

Enterprise Spotlight: Making the most of multicloud



Credit: Shutterstock

For IT leaders navigating multicloud environments, success depends on strategic alignment across business units, robust governance frameworks, and proactive security postures. While multicloud offers agility and vendor flexibility, it also introduces challenges in visibility, compliance, and developer productivity. In this special report, you'll learn how to take advantage of benefits of using multiple clouds, avoid common

pitfalls, and ensure that multicloud is worth the investments.

CONTENTS

- 2** 5 challenges every multicloud strategy must address
- 7** Securing a multicloud environment
- 11** Multicloud ROI: Maximizing value and efficiency
- 17** How to excel in multicloud: The new checklist

From the editors of Foundry's enterprise IT sites:

CIO **CSO** **COMPUTERWORLD** **InfoWorld** **NETWORKWORLD**

5 challenges every multicloud strategy must address

Managing multiple providers in a single environment poses distinct challenges. Here's how to ensure your multicloud strategy is secure, harmonious, and cost-effective.

BY **BOB VIOLINO**

It's no longer a question of whether enterprises need multiple cloud services, but which ones they should deploy and how best to craft a multicloud strategy that creates the most value for the business. That strategy had best take into account the challenges organizations are most likely to face on their multicloud journey. Here are five potential issues CIOs and other IT leaders must be aware of when planning or maintaining a multicloud environment.

AI'S MASSIVE IMPACT

The AI juggernaut is affecting just about every aspect of the IT stack, cloud services in particular. But when it comes to running AI workloads in multicloud environments, complexity compounds. Key hurdles include ensuring data security, interoperability, and performance optimization.

Enterprises often need to integrate AI and machine learning models across

a variety of cloud environments, which can be a complex undertaking due to the different APIs and data formats necessary to do so.

Transferring AI data among various cloud services and providers also adds complexity — and significant risks.

“Tackling software sprawl, especially as organizations accelerate their adoption of AI, is a top action for CIOs and CTOs,” says Mindy Lieberman, CIO at database platform provider MongoDB. “AI is transforming processes and empowering employees to focus on their most impactful work. But every new initiative can add to the complexity of an already sprawling tech stack.”

Failing to deploy [active governance initiatives](#) can lead to uncontrolled consumption, rising costs, and deepening technical debt, Lieberman says. “Without managing that debt, organizations can't move with the agility needed to compete in today's [demanding] economy,” she adds.

AI can also be part of the solution, Lieberman says. “When leveraged effectively, it can help identify redundant systems, improve governance, and intelligently monitor software usage,” she explains. “AI tools can even help IT teams in their efforts to modernize legacy tech infrastructure and consolidate on modern, cloud-native platforms.”

CIOs need to monitor cloud services consumption closely, using AI to eliminate complexities of the multicloud environment. “The solution landscape is complex and evolving quickly, so technologies need to be evaluated not just on what they can accomplish today, but where you expect them to be in six to 12 months,” says Lieberman.

DATA SOVEREIGNTY REQUIREMENTS

A multicloud environment can complicate the management of data sovereignty. Companies need to ensure that data remains in line with the laws and regulations of the specific geographic regions where it is stored and processed.

Addressing this challenge requires careful planning and ongoing management to navigate the diverse regulatory landscapes in non-US locations.

“As a publicly traded, multinational company, we must follow the regulations and reporting requirements in all the

countries where we operate,” says Scott duFour, CIO at financial services provider Corpay.

For example, the General Data Protection Regulation (GDPR) requires that Corpay’s EU customers’ data stays within the EU. “So, we have to create a new instance in the EU landing zone, increasing our costs,” explains duFour.

This also applies in the US, duFour says. IT has forged a data governance partnership with Corpay’s compliance team to adhere to reporting requirements for the company as well as its third-party partners.

“This [is] especially true in California, which is leading the way with data privacy legislation in the US,” says duFour. “Being compliant is non-negotiable, but we still must strike a balance between expanding and [consolidating] our cloud-based service footprint on a case-by-case basis, with the goal of managing costs and driving revenue.”

CYBERSECURITY RISKS

Deploying even one cloud service [can present cybersecurity risks](#) for an enterprise, so having a strong security program in place is [all the more vital for a multicloud environment](#). The risks stem from expanded attack surfaces, inconsistent security practices among service providers, increased complexity

of the IT infrastructure, fragmented visibility, and other factors.

IT needs to be able to manage user access to cloud services and detect threats across multiple environments — in many cases without even having a full inventory of cloud services.

“Managing access and protecting data in a multicloud environment requires a multifaceted approach,” argues Scott Simari, principal at Sendero Consulting. “Think of it like securing a physical data center: You establish a defense perimeter using firewalls, log monitoring, malware protection, and antivirus solutions.”

Even though cloud service providers offer their own security features, most companies will still “ring-fence” their own networks within each cloud using their preferred security tools, Simari says.

“The [challenge in multicloud](#) is ensuring consistency and appropriate measures across different providers,” explains Simari. “Security standards and regulatory requirements can differ, and certain types of data may have specific mandates.”

Sendero’s work with a utility company that owns and operates nuclear power plants highlights this. “Federally regulated data can only reside on government-controlled instances of the cloud — like Microsoft’s federally approved cloud, not their commercial cloud,” says Simari.

