CHAPTER 1

The Ever-Changing Landscape of the Cloud

When we conceived the idea of this book, we first wanted to ensure that you have a high-level view of how cloud technologies have changed and disrupted various industries in the recent past. The latest innovation in technology, "the Cloud," has changed things for good. Various organizations big and small are impacted and have been forced to adopt and include cloud technologies as part of their modernization strategy. No matter how big or small your organization is, which technology or product you use, and how you use it, you need to know what is happening in your environment, which triggers or events are important, and when and how you should react. Effective monitoring of the environment helps you achieve that. Monitoring is just not a collection of a few steps or actions; it is a complete process on its own that is unique to each organization and business. This is a cloud adoption and digital modernization journey.

The digital modernization journey can be both exhilarating as well as exhausting for enterprises as there are many moving parts to be taken care of during cloud adoption. This includes but is not limited to migration considerations, security, resiliency, high availability, and monitoring.

B. Chakraborty and S. A. Karthikeyan, *Understanding Azure Monitoring*,
https://doi.org/10.1007/978-1-4842-5130-0_1

For most organizations, the landscape is often hybrid, where some crucial application components remain on-premises during the initial phases while other tiers of the architecture are moved to the cloud. Stitching these components together in the monitoring layer often becomes a challenge, especially with the multitude of monitoring tools available in the market, both cloud native as well as third party. This book will attempt to cover the various architectural constructs of Azure monitoring capabilities and how it can be leveraged by an enterprise to respond to the growing operational and security requirements in the cloud.

In this chapter, we will quickly touch upon how public cloud computing changing the operational aspects of modern enterprises – those who have adopted, those who are born in the cloud, and those who are still strategizing and identifying what works for them and what doesn't. In each case, they need to identify how things change to be in a fully functional operationalization state.

The Traditional and the New

Let's look at how various industries and organizations at various maturity levels look at public cloud technologies.

Any change is complex and complicated. It is a process and cannot be achieved overnight. The same applies to cloud journey for digital modernization as well. Today, in every industry, many companies have accepted the need for cloud technology adoption. Based on the maturity level of the organization, they are looking to invest and innovate in always available, economical, resilient cloud infrastructure. Let us now look at how various industries, based on their scale of operation, are adopting the cloud and why.

Start-ups: They are the happiest segment to adopt the cloud technologies, the main reason being that there is no upfront capital expenditure. Most cloud providers offer a "pay-as-you-go" model in which

you pay only for what you consume and only incur operational expenses. You will not be investing your money in an asset that you do not know how long you would really use. Furthermore, based on your usage, you can easily add or reduce resources and so you eventually pay less. Additionally, you do not need to hire someone to plan or procure any resources; it's just out there, and you can start consuming at the click of a button. This not only helps to reduce the risk of capital investment but also protects from unfortunate loss in case of venture failure.

Mid-sized organizations: This segment still can move quickly comparatively to the giant enterprises who have a lot of restrictions due to their scale of operations. They would like to innovate quickly, while also spending less time and effort to re-create an environment and restart experimentation again. At the same time, they would like to expand operations to new countries, regions, or reach out to new consumer segments, etc., making cloud technologies their best bet. The new age cloud technologies enable them to expand and effectively use resources and reduce costs and, at the same time, attain higher security compliance and governance. Exploring new markets and consumer segments or launching new product lines or categories become much easier.

Enterprises: Out of several challenges, the most prominent one for the modern enterprises is to maintain continuous growth without hurting any existing customer base or market. While the competition is very steep with several giant enterprises competing with each other in the same industry, it has pushed them to adopt a place to achieve higher resiliency, improved experimentation, security and compliance, hyperscalability, and quicker launch cycles of products to stay ahead of the competition. They are also well placed to introduce a good bargain in terms of pricing and contracting with the cloud vendor, owing to the sheer scale of operation and consumption.

Now let us look at some of familiar industries and how they are adopting the cloud and what parameters they look at while choosing a cloud vendor.

