service running on local service providers like Saudi Telecom.

---

[37] Cloudify/IOD State of Enterprise MultiCloud Report, 2017

The specific legal framework around data sovereignty in Saudi Arabia is relatively similar to the GDPR. CSPs are not able to move data of a certain sensitivity outside of the country and must notify their customers of any transfer of data.

Saudi Arabia's Cloud Computing Regulatory Framework (CCRF) is another initiative that could have far reaching impact. Here, CSPs have the responsibility to remove any "unlawful or infringing content", which is defined at their own discretion, as well as that of the Communications and Information Technology Commission.[38]

Regulatory inconsistency throughout the Middle East and Africa could also lead to compliance gaps for both CSPs and enterprises operating in the region. The creation of new public sector bodies offering cloud services could be an alternative to the potentially unregulated CSPs. As a case in point, the UAE's Telecommunications Regulation Authority has been able to offer public cloud services, including IaaS and email as a service, to governmental and semi-governmental bodies as part of a marketplace[39]. This type of model could standardise the way companies interact with the public cloud, as well as ensuring compliance.

Regulatory Impacts on Multi-Cloud Uptake

The necessity of storing some data both locally and internationally will pressure many enterprises to be multi-cloud, whether they like it or not.

"I don't think that any time in the next 10-15 years you are going to be in a situation where Amazon or Azure is going to be present in every single country in the world. Therefore, by necessity, organisations will need to have multi-cloud," says Mohammed Owais.

Another impact of regulation on multi-cloud adoption, especially in the Middle East, is the occasional stipulation that certain types of data must be stored on private, clouds. Enterprises could be reticent to pay for multiple public clouds, on top of a private cloud.

The EU GDPR, meanwhile, may force companies to make difficult choices and keep their cloud provision within certain boundaries, which could impact on multi-cloud adoption.

"The privacy issues with GDPR make it easier to leverage a single cloud solution, so I think that is going to drive a lot of decision making in terms of whether they're going multi-cloud or not," says David Linthicum.

More than ever before, businesses must be assiduous and empathetic to the trust customers place in them, as well as their duty to mitigate against an increasingly complex cybersecurity threat landscape.

Training programmes should already be in full swing, ensuring data privacy nuances are grasped and staff understands their role in keeping all forms of data safe. This should be supported by substantive policies concerning data handling and customer interaction. Sustained credibility in this space is difficult to achieve but can ultimately serve as a launch pad for better service innovation and profit.

---

[38] CITC Cloud Computing Regulatory Framework, CITC.gov
[39] https://gulfnews.com/business/sectors/telecoms/tra-creates-a-marketplace-for-cloud-services-1.2104509

Infrastructural Issues

“Bandwidth is probably the most limiting factor for the use of cloud in general and multi-cloud in particular. Although that is being addressed very, very quickly all over the place,” says Toni Prince.

This all leads to a situation where countries have to demonstrate their engagement with the cloud, in order to be provided with data centres. To do that, they need to take significant infrastructure risks. This “catch 22” may be another limitation on cloud uptake.

The presence of data centres across EMEA also affects multi-cloud uptake.

Roy Illsley provides an example. “How many Amazon datacentres are there in Madrid,” he asks. “None. Amazon builds the data centres to meet the demand, but it’s a bit of a chicken and egg. If there are no Spanish data centres then is Spain going to use the cloud? So, there are still quite a lot of areas of the world where cloud adoption is lagging.”

Toni Prince also points to areas where the physical cabling is located can make a big difference. “For example, countries that are on the coasts of Africa, around where the cable passes, are more or less okay, and those inland are less open to connectivity,” he explains.

Arthur Goldstuck sees infrastructural issues as being a key determinant of uptake.

“The presence of data centres is a key driver of cloud uptake trends across Africa,” he says.

While the availability of data centres from the larger providers in Africa is low, there are two proposed Azure data centres in South Africa. AWS has a single data centre proposed for Bahrain, and Azure has two for UAE, implying that both brands have a vested interest in competing to be the primary provider in Middle East region.

