NUTANIX

7 MOST COMMON

CLOUD ADOPTION MISTAKES

Organizations are rapidly adopting multi-cloud strategies, evaluating ways to foster greater agility and enable more rapid innovation. We've been tracking public cloud adoption and consumption of over $1 billion on an annual basis among our customers, providing a variety of interesting insights that we share in the Nutanix Annual Public Cloud Usage Report.

In conversations with many small and medium businesses (SMBs) and enterprises, we noticed that organizations often struggle with their infrastructure costs after initial cloud adoption due to lack of proper cloud strategy, planning, and governance mechanisms. Cost visibility and governance have evolved into primary challenges for organizations. This calls for a well thought-out cloud strategy.

While interacting with cloud decision-makers and budget owners like Heads of Cloud Strategy, Heads of IT, CIOs, CTOs, IT managers, and CFOs to understand their pain points, we realized that many companies make similar mistakes. What follows are some of the most common mistakes that executives and managers make while moving into cloud, so you can adequately prepare for **your cloud journey**.

1

Having an old infrastructure mindset

Organizations adopting cloud as part of their infrastructure strategy often forget how necessary change management is. They overlook or underestimate the type of company culture required for seamless cloud adoption and management. Many customers manage cloud operations like a traditional on-premise setup with the mindset that the only change is in the provisioning process. Without a significant change in terms of how organizations approach planning, monitoring, and managing cloud infrastructure, there can be an explosive impact on cloud spend.

Understanding the precise costs and challenges that the cloud will introduce isn't easy. Despite a detailed, pragmatic approach towards building a cloud strategy, a majority of organizations still fail at some point. And our cloud geeks attribute it to 'blind spots' that get overlooked either due to complexity or lack of awareness. Soon enough, in some cases, these blind spots might take the team back to the boardroom.

To usher in the right approach towards building a seamless and successful public cloud strategy, we've collated the top seven blind spots that smart companies watch out for during their cloud-first and cloud-ready journey.

CALCULATING THE 'REAL' TOTAL COST OF OWNERSHIP (TCO)

Many companies have realized that the real benefit of cloud computing is not the cost savings it can bring. But it is the agility and time-to-market. And the prominent factor that plays a vital role in bringing such a nimbleness are the TCO models. However, many companies don't define the actual TCO. They just go by the cloud infrastructure cost data alone, which may save some operational expenses in the short term but not in the long term. Hence, they end up missing the market when it comes to IT's ability to deliver the real value of the business.

The way forward is to consider TCO models that also identify gray areas, and take them into account during calculations. Mainly, these models must understand the actual value of cloud-based technology. Plus, they should & must take critical factors into account too, like existing infrastructure in place, existing skills & workforce involved, the cost of all the cloud services when in operations, value of agility & time-to-market, future capital expenditures, and risks relating to compliance issues.

KNOWING WHO OWNS THE DATA IN THE CLOUD, AND HOW TO RECOVER IT

Understanding the terms of a cloud service is paramount. Agreed. But it is more critical to know who owns the data in the system. The decisiveness lies in carefully checking the terms and conditions of the contract and ensure the data policy includes all the fine lines that ensure the actual owner owns the data.

By doing so, you, as a user, can own and recover the data on-demand. Above all, your service provider cannot access, use, or share your data in any shape or form without your written permission.

HAVING STRONG SERVICE LEVEL AGREEMENTS (SLAS)

While you focus on putting data policy and terms of cloud service in place, you should not change the spotlight on SLAs. A strong SLA goes a long way in monitoring, measuring, and managing how the cloud service provider's services are performing. The essence lies in working closely with lawyers who can help define strong contracts. And also help you get what you want from the service, and whether this can be expressed in the contract.

If you still find this less important, then consider this scenario: You have SLAs with AWS but have no idea how its SaaS offering is performing. That's because AWS provides figures for the performance of the infrastructure, not the software.