Banking, finance, and insurance: If you speak to any bank or insurance organization, the first word they would utter is "Security," the second is "Compliance," then everything else can follow. Of course, for obvious reasons, gaining trust in someone else's premises takes a while to grow, especially when you are dealing with someone else's money and keeping all information on someone else's platform. The adoption has been slow but it's gaining momentum for specific operations. For example, every bank wants to engage their customer effectively, keep an open communication mechanism, innovate on their products, and reach out to more customers. While the same holds true for the insurance sector, they also would like to run risk profiling and huge queries against millions of customer records before providing any loan or insurance. The advent of FinTech companies made competition more tough. Unlike any traditional banks, FinTech companies are leveraging cloud tools/technologies like big data analytics, blockchain, machine learning to learn consumer behavior, much faster loan approval processes, and live customer interaction with video conferencing, etc. These have been disrupting the industry as a whole, opening up new avenues and changing how this sector used to operate. Among all these, to maintain the security posture, they need to know "what," "when," "how," "who," "where" of any event and its impact; they need a strong monitoring mechanism of every service they use and deploy.

Retail: Like banking, finance, and insurance, security, customer engagement and availability of the platform are the core aspects that the retail industry looks for while selecting a cloud platform. In terms of other priorities, these include providing the latest, freshest, and greatest customer experience, using an interactive platform that can provide a wide variety of choices, the capability to integrate with other service providers (e.g., banks and payment gateways) for loan processing and secure online payment. We notice the adoption of the cloud in this industry is faster since the very nature of the cloud platform being hyperscale, creating global presence in a minimal time frame, quicker

onboarding, and the ability to reach out to customers from other countries at a very reduced cost. It reduces the capital investments on IT assets in other countries. You can now deploy a website in minutes without having to create any virtual machines, build a network infrastructure, and upload your product catalogue.

Media and advertising: Exabytes of data, large-sized files, formatting, encoding-decoding, and delivering them in various forms and sizes of devices are the core operations involved in this industry. Hyperscale processing, availability in minutes, and the capability of serving a global customer base are the key demands of this industry. At the same time, when to scale; what went wrong, when; and preventive measures to be taken are the key metrics the organizations need to know.

Manufacturing, oil and gas: These were a little late into the cloud adoption until IoT (Internet of Things) picked up the pace. The processes in HR, supply chain, customer engagement, CRM systems, etc., were among the early to onboard. Embedding some of the special chips into the actual manufacturing devices was the difficult part. Predictive maintenance, predictability in terms of quantitative outputs, and ensuring greater quality are the key drivers to move to the cloud. Whether it is deep sea exploration; or identifying and researching the quality of oil in the rocks, which requires high performance computing, new age computing has it all to serve this industry to the fullest.

On similar lines, we have health care, engineering and software, education, and so many more industries that have key requirements and reasons for choosing a cloud-based solution. At the same time, monitoring all the services hosted and making sure appropriate processes and tools are in place to handle any security and non-security events are key to its success. Microsoft Azure, being one of many cloud services providers, does just that. Let's us now look further into Microsoft Azure and see how it can help achieve key business objectives.

Microsoft Azure as a Strategic Choice

There are several public cloud service providers, and among them we have a few that really stand out: Amazon Web Services (AWS), Microsoft Azure, Google, Oracle, IBM, and Alibaba Cloud. It is always a matter of debate and discussion of which one is better? Who has better services for a lesser price? Who can satisfy my need better and generate value for me? And there are so many similar questions. While each of these service providers has similar services and certain times, each one is better than the other in certain ways, the main question that matters to most of the customers is which one can meet my requirements better and become a partner in my transformation journey?

As an architect, it will always be difficult to choose one over the other in terms of value; as a consultant or seller, there will always be a way to compare and contrast the features and capabilities. However, we all know that for one reason or other, we can always find the most suitable one that can meet our requirements and provide better value for our money. In the context of this particular book, let us look at some of these aspects specific to Azure before we dive deep in to the monitoring pieces. The items discussed next set the context of the capabilities that we will explore in upcoming chapters as well.

Decades of experience: Microsoft has been a leading software and services provider over the last three decades. Although it is one of the best choices in the enterprise segment, it has very good focus and presence for the middle and small businesses too. Its existing ISV ecosystem and strong and innovative services development have been able to deliver what is expected of them. This is why, as of today, Microsoft Azure serves more than 95% of the Fortune 500 companies. Enterprises trust Microsoft Azure.

