The Enterprise Cloud Management Landscape Report 2018

RESEARCH CONDUCTED BY VIB

Sponsored by  SCALR

Table of Contents

Executive Summary

IT organizations in large enterprises are facing increasing pressure to deliver solutions faster while still maintaining cost and security standards. While the cloud enables companies to innovate faster, enterprises face significant challenges around meeting corporate requirements.

IT leaders struggle to balance the needs of multiple enterprise constituencies: End-users who require a fast provisioning experience that fits their work, whether they are basic or power users; and corporate IT, which must make sure the platform is secure, cost-effective and follow compliance standards, especially in heavily regulated spaces.

These considerations and more make it difficult for an enterprise to dive "head first" into a public cloud environment, and lead most companies to a carefully constructed Hybrid Cloud strategy, which leverages both existing infrastructure and new public cloud investments.

Scalr recently sponsored an independent, third-party survey conducted with **IT leaders in enterprises with over $500M in annual revenue**. The purpose of the survey was not only to **identify the leading platforms and tools used in the enterprise cloud landscape, but also what are the top concerns and challenges** IT organizations are facing.

The survey revealed new data about the main drivers for cloud adoption at large enterprises, and the primary careabouts when designing cloud strategy. In addition to ranking the mix of vendor platforms in their cloud environments, respondents prioritized concerns around security, cost, automation and self-service.

Key Findings

- **Cloud Platform Usage:** AWS still dominates as the most popular public cloud, but Microsoft Azure is more likely to be used for both development and production.
- **Top Concerns:** The concerns are broken down into the below categories and subcategories, and ranked by relative importance.

COST	SECURITY	AUTOMATION	SELF-SERVICE
Cost Visibility and Accountability	Workload Security	Ecosystem Automation	Guardrails & Governance
Budgeting & Financial Policies	User Security	Application Lifecycle	Differentiated Self-Service
	Compliance		

In the Security category, for example, **User Security was ranked higher than Workload Security and Compliance**. User Security refers to role-based access control (RBAC), permissions, compartmentalization and the general system of "who can do what, where and how much."

Security was also ranked as the **top concern** in cloud operations **by 59% of respondents**, with **Cost** coming in at a close **second**.

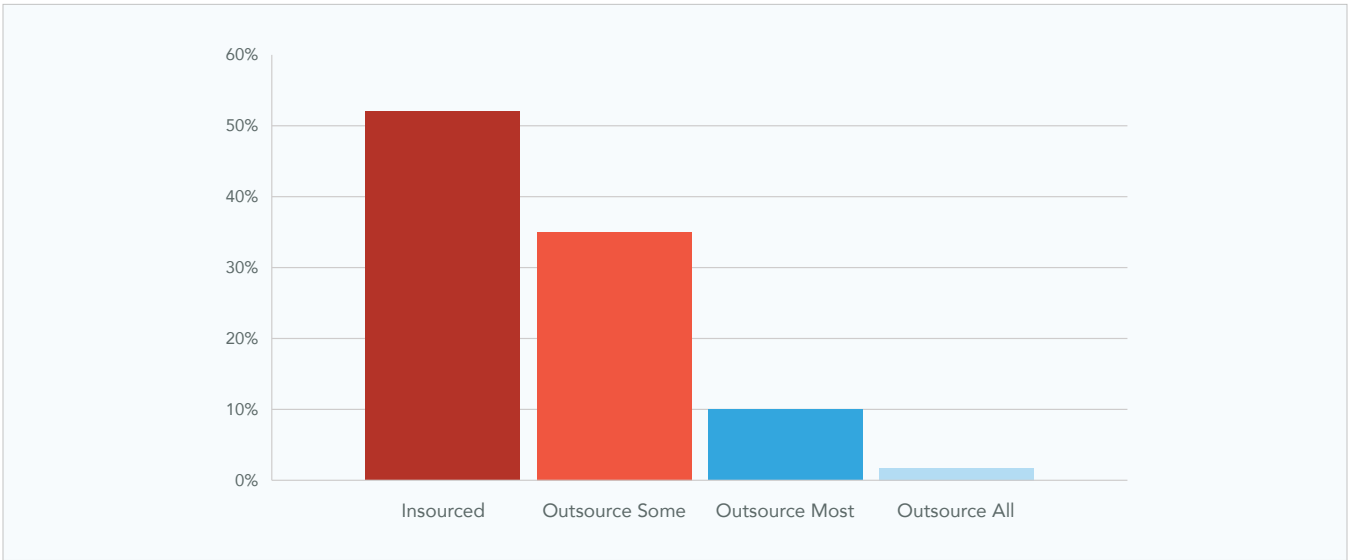
- **Cloud Management Platform:** An overwhelming majority, 81% of respondents, indicated they either have a Cloud Management Platform in place or are currently evaluating one.

1. The Management & Distribution of IT

While in smaller companies IT may be composed of a few employees who handle infrastructure, identity and tooling, enterprise IT is typically a massive organization that spans multiple functionalities. Some enterprises choose to manage all IT operations in house, while others find a benefit in outsourcing some or all IT efforts.

The first step to better understanding how enterprises use cloud is to understand the structure and distribution of IT. According to the survey, **52.6%** of respondents indicated their companies **are fully insourced**, meaning that everything from architectural decisions to implementation and operations is done in-house.

35.6% of respondents indicated that **technology and architectural decisions are done in-house, while operations are outsourced**. Only **11% outsource most or all** of their IT efforts.



Most companies choose to handle IT efforts in-house due to several factors. First, no two enterprises are the same. While companies in similar verticals experience common challenges, the customizations required to create the most efficient and agile business are unique. Secondly, with the advent of cloud technologies and the cloud management ecosystem, much of the work can be done in-house with significantly less overhead than was previously possible. The third factor has to do with the geographic footprint of large enterprises.

