The Public Cloud Governance Imperative

Pathfinder Report

September 2022

Commissioned by

vmware®

451 Research

S&P Global
Market Intelligence

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About the Author

William Fellows

Founder & Research Director, Cloud Native

As Research Director, William is responsible for the Cloud Native Channel at 451 Research, a part of S&P Global Market Intelligence. With a 20+ strong team of collaborators, this Channel provides a point of intellectual convergence for 451 Research around cloud native computing and offers customers a direct path to understand its adoption and impact across all sectors.

William has a long history of tracking cloud infrastructure, beginning with its foundational elements such as distributed and grid computing and virtualization, establishing and running 451's Cloud Transformation Channel for more than a decade. He created 451 Research's early adopter research program, working with enterprise end users and innovators, and he created 451's Digital Economics Unit in 2014 and the Blockchain Center of Excellence in 2017. In 2020 he formed the Cloud Native Channel to focus on the re-platforming to cloud native constructs and such as containers, service mesh, Kubernetes and serverless, from application and infrastructure perspectives. William has been a member of the European Commission Cloud Expert Group, co-authored The Future of Cloud Computing Report and worked on various EC-funded cloud projects.

Prior to starting 451 Research, William was a financial and technology journalist with ComputerWire (now part of Informa) in London and New York. He has held various senior management roles at 451 Research since 1999. William has a master's degree in computing science from the University of Portsmouth, and a BA in Government and Sociology from Essex University.

Executive Summary

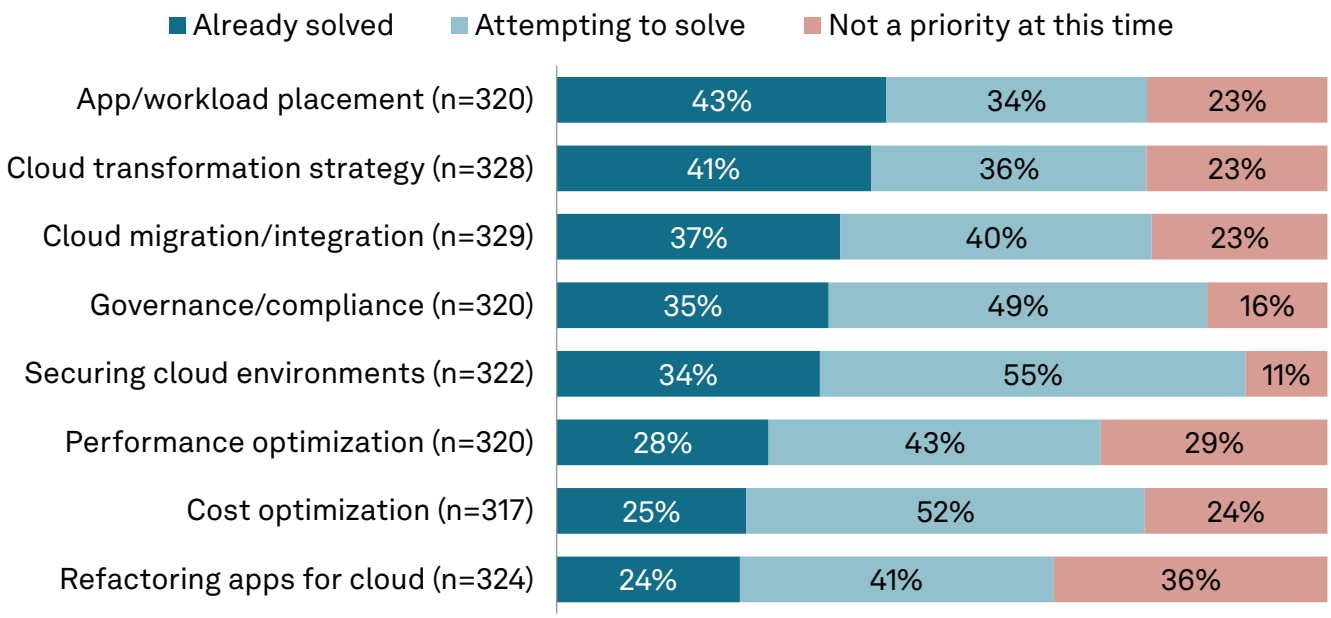
Application and cloud transformation are still underway at most organizations, and they are changing software development forever. We are entering an era in which cloud will no longer be seen as a separate IT category: quite simply, cloud is IT. Organizations are racing to deliver new products and services by leveraging software running in the cloud. They are seeking to build, operate, manage and secure workloads here, there and everywhere with ecosystems of public, private and edge clouds and enabling software. Cloud native has shifted modern software development from a model shaped by browser-driven consumption concerns to one focused on optimizing the software architecture to achieve improved longevity, security, supportability and resilience. Cloud native enables successful enterprise DevOps, whereby developers and IT operations teams collaborate for faster releases, greater efficiency and readiness for market changes, and the whole notion of "shift left" comes from cloud native.

