Agencies Secure Newly-Deployed Cloud Technologies

A new survey by Fortinet and Amazon Web Services found that much like in the private sector, the work-from-home (WFH) trend during the pandemic encouraged federal agencies to adopt cloud technologies—and the vast majority of agencies have growing concerns about securing cloud data.

A full 77% of the government IT professionals surveyed said they are concerned about securing the cloud and 82% say that their future strategies will include a comprehensive plan that looks across the agency's operations to evolve and manage security.

Nearly 83% also said they want either a private or hybrid cloud, indicating that federal agencies want the ease of use and cost savings of the cloud, but don't want their data in the public cloud.

"With the public cloud, the organization gets placed in a rack of servers in a room and they don't always know who's with them," said Jim Richberg, Fortinet's public sector field CISO and vice president of information security. "Even for non-classified data, most federal agencies want to put it in a cloud where at least they know about how the access gets managed and configured."

Marty Hess, AWS alliance lead for cloud security at Fortinet, said that the proposed Joint Enterprise Defense Infrastructure (JEDI) project for DOD was a good example of where many agencies may head.

"AWS has a GovCloud designed for the public sector," and is expanding capabilities in other countries such as Australia and Bahrain, said Hess. "Agencies need to understand that under the AWS shared responsibility model, the contracting agencies are responsible for securing the data."

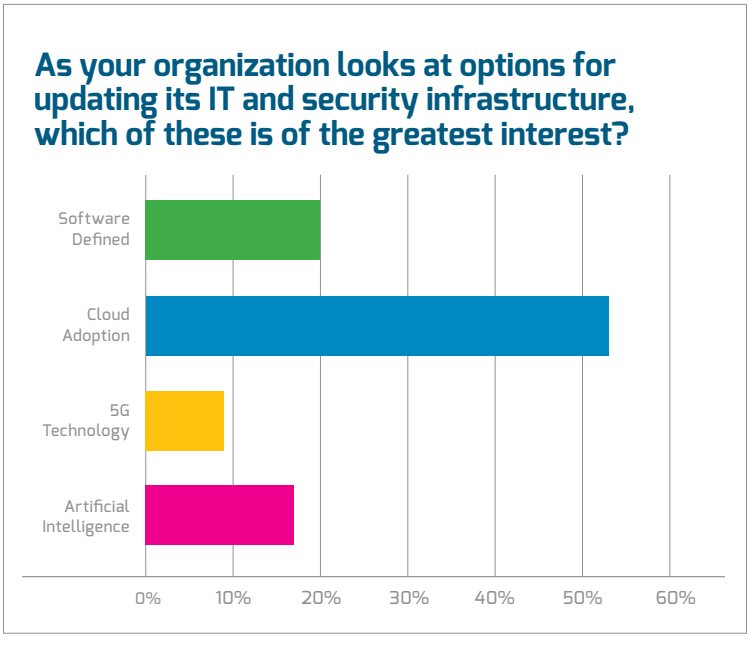
Richberg pointed out that there really aren't that many "pure" private clouds in the government and the ones that have been developed over the past decade or more are mostly for the national security agencies.

"DOD and the intelligence community actually pioneered cloud adoption with the private clouds built for intelligence," said Richberg. "But overall, most agencies will prefer some kind of hybrid setup."

The survey also found that telework will continue on after the pandemic, as 86% of federal security managers said they will either maximize telework or follow a hybrid model where telework will get split with time in the office.

"We're starting to see the federal government looking to hire people who will never come into the office," said Richberg, who adds that federal agencies will continue to mirror the private sector and hire the best person for the job, regardless of geographic region.

