Securing the Future of Government

Misconceptions about the cloud are hampering adoption

As agencies strive to modernize their IT infrastructures, many are turning to cloud technologies to get the job done. Modernizing infrastructure is not only an important priority detailed in the President's Management Agenda, but it is considered the best path toward genuine digital transformation, which will allow agencies to take advantage of digital technologies from connected devices and remote collaboration platforms to automation and artificial intelligence.

According to a recent survey conducted by FCW and sponsored by CrowdStrike and Amazon Web Services, IT modernization was the top reason agencies chose to embrace the cloud. Other drivers included meeting federal requirements and standards and easier data access. Cloud computing also helps agencies reduce costs, provide more responsive service to citizens, and increase flexibility and agility to meet changing mission requirements.

Yet about one-quarter of respondents indicated that they are not making much use of cloud today, largely because of security concerns. That's a fairly high number, considering both the benefits of cloud and directives from government.

While security concerns are very real, there are also misconceptions about cloud security. These misconceptions shouldn't deter agencies from moving forward with cloud projects, said James Yeager, vice president of Public Sector at CrowdStrike.

"The path to digital transformation must come with a security-first mentality. No exceptions," he said. "But misconceptions about the cloud are hampering adoption, and they shouldn't be. There are too many people who overthink the cloud, and that can cripple organizations as they look to innovate. The cloud is an enabler and a vehicle for transformation – security cannot be sacrificed in this journey."

Security is front of mind

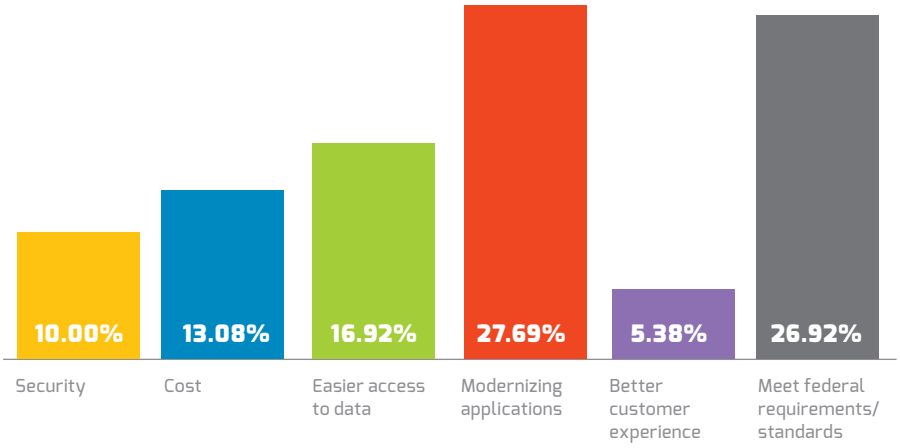
Agencies that have embraced the cloud are doing what they can to remain secure. The majority are relying on the NIST Risk Framework or FedRAMP. The rigorous FedRAMP process certifies cloud services and products for security, while the NIST Risk Framework sets forth a series of information security policies and standards to help workloads remain secure.

"Let's give credit where credit is due," Yeager said. "The federal government has done a tremendous job with these standards. They are so good that we're seeing more and more state, local and higher education organizations looking to these standards to help satisfy some of their own requirements when migrating to the cloud."

But even with these measures, agencies are still concerned about cloud security. One issue that came up over and over again in the survey concerned security in the era of increased remote work. Concerns typically revolve around visibility and control, securing the remote worker edge, identifying new IT patterns, and shoring up network connections. With remote work destined to continue long after the current pandemic, this may be an ongoing concern.

What were the reasons for moving to the cloud?