Company focus and growth: The company has been investing heavily into the development of cloud-based technologies and product areas like blockchain, cybersecurity, IoT, containers, virtual reality, artificial intelligence, gaming, privacy, and security. In recent news, Microsoft

stated that it will invest $5 billion globally in IoT over the next four years. News from January 2017 stated that Microsoft will continue to invest over $1 billion a year on cybersecurity. Its commitment to the common good – "Cloud for Global Good" is a page that you must visit to know more about Microsoft's policy road map: https://news.microsoft.com/cloudforgood/.

Global presence: Per recent data and information on Microsoft's website, its Azure services are available in over 140 countries, 54 regions worldwide, and up to 1.6 Pbps of bandwidth in a region – more than 130 edge node locations and 70,000 miles of fiber and undersea cable systems. These figures ensure its dominance in any country to serve the customer and stay close to them.

Wide partner network: Microsoft is well known for working with partners and reaching out to a larger customer base. It has a very wide range of partner programs that helps partners to leverage the new business opportunities in the cloud world through tools, resources, training, presales technical help, and best practices to grow their business. At the same time, they help to build necessary capabilities for Microsoft Azure and show to use it to their advantage. Microsoft reportedly has more than 64,000 cloud partners with various competencies – more than AWS, Google, and Salesforce combined.

Focus on open source: Microsoft has extended its Azure platform to support most open source languages, operating systems, tools, and frameworks. Microsoft recently acquired GitHub wherein it shares APIs, SDKs, and several open source projects, for example, Visual Studio Code, .Net, and TypeScript where Microsoft developers contribute every day. It's a must to visit: https://github.com/Azure. For open source releases, visit: https://opensource.microsoft.com/. Microsoft Azure supports an extremely broad selection of programming languages and tools, such as: .NET Framework, Node.js, PHP, Python, Ruby, Java, and more. Microsoft Azure fully supports hosting Linux virtual machines. In fact, 25% of Virtual Machines running on Microsoft Azure are running a distribution of Linux.

Hybrid cloud: Microsoft Azure can be easily used as an extended datacenter for its customers. Every customer wants to experience, test, and then host their workload on Azure. Once they are happy and satisfied with its services and capabilities, that is when the first step to migration is taken. Microsoft Azure can be integrated with an on-premises datacenters and branch offices with VPN connectivity, ExpressRoute, and Azure WAN. With such integration, an application can be deployed on Azure and at the same time can leverage all on-premises resources. An integrated monitoring and security posture can also be implemented across the IT assets, deployments, and ensure governance. For a true hybrid cloud experience, customers and partners can leverage Azure stack for similar Azure-like experiences on-premises. It's also worth mentioning the fact that since both Azure Stack and Azure leverage the same architecture, the same application once deployed can easily be ported or migrated from Azure to on-premises or the other way around without having to make any application changes. This is a huge win for customers.

Strong support and services system: Microsoft is well known for its support and consulting services. It has an established process and support model to help the customer when required, based on 24x7x365 days and critically based SLAs.

Given some of the core factors as discussed, Microsoft Azure is a strategic choice for customers, and we see good case studies of digital transformation in various industries. Visit `https://azure.microsoft.com/en-in/case-studies/` for more details.

The Multi-Cloud Strategy

With the higher adoption of cloud, most organizations prefer to adopt a multi-cloud strategy to host their application. This is due to various reasons, including breaking provider dependency, increasing reliability, better cost negotiation, reducing the attack surface, adopting

a development model that fits across cloud deployment, and a safe datacenter exit strategy. Deciding a strategy is one challenge and implementing it is another. Operationalization and monitoring across the cloud and having visibility of end-to-end deployment is a difficult task to achieve without the right set of tools and methods. At times, the same monitoring tool may not be sufficient for the needs and requirements to be used to integrate with other tools to achieve the required goals. Hence, choosing the right tool for your needs is absolutely important for multi-cloud strategy success.

Operationalization and Learning Curve

The cloud adoption journey starts with an envisioning phase where an enterprise cloud adoption strategy is defined. The vision and scope should be clear and well defined to give the organization a sense of direction. While there is a huge demand for a cloud-first approach for new applications, transformation of existing applications could result in a hybrid architecture. In both approaches, cloud adoption moves through the cycle shown in Figure 1-1.

