The Hitchhiker's Guide to Cloud Transformation

virtusa

Table of Contents
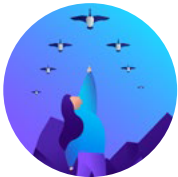
> # Space is big. **Really big.** You just won't believe how vastly, hugely, mindbogglingly big it is."
>
> **- Douglas Adams**

Although the cloud is comparatively smaller than space, most businesses still find working out the best way to capitalize on the full potential of the cloud mindboggling.

It's accepted that the cloud will deliver cost benefits, can dynamically scale, accelerate the pace of business, and foster innovation. However, there's little consensus about how best to achieve this. There's no single, right way to implement and operate the cloud. A company's strategic objectives architectural paradigms and level of cloud maturity all combine to shape the right way to build and run cloud- and this makes cloud adoption and exploitation complex. Really complex.

To help companies to adopt and get the most out of their cloud programs, Virtusa's Cloud Transformation practice has created this brief "Hitchhiker's Guide".

We hope you find our report interesting and useful.

Kris Canekeratne
Chairman and Chief Executive Officer,
Virtusa Corporation

Introduction

Cast your memory back just a few short years. Back then, enterprise computing predominantly meant bare-metal servers, switches, routers, hypervisors, storage, network, and middleware. Our choices were limited, and our technology options were driven by the choices that our peer groups were making and analysts' Magic Quadrants. In these simpler times, it was easy to define and secure the boundaries of enterprise computing.

Now, the enterprise computing world has newer guests, Cloud Service Providers (CSPs). CSPs (AWS, Azure, GCP) are investing billions in creating elastic storage and computing infrastructure. On top of this, they are creating compelling capabilities that can help you to build what, a few years ago, would have been considered unimaginable. CSPs have made public the same technologies that helped them scale and succeed and, more importantly, are building innovative tech solutions and components and making them available at a fraction of their previous cost.

Imagine building a video streaming app, mashing social media capabilities, and adding machine learning analytics, all in real-time. In the past, this would have cost a fortune and burned months. Now, using capabilities available from AWS, Azure, or GCP, an app like this can be built cheaply in days. This shift has fueled a technology revolution across the globe, as the rising number of tech entrepreneurs and unicorns show.

Planning a Cloud Transformation

Reimagine your business for the cloud computing era

by Bob Graham

Multiple surveys show that leveraging the cloud in the enterprise is among the top priorities for companies today. There are various drivers for this, varying from cost savings, increased flexibility, time to market acceleration, and beyond. It seems everyone these days is striving to put their "head into the cloud."

As we look at enterprises leveraging the cloud, we can see that we are in what is being called Wave Two of cloud transformation. Wave One consisted primarily of the "lift and shift" approach that was very focused on infrastructure benefits, typically with a single cloud provider combined with on-prem and/or private cloud. This wave was primarily driven by IT with a focus on virtualization and a goal of infrastructure modernization benefits. It was also characterized more by an ad hoc and experimental approach.

Wave 2 introduces a major shift in approach and a business transformation mindset. Rather than "lift and shift," we now see a focus on application modernization. Instead of an ad hoc approach, we now see the emergence of a cloud-first approach and top-down strategy. Rather than single-source cloud, enterprises are now going towards hybrid multi-cloud environments. Perhaps more importantly, organizations are now considering how cloud-native strategies can change revenue, improve customer experience, and allow them to bring new ideas to market and respond to customer demands more quickly. In today's ultracompetitive environment, businesses that can build and deliver applications quickly in response to customer needs will build enduring success.

Context	Cloud 1.0 Mindset	Cloud 2.0 Mindset
Approach	Experiment / Ad hoc	Define strategy to transform
Workloads	Lift and shift	Refactor, replatform, cloud-native
Cloud models	Single cloud / Hybrid	Hybrid multi-cloud
Cost / Value	Infrastructure savings	Cloud as driving business benefits
Compute model	Instances -> containers	Serverless & API
Modernization	Infrastructure modernization	Application modernization
Org impact	Technology only	Business outcomes

Unmet expectations

As we have moved from Wave One to Wave Two, the stakes, costs, and expectations have risen considerably. Many organizations have found that their cloud transformation efforts have not been meeting expectations. A study from QA Vector Insight[1] showed that most companies surveyed had major gaps in meeting expectations, with many categories having gaps that exceeded 50% of the anticipated benefit. These gaps exist in a number of categories, such as cost, customer experience, and resiliency.

Such a level of expectation gap speaks to a poor process in strategy and planning in cloud transformation programs today. Many faulty approaches rush to focus on doing a technical application inventory assessment and, from there, make cloud migration decisions. From our vantage point, a better approach to ensuring a strong cloud transformation plan is the one that considers both business and IT attributes and combines financial analysis.

Cloud migration expectation gaps

Culture
41% : 14%

Innovation
48% : 19%

Customer Experience
22% : 51%

Resiliency
62% : 28%

Scalability
62% : 30%

Efficiency
43% : 22%

Speed
57% : 30%

Cost
63% : 33%

● Target benefits
● Actual benefits achieved

Comprehensive due diligence

As most organizations are looking at hundreds and even thousands of applications when considering how to migrate their portfolio, we suggest a review of three areas from both macro and micro perspectives.

1 **Application Architecture**
Conduct a macro analysis to provide an application inventory with a functional and technical group along with data architecture and data asset inventory

2 **Business Architecture**
Create a macro business capability model (BCM) to show strategic and operational architectural context, including products, customers, users, and L1/ L2 capabilities

3 **Financial Analysis**
Analyze the spend by application and BCM L1
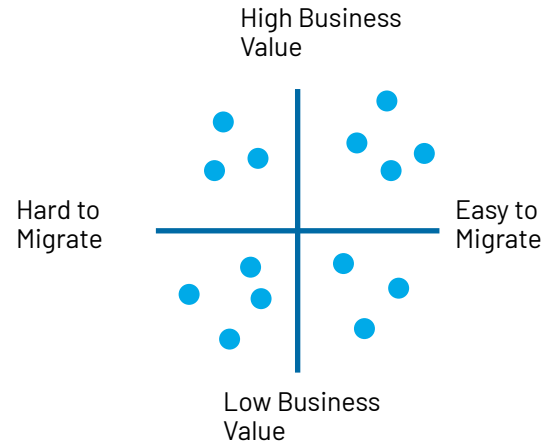
This macro analysis yields several deliverables. First, it delivers a comprehensive application inventory that, with a capture of business capabilities, can be viewed through both business and IT lenses, allowing us to generate a macro view of the business value and migration complexity.

Second, we are able to take this data analysis and create an initial 6R strategy (Rehost, Re-platform, Repurchase, Refactor, Retire, and Retain) by application and combine it with the total cost of ownership information to create a macro 6R disposition with cost and timeline.

6R status

This unique methodology then allows us to show this information in a business context. For example, we can answer the question that for a given capability, for example, customer onboarding, how many applications support this capability, and link the 6R status of all applications that support customer onboarding and align it in a roadmap view. This last point becomes extremely important in making decisions around migration. When the macro phase is completed, we can launch a micro analysis phase that will allow us to develop:

Application Architecture
Application component view, application infrastructure future state, data asset architecture

Business Architecture
L3 level 6R portfolio analysis

Financial Analysis
Rationalization options for application, infrastructure and data

6R Strategy	Time	Cost
Retain	⧗	$ $ $ $
Retire	⧗	$ $ $ $
Rehost	⧗⧗	$ $ $ $
Re-purchase	⧗⧗⧗	$ $ $ $
Re-platform	⧗⧗⧗	$ $ $ $
Re Factor	⧗⧗⧗⧗	$ $ $ $

Migration Complexity

Virtusa Cloud Transformation's approach enables us to look at business-specific workloads and determine which CSPs are the best match. Our unique methodology then ensures that both IT and the business can see their portfolios across different matrixes and with that make better informed decisions about how to proceed on their cloud journey.
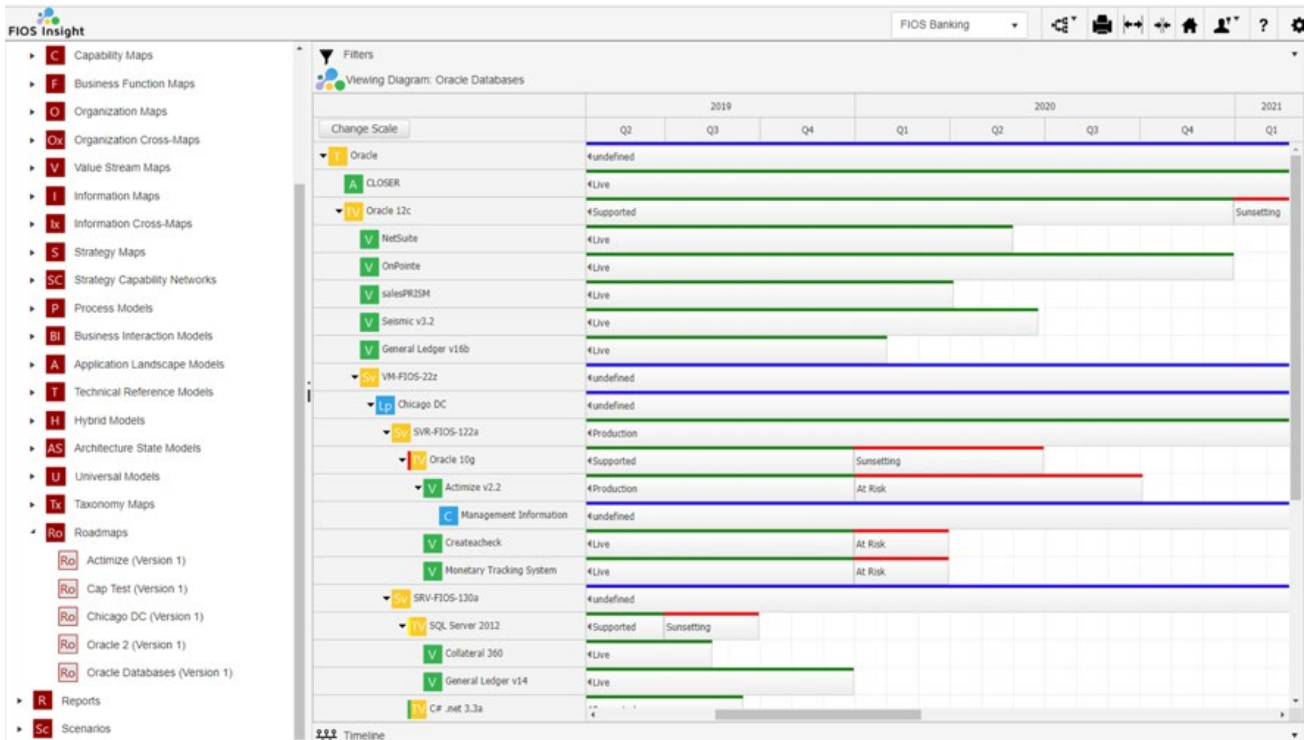
Lastly, a business capability driven approach easily allows organizations to drive to a microservices architecture and leverage container and orchestration technologies or serverless computing.

Applications built on microservices are ultra-scalable and can be more easily distributed across a compute environment and take better advantage of all that the cloud can offer.

How Virtusa can help

The ability to look at portfolio transformation roadmaps by business capability, applications, and then workload type while being able to see associated cost and timelines are elements of Virtusa's methodology for cloud transformation that set us apart. A second key benefit is that in today's rapidly changing world of cloud, it is very prudent to have a hybrid multi-cloud strategy.

Multi-cloud is important in particular because cloud service providers (CSPs) are building out unique platform features that differentiate how they can support different business capabilities and workloads. For example, a health care organization could take advantage of AWS' Comprehend Medical, which provides a natural language processing service that makes it easy to use machine learning to extract relevant medical information from unstructured text. This approach can be leveraged for a cloud refactor solution.

Virtusa's cloud transformation approach enables us to look at business-specific workloads and determine which CSPs are the best match. Our unique methodology then ensures that both IT and the business can see their portfolios across different matrixes and with that make better-informed decisions about how to proceed on their cloud journey.

Destination: The hybrid, multicloud world

by Senthil Ravindran and Narasimham H

Software is business now

Creative ideas are codified and hosted in containers that float through the seas of elastic storage and computing owned by Cloud Service Providers (CSPs). Until a few years ago, enterprises were running RFPs to select a CSP and mandated that their organization only leverage the chosen one. This worked well for choosing a commodity provider, where the only real difference was often just price. However, looking at the speed at which CSPs are evolving and innovating, the strategy of partnering with just one CSP has become outmoded. A more sensible approach is to develop a tech vision driven by business needs as different CSPs offer unique benefits. This calls for a hybrid approach.

A hybrid cloud model combines on-premise infrastructure with a public cloud. A hybrid model delivers the advantage of custom fitting the best technology to accelerate the implementation of new functionalities.

On-Premises / Private Cloud

- Predictable and secure
- Performance sensitive
- Mission-critical

Service Providers / Public Cloud

CSP'S
AZURE
GCP
AWS

- Scalable and elastic
- Cloud-native applications
- Corporate IT; Hosted

Multicloud means that you will be leveraging two or more CSPs, for example AWS and GCP, or AWS and Azure, or GCP and Alibaba Cloud, etc.

With a hybrid multicloud model as part of your cloud transformation journey, be aware of these five key prospects:

1 **Flexibility and speed**

2 **More effective self-service**

3 **Faster delivery of new products and services**

4 **Better cost control**

5 **Lock-in avoidance**

Flexibility and speed

The most vital gain of a well-architected hybrid multicloud is improved business agility. You have complete freedom to select the right cloud environment to suit development and testing needs, which means that you can quickly deliver new requirements or support new applications and deliver them based on the relative strengths of each CSP. Production loads can be replicated in a non-prod environment, which is especially useful during the early life of applications. Many trades experience material peaks and troughs in demands, which equate to peaks and troughs in demand for tech resources: for example, in retail during Thanksgiving, Cyber Monday, or year-end holidays. The issue of managing activity spikes is history given the cloud's ability to auto-scale on a pay-as-you-go basis, this also yields cost benefits when compared to traditional cluster maintenance approaches. The hybrid multicloud gives you the competence to respond flexibly to demands.

More effective self-service (= less work for IT)

A well-designed hybrid multicloud can allow IT stakeholders, whether they are developers or line-of-business leaders, to gain access to IT infrastructure and services through a self-service portal. Along with instant access to services, it also eases the load on IT, preventing bottlenecks, and enabling change execution and environment setup to be done faster than ever before.

Faster delivery of new products and services

Hybrid multicloud can assist in delivering new products and services quickly by eliminating the roadblocks that traditionally slowed development teams. New digital services become easier to create, deploy, and test (Functional Testing and Non-Functional Testing). Teams get better access to the resources they need when they need them. Companies are enabled to create best-of-breed solutions by selecting the best-fit CSP-provided service based on need.

Better cost control

A hybrid multicloud directs you to run every service in a pay-as-you-go model to help reduce TCO in infra and datacentre management. Designing datacenters to satisfy holiday or business peak loads will only lead to more idle time in the infra set up – a very old and poor choice compared to the ability to respond vigorously and elastically through auto-scaling. From a multicloud-specific perspective, this enables businesses to mitigate risks such as being locked into a vendor that is increasing the price of services.

Evade vendor lock-in

If your roadmap is a cloud-only direction, it would become highly impossible to avoid getting locked into cloud vendors. Retrieving data from the cloud can quickly turn expensive and so you need to be fully aware of the implications before moving or saving data from data centres to the cloud. Creating a decision matrix will help you make the best decisions about what to run on-premises and what to run in the cloud. Questions like Why cloud? Which cloud? Why not cloud?, will help you avoid vendor lock-in and will open doors to adopt a hybrid multicloud strategy.

As you plan to accept a hybrid multicloud approach, you should be prepared and flexible to make changes to your IT as and when needed. This is because obsolete and isolated infra stacks heavily depend on specialized IT crews with in-depth knowledge of technology such as networking, storage, and system administration, whereas hybrid cloud can be managed with IT generalists.

The move to hybrid eradicates much of the time spent dealing with routine user requests and trouble tickets, allowing your team to swing focus from infra administration to optimizing and growing your business-critical applications and services. This is a much better use of resources (and a far more fulfilling job for your tech team).

