Transforming Cloud Ops Management for Maximum Business Agility

Combatting Waste and Risk for Optimized ROI

bmc

Table of Contents

Executive Summary

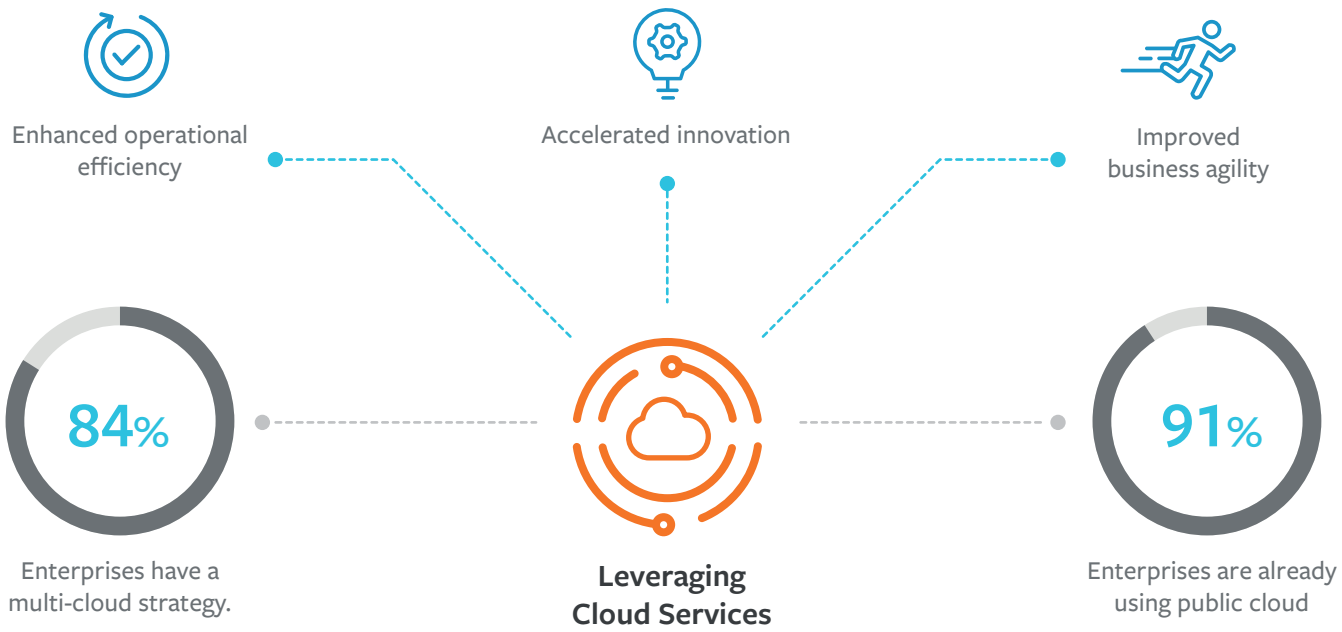
Enterprises are accelerating their move to the public cloud, and expanding their use of multiple cloud services. However, while the momentum around cloud migrations and cloud-native development continues to pick up steam, many operations teams lack the capabilities they need to efficiently and proactively manage cost and security once production services are running in the cloud. As a result, organizations are increasingly exposed to cost overruns, wasted expenditures, and security risk.

To combat these risks, IT organizations must achieve total visibility, leverage machine learning, and employ automated controls across their entire public cloud estate, so they can proactively manage costs, security, and compliance. Read this white paper and discover the cloud operations management capabilities necessary to help organizations optimize their multi-cloud security and cost efficiency, so that they might maximize their ROI on their growing cloud investments.

Rocketing Skyward

Drawn by a number of benefits, decision makers in virtually every type of organization are growing increasingly reliant upon cloud services. By leveraging cloud services, executives are looking to gain improved business agility, accelerated innovation, enhanced operational efficiency, and more.