Next, we examined the geographical distribution of IT operations and users. **74%** of respondents indicated their IT operations and users **span two or more geographical regions**, while the remaining **26%** said their IT teams are primarily focused on one region.

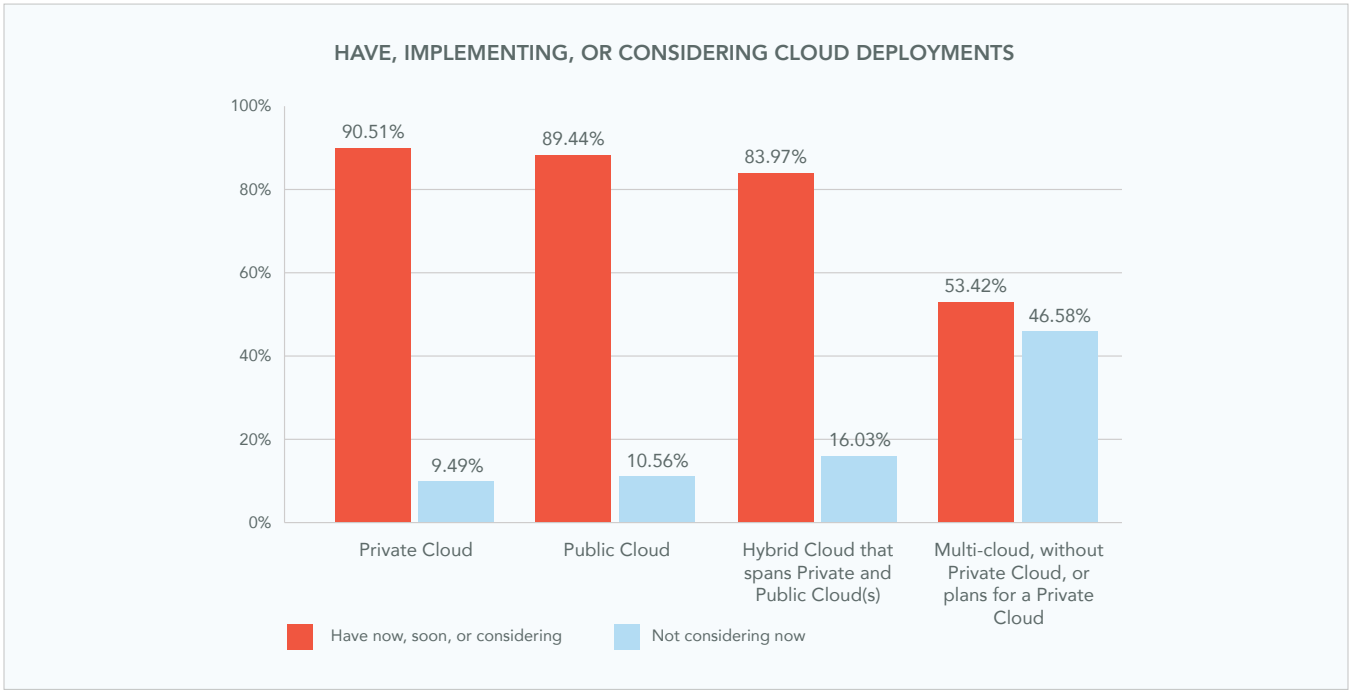
> ***"We have 33 locations in the US", "We have global operations across North America, Latin America, Europe and Asia", "We're active in Canada & US, France & Germany, China & Taiwan", "We support thousands of remote workers".***

The typical enterprise IT tackles most challenges and initiatives in-house, and supports an organization that spans multiple geographical regions in a variety of use-cases.

2. Cloud Deployment Models

The terms "Hybrid Cloud" and "Multi-Cloud" often have different meanings for different companies. Regardless of the specific mix of platforms that make up each of these cloud strategies, the survey confirmed the primary approaches that are being used. Private Clouds, which are mainly VMware-based, still dominate enterprise cloud strategy with approximately **75%** of respondents indicating their company either **has a private cloud in production today or expects to soon. 66% said the same about Public Clouds**.

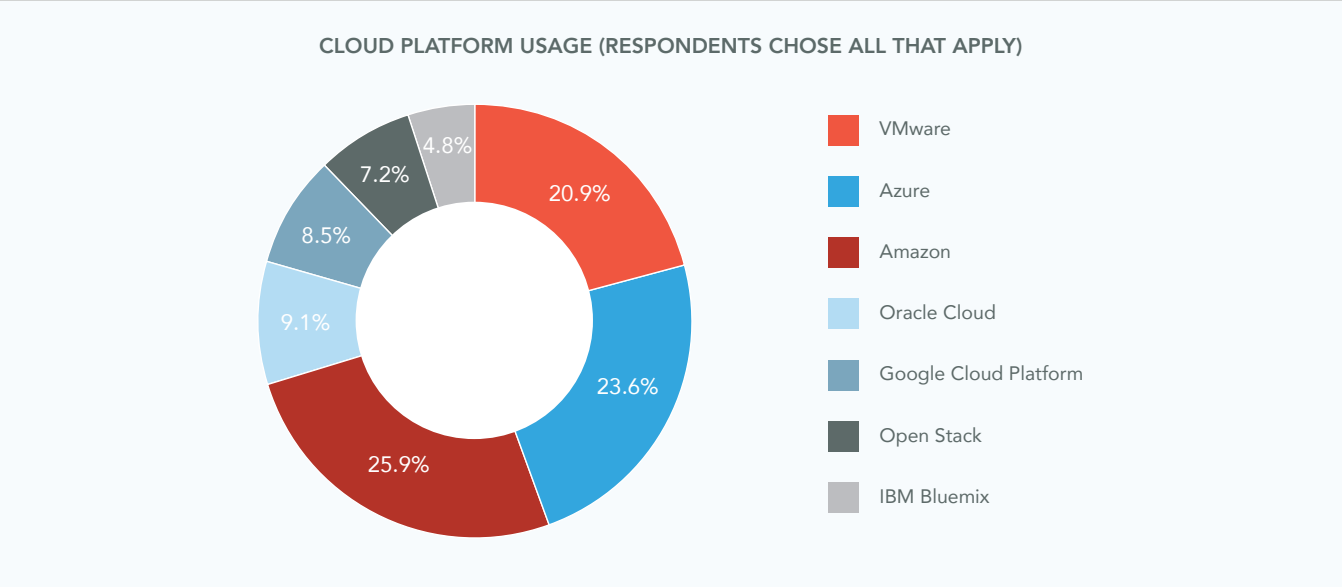
The rise of the Public Cloud's strategic importance in large enterprises is undeniable, as the majority of enterprises seem to be settling on a strategy that spans Private and Public Clouds. **32% have Hybrid Cloud in production** today, **17% expect to have Hybrid Cloud in production** soon, and **27% are currently considering** a Hybrid Cloud strategy.