Organizations are improving operational velocity, but they must also ensure operations are secure, controlled and available. While developer enablement and the developer experience are now strategic to the enterprise, the greater use of cloud and the vast number of services and components spread across the major public clouds creates IT complexity and operational challenges that can undermine the efforts to execute on digital transformation strategies.

Organizations are embracing multicloud — sometimes as a consequence of a merger or acquisition, but more often because of data compliance or to access a particular cloud provider's unique service. Multicloud offers many advantages, but along with those come challenges. Multicloud environments tend to be assembled by happenstance rather than by design, meaning there is an inevitable shortfall when it comes to governance. However, in order to reap the benefits that come with using public clouds, organizations must handle multicloud environments consistently, which is where the hard work begins. Multicloud governance and policy management help to address public cloud governance by configuring high-level organizational rules, or cloud "guardrails," across public clouds, enforcing and checking compliance (i.e., checking drift from the desired state) and remediating drift and violations across public clouds.

According to our research, most organizations are still attempting to solve issues associated with public cloud governance/compliance and security; only a third of respondents say they have already solved these issues (see Figure 1). Even fewer have solved cost and performance optimization issues — areas where cloud automation platforms must also be leveraged.

Figure 1: Progress in Addressing Public Cloud or Hosted Infrastructure Challenges



Q. For each of the following challenges associated with public cloud or hosted infrastructure, please indicate whether your organization is currently attempting to solve the issue, has already solved it, or it is not a priority.

Base: Using or planning to use IaaS/PaaS or hosted private cloud

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Budgets & Outlook 2021

Identifying the Drivers of the Shift-Left Movement

It is the cloud "operating model" that delivers the cloud experience, not the venue per se. The specific location of private, public and edge cloud environments is therefore less important than the challenge of integrating the infrastructure/application resources in a way that provides a consistent "landing zone" experience across the IT estate and the ability to move data and workloads freely and securely between venues with low-latency and high-performance interconnections. All of this is leading into a storm of complexity, compounded by the vast number of services and components that are spread across the major public clouds. When we asked our Voice of the Enterprise survey panel to characterize the complexity of their organization's cloud IT environment, nearly three-quarters rated it as highly or moderately complex. The most commonly cited factors contributing to that complexity are technical debt, application modernization, compliance for regulated workloads and data silos. Nearly three-quarters of organizations currently use multiple cloud platforms, and 451 Research's Cloud Price Index now tracks more than three million products (SKUs) that can be purchased from the major hyperscalers alone.

Governance is a perennial challenge, and considerable effort is needed to bring this under control given the conditions described above. The expansion of cloud usage and the uptick in cloud migration resulting from organizations' IT responses to the COVID-19 pandemic are no doubt additional contributing factors. In short, governance, risk and compliance takes on ever greater importance as enterprise IT estates become ever more "cloudy."

As a consequence, there is a growing, unmet need for automated public cloud governance and policy management for cost, performance, security, networking and configuration across both greenfield and brownfield environments. Key requirements include ensuring that infrastructure and applications are secure to meet enterprise standards, that application performance and availability can always be seen regardless of whether a workload runs on a public or private cloud, and that cloud budgets and cost can be optimized.

We believe organizations must embrace "shift left" (putting in controls early in the process), and seek automated approaches wherever possible, ensuring their governance practices and guardrails are developer-friendly (integrated with workflows and tools) and expressed in plain language. Some guiding principles are:

