



SURVEY:

Federal IT embraces cloud for network management

While federal technology leaders still have some reservations about the cloud, they are moving swiftly to shed their legacy systems in favor of a more centralized and modernized approach. They're shifting not just applications but also infrastructure, including network management, into the cloud.

"There's still a preference for on-prem, but they are definitely moving in this direction," said Barry Kroneberger, Director of Federal Systems Engineering at Aruba, a Hewlett Packard Enterprise company.

In a recent survey of dozens of federal IT executives, Aruba found a distinct trend toward cloud adoption.

Especially intriguing is the willingness on the part of feds to leverage cloud in support of mission-critical applications, as well as their interest in utilizing cloud to meet their infrastructure needs.

Overall, the data show a clear trend toward accelerating cloud adoption.

Building momentum

Among survey respondents, only 15 percent said their entire IT environment is on-prem today. Hybrid approaches dominate: Some 39 percent have some cloud and are mostly on-prem, while 33 percent use some on-prem and mostly cloud. Twelve percent are all cloud.

Even more telling are their responses when asked where their IT environment will be just two years from now. Thirty-nine percent said they would be mostly cloud by then, and the all-cloud group rises to 17 percent.

"Government agencies want the benefits that come with cloud — the scalability, the speed, the ability to centralize their fragmented processes. They are finding more and more ways to support their mission requirements in a cloud environment," Kroneberger said.

Infrastructure use cases

The survey also revealed a shift in the types of use cases that government is bringing to the cloud. Where initial implementations focused on user-facing applications, cloud today increasingly is helping government to meet its IT infrastructure needs.

Asked what they might support with a cloud implementation, 34 percent pointed to mobile device management and 29

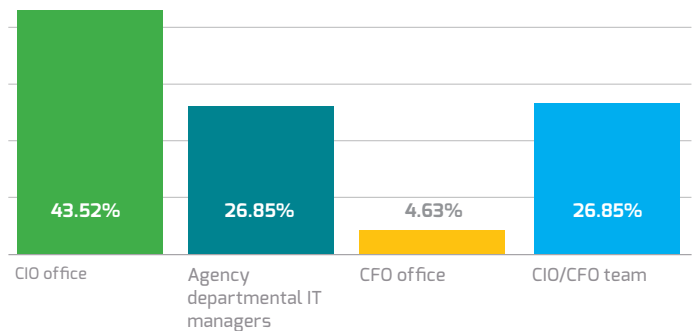
percent indicated firewall configurations. Threat proofing and device proofing also ranked high. Especially noteworthy: Fully 41 percent of respondents said they would turn to cloud for network management monitoring.

"As people are moving their infrastructure solutions to the cloud, network management is key to that," Kroneberger said.

By shifting network management out of the on-prem environment, IT leaders have the opportunity to swap out piecemeal solutions in favor of a more consolidated approach to network management.

Who in your organization is the key decision maker when it comes to adoption and use of cloud networking?

Answered: 108 Skipped: 0



"Today they might have one solution for routers, a different solution for firewalls. They may come from a single vendor or from multiple vendors, and IT doesn't have the tools that allow for this to be managed from a single pane of glass, under a single infrastructure," Kroneberger said.

With a cloud-based approach, it's possible to consolidate those management operations. Beyond driving much-needed efficiencies, this strategy also empowers IT leaders with deeper analytical insights.

"The cloud gives you the visibility, the analytics, the configuration — all the troubleshooting tools you need," Kroneberger said.

Overcoming obstacles

Even as they move toward wider and deeper cloud adoption, IT leaders still express concerns.

Fully 84 percent of respondents said security remains a barrier to cloud network adoption. Thirty percent worry about performance and 44 percent are concerned about reliability. Over a third (32 percent) cite vendor lock-in as a barrier and nearly half (45 percent) point to Return on Investment (ROI) as a hurdle.

