CloudCheckr

eBook

7 Key Challenges Cloud MSPs Must Overcome

Best Practices to Scale Services and Fuel Business Growth

Intro

The landscape of the MSP industry is rapidly changing. A new breed of cloud-native MSPs is emerging and seeing rapid growth in the marketplace. At the same time, traditional MSPs are being forced to adapt to the new cloud landscape, presenting significant internal challenges as they transform the way they deliver IT services.

But what makes the front-runners in today's burgeoning cloud market stand apart from the competition?

In its recently published Magic Quadrant for Public Cloud Infrastructure Managed Services Providers, Worldwide, IT insights company Gartner highlighted some of the key qualities the modern cloud-oriented MSP needs in order to establish itself as a leader in its field.

Adoption of cloud best practices and in-depth knowledge of the three leading IaaS providers, AWS, Microsoft Azure and Google Cloud Platform distinguished the top MSPs from other companies included in the research. The report also put a strong emphasis on leveraging **cloud-native capabilities** and the implementation of DevOps tools, including **automation** and **infrastructure-as-code (IAC)**.

However, while traditional MSPs are waking up to this new reality of the cloud, as they seek to integrate a new approach to delivering IT into the services they offer, they find themselves expanding into areas outside of their comfort zone.

MSPs may be held back by their lack of knowledge, their current processes, and their organizational mindsets. The first step for the MSP to drive business and grow margins through their reseller business is to understand that it is more than just a strategic shift in business, but a growth process: one that will require time and attention. That said, knowing the most common hurdles MSPs face when becoming a more modern, cloud-native business will surely make the transition smoother.

This paper offers insight to help MSPs who are providing cloud services to customers, but are experiencing growing pains, to overcome the challenges of cloud migration and growth at scale—so they can gain a competitive edge and tap into the huge potential of the cloud MSP marketplace.

The Growth Potential of the Cloud

More and more companies are integrating the cloud into their IT services, attracted to the many cost- and efficiency-related benefits of modernizing their infrastructure. At the same time, the leading IaaS platforms are providing new services designed to help enterprises migrate large-scale legacy applications to the cloud. They're also forging partnerships with former competitors in the traditional computing arena, such as virtualization software company VMware, in a bid to help customers embrace a hybrid approach to IT.

This new era of cloud maturity and widespread enterprise adoption presents a massive opportunity for growth to MSPs that are prepared to adapt and continually evolve in a rapidly advancing industry.

However, as the number of customers signing up for for cloud services increases, so does the complexity of managing their accounts. It can become a daunting task to both address the customer's needs and oversee an internal team engaged in a shift in roles and responsibilities. The process of defining change, incident, cost, patch, knowledge, security, and access management—then implementing and perfecting those processes—is no easy feat.

Not only that, but MSPs also need to understand how to make the most efficient use of cloud resources, so they can give their customers the best possible value and increase their own profit margins at the same time.

1. Migration

Key Challenges

- ✔ Lack of onboarding
- ✔ Outdated architecture
- ✔ Legacy databases
- ✔ Lack of planning

A popular model of cloud adoption is lift and shift migration. Lift and shift means that rather than rearchitecting a whole application, an organization migrates the environment as-is, then slowly implements cloud design principles on the architecture. The assumption is that this transition will happen after a quarter, maybe two. But, in reality, once a company migrates a workload to the cloud (leveraging the services of an MSP), the organization

immediately begins using the production environment of the cloud. But, it is important to remember that while planning a time frame is all well and good in reality the process can take longer than initially was planned.

At this point, handling these projects is not so straightforward for the MSP, as the infrastructure is partially manual and partially automated, requiring specialized knowledge to manage and offer support. Additionally, there are some legacy components in the architecture that never fit with cloud design principles and will keep the environment prone to failures. Lastly, some MSP customers maintain older versions of databases and large datasets that ensure data migration remains a never-ending task. A lot of time and effort is required to identify the right migration procedure without any data loss or table drops.

A better option would be for the MSP to deal with these issues as part of the original lift and shift operation itself, rather than move their customer to the cloud only to run into problems later. By identifying potential issues, planning ahead (for example, a custom lift and shift) and documenting those in advance for the customer, the MSP is guaranteed a smoother transition and a happier customer.

A Roadmap to Success

Some of CloudCheckr's top partners include MSPs such as Rackspace, CorpInfo, Smartronix, and Relus, who have tapped into a niche in the marketplace by specializing in helping organizations migrate to the cloud. These companies believe the secret to their success lies in the way they help their customers build roadmaps right at the beginning—to ensure smooth, sustainable, and scalable deployments.