Every day, more workloads and services are moved to or developed in the public cloud, and cloud usage continues to see explosive growth. According to Gartner, IaaS spending in 2019 is projected to reach $38.9 billion, up 27.5 percent from 2018, making it the fastest-growing segment of the public cloud services market.[1] Similarly, PaaS expenditures will grow 21.8 percent between 2018 and 2019, reaching $19.0 billion.[2] Given these statistics, it is no surprise that 91 percent of enterprises are already using public cloud, and that 84 percent have a multi-cloud strategy.[3] Plus, the size of cloud investments are significant: 50 percent of enterprises now spend $1.2 million or more in the public cloud[4] and familiar names like Apple and Lyft invest much more.



1 Gartner, "Forecast: Public Cloud Services, Worldwide, 2017-2023, 1Q19 Update," April 2019
2 Gartner, "Forecast: Public Cloud Services, Worldwide, 2017-2023, 1Q19 Update," April 2019
3 RightScale, "2019 State of the Cloud Report from Flexera," January 2019, https://info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019
4 RightScale, "2019 State of the Cloud Report from Flexera," January 2019, https://info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019

Ready. Fire! Aim.

For many cloud operations teams, the move to the cloud has happened too fast. The current tools and approaches used for managing cloud operations simply haven't kept pace with modern multi-cloud realities. Many teams have discovered that the process and technology they use for on-premises IT operations management simply do not translate well to the rapidly changing dynamic of the public cloud.

Within many organizations, cloud ops teams are relegated to using a patchwork of point solutions that are specific to a particular technology or cloud service provider. For example, a team may use one tool for managing Azure provisioning, another tool for AWS monitoring, one tool for managing container security, and so on. As a result, cloud ops teams lack unified visibility and controls that span across all their organization's cloud platforms, services, and accounts. Not only does this degrade staff efficiency, but the maintenance overhead of this collection of solutions places undue burden upon time-constrained and highly paid cloud ops staff, whose time would be better spent on the strategic efforts that boost business performance.

The Negative Repercussions of Disjointed Visibility and Control

Cloud Operations are struggling with siloed tools, limited visibility, and impaired governance. Not only does this present a number of immediate challenges, but the scope of those problems continues to expand as the number and size of cloud implementations continues to grow.

Heightened risk of security exposure

A single misconfiguration of a cloud resource can expose critical data, including customer records, intellectual property, and more. This exposure can leave the business vulnerable to data theft, fines associated with non-compliance, and financial damages due to lost revenue and future opportunities.

The cloud itself is not inherently insecure—in fact, a compelling argument can be made that AWS, Microsoft, and Google can outspend most enterprises on security. However, the reality is that teams in most enterprises struggle to use the cloud securely. There are several factors contributing to the cloud security quagmire:

- Teams in more than half of organizations mistakenly believe that their cloud provider owns all or the majority of the responsibility for their data security.[5] These teams fail to comprehend their role under the shared responsibility model of cloud security.
- The enterprise cloud footprint is under a constant barrage of change. To this point, 78 percent of product teams are using Agile to accelerate their product development.[6] As a result, armies of 2-pizza dev teams are pushing production updates more and more frequently, and each update raises the prospect of a resource inadvertently getting misconfigured.
- Cloud resources must be configured appropriately if they are to be secure, but with limited tools, it is difficult to find and fix those misconfigured resources. In fact, 73 percent of enterprises cite a lack of security visibility within their cloud infrastructure due to provider limitations.[7] Further, resource misconfigurations are the number one cause of cloud security failures. Not surprisingly, publicly disclosed exposures due to misconfigured cloud resources grew 20 percent over the prior year, with nearly 1 billion records exposed.[8]
- Too often, staff are ill-equipped to enforce role-based privileges, which opens the organization up to malicious or careless insiders.