MAKING COMPLETE USE OF ELASTICITY OF THE CLOUD

Many enterprises fail to develop a cloud strategy that are linked to business outcomes, because they miss out leveraging the real benefits of elasticity feature that a cloud offers. They purchase instances in bulk to handle peak demands, like how they did with on-premise IT infra, and then turn a blind eye towards idle resources that could be optimized easily. They also overlook the fact that 'anything and everything' on the cloud can be codified. And APIs can be used to automate the tasks on the cloud completely.

BRIDGING THE CLOUD SECURITY AND COMPLIANCE GAPS PROPERLY

With the choice of public cloud, which features a shared responsibility model, its users are responsible for their data security and access management of all the cloud resources. While building a cloud strategy, one should respect the fact that the freedom of elasticity that the cloud offers is accompanied by greater responsibility. And this responsibility can be administered only by bridging the cloud security and compliance gaps correctly. How? By adopting continuous security and making a habit of regular audits and backups, preferably automated.

2

Not having upfront governance policies

In conversations with customers we often hear of key challenges organizations face incorporating public cloud assets into their portfolio. Many application owners and technology budget owners are surprised by the unexpectedly high costs of their cloud services and find it challenging to achieve adequate usage governance across the organization. To prevent uncontrolled cloud spend, and to enable more accurate resource planning, cloud teams often seek better visibility. But control of service consumption throughout their cloud environments depends on policy as well.

For most businesses, creating governance policies is usually an afterthought. This leads to mismanagement and friction in thought processes amongst business, product, engineering, and IT teams. Having a cloud resource and usage tagging policy in place before starting to use cloud helps to establish control over the lifecycle of cloud infrastructure investments. Creating customized governance policies—including cost allocation and budget enforcement across multiple teams is a good cloud strategy and helps you track all cloud spend and map consumption to business units easily.

Scaling your cloud infrastructure means that your policies will need to scale with it. This means you must evaluate how growing your environment will impact the management principles we discussed earlier. Policies directly influence performance, availability, security, capacity, cost, compliance, & disaster recovery. Certain policies in one domain may also have an impact on policies set in other areas, so be aware of how everything is connected and potential ripple effects.

And if you're growing your presence in the cloud, you are likely growing your staff and business operations. The number of people you're adding, their location, their scope of work, and data access level are things you need to consider. You'll also need to think about educating your staff on how their cloud activity directly correlates to your business' bottom line. Remember, despite having automated tools at your disposal, success is not completely technology driven. Your employees are a very important variable to consider.

You should have a detailed understanding of the current human resources, processes and technology frameworks. The next step is to build the necessary frameworks that can empower IT teams to do what the business needs, while also allowing end-users the flexibility they need and demand to do their jobs well while benefiting from the features that the cloud offers.

It is important to define the account hierarchy for your cloud, based on business needs and data ownership. Defining this core governance structure with clearly articulated processes can help simplify governance greatly. The more detailed the access definitions are, the greater the security. This eliminates the need to tial attackers. It also helps you assign responsibilities within the team and grant only the required access to each team member, with only a limited number of actions permitted for each user. To give an example, one person may be responsible for managing one particular aspect and another for a different aspect,

then they each get permission for the same subscription, based on their roles. Users can either be assigned standard roles or well-defined custom roles.

TRACKING AND MANAGING RESOURCES

Having the ability to track and manage all existing cloud resources is also extremely important. One great way to track resources, since users are likely to add more resources, is by creating parameters by department, customer, and environment. Metadata can be attached to resources through tags that provide data about the resource or the owner. Using tags is a great way to not only aggregate and group resources in numerous ways, but the data can also be used for chargebacks.

Tags are especially useful when you are dealing with a complex variety of resource groups and resources. Tags allow you to visualize your assets in the most intuitive manner that works best for you. For instance, it could either be based on similar roles or departments or any other division that makes sense. In the absence of these tags, managing multiple resources can often be challenging. Let's say you need to delete resources associated with a particular project, finding each resource that corresponds to that particular project can be a veritable nightmare. In such a scenario, well defined tags can be a real lifesaver.