GCP has no publicly disclosed locations in either the Middle East or Africa, with the closest being in Mumbai. However, GCP has a secret data centre presence in Africa – possibly for security reasons – suggesting they are aiming to compete with Microsoft and AWS.

The presence of data centres and appropriate infrastructure can accelerate a region’s adoption of multi-cloud. At the same time, some countries are looking at ways of getting around infrastructure limitations.

“In countries where they have limited infrastructure it is really about leapfrogging those limitations. In Nigeria in particular, but also in Kenya, it is about gaining business efficiency and scalability,” says Arthur Goldstuck.

Future Challenges

Future regulatory changes are impossible to accurately predict, especially across a set of regions as diverse as EMEA. However, there are some recurring trends.

Overwhelmingly, there is a tendency in Europe and the Middle East towards consumer data protection. Recent legislation in some of the GCC countries, as well as the EU GDPR, suggest a trend towards consumers having more control over their data. Whether this will happen across Africa and in all Middle Eastern (and non-EU European) countries remains to be seen. Some African countries have strong data

protection policies such as South Africa's POPI Act. New issues and challenges will come to the fore as technology and cultures continue to change.

Issues with developing entirely new compliance strategies for each territory could lead to new platforms and services specific to a region's regulatory idiosyncrasies. The result will be third party services that standardise compliance across regions. These services will probably be delivered as part of the AWS or Azure service offering.

The impact on enterprises' internal organisation will also be transformative. The siloing of a company's legal and IT teams will be undesirable. There will be a growing necessity for the legal team to grasp which aspects of multi-cloud are touched by shifting regulations. Therefore, we should expect to see some future crossover between these departments.

Data often exists without borders, and the establishment of conflicting regulation from one country to another can lead to enterprises having to choose which regulation is more necessary to follow. For example, businesses storing UK customer data in the US may have to contend with both the US CLOUD Act and EU GDPR. In this case, the EU GDPR would take precedence because the data relates to European consumers, although certain interactions may be less clear in the future. The development of new regulations, for example the CCRF in Saudi Arabia, may cause conflict with established practices for many businesses.

Non-traditionally located data centres could also play a huge part in the accessibility of data for enterprises. Microsoft first attempted Project Natick in 2016, which entailed an underwater data centre powered by renewable energy (tidal energy and cooling from the surrounding water). This experiment was not an initial success, but Microsoft have announced a Phase 2 of the plan that could see it become more viable. The Natick Phase 2 vessel, "Northern Isles", was deployed in June 2018.[40]

Space could be the next frontier. ConnectX, for example, is a series of small satellites that stores digital currency. Elsewhere, SpaceX's recent launches suggest that the cost of sending material into orbit is declining.

If there is uneven regional distribution of data centres, there could be a clustering of businesses in certain areas. For example, if South Africa has Azure data centres but the rest of the continent doesn't, this could mean a relocation of enterprises in order to capitalise on connectivity and lower latency.

Implications for Enterprises

- The constantly shifting regulatory landscape presents a number of challenges, including significant awareness-raising and education programmes on data regulations and associated best-practice.
- Infrastructure limitations can inhibit the development of a multi-cloud strategy. If there is only one consistent and trusted data centre available, it will be difficult to develop a successful multi-cloud strategy. The development of more consistent and trusted data centres, potentially supported by government investment, will drive more multi-cloud adoption across EMEA.
- The preference for private cloud increases with certain regulatory difficulties, especially in places where data sovereignty is a difficult issue. The necessity of developing private cloud resources as regulations change can be a hindrance to the development of a multi-cloud strategy.

[40] Microsoft, Natick Research webpage

- Change is rapid. Certain areas can develop infrastructure very quickly, regulations can change rapidly and smaller CSPs can go out of business or lose data centres to attacks. It will be increasingly important for businesses to be agile and flexible.