5 Enterprise Management Associates, "Security Megatrends 2019," January 2019, https://www.enterprisemanagement.com/research/asset.php/3695/Security-Megatrends-2019

6 SiriusDecisions, SiriusDecisions Summit 2019

7 Enterprise Management Associates, "Security Megatrends 2019," January 2019, https://www.enterprisemanagement.com/research/asset.php/3695/Security-Megatrends-2019

8 IBM, "2019 IBM X-Force Threat Intelligence Index Report," https://www.ibm.com/account/reg/us-en/signup?formid=urx-36763

Limited governance

Agility is often one of the primary objectives that drive cloud adoption. However, the limited tools in place and the manual processes they impose, work directly against these objectives. For example, one of the advantages of cloud services is the ability to offer self-service consumption models to user groups. However, with limited tool sets and controls, cloud operations teams simply cannot address governance requirements while enabling users to take full advantage of this self-service access.

Misalignment and impaired agility

Often, cloud management approaches are not integrated with existing IT systems and workflows. This introduces additional overhead for cloud ops teams, who must contend with disjointed workflows, time-consuming reporting processes, and inefficient, or ineffective, collaboration. These labor-intensive efforts do not scale and they impede business agility. Further, if these inefficiencies make it difficult for teams to keep pace today, consider how things will look moving forward, particularly as the increasing reliance on continuous integration/continuous delivery (CI/CD) approaches is poised to dramatically accelerate the rate of change in cloud infrastructures.

Ineffective cost management

Within many organizations, cloud ops leaders are largely consigned to reacting to the prior month's bill, rather than proactively tracking or controlling costs. Operating this way, it is next to impossible to keep costs aligned with budgets. What's worse is that cloud ops staff cannot take any measures to ensure resources are being spent wisely. Instead, money and resources are being wasted, whether though overprovisioning or idle resources. In fact, more than one quarter of cloud expenditures, 27 percent, is self-reported as waste.[9] When one considers how much most organizations are spending, again, half of enterprises spend at least $1.2 million in the public cloud, this wasted operational expense is a stiff headwind against operating income—and the bigger the cloud expenditure, the bigger the waste.

9 RightScale, "2019 State of the Cloud Report from Flexera," January 2019, https://info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019

There Must Be a Better Way

Key Requirements

Quite simply, Operations need a cloud management solution that is aligned with the enterprise's multi-cloud footprint. To proactively and efficiently manage cloud operations, organizations need a unified platform for establishing policy-based governance of multi-cloud security, compliance, and cost. Following are some of the key requirements such a platform must address:

- **Multi-cloud support**. Cloud Operations need a central platform that offers unified support of multiple cloud providers, especially the "big three"—AWS, Azure, and Google Cloud.
- **Machine learning and advanced analytics**. To proactively manage operating costs and security in increasingly dynamic cloud environments, Operations need platforms that leverage analytics and machine learning to provide predictive insights and recommendations, so they can intervene before issues spiral out of control. These platforms need to harness advanced algorithms that enable better forecasting and budget management.
- **Governing guardrails**. To achieve the agility required, teams must have platforms that offer the intelligence and automation needed to establish so-called "guardrails." With these automated, policy-driven mechanisms in place, operations teams can provide their end users with convenient, self-service access to cloud resources, without compromising governance.
- **Service-level visibility**. While it can be easy to see how a specific cloud resource is performing with currently available tooling, it can be cumbersome to understand how top-level business services are performing. Now more than ever, Cloud Ops need service-level views that enable owners to manage security and cost within the context of their business services, which is essential for agile optimization.
- **Automation**. Given the scale and velocity of change within modern multi-cloud environments, automation is essential. Teams need automation to establish closed-loop processes, speed implementations and changes, and simplify complexity. For example, teams should be able to run automated security checks that not only find misconfigured resources, but fix them. This should also include an ability to connect with enterprise incident and change management workflows, so service delivery teams can not only resolve issues quickly, but do so with a fully documented audit trail.
- **Easy deployment and use**. To effectively manage their cloud footprint, teams need a cloud management solution that exhibits all the attributes that made the cloud so appealing in the first place. These teams need platforms that offer the ease of SaaS delivery as well as pre-packaged content and integrations that ensure fast time to value.