You can download our Smart Tag Management for Cloud Governance ebook for help with managing cloud resources with programmatic controls.

AUTOMATION

Given the complexity of cloud operations, expecting governance to be performed by an already loaded IT team is unfair and often ineffective. Managing cloud governance manually is not a realistic expectation. Using automation is key for effective governance.

Cloud automation is a fundamental building block for the cloud computing paradigm. The aim of automation essentially is to make all cloud related activities as fast and efficient as possible, with little manual intervention. This is possible through the use of numerous software automation tools. The objective is to overcome the complexity that cloud computing orchestration brings with respect to deploying different resources in the cloud. With automation tools, requests around deployment and allocation of resources can be addressed quickly and efficiently without intervention from the administrator. The administration needs to simply choose the right options and the software takes over from that point. It makes governance much simpler when IT is rid of repetitive and time-intensive tasks that can be automated. With an effective rules engine, automation can help curb extra spending and consumption, and also optimise the use of resources by shutting down workloads when they are not required. The last important aspect that governs cloud governance practices is a thorough understanding of the objective of your cloud implementation. Is your focus on improving IT efficiency? Or are you expecting your cloud to drive business innovation? If you have multiple goals, then you need to ensure that they're not at odds with each other.

Equally significant is an understanding of the overall business strategy and the direction in which the company is heading. All these factors impact your cloud governance strategies. While there is no debate about the relevance of cloud computing, effective cloud governance is essential in order to reap maximum benefits.

3

A lack of control provisioning resources

Cloud gives developers and organizations the freedom to experiment and scale with ease. But with freedom comes a great responsibility to protect the growing attack surface. Which explicitly means – you must have adequate security in place at every level from the perimeter to the application. Infrastructure periphery is the entry point to your premises and it is very important that it is secured. There are different ways to build the security around your infrastructure. Keep in mind it is next to impossible to manually manage and monitor cloud operations performed by each and every person.

Remember, IT no longer has full control over the provisioning, de-provisioning and operations of the cloud infrastructure. This decentralized ownership has increased the complexity for IT teams to provide the compliance and risk manage-ment policies required to protect their businesses. IT needs to find new ways to exert soft controls to protect the business, while not inhib-iting the agility their stakeholders expect now from the cloud. How do they do that exactly? Well with your help of course!

From a network perspective, ensure that you have segregated network and subnet ranges. Especially your application and data store should reside on the private subnet, and entry should only be allowed from single source i.e. load balancer. Deploy site to site VPN connectivity, and direct connect in case of communication between two data centers or sites. Provide client to site VPN connectivity for people to connect to the infrastructure if required remotely. Build network access controls to only allow specific protocols and ports to traverse the data to and from.

By leveraging automation tools to enforce security and compliance controls, organizations will achieve regulatory compliance at speed, and at scale. The cloud effectively blurs the lines between the platform security and application security, as the automation of compliance and regulatory tests along with application specific quality tests will be the norm.

Staying in the know of the vulnerabilities with your applications, microservices and infrastructure is of utmost importance. If ignored, these vulnerabilities open up the entry gates for intruders and hackers of all kinds. Organizations should perform application and infrastructure vulnerability assessments on a regular basis, and any risks are identified, the security team should work towards remediating those immediately.

Security experts can use different tools available in the market to perform static and dynamic vulnerability assessments to identify risks and different severities. You should also perform host level vulnerability assessments too, by running different tools to identify any risks at the OS level. Developers might be using open source or third party libraries as part of their code base and it is important to assess those libraries and keep them up to date to avoid any security risks. Run these assessments on a monthly or quarterly basis, or as per business requirements.