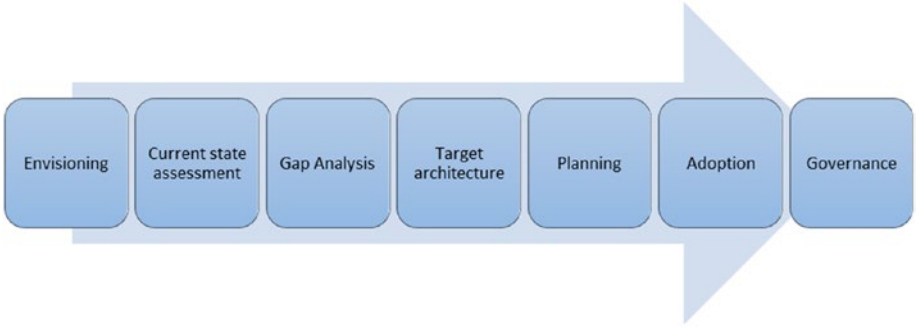

Figure 1-1. *Cloud adoption cycle*

1. **Envisioning:** High-level goals and objectives of digital transformation are defined at this phase. It is important to consider how an organization wants to adopt a public cloud and at what velocity, aligning it with the business requirements.

2. **Current state assessment:** Thorough assessment of current state architecture is important to baseline the maturity levels of an organization to adopt a public cloud. Based on the assessment, it will be easier to define the adoption approach, identify the gaps, and kick-start the planning activities.

3. **Gap analysis:** This exercise will help to identity that the application requirements match with the configurations available in cloud technologies. Any bottlenecks like legacy applications, hardware dependencies, platform mismatch, etc., should be identified at this phase.

4. **Target architecture:** The future state in the target public cloud platform, covering at minimum the logical components and their placement, should be defined before moving on to the adoption phase. This can be further iterated to sketch out the high-level technical architecture covering the security, identity, and monitoring components along with basic compute, storage, and network detailing.

5. **Planning:** The outputs from the previous phases should help develop a detailed migration/adoption plan. Risk mitigation based on the Gap analysis should also be factored into this plan. A dry run or POC can also be part of the planning phase to gain more confidence and iron out the challenges.

6. **Adoption:** The adoption or migration process should be done in such a manner as to avoid disruptions in day-to-day business. Sometimes it could be inevitable, but the impact can be minimized with diligent planning.

7. **Governance:** Post-adoption, many organizations find it difficult or overwhelming to adapt to the new technologies and processes. It is important to ensure that a governance plan is in place, which covers various factors like ramping up the organization's IT team, defining security cadence, as well as a monitoring framework.

Migrating or deploying a workload to the cloud is easy, but consuming, maintaining, and adopting the new environment is the difficult part for most organizations, especially when they have multiple clouds, several autonomous organizational structures, and various toolsets on-premises. Which one would work seamlessly and which one requires to be integrated is a task that is most often-debated and discussed questions during the build stage of any cloud adoption. In any scenario, however, there is a learning curve that the IT services has to recognize and accept. Defining new roles and responsibilities or establishing a CoE team that can help in the process is important in this stage.

This discussion should have given you a fair idea of how cloud is changing the way we operate, what are the key aspects any organization look for when they think about cloud journey, key capabilities required

by the provider to support such requirements, how adopting a new tool or service requires investigation into its capability to serve multi-cloud deployments, and the learning curve to operationalize. How familiar the tool is, how easy to integrate and operate and what is already in use currently usually decides the adoption. We also looked at how Microsoft is committed to this journey and provides the assurance that their necessary tooling and support make this happen.

An Architect's Challenge

Traditionally, monitoring is an infrastructure or security architect's favorite subject and is discussed mostly at this level. However, with the challenges experienced early on in in the cloud world, it takes center stage during solution development, and the build and stabilization stage, ensuring there are no gaps when it comes to fully operationalize. Hence as an architect (Solution, Infra, Security, or software) overall, there are very common aspects at hand that require attention.

What is the current practice and who handles monitoring?
The lines are often blurred when it comes to monitoring different components of the application in the cloud. For example, the network team will focus on the network layer monitoring and security, the infrastructure team might look into the aspects of OS monitoring, while the application team will use application-specific tools to look out for application anomalies, performance metrics, etc.