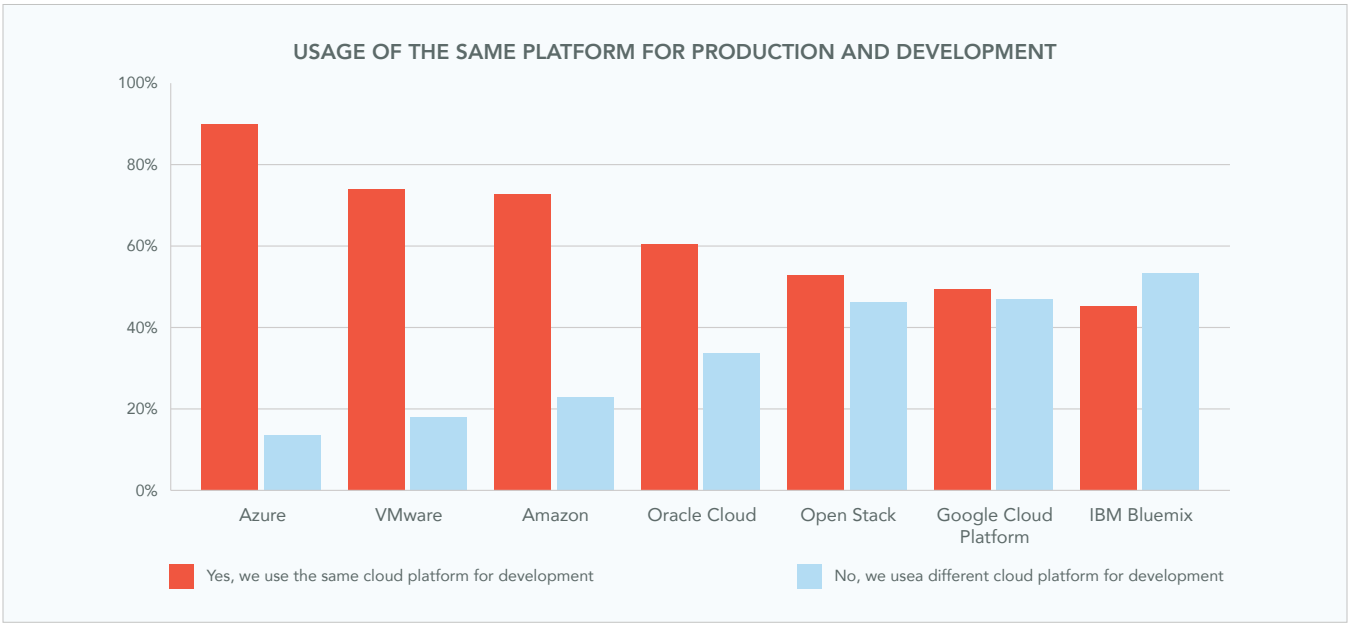
> ***"My organization runs a workload that requires large pools of storage and networking resources on a private cloud, such as OpenStack. At the same time, we have a workload that needs to scale up or down quickly on a public cloud, such as Microsoft Azure or AWS. Each workload is running on the ideal cloud, but now we have multiple clouds to manage."*** - Anonymous Survey Respondent

3. Cloud Platform Usage

As expected, we confirmed that AWS, Microsoft Azure, and VMware continue to lead the pack as the most widely platforms. However, we dug deeper to understand how these platforms are used.



While AWS remains the most popular cloud platform, it is not the most likely to be used for both Development and Production. That honor falls to Azure, with 88% of users giving the affirmative. **72% of respondents who use AWS indicated they use it in production**, while **83% said the same for VMware**, and **81% for Azure**.