2. Inventory Management

Key Challenges

- ✔ Complexity and clear visibility
- ✔ Keeping up-to-date inventory
- ✔ Maintaining compliance

With a growing environment in which hundreds of resources are provisioned and decommissioned across an MSP's customer environment, it is necessary to have proper inventory management controls to ensure complete visibility to pinpoint any issues or gaps in the environment. Originally, to tackle this, MSPs began adopting configuration management databases (CMDBs).

However, with dozens or even hundreds of customers spinning up new resources at a rate never seen before, today's cloud MSP needs accurate, comprehensive and up-to-the-minute information on its customers' inventory. This is essential to maintaining cloud cost efficiency—because you simply can't manage what you don't know you have. But, by offering real time data and analytics, customized reporting, and actionable intelligence, MSPs can help their customers identify unused or underutilized resources and achieve their cloud optimization goals.

In addition, for customers concerned with compliance, it is better to provide automatically generated reports and documents, as manual reporting is less reliable—owing to the potential for human error.

3. Security

Key Challenges

- ✔ Managing disparate security requirements
- ✔ Maintaining control and transparency
- ✔ Identifying potential security issues

Security is very often a concern for organizations who want to move to the cloud. For the MSP, satisfying every customer's specific security needs can be challenging as compliance requirements vary from organization to organization, industry to industry. Ideally, the MSP will have their own security and compliance standards rather than attempting to craft out controls based on each customer's preferences and requests. Specifically, the MSP should provide global standards according to NIST, HIPAA, FedRamp, or other guidelines for heavily regulated industries. This eliminates a lot of discussions when submitting an RFP or at the outset of an engagement with a new customer, and can help MSPs streamline their operations.

Another security-related concern for the MSP comes into play when customers or their internal teams (development, operations, security, etc.)

make changes to their environments without informing their partners. Such a lack of transparency puts both the customer's account and the MSP's reputation at risk. In a classic case, a developer on the client's side committed his access key, as well as his secret access key on GitHub, along with the source code. The keys were picked up by an attacker who leveraged them to launch more than 100 high compute resources against a known media organization. The media organization's website was impacted; and they subsequently filed a lawsuit against its MSP. It was problematic for the MSP, even though they had no involvement in the incident; the responsibility to ensure the security of the client's account and compliance is one the MSP cannot afford to ignore.

To protect themselves from such incidents, MSPs can track resource configuration changes by leveraging AWS config services and set up alerts for security events—such as a port that's been opened up for the internet, a user disabling their MFA, a password policy modified, or the use of a root account used. In some cases, however, setting up security alerts for a violation is not sufficient; an alert needs to be programmed for successful events, too. In the GitHub use case above, high compute resources were launched without detection. It was a success event (an event where the user had the necessary permissions and was able to perform the action as intended), but an alert should be configured to notify if multiple such events occur within a short timeframe. Identifying potential security risks is a significant responsibility for the MSP, who would be wise to assign a dedicated team to deal with this task.

4. Robust Integration and Delivery

Key Challenges

- ✔ Adapting workloads to a different environment
- ✔ Rationalizing the operational lifecycle
- ✔ Maintaining consistent, robust infrastructure

One of the key challenges faced by MSPs revolves around integration between the customer's application and cloud principles. There are several issues to consider before migrating an application to the cloud. One point to consider is how it will run once it's off-premises. The majority of the workloads migrated to the cloud are still running as if they were on-premises. The tightly coupled applications, hard-coded values, as well as

lengthy and manual start-stop procedures are just some of the examples that make operations difficult to manage.

Let's review a use case of a media organization that deployed their environment on top of a public cloud IaaS provider. All three environments—dev, test and prod—were deployed in the same virtual cloud with some resources (centralized authentication, repositories, etc.) shared between all three environments. When it came time to perform patch management, it was tough to patch the EC2 instances, as the environment was not built to support bootstrapping. The patching needed to be performed on the running instances. The typical patch cycle moves from dev to test to production, but when they performed patching on their shared services, it brought the entire environment down. This made the approval process for their patch cycle very tricky and time-consuming, requiring multiple back and forth communications between teams. Also, they didn't have the capability to perform zero-day vulnerability patching and, instead, operated with blind optimism that no one would attempt to hack their environment because they could only patch after weeks or months.

For such customers, it is important to leverage DevOps and cloud design principles, taking a step-by-step approach to preparing the customer's environment so it adheres to standards. The starting point can be to leverage ISV partners or a cloud architect team to identify and eliminate the pain points in the application and architecture, and then design the environment to handle any failure. The next step would be leveraging DevOps pipelines to build and clear down environments. This was a common thread throughout the Gartner report, whereby leading MSPs help their customers achieve consistency in their architecture, boosting the confidence of the entire organization.