One additional non-negotiable when it comes to maintaining cloud security is establishing a security checklist. You should have a plan for:

- Access Management
- Data Security
- Infrastructure Security
- Microservices Security
- Threat Management
- Vulnerability Management
- Secure SDLC
- Logging & Auditing
- Incident Response
- Compliance

You can actually download our Top 10 Cloud Security Trends for 2019 ebook for help. Use this action plan to identify the strengths and weaknesses of your current approach to cloud security. It includes recommendations to improve your technology stack, as well as advice on internal change management.

4

Not effectively utilizing pay-as-you-go

Is the 'pay as you go' model saving you money, or is it costing you more? If you don't know which resources are underused and unused, you're just throwing money away by paying for what you don't need. Cloud management platforms help you to 'save' costs while using the 'pay as you go' model by tracking unused and underused resources. This way, you can put your money where your mouth is by identifying recurring costs. One example being smart capacity planning utilizing reserved instances from AWS.

Amazon EC2 Reserved Instances are a great way to save money on your Amazon EC2 bill, provided you have purchased the right RIs at the right time. Therefore, in order to optimize your cloud costs, it is vital to learn how to choose, purchase, and apply the right Reserved Instances for your AWS cloud infrastructure.

SAVINGS

In your AWS cloud ecosystem, RIs provide the greatest savings. You can lower the costs of the resources you are already using in comparison to on-demand pricing. Generally, EC2 and RDS RIs are contenders for projecting the highest figures in your AWS bill. For that reason, it's best to opt for EC2 and RDS reservations.

Case-in-point: Consider an e-commerce website running on AWS on-demand instances. Unexpectedly, it starts gaining popularity among customers. As a result, the IT manager sees a huge spike in their AWS bill due to unplanned sporadic activity in the workload. Now, they are under pressure to control both their budget and efficiently run the infrastructure.

A swift solution to this problem is opting for instance reservation against on-demand resources. By reserving instances, they can not only balance capacity distribution and availability according to work demands, but he can also reap substantial savings.

CAPACITY RESERVATION

With capacity reservation, you're guaranteed to be able to launch an instance at any time during the term of the reservation. Plus, with AWS's auto-scaling feature, you can rest assured that all your workloads are running smoothly—even if there's a spike. There is a catch though; with capacity reservation, there will be a lot of underutilized resources, which will be charged whether they are used or not.

Case-in-point: Picture this: you're running a social networking app in your US West-1A. One day, you notice a spike in the workload as your app goes viral. In such a scenario, reserved capacity and auto-scaling together ensure that the app will work seamlessly. However, during the off-season when the demand is lower, there will be a lot of underutilized resources that will be charged. Regular health checks and management will provide both resource optimization and cost optimization.

ALWAYS DR READY

AWS supports many popular disaster recovery (DR) architectures—from smaller environments ideal for small customer workload datacenter failures to massive environments that enable rapid failover. Since AWS already has data centers in several regions across the globe, it is well-equipped to provide nimble DR services that enable rapid recovery of your IT infrastructure and data.

> **Case-in-point:** Suppose the US east coast is hit by a hurricane and everybody lines up to move their infrastructure to the US-West regions of AWS. If you have reservations in place beforehand in US-West, then you're guaranteed protection. Thus, your critical resources will run on US-West without waiting in the queue.

You can learn more by downloading this strategic guide for optimizing cloud consumption by effectively purchasing AWS Reserved Instances.

5

Not performing continuous cleanup

Cloud gives you the freedom to provision on-demand IT resources. However, over-provisioning cloud resources take a toll on cloud spend. Lack of cloud usage monitoring leads to uncontrolled spend on unused cloud resources like VMs, databases, load balancers, and networks. Even when organizations begin to architect systems with many resources in response to a spike and will remain underutilized during normal workloads. This stems from a failure to take advantage of cloud constructs like auto-scaling or scheduled scaling.

Organizations must develop a solid cloud strategy and processes to continuously monitor cloud usage and eliminate wasteful resources to achieve adequate cloud governance. On average, customers waste 5-25% of their costs on resources they no longer utilize. While cloud offers a convenient "pay-as-you go" pricing model, it's imperative that you develop a "consume-or-eliminate" culture for effective resource utilization.