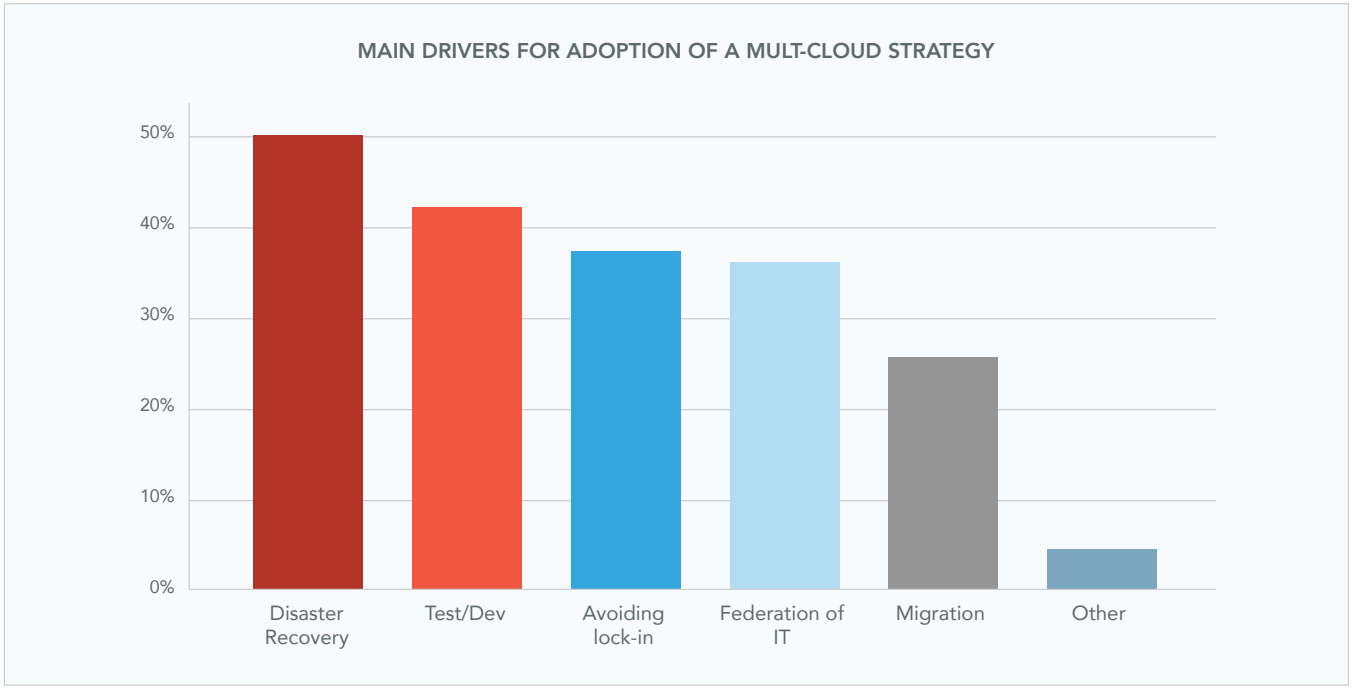
4. Key Drivers for Cloud Adoption

Enterprises turn to cloud for a variety of reasons. Some want to capitalize on existing investments in datacenter infrastructure, some are looking for more cost-effective ways to spin up resources, and some want to achieve a higher level of fault tolerance and disaster recovery for their applications.

We asked survey respondents to rank the key use-cases that drove them to adopt, or plan to adopt, a multi-cloud strategy. **50% indicated that Disaster Recovery was the top driver**. A lot of the tools required for a successful Disaster Recovery, High Availability, and Fault Tolerance strategy are built-into the public cloud platforms. Enterprises often need to find the right way to automate application provisioning and lifecycle in a way that best leverages these tools, across different platforms.

Respondents ranked the ability to use **a secondary platforms for Dev/Test environments as the second most important driver**, and avoiding lock-in and Federation of IT as third and fourth, respectively.

The Federation of IT refers to extending self-service to teams without sacrificing policy-based controls. Essentially, giving teams the flexibility they need while ensuring best practices and compliance. **36% of respondents ranked Federation of IT as a key driver**.



> *"We deploy to other clouds only if differentiation of services warrants deviation from primary cloud provider"*
> - Anonymous Survey Respondent

5. Top Enterprise Concerns When Adopting a Hybrid/ Multi Cloud Strategy

Cloud adoption typically happens in cycles. Enterprises often find that they are already in the cloud, without any strategy in place, due to application teams going directly to AWS in order to be more productive. This results in a spike in cost, which can be difficult to account for since no tagging or policies were in place. Once the company chooses to adopt cloud and start deploying massive workloads in development and production environments, security concerns soon arise.

These challenges and many others have varying level of importance and impact for different companies, depending on vertical, company culture, types of applications under development and more.

Based on conversations with IT leaders, IT operation teams and CIOs, we placed the main multi-cloud concerns in four categories:

Cost - The ability to track spend, assign it appropriately, and enforce policies and quotas that prevent overspend.

Security - Reducing the attack surface of workloads, ensuring user security through RBAC (role-based access control), and enforcing compliance policies.

Automation and Orchestration - Application Lifecycle automation and the automation of the cloud platform's interaction with other tools in the IT ecosystem.

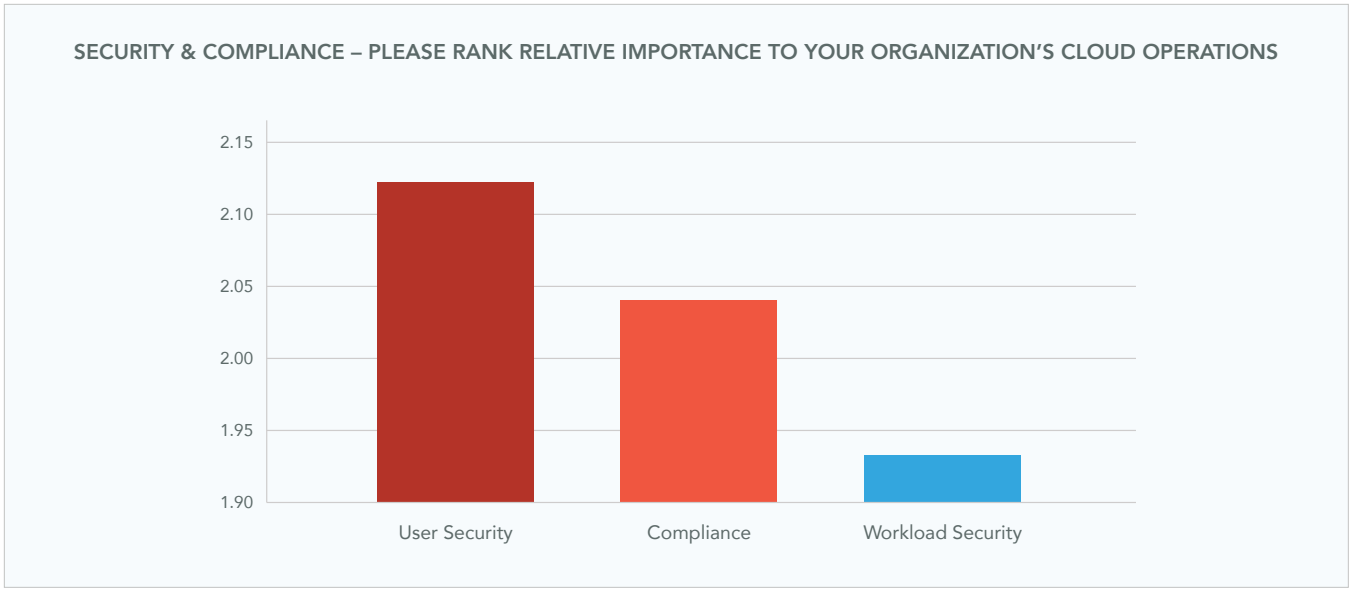
Self-Service - The user experience of provisioning cloud resources, productivity, and the ability to enforce governance policies that ensure responsible cloud usage.