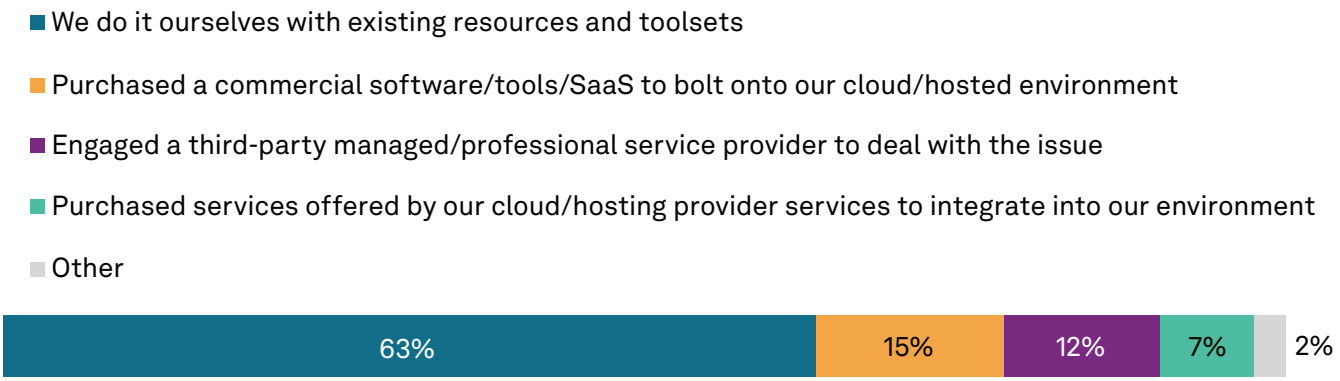
- **Keep an eye on the prize.** Buyers should determine the suitability of public cloud governance tools in terms of how effectively they support the desired business outcomes.
- **Occupy the driver's seat**. The platform should enable organizations to make decisions about how and where to take advantage of cloud services, avoiding vendor lock-in.
- **It's not all about technology.** Larger organizations with a growing cloud presence are learning that cloud-governance challenges extend beyond the immediate technical controls that need to be applied. They also include alignment with organizational structures, workflows and cross-functional teams. This may require some internal adjustments to both team structures and roles.
- **Successful projects require a top-down mandate.** Standardizing any aspect of governance across organizational boundaries requires a top-down impetus that is comprehensive and sustained to support new, more effective ways of working that span the project life cycle.
- **Embrace automation.** The complexity of modern cloud-native, multicloud IT environments has made automation a more crucial technique. The amount and pace of change means that most teams don't have enough people to execute all of the required governance, management and monitoring functions.

- **Aim for auto-remediation**. Organizations seeking visibility, faster service delivery and savings associated with a reduction in manual intervention of their infrastructure will need governance tools that can automate processes and offer auto-remediation against policy.
- **Treat IT as a production system instead of a support system**. The C-suite points to multicloud and cloud native as IT weapons to bring to the fight against variables such as uncertainty and rapidly changing market conditions. The ability to govern public multicloud use at scale from a single point of control should be a cornerstone of enterprise IT.
- **Cloud first requires a policy-first posture**. Cloud governance for large organizations not only requires a focus on developer-centric constructs, but it must also start with a policy-first approach that is then assessed continuously.

The Emergence of the Automated Cloud Governance Platform

Recent 451 Research data reveals that nearly two-thirds of enterprises surveyed are still trying to solve the challenges of governance and compliance using their own resources and assets (see Figure 2). Just 15% have purchased a commercial software tool to use with their cloud, 12% have engaged a third-party service provider to deal with the issue, and 7% have purchased services from their cloud provider to integrate into their environments. Given the breadth of the problem and the acceleration of public multicloud use, we believe it will become increasingly difficult for enterprises to develop and maintain their own automated platforms and tooling sufficiently to deliver the level of governance and policy management required. This indicates a significant unmet need for automated approaches to public cloud governance.

Figure 2: Progress in Solving Governance and Compliance Issues



Q. You indicated that you have solved, or are attempting to solve, the issue of governance and compliance. Which of the following best describes your organization's current/planned approach to dealing with this challenge?

Base: Have solved, or are attempting to solve, the issue of governance and compliance (n=41—Note: Base sizes below n=50 should be interpreted anecdotally)

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Budgets & Outlook 2021

Most organizations still use spreadsheets to manually track policy and exception data across their clouds. Their tracking solutions also generally involve several tools, many of them siloed, such as PowerShell, native API scripting and custom scripting. Traditional IT policies and processes formerly captured in writing or held as "tribal knowledge" don't support the move to much-needed automation of a new, agile operations model. These governance processes and tools were not built for real-time operations, so enterprise cloud practitioners face some key challenges, including:

- Processes that are constrained by internal silos.
- Difficulty managing sprawling multicloud assets/resources.
- Prevailing reliance on manual interventions.
- Poor support for developers who move very quickly to bring new products to market.

Ideally, organizations would be able to create "landing zones" across clouds to achieve consistency in terms of security, performance, availability and cost. But in practice, this doesn't work because the various clouds use different tools and have different requirements. And when an organization starts using more clouds, typically much of the landing-zone design and policy operation won't be fully documented into libraries, meaning security teams have to do one-off remediations. Implementing governance today therefore requires the use of multiple tools and technologies, which results in complex environments that must be managed by IT teams. Businesses would much rather incorporate multicloud practices that provide them with:

- Better governance and controls over specific/overall cloud service costs.
- Assured data security and sovereignty controls.
- Adherence to compliance/regulatory rules.
- Guaranteed performance.

