Using AI to Transform CloudOps and Accelerate Innovation

AI, automation, and policy-based governance enable Cloud Operations teams to predictively optimize cloud cost and enhance security

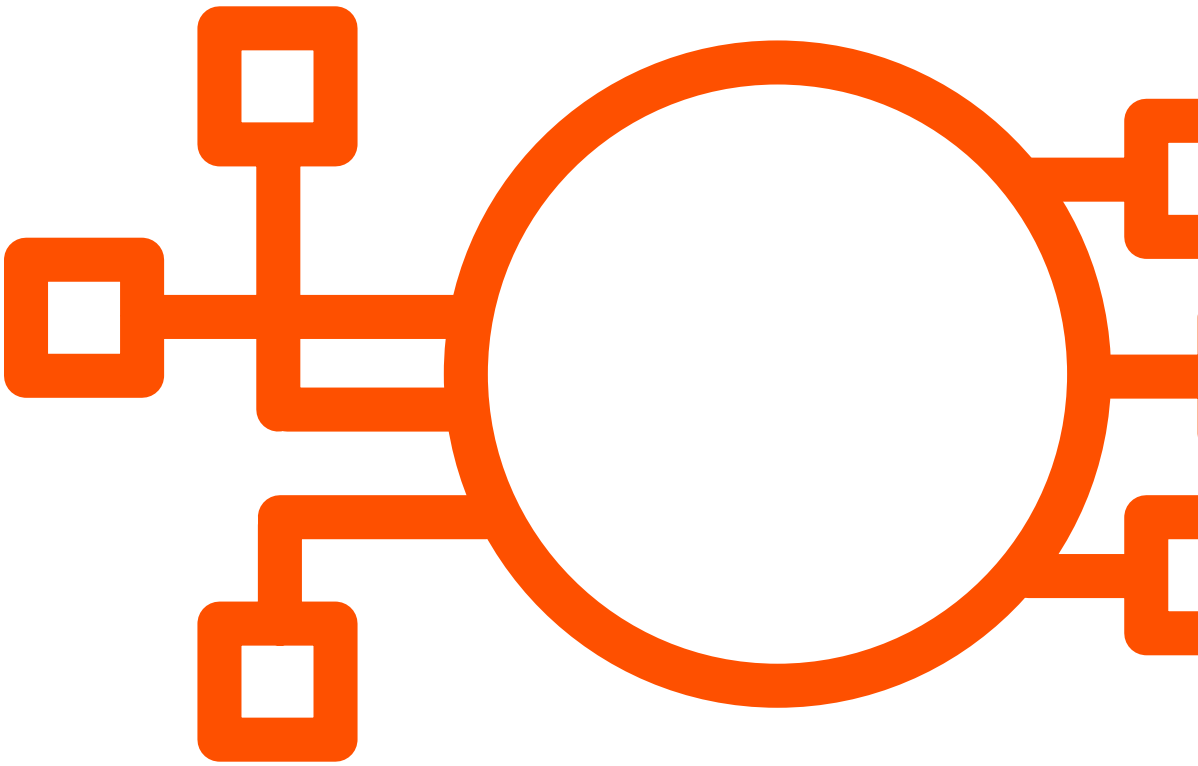
bmc

Table of Contents

Introduction

Cloud swooped in to solve the compute problems companies faced in an era of rapid digital transformation, when requests for resources started to outpace the speed at which IT operations could deploy infrastructure and applications to fulfill business demand. Add to that the resources developers need to enable rapid innovation and deliver new products and services to customers and public cloud usage became the wild, wild west of computing.

Despite its widespread adoption, cloud computing continues to represent concerns for adopters—even while they continue to invest in the cloud. Research from CollabNet VersionOne shows that 97 percent of organizations are using agile development methodologies in some form, which strengthens the need to adopt cloud. According to Vanson Bourne research, 57 percent of organizations that used public cloud services reported one or more incidents of shadow IT, which in many cases circumventing IT can risk forecasting accuracy and hamper controlling spend. That figure relates directly to 2019 data from 451 Research showing that 57 percent of some 300 respondents worry daily about cloud cost. Literally billions of records were exposed in 2018, which explains why some 93 percent of enterprise reported being very worried about cloud security, according to the 2019 Cloud Security Report by Cybersecurity Insiders.