It's inviting cost trouble if anyone in any of your IT department is able to purchase and spend on anything they wish, without a systematic order in place. Know exactly where each penny is going, by the tagging feature provided by CMPs. It helps you in analyzing resources by business units. Efficient tagging for your cloud infrastructure is a blessing in disguise that will save you piles of money in the future. Without it, you place your organization at great risk for sprawl.

Cloud Sprawl, as defined by Techopedia is "the uncontrolled proliferation of an organization's cloud instances or cloud presence. It happens when an organization inadequately controls, monitors and manages its different cloud instances, resulting in numerous individual cloud instances which may then be forgotten but continue to use up resources or incur costs since most organizations use pay for public cloud services."

As businesses start to adapt cloud services, many are suffering because of cloud sprawling. What's more, the different departments within the organization are using different systems to solve different issues within the cloud. Often organizations do not know how it works and where the gaps in the business are. Additionally, because of the lack of knowledge in cloud technology to begin with; more and more organizations are losing money; while they could potentially be saving it.

SaaS-based platforms and applications best help organizations with this very thing. They make organizations cloud management easier while ensuring efficiency. With SaaS, organizations can leave the maintenance of the physical servers and cloud-based software applications to the SaaS provider. Instead, organizations can use the cloud whilst the SaaS provider manages everything at a subscription fee. Software updates, management of developed software application, and so on are all managed through a web browser. Though you lose some amount of control on the customization of the product; management, updates, and maintenance will no longer be your organization's headache.

6

Not pursuing a DevOps culture

In the cloud, automating provisioning, configuration management, and disaster recovery is easy, but most organizations have yet to adopt DevOps practices. It's important to nurture DevOps culture across your IT and engineering teams to reduce manual effort and increase reliability. Without incorporating DevOps automation as the center of your cloud adoption, you are likely to face increasing challenges in managing cloud services and applications. With DevOps businesses have experienced higher business value, better alignment with IT, helps break down silos, helps build a flexible and software enabled IT Infrastructure.

DevOps is the change in IT culture. It focuses on rapid IT service delivery through the adoption of agile and lean practices in the context of a system-oriented approach according to Gartner. An amalgamation of two words, 'development' and 'operations' it aims at combining software development and software operations. It breaks the barrier between development and operation teams. The collaborative work between them leads to the benefit of combined skill. Operations and development professionals or engineers participate in the entire service lifecycle (which means starting from design to development and till the production support stage). It is characterized by autonomous teams and a constantly learning environment. If you are ready for this adoption, it implies that you are ready to change fast, develop fast, test fast, fail fast, recover fast, learn fast, and also prep fast for product launches.

Large enterprises have adopted DevOps at large (at an enterprise-level). It will finally take the center stage. One of the key benefits that DevOps enables is enhanced collaboration between developers, QA and testing professionals, Operations personnel, people from business planning and security teams.

There are many DevOps tools that are good for different aspects of meeting the requirements of the delivery cycle. Most of the tools that are available help to automate some aspect of the process of software delivery. Tools like Jenkins, Docker, AWS, GitHub, and JIRA are already quite popular in the market.

With DevOps comes a new way of organizing business structure. Managers have been interested in improving cross-department communication in more than one way. DevOps introduces a necessity for collaboration and consolidation between all aspects of an organization and mutual aid between developers, SQA testers, security testers, and every other staff member of the IT sector.

Application security and DevOps must go hand-in-hand. An opportunity lies with to make security an integral part of development and truly build secure coding practices into the early stages of the software development life cycle (SDLC). Thus, DevSecOps can attain the goal of safely distributing security decisions at speed and scale to those who hold the highest level of context without sacrificing the required safety.