Implications for Consumers

- The ability to access services in a certain geographical area will be complicated by regional regulatory differences. For example, a consumer accustomed to certain privacy rights may find those superseded by other local regulation.
- Constant education is needed from both government and business. For example, some consumers may not be aware of the intricacies of legislation like the EU GDPR, where they have significant data protection rights such as “the right to be forgotten”.
- Open and transparent communication of consumer rights on privacy regulation, especially within the EU, will be a core influence on the adoption and engagement with multi-cloud services.

Outlook: Time for a Global Standard

Enterprises can be impacted by local regulation and infrastructure in different ways. For example, bandwidth issues are most prominent in the Middle East and Africa, whereas the GDPR poses new challenges for anyone doing business in the European Union.

The FOMC report concludes that a global standard for data protection is needed within five years. Without it, there will be chaos. As ever, businesses should stay compliant with existing legislation. They should also not see it as a box-ticking exercise. It is easy to become mired in perceived regulatory impediments, blindly chasing compliance without heeding the bigger picture. Today’s tech-conscious consumers and customers will increasingly only want to work with the most trustworthy data handlers. There is a big opportunity to differentiate with best practice and service delivery, particularly in the context of multi-cloud’s potential.

Concluding thoughts

No single cloud solution will suffice in a modern digital world

Within five years, most businesses will need to be multi-cloud savvy for compliance, security, customer service, and basic competitiveness. Wavering technological laggards are likely to fall by the wayside. Automation, orchestration, and optimisation is now the mantra for today's businesses and governments.

Expect a number of milestone multi-could moments in the coming years where industries are reshaped, legislation is altered (such as a global standard for data protection) and entire societies benefit from digital transformation. Also expect challenges ranging from cyber-security threat evolution and a looming skills gap to infrastructural deficiencies. Multi-cloud uptake and benefits will have significant regional differences, but its overall trajectory and influence is unstoppable.

A faster moving future

The cloud is a powerful way for organisations to strengthen legacy infrastructure by customising their strategy to ensure that security, policy controls, skills, and business models are constantly attuned to the speedy rate of innovation.

Meanwhile, cloud providers are set to differentiate themselves through serverless capabilities and regional differences in data centre locations – all of which make leveraging multiple cloud providers a necessity to get the best results.

One of the noticeable disagreements among FOMC experts is the direction of open source.

While some experts claim that its adoption is in decline, others believe that it is flourishing and will only continue to grow. The fear of vendor lock-in, as well as access to more integrated dashboards, can complicate multi-cloud adoption and some experts say open source could help. Others feel that trust issues and the constant innovation rate of the larger cloud service providers could prevent further uptake.

David Linthicum, for example, sees open source's demise on the horizon.

"We still have a significant shift away from open source. So, we are coming to the demise of OpenStack, and a few open source players that are making it like Kubernetes. Those seem to be being pushed aside right now," he told FOMC.

In contrast, Eric Marks claims that open source is "getting more popular, not less. It's becoming more and more viable – you are going to have a full IT stack that is all open source components."

He goes on to suggest that a lack of open source options could hit the development of intelligent dashboards for various levels of abstraction (i.e. security, monitoring, compliance and containers), as well as the ability to communicate between multiple clouds. "There will be 'multiple panes of glass' – different monitoring systems for each aspect," he says.

The importance of automation

A dashboard that standardises security across cloud services may not do so across serverless architectures or may not cover all the flaws open to exploit. Nevertheless, for multi-cloud optimisation and governance, potentially encompassing single-pane analytics and automation will be fundamental drivers for multi-cloud optimisation and governance, potentially encompassing single-pane analytics. Real-time compliance and per-app services will be important to deliver strong performance and more efficient security to protect vital data.

The skill to scale on a per-app services basis is a strong prospect for the future of multi-cloud. With the right cloud orchestration solutions, organisations can now quickly deploy critical application and security services for every app, anywhere.

In the next five years, it is imperative that DevOps and NetOps work more collaboratively and embrace change in work practices to better control the cloud and keep pace with increasingly sophisticated cybercriminal behaviour and an evolving attack surface.