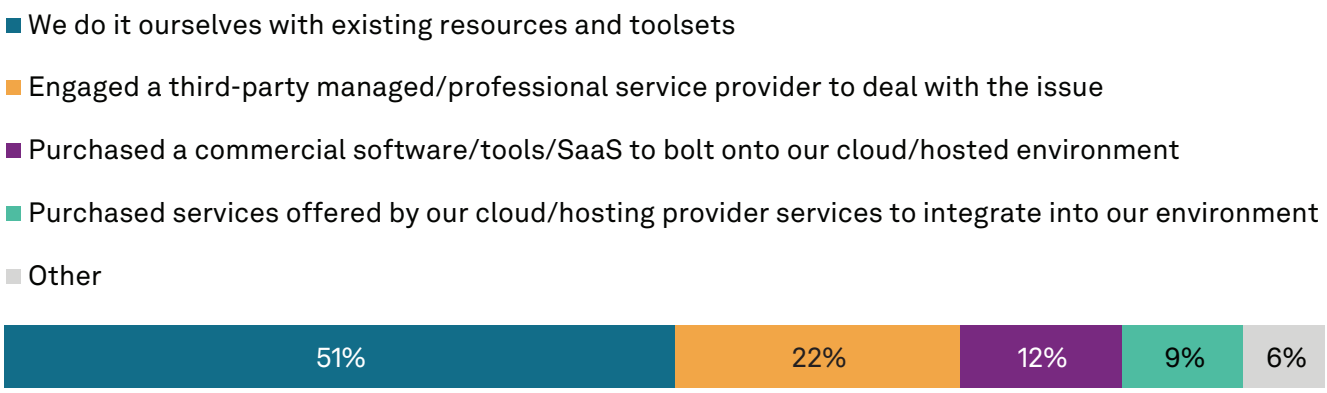
What will it take to deliver this? Going forward, the benchmark for supporting successful guardrail operations will be cloud automation platforms that allow operators to see any environment in any cloud plus all of the changes taking place — or required — in a self-service fashion. This can only be achieved via a streamlined process using human-readable (such as YAML) templates to describe the desired state of the cloud, as well as everything about its network and attached policies. Ultimately, this will result in the delivery of a single-button approach for managing each of the supported clouds with a built-in policy action or response. Templates ensure standard approaches to cloud service policy definition and/or landing-zone creation. A policy library may include templates for bootstrap, network, security, cost, configuration and performance, etc. In this way, the cloud automation platform can take advantage of native cloud policy engines as well as third-party policy engines and provide permissions by using service roles and user roles.

Moreover, because policy libraries are reusable for any cloud, organizations would be able to connect different policy engines that are already in place – such as drift management or policy violation – rather than rebuild or integrate them for use with this approach. (This in itself brings considerable operational benefits in terms of time and cost savings, in addition to the foundational guardrail services). Furthermore, monitoring consoles that offer visibility at all levels of a public cloud service — to view the template and code for any environment, plus the drift that may have occurred — should generate options for auto-remediation against the change or drift to ensure that the tolerance to process rules/governance is maintained. If the new state is accepted, this should then be written back into the desired state in the template to reflect the (new) real state of the cloud service and not just the original base. Not all remediations need to be auto-triggered — customers may want to set approval policies before remediations are applied, and the offline communication between teams can be a big roadblock. However, it is imperative that a user's persona defines the appropriate policies, but that implementation resides with the cloud development team. Today, such operations require multiple tools. In future, we believe these platforms will begin to offer:

- A consolidated view of multiple public cloud accounts for central management.
- Automated controls over cloud service drift to "correct" processes and services.
- Rule-based remediations and interventions.
- Cost/security/sovereignty governance requirements maintained at all times in real time.

This latter issue is of particular concern in today's multicloud world. When dealing with multiple clouds that have different security controls, risk postures and vulnerabilities, applying an organization-wide security policy/framework is a particular challenge. More than half of organizations surveyed are attempting to solve this issue using their own tools (see Figure 3), while 22% have engaged a third-party managed/professional service provider to deal with the issue, another 12% have purchased a commercial software tool to use with their cloud environment and fewer than 10% have purchased services offered by their cloud provider to integrate into their environments.