“This necessitates a tailored approach to data loss prevention and security apparatus for each cloud.”

While general security practices apply regardless of whether an enterprise uses a single or multicloud environment, a multicloud setup enhances the case for adopting more rigorous practices, Simari says. This includes centralizing identity and access management to ensure user provisioning and authentication across all platforms.

“It’s also crucial to apply least-privilege or just-in-time access principles, which grant users only the necessary permissions for the shortest possible duration,” argues Simari. “Organizations should also prioritize encrypting data both at rest and in transit, while centralizing key control for managing encryption keys across disparate cloud services.”

NEED FOR FLEXIBILITY AND OBSERVABILITY

As technology evolves to solve increasingly complex problems, the infrastructure and services needed grow more sophisticated as well, says Bryan Wall, senior competency leader, cloud engineering at Experis, a provider of staffing and managed services.

“With greater complexity comes more potential avenues of failure, but also more opportunities for customization

and optimization,” says Wall. “Each cloud provider offers unique strengths and weaknesses, which means forward-thinking enterprises must know how to leverage the right services at the right time.”

The key to harnessing the advantages of multiple clouds lies in flexibility and observability, Wall says. “Flexibility begins by ensuring that custom software is not tightly bound to a single provider. Containerization and cloud-agnostic orchestration allow teams to deploy workloads anywhere, aligning specific applications with the providers best suited to their needs.”

This flexibility, however, requires operations teams to understand the nuances of each cloud. “Observability is what makes this manageable at scale,” explains Wall. “A holistic monitoring and cost-management platform is essential to unify disparate tools and provide actionable insights.”

As organizations expand across multiple hybrid cloud platforms, maintaining clear visibility becomes increasingly complex, says Chris Thomas, principal at Deloitte Consulting. “Without robust, cross-platform observability, it’s easy for issues to go undetected, impacting everything from compliance to customer experience,” he says.

To address these challenges, organizations are adopting unified

monitoring solutions that aggregate data from all hosting platforms, enabling real-time insights and proactive response, Thomas says. “Organizations should give thought to using AI-driven analytics to identify patterns and anomalies that might otherwise be missed in siloed environments,” he recommends.

COST CONCERNS

Keeping costs under control in a multicloud environment can be a challenge for enterprises. This is deeply intertwined with effective financial management, often referred to as [FinOps](#), Simari says. FinOps is a cloud management practice focused on optimizing spending by fostering collaboration among IT, finance, and business teams.

“FinOps is about ensuring you’re a responsible steward of your cloud resources and ensuring that you’re not leaving money on the table,” explains Simari. “This means diligently conducting cost-benefit [analyses] for any services you use and being mindful of consumption and operational costs.”

Without proper oversight, it’s easy for expenses to escalate, Simari says. “When conducting these analyses on behalf of our clients, we’ve seen that some organizations are paying for way more cloud space than they need,” he reveals.

“FinOps involves ongoing monitoring of usage, optimizing resource allocation and leveraging pricing models effectively across different cloud providers, to ensure organizations are getting the most value for their investment.”

Containing software-as-a-service (SaaS) costs is especially challenging for Corpay, which has grown its business largely through acquisitions.

“Each company we [acquire] has its own environment such as AWS or Azure, so we have to move them over to our landing zones to maintain security and operational control,” says duFour. “With each acquisition, we have a goal of creating synergies and alignment that help control costs and prevent creep, while maximizing the benefits and efficiencies we gain. As we add additional companies to Corpay, this will continue to be an on-going exercise.” ■

Securing a multicloud environment

From inadequate visibility to access management complexity, multicloud environments take baseline cloud security issues to another level.

BY MARY K. PRATT

A multicloud environment is now standard for midsize and large organizations, with tech leaders opting to use multiple cloud providers for the improved flexibility, resiliency, and additional advantages that operating in multiple clouds brings.

But a multicloud approach also comes with challenges, particularly when it comes to security.

In fact, CISOs listed managing multicloud and hybrid cloud as one of their organization's biggest cybersecurity challenges, according to the [2025 Cloud Security Report](#) from Check Point Software Technologies. It came in at No. 3, after safeguarding high-value assets and intellectual property and enhancing threat visibility and detection.

Securing a multicloud environment isn't a singular challenge, however; it's a whole host of them. Here is a look at the most significant challenges CISOs and their teams face in this space.

ACHIEVING ADEQUATE VISIBILITY ACROSS ALL CLOUDS

This challenge tops the list for many security leaders. Experienced CISOs acknowledge that getting an accurate and complete picture of the IT environment has long been a tough task — whether it's all on prem or all in the cloud. But they stress the job is more complicated and complex in an environment that sprawls across multiple cloud providers.

That sprawl makes it harder for CISOs to “have confidence that they're looking across the environment holistically, that they're looking for all the right things, and that there isn't some security piece that they've overlooked,” argues Randy Armknecht, who as a managing director at consultancy Protiviti leads its global infrastructure, cloud, and security engineering practice.

CISOs, of course, have some visibility across all their cloud deployments. Indeed, they may even have great visibility

into one of their cloud environments — typically the first cloud the organization adopted, because they had invested heavily in training their teams to use that provider's observability tools when they first made the move to that cloud.