For each of these concern areas, respondents ranked the relative importance of components within each area.

5.1 Platform Security

The results revealed administrators generally rate **User Security as a bigger concern than workload security and compliance**. The takeaway here is **not** that User Security (RBAC, permissions, etc.) is more important than other aspects of secure resource usage, but that **User Security is more likely to be the root cause that affects the other aspects**.

A multi-cloud platform with automated and standardized User Security in place will have an easier time ensuring both compliance and workload security.

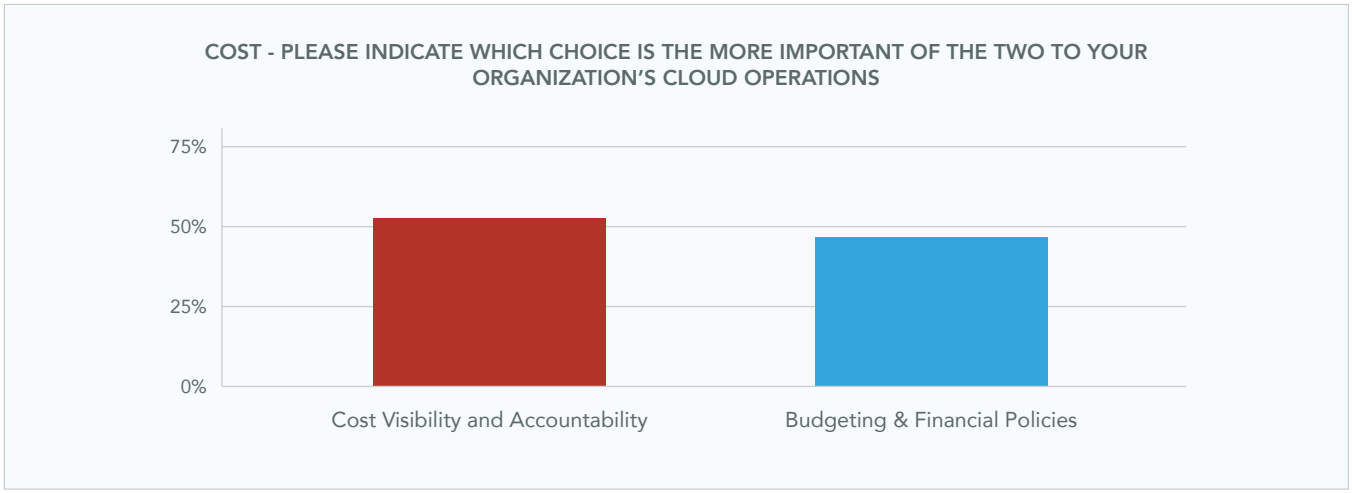


5.2 Cost Control

When it comes to cost, respondents were asked to select which concern was more relevant to their cloud operations:

- **Cost Visibility & Accountability** - Tracking spend and assigning it appropriately
- **Budgeting & Financial Policies** - Enforcing budgets, cost reduction policies, quotas, preventing overspend by assigning lifetimes to applications and making sure users provision the right sizes of machines, etc.

As expected, both concerns were almost equally important to enterprises, with **52%** of respondents **indicating that Cost Visibility and Accountability was more important**.



These results reaffirm that while cost reporting is essential, cost control requires more than visibility. It's also the ability to create solutions out of cost insights. Enterprises are adopting an active approach to cost management, and implementing financial policies directly into the provisioning workflow in the form of quotas, which ensure compliance with reserved instance profiles, accountability and more.

> ***"TCO is key to our budgeting", "I Have Cheap Bosses"*** - Anonymous Survey Respondents

5.3 Automation & Orchestration

Orchestrating complex ecosystems is quite challenging for many enterprise IT organizations. Different sets of tools and solutions tend to evolve within the company, and it is often IT's job to make sure these tools work together as a dependable platform.