Summarizing the benefits of adopting a hybrid-cloud model

1 Operational excellence

One of the key paybacks of implementing a hybrid cloud solution is increased flexibility over your IT operations. As demands from the environment changes and new business requirements continue to increase, having the ability to reconfigure and fine-tune the cloud environment makes it easier to adapt to those changes with minimal or no disruption. We can continually improve supporting processes and procedures based on the significance of the process by getting ready for planned and unplanned events like sales promotions and their deployment.

2 Security through speediness

CSPs go to great lengths to make sure that customer data is protected by ensuring that the data in transit and at rest, both are encrypted. Hybrid-cloud also allows for the capacity to shield evidence and assets. This can be attained by performing due diligence for cloud readiness, which includes risk evaluations and resolving issues over routes, while having security controls over multi-tenanted network infra and applications through proper access and authentication controls, and accountability. Even if information is stocked in a private environment, there would be considerable interconnectedness between the private environment and public cloud, for data to be used by applications, data analysis and other such processes. Tactics like data masking, bit encryption and decryption would still be ensured to guarantee data security.

3 Scalability through consistency

Businesses now can pull the roomy supremacy of cloud computing to swiftly and proficiently increase the functional dimensions for their vital data, assets, and processes. Hybrid cloud offers the opportunity for companies of all sizes to compete with more traditional players sooner than ever before, by removing barriers to growth. Also, public cloud makes it easier to develop new applications by leveraging powerful analytics programs that can be beyond the competence of a small businesses.

4 Cost through consumption model

Datacentre operations need heavy lifting for racking, stacking, and powering servers.

This can be eliminated by using CSPs, which will ease TCO spending on datacentre operations and can focus on the customers' and organizations' forecasted missions. Hybrid cloud offers scalability and is a prominent alternative to a purely private cloud, which can be enormously expensive to update or expand over time. Implementing the hybrid cloud solution enforces some additional costs to establish a public environment but, in the long run, can significantly lower return on investment (ROI)

5   From one-trick pony to hybrid wonder-horse

The primary objective of every CSP is to convince companies that they are the best in town, move all their workloads into their public cloud, and then encourage them to consume as much storage and compute as possible. This is where they are hoping to become your "Preferred Cloud Partner" in marketing terms. But they have realized that for most large companies, this will never happen for a variety of reasons, ranging from cautious procurement strategy to avoid vendor lock-in to several others. All CSPs have unwillingly signed up to the reality that enterprises will always have some workloads on-prem, e.g., move something to AWS or build something in GCP and Azure.

Hybrid multi-cloud, if done correctly, can help you leverage the best of the CSP worlds, but will also increase the complexity of your enterprise technology landscape. Communicating across public clouds means there might be redundancies, latency constraints, overcomplicated Identity, and access management controls, exposing yourself to security vulnerabilities. **This is not for the weak-hearted.**

Cloud foundation

by Madhavan Krishnan

Getting the basics right:

The setup of the cloud foundation is as important to any company's cloud adoption journey a physical foundation is important to a building. Logically, without a strong foundation, your future cloud workloads could tumble to the ground.

When we consider the elements of a cloud foundation, we need to think about:

1 Core Cloud Services

2 Cloud Management

3 Network & Security Services

4 Acess & IAM

5 Application Services

6 DevOps

7 Finance Services

In addition to these elements, we also advise that the setup of a cloud foundation also includes a **cloud management platform**. This simplifies the management of ongoing operations in the cloud, especially given the rising popularity of complex, multi-cloud platform deployments.

In contrast to the foundation of a house, which in the vast majority of cases only needs to be altered in extreme circumstances, cloud foundations need to be constantly reviewed as the needs of the business, policies, technologies, and standards shift (on what often feels like a daily basis).

Building the right, comprehensive cloud foundation ensures the long-term success of your cloud program.

Cloud foundation services are categorized into four main areas:
- Core services = Network services
- Security services = Access, authentication, and authorization
- DevOps services = Application services
- Cloud management = Operational services

These services offer inbuilt guardrails for developing, migrating, and running cloud operations and ,ensuring security and policy compliance. In a well-managed cloud infrastructure, the majority of these services will be configured as code and automated, which makes deployment and operation more efficient.

What to focus on next

1 Evaluate the critical steps of cloud foundation and start implementing those in phase one

2 Keep track of all remaining cloud foundation services not covered in phase one and look to implement those as soon as possible

3 Conduct workshops with application owners to understand and finalize the baseline environments, tools, and technologies which should be standardized across the organization, including approval from the security team
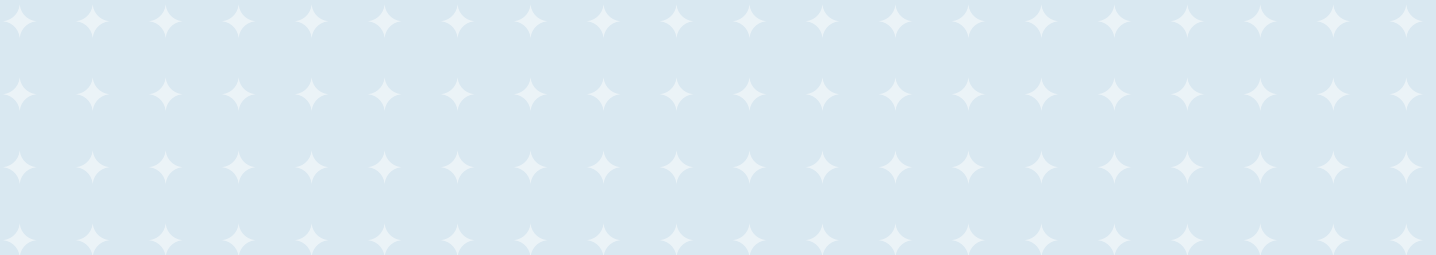
Augmenting CSP's services with best-in-class tools to help you build a better foundation

Virtusa's approach to designing and implementing cloud foundations leverages three types of assets. First, we draw on the ever-evolving and expanding capabilities and services of CSPs. To this, we add Virtusa's home-grown accelerators, such as Virtusa's Cloud Management Platform (vCMP), to bring in consistency and operational flexibility for managing hybrid / multi-cloud deployments. Lastly, we select the best open source tools on the market. Combining all three elements enables Virtusa to work with clients to accelerate the delivery of a cloud foundation that balances best in class and bespoke elements.

CHAPTER 2

Migrating to the Cloud

Securing a boundaryless organization

by Madhavan Krishnan

A framework for securing your business in the era of continuous cyber attacks and privacy laws

Now that we're in the cloud age, the traditional cybersecurity practice of protective firewalls installed on-premise with a DMZ and trusted networks has become irrelevant. Cloud adoption means the adoption of a highly distributed environment. This means operating in a virtual ecosystem with no specific boundaries; the old security paradigms just don't hold up here.

Four key trends are pushing enterprises towards a boundaryless model:

1 Mobile Workforce

2 Cloud Adoption

3 Collaboration with Partners

4 Internet of Things

Mobile workforce

Mobile devices are ubiquitous in the office, whether these be company assets or BYOD devices, and organizations have been quick to recognize the value of corporate mobile apps that give them access to remote workers (or access employees 24/7). Yet it's not all good news. Mobile devices open weak entry points in an organization's network. An attacker can remotely monitor them for sensitive information, passwords, account data, etc. and accessing a stored password on a mobile device can give bad actors access to an organization's sensitive resources. Virtual private networks (VPNs) once provided encrypted connections for remote users. However, VPNs offer access to almost any internal system or data, which is too dangerous in today's digital business age.

Internet of Things (IoT)

With IoT, devices deployed at different locations connected to various networks gather, communicate, analyze, and process information. However, this also creates a new attack surface, and there is potential for IoT data to be completely compromised. In some cases, sensitive data, such as patient health-related information, maybe unwittingly shared, and as each new link is added to the IoT ecosystem, security risks become exponentially greater.

Collaboration with partners

In today's digital age, companies are compelled to share some level of network access with vendors and partners to do business effectively. Unfortunately, these third-party connections create substantial cybersecurity risks. They could open the door to an attack via what is assumed to be a "trusted connection" with authorized access from Third Party Provider's end and vice versa.

Cloud Adoption

Cloud adoption is also ubiquitous and brings new threats that span across IaaS, PaaS, or SaaS adoption. A July 2018 survey by Forrester found that 86% of respondents characterized their organizations' cloud strategy as 'multi-cloud'[2]. Although every cloud service provider is actively investing and managing security, the "shared responsibility model of security" in a multi-cloud architecture means that no CSP is entirely responsible for the security of cloud assets. For example, securing the data layer is always the responsibility of the customer. According to Gartner, "Through 2025, 99% of cloud security failures will be the customer's fault."[3]

Identify a security strategy

Given these four new risky access points, it is imperative to introduce a new layer of security to outpace this rapid adoption of IoT, social, mobile, analytics, and cloud (ISMAC) technologies. Some of the high-level strategies to secure such boundaryless organizations are:

1 Zero Trust Systems

2 Identity and Access Management

3 Data-Centric Security approach

4 Endpoint protection

5 Threat Intelligence, Monitoring, and Alerting

Zero Trust systems

Traditional IT network security is based on securing boundaries. This approach makes it hard to access systems from outside the network, but insiders of the network are trusted by default. The problem with this approach is that once attackers gain access to the network, they have unfettered access to everything inside.

A Zero Trust network strategy assumes no users or machines can be automatically trusted, as there are attackers both outside and within the network. No entity is trusted by any other entity without authentication. Zero Trust network strategy is a holistic approach with no single specific technology associated with it; it is an incorporation of several different principles and technologies.

One of the principles of Zero Trust is segmentation, which is the practice of breaking up security perimeters into small zones to maintain separate access for discrete parts of the network. For example, separate subnets and access and routing policies can be established within cloud virtual networks that utilize segmentation. A user or entity with access to one of those zones will not be able to access any of the other zones without separate authentication.

Zero trust systems need to be monitored to check how many different users or entities are trying to access different resources and from which devices, locations, etc. This approach can be made more effective by coupling it with AI/ML aided behavioral analytics that can implement risk-based access controls to sensitive critical/high privileged resources.

Identity and access management

The difficulty of authenticating users will only increase as mobile use increases, and IP protocols spread to other areas of the organization. Identity and access management identifies individuals and entities and controls their access to the resources by associating both user rights and restrictions.

Whether the identity directory runs on-premise or in the cloud, its integration with various apps and security tools is critical. It defines policies that users, entities, and devices are allowed to execute on the network, and the role-based action users can take, which can be additionally dependent on device type, location, privileges, and other factors.

Data-centric security approach

With no specific secure perimeter for organizations to safeguard, developing cybersecurity strategy from network-centric toward a more mature data-centric. Content is to be analyzed at the point of creation to classify its sensitivity. The main criterion of data-centric - security is classification and encryption to protect data wherever it resides and moves. Then restricted access controls must be applied appropriately so that only those users/entities with the proper business need can access it.

Discovery and Classification

The development of a data-centric security strategy begins with a thorough assessment of the types of data held by the organization and an evaluation of which data needs to be protected. Data discovery is the process of scanning files, folders, and databases, and comparing the contents with an organization's predefined sensitive data rule-set. After discovery, the classification of sensitive data, such as intellectual property, financial data, and customers' personal information, helps organizations design a practical data protection strategy.

Encryption

Encryption using a strong algorithm such as AES-256 (the advanced encryption standard) is the most effective way to protect sensitive data against breaches. Key management systems should be in place to ensure authorized users can decrypt and use the data they need while also restricting unauthorized users.

Data must be encrypted when transmitted across networks to be protected against eavesdropping or MITM attack of network traffic by hackers. The types of transmission may include server-to-server, client-to-server, or any data transfer between core systems and third-party systems.

With a data-centric security strategy, IT security can become an enabler of future innovation, rather than an obstacle to business as usual.

Endpoint protection

Endpoints such as notebook computers, tablets, or smartphones are prone to attack. Hackers target to penetrate corporate systems where users access the data, and these are the places where they may "exfiltrate" their data from unauthorized threat actors, intentionally or unintentionally. Endpoint security solutions protect devices from malware, enforce various company policies, and provide secure connectivity. This is where data access and sharing can be detected, and user behavior can be gathered to drive analytics.

Threat intelligence, monitoring, and alerting

Customers now must manage the security of a multi-cloud architecture from a unified perspective. Interestingly, a recent development is Google's Anthos, and Microsoft Azure's Arc (currently in Beta), which not only allow organizations to run applications on-premise and in the cloud, but also securely manage workloads running on third-party cloud providers, giving organizations the freedom to deploy, run, and manage applications on the cloud of choice.

Real-time global and local threat intelligence is shared across the distributed network and is analyzed and orchestrated through a central management console for a fast, efficient response to even zero-day attacks.

A good governance system enables data tracking, ensuring tracability to exactly where the data resided and who has accessed it, and helps to demonstrate compliance with any regulatory requirements.

Virtusa's Cybersecurity Initiatives

Virtusa, in collaboration with its technology partners, has developed a robust portfolio of solutions and services to secure boundaryless organizations.

Virtusa has extensive experience in delivering identity and access management solutions across federation and cloud enablement, authentication and access control, ID governance, and architecture. Virtusa's IAM offerings have defined access policies, apply the principle of least privilege, separation of duties, support role-based privileges, MFA, single sign-on (SSO), and have AI/ML ingested user entity behavior analytical capabilities and an automated workflow to identify any unauthorized activity and alert the stakeholders concerned.

Virtusa Threat Intelligence Service (vTIS) monitors the internet to collect data of 3 Billion IP addresses, all global domains/subdomains, paste-bin leaks, dark-web, honeypot data, etc. to discover and monitor digital attack surface and potential breach risk and validates compliance of NIST 800-13, FISMA, ISO27001, PCI-DSS, and GDPR among other regulations. vTIS also enables enterprises to monitor corporate cyber risk posture as well as third party ecosystem risk posture, performing non-intrusive cyber risk assessments to convert data to risk intelligence in the form of a scorecard.

Virtusa's NextGen Security Incident and Event Monitoring uses AI/ML for data processing, data visualization, and incident reporting. It provides live monitoring of unusual activities across infrastructure, user and entity behavioral analytics, and automated workflows to email and SMS the asset owner.

ARTICLE 5

Regulator's perspective

by Kumar Raju Kosuru

Regulators around the world are embracing global change with the advent of cloud computing and open data. A real wave of cloud usage, which began in the early 2000s, has provided several businesses with scalability, efficiency, and on-demand content management. Businesses are now moving towards a cloud-first strategy with end to end technology supported by cloud providers. Today, over 80% of the businesses have a multi-cloud strategy with year on year growth of over 6% by simply adopting cloud[4]. There is an ever-increasing number of demand for companies to move towards cloud ranging from monolithic enterprise products to emerging FinTechs. On the contrary, public organizations are now looking to adopt the cloud to leverage benefits gained through advanced technologies such as Machine learning and data analytics.

However, these cloud solutions are increasingly dominated by a few cloud providers that we now call the Big 4 – Amazon, Microsoft, Google, and Alibaba.

These global players are now well known for eavesdropping, selling sensitive data such as health records, and racing towards a global market share. There are now global alliances being formed to compete against each other. In June 2019, Microsoft partnered with the competitor Oracle to take on Amazon in the cloud market. Understanding these changes at a macro level is critical for regulatory bodies around the world. In Dec 2012, ENISA, European Network, and Security Agencies released guidance on Cloud computing, highlighting benefits, risks, and recommendations for information security. In Feb 2019, EBA, European Banking Authority, released guidance9 on outsourcing arrangements with an emphasis on governance framework and outsourcing process when engaging with technology providers. Guidance from public bodies can provide evolving regulatory views; however, risks involved in cloud adoption, particularly complexities with the public cloud cannot be ignored.

While the public cloud adoption has received more scrutiny compared with the private cloud, a review of the market trends by Synergy Research Group[5] shows that market adoption of the pubic cloud grew by 37% from the third quarter of 2018.