However, CISOs frequently lack the resources — time, skills, and tools — to extend that visibility into the other cloud setups as their organization expanded, Armknecht says. And even if CISOs and their teams are well versed in the observability tools provided by each cloud provider, they typically still struggle with managing information from those multiple tools, he adds.

"Most security practitioners feel more at home in one cloud than the others, and they may feel really good about one of them, but they do not have the same level of confidence about the others," explains Armknecht.

Technology advances are helping CISOs overcome this challenge. Armknecht points to tools such as [cloud-native application protection platforms \(CNAPPs\)](#) that offer multicloud observability.

He sees the use of such tools as an imperative. "I'm a fan of getting full visibility as quickly as you're able. I would not want to be at the table being asked why we didn't know about a problem that led to a breach," he says.

BALANCING THE EASE OF A UNIFORM SECURITY PROGRAM WITH THE BENEFITS OF A PROVIDER-SPECIFIC APPROACH

Some CISOs opt to have a single security program for their entire cloud environment while others take a cloud-specific approach. Each strategy has pros and cons, says Wolfgang Goerlich, IANS Research faculty and a public sector CISO.

"If you're treating all clouds the same, if you have a unified security program, then that means you're not using the native security tools and you're not driving the value out of each cloud. And not all solutions will pull in data [from each cloud provider] with fidelity, and not all apps will be as granular as the native tools," he explains. "But if you go native, if you do a deep dive into each cloud, you add more tech and you probably won't have teams who can work across the different clouds, so you create more challenges with processes, staff, and technology."

Goerlich doesn't list one option as better than the other, but instead stresses the need to weigh the benefits and drawbacks of each one when devising an enterprise security plan.

"It's all about the tradeoffs," he says. "You can organize your team by cloud to drive more value from native capabilities, or have your team know enough about

each cloud to effect change, or take it to a high level and not use the native tools.”

FALLING SHORT ON THE BREADTH AND DEPTH OF SKILLS REQUIRED TO SECURE MULTIPLE CLOUDS

Securing multicloud environments requires more skills than the skills needed to secure a homogenous environment — a requirement that adds more stress onto CISOs who are already struggling to keep up with all the skills now needed to protect a modern enterprise.

Moreover, the skills the team does have tend to be unevenly distributed.

“Most companies lean into one cloud and their skills hone in on that one cloud provider, but that means they lack the skills for the others,” argues George Gerchow, faculty at IANS Research and CSO at Bedrock Security.

For example, a team skilled at collecting logs from AWS may not have the aptitude to confidently handle the same task in Azure and vice versa, he says. “Even at a high level, the logs themselves are different from cloud provider to cloud provider. How you ingest all the right logs to do security investigations as well as how you find security vulnerabilities is different,” explains Gerchow.

Having a well-thought-out security strategy to balance the ease of a uniform

security program with the benefits of a provider-specific approach (Challenge No. 2) can help identify the needed skills.

Then CISOs need a solid training program to ensure staff members have the skills they need to successfully execute the strategy across the multicloud environment and with each cloud provider, Gerchow says. In other words, CISOs must invest enough in getting their people trained to work effectively in each cloud used by the organization.

GETTING CONFIGURATIONS RIGHT

Getting configurations right in any environment is a difficult task, but security leaders say both the scale and the scope of a multicloud environment make that task exponentially more challenging, according to Gerchow. That’s because each cloud provider has its own set of services, APIs, and management interfaces, as well as its own rules and systems for managing configurations.

Taken all together, that puts more stress on security teams, who must not only learn and master all the cloud-specific tools and techniques but also keep track of which tools and techniques apply to which cloud provider to ensure they don’t make a configuration mistake.

Mistakes are common: The [2024 Cloud Security Report from Check](#)

Point found that 23% of survey respondents who had experienced a public cloud security incident blamed misconfigurations. Common misconfigurations include overly permissive access controls, exposed storage buckets, unencrypted data, and inadequate network segmentation — all of which can lead to data breaches and unauthorized access.

GETTING IDENTITY AND ACCESS MANAGEMENT RIGHT

CISOs face similar challenges with identity and access management (IAM) in a multicloud environment, says Jeffrey Brown, former CISO for the State of Connecticut and now a cybersecurity advisor for financial services and state government at Microsoft.

To be clear, CISOs struggle with IAM in an on-prem and single-cloud environment, too. But they face more challenges in getting IAM right in a multicloud environment because they must work across the different cloud providers, each with their own IAM systems, operating models, policies, and procedures. And they must manage user identities, roles, and access control mechanisms for each cloud. All this gives CISOs exponentially more to track and manage.

Moreover, multicloud environments also have more nonhuman entities

(such as APIs and services) that must be managed across multiple clouds, too, further adding to the complexity and scale of IAM in a multicloud environment.

And, of course, each identity has to be managed over its life cycle — further compounding the size of the challenge. All this can — and often does — lead to inconsistent policies, as well as inconsistent monitoring and enforcing of access controls.

The challenge is so significant that Brown lists identity and access management as the No. 1 challenge security teams face in a multicloud environment. However, it's not an insurmountable problem, he says.

"If you don't have a formal program, then formalize it. You need a named executive in charge of the program, whether it's you as CISO or someone else. It can't be nobody," says Brown, who is also a faculty member at IANS Research. Implement "strong authentication everywhere and a comprehensive, unified strategy."