The Benefits of Cloud Continue to Attract Enterprise Companies

Now that cloud adoption is mainstream, it is time for Cloud Ops to mature their approach to cloud governance, so that their internal customers are equipped to effectively manage budget, optimize cost, and securely configure public cloud resources across the cloud footprint. Cloud Ops teams recognize they must evolve how they manage distributed cloud instances to control costs, ensure security, and optimize resources.

Let's be clear: the benefits of cloud continue to attract enterprise companies looking to increase business agility, accelerate innovation, and improve operational efficiencies. According to 451 Research, cloud is now mainstream with 90 percent of organizations surveyed using some type of cloud service, and 69 percent of enterprises will have multi-cloud/hybrid IT environments in 2019.

According to Gartner, "the fastest-growing segment of the market is cloud system infrastructure services (infrastructure as a service or IaaS), which is forecast to grow 27.6 percent in 2019 to reach $39.5 billion, up from $31 billion in 2018. By 2022, Gartner expects that 90 percent of organizations purchasing public cloud IaaS will do so from an integrated IaaS and platform as a service (PaaS) provider, and will use both the IaaS and PaaS capabilities from that provider."[1]

At the same time, Vanson Bourne research reveals that just 6 percent of organizations that used public cloud services reported staying under or within budget, yet another 35 percent said they overspent, exceeding planned budgets. Not being able to predict the potential cost of a cloud deployment is driving the need to better manage cloud deployments on-premises and off.

> Between idle resources and overprovisioning, wasted cloud spend will exceed $14.1 billion in 2019.
>
> Source: ParkMyCloud

Fortunately today's enterprise companies can now turn to technologies such as machine learning and artificial intelligence to gain visibility into cloud costs, security, and usage. Advanced cloud operations management technologies will equip Cloud Ops teams with the right tools to realize the benefits of multiple cloud deployments while also avoiding unexpected charges and hidden security risks.

1. Gartner Press Release, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019, September 12, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019.

Balance Governance and Agility

Cloud computing contributed to a significant shift in purchasing power across IT organizations. Readily available cloud services enabled business owners, developers, and really anyone with a credit card to roll out new instances as needed, rapidly accelerating agile innovation.

The problem lay when such cloud usage is outside of centralized governance. Considering the scale and rate of change in the public cloud, it is not humanly possible to manually track the resources used when and for what business purpose.

> Monitoring cloud services for new vulnerabilities worried 43 percent. Going through audits and risk assessments concerned 40 percent and monitoring for compliance stood out to 39 percent of respondents.
>
> Source: 2019 Cloud Security Report by Cybersecurity Insiders

Cloud Ops teams realize their developers must access cloud resources as they need them throughout the development lifecycle. That means Cloud Ops must strike a balance between ease of use to appeal to their developer community and governance to maintain compliance and security.

Businesses want to embrace the rapid pace of innovation within their development teams making it imperative that Cloud Ops embrace tools that streamline innovation and empowers their internal customers to innovate rapidly within sensible governance guardrails.

For Cloud Ops teams, that means trying to manage cloud resources across multiple environments, on-premises and with public providers, and understanding the costs associated with usage. It also means trying to get a holistic view across environments with disjointed point products, which adds to the lack of total visibility and limit proactive responses due to lack of integration.

That's why organizations must adopt a unified platform that can establish and enforce policy-based governance across all cloud instances.

Sophisticated cloud management platforms should:

- Manage both security and cost across multiple public cloud platforms and accounts;
- Use machine learning and predictive analytics to proactively manage expenses; and
- Engage automation with policy-based governance to optimize cost and enhance cloud security.

Predictive Cloud Cost Management

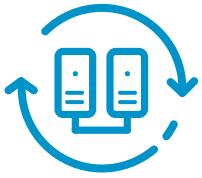
With visibility into cloud usage for cost purposes, Cloud Ops teams can also get a better idea of upcoming resource needs so they can plan for budget. Using machine learning, advanced analytics and automation, Cloud Ops teams can get a picture of what normal cloud usage—and spend—looks like and be proactively alerted when there is a spike in demand for resources.

The technology can also take action based on established processes. For instance, cloud management tools can automatically move on-premises workloads to the cloud if there are cost-effective resources available that can help the company avoid missing service-level agreements. With intelligent multi-cloud management, enterprise companies can monitor daily compute usage and costs. The technology should provide summaries by application, service type, provider and other factors.