5. Meeting the SLA

Key Challenges

- ✔ Meeting SLA obligations
- ✔ Automating procedures
- ✔ Recovery planning

MSPs are under intense pressure to meet the Service Level Agreement (SLA) signed with each customer, as any breach leads to penalties. As each customer has its own architecture design, configuration, and pattern, it

is a herculean task to be aware of and informed about every customer's environment. The only way to achieve this is to have strong, knowledge-base management controls with runbooks created for every possible scenario and leveraging automation as much as possible. Automation brings consistency to the system and ensures there are no human errors.

While onboarding a customer to your MSP platform, it is vital to identify the recovery time objective (RTO) and recovery point objective (RPO) for the customer's environment so that necessary controls can be activated ahead of time. Multiple dry-runs can be performed to ensure the SLAs are met in the event of an outage or disaster.

6. Cost Management

Key Challenges

- ✔ Clear visibility across a multitude of customers with multiple accounts
- ✔ Dealing with changes made by the customer's team
- ✔ Difficulty in knowing whether old resources can be deleted or not
- ✔ Coordination with the customer's team on account cleanup

Cloud customers count on cost management as a key value provided by their MSP. They demand the cost of public cloud use be regularly monitored and optimizations performed. As with overseeing security in the cloud, effective cost management requires full visibility across all customer deployments, including each of their individual accounts. It's also essential to have measures in place to deal with infrastructure changes made by customers' own teams.

Cleaning up a customer's cloud also represents a significant challenge for MSPs. It can be difficult to establish whether old resources should be deleted or not, requiring careful coordination with the customer.

The best way to tackle cost management issues is to leverage automation. Automation can be categorized into two aspects: reporting-driven and action-driven. While reporting-driven automation provides information to the customer, action-driven automation can engage in the actual cleaning up of resources. When it comes to reporting-driven automation, an example includes one in which purchase recommendations for discounted

alternatives to on-demand instances are provided to the customer with a possible percentage in savings. Or it could be a report that identifies resources that are ripe for rebalancing or reallocation to make better used of discounted capacity. On the other hand, action-driven automation can include the cleanup of snapshots that are older than 90 days. Cost management plays a vital role for the customer and is a key decision point for contract renewals.

Leveraging Tagging Policies

Resource tagging is essential to successful cloud cost management practice. A clear a consistent tagging policy will help MSPs keep track of resources as well as provide the information necessary for automated cleanup of snapshots in line with customer lifecycle policies.

7. Account Management and Billing

Key Challenges

- ✔ Dealing with complexity
- ✔ Issues with consolidated bills
- ✔ Cost allocation of discounted resources

With increased adoption of a multi-cloud strategy and multiple account deployments, consolidation of accounts becomes quite a challenge for the modern MSP. Internal administrative organization is critical for public cloud providers, as they take on consolidated billing. There are times when credits applied to a master account show up in a child account (typically, customer accounts). Then, when the customer receives their invoice, they may see one figure on the billing console and a different one on the actual invoice received. This leads to chaos, confusion, and mistrust.

Let's consider an organization that has created a new customer account to deploy the customer-specific environment and invoice them based on their usage. It is feasible to do cost management for a handful of customer deployments, but becomes tricky to do so when the number of accounts runs into the double and triple digits.

For AWS service providers, management of Reserved Instances (RIs) also gets tricky as in some cases, the customer purchases RIs on his own personal account, but in other cases, the MSP purchases consolidated RIs. When MSPs purchase RIs on behalf of their customers and can efficiently

leverage consolidated billing, they recognize better margins while passing on the appropriate pricing through customer invoices.

Multiple cloud management platforms in the cloud ecosystem have emerged to solve cost management problems for MSPs, such as invoice generation, chargebacks, and billing—while offering recommendations for potential cost savings. With a comprehensive management tool, MSPs can suppress or assign credits, automate their invoicing, and receive a deeper level of insight about their margins. Also, some companies have created a dedicated position/team in their organization for cloud financial management where it is the responsibility of the individual, or the team, to research and identify the best approach to cost savings for both parties.

Summary

Of all the challenges above, the first and most basic one, is profitability: MSPs need to carefully determine the best cost model for the various environments they're managing, as some customer deployments can be time consuming, while others might be more demanding of DevOps. Success requires the right tool sets, and a confident, dedicated team. With a broad range of projects and environments, there is a significant need to recruit employees or consultants with varying skillsets. To meet industry demand, hefty salaries and perks need to be provided to such individuals, which may make it more difficult to see a profit.

With the rate of innovation in the cloud, the above challenges require more than just human efforts to solve them. MSPs need to adopt automation to ensure consistency in their offerings. This ups the level of system efficiency and allows for greater transparency between the customers and the MSP, cementing the MSP's role as trusted service provider and advisor.