Positive Business Impact

By leveraging an advanced cloud management solution, organizations embracing the public cloud can achieve these objectives:

- **Cloud cost savings**. Analytics and machine learning can help teams root out idle or overprovisioned resources draining their budgets, and automation makes slashing waste straightforward.

- **Strengthened cloud security posture management**. With advanced cloud management solutions, teams can gain the capabilities needed to optimize policy-driven governance. These teams can leverage closed-loop security that automates the process of finding and fixing resource misconfigurations, significantly enhancing security and compliance by dramatically diminishing windows of exposure.
- **Better governance**. When users have self-service access to resources, the need for shadow IT is marginalized. The result? Improved governance of cloud usage across the entire cloud estate.
- **Greater staff productivity**. With machine learning and selective automation, cloud ops personnel have more cycles to rise above the noise and maximize the quality of the service they provide.

Cloud Operations Management from BMC Software

Within enterprises embracing the public cloud, operations teams need an advanced platform that enables proactive cloud operations management. These capabilities are vital to ensuring cloud ops are secure, efficient, and cost effective. The Cloud Operations Management solution from BMC Software uses machine learning, analytics, and automation to translate insights into action. With this solution, teams can optimize governance of cost and security across AWS, Azure, and Google Cloud.

Key Features

The Cloud Operations Management solution from BMC Software simplifies and optimizes cloud operations management with these capabilities:

Superior machine learning

With this solution, customers can leverage machine learning and predictive analytics to proactively manage operating expenses and security policies. The solution offers predictive insights into exposed assets, accounts, and resources, and it provides capabilities for tracking spending and predicting cost overruns.

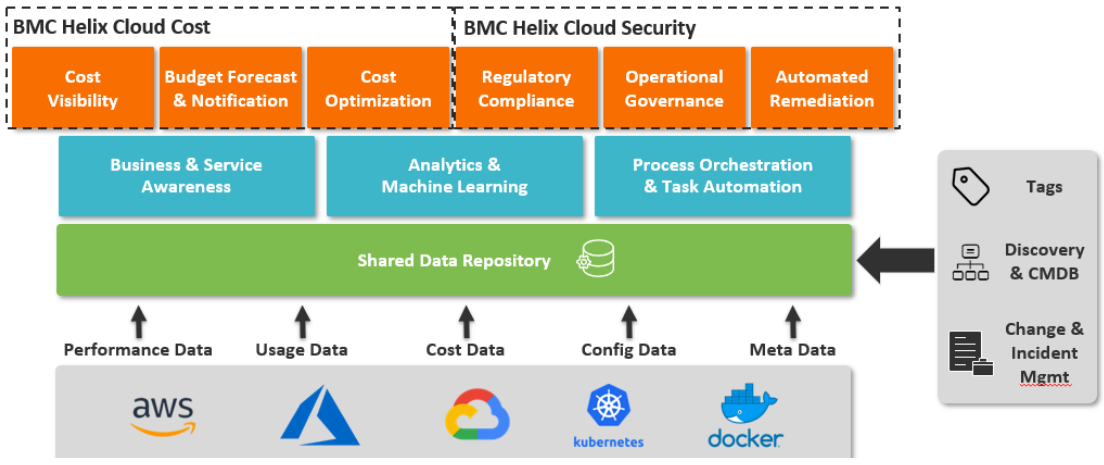
Targeted automation and guardrails

With our solution, teams can establish unified orchestration across multiple cloud platforms, services, and accounts. The solution helps customers maximize automation and eliminate the bottlenecks associated with tedious, manual tasks. The solution delivers the following capabilities:

- Automate cost optimization actions, including retiring idle assets and right-sizing overprovisioned resources.
- Automate the detection and resolution of cloud resource misconfigurations, significantly reducing windows of vulnerability.
- Run automated scans every time a new resource is deployed or an existing resource is modified.
- Use policy-driven automation to establish guardrails that optimize the performance, cost, security, and compliance of cloud environments.