Public Cloud Services – Market Share Trend
Public IaaS & PaaS - excludes Hosted/Managed Private Cloud

Source: Synergy Research Group
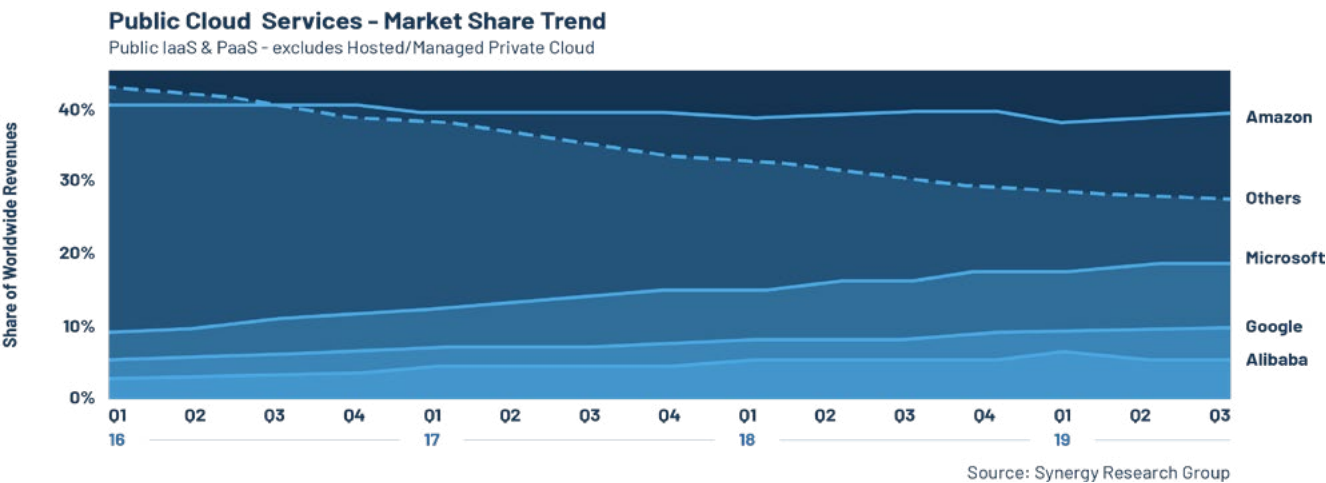
The growth potential of the public cloud market and reliance on the Big 4 technology firms need similar experimentation and industry tests like the ones conducted for medical treatments. Solutions need to be tested for possible benefits, side effects, and long-term sustainability.

Tenets of trust, reliability, and control

On October 2019, Angela Merkel has expressed concerns about outsourcing data to US companies and unveiled a plan for 'digital sovereignty' with the European cloud computing initiative, called Gaia-X7. In the same period, an FT investigation revealed that some highly personal health information that internet users enter on websites was being transmitted to Google's advertisers, raising further questions[6].

These developments and investigations continue to provide more transparency on how technology companies such as Google operate, thus providing real examples for reforming regulatory framework and policies.
Any application migration to cloud requires assessing the regulatory risks not just at the project start but as an adaptive risk management during the entire lifecycle.

A new cloud world needs to exhibit the qualities of trust and reliability while providing control back to the public or government. In essence, technology cloud solutions should be componentized and viewed in parts without the provider having control. It is critical for the cloud adoption program to adopt a framework that is in line with the local regulatory framework on IT outsourcing.
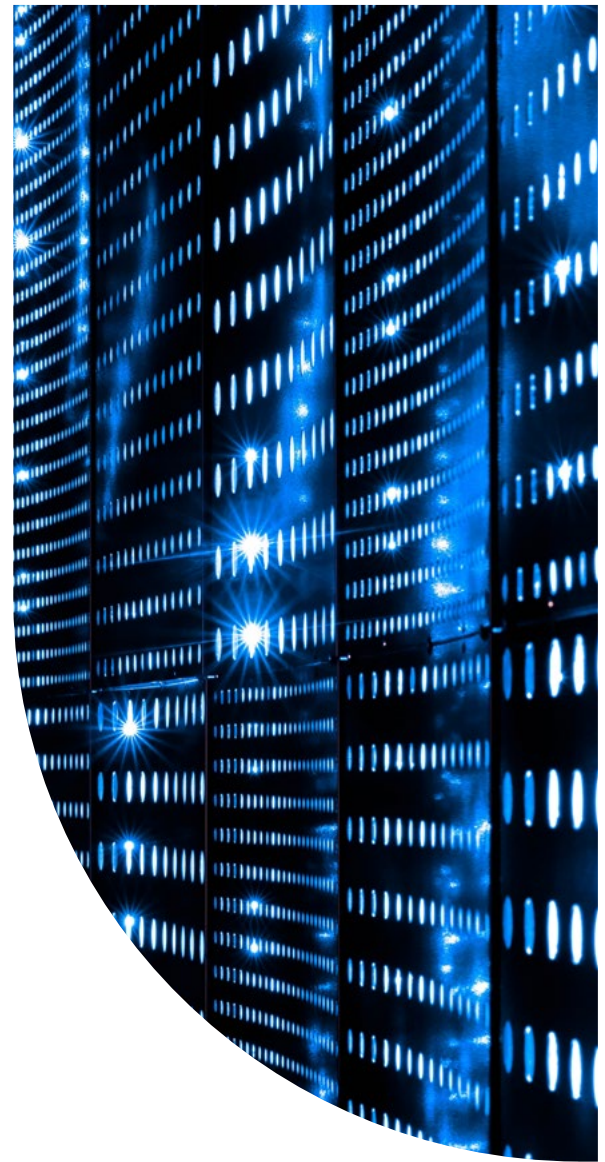
Below framework from Virtusa illustrates how such risks should be viewed as tools for adaptive risk management,

Tenets of risks	*What can go wrong?	Why?
Trust	Availability of chain	Reliance on internet connectivity and single points of failure
	Loss of ownership	Potential of ceding ownership
	Management interface compromise	Increased risk of management interfaces over the public internet
Reliability	Lock-in	Limitations on data, service and application pordability
	Malicious insider	Though unlikely, it is important to classify certain roles as high risk
	Isolation failure	Failure to provide separate storage, memory, routing and reputation between tenants
Control	Data protection	Unable to prove if data is handled in a lawful way
	Insecure or incomplete data deletion	Adequate and timely deletion of data may be impossible
	Data sharing for commercial purpose	Complicated web of data sharing and influence on consumer activity

*Source: ENISA Report[7]

Regulatory risk assessment

Adaptive risk management requires an ongoing agile approach to monitoring and assessing the risks. Post financial crisis of 2008, the regulatory landscape has drastically changed and enforced the banks to report against any potential defaults on the derivative products. In the context of the cloud, though there is no such guidance on reporting standards, any cloud migration needs to maintain an incremental audit of risks and the likelihood of a negative impact. Cloud solutions need to be loosely coupled with a backup strategy in the event of foreseen risks. Hence, application migration to the cloud would need a comprehensive risk mapping for every use case. An illustration of such mapping is shown below with high and medium risks are highlighted in the table.

Trust (loss of ownership)

	Probability of Incident	Very Low	Low	Medium	High	Very High
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Reliability (isolation failure)

		Very Low	Low	Medium	High	Very High
Business Impact	Very Low	0	1	2	3	6
	Low	1	2	3	4	6
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

*Source: ENISA Report[8]

Virtusa with its clients across the globe and partnership with global cloud providers continue to evolve the framework and tools that are required for the adaptive risk management for cloud adoption. A combination of our engineering culture and domain expertise fuels the needed change in businesses towards risk-managed cloud adoption.

Migration factories

by Kumar Raju Kosuru

Developing a cloud migration factory and an agile "start right" approach

All businesses have IT estates that include multiple applications, multiple flavors of hardware, and multiple data centers. It often seems like a "no-brainer" to migrate this complex tangle of tech into the public cloud, where it can be magically transformed into an elegant and flexible cloud-native estate. Rather predictably, there is no magic approach to migration, which means that businesses need to make tough decisions about what, how, and when to migrate elements of their existing estates into the cloud. Adopting a Cloud Migration Factory approach helps companies make these decisions easier as it offers a way to prioritize migration roadmaps based on its immediate value and the extent to which the migration will help the organization progress towards their longer-term strategic objectives.

The factory approach can be applied to hybrid, multi-cloud, or single CSP architectures and enables businesses to increase the agility of their tech while delivering cost reductions associated with reductions in IT operations spend and capital investment in hardware. This approach also helps companies to rapidly develop highly virtualized enterprise systems that run across private and public clouds and integrate third-party enterprise applications and service environments at the edge.

At its heart, adopting the factory approach involves a fundamental shift away from focusing on tech components and towards the business services that they support. This business value focus is then reflected in each of the five key linear steps in the migration process:

Vision & Strategy

Ensure alignment with business and IT strategy

Assess & Plan

Assess portfolio for cloud suitability and cloud migration viability

Design & Build

Set up a secure cloud environment based on workload requirements

Migrate & Validate

Transition workload to the cloud environment

Run & Optimize

Manage the cloud-based systems, including service
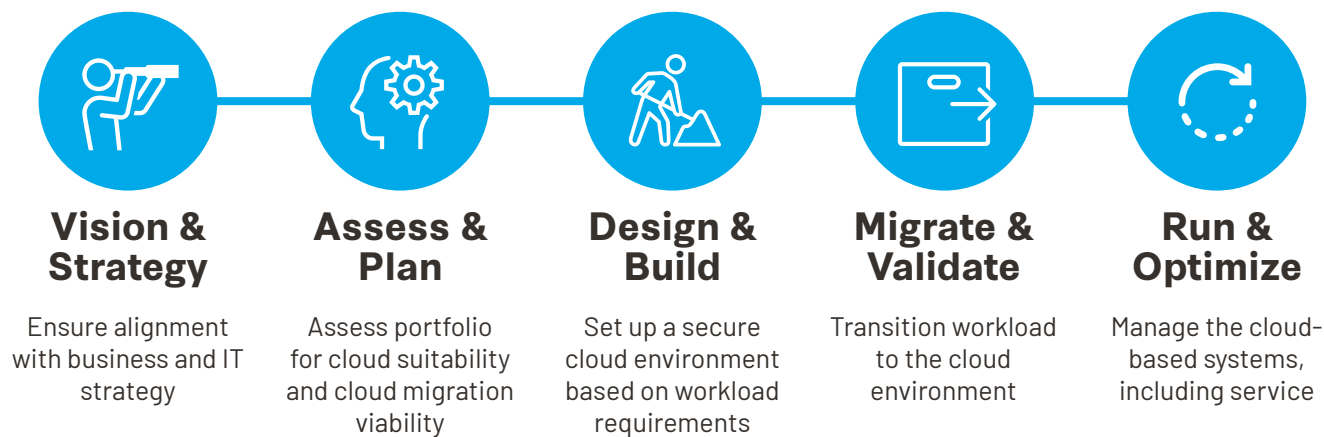
Vision & strategy

Assure the businesses' wider priorities are reflected in the framework that you're using to prioritize migration. These could include a short-term focus on cutting cost, reducing reliance on aging technology, or could reflect a long-term strategic objective to enter a new market that requires specific technology or data.

Assess & plan

Using a framework such as a business capability model, which we covered earlier in this book (see Reimagine your business for the cloud computing era), businesses can rapidly evaluate their tech portfolio to create a prioritized long list. This additionally factors in not only the value created by the system but also the cost of change associated with migration.

Design & build

Evaluate the cloud architecture that best positions you to deliver your organization's roadmap, rather than delivering siloed, individual solutions.

Migrate & validate

Use planning and migration tools to structure and assure an effective migration.

Run & optimize

Work with your cloud team or managed service provider to track and iteratively perfect your performance and manage TCO.

Discovery of the entire application landscape

The application portfolio assessment approach and model is proven and tested across large-scale cloud migrations very successfully. We understand that each enterprise has specific nuances, and this methodology will be adapted to meet those requirements.

Building the foundation for cloud migration

Building a comprehensive cloud foundation is essential to the longevity of workloads that will be deployed. The following services offer predesigned guardrails for building, migrating, and running cloud operations, in a secure and compliant setup. These services in well-managed cloud infrastructure will be configured as code and automated to a large extent. Virtusa will bring in a tried-and-tested set of tools and accelerators with best practices to come up with the cloud foundation design in the shortest possible time.

Migration Factory Model

The cloud migration factory model employs repeatable processes and re-usable artifacts for migration. The model identifies and aligns with organizational platforms (infrastructure and applications), architecture blueprints, policies, and guidelines – all to provide balanced cloud portability. Virtusa has an automated solution approach for many of the migration patterns and architecture blueprints that can accelerate our client's cloud migration journey by 25-30%, from both the time-to-market and cost of migration.

The Cloud Migration Factory Model

Executive Sponsors & Steering

PMO, KPI, Metrics and Governance

Migration Factory Framework

Public Cloud Migration

Private Cloud Migration

Assessment Report

Cutover

Migration Planning	Design, Build & Migration Factory		Test Factory	Deployment Factory
	Solution Blueprint	HLTD Construction		
Product Owner	Application Migration	Security Audit/ Scan	Functional	Budget Mgmt
Scrum Master	Pre-production build	Production Build	Integration/ regression	Release Mgmt
Scrum Team	Data Transfer	Network Design	Performance	Deployment & Rollout

Shared Team (Scrum of Scrum)

Architecture | Platform | Security | Program Mgmt | DBA | TDA | DevOps

Operate

Virtusa offers an end-to-end portfolio of services to manage every aspect of your applications running in the cloud. Our full-stack cloud monitoring and management solution will employ best-of-breed tools and industry frameworks to support a 24/7 operation. Virtusa adopted this approach to support its clients' requirement of managing hybrid / multi-cloud deployments. Virtusa operates multiple state-of-the-art global cloud command centers to support all our clients across the globe.

As digital and cloud technology becomes more critical to growth and innovation, business users will be able to draw on data and application services quickly to launch new products and services, gaining first-mover advantage or as a way to catch up to the competition. Virtusa's deep experience in cost management minimizes the cost and duration of cloud projects.

Running your cloud

DevOps on steroids

by Brian Shaw

Quickly and reliably delivering change is critical for all businesses.

Long-standing practices and policies around cybersecurity, governance, regulatory mandates, and data protection have turned the process of releasing even the smallest changes to our customers into a seemingly never-ending process which can take months to navigate. Sometimes is can feel as though we're under control of the officiously bureaucratic Vogons from The Hitchhiker's Guide to the Galaxy.

DevOps offers us a set of practices to improve the way we deliver change. To do so, we must break down the traditional organisational silos of responsibility and the proverbial wall which exists between our software engineers and operations teams. We have all read countless articles about the success stories and benefits of adopting DevOps, but it seems many of us get stuck in even knowing where to start or how to navigate the seemingly endless ecosystem of tools, patterns, and approaches available. We need something more prescriptive.

Site Reliability Engineering (SRE), coined by Google as a way of operating production systems, is becoming the prevalent way to implement DevOps. SRE places a focus on software engineering and operations as a way to achieve speed and reliability at scale and provides us with a stronger framework to operate more effectively[9].

The original leaders of the DevOps movement coined the acronym CALMS to describe the pillars of the philosophy - Culture, Automation, Lean, Measurement, Sharing[10]. The five pillars of CALMS will help us navigate our way to embracing SRE and implementing DevOps by creating a culture of trust and sharing, using tools and automation to our advantage, and constantly measuring performance and adjusting our approach.

A Culture of Trust

Culture based on trust is the foundation to DevOps success. Trust enables breaking down silos and shifting ownership and responsibility from centrally managed teams to the engineers and who build and run the software that drives our business and serves our customers. All stakeholders involved in the lifecycle of an application including the developers writing and testing code, security, governance, business continuity, IT operations, and even senior management must work together to build trust. No one is excluded.

Tools and automation

It is easy for us to get caught up in the tool and automation race, but it is critical to remember that tools and automation are enablers to achieving business objectives – they are not themselves the objectives.

Tools help us build better products, solve problems, report our progress, and everything in between. There are so many tools fighting for our attention that it is difficult to pick the right ones to use. The best approach is to pick the tools that meet your requirements and integrate with your workflow and customise minimally when required. According to the Accelerate State of DevOps Report, the most important factors in selecting tools is ease of use and ability to accomplish job-related goals. The report also tells us that companies who rely on custom-built proprietary tooling rank among the lowest performers in achieving DevOps maturity, while those using a broad mixture of open source and off-the-shelf tools are among the highest performers (DORA & Google Cloud, 2019).

Automation is the glue that ties everything together and often becomes our primary focus when embarking on our DevOps journeys. Good evidence exists to tell us we're right; Both the State of DevOps (Puppet Labs, et. al., 2019) and Accelerate State of DevOps (DORA & Google Cloud, 2019) repots tell us that the most advanced practitioners of DevOps have more automated processes than those who are considered less advanced.