Advanced tools can also rank cloud instances from most to least expensive and identify resources that could be consolidated or eliminated. And a centralized dashboard gives a unified view of on-premises and public cloud infrastructure expenditures, with data relevant to IT and business users alike.

Other facets of a sophisticated cloud management platform should include:

Automated cost optimization actions, including retiring idle assets and right-sizing overprovisioned resources.



Automated detection and resolution of cloud resource misconfigurations, significantly reducing windows of vulnerability.

Automated security checks run every time a new resource is deployed or an existing resource is modified.

Policy-driven automation to establish guardrails that optimize the performance, cost, security, and compliance of cloud environments.

Cloud Security is a Different Beast

With the advent of cloud, one of the biggest concerns was security: companies worried about putting their own and their customers' data in a shared public computing space.

While that concern obviously hasn't slowed the adoption of cloud, the risk associated with using cloud platforms hasn't been entirely mitigated either. In fact, 93 percent of enterprises are worried about their public cloud security, so much so that 55 percent expect to deploy a new solution within the next 12 months, according to the 2019 Cloud Security Report by Cybersecurity Insiders.

According to Enterprise Management Associates, more than 50 percent of cloud users mistakenly believe that their cloud service provider is responsible wholly and partially for security, proving that cloud users don't completely understand the responsibility they have to secure their cloud environments.

For instance, If the cloud resource being used has a configuration setting, then the cloud user is responsible for the security of it. That means every time developers are pushing changes to production, the configuration settings must also be checked that they are securely configured.

> The top two operational security headaches SOC teams are struggling with are compliance (34 percent) and lack of visibility into cloud security (33 percent).
>
> Source: 2019 Cloud Security Report by Cybersecurity Insiders

The visibility and insights gained from an intelligent cloud management platform will directly benefit an organization's security profile as well. While the service and application owners are ultimately accountable for securing their public cloud footprint, the Cloud Ops teams is responsible for governance oversight. That means they create and distribute the security and compliance policies and remediations, equipping the service and app owners with the tools and knowledge they need to manage their security posture.

> 73 percent of enterprises cite a lack of security visibility within their cloud infrastructure due to provider limitations.
>
> Source: Enterprise Management Associates, Security Megatrends

Cloud Ops also must understand what the service and apps owners are using to create adequate and accurate governance policies to meet compliance requirements and protect the company's assets in the public cloud. Because Cloud Ops want to enable business agility, not hinder it, they must adopt governance policies and tools the apps owners can easily embrace.

To transform and strengthen cloud security posture management, an intelligent cloud management platform should provide comprehensive and sophisticated security capabilities that include:

- Automated "find and fix" capabilities for resource misconfigurations;
- Closed-loop security management, which ties into incident and change management workflows;
- Automatic self-driving security, which radically minimizes the window of vulnerability;
- Prioritization and exception handling to triage the security backlog;
- Role-based access control and multi-tenancy; and
- Policy-driven cloud governance.

Cloud Ops teams should be able to run automated security checks—whether on-demand, regularly scheduled, and/or in the moment of change—that not only find misconfigured resources, but also fix them. This should also include an ability to connect with enterprise incident and change management workflows, so application teams can not only resolve security and compliance issues quickly, but also do so with a fully documented audit trail.

Cloud Smart Strategy

Cloud is a viable, practical option for many companies. The current reality simply requires a new level of maturity and predictive intelligence with enterprise cloud strategies.

Companies realize now that cloud is not a set-it-and-forget-it undertaking, but requires consistent, proactive monitoring across complex environments. With the right technology in place, enterprise Cloud Ops teams can depend upon cloud resources to meet business and customer demand without worrying about incurring unknown costs or leaving vulnerabilities exposed to malicious attackers.

Cloud Ops teams today can control their sophisticated environments with the right tools that use machine learning and AI to help optimize their multi-cloud deployments. They can also now be sure to keep costs under control and prevent misconfigurations from leading to breaches with the help of intelligent automation. The power of cloud can only grow for enterprises embracing the right intelligent management platform.

For more information

Learn how BMC transforms cloud operations management at www.bmc.com/cloudops.

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**