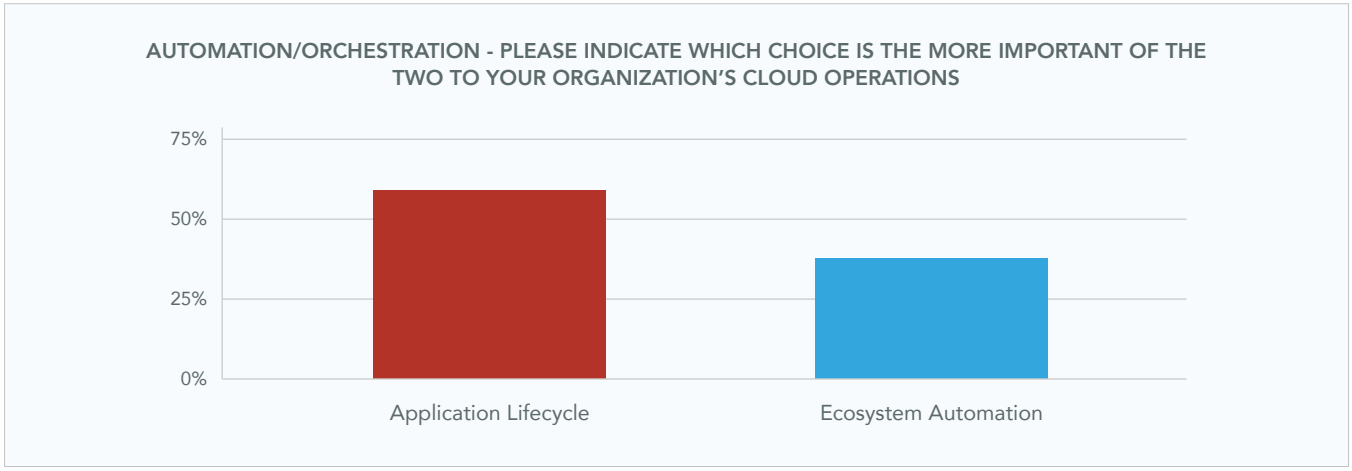
In addition, IT monitors and supports application teams as code moves from development to staging and production. In order to ensure these processes are safe and scalable, application lifecycle automation ensures that the relevant events occur on every deployment.

Survey respondents were asked to choose which aspect of Automation and Orchestration is the larger concern for their organization:

- **Application Lifecycle** - Automate events in the application lifecycle from provisioning, to maintenance, autoscaling and reclamation
- **Ecosystem Automation** - Automatically trigger interactions between tools based on events on your cloud infrastructure, (i.e., every time a resource is provisioned, update the CMDB, have the IPAM system register the addresses, etc.).

63% of respondents said application lifecycle automation was more important. Application Lifecycle automation governs the Order Of Operations for provisioned workloads and ensures the seamless transition between different stages of application development.

> ***"Documentation is only slightly more important than reclamation of resources"*** - Anonymous Survey Respondent



5.4 Self-Service

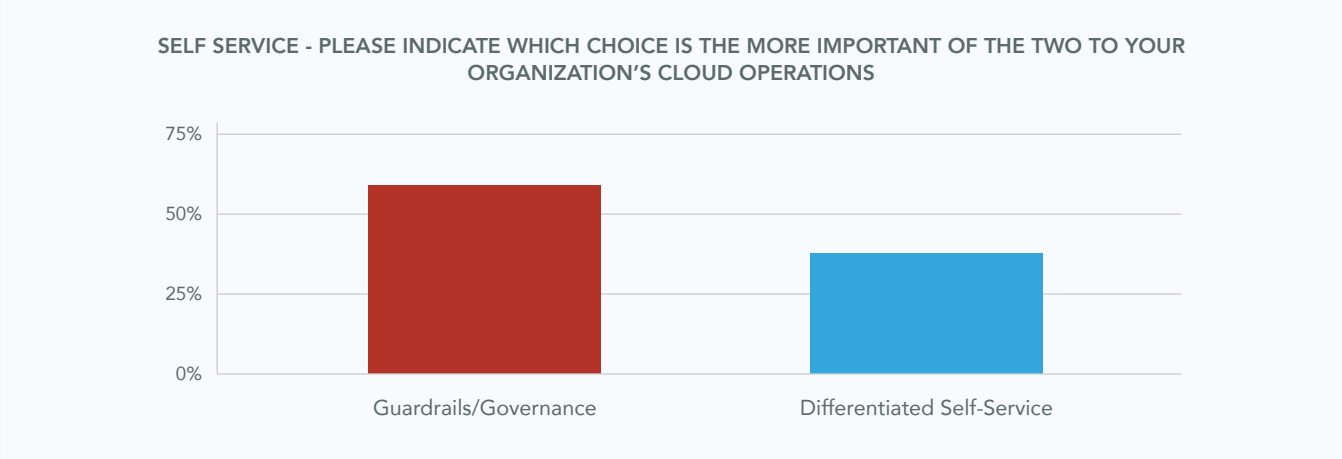
Self-Service stands at the front-end of complex cloud environments. The methods organizations use to deliver Self-Service workloads to application teams and different end-users often determine the productivity of individual teams and agility of the overall business.

Enterprise IT typically serves a wide variety of users, from basic users who value ease of use, to advanced power users who value operational flexibility. In both cases, organizations must find a balance between user productivity and compliance with best practices and company policy, especially in hybrid or multi-cloud environments.

Survey respondents were asked to indicate which aspect of Self-Service is a bigger concern for their organization:

- **Guardrails/Governance** - Building guardrails to keep usage within company policy while still providing users the flexibility they need.
- **Differentiated Self-Service** - Providing each type of user the workflow that makes them most productive. Basic users get an easy one-click service catalog, power users get more advanced consoles and APIs.

58% of respondents indicated that Guardrails and Governance are more important to their cloud operations. Building a standardized provisioning workflow ties together the points previously discussed in this paper - Security, Cost and Automation. A Director of IT from one Fortune 20 company said that he uses guardrails to create an environment in which users can "innovate and fail safely."



5.5 Relative Importance of Cloud Concerns

While Security, Automation, Cost and Self-Service play important roles in a multi-cloud environment, organizations often have to choose the main driver behind their cloud strategy. Survey respondents were asked to rank the relative importance of these concerns to their cloud operations.

