The Retailer’s Guide to Multi-Cloud Adoption

Improve the speed and success of cloud application deployments
# Table of Contents

03  Executive Summary  
04  The multi-cloud imperative  
05  Cloud deployments do not always succeed  
08  Overcoming cloud adoption challenges  
09  Cloud Provisioning: Migration and cloud-native  
11  Accelerating multi-cloud adoption and success with BMC  
15  Conclusion
Executive Summary

While adoption trends show that retailers continue to move to the cloud in large numbers, many are struggling to accelerate their initiatives. Although the cloud can improve business agility, accelerate innovation, lower costs, and enhance operational efficiency, IT organizations often run into obstacles that can complicate deployment, lead to excess capacity and wasted spending, and compromise security and compliance. To accelerate and increase the success rate of multi-cloud adoption, organizations should follow a comprehensive, end-to-end adoption framework backed by machine learning, automation, and unified visibility across the environment. By taking this holistic approach, they can avoid pitfalls and maximize the results delivered by their multi-cloud strategy.
The multi-cloud imperative

Public cloud adoption is widespread and growing. According to Gartner, IaaS spending was projected to reach $38.9 billion in 2019, with PaaS expenditures reaching $19.0 billion, both increases of more than 20 percent over the previous year¹. A full 91 percent of enterprises are already using public cloud, and 84 percent have a multi-cloud strategy². Half of all enterprises now spend $1.2 million or more in the public cloud³.

Trends like these hardly come as a surprise. By leveraging cloud services, organizations can become more agile and innovative to compete in digital markets. Public cloud environments offer the flexibility and scalability needed to support agile methodologies like DevOps, bring new products to market quickly, and keep pace with rapidly shifting demand while avoiding waste. For IT, the cloud allows greater operational efficiency, better cost control, and faster adoption of new technologies and capabilities.

A multi-cloud strategy can increase these benefits further, allowing IT, application developers, and business owners to choose the right service for each app, project, or use case according to technology, cost, and other considerations.

Given both the benefits of multi-cloud adoption and its prevalence across organizations of all types, the ability to complete these initiatives quickly—and manage them effectively—is critical for the modern digital enterprise. And yet many still struggle to do so.

Cloud deployments do not always succeed

Cloud initiatives can fail for many reasons. Sometimes the organization lacks a clear business case or a well thought-out plan for their adoption. Operational challenges can come into play as well. One way or another, cloud adoption often falls short of the expected business value. In one recent study, more than one-third (37 percent) of U.S. businesses reported that they have failed to realize notable benefits from cloud computing⁴.

The cloud adoption challenges companies face—and the resulting negative consequences—can quickly turn the promise of the cloud into an ongoing nightmare for IT.

⁴ Unisys, “Cloud Success Barometer,” 2019
Poor visibility into application dependencies

Perhaps the top cloud migration challenge today is a lack of understanding of the relationships among applications, hardware, and networking devices in the environment, and the business services they support. Mapping these dependencies is notoriously difficult—both on-premises and in a rapidly evolving, constantly changing multi-cloud environment. But without this understanding, it is virtually impossible to migrate applications quickly, efficiently, and successfully.

Excess capacity creates waste

The average organization wastes 40 percent of its cloud spend on oversized, idle, or abandoned resources. Cloud consumers within the organization are typically more eager to provision the resources needed for their projects than they are to spin down capacity that’s no longer needed. In fact, 70 percent of cloud resources are used only periodically, and 15 percent aren’t used at all. This adds up quickly—and it’s especially problematic considering that cost advantages were supposed to be a key part of the cloud’s value proposition.

Ineffective cost management

The typical cloud initiative comes in 23 percent over-budget—and 30 percent of the money spent is wasted. This is all too understandable. It can be difficult to accurately predict costs and identify the most cost-efficient cloud environment prior to migration. The very flexibility and scalability offered by the cloud also means that the level of resources being purchased can fluctuate quickly. Without an effective way to track and control costs, cloud operations teams end up simply reacting to each month’s bill rather than taking proactive measures to keep costs aligned with budgets.
Misconfigurations compromise security and governance

Misconfigured cloud resources are common for many organizations, and they’re growing more prevalent. On average, 36 percent of AWS resources have Critical/High Severity misconfigurations. That’s a significant problem given that such errors are the top cause of cloud security breaches. A single misconfiguration of a cloud resource can expose critical data, including customer records, intellectual property, and more. This can leave the business vulnerable to data theft, fines for non-compliance, and financial damages due to lost revenue and future opportunities. In 2018, nearly one billion records were exposed publicly due to misconfigured cloud resources, a 20 percent increase over the prior year.