What tool do they use, and is it compatible?
Most organizations will have existing investments in monitoring tools to monitor their on-premises datacenters. It is important to analyze the compatibility of existing tools with the cloud-based architecture, find a common ground, and reuse as much as possible.

Will the existing or new tool be able to monitor the existing workload on the cloud?
Cloud-based workloads are hosted and managed much differently than when they were hosted on-premises. Moving forward from IaaS, capability of monitoring PaaS- and SaaS-based services are also the demand of the hour. If this falls beyond the capability of existing tools, a new tool should be considered.

Will it be able to monitor the new application developed for the cloud?
Cloud-first development strategies results in applications with a sea of difference from their traditional counterparts. Also, it is often seen that organizations tend to move away from monolithic architectures, adopting a microservices approach in the cloud during modernization of their workloads. Monitoring tools should be evolved to cater to all these use cases.

What level of integration does it provide with on-premises tools?
Integration of cloud-based monitoring tools with on-premises tools is important to implement a "single pane of management" strategy. Hopping between tools is what any IT team would want to avoid at any cost.

What is the learning curve to adopt a new tool, and who provides it?
If the new tool being considered is drastically different from existing ones, the learning curve and time taken to adapt and well train the IT team adds to the timelines taken to completely operationalize the environment.

Can it provide end-to-end visibility of my IT deployment?
This reiterates the point of a single pane of management, where the monitoring tools should be able to give full visibility of the IT deployment health.

Will it be able to monitor my virtualized assets and devices deployed in the cloud?

Many devices like firewalls, IDS, IPS, load balancers, etc., will have their virtualized counterparts deployed in the cloud, either native or from third-party solution providers. The tool being used should be capable of monitoring the health of such a diverse portfolio of devices.

What about my PaaS and SaaS services?

With digital modernization, PaaS and SaaS services get introduced to the IT landscape, which will come under the purview of monitoring.

What data does it hold and where if it is a cloud-based service?

With monitoring data coming in from different sources, we need to ensure the safety of this data in transit and at rest as it contains valuable information about the current state of affairs in your IT landscape.

What is the reliability and scale of the system?

The tools being considered should be resilient, reliable, and designed with the capability to scale when required. As more and more applications get added to the portfolio, being restricted by the scale of a tool is not acceptable.

What are its analytics and telemetry capability?

Having raw data is not very useful, unless you can derive intelligence out of it. The tools being used should have the analytics and telemetry capability to get this done without the customer having to spend hours to build it in as an add-on.

Can it integrate with my existing ticketing and SIEM systems?
The goal of monitoring tools, in simple terms, is to bring any anomalies to the attention of the right people. Some tools might offer plug and play capability to your existing ticketing and SIEM systems, while some might offer it in parts.

How do I define my diagnostic and logging data storage?
Diagnostics data is often found to grow exponentially over a period of years, months, or even weeks depending on the scale of your application. The right sizing and management of diagnostics and logging data storage are crucial components of operationalization.

Are there any alternate tools that can do this in an easier way?
We need to objectively analyze the time taken for deployment and the learning curve as well as other factors like reliability and scalability before finalizing the monitoring tool.

Will I require a separate deployment for my monitoring system, or is it cloud based in its entirety?
If a new tool is being considered, it is smarter to consider cloud-based options as managing a different deployment for a monitoring system will introduce additional overhead costs.

What value does it provide in addition to my existing system?
If the new tool does not provide any compelling value addition, it might make more sense to integrate the cloud-based environment with the existing monitoring tools.

How much does it cost?
Some tough calls should be made whether to continue with the existing capital investment approach or move toward a pay-as-you-go pricing model.

What is the implementation and management overhead?
If a significant investment of time and money is required to implement and manage a new tool, it might be prudent to use a more cloud-aligned version of the existing tool with minimal configuration overhead.

Will it reduce my existing pain points?
Traditional monitoring tools may not have all the functionalities when compared to their new Gen counterparts, and these requirements should be evaluated carefully to understand the trade-offs. For example, you need mobile interfaces or applications to check the status of your deployment even when you are not in front of your computer, or it could be as basic as integration with your ticketing system.

Does it follow industry standards?
A matured monitoring tool is expected to support certain standards, say multiple probing and heard-bear mechanisms, out-of-box dashboards, reports, agentless monitoring wherever possible, etc. Any new tool in consideration should match up with these expectations.