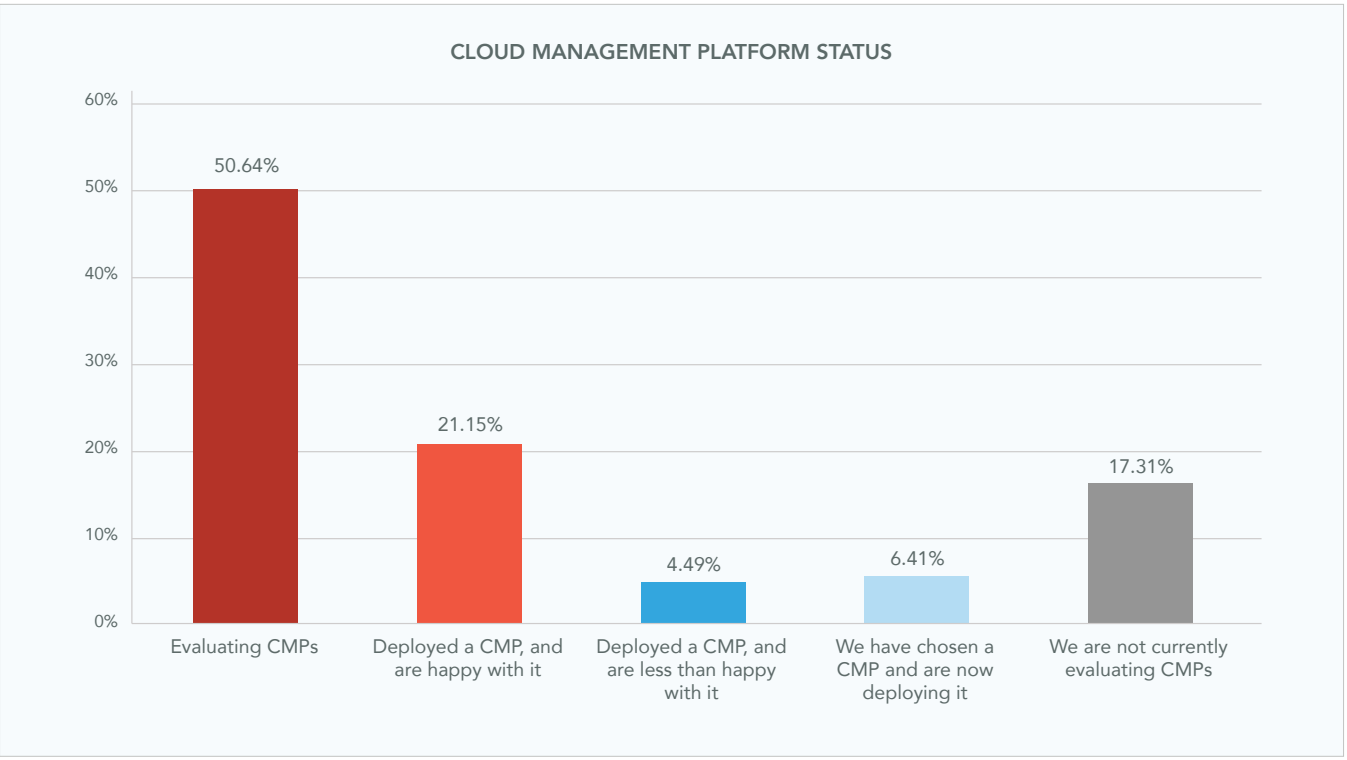
Security was ranked as the leading concern by a wide margin, followed by Cost. It's important to note that for the purposes of this survey, **Compliance** is represented under the Security category.

6. Adoption of Cloud Management Platforms

As signified by this study, most enterprises are adopting some form of multi or hybrid cloud strategy, while serving multiple business units or teams with different needs. All the while, IT is tasked with maintaining best practices and compliance with cost and security standards.

The emerging path to tackling these challenges is through the use of Cloud Management Platforms, which help enterprises giveteams the flexibility they need while maintaining policies. Over **82% of respondents from enterprises with over $500M in annual revenue are either using a CMP today or evaluating one**.

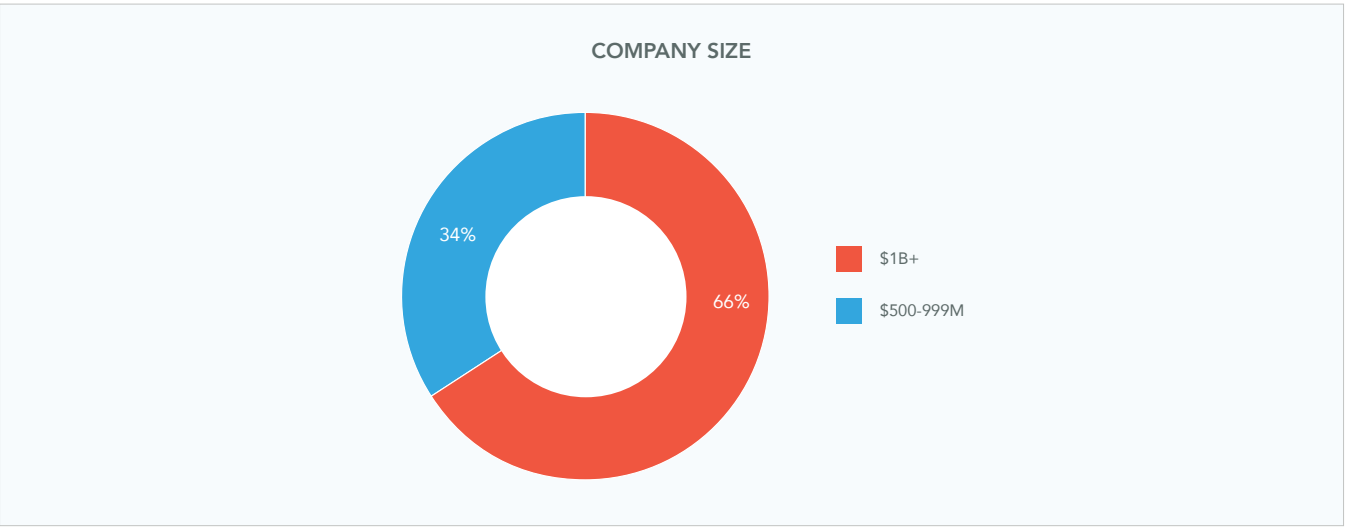
A successful implementation of a Cloud Management Platform balances the needs of multiple enterprise groups, from enforcing security and cost standards, to enabling accountability via clear ownership of resources, and improving user productivity through customized provisioning workflows.