The risks posed by misconfigurations are compounded by a longstanding shortage of security professionals. Worldwide, an estimated 4.1 million existing security positions remain unfilled. Too often, the limited staff that is in place is unable to keep up, leaving the organization vulnerable to malicious or careless insiders. Meanwhile, the enterprise cloud footprint changes constantly, with 78 percent of product teams using Agile to accelerate their product development. Production updates are pushed more and more frequently, each raising the prospect of an inadvertent resource misconfiguration. In this light, it’s understandable that more than half of security professionals (51 percent) say that their organization is at moderate or extreme risk.

Inadequate tools

While cloud adoption has proceeded quickly, organizations have lagged in the tools needed to support it effectively. Only one-third of organizations are currently using the multi-cloud management tools essential to manage these resources cost-effectively and ensure strong governance and security. And as multi-cloud architectures grow more complex—as they inevitably do—they become even more challenging to manage. Among many other problems, this contributes to the lack of visibility into application dependencies discussed earlier. IT organizations are in dire need of easily deployable multi-cloud discovery solutions that can provide an end-to-end, up-to-date mapping of assets, dependencies, relationships, and business services involved without requiring coding or leaving blind spots.

IT organizations also suffer from a lack of automation, which is vitally needed to keep up with the scale and velocity of modern multi-cloud environments. Teams need automation to establish closed-loop processes, speed implementations, strengthen security, and simplify complexity. For example, teams should be able to run automated security checks that both find and fix misconfigured resources, connecting with incident and change management workflows to capture a fully documented audit trail.

⁵ SiriusDecisions Summit 2019.
Overcoming cloud adoption challenges

More effective cloud adoption begins with a more comprehensive, step-by-step framework to guide the initiative. The plan should address the following steps:

1. **Build skills and assess applications** – Do you have the skills in place to complete your initiative and manage your cloud resources effectively? If not, how will you address these requirements? It’s also critical to discover, prioritize, and plan your existing application portfolio and business services for migration to prepare for the next step. Select your cloud provider and services – Which applications and services will you want to run in the cloud, and from where will they be delivered? Cloud providers vary in their technological strengths, capabilities, and geographic coverage, so it’s important to make an informed selection.

2. **Architect services and mitigate risk** – Based on the services that will be consumed, and by whom, you should set up cloud provider accounts and privileges thoughtfully with an eye to maintaining security and control.

3. **Estimate billing and establish governance** – How will you manage the financial side of your cloud services? Will you charge costs back to business units, and if so, how? How will you build governance into cloud operations to avoid runaway costs?

4. **Provision and automate cloud services** – At this point, you’re ready to put services into your public cloud environments and perform migrations. We’ll discuss this step in more detail below.

5. **Operate cloud environments at scale** – Once your cloud resources are up and running, the focus shifts to ongoing operations, with an emphasis on improving efficiency, controlling costs, maintaining quality, ensuring security and compliance, and maximizing performance and availability.

It’s important not to skip any of these steps—especially the first few. In their eagerness to get started, companies are sometimes tempted to begin with the deployment in step 5. The chances of success with this approach are low.
Cloud Provisioning: Migration and cloud-native

There are two basic approaches to cloud provisioning, each with its own considerations, challenges, and required capabilities.

**Rehosting and refactoring, a.k.a. lift-and-shift**
While sometimes viewed as a quick and easy way to access the benefits of the cloud, moving an existing application to the cloud as-is often means missing out on most of its benefits. Still, about 45 percent of organizations take this approach. Key challenges include understanding application dependencies, optimizing capacity and cost, ensuring security, managing risk, and ensuring service availability and performance.

An understanding of application dependencies and costs are vital parts of a complete business case for the cloud. You need to know which resources you’ll need, how much capacity is required, and at what cost to budget accordingly. This makes visibility and mapping across your ecosystem essential. Once you understand your applications, their dependencies, where they’re running, and how the environment is behaving, you can more accurately assess how applications will behave in the cloud. You can also determine whether to optimize your environment before or after migration, assess project costs, and avoid surprises.

Your service model and map of your environment, including both on-premises and SaaS assets, will help ITSM teams ensure consistent governance and processes across both types of infrastructure through a holistic, end-to-end approach.

Cost minimization and optimization is an ongoing requirement. Capacity optimization, including aligning current resources and demand as well as planning accurately for future demand, will help you prevent waste while ensuring high-quality service.

Lack of visibility to deployments in the public cloud can make it difficult to maintain the performance, health, and availability of applications and services that have been migrated. Companies need a way to detect problems wherever they occur and automatically open an incident in ITSM.