CISOs who struggle here should start small, he adds, focusing on privileged users who have higher-level access to systems and data within an organization than standard users and who, as a result of that higher-level access, are more frequently targeted by hackers. ■

Multicloud ROI: Maximizing value and efficiency

IT experts offer advice for calculating ROI in a multicloud environment, including cloud cost management, performance insights, and effective governance to boost business outcomes.

BY JOSH FRUHLINGER

We live in a multicloud age. According to a recent [survey](#) of IT leaders from HostingAdvice.com, 89% of respondents say organizations should never rely on a single cloud provider. Rather they turn to hyperscale providers like Azure AWS and Google as well as smaller providers for cloud services. But that doesn't mean everything is smooth sailing. In fact, 73% struggle with security complexity, and 45% worry about vendor lock-in.

And then there's a problem looming in the background. How do you make sure your multicloud spending is paying off? What is multicloud's return on investment (ROI) and how can you improve it? For those answers, we turned to executives and cloud professionals to find out more about their tools and tricks of the trade.

HOW MULTICLOUD PAYS OFF

Multicloud architecture offers increased resilience, which is one of the clearest

ways they can deliver ROI. "No one wants to say it out loud, but major cloud outages do happen," says Bill Hineline, field CTO at Chronosphere. "When they do, having 10 zones in one provider means nothing. That's when multicloud earns its keep." For organizations with steep per-minute downtime costs, being able to failover across providers can be a financial and reputational lifeline.

But different cloud providers are more than just identical storage and compute clusters, and a multicloud architecture can provide your enterprise with the best tools for specific jobs.

"Each of the clouds are better at certain workloads," says Mike Bilodeau, head of marketing at Baseten. "Depending on your business and what you're building, it can make sense to just use different clouds for different products." Hineline agrees: "You might run analytics in GCP [Google Cloud Platform] while keeping core workloads in AWS."

Jimmie Lee, CEO of JLEE & Associates, adds that “one cloud provider may offer a lower cost for storage, another may offer better pricing for compute or AI transactions. When implemented correctly, these gains significantly help reduce costs.”

Performance is another place where multicloud can shine. Bilodeau says that locating workloads closer to end users across cloud regions can reduce latency and increase responsiveness. “The classic stat from Amazon is that for every 100ms of added latency, they lost 1% of topline revenue,” he says. “Using multicloud to get workloads closer to customers can help to address this.”

The leverage goes beyond architecture. In AI-heavy environments, inference costs can quickly dominate a company’s cloud spend. “We’ve seen firsthand that for many large companies, inference costs overshadow all other cloud costs by an order of magnitude,” reveals Amir Haghihat, CTO of Baseten. “Being multicloud gives them non-trivial leverage in contract negotiations.”

It also increases access to scarce resources like GPUs. “Demand for the latest hardware is so high that getting things like B200s can be difficult,” says Haghihat. “Being multicloud lets you more easily take advantage of the

better price/performance wherever those GPUs are available.”

Multicloud also gives enterprises the flexibility to fine-tune their operating cost structure by splitting workloads between public and private cloud. Joe Locandro, global CIO at Rimini Street, saw this firsthand.

“We were running large predictive models for the energy grid, and that required massive compute power,” explains Locandro. “Migrating to a more sophisticated cloud reduced simulation time from 12 hours to two, which allowed the team to run 300% more simulations per month.”

WHERE MULTICLOUD FALLS SHORT

All those multicloud benefits no doubt sound like a cash-register’s *ka-ching* to tech leaders. But all the experts we spoke to emphasize that getting that ROI depends on execution and the ideal outcomes are often elusive. In practice, many organizations find that multicloud can just as easily introduce friction, redundancy, and diminishing returns.

“Flexibility’s a myth if your team spends half their time context switching,” says Christian Khoury, CEO of EasyAudit. “We saw productivity drop when engineers had to juggle two cloud consoles, two IAM systems, two sets

of docs.” Rather than enabling agility, multiple environments can bog teams down with duplicated tooling and incompatible workflows. And once you’ve managed to deploy your applications, you may find that you take a performance hit.

Even the idea of workload portability — a central pillar of many multicloud strategies — rarely plays out the way companies expect. “One lie that organizations tell themselves is that a multicloud strategy enables applications to move between cloud services as needed,” says Andy Ellis, partner at YL Ventures and former CSO at Akamai.

“The reality is just about the opposite.” In most cases, apps are tightly integrated with provider-specific services — some of which were the specialized features that led you to choose multicloud in the first place. “You can no longer model applications as a ‘rack of servers, just virtual,’” he adds. “Applications are an ecosystem of microservices, many of which you pay for.”

This tight coupling doesn’t just limit portability — it also undercuts negotiating power. “You don’t really have the leverage to threaten to move existing applications easily,” argues Ellis. “Cloud migration projects are arguably more expensive than data center migrations used to be.” Providers know this, and while they have an incentive to retain your business,

the cost and complexity of switching becomes a form of de facto lock-in.

WHY YOU NEED TO JUSTIFY THE ROI OF MULTICLOUD

The right question isn’t whether multicloud saves money — it’s whether it’s worth the cost. That’s how Forrester analyst Tracy Woo frames the issue. “Almost everyone understands that you’re not going to migrate workloads to the cloud just to save money,” she says.