Fast, efficient deployment, operation

With the Cloud Operations Management solution from BMC Software, enterprises can establish unified control across their multi-cloud



implementations, including AWS, Azure, and Google Cloud. Featuring support for Kubernetes and Docker, the solution offers comprehensive capabilities for securing containers, including hardening host OSs. This SaaS solution comes pre-packaged with extensive content, which means teams can start managing cost and security in their public cloud in five minutes.

Service-level views of security and cost

Our solution helps organizations manage technology within the context of running the business. The solution enables digital service developers and line-of-business stakeholders to manage the costs and security posture of their service.

The solution's real-time, service-level views can help executives boost business performance by comparing the cost and security of a number of applications. Based upon these comparisons, managers can acknowledge teams that are performing well, and uncover best practices and recommendations that can be shared across the organization.

Benefits

By leveraging the Cloud Operations Management solution from BMC Software, organizations can realize a range of compelling benefits:

- **Optimized cost management**. This solution helps teams establish more accurate forecasting and improve alignment with budgets and plans. The solution delivers predictive alerts on potential outages or budget overruns, enabling staff to take corrective action before issues arise.
- **Enhanced operational efficiency**. With our solution, teams can establish the broad-based automation that offloads manual efforts from staff and reduces errors and delays. The solution provides the unified visibility and controls that help improve staff collaboration and productivity.
- **Strengthened security**. With the solution, operations teams can reduce the incidence and duration of misconfigurations that can expose the business to data theft and penalties for non-compliance.
- **Improved business performance**. The solution enables teams to eliminate the significant waste associated with overprovisioning in cloud deployments, helping ensure maximum business utility from every dollar invested in the cloud. With the solution, teams can ensure consistent adherence with security policies and compliance mandates, while enabling user groups to fully leverage the agility and scalability of the public cloud.

Solution Components

- **BMC Helix Cloud Security**. This solution automates security testing and remediation of IaaS and PaaS resources across AWS, Azure, and Google Cloud. The solution facilitates consistent, auditable compliance with security policies and mandates, and equips teams with an extensive array of pre-packaged policies based on best practices. The solution implements the CIS framework for Docker and Kubernetes to drive container configuration security.
- **BMC Helix Cloud Cost**. This solution enables cloud buyers and budget owners to centrally track cloud usage, costs, and budgets. BMC Helix Cloud Cost provides the insights and automation needed to optimize management of budgets and resources, including right-sizing over-provisioned assets and releasing idle VMs. This offering delivers automated recommendations and actions on resource usage, providing support for cost reduction efforts. With the solution, teams can establish controls that ensure user groups adhere to business guidelines for using and purchasing cloud resources.

Conclusion

Both the scale of cloud usage and the rate of change within the enterprise's public cloud footprint are accelerating. Fumbling with a legion of limited, point-specific tools, Cloud Ops departments are ill-equipped to keep pace with this change. These factors expose the business to cost overruns and security risks, while crippling the organization's ability to fully achieve its cloud objectives. With BMC Helix Cloud Security and BMC Helix Cloud Cost working together, organizations can gain centralized, efficient control over their multi-cloud deployments, enabling optimized governance of cloud cost and security without hamstringing business agility.

For more information

To learn more, book a demo, or take a free trial, be sure to visit:
bmc.com/cloudops

You can learn more about specific components of our cloud management solution at:
BMC Helix Cloud Security
BMC Helix Cloud Cost

About BMC

BMC delivers software, services, and expertise to help more than 10,000 customers, including 92% of the Forbes Global 100, meet escalating digital demands and maximize IT innovation. From mainframe to mobile to multi-cloud and beyond, our solutions empower enterprises of every size and industry to run and reinvent their businesses with efficiency, security, and momentum for the future.

BMC – Run and Reinvent **www.bmc.com**

514866