A number of trends are emerging to offset these concerns. In terms of security, the topmost worry among IT leaders, the increasing implementation of the government's FedRAMP criteria is helping to ease the fear.

"Government agencies can point to FedRAMP's comprehensive list of security requirements for cloud service providers, and they can feel confident in that," Kroneberger said. "As more and more providers adopt FedRAMP and get their solutions authorized, we see that fear continue to recede."

Aruba announced recently that its Aruba Central cloud-native network management and analytics platform has achieved a formal "Authorized" designation from FedRAMP. That makes it the first AI-powered solution for unified WLAN, switching, VPN, and WAN cloud infrastructure to achieve the FedRAMP designation.

In terms of performance and reliability, the same analytics and monitoring tools that help drive operational efficiency in the cloud can also serve to lessen those concerns. On the whole, cloud and hybrid solutions are at least as robust and reliable as on-prem solutions and, what's more, they come with the tools IT leaders need to monitor and validate those performance levels.

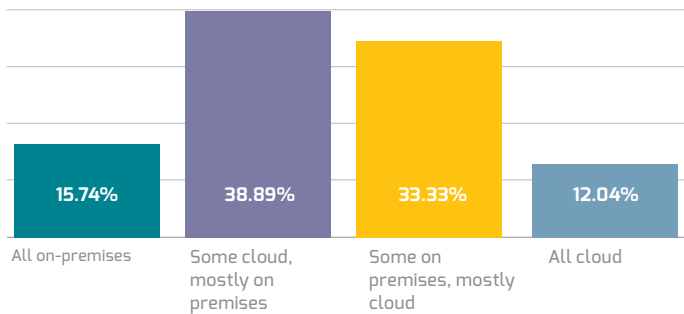
When it comes to ROI, government agencies may do well to broaden their vision of what constitutes a meaningful return. Certainly some upfront cost saving is possible: Continuous as-a-service upgraders (Change to upgrades) in cloud reduce expenses related to the ongoing refresh of on-prem hardware. But the real return on cloud goes even deeper.

"We should be looking to define ROI around the business drivers, the efficiency that cloud brings to the mission set," Kroneberger said. "Just on the IT side, you gain so much in terms of the effort spent on configuration, management, day-to-day operations and troubleshooting. All that is simplified through the cloud, which in turn improves your overall ability to meet the mission more efficiently and effectively. That's the true ROI of a cloud investment."

Respondents seem to recognize the value here. While 56 percent point to resource savings as a benefit of cloud and

Which statement below best describes your organization's current total IT (Information Technology) environment (infrastructure, applications, data analytics, etc.)?

Answered: 108 Skipped: 0



62 percent cite cost savings, over half (52 percent) recognize simplicity of deployment as a major win, and 61 percent see the value of having integrated services. These key mission drivers help to demonstrate the ongoing ROI of a cloud investment.

An even more potent marker of federal IT leaders' embrace of the cloud: 70 percent of respondents said they are using cloud for mission critical applications. That's a strong indicator of how far feds have come in their embrace of cloud capabilities.

Aruba has the tools to empower federal agencies as they position themselves to leverage cloud in support of their networking needs.

"We have built our products to take advantage of the cloud environment — the simplicity, the potential for integration," Kroneberger said.

Aruba works in partnership with existing on-prem solutions, which helps to alleviate those fears about vendor lock-in. With its FedRAMP "Authorized" status, Aruba Central offers the high level of security assurance federal IT leaders need as they migrate their environments to a more efficient, scalable, and flexible future in the cloud.

For those on the journey, it makes sense to take a measured approach. While the cloud has many potential benefits, especially in support of network management, it's important for IT teams to carefully evaluate the mission need, the available skill sets, and the overall organizational readiness. Many will find that a hybrid approach eases the transition.

"First you need to find a solution that you can feel confident about from a security standpoint," Kroneberger said. "From there, hybrid solutions can be an important component, a way of ensuring that you continue to meet the mission effectively, even as you are transitioning to that new environment."