“So the next question is: Is it worth it? And that gets tied into conversations beyond cost management.” Many companies aren’t making these decisions as part of a long-term plan, Woo says. “A lot of the so-called ‘strategy’ was just: everyone else is doing it, we should do it too. That was especially true during the pandemic.”

For companies still building toward scale, multicloud may not even be relevant — yet. Baseten’s Bilodeau notes that “regarding the latency question, people typically do not realize [they have latency problems] until they hit a certain level of scale.” To solve such problems, “most companies aren’t going to go multicloud at the start, because it’s such an investment in infrastructure versus getting product adoption.” But once a company hits a certain threshold — either in traffic, performance

requirements, or customer demand — the pressure to go multicloud grows.

The problem is that this growth rarely unfolds as part of a clean strategic rollout. Often, technical teams default to the tools they know. “We didn’t want multicloud,” says EasyAudit’s Khoury. “We ended up with it because different teams picked what they knew. Devs went GCP. Ops went AWS. Then legal said we needed a private cloud option for one enterprise deal. Welcome to vendor hell.”

Even mature enterprises often inherit multicloud complexity unintentionally. As YL Ventures’ Ellis puts it, “Mergers and acquisitions bring cloud environments with them, and you accumulate cloud services at a rate commensurate with your growth. Development teams may bring expertise in different cloud technologies, and they’ll build with what they know,” he adds. “And partnerships you’ve had in other areas of your business may have driven discounted rates from your partners to adopt their cloud services.”

Sometimes, the decision isn’t even internal. Baseten’s Bilodeau explains that for vendors selling infrastructure software, customer preferences can dictate cloud choices: “Some companies are ‘AWS’ or ‘GCP’ shops. If your software doesn’t run in those clouds, it can be a dealbreaker.”

Woo agrees: “A lot of people don’t have a choice. There may have been

political reasons, or a rogue engineer, or a partner demanding it — suddenly, you’re supporting what everyone else wants.”

The result is an architecture cobbled together from one-off decisions, rather than a cohesive plan. “Often, we find that our clients are using numerous different cloud services and offerings,” says JLEE & Associates’ Lee. “These were frequently what was architected or recommended to them, without a more comprehensive and multi-year strategy.”

To navigate this complexity, commercial-minded IT leaders need to step up. “Typically, IT departments view cloud providers from a technical and risk lens,” explains Rimini Street’s Locandro. “It’s up to the commercially savvy CIO to put in place good metrics, monitoring, and awareness of costs to really understand the value.”

TIPS FOR IMPROVING YOUR MULTICLOUD ROI: STRATEGY, STRUCTURE, AND SKILL

Multicloud can deliver meaningful returns — but only if you’re [intentional about how you use it](#). The benefits don’t materialize just because you have accounts on multiple platforms.

“When not implemented correctly, multicloud product costs can spiral out of control,” warns JLEE & Associates’ Lee. And Rimini Street’s Locandro adds that

for many organizations, multicloud TCO, including administration, monitoring, and [upskilling](#) workers, “is adding up to much more than initial expectations and vendor promise.”

Without governance, observability, and architectural discipline, you risk higher costs, team confusion, and missed opportunities. Here are the steps the experts we spoke to recommend to make multicloud worth the investment.

Only use clouds you really need. This one might seem obvious, but it’s a piece of advice often neglected in practice. “Too many leaders see multicloud as a status symbol instead of a strategy,” says Drew Firment, chief cloud strategist at Pluralsight. “It’s not about having ‘more clouds’ — it’s about having the right clouds for the right reasons.”

At EasyAudit, Khoury’s team asked a blunt question: “What’s the actual value of each cloud in production?” Anything that wasn’t supporting a core service or compliance requirement was flagged. “We weren’t chasing theoretical redundancy — we were trying to kill zombie infra and get one bill under control before explaining three,” he says.

Cloud costs and observability are tied together. “Many teams still treat cost as a line item, not a governance practice,” says

Chronosphere’s Hinline. He adds that the same goes for observability. “Teams that do multicloud well have treated both as first-class citizens. That means tight tagging discipline, clear ownership, and intentional instrumentation. If your FinOps team can’t trace a dollar of spend back to a service and a team, you’re flying blind.”

YL Ventures’ Ellis agrees: “Without visibility into how cloud services are being used, it can be an exercise in driving a bulldozer through a china shop.” Instead of clamping down with heavyweight processes, he suggests “white glove services from the beginning” to onboard teams into cost-efficient environments.

Review your architecture to root out inefficiency. Ellis recommends basic hygiene like identifying duplicate accounts with the same provider. Doing so “can give you better pricing as you purchase in volume,” he argues.

Even simple practices can reduce waste. Rimini Street’s Locandro says he’s had “developers spinning up test and dev environments and then forgetting to shut down the environment when they had finished. You need to turn off environments when finished, rather than leave the cloud tap continuously running.”

Measure what matters: Productivity and outcomes. “Multicloud investments

need to be measured by meaningful productivity gains and business outcomes,” says Firment. “If you’re not achieving faster deployments and improved customer value, then you’re just racking up cloud bills with a fancier name.”