With the rapid changes happening in DevOps, traditional security ceases to be an option. Very often, the traditional security is far too late in the cycle and too slow to be cooperative in the design and release phases of a system that is built by iteration. However, with the introduction of DevSecOps, risk reduction cannot continue to be abandoned by either the business operators or security staff; instead, it must be embraced and made better by everyone within the organization and supported by those with the skills to contribute security value into the system.

This culture has a positive effect on efficiency and progress of software life-cycle and software delivery. Since there has been positive feedback on this culture, the management team will most likely try to implement this method on a company-wide scale. After all, it is perceived as well-organized and profitable.

7

A lack of automated remediation capabilities

Despite following every best practice, attacks will happen and your environment will be tested. The best solution is to be ready for anything. Implement a holistic incident response model that remediates security vulnerabilities and incidents as soon as they arise.

With the dynamic nature of the cloud, it's important to continuously monitor your infrastructure to discover anomalies, validate security best practices and uncover any weaknesses. This is obviously impossible if you are considering a manual process. But with the infrastructure standardization introduced via the cloud, in conjunction with programmatic controls, automation of security best practices has now become a reality.

Knowing your cloud compliance and security posture in real-time is the best way to bulletproof your cloud infrastructure and sustain business continuity. Automation allows for you to quickly assess and mitigate vulnerabilities in real-time, while the best tools also provide remediation functions to resolve issues. Remember, incident response is about threat resolution and not simply threat awareness.

Taking a security-first approach in the cloud and achieving a state of continuous compliance is the answer. This approach can lower your costs, minimize risks, and reduce complexity in your cloud and cloud operations.

The security-first model must focus on maintaining continuous monitoring and management of cloud security risks and threats. You must leverage modern tools and automation techniques to:

- Monitor security threats through real-time discovery.
- Understand the security threats through deep insights.
- Act on threats through automated policies, processes, and controls.
- Measure security and compliance results through robust reporting capabilities.
- And now how would you ensure that your cloud is secure and compliant to these actions? The best method is to use a platform that continuously monitors and manages your cloud security against set policies and compliance processes and framework.

This model would ensure:

- Complete and unified view across all your cloud accounts
- Generation of compliance reports
- Identification, prioritization, and remediation of compliance risks
- End-to-end lifecycle compliance monitoring
- Audit reports that demonstrate round-the-clock security management and compliance

What to do now?

Optimizing your cloud adoption experience will require just as much attention to human resources as much as technical. For the human side, we have an abundance of information around cloud adoption and management strategy on our website. You can access these assets by visiting Nutanix Resources. You can also stay up to date with the latest content we have by bookmarking our Nutanix Blog site.

As for the technical side, we'd recommend you invest in a robust cloud management platform that optimizes the aforementioned vulnerabilities. And lucky for you, Nutanix has just that. It's called Nutanix Beam.

Beam is a multi-cloud governance service that provides organizations with deep visibility and rich analytics. It monitors cloud consumption patterns and proactively identifies idle and underutilized resources. The solution delivers specific recommendations to right-size infrastructure services and ensure optimal cloud consumption. Not to mention, it provides one-click fixes for cost optimization and security compliance across your cloud environments.

Beam also automates cloud security compliance using 250+ audit checks. You can identify security vulnerabilities in real-time, using policy based automation to resolve potential threats before they become concerns. Beam helps you certify and maintain compliance with regulatory policies such as HIPAA, ISO, PCI-DSS, CIS, NiST and SOC-2. With Beam you gain complete visibility, optimization and control over your cloud consumption to ensure cost governance and security compliance.

Pretty impressive right? We think se too. We'd like to give you an opportunity to experience the greatness that Beam is. If you're interested, enjoy a free 14-day trial of the platform to test it out. Protect your data, your reputation, and ultimately your business.

NUTANIX
YOUR ENTERPRISE CLOUD

T. 855.NUTANIX (855.688.2649) | F. 408.916.4039
info@nutanix.com | www.nutanix.com | @nutanix