There is no one-size fits-all approach to determine which processes to automate in which order. The best approach varies depending on business needs, pain points, and even automatability of the given tasks. We generally want to look at the process where we can achieve a good balance between simplicity of automation and overall impact of automating – if we can save hours of repetitive manual overhead though a simple technical automation then we should take advantage. Automated builds and unit tests rank among the most common automations, with roughly 90 percent of the most advanced DevOps adopters fully automating these processes Automated infrastructure provisioning and deployment is another key area, with over 70% of the leaders operating in this manner[11]. The use of cloud plays an important role in infrastructure automation[12].

As the DevOps field grows and matures, there is a growing focus on shifting security testing and audit capabilities into the automated DevOps pipelines. Automation also plays an important role in security management.

Measure and Adjust

DevOps and SRE doesn't end – we can't simply 'DevOps' something and move on to the next project. We must continue to measure our progress against our objectives and make adjustments and course corrections that help achieve business objectives. As we mature in our journey, we naturally build more trust which unlocks our potential for further growth and maturity in our DevOps practices.

The 5 stages of DevOps evolution pictured below provides us with a set of guidelines to measure our maturity against.

Stage 1: Normalization

Application development teams use version control

Teams deploy on a standard set of operating systems

Stage 2: Standardization

Teams deploy on a single standard operating system

Build on a standard set of technology

Stage 3: Expansion

Individuals can do work without manual approval outside team

Deployment patterns for building apps / services are rescued

Infrastructure changes are tested before deploying to production*

Stage 4: Automated infrastructure delivery

System configurations are automated

Provisioning is automated

System configs are in version control*

Infrastructure teams use version control*

Application configs are in version control*

Security policiy configs are automated

Stage 5: Self-service

Incident responses are automated

Resources are available via self-service

Application are rearchitected based on business needs*

Security teams are involved in technology design and development*

Stage 0: Build the foundation

Monitoring and alerting are configurable by the team operating the service

Reuse deployment patterns for building applications or services

Reuse testing patterns for building application or services

Teams contribute improvements to tooling provided by other teams

Configurations are managed by a configuration tool

*These practices are highly correlated with the stage

Source: Puppet Labs, CircleCI, Splunk (2019). 2019 State of DevOps Report[13].

Operating the cloud

by Kumar Ramamurthy and Rizul Khanna

How to run your hybrid, multi-cloud environment efficiently.

Companies increasingly use "particular clouds for particular workloads." Why? Because different clouds are better at certain things than others. Customers who have a multi-cloud environment usually have stitched a custom mesh of various services from different CSPs that may interact with each other. Given that even companies that go all in on one vendor end up using multiple clouds, how is an organization supposed to ease its multi-cloud management headaches? Managing a multi-cloud environment is a difficult and arduous job. Management of such a complex mesh of services needs a centralized "pane of glass" to act as a cloud management platform to help teams to operate cloud environments efficiently.

The ideal solution is always an evolution

An ideal solution that addresses this problem is a centralized hybrid cloud management platform (CMP) to support customer workloads on all public and private cloud/infrastructure for IaaS, PaaS and cloud-native services with a configuration management database (CMDB) per each customer, from which the console draws all information. The CMDB should also be extensible to accept more data from workloads and be able to expose that data via APIs for a customized console to be built. It's comprised of alert management, trigger enablement, monitoring, and scheduling capabilities.
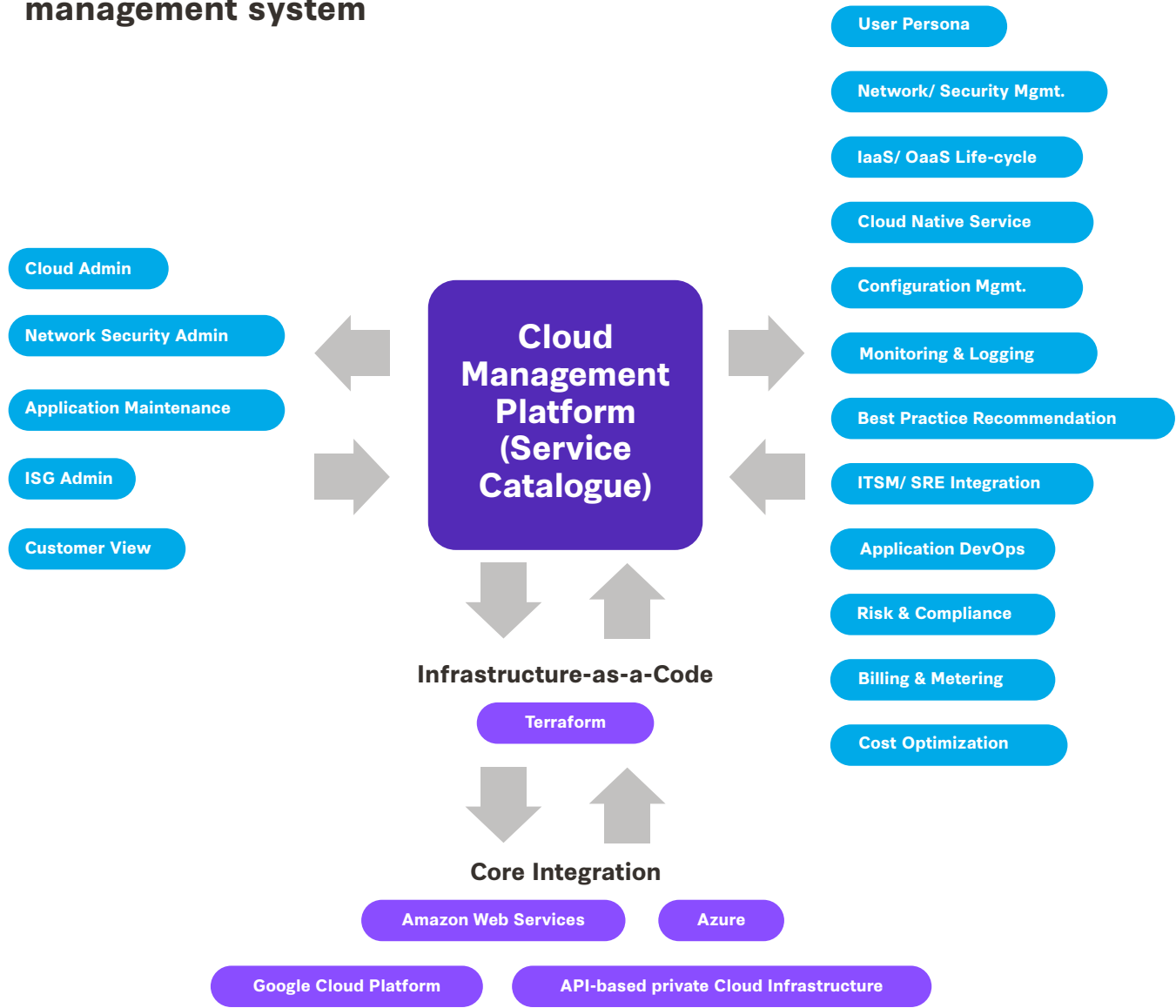
The essential features of a multi-cloud management framework

1 Abstract communication between CMP and target cloud platform via an infrastructure as code script (e.g. Terraform).

2 A blueprint of library of scripts for workload for CSPs, available out of the box

3 Versioning of blueprints against the CSP services and their versions.

4 Base blueprint availability for customization

5 Open data exchange between the CMBD, the console, and the CSP service

6 Rich set of capabilities for discovery, template-based provisioning, orchestration, and automation; operational monitoring and management; governance; and cost optimization across multiple public and private clouds, as well as virtual and bare-metal servers.
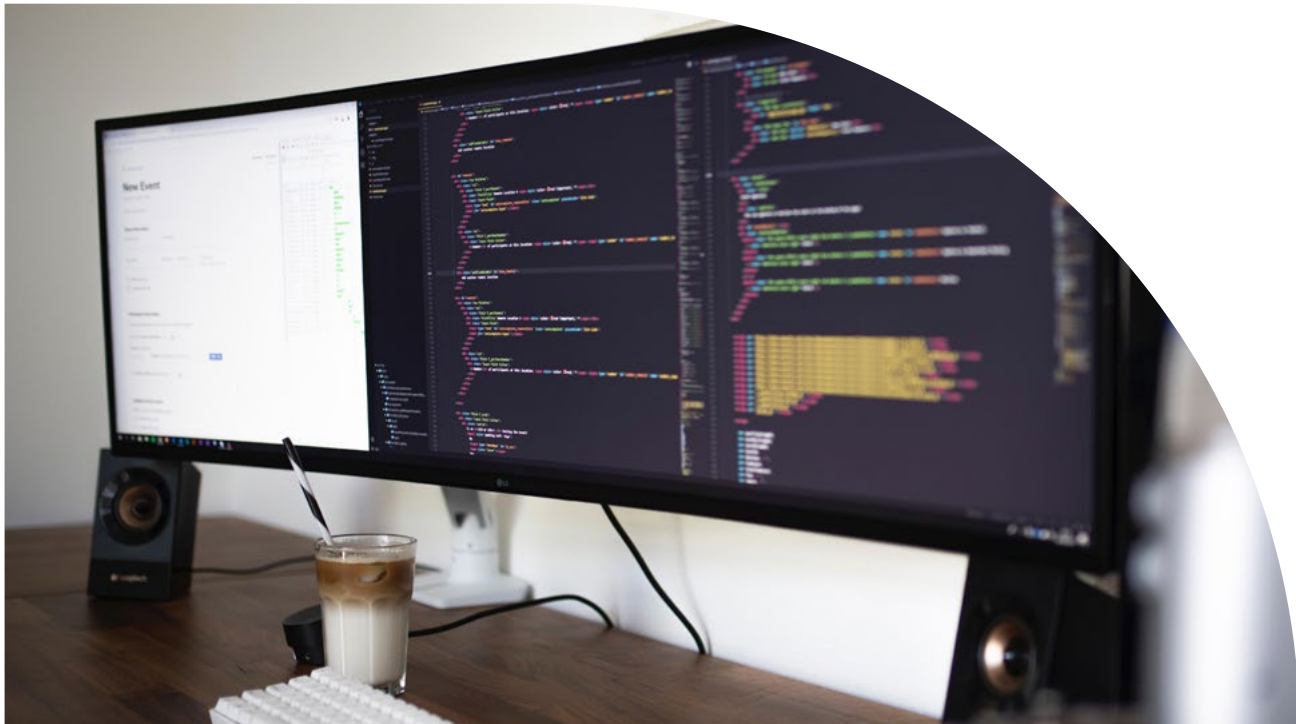
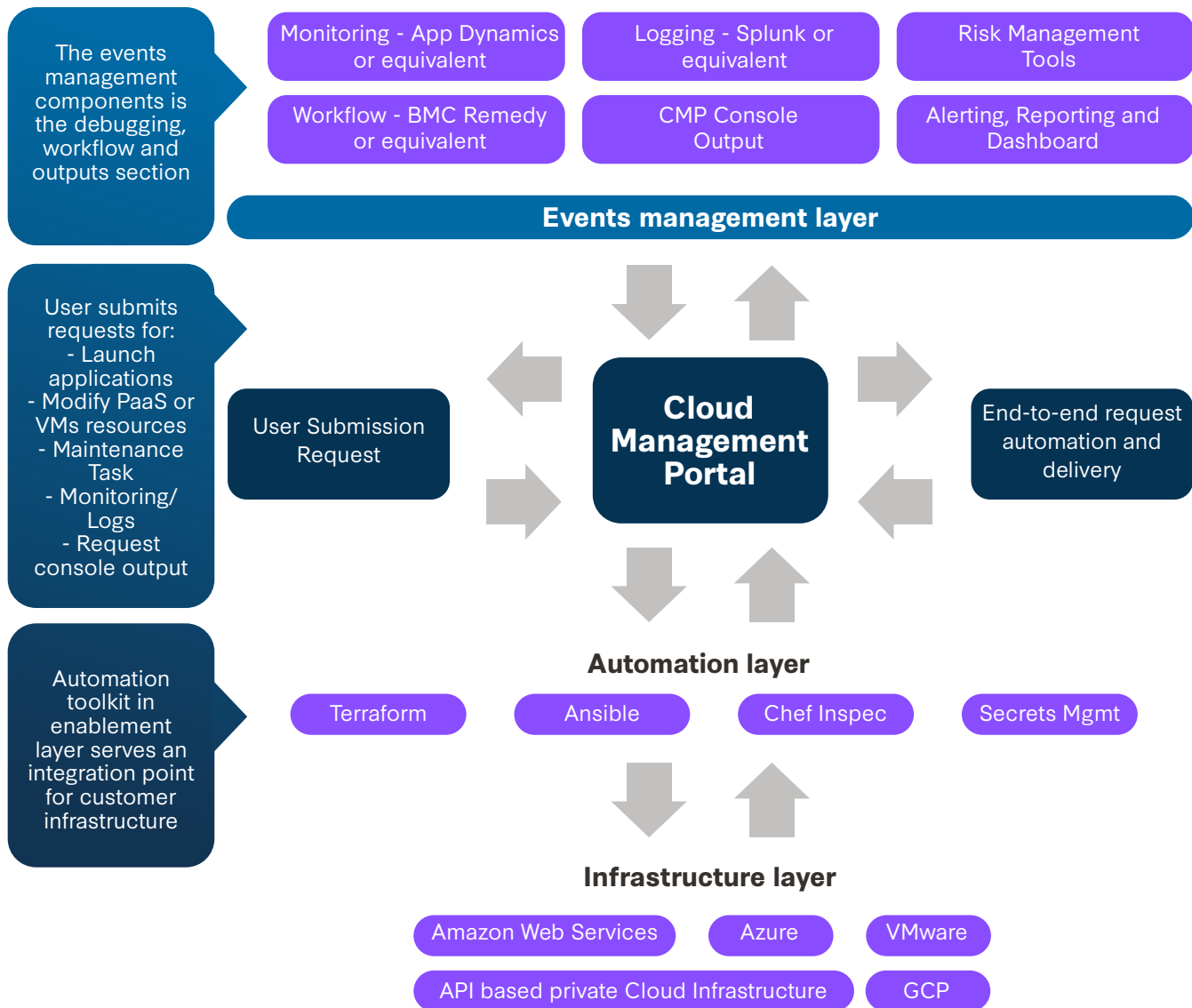## Advantages of a hybrid, multi-cloud management system

1 Automated discovery of all your cloud resources, including those provisioned through the native cloud consoles.

2 Public and private cloud resources in one view with actionable information that enables you to reduce costs, improve infrastructure efficiency, and close security holes.

3 Multi-cloud tags that sync bidirectionally with native cloud tags to organize, automate, and report on resources and costs across clouds.

4 Standardized architectures that meet corporate guidelines for versions, patches, and configurations.

5 Orchestration with any API and built-in support for cloud compute, storage, and networking as well as dozens of pre-built Flexera plugins for extended cloud services.

6 Works with your favorite configuration tools including Terraform, Chef, Puppet, Ansible, Salt, Bash, and Powershell, as well as native cloud templates.

7 Server and application monitoring with alerts and escalations that initiate sophisticated orchestration and automation.

8 Automated backup, auto-scaling arrays, and automated failover.

9 Ability to quickly roll out patches across your operating cloud servers.

10 Automation of your governance controls by using a broad set of out-of-the-box policies or by creating custom policies tailored to your needs.

11 Avoidance of security holes with policies that identify and alert on misconfigured networking options, unsecured data storage, and noncompliant resources.

12 Reporting and other features for optimizing your costs across all clouds and accounts to eliminate wasted spend.

Example of a hybrid cloud management system

Cloud Admin

Network Security Admin

Application Maintenance

ISG Admin

Customer View

User Persona

Network/ Security Mgmt.

IaaS/ OaaS Life-cycle

Cloud Native Service

Configuration Mgmt.

Monitoring & Logging

Best Practice Recommendation

ITSM/ SRE Integration

Application DevOps

Risk & Compliance

Billing & Metering

Cost Optimization

Cloud Management Platform (Service Catalogue)

Infrastructure-as-a-Code

Terraform

Core Integration

Amazon Web Services

Azure

Google Cloud Platform

API-based private Cloud Infrastructure

How are companies and service providers, like Virtusa, solving the problem with tools available at their disposal today?