Figure 3: Progress in Applying an Organization-Wide Security Policy/Framework



Q. You indicated that you have solved, or are attempting to solve, the issue of application of an organization-wide security policy/framework. Which of the following best describes your organization's current/planned approach to dealing with this challenge?

Base: Have solved, or are attempting to solve, the issue of application of an organization-wide security policy/framework (n=65)

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Budgets & Outlook 2021

This is a problem highlighted by an IT engineering practitioner at a large financial services company (and a participant in our Voice of the Enterprise survey panel). In the decentralized development model, which is now commonplace and increasingly enabled by the use of modern cloud-native constructs and DevOps processes, each line of business is following its own best practices and its own tools for scanning vulnerabilities. The view is that to help prevent breaches that exploit this loosely coupled environment, enterprises should have more automation and governance as part of a more solid enterprise-level practice to secure the decentralized development cycles that are in operation.

"Development work is very decentralized, and every line of business … **each of them follow their own good practices and their own tools for scanning vulnerabilities** … I would like to see **more** of **governance** on our cycle and a more solid enterprise-level type of secure practices and **automation** for preventing the same type of issues that caused the SolarWinds incident."

IT/engineering manager/staff

10,000-49,000 employees, $5B-$9.99B revenue, financial services

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Application Modernization 2021

The cross-functional impact of multicloud governance is a shared responsibility for automation across clouds. As such, the tools will need to support a range of use cases:

- SecOps, NetOps and FinOps admins — to track approvals and exceptions across public clouds with centralized policies and compliance visibility.
- Cloud ops admin — to curate, templatize and package compliant cloud environments.
- SRE admin — to gain access to compliant cloud environments in a self-service operation and set up just-in-time access for cloud developer users.
- Cloud dev — to gain just-in-time access to requested environments.

Conclusions

There is considerable benefit to embedding the "guardrails" enforced by an automated cloud governance platform inside the infrastructure, as a mid-level manager at a large consumer/retail enterprise observed. This is because the use of cloud native typically rests on an underlying assumption that development teams are agile (using DevOps processes, for example), and that they will have everything they need to develop a required application successfully without crossing organizational boundaries. Whether a resource is developed internally or provided by a third party, the key is that development teams can implement their knowledge quickly and easily. Embedding guardrails within the infrastructure allows developers to create what they have been asked with minimal oversight.

"A lot of cloud native assumes that the development team is an **agile development team**... where they have everything that they need in order to **develop the application without organizational boundaries** having been crossed. This is important for us because... when we have new outsourcers come in, we want to let them use what they know quickly and easily and **hide the guardrails inside of the infrastructure** and allow them to create what we've asked them to do without a lot of oversight."

Mid-level management

100,000+ employees, $10B+ revenue, consumer/retail

Source: 451 Research's Voice of the Enterprise: Cloud Hosting & Managed Services, Budgets & Outlook 2021

Today, enterprises have mandates to ensure they are complying with policies in real time, especially when onboarding cloud workloads — on an ongoing basis. We see automated public cloud governance as imperative to delivering cloud landing zones that are always compliant with their stated policies. This helps organizations harness the power of multicloud to achieve their goals. Without this, it is difficult to ensure compliance across clouds, and when an issue is resolved, remediations are manual and inconsistent. Organizations need to address such public cloud governance challenges with consistency across their multicloud environments.

We believe cloud automation platforms are now beginning to emerge that could offer some resolution of these issues, by:

- Providing for central policy administration.
- Offering streamlined processes and process controls for different business units and stakeholders.
- Allowing integration of cloud silos within the organization.
- Offering better alignment of cloud services to business goals.
- Providing easy-to-use self-serve access.

Infrastructure-as-code approaches to automated cloud provisioning services for policy and infrastructure must satisfy the requirement that environments be compliant with an organization's rules for configuration, security, network, performance and cost. These mechanisms will run high-level rules (policies) using code templates to provide ongoing governance for both private and public cloud environments. The rules are applied to achieve a "desired state" for an environment that aligns to the intention of an organization's policies. In this way, policies are centralized, enabling organizations to deploy them in a self-service fashion, to observe the results and take the necessary actions to meet their business objectives.

As organizations move critical applications and data to the cloud, the governance, security and risk management stakes skyrocket. Increased technical complexity, greater demand for faster time to value and a much greater number of cloud initiatives have created a "perfect storm" for DevSecOps, IT and FinOps teams. Implemented well, we believe cloud governance and policy management "guardrails" can deliver organizations complete visibility into their cloud activity, enabling them to take control, which is foundational for optimizing performance, lowering operational costs and minimizing security risks as cloud usage grows.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence