Uncovering the Advantages, Challenges, and Risks of a Successful Multi-Cloud Strategy

Federal agencies are largely taking advantage of the variety of cloud services available to them to support their missions, adopting a multi-cloud strategy. But to successfully attain the benefits of multi-cloud, agencies need to pay attention to three critical areas: performance, visibility and security. By prioritizing these three things, while avoiding any number of pitfalls that may introduce risk or complexity, agencies can get the most out of their cloud services.

"I think with a lot of the granularity and the capability that a Secure Access Service Edge provider gives agencies, it can quickly seem complex," said Mark Mitchell, enterprise security architect at Netskope, and former federal enterprise security architect at the Office of the Comptroller of the Currency. "But I think those are three areas that when you're dealing with cloud services, you can really bucketize everything into those three areas because they're all interdependent and necessary for really being able to focus more on mission goals and not get caught up in a lot of the maintenance of cloud services and security of cloud services."

Avoiding complexity

Multi-cloud environments require careful management to address challenges in what Mitchell calls horizontal and vertical cloud stacks. In a horizontal setup, agencies often use multiple services across different cloud platforms, including software-as-a-service providers, which can lead to difficulties in controlling access and managing sensitive data. The main issue arises when services interact in ways that aren't immediately visible, creating gaps in security and performance.

Visibility is important to effectively manage these activities and create a true zero trust architecture, ensuring that only authorized actions are taken based on specific user behavior.

On the other hand, vertical cloud stacks — where an agency's multi-cloud architecture contains providers that build their services on top of other cloud vendors' infrastructure — challenges can arise with performance, security and control. With multiple layers involved, agencies lose direct visibility and oversight, which can introduce performance impacts and security gaps. For example, when a SASE vendor uses public cloud services for transport, it adds complexity and potential vulnerabilities that are harder to manage.

> Successful multi-cloud strategies all focus on performance, visibility and security. But both "vertical" and "horizontal" cloud stacks have their own potential pitfalls.

"It's important to have complete visibility, and then from that understand your risk. Because there's a lot of risk that exists that's not being addressed and usually is pretty easy to address," Mitchell said. "Then being able to layer in either the threat or data protection policies that you're then able to control access or protect data movement or maybe shut down data movement because of some threat that's been seen."

Meanwhile, performance is integral to any security architecture, particularly when dealing with cloud services. A slow system compromises usability, making security tools ineffective if they hinder the user experience. For federal agencies, it is essential to find a balance between security and performance.

How agencies can address these challenges and meet compliance mandates

Secure Access Service Edge solutions, like Netskope's platform, allow agencies to monitor and analyze all activities within their cloud environment, providing both real-time threat detection and data protection through full packet inspection. This true instance awareness enables agencies to implement security policies based on the specific context of user behavior, data sensitivity and the actions being performed.

Data protection also becomes more effective when agencies can identify anomalous behavior. For example, if an administrator's account is accessed from an unusual location or an unexpected device, the system can automatically adjust security settings or block specific activities to mitigate risk.

"I always call it compliance debt, and it's just the expense of maintaining and managing resources just to focus on typically a paper exercise of keeping track of compliance — baseline scans on cloud services. The fact that we automate that and can provide ways of sending these dashboards out to those that are responsible for mapping them, also reduces some of the burden from a resource and expense perspective on customers."

"When I talk about true instance awareness, that's the kind of response that you would expect for zero trust architecture implementation," Mitchell said. "These are the things that enable you to react in real time to a threat or an anomaly. And it's only available through being able to decode and understand activities in instances."

Meanwhile, Netskope's new edge network prioritizes performance while maintaining robust security. The network allows for faster response times and eliminates the need to rely on third-party infrastructure. By controlling the network's egress points and peering arrangements directly with cloud providers like Microsoft, Netskope ensures optimal performance while securing sensitive data.

Compliance with mandates

Agencies have to comply with numerous mandates cybersecurity mandates, including directives from the Cybersecurity and Infrastructure Security Agency and memorandums from the Office of Management and Budget. Netskope's solutions help agencies meet these compliance standards by automating security scans and mapping existing security measures to federal mandates, significantly reducing the administrative burden.

"I always call it compliance debt, and it's just the expense of maintaining and managing resources just to focus on typically a paper exercise of keeping track of compliance — baseline scans on cloud services," Mitchell said. "The fact that we automate that and can provide ways of sending these dashboards out to those that are responsible for mapping them, also reduces some of the burden from a resource and expense perspective on customers."

netskope

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust Netskope to reduce risk and gain full visibility and control over cloud, SaaS, web, and private application activity—providing security and accelerating performance without trade-offs. Learn more at www.netskope.com/federal.

©2025 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized "N" logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners. 06/25 OS-902-2