The events management components is the debugging, workflow and outputs section

| Monitoring - App Dynamics or equivalent | Logging - Splunk or equivalent | Risk Management Tools |
| Workflow - BMC Remedy or equivalent | CMP Console Output | Alerting, Reporting and Dashboard |

Events management layer

User submits requests for:
- Launch applications
- Modify PaaS or VMs resources
- Maintenance Task
- Monitoring/ Logs
- Request console output

User Submission Request

Cloud Management Portal

End-to-end request automation and delivery

Automation toolkit in enablement layer serves an integration point for customer infrastructure

Automation layer

Terraform   Ansible   Chef Inspec   Secrets Mgmt

Infrastructure layer

Amazon Web Services   Azure   VMware

API based private Cloud Infrastructure   GCP

Cloud economics

by Chamindra De Silva

Often in our cloud deployments we come across counterintuitive complaints about the higher cost of cloud infrastructure compared with existing CPE data centers in typical "lift and shift" migration approaches. While this elephant in the room can be addressed with a simple total cost of ownership (TCO) calculator, macro benefits, such as improved business agility and opportunity cost, are typically not factored in. This means that the full benefit of cloud deployment is never captured. A key reason for this is that while ROI and TCO calculations are well defined and supported by significant amounts of benchmark data, quantifying the macro benefits involved, - business agility, resilience and other factors - requires more time to assess. This article provides an approach that you can use to evaluate the benefit of the cloud more holistically.

" There is one rule for the industrialist and that is: *'make the best quality goods possible at the lowest cost possible, paying the highest wages possible'.***"**

- Henry Ford

The corporations at the end of the universe

Companies that have survived the cloud transformation have managed to balance five things well: The rapid adoption of new technology; improving productivity of talent; increased TTM; being responsive to users; and not being vulnerable to security issues as they grow rapidly. The rise of Amazon, Netflix, Airbnb, and Uber are a testament to the disruptive economics of the cloud that enabled these once unknown companies to grow at light speed and displace the elephants in the market that were too slow to move and left in the dust. None of these companies would have succeeded without an elastic infrastructure and economic cloud model. Cloud provided them with a platform to experiment rapidly, evolve, and gave them a level of agility that made it very hard for competitors to catch up. If only large enterprises had unlocked the talent within their organizations, then the cloud would have provided them with an avenue for rich entrepreneurship. Another hands-on example comes from a hackathon that Virtusa ran with Google. We invited both regtechs and banks to participate in multiple regtech challenges. Interestingly those at the top of the leaderboard were

the bank teams, who told us that they were just a subset of untapped talent within banks that was not getting an opportunity to flex its innovation muscle.

Simple "lift and shift" approaches, though easy to calculate in terms of ROI, are really just the tip of the quantifiable benefit the cloud can provide and the least of its real benefits. A study from IDC, available on the next page, shows that the greatest benefit can be provided in business productivity, followed by staff productivity, then risk mitigation, and lastly followed by infrastructure TCO reduction.

Average Annual Benefits per Organization

8%	$1,758,900
13%	$2,629,000
32%	$6,736,700
47%	

- Business productivity benefits
- IT staff productivity benefits
- Risk mitigation - user productivity benefits
- IT infrastructure cost reductions

Total average annual benefits:

$20.97 million

Source: IDC, 2018

To create a more holistic ROI model for cloud we need to consider these four key areas in our ROI equation. These are given in the table below with some estimates of cost saving from AWS and IDC.

More ROI and Revenue benefit →

Area	TCO	Operational Resilience	Development Productivity	
Descriptions	Cost avoidance and savings typically by migrating infrastructure cost	Incident and outage reduction and reduced security risk	Improving development and ops. team productivity	Get apps to market faster to size on emerging opportunities before the competition
AWS Median	19% overall cost reduction	43.4% reduction in overall incidents	2x staff productivity benefit	18.8% time to market of new apps
AWS Best Cases	51% overall cost reduction	43.4% reduction in overall incidents	10x staff productivity benefit	1000% increase in innovation pipeline
IDC Forecast	32% lower cost in 5 years	$32,316 savings per 100 users	$82,809 saving per 100 users	$120,986 gain per 100 users

← **More well defined, mature ROI calculations**

Elastic economic models: the greatest benefit

As shown in the table and diagram on the previous page, cloud computing's greatest economic benefit is its ability to deliver business agility by providing an elastic business model. This economic model is fundamental to the rapid growth of start-ups like WhatsApp, Monzo, and Netflix, which have been able to grow their organizations through multiple, rapid rounds of seed funding to capture the lion's share of emerging markets. A similar model can be applied internally by large organizations to place bets on their product lines and rapidly respond to market demand at a lower opportunity cost. Such a facility can enable and liberate budding "intrapreneurs" within your organization to come up with the next big product and provide a platform for them to fail fast without incurring massive upfront infrastructure costs. Thus, the cloud reduces the cost of failure by providing an elastic cost model for your successes. The diagram below shows the relative savings provided by a successful, rapidly growing public cloud project, compared with a hosted private data center, or a fixed capacity private cloud model.
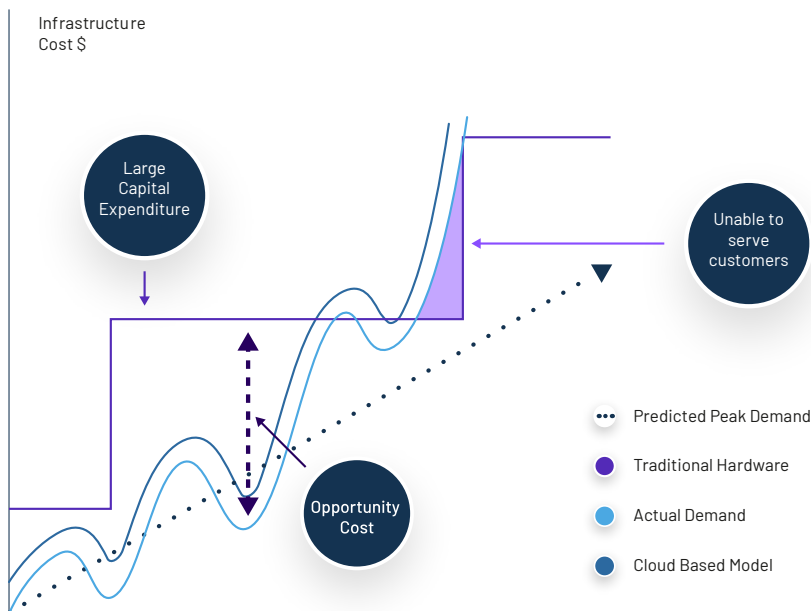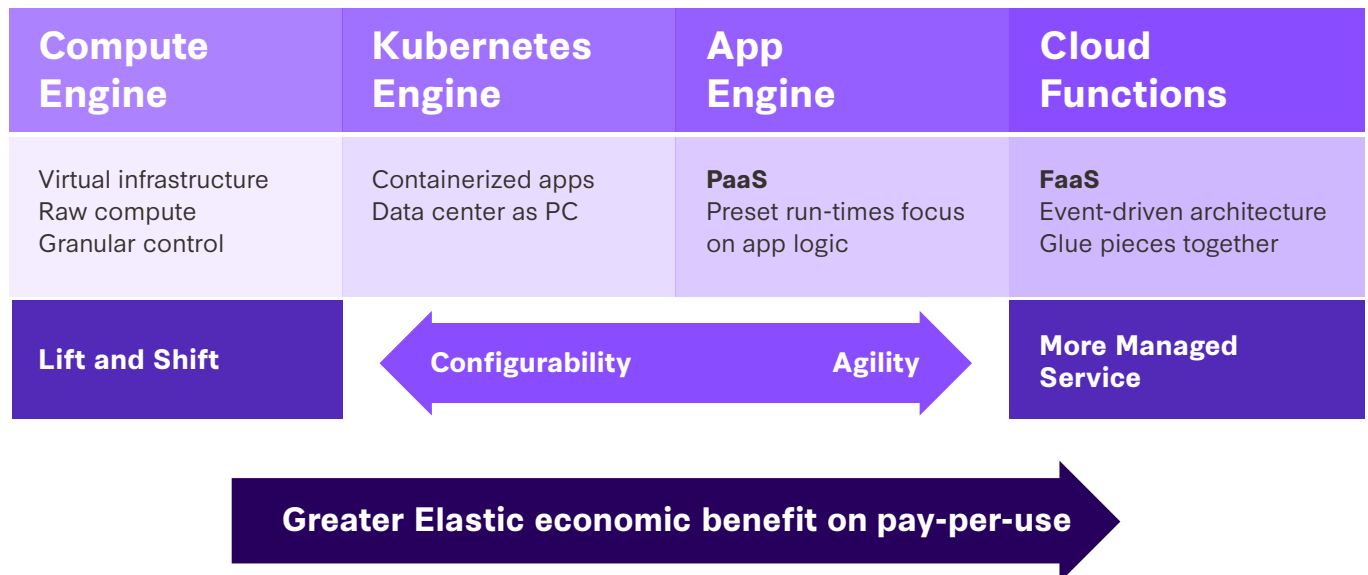

DIAGRAM: DATA CENTER VS. ELASTIC COMPUTE MODEL FOR PRODUCT GROWTH

On the growth of a successful product, we can see in the diagram in the study from IDC that wastage in capacity presents an opportunity cost and also resilience issues caused by lack of capacity to deal with rapid demand. More importantly, should the demand suddenly ramp down for whatever reason, one is able to rapidly ramp down costs and fail fast with a low cost exit.

In addition, CSPs provide a large range of elastic computing options that greatly reduce setup and management overheads. This enables companies to place new bets in a variety of managed container options, such as the CSP-specific AWS Elastic Beanstalk or Google App Engine, or hybrid strategies (such as the Kubernetes container model) that permit you to reuse your existing data center investment and then elastically scale cloud capacity and compute or failover to the cloud. The diagram below shows the different elastic cloud options that Google provides as an example.

Compute Engine	Kubernetes Engine	App Engine	Cloud Functions
Virtual infrastructure Raw compute Granular control	Containerized apps Data center as PC	**PaaS** Preset run-times focus on app logic	**FaaS** Event-driven architecture Glue pieces together
Lift and Shift	**Configurability** ← → **Agility**		**More Managed Service**

Greater Elastic economic benefit on pay-per-use →

Towards a more holistic RoI equation for cloud

Looking at cloud costs holistically involves considering all elements from the traditional TCO reduction in infrastructure costs (server, storage, network, compliance, and security costs etc.), but also needs to factor in business agility. Rather than try and model abstract factors to quantify commercial opportunity, we can represent these benefits in more concrete terms by focusing on application development cost savings, such as increased developer productivity, portioning speed, and net new revenue derived by a faster time to market.

Server Costs	Hardware - Server, Rack Chassis PDUs, ToR Switches (+Maintenance)	Software - OS, Virtualization Licenses (+Maintenance)	Facilities Cost		
			Space	Power	Cooling
Storage Costs	Hardware - Storage Disks, SAN/FC Switches	Software - Backup	Facilities Cost		
			Space	Power	Cooling
Networks Costs	Network Hardware - LAN Switches, Load Balancer Bandwidth Costs	Software - Network Monitoring	Facilities Cost		
			Space	Power	Cooling

IT Labor Costs	Server Admin, Virtualization Admin, Storage Admin, Network Admin, Support Team
Extras	Project planning, Advisors, Legal, Contradictors, Managed Services, Training, Cost of capital

Additional Impact

Cost of delays
Risk premium
Competitive abilities
Governance

Application development productivity	Revenue gained by a faster time to market	Opportunity cost saved taking into production

A true equation of the cloud's economic benefit needs to factor in business agility and also organization-specific benchmark data. The traditional equation for TCO Cloud saving normally focuses on infrastructure saving and is given as:

$$ROI = \frac{(\text{Infra Cost Savings})}{(\text{Sunk Cost + Migration Cost})}$$

However, the real ROI for Cloud needs to factor saving on application development and revenue growth as a result of rapid cloud deployments to meet market demand:

$$ROI = \sum \frac{(\text{Business Agility Benefit + App Dev Productivity + Infra Cost Savings + Resilience Savings})}{(\text{Sunk Costs + App Refactoring Cost + Infra Migration Costs})}$$

Many of the organizations we work with today already actively track these factors, but they are harder to obtain and, in certain instances, approximation may be needed in the interests of time.

The table below gives some indication of how you might capture the variables mentioned in the equation on the previous page in your ROI formula:

Infrastructure Costs	Hardware costs; Database licensing costs; OS licensing costs; Power costs; Facilities costs; IT administration efficiency; Database administration efficiency; Help desk support efficiency
Application Development Productivity	Application development productivity; on-demand Dev and QA environment creation speed; increased innovation/POC productivity; deployment productivity
Business Agility Benefit	Improved time to market; increase in number of products/features released; business analytics efficiency; clicks per month; conversion rates
Resilience Savings	Productivity loss avoided benefits; revenue loss avoided benefits; regulatory compliance cost savings; security incident reduction benefits; business continuity benefits
Sunk Costs	Current data center costs; current enterprise license costs; current staff costs
Application Refactoring Costs	Application refactoring costs; application re-engineering; CI/CD/ Infrastructure-as-a-Code enablement costs
Infrastructure Migration Costs	Application virtualization costs; application containerization costs; data migration costs

Reducing the impact of sunk costs

Sunk costs are often put forward as counters for rapid cloud migration. They represent a local minima that organizations need to get over, but there are strategies for mitigating sunk costs. With regards to on-premise data centers, one can repurpose them to a hybrid cloud model using platforms such as IBM OpenShift, AWS Outposts, and Google Anthos. This will allow organizations to repurpose this investment while retaining the elastic benefit of the cloud. In certain situations, it might even end up being more economically viable than a pure cloud strategy. In terms of the sunk costs of staff, it is not hard to retrain IT staff into cloud certified professionals, and they can shift more of their time saved into supporting development in a DevOps function. This will provide further optimization for development and time to market. Finally, in terms of licensing costs, companies like Microsoft offer cloud compatible migration options to transfer your licenses to the cloud.

Additional best practices for creating your ROI model

- Factor your organization's appetite for investment into the ROI calculator more holistically. If the TCO reduction is sufficient, it is better to proceed, but define a clear measurement strategy for other areas of focus, such as business agility and productivity.

- Use many of the available TCO tools to do this analysis, which also utilizes benchmark data to provide an estimate.

- Use at least a three-year window for your ROI calculation to overcome migration costs.

- Remember to factor in the infrastructure depreciation costs of your CapEx. Most tools for the TCO calculation provide this based on benchmark data.

- While the best stakeholders to discuss cost savings are to be found in finance, procurement and IT, the best stakeholders to discuss the more holistic ROI calculation are the business and product owners.

- Take a small sample set of applications and assess potential benefits in business agility, reliability, and development productivity. Decide if an elastic economic model is beneficial for the applications and extrapolate through application classification for the rest of the landscape.

- Many providers also provide significant discounts aligned to their costs which should be optimized (such as four tiers of cloud storage costs) based on access frequency, the persistent use of discounts for known minimum capacity, or right-sizing VMs from the multitude of options of granularity not available to you in data centers.

- Hybrid cloud strategies enable you to take the sunk costs out from the equation and might also result in better savings than a pure cloud strategy in certain instances.

On average migrations are deriving a 20% cost saving from cloud migration using predominantly lift and shift strategies. The greatest opportunity, however, is in business agility, which can provide a 10x benefit to certain product lines by helping to get more market share and improve conversions. Creating an elastic cloud development model provides you with the economic benefits of reducing the cost of failure and reducing wastage on success for rapid growth. More importantly, the cloud enables you with an economic model that liberates your intrapreneurs who might give you the next major product innovation to provide you with > 1000% benefit. The real question is whether can you afford to lose that opportunity.

Monitoring and managing a smarter cloud

by Chamindra De Silva

Virtusa's Polycloud Intelligent Engagement Solution

Organizations embarking on the cloud journey are struggling with compliance (including security), performance, and cost optimization issues. Furthermore, the distributed and hierarchical enterprise has no way to provide all of their teams with complete visibility of their system performance, bottlenecks, and risk indicators. Without this visibility, it's difficult to incentivize teams to optimize their cloud. This issue becomes worse as enterprises move from single CSP play to cloud strategies.

Virtusa's PolyCloud Intelligent Engagement Solution taps into various tools provided by the different CSPs and synthesizes that data into a common dashboard with deep drill-downs and predictive alerts, providing the means to increase transparency and accelerate their cloud maturity journey.

The solution leverages Virtusa's experience in driving engagement at multiple levels, through actionable intelligence and gamification, to accelerate cloud transformation within enterprises.

Here are some examples of specific sources of data the platform taps into AWS Cloud Watch and Trusted Advisor, GCP Stack Driver, and Forsetti.

Key feature highlights include:

Actionable KPI's on compliance, performance, and cost

Actionable KPIs/metrics built from raw data are used to drive intended behaviors across the following main focus areas:

1 Compliance

KPIs derived from the violations of policies/best practices are used to provide immediate transparency to teams, which help them pro-actively correct what could become expensive mistakes.
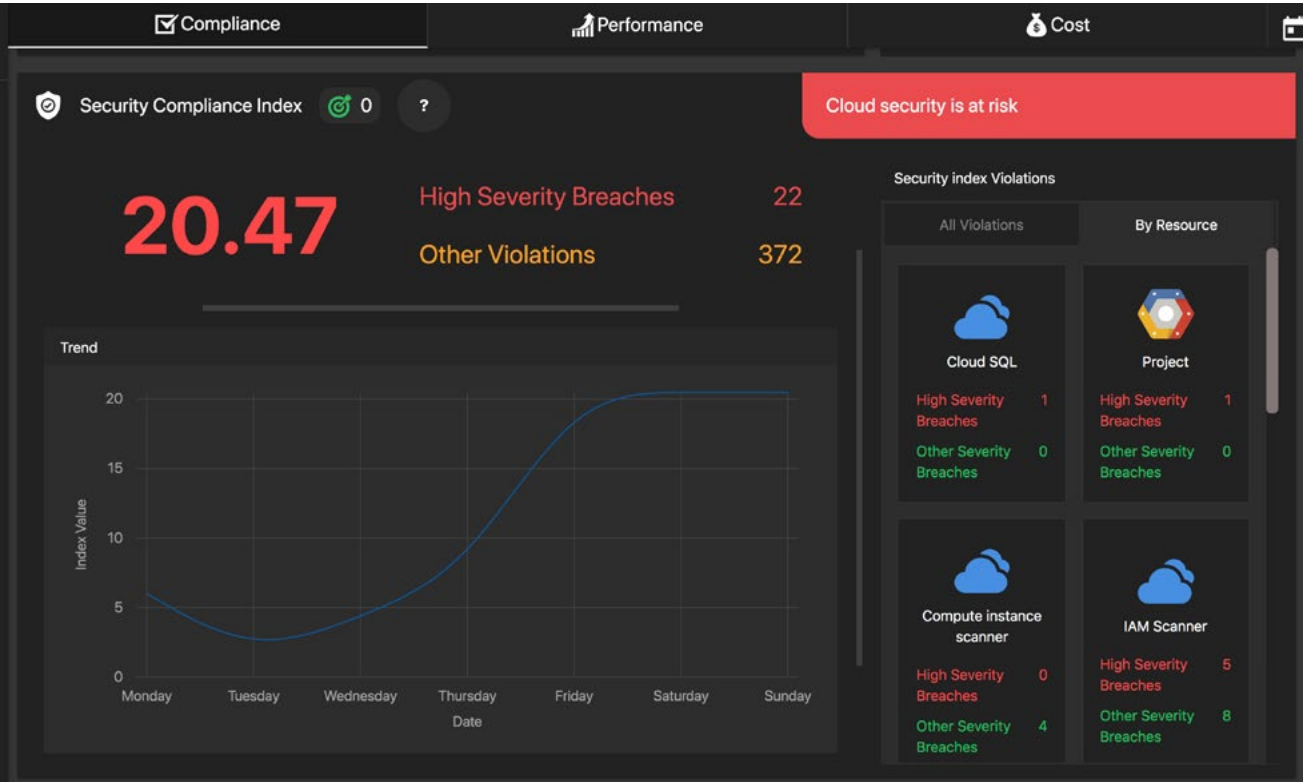
2 Performance

KPIs considering the performance of cloud resources and applications with an aim to fine-tune and scale the solutions deployed on the cloud.

3 Cost

KPIs considering current usage and associated costs with a view to optimizing spend.

Metrics are linked to actionable "next best" measures, which should be actioned based on priority indicators.

Smart insights and predictive analytics for risk mitigation

Intelligent risk assessment module review heuristic data and provide predictions on imminent threats.

Real-time alerts which direct users to immediate actions to be taken / areas to address.

Application insights and meaningful grouping allows tagging of resources into meaningful groups and enterprise hierarchies (e.g. applications, teams, org units) so that actions can be driven through an organization's natural hierarchy.
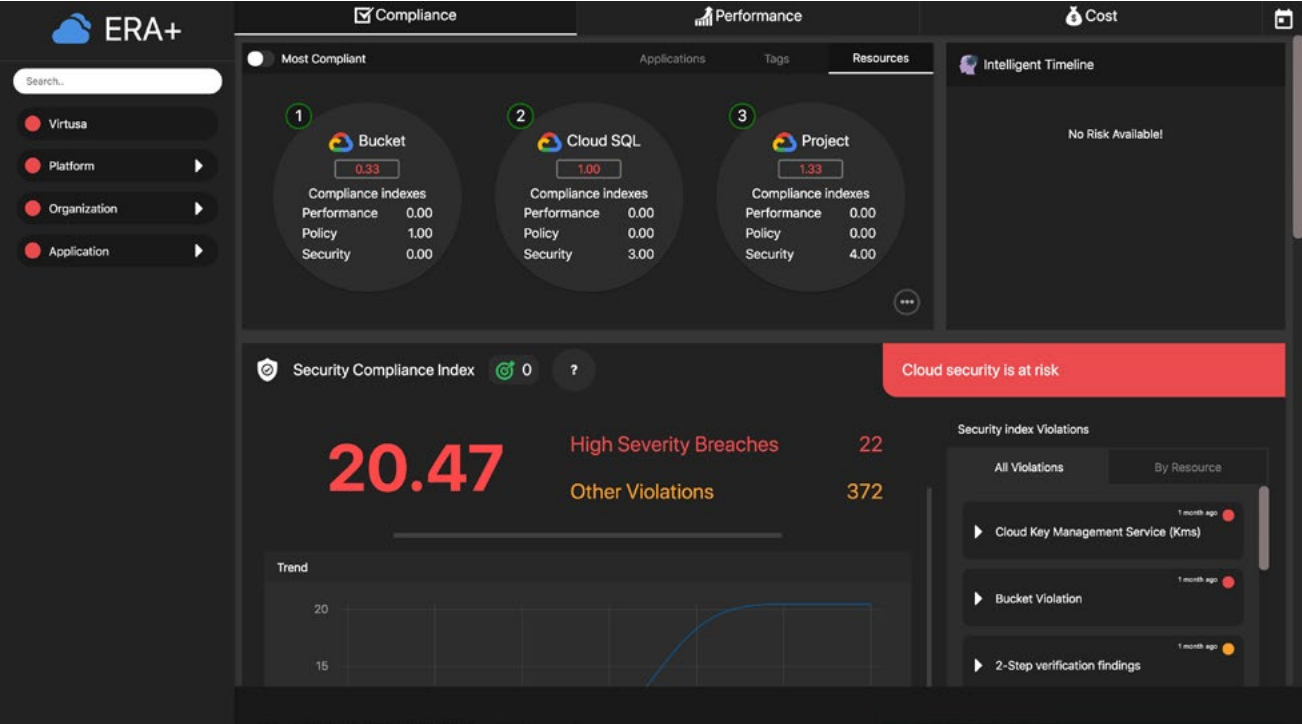
You can also slice and dice your data based on other logical groups (e.g: Tags and Labels)
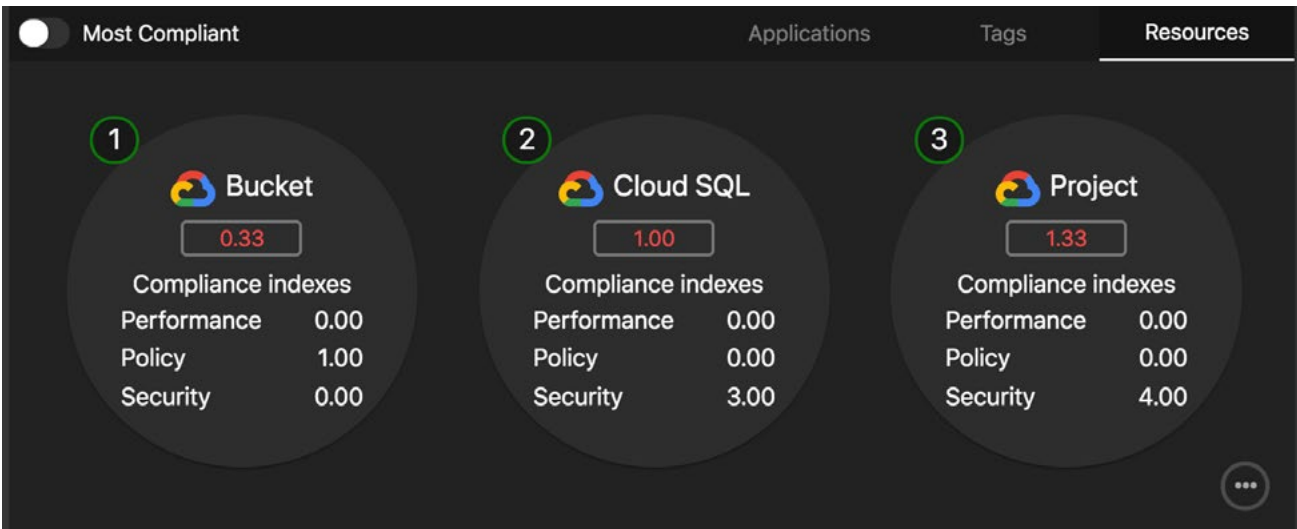
Cloud gamification and intelligent engagement

Resources and data (such as risks, telemetry, and cost data) are weighted and aggregated into a score index for use in leaderboards and gamification.

Leaderboards highlight the top three and bottomthree of each focus area.

An enterprise's cloud transformation journey is by no means a trivial undertaking. Apart from skills and competencies, it requires focus and engagement from all stakeholders on critical aspects needed to achieve the outcomes. With Virtusa's PolyCloud Intelligent Engagement Solution, different stakeholders of the organization are able to get insights on different aspects of the cloud journey that are relevant and critical to them. Users of the dashboard will be able to address critical issues immediately without having to wait for separate manual reviews typically done at later stages of the life-cycle. PolyCloud intelligent Engagement Solution can be applied at any stage of the transformation journey to improve the quality of outcomes of an organization's cloud journey.

Grow and Transform

ARTICLE 11

Unleashing cloud creativity

by Stephen Wood and Sunil Krishnan

Using cloud as a springboard for innovation

Most companies begin their cloud transformation journey considering migration as a way to increase their bottom line. The business case for migrating existing systems and data to the cloud is clear and well known: moving to the cloud reduces CapEx spikes, minimizes the cost around infrastructure and app maintenance, and enables scalability without long ramp-up periods. What is less frequently talked about is the cloud's potential to drive-top line growth. In order to achieve this, we need to think beyond optimization and start thinking about the cloud's potential to drive innovation. The truly transformative potential of cloud does not come from doing what you've always done, but doing it faster, cheaper, and at scale, it comes from harnessing the cloud to enable businesses to do what wasn't previously possible.

For existing businesses, this can happen in a number of ways:

1 Starting up a new separate, cloud-native business

2 Founding an ecosystem, or playing a radically different role in an ecosystem

3 Creating previously impossible experiences and products

Fundamentally, all of these opportunities draw on the plug-and-play nature of cloud-native technology that enables business to reduce the risk and cycle time for exploring, creating, and validating new opportunities, whether they be technologies, partnerships, or business models.

Be your cloud-native competitor

As traditional businesses watched their industry being redefined by new, cloud-native entrants, we witnessed a predictable cycle. "Heritage businesses" saw the speed at which new entrants evolved their products and experiences, but knew that their own legacy tech and operating models would prevent them from accelerating at the same pace. Other brands saw the threat of being displaced by new entrants as more critical than the threat of cannibalizing revenue, and so they set up new, cloud-native businesses. As cloud-native technologies have proliferated, it's become easier to spin up a new venture in which all core business functions and customer-facing systems are delivered by LEGO-like plug-and-play technology components.

Create a dynamic cloud ecosystem

The interoperability of cloud-native technologies and standard integration via APIs and microservices has also enabled businesses to create new joint ventures, through which partners could be one or many third-party companies, public sector bodies, or the nebulous hoard known as "the crowd". Being able to rapidly create ecosystems at a previously unheard of scale has enabled organizations to deliver value to millions at a previously impossible price point. The cloud fosters unexpected partnerships and opens up new commercial models that address momentary windows of opportunity (business cases become easier when they don't involve building new infrastructure).
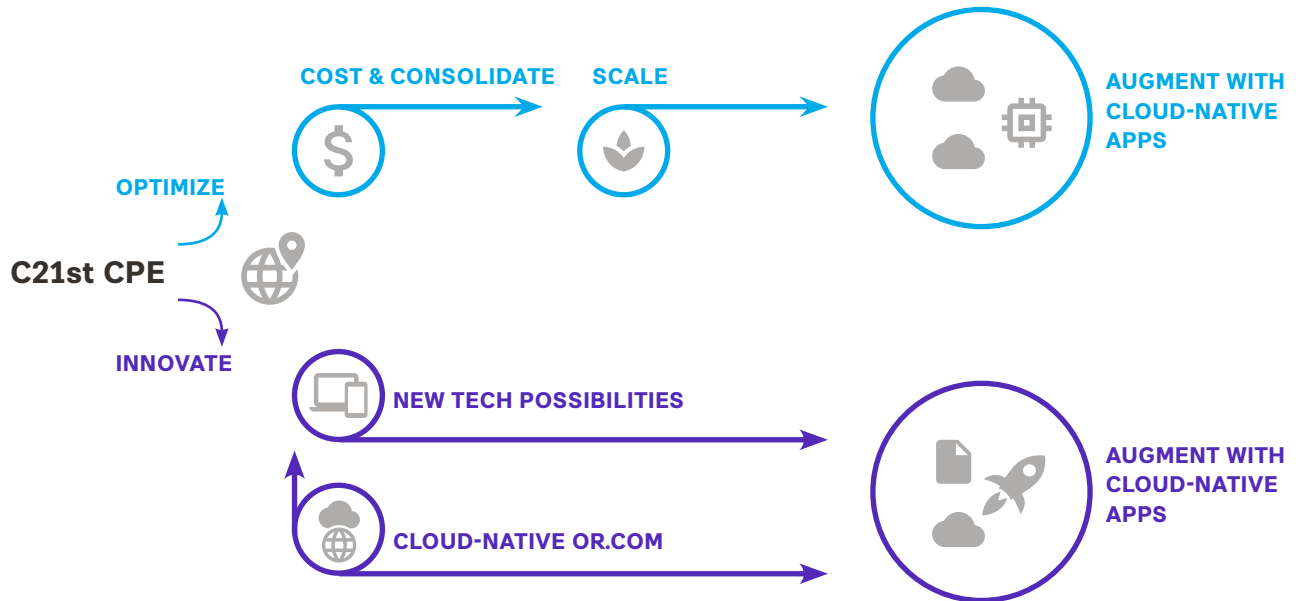
Making the next impossible thing possible

Although the major CSPs are still keen on stressing the efficiency and effectiveness of cloud transformation, if you dig a little deeper in the messaging, there's also an innovation theme. The integration of AWS with Amazon DeepLens offers a deep-learning enabled video camera for developers to build solutions that process images and videos. Google Cloud Platform's Dialogflow accelerates the development of AI-enabled voice/text conversational interfaces. Microsoft Azure stresses the cloud's role in making its augmented reality HoloLens feasible. These examples demonstrate how standards-based integration and applying AI to big data at cloud scale can enable unprecedented, game-changing innovation.

Using cloud as an innovation springboard

	Doing the basics	Developing	Mastery
Tactic	Optimization and Augmentation	Point-Innovation	Disruptive Innovation/ Transformation
Emerging Tech	Use the cloud to explore and prototype with emerging technologies.	Rapidly prototyping and deploying cloud-based emerging tech modules for either hybrid or pure cloud models. These create USPs. Drawing on common cloud-native tech for core business functions.	Creating a portfolio of emerging technology components that can be hot-swapped into new ventures. Monetizing the IP from emerging tech developments and collaborations in CSP marketplaces.
Business Models		Creating cloud-based, stand-alone ventures or joint ventures that harness emerging tech for specific use cases with mid-to long term lifespans. Focus on core niche or adjacent industries.	Operating a cloud-based platform that enables the rapid ramp-up of ventures that combine multiple players that can capitalize on time-limited opportunities. Ability to spin out ventures beyond the traditional niche.

What to do, now and next

What to focus on **now:**

1 Evaluate how well your company's innovation program factors in the role that cloud needs to play to assure that its unique abilities to scale and flex define options and inform decisions about solution viability.

2 Given the speed at which cloud-native businesses introduce new tech, evaluate whether your approach to innovation enables you to take ideas to production within weeks.

3 Evaluate how quickly your company can easily establish the commercial structures that enable collaboration. Can NDAs be put in place? How easy is it to define operational and commercial models? These factors will define how easy you are to partner with.

4 Focus on the front end of your innovation pipeline. Do you have a range of methods for engaging with different stakeholder groups to solicit new ideas and problem statements? How do you support participants through the innovation cycle to assure that the initial enthusiasm doesn't turn into frustration or apathy?

5 Create a clear plan for how the key tech that flourishes in a cloud environment could drive radical transformation within your niche. For example, consider the impact of large scale, AI-driven decision-making or the potential of IoT to extend and redefine your customer experience.

What to focus on **next:**

1 Evaluate how your innovation program can create those 10x ideas by drawing on the capabilities of the cloud. What tactics do you deploy to assure that your program doesn't just generate "incremental innovation", which is often indistinguishable from "optimization"?

2 Evaluate your company's plan for cloud migration and create a conceptual strawman for a green field, cloud-native alternative. Identify how this model could be augmented with emerging tech to disrupt the status quo. Identify how core capabilities could be reused as the foundation of other businesses, for example a generic order-to-cash process or a customer on-boarding process.

How Virtusa can help

Virtusa's Open Innovation Platform provides a CSP-agnostic way to capitalize on emerging technologies by developing new cloud-native applications. It supports the entire innovation process, from ideation and emerging tech discovery through to technical prototype development. The platform creates a virtual innovation lab in the cloud that companies can use to engage with emerging tech community, from fintechs and academics through to internal "entrepreneurs."

The platform offers the workflow traditionally found in innovation management tools, which assure good pipeline flow so that more of the best ideas make it to production. It also offers a sandbox in which new solutions can be bolted together quickly and tested with meaningful data.
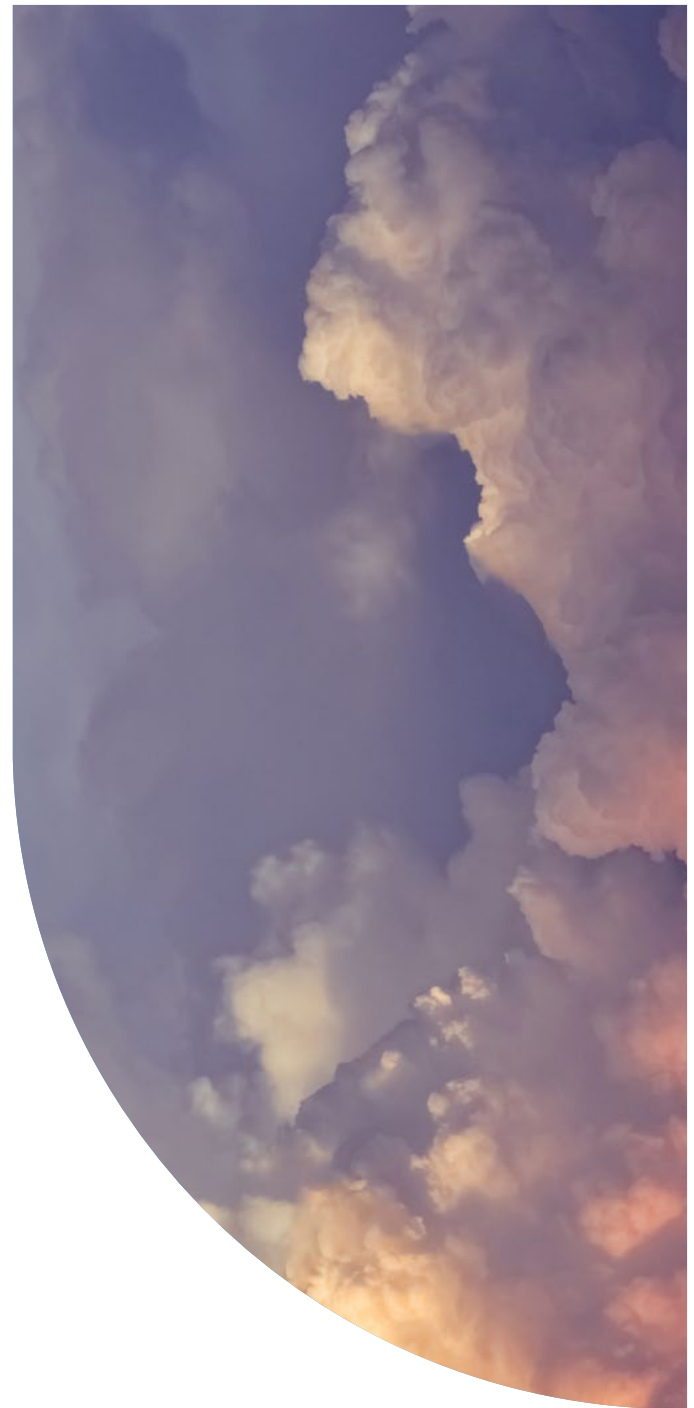
Data to insights

by Chamindra De Silva

49% of companies are using the cloud for AI services, and 85% of enterprises will start using cloud in next two years for generating insights from data. This could either be using cloud AI development services or cloud AI software and applications. An obvious question arises: Can an organization avoid adopting cloud and still tap the huge latent potential within the massive amount of data that it produces? The answer is "no". We not only see this in industry trends, but also through logical deduction.

Looking back, we can see that the majority of the AI trends predicted in 2018 have been implemented and that the barriers to adoption have been materially lowered by CSP-delivered AI offerings and tech enablers. While these trends have delivered tremendous value, it has not been sufficient to assure long-term competitive advantage. The ever-accelerating pace of innovation has meant that identifying and capitalizing on the next new AI trends early makes the difference between staying ahead

and staying in business. CSP offerings, which range from data infrastructure to highly accurate, scalable and customizable AI models and solution frameworks, offer immediate ROI. Aggressive competition between leading CSPs has fragmented the market but it has also created the hybrid-cloud paradigm, which gives businesses multiple ways to adopt cloud-based AI.

Democratization   Alternative Computing   Ubiquitous AI

Decentralization   AI-as-a-service   Intelligent Assistants

Enterprise Conversational AI   Ethical & Explainable AI   Robotic Workforce

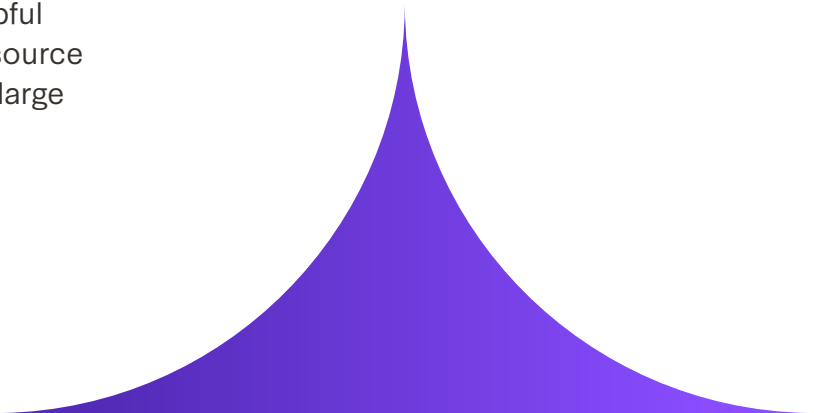# Why the cloud will become the natural choice for building intelligent applications

1 The accelerated evolution of AI frameworks and technologies has been driven by the opensource community. This boggling range of choices has presented a challenge for capital-stretched companies that need to minimize exploration costs and reduce the trial-and-error-based approach.

2 Laggard organizations that missed the early adoption of AI due to organizational focus, lack of investments, or other barriers are now turning towards cloud AI to catch up with competitors and fast-track AI adoption.

3 Due to a lack of AI experts, and in a bid to make the AI easier for nonexperts, organizations are pushing staff toward easy-to-use AI Cloud Services in areas including data, AI, integration, and DevOps to build next-generation solutions.

4 Cloud-based applications, such as vision, audio, and video analytics, are changing the market. These need cloud as they're based on advanced technologies, consume massive amounts of data, and need significant infrastructure.
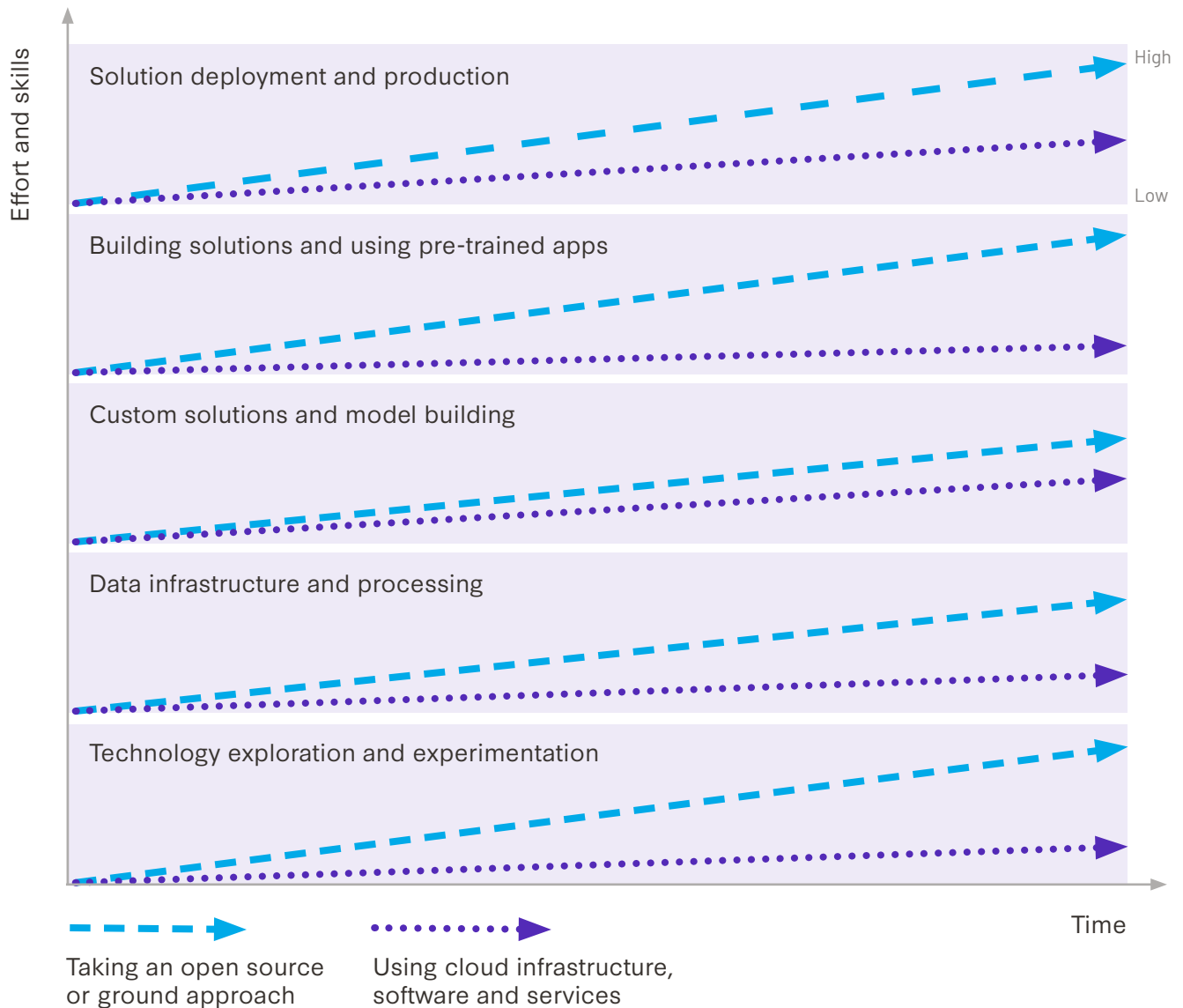
Understanding the economics of cloud AI

Leveraging loads of enterprise data and generating actionable insights can only be achieved successfully if done with net-positive ROI in the short-term and achieving the economies of scale in the medium and long-term. With a rapidly changing technology environment and a need for advanced technical capabilities and skills to cut through the clutter of market competition, businesses require a thorough analysis of emerging cloud capabilities, including how well they align with organizational objectives and priorities. In their journey from building the data infrastructure to generating the patterns, organizations go through the following critical path:

- Technology exploration and experimentation
- Building data infrastructure
- Custom-built models and applications
- Using pre-trained APIs for advanced applications
- Engineering and production

The following diagram depicts the role of cloud offerings in each of these stages and how helpful they prove to be in reducing the effort and resource requirements needed to build innovative and large scale business applications.

Approximate effort over medium to long term

Effort and skills

Solution deployment and production — High / Low

Building solutions and using pre-trained apps

Custom solutions and model building

Data infrastructure and processing

Technology exploration and experimentation

Time

Taking an open source
or ground approach

Using cloud infrastructure,
software and services

What to do now

Short-term objectives.

Identify the organizational readiness in terms of data availability, access, security, and any regulations involving storage and consumption of data that would lead to building data infrastructure fit for various business needs.

Lay out the critical focus areas and business use cases that have immediate and medium-term priorities and would propel value generation across business segments.

Formulate the data and technology access required to engineer such applications by keeping the business benefits at the center of discourse. Understand the technology maturity and market readiness for listing down the products, platforms, and skills required. For example, to what extent does the enterprise wants to use IoT in their business applications?

Create a target-oriented cloud strategy that combines the best of the offerings from various CSPs and open-source technologies to come up with a value-driven operating model.

How Virtusa can help

Virtusa delivers a platform-agnostic approach of solving business problems with AI. To achieve the acceleration and scale for helping our clients in their data-led transformation programs, we have divided the solution-building journey in to three different steps.

1 Formulating the best possible approach for solving a business problem and building the accelerators that can be onboarded or plugged-in to any product or platform of choice.

2 Evaluating the products and platforms that offer full or partial off-the-shelf capabilities and the level of customizations allowed to make the solution more contextual.

3 Mapping the possible technology alternatives from step two (above) with an organizational focus, existing technology stack, and a degree of scalability and reusability required.

For example, in order to create a voice-based smart search solution for a company that has focuses on a specific CSP, we bring in the right AI algorithms from our model zoo (a repository of pre-trained AI/ML models built on synthetic, public, and masked data), use the right opensource or third-party frameworks (after evaluating its compatibility with that CSP) and scale this solution using the native services provided by the CSP in focus.

In this way, we ensure that our entire focus remains on the quality of the solution while not getting lost in the intricate web of technology products, platforms, and cloud offerings.

Building cloud-native apps with APIs

by Anindya Bhattacharya

Addressing today's Frankenstein tech

Over their lifetime, large companies amass a huge amount of tech baggage. Each new project bolts solutions onto a legacy core. In time, this approach leads to what is optimistically called a "hybrid" landscape, although it's more honest to call this a "Frankenstein landscape": one that is bolted together, rather than elegantly architected.

A Frankenstein architecture can be identified by the following symptoms:

1 A long list of customizations and rewrites which have been put in place to fix, upgrade, and augment legacy apps

2 A sprawling landscape systems-of-record behemoth, all of which are mission-critical and which rarely tampered with

3 Fast-and-agile (less-predictable) systems-of-engagement business enablers

4 A largely monolithic or layered architectural design

5 A tightly coupled solution architecture, which makes integration and customization a daunting task

The challenges with Frankenstein tech

This approach generates well-known problems for businesses, such as a slow pace of change. Interdependencies between tightly coupled, diverse technology stacks makes release management complex and slows down the change (e.g. lengthy lead times for scaling up.)