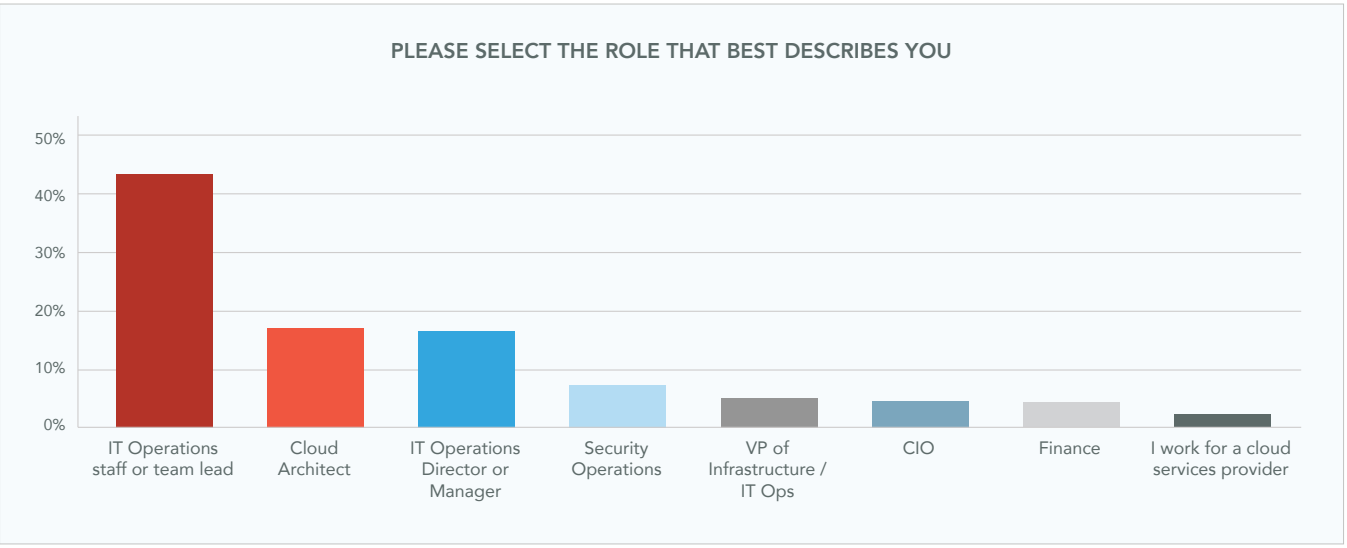
> ***"Someone thinks we're going to build our own CMP, this will likely fail though"*** - Anonymous Survey Respondent

7. Survey Respondents - Who Participated?

The Cloud Management Landscape survey focused on respondents in IT leadership and operations positions in enterprises with over $500M in annual revenue. The majority of the respondents work for $1B+ companies.



Approximately **44%** of respondents are in IT operations positions, and the rest are in a variety of IT or IT related positions such as Cloud Architects, CIOs, VPs of Infrastructure, Security and more.



8. Methodology

ViB polled 458 respondents, representative of it's community of over 100,000 IT professionals involved with managing public, private and hybrid clouds. To insure accuracy, respondent response data was subject to analysis against level of respondent engagement criteria (level of attention) which is a primary indicator of respondent data quality. ViB also utilizes industry best practices in question formation to eliminate interpretation ambiguity, and eliminate well-established forms of response bias. The survey had a 4.6% margin for error at a 95% confidence rate using traditional calculation methods, and when adjusted for screening and respondent data quality analysis had an effective margin of error of 3.16%

ViB's advanced survey methodology brings accuracy and understanding to new levels through an innovative approach at the PhD-level nexus of research art and science. ViB employs advanced screening techniques to insure respondents are representative of precisely targeted populations and advanced behavioral approaches to insure they are fully engaged in providing credible, carefully considered responses. ViB combines this with strong technology domain expertise, and sophisticated survey design and analysis to fully capture all relevant dimensions of interest including the most difficult to surface impactful insights. ViB has programs for all budgets, and require little to no client survey expertise, time, or effort to deliver outstanding results.

9. About Scalr

Scalr was founded in 2007, right at the dawn of the public cloud revolution, from the challenge of federating dispersed IT teams over common cost and security standards while preserving local autonomy. Thus was born the Scalr Organizational Model, a model that combines proactive and reactive policies with a hierarchy that maps to your organization's structure. The result is the Scalr Enterprise-Grade Cloud Management Platform which enables today's enterprises to achieve cost-effective, automated and standardized application deployments across multi-cloud environments.

The Scalr Enterprise-Grade Cloud Management Platform enables today's enterprises to achieve cost-effective, automated and standardized application deployments across multi-cloud environments. Scalr utilizes a hierarchical, top-down approach to policy enforcement that empowers administrators to find the balance between the needs of finance, security, IT and development teams. Leading global organizations have selected the Scalr platform, including Samsung,, NASA JPL, Gannett and the Food & Drug Administration.