Security and compliance needs in the cloud are in many ways different from what they are on-premises. As you move VMs to IaaS resources, remember that the cloud service provider is not responsible for ensuring the security of your configurations—you are. This means automated security solutions that can find and fix misconfigured cloud resources are a must.
Cloud-native application deployment (re-architecting and re-building)
In this scenario, companies typically leave on-premises applications and services where they are, and put new projects in the public cloud. As part of this strategy, on-premises resources can be refactored and rewritten to use cloud-native resources available from the cloud service provider. Challenges here include cost management and optimization, security and compliance, performance and availability, and integrating DevOps with ITSM processes.

Similar to the visibility problems that come with lift-and-shift initiatives, ensuring the performance, health, and availability of cloud-native applications and business services can be hampered by a lack of sufficient monitoring of resources in the public cloud. Here too, companies need to be able to detect problems anywhere in the cloud and automatically open an incident in ITSM for rapid resolution.

To keep multi-cloud costs in line with budget, companies need to be able to detect anomalies and predict cost over-runs before they happen while there’s still time to take corrective action. To optimize costs, they should gain insight into opportunities to lower monthly bills on an ongoing basis, and have the capability to charge back costs to the appropriate organization.

Misconfigured cloud resources put security at risk. To address security exposures, companies need an automated capability to check configurations, identify exposures, generate a prioritized list of changes needed, and take corrective action. If a change is needed, an incident should be created automatically in ITSM.

Automation is key in all of these areas. Companies deploying cloud-native applications are DevOps-driven businesses, and developers like to write code—not spend their time dealing with monitoring, security, and cost management. Automation can solve this problem and allow developers to do what they do best.
Accelerating multi-cloud adoption and success with BMC

To ensure the success of multi-cloud deployments, organizations need a solution containing products that complement each other and work together to ensure migration and cloud-native deployment success. The Accelerate Multi-Cloud Adoption solution from BMC Software includes BMC Helix Discovery, BMC Helix Capacity Optimization, BMC Helix Cloud Cost, BMC Helix Cloud Security, and BMC Helix Monitoring.
Scenario 1

Rehosting and refactoring (lift-and-shift)

**Step 1:** Start with **BMC Helix Discovery.** This will show the applications, their dependencies, and the IT assets you have deployed (both on-premises and in the cloud), how they are connected and interrelated, and which business services run on which assets. This will help you begin planning your migration and determine the right priorities, content, and sequence for moving business services to the cloud.

**Steps 2 and 3:** Here, you’ll continue planning your migration, including selecting your cloud provider and required services. **BMC Helix Capacity Optimization** will help you understand your current and forecasted capacity requirements. It can also simulate your migration to the cloud, perform right-sizing of the cloud environment, and estimate capacity savings.

**Step 4:** The next step involves **BMC Helix Cloud Cost,** which reduces cloud expenses by optimizing cloud resource costs, eliminating wasted spend and budget over-runs, and proactively alerting you about potential cost over-runs before they happen so you can take preventative action.

**Step 5:** Next, you can lower costs, improve efficiency, and strengthen security with automation. **BMC Helix Vulnerability Management** and **BMC Helix Cloud Security** can ensure that the resources in the cloud environment are efficiently managed, properly configured, compliant with policies and regulations, patched, and remain secure.

**Step 6:** Finally, **BMC Helix Monitor** will help you manage the availability and performance of business services.
Cloud-native application deployment (re-architecting and re-building)

Since you aren’t migrating existing on-premises applications in this scenario, you can start with Step 4 of the Accelerate Multi-Cloud Adoption process.

**Step 4:** The first step for the cloud native application deployment scenario involves **BMC Helix Cloud Cost**, which manages expenses and optimizes cloud resource costs and eliminates wasted spend and budget over-runs.

**Step 5:** Next, you can lower costs, improve efficiency, and strengthen security with automation. **BMC Helix RemEDIATE, with BMC Helix Cloud Security and BMC Helix Vulnerability Management**, use automation to ensure that the resources in your cloud environment are efficiently managed, properly configured, compliant with policies and regulations (Center for Internet Security, Payment Card Industry, GDPR), fully patched, and secure.

**Step 6:** Finally, **BMC Helix Monitor** will help you manage the availability and performance of business services.
Conclusion

As the scale, complexity, and speed of change of multi-cloud environments grow, simplifying provisioning and management is mission-critical. By taking a step-by-step approach to planning, backed with a complete, automated multi-cloud management solution, organizations can provide high-quality service while optimizing costs and capacity, and ensuring security and compliance. In this way, you can accelerate and increase the success of your multi-cloud strategy while maximizing its benefits, including better business agility, faster innovation, and enhanced operational efficiency.

For more information