Legacy systems typically scale by adding hardware. This involves securing funding, purchasing, and then deploying infrastructure, which is seldom a real-time activity. In the worst-case, it may even be tied to annual budgeting cycles.

Scale everything, or scale nothing: A monolithic architecture prevents targeted, on-demand scaling. It's just too complex to try and scale specific elements, so increasing capacity involves uplifting entire systems (e.g. complex maintenance processes).

Deploy everything or deploy nothing: A monolithic layered app makes it extremely difficult to selectively amend or upgrade individual architectural components should it be necessary.

Describing monolithic architecture

Execution	Technology	Operations
One single business solution delivered through an environment comprised of disparate disconnected technology assets and orchestrated through multiple tools within the constraints of strict business SLAs.	More focus on centrally governed orchestration and less choreography of distributed components.	Strict waterfall-aligned planning • Release cadence hinders the agility ask of the systems. • Hardware provisioning fails to cope up with the elasticity of business demands.
	A tightly coupled architecture too inflexible to respond to demands of change.	Development teams strictly aligned to skills and silo matrix.

Breaking monolithic apps with APIs and microservices

Breaking monolithic apps with APIs and microservices APIs offer a means to democratize a distributed and componentized enterprise architecture. An API-driven architecture enables the delivery of componentized applications with fine-grained architectural patterns.

APIs act as a software "glue" layer enabling different apps to communicate with each other. This format of the communication is agreed in a "contract" called an OpenAPI specification, formerly called a Swagger file.

Adopting an API-based architectural approach involves:

Taking an inside-out, API-first design approach that contrasts with the traditional SOA approach

Creating and evolving API and microservices design patterns

Creating and evolving mesh architectural and design patterns

Shifting to an API paradigm also involves changing the way that applications are managed. In the world of APIs, the traditional smart-broker approach to orchestration is replaced by intelligent actor-driven choreography. By combining this with a rejection of the monolithic application in favor of a microservices "shared nothing" architecture, organizations build an infinitely more flexible tech infrastructure that is event-driven and follows reactive architectural patterns.

The model brings two new issues. First, release management for a large inventory of fine-grained components managed by small, multi-skilled teams is challenging, but the challenge can be managed by adopting a rules-driven DevOps pipeline. Second, an API-microservices architecture has the potential to clog networks with "chatty" components that create heavy payloads (e.g., text-based JSON over REST/HTTP). This risk can be mitigated via a combination of thorough testing and operational monitoring.

Comparison of a monolith vs. microservice-based architecture

A Layered Architecture:
Architectural components stacked up on a single shared runtime and communicating over interfaces to form a monolith. Actual implementation details (threads, contexts) tend to leak across layers and make the architecture harder to scale and maintain for the inherent complexities.
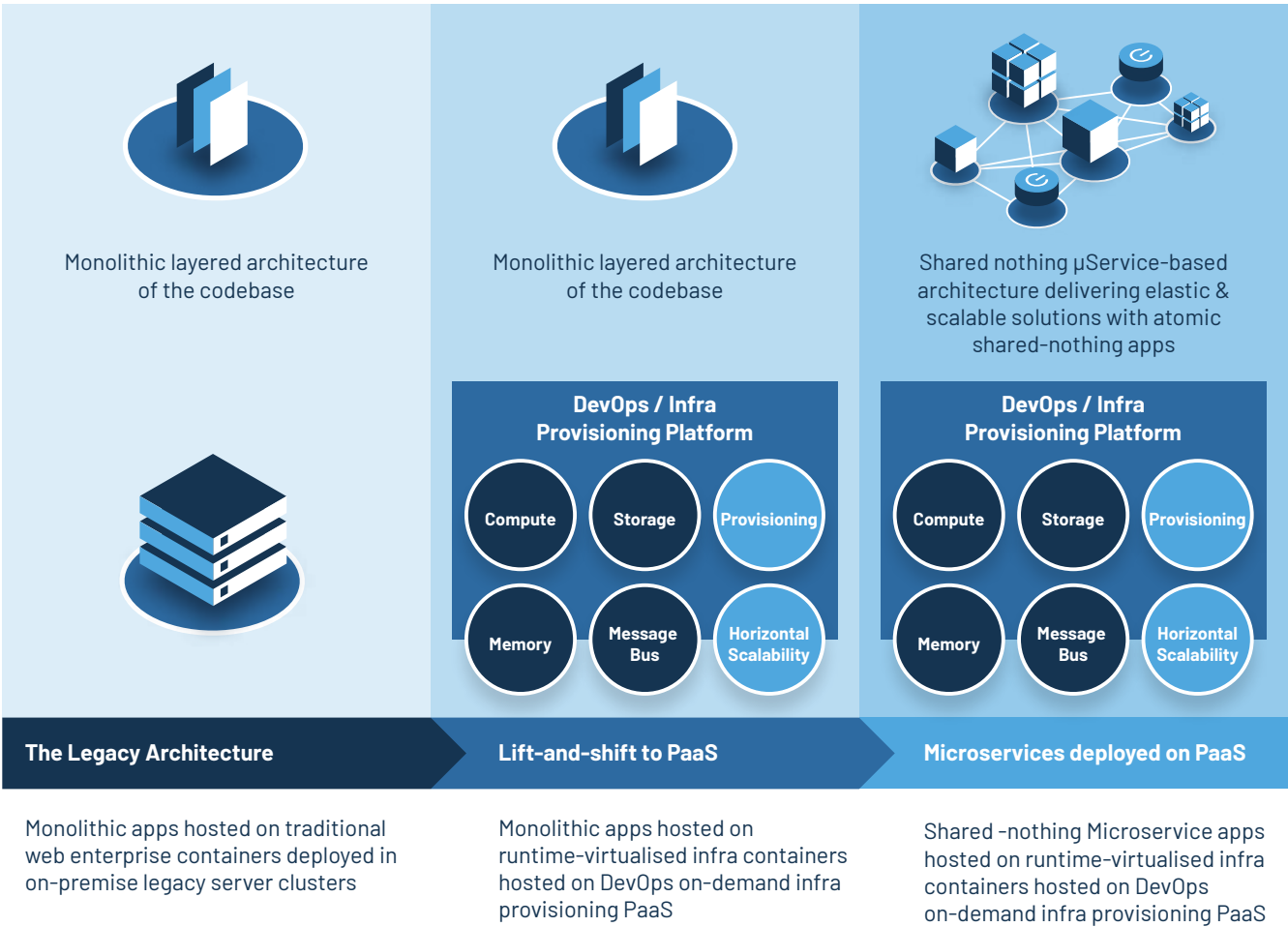
A Hexagonal (Microservice) Architecture:
Loosely coupled contexts and independent architectural components running on multiple shared-nothing runtimes and communicating via ports, adapters and binding based dependencies only. Applications can be seamlessly scaled without bounds. Maintanances is simple and customizable to the NFR / business asks of each components.
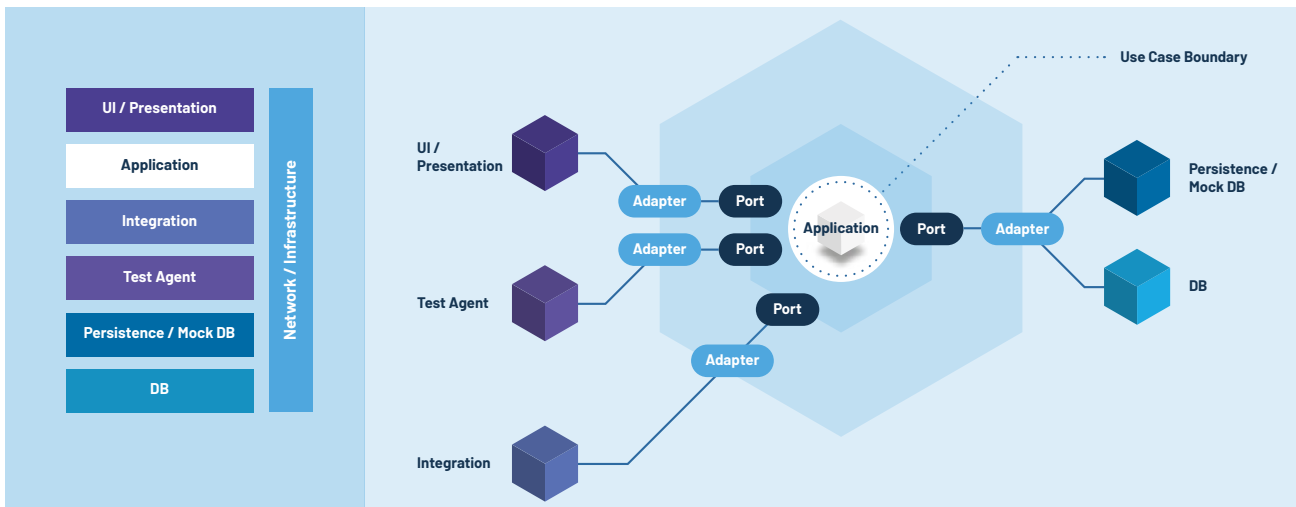
Monolith to microservices transformation journey

[Exhibit- This diagram shows a typical journey from monolithic to API-based technology stack]

Monolithic layered architecture of the codebase

Monolithic layered architecture of the codebase

Shared nothing µService-based architecture delivering elastic & scalable solutions with atomic shared-nothing apps

DevOps / Infra Provisioning Platform

Compute | Storage | Provisioning
Memory | Message Bus | Horizontal Scalability

DevOps / Infra Provisioning Platform

Compute | Storage | Provisioning
Memory | Message Bus | Horizontal Scalability

The Legacy Architecture

Lift-and-shift to PaaS

Microservices deployed on PaaS

Monolithic apps hosted on traditional web enterprise containers deployed in on-premise legacy server clusters

Monolithic apps hosted on runtime-virtualised infra containers hosted on DevOps on-demand infra provisioning PaaS

Shared –nothing Microservice apps hosted on runtime-virtualised infra containers hosted on DevOps on-demand infra provisioning PaaS

Typical stages of a monolith to microservice transformation journey

Impact Area	Present Day	Transitional State	Target State
Teams	Monolith development tightly coupled to assigned team	Monolith development tightly coupled to assigned team	Independent development assigned to loosely coupled teams
Functional scalability	Not an option	Not an option	App components can be functionally scaled
Infra scalability	Infra can only be vertically scaled	On-demand horizontal scaling of virtualized containerised infra	On-demand horizontal scaling of virtualized containerised infra
Software License	Software license tightly coupled to assigned on-premise server cluster nodes	Software license provisioned on-demand	Software license provisioned on-demand

How Virtusa can help

Virtusa's Cloud Transformation practice has significant experience working with clients to evaluate how to transform monolithic applications into API-connected microservices. We partner with all major CSPs, including Google Cloud Platform, Amazon Web Services, and Microsoft Azure. We also partner with specialist API-management tech providers, including Google's Apigee, Kong, and WSO2 whose solutions create and publish APIs, police their usage, and monitor performance.

1 **Virtusa's cloud transformations solutions**
Virtusa provides clients with a suite of innovative tools, products, and accelerators that help companies to accelerate the development of cloud-native apps.

2 **The DevOps-based API factory model - Seamless scaling to the next level**
Our API factory model takes the shared-nothing architecture of microservices to the next level, using a CI/CD-based API build pipeline to deliver a seamlessly scalable solution, orchestrated by a Terraform infra-provisioning pipeline.

Key features:

1. Continuous optimization through an iterative approach to development and optimization, which monitors the operational and performance metrics to evaluate how to prioritize components for fine-tuning.

2. Automated software quality checks performance improvement delivered by a site reliability engineering model.

3 **Microservice-coding accelerators**
Virtusa has developed coding accelerators and automated, rule-based boilerplate microservices framework generators which cut down the development time for APIs by up to 30-40%.

4 **Virtusa's Open Innovation Platform**
Virtusa's Open Innovation Platform provides a CSP-agnostic way to capitalize on emerging technologies by developing new cloud-native applications. It supports the entire innovation process, from ideation and emerging tech discovery through to technical prototype development. The platform creates a virtual innovation lab in the cloud that companies can use to engage with the emerging tech community, from fin-techs and academics through to "intrapreneurs". The platform offers the workflow traditionally found in innovation management tools assuring good pipeline flow so that more of the best ideas make it to production. It also offers a sandbox in which new solutions can be bolted together quickly and tested with meaningful data.

References

1. Cloud migration 2.0: shifting priorities for application modernization in 2019: Retrieved March 18, 2020 from https://www.qa-financial.com/public/storage/videowhitepaper/whitepaper_file/qa-vector-and-cast---cloud-migration-2-0---shifting-priorities-for-application-modernization-in-2019-making-sense-of-cloud-transitions-for-financial-and-telecoms-firms-1571751840.pdf

2. A commissioned study conducted by Forrester Consulting on behalf of Virtustream (July 2018): Multi-cloud Arises From Changing Cloud Priorities. Retrieved March 18, 2020 from https://www.virtustream.com/lp/forrester-multicloud-study;

3. Kasey Panetta (October 10, 2019) Is the Cloud Secure. Retrieved March 18, 2020 from https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

4. Flexera, (2019, RightScale 2019 State of the Cloud Report from Flexera. Retrieved on March 18, 2020, from https://info.flexera.com/SLO-CM-WP-State-of-the-Cloud-2019

5. Synergy Research Group (October 29, 2019), Amazon, Microsoft, Google and Alibaba Strengthen their Grip on the Public Cloud Market. Retrieved on March 18, 2020 from, https://www.srgresearch.com/articles/amazon-microsoft-google-and-alibaba-strengthen-their-grip-public-cloud-market

6. FT Article (PUBLICATION DATE) Privacy uproar shows Google cloud business has a trust problem, Retrieved March 18, 2020, from https://www.ft.com/content/a2afd690-0703-11ea-a984-fbbacad9e7dd

7. Janosch Delcker (9/26/19), Germany's plan to control its own data. Retrieved on March 18, 2020, from https://www.politico.eu/article/germanys-plan-to-control-its-own-data-digital-infrastructure/

8. European Union Agency For Cybersecurity Report (Publication date), Risk Assessment. Retrieved on March 18, 2020, from https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security/risk-assessment

9. European Banking Authority, (25 February 2019), EBA Guidelines on outsourcing arrangements. Retrieved on March 18, 2020, from https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements

10. Vargo, S., Fong-Jones, L. (2018, May 8). SRE vs. DevOps: competing standards or close friends?. Retrieved on March 18, 2020, from https://cloud.google.com/blog/products/gcp/sre-vs-devops-competing-standards-or-close-friends

11. Willis, J. (2012, May 1). DevOps Culture (Part 1). Retrieved on March 18, 2020, from https://itrevolution.com/devops-culture-part-1/

12. Nicole Forsgren (August 22, 2019), 2019 Accelerate State of DevOps Report. Retrieved on March 18, 2020 from https://cloud.google.com/blog/products/devops-sre/the-2019-accelerate-state-of-devops-elite-performance-productivity-and-scaling

13. Puppet, CircleCI & Splunk (2019), 2019 State of DevOps Report. Retrieved on March 18, 2020 from https://puppet.com/resources/report/state-of-devops-report/

I ♥ CLOUD
TRANSFORMATION

We are
innovation
engineers

vírtusa

vírtusa

About Virtusa

Virtusa Corporation (NASDAQ GS: VRTU) is a global provider of digital business strategy, digital engineering, and information technology (IT) services and solutions that help clients change, disrupt, and unlock new value through innovation engineering. Virtusa serves Global 2000 companies in the Banking, Financial Services, Insurance, Healthcare, Communications, Media, Entertainment, Travel, Manufacturing, and Technology industries.

Virtusa helps clients grow their business with innovative products and services that create operational efficiency using digital labor, future-proof operational and IT platforms, and rationalization and modernization of IT applications infrastructure. This is achieved through a unique approach blending deep contextual expertise, empowered agile teams, and measurably better engineering to create holistic solutions that drive business forward at unparalleled velocity enabled by a culture of cooperative disruption.

cloud.virtusa.com

virtusa