Answered: 130 Skipped: 10

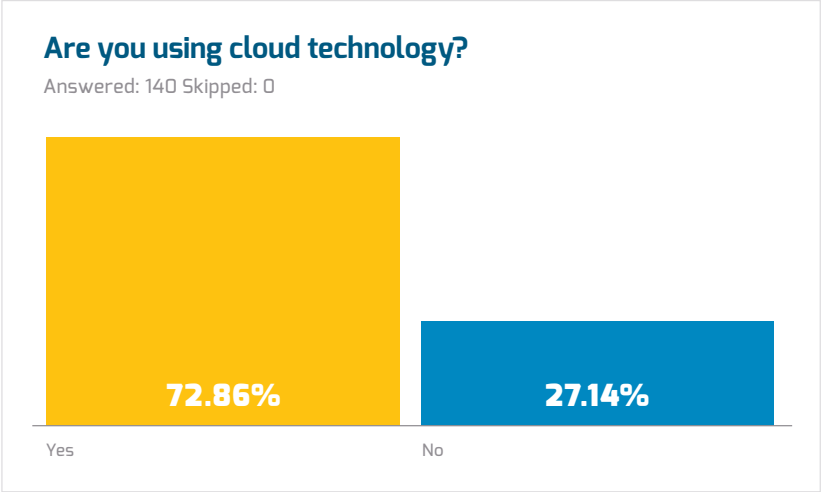


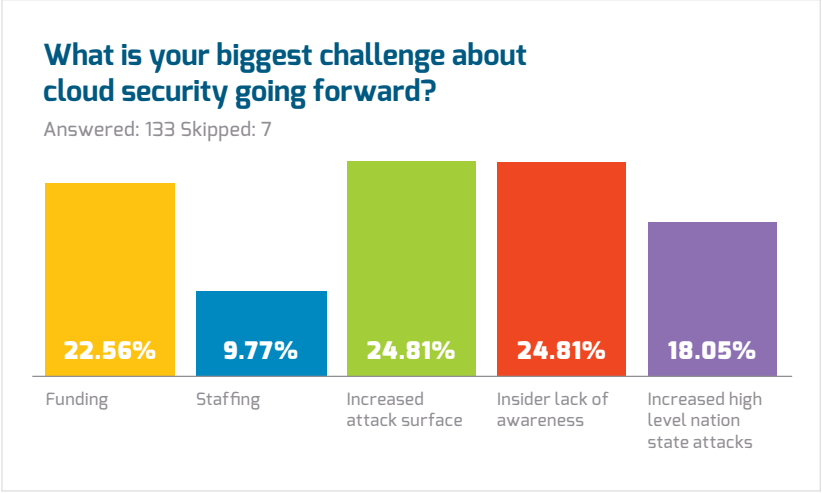
PRODUCED BY: FCW
SPONSORED BY: CROWDSTRIKE aws

These concerns are valid, Yeager said. "Bad actors are always looking for moments of crisis such as today's forced work-from-home scenario," he said. "They consider these moments to be opportunities, because organizations are highly distressed, disorganized, or in some a state of transition."

Respondents also voiced concerns about the increased attack surface of the cloud, along with insider lack of awareness. With a greater attack surface, hackers have more opportunities to penetrate perimeters and exploit vulnerabilities.

"The attack surface does expand when you go to the cloud," Yeager noted. "There is so much peripheral technology in the cloud that interacts with virtual assets, and all of it needs to be identified, monitored, and secured."





Cloud security issues are surmountable

"These are very real issues, but they shouldn't stop agencies from embracing the cloud", Yeager said. "It starts with having a plan—one that is flexible and agile enough to change as external and environmental conditions change. It's also important to have the right tools to fight back—tools that can meet and exceed federal standards and requirements."

Any approach to cloud security also should incorporate Zero Trust—a security concept that requires all users, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validating security configuration and posture, before being granted or keeping access to applications and data.

"The perimeter has effectively dissolved, and this creates a considerable amount of potential risk," Yeager explained. "It's essential that organizations know exactly who is accessing their infrastructure, where they are accessing the network from, what systems they are using, and what mechanisms they are leveraging to gain access to the network and applications. And then once you have that information, validating with assurance that these assets and the conditions of the IT environment are what they say they are and can be trusted."

One of the issues is that many people don't understand exactly what Zero Trust is. It's not a technology; it's an outcome you're looking to achieve. It can be accomplished in many ways, with many different technologies from multiple vendors. But it's critical.

When thinking about cloud security, don't forget about the endpoints. This peripheral technology—not just desktops, laptops, and servers but sensors, workloads, containers, and mobile devices—are important entry points to the cloud. The rule of thumb is this: if you have technology in your environment that interacts with the cloud, it must be secured. Endpoint security can be delivered as an endpoint detection and response solution, which helps ensure comprehensive detection and prioritization of advanced threats on all endpoints.

By adopting a proactive approach and the right technologies, the cloud can be a very secure place. That allows agencies to drive cost and complexity out of the environment while maintaining full cyber-resiliency.

"The cloud is not just a destination; it's a vehicle to help drive innovation and to help empower digital transformation," Yeager said. "That's precisely how we beat the adversary: we out-innovate them. Develop speed and efficiency, because these are the characteristics they covet and harness as key ingredients for success to their campaigns."