Is it from the same provider or from a different vendor?
Organizations could leverage the existing support ecosystem if they transition to a cloud-based tool from the same service provider or vendor. Getting a new vendor onboarded and establishing rapport could again add on to the timeline of the operationalize phase.

Is it futuristic, and what is its future road map?
The capability of the service provider to stay ahead of the market requirements should be closely analyzed. How they have fared in the past and what is being announced in the road map are key factors in this.

Will it align with my existing security posture?
New tools should be able to maintain, if not improve, the overall security posture of your IT deployment. What more it brings to the table for the latter will be interesting to explore.

What level of automation can I achieve with this?
Be it onboarding, ad hoc configurations, or ongoing maintenance, automation should be built into the DNA of any monitoring tool. It is wasteful to spend man hours on items that can be easily automated using scripts or scheduled tasks. Maturity with respect to automation becomes one of the key decision points while selecting the monitoring tool.

This is new to me; how do I get best practices and recommendations?
Last but not least, the customer should get enough confidence from the vendor or service provider that an optimal monitoring system can be implemented in place using the tool, and the relevant best practices and recommendations required for the same will be provided. It could be through how-to-do documents, webinars, classroom trainings, etc.

Key Architectural Constructs and Operational Efficiency

We monitor for predictability, proactivity, security posture, incident response, and operational efficiency. However, it's important to understand how quickly you can gain insights from the piles of data collected in various forms, what reports we can generate to visualize, and how we can automate certain tasks to be more efficient and responsive.

Derive Intelligence from the Noise

The enterprise IT landscape is vast. Monitoring and logging information from different components often results in information overload. The monitoring toolset should have the capability to filter through this noise and find the information, trends, or occurrences that are relevant to the organization. For example,: a random event occurring intermittently in your server could point to a deeper issue that will go unnoticed if a proper trend analysis is not done. Manually writing queries to extract this information is cumbersome or near to impossible. Hence the tools should come equipped with these to quickly retrieve information relevant to your application's health.

Visualization and Reporting

As environments become complex with multiple component dependencies, it becomes difficult to pinpoint the root cause when something goes wrong. For example, a degraded performance of the application could be related to a faulty component in the hosting environment, faulty code, or even due to an organized attack on the front end. Getting results from querying the logs or checking the system health status of independent elements may not give you the big picture – hence

the importance of visualization. When data from all these sources are visualized on a single dashboard with their dependencies marked out, it is easy to spot the stray element causing issues. Today, all leading tools come built in with some visualization elements or the ability to plug in to visualization services. It is the maturity of this aspect that should be considered in terms of ease of configuration, variety of reports, ability to interconnect elements, etc., while finalizing the tool.

Automation and Auto-Remediation

As explained in the previous section, the level of automation offered by the tool is a major deciding factor. In the event of an error, it is desirable that the tool can perform first aid through auto-remediation mechanisms. Using auto-remediation, you could nip many minor issues in the bud before it escalates, giving you breathing space for further root cause analysis. It could be a script executed natively by the tool or even an API call to another automation tool. For large-scale environments, this feature is a "must have" rather than a feel good add-on.

Incident Response and Triaging

Anything that goes beyond auto-remediation should be channeled to an incident response team. The majority of tools have alert mechanisms built in, where emails, SMS, etc., can be sent to relevant operations team members. However, this could lead to disjointed efforts with multiple people looking into the same issue when an alert is received. Hence the tool should have the intelligence to integrate the alerts with proper ITSM channels and triage it based on the criticality.

Summary

In this chapter, we looked at various industries and what aspects of the cloud interests them, as well as what capabilities they usually look for when it comes to monitoring. Non-negotiable capabilities, functionalities and features aligned to organizational strategy are probably some of the most difficult questions to answer. When we propose a monitoring solution, we should be well prepared to face these questions and how to address them. We should include monitoring as a main agenda item when developing or delivering a software, solution, or project. The monitoring tool or product is a solution on its own and should have all the important design constructs baked into it. It is an undisputed pillar for a reliable system. We cannot depend on our system's reliability if the monitoring system itself is not reliable.

In the next chapter, we will look into Azure monitoring and how it addresses all the various aspects we have discussed so far. We will also look at its core capabilities, and how to achieve them.