More security gaps will emerge over time and place multi-cloud users at greater risk. With no security standardisation, many enterprises may have to adapt their security strategies to function across new platforms.

Keeping control

No single cloud option best serves all infrastructure demands. The era of cloud migration is swiftly accelerating, and the future of the multi-cloud world is set to open a wider spectrum of profitable opportunities for businesses to achieve improved agility, greater scalability, better aligned operational costs, as well as a clearer focus on business retention and expansion. With advanced security combined with cloud automation solutions, organisations can dramatically improve their ability to efficiently orchestrate cloud usage and manage their operations more effectively.

Deal with disruption

The FOMC report highlights that skills need to swiftly evolve, and cloud architects will have to master comprehensive solutions delivering panoramic visibility and analytics, highly intelligent and contextual awareness, as well as sophisticated policy controls.

With the future in mind, expect the unexpected. New serverless architecture will enable enterprises to cut time-to-market and enable simplification of processes, as well as function through intelligent automation and machine learning. As disruptive technologies emerge, EMEA organisations need to be prepared to undergo significant change to remain relevant.

Final Thought

Be prepared for the future of multi-cloud and expect the unexpected.

Appendix – Definitions

Multi-cloud: managing resources across two different clouds or more, regardless of location (i.e. multiples of public and/or private cloud; a mix of on-premises and public cloud with integrated platforms)

Hybrid cloud: The practice of integrating one public cloud, and one or more private or on-premises clouds.

Serverless: Serverless architecture involves running code through a third party service that eliminates the need for an enterprise to provision and keep up servers themselves. Serverless applications can be run in containers. The most famous is AWS' Lambda.

SDN/NFV: Software Defined Networking and Network Function Virtualisation are two similar network architecture technologies that work towards virtualising classes of network node functions.

SaaS: Software as a Service is a software licensing and delivery model where software is available to be used via a subscription model. One famous example of this is Microsoft's Office 365.

PaaS: Platform as a Service is a category of cloud computing services that provides a platform that allows customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.

IaaS: Infrastructure as a Service refers to online services that provide high level APIs that can run various infrastructure services such as security and scaling.

DBaaS: Data Base as a Service is a method of running a database via a cloud computing platform.

S3 Bucket: S3 is Amazon's cloud storage system. A single bucket is an area that can be used for storage.

GDPR: EU's General Data Protection Regulation, a set of policies that regulate consumer access to their data.

CLOUD Act: Recent U.S. legislation that asserts that U.S. data and communication companies must provide stored data for U.S. citizens on any server they own and operate when requested by warrant, but provides mechanisms for the companies or the courts to reject or challenge these if they believe the request violates the privacy rights of the foreign country the data is stored in.

CCRF: Cloud Computing Regulatory Framework in Saudi Arabia, which includes the rights and obligations of the service providers, individual customers, government entities and enterprises.

PCI: The Payment Card Industry Data Security Standard is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

POPI Act: The South African PoPI Act ensures that all South African institutions conduct themselves in a responsible way when collecting, storing or sharing personal information by holding them responsible if they abuse or compromise that information in any way.

Open Source: Software which is freely available and can be distributed and modified.

DevOps: A software engineering culture that aims at unifying software development and software operations within an organisation.

DevSecOps: The mindset of ensuring that everyone is personally responsible for security.

About Foresight Factory

Foresight Factory (formerly Future Foundation) is a consumer analytics company, specialising in trends. We blend data to predict and size commercial opportunity and have partnered with our clients over 20 years to help them be truly customer centric in their decision-making.

Our expertise is understanding what consumers worldwide want now and in the future and translating this into recommendations for brand management, product development, loyalty, customer service delivery and other key touch points on the consumer journey.

foresightfactory.co

About F5 Networks

F5 makes apps go faster, smarter, and safer for the world's largest businesses, service providers, governments, and consumer brands. F5 delivers cloud and security solutions that enable organisations to embrace the application infrastructure they choose without sacrificing speed and control.

For more information, go to **f5.com**

WE MAKE APPS GO FASTER. SMARTER. SAFER.