Upskill your team — and guide them to the finish line. “Flexibility only turns into faster delivery if your people are trained to navigate the differences,” adds Firment. But you shouldn’t expect every developer to master every cloud. “The goal is to build once, run anywhere, and deliver fast.”

That requires architecture that supports smart decisions. As Ellis notes, “Developers will often head for the lowest friction path, so the more you can make it easy for them to adopt the platforms that save you the most money overall, the better off you’re going to be.”

MULTICLOUD COMPLEXITY DEMANDS A SMART ROLLOUT

If multicloud once seemed like a technical upgrade — or even a badge of sophistication — it now demands something deeper: a strategic lens that connects cloud architecture to business outcomes. That evolution is happening in parallel with the changing role of IT itself.

“I think the context behind [the ROI multicloud] question is something that a lot of teams are being pushed to,”

says Forrester’s Woo. “And the reason they’re being pushed is because IT used to just be IT — you had a desktop, you had some applications loaded on it. Now IT strategy has really become this enabling backbone for business or digital transformation,” she adds. “It’s started to level up higher and higher, and that’s why you have cloud really transforming the way people do work. The bigger question that looms beyond that: What’s the ROI for multicloud?”

For organizations that treat multicloud as a checkbox — or let it sprawl without structure — the answer may well be “not much.” But for those that align cloud architecture with business priorities, cost discipline, performance targets, and a realistic assessment of team capacity, multicloud can be the foundation for long-term agility and resilience, and provide a return on the initial necessary investment and then some. ■

How to excel in multicloud: The new checklist

Here's what experts are saying about the challenges and opportunities in multiple cloud operations.

BY ISAAC SACOLICK

Several years ago, I wrote a [multicloud readiness checklist](#) and discussed the [advantages of hybrid multicloud](#). Today, the vast majority of medium-sized businesses and large enterprises diversify with multiple hyperscalers, operate private clouds, deploy to edge infrastructure, and manage data across a sprawl of SaaS, low-code, and other platform services.

The question today is not whether to support multicloud operations but how to excel at it. IT operations must deliver business value through agility, speed, efficiencies, cost savings, and risk reduction. Given these challenges, I asked experts how they and their teams are excelling in multicloud operations. The following checklist distills their best practices.

COMMUNICATE WHERE MULTICLOUD PROVIDES BUSINESS ADVANTAGES

There are many reasons why businesses operate in multiple clouds. Understanding

past decisions is important, but it is even more critical to communicate a vision statement of objectives and how new investments drive business advantages.

“The question isn’t whether companies are ready for multicloud; it’s whether they’re ready to compete against those already ahead because of it,” says Jon Alexander, SVP of product in cloud technology at Akamai. “AI is accelerating this divide, automating configurations and predicting infrastructure needs in ways that give multicloud-native companies an increasing advantage. What sets them apart is building on infrastructure that moves with the business, not against it.”

When communicating business advantages, provide metrics that quantify business value and create a narrative on the competitive impacts. Look for inspiration in the news, especially when strategic shifts in technical capabilities or a vendor’s business strategy help explain IT’s objectives.

“The Broadcom-VMware fallout shows what happens when critical infrastructure

is locked into a single ecosystem,” argues Sharad Kumar, entrepreneur and investor. “True multicloud readiness means designing for portability — not just for performance, but to protect against pricing shocks, licensing changes, and ecosystem consolidation.”

Other aspects of the vision statement and IT’s cloud operations plan should focus on business and compliance requirements. “Multicloud is a response to constraints, such as data residency, mergers and acquisitions, or vendor lock-in avoidance,” says Jimmy Mesta, co-founder and CTO at RAD Security. “Technically, multicloud makes sense if your workloads demand it, for example, GPU-optimized regions, proximity to partners, or specific service availability.”

Checklist recommendations:

- Develop and update a CloudOps vision statement, services roadmap, and operations review at least twice a year.
- Establish a cloud center of excellence to define best practices and establish governance.

ALIGN MULTICLOUD OPERATIONS WITH GENAI OBJECTIVES

Most enterprise cloud strategies were developed before the generative AI era. A cornerstone of today’s multicloud

strategy should focus on the enterprise’s objectives in [generating business value from genAI](#) and updated [digital transformation strategies](#).

Nandakumar Sivaraman, SVP and chief architect of enterprise data at Bridgenext, notes that “AI/ML introduces new drivers for multicloud adoption.” It goes “beyond traditional resilience or lock-in avoidance to strategic access,” he says, “by enabling organizations to tap into specialized AI services, diverse foundation models, and region-specific data capabilities.”

“Every aspiring IT leader must consider how they will harness new technology, especially genAI, to drive innovation and create lasting impact within their organization,” says Michael Ameling, chief product officer at SAP Business Technology Platform and member of the extended board. “Overarching business success comes from leveraging emerging tools in the IT space to unlock value, fuel growth, and bolster efficiency.”

Checklist recommendations:

- Catalog and track genAI models from cloud providers such as AWS Bedrock, Azure OpenAI, and Google Vertex AI.
- Review how AI agents from enterprise SaaS platform providers use zero ETL and other data integration

strategies with hyperscalers and private cloud technologies.

SECURE HIGH-PERFORMING CLOUD-TO-CLOUD NETWORKS

Some organizations may have stumbled into multicloud architectures with minimal architecture planning through mergers and acquisitions. Others opted for innovation, speed, or flexibility when defining cloud architectures rather than looking holistically at operations, performance, and security. One place to address gaps is in understanding cloud-to-cloud integrations and reviewing options to optimize networking.

“Most organizations use multiclouds, yet the ability to seamlessly and securely interconnect these environments remains a significant challenge,” argues Bratin Saha, chief product and technology officer at DigitalOcean. “Cloud providers are increasingly offering native interconnect solutions to simplify secure, high-performance connectivity across multicloud environments, enabling customers to establish private connections across cloud providers or on-premise data centers.” By bypassing the public Internet, such solutions “enhance security, reduce latency, and optimize multicloud and hybrid-cloud networking,” he adds.

Checklist recommendations:

- Evaluate dedicated cloud interconnect options such as AWS Direct Connect, Azure ExpressRoute, Google Cloud Interconnect, as well as partner colocation facilities and offerings from network service providers.
- Design redundant network paths, end-to-end encryption, and network segmentation based on zero-trust principles to improve resiliency.

UNIFY IDENTITY MANAGEMENT AND SECURITY ACROSS CLOUDS

Provisioning infrastructure and locking down access is far simpler for businesses that standardize on one cloud and perform little application development work. However, multicloud enterprises have DevOps teams modernizing applications, data science teams developing AI models, and business teams looking for integrated workflows. Centralizing identity, entitlements, and security monitoring is essential for organizations to avoid risks and to secure the full life cycle, from development through production.

“Without federated identity, unified telemetry, and real-time policy enforcement, you’re flying blind,” says Mesta of RAD Security. “Architect for observability across cloud lines, including network, data, and identity, and automate

least privilege across providers. Make sure your detection, incident response, and compliance workflows don't break when an asset lives in the wrong cloud."

Checklist recommendations:

- Centralize identity and access management across clouds.
- Establish consistent security monitoring, logging, and threat detection across platforms.

OPTIMIZE WORK PLACEMENT FOR PERFORMANCE, COST, AND COMPLIANCE

As of this writing, AWS has over 850 EC2 instance types. Azure has six types and 19 families, and Google Cloud has thousands of combinations of machine families, series, and types. Then, there are dedicated versus reserved instances, serverless computing options, and edge deployments to consider. These are all choices architects and IT engineers must consider when deploying applications and must optimize for performance, cost, compliance, and other considerations.

"A key driver of this evolution to hybrid and multicloud environments is the rise of edge functions, which enable code to run closer to end users via content delivery networks," says Avishai Sharlin, division president of product and network at Amdocs. "Edge functions reduce

latency and support real-time, location-based updates. For industries such as IoT, telecommunications, and media where low-latency performance is critical, these capabilities will foster faster innovation and more responsive services."

Checklist recommendations:

- Develop work placement selection criteria around performance, cost, compliance, resilience, and innovation drivers.
- Review where workload portability is required or advantageous and consider containerization, cloud-agnostic frameworks, and other abstraction layers.

EVOLVE A DATA GOVERNANCE STRATEGY FOR GENAI OPPORTUNITIES AND RISKS

AI agents and private LLMs are forcing technology leaders to develop AI governance plans and evolve their data strategies. Multicloud enterprises need to create policies, integrations, and operations to ensure critical data is labeled, secured, and accessible to enable the development and deployment of AI capabilities.

"To demonstrate the effectiveness of data governance, security, and operations, track key performance indicators like the percentage of data covered by access policies, the

reduction in data breach incidents, and the improvement in data accessibility for authorized users,” urges Bart Koek, EMEA field CTO at Immuta. “These metrics illustrate business value by showcasing reduced risk, improved compliance, and enhanced data-driven decision-making, justifying further investment and fostering a data-centric culture.”

As the business demand for AI capabilities grows, organizations operating in multiple clouds should consider [AI governance platforms](#), [data fabrics](#), and [data security posture management](#).

“Establishing an offensive security strategy through data and AI governance starts with real-time, continuous IT visibility,” says Tim Morris, chief security advisor at Tanium. “Enterprises should prioritize visibility into not just how these IT services are performing but also how and why they’re being used and who is using them through contextual data and metadata. This will give organizations a clearer view into the usage, effectiveness, and profitability of tools, leading to cost savings and investment in other technologies.”

Checklist recommendations:

- Ensure backup and disaster recovery strategies span across multicloud environments.

- Classify data by sensitivity, residency, retention, and other confidentiality and privacy requirements.

ACCELERATE AGILE ARCHITECTURE PRACTICES

Consider the sizable gap between the hyperscaler infrastructure options and the technical debt and backlog of app modernizations facing many organizations. IT should adopt agile solution architecture practices and leverage [genAI in app modernizations](#) to avoid issues with lift and shift migrations.

“While enterprises rapidly adopt AI for development, operational management lags across SDLC, DevOps, ITSM, and IT operations,” says Vikram Murali, VP of application modernization and IT automation at IBM. “Teams struggle to manage complex applications with outdated tools, creating debt that undermines AI initiatives. GenAI can enhance automation and data interpretation, helping teams shift from reactive to predictive operations and reducing technical debt.”

Checklist recommendations:

- Invest in automated and [continuous testing](#) on mission-critical applications and others with [continuous deployment](#).
- Create [observability standards](#), [feature flagging](#) capabilities, and [canary release](#)

strategies when migrating to cloud-native architectures.

ESTABLISH FINOPS AS A CORE COMPETENCY

Multicloud architectures have an inherent cost in procuring technologies and developing operations that span multiple networks, tools, and service providers. Multicloud strategies require FinOps practices to track costs and enable better decisions around performance tradeoffs.

“Integrating FinOps practices early in development can prevent cost debt accumulation,” reveals Ananth Kumar, leadership at ManageEngine. “To keep workload costs accountable, use right-sized environments, automated tagging, and usage alerts during the development and testing phases. This shift-left methodology guarantees scalable choices without causing unprecedented cloud expenditures in the future.”

Checklist recommendations:

- Forecast and measure each application’s typical versus peak usage periods to optimize infrastructure and automate autoscaling.
- Monitor resources for inactivity and automate ramp-down to save costs and reduce carbon emissions.

DRIVE TRANSFORMATION IN ITOPS WITH AIOPS

AIOps is a critical capability in multicloud environments as it can correlate alerts and improve IT’s time to resolve incidents. Today’s applications are increasingly complex, with transactions that span many APIs, microservices, and SaaS endpoints.

The increased complexity makes managing service-level objectives challenging for SREs. Monitoring services and resolving incidents will become more important as organizations deploy AI agents and agents become integrated with standards like the Model Context Protocol.

As agentic AI continues to evolve, “AIOps platforms will become increasingly autonomous, taking action rather than purely advising operators,” says Jonathan LaCour, CTO at Mission. “With the reduced operational load, IT engineers will be able to spend more time leveraging their most valuable capabilities — critical thinking, problem solving, and automation. By working in collaboration with AI, IT departments will be able to rapidly accelerate automation, including threat detection, cloud management, and day-to-day operational activities.”

Checklist recommendations:

- Deploy centralized monitoring of workloads, AIOps capabilities, and

automation with platforms that work across cloud providers.

- Continuously improve the robustness of CI/CD pipelines, [infrastructure as code](#), and [container orchestration](#), especially on workloads hosted across multiple clouds.

ESTABLISH A LEARNING CULTURE THAT CHALLENGES ASSUMPTIONS

Many IT professionals will struggle to keep up with the rapid changes in cloud and AI capabilities, along with security and regulatory constraints. So, even though lifelong learning appears last on this checklist, it may be the most important requirement for organizations committed to digital transformation as a core competency.

“In order to be most effective with genAI capabilities, professionals working in operations roles must develop a mix of technical and analytical AI skills, including learning the basics of AI, machine learning, and deep learning,” says Anant Adya, EVP at Infosys Cobalt. “Organizations must continue to upskill their employees and provide a plethora of internal resources for ops professionals to understand better how AI can enhance their work.”

Checklist recommendations:

- Foster a learning culture through skill development, learning experiences,

workshops, labs, hackathons, certifications, and gamification.

- Promote cross-functional collaboration between development, security, ITOps, and FinOps.

THE NEW MULTICLOUD CHECKLIST

Multicloud has its advantages and challenges. IT leaders should take a proactive approach to defining IT’s strategy for delivering business impacts and standardizing on an approach that simplifies operations. The complete “Excelling in multicloud” checklist is a good place to start.

1. Develop and update a CloudOps vision statement, services roadmap, and operations review at least twice a year.
2. Establish a cloud center of excellence to define best practices and establish governance.
3. Catalog and track genAI models from cloud providers such as AWS Bedrock, Azure OpenAI, and Google Vertex AI.
4. Review how AI agents from enterprise SaaS platform providers use zero ETL and other data integration strategies with hyperscalers and private cloud technologies.
5. Evaluate dedicated cloud interconnect options such as AWS Direct Connect, Azure ExpressRoute, Google Cloud

Interconnect, as well as partner colocation facilities and offerings from network service providers.

6. Design redundant network paths, end-to-end encryption, and network segmentation based on zero-trust principles to improve resiliency.
7. Centralize identity and access management across clouds.
8. Establish consistent security monitoring, logging, and threat detection across platforms.
9. Develop work placement selection criteria around performance, cost, compliance, resilience, and innovation drivers.
10. Review where workload portability is required or advantageous and consider containerization, cloud-agnostic frameworks, and other abstraction layers.
11. Ensure backup and disaster recovery strategies span across multicloud environments.
12. Classify data by sensitivity, residency, retention, and other confidentiality and privacy requirements.
13. Create observability standards, feature flagging capabilities, and canary release strategies when migrating to cloud-native architectures.
14. Monitor resources for inactivity and automate ramp-down to save costs and reduce carbon emissions.
15. Invest in automated and continuous testing on mission-critical applications and others with continuous deployment.
16. Forecast and measure each application's typical versus peak usage periods to optimize infrastructure and automate autoscaling.
17. Deploy centralized monitoring of workloads, AIOps capabilities, and automation with platforms that work across cloud providers.
18. Continuously improve the robustness of CI/CD pipelines, infrastructure as code, and container orchestration, especially on workloads hosted across multiple clouds.
19. Promote cross-functional collaboration between development, security, ITOps, and FinOps.
20. Foster a learning culture through skill development, learning experiences, workshops, labs, hackathons, certifications, and gamification. ■