"The vast majority of people still want the option to work-from-home at least part of the time and the federal government understands that," Richberg said. "The trend towards hiring the best person for the job regardless of location will help federal agencies, especially in more remote jurisdictions. It's not always easy to find a cloud architect in the middle of the country. "



What Fortinet brings to the party

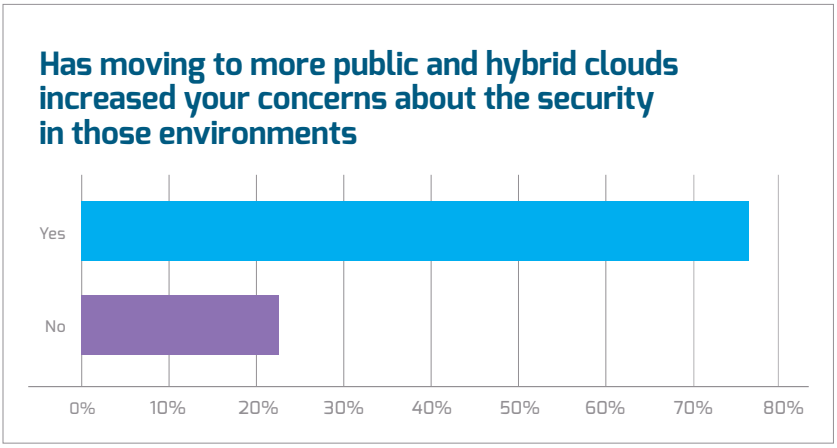
The Fortinet and Amazon Web Services survey also found that 57% of security managers were concerned about ransomware, while 20% of the group worried about nation-state attacks.

Richberg said he was surprised in the wake of the SolarWinds and Hafnium attacks that ransomware was the top concern compared to nation-state attacks.

"Ransomware out-polled nation-state attacks in the study by almost 3-1, and this was after we saw the SolarWinds and

Hafnium attacks where APTs were targeted at the federal government," Richberg said. He wondered, however, if survey respondents were being sympathetic to the pain felt by others more directly affected by the increase in highly-visible ransomware attacks.

In almost all the cases, whether it's SolarWinds, Orion or the Hafnium attacks, Richberg say most of these breaches are caused by compromise of users and endpoints. He said agencies have to adopt a "don't trust and verify" approach that's embodied in the Zero Trust concept.



Moving forward, agencies have to validate each user and device that comes on the network and assign different privileges for each work session and application according to the task at hand. Users should only be given the level of access needed for the task at hand; for instance, if an application only requires reading data, access should not automatically bestow the ability to write to or delete files as well.

"There's no one-size-fits all. It's Zero Trust," Richberg said. "In the past, if a security solution took even 10 seconds to validate, it was often viewed as too long and people would complain that security is slowing down the business. Most network traffic—data in motion—is now encrypted, and and many firewalls struggle to decrypt and inspect traffic without slowing throughout and network performance dramatically. But we have next generation firewall technology that allows agencies to decrypt and review traffic with minimal impact to performance, allowing and agencies to look at content and behavior and see if something is not normal. If it's not normal, it can be flagged or the system can be set to stop it, depending on how the agency configures the device based on the severity of the anomaly."

Richberg said federal security managers need to understand that the U.S. government is a primary target for the Advanced Persistent Threat or APT activity of nation-state adversaries. In these circumstances, timely backups are important, but real time monitoring and endpoint detection and response capability become important as well.

"We have a product that can automatically put a piece of unknown code it encounters into a virtualized setting—a sandbox—to execute, and if the code starts to run a global encryption function, then we know there's a problem since that is ransomware behavior" Richberg explains.

Richberg said security teams also need to take advantage of artificial intelligence and machine learning. He said while the attackers can leverage AI in areas such as content generation to make more authentic 'bait' for spearphishing, AI and ML will on balance prove more beneficial to defenders by making real-time correlations that can help detect anomalous behavior and prevent successful attacks.

Richberg also understands why so many federal security mangers are concerned about securing data in the cloud, noting that different clouds have different levels of native security.

"Very often agencies have data on-premises and then data in an off-campus private cloud," Richberg said. "Then they might possibly have assets in a third, fourth, fifth and sixth public cloud provider and they struggle to manage it all. Our cyber threat intelligence gives agencies the visibility so they can manage the virtual firewalls in all of those clouds, and have identical security controls and policies in all of these environments," he said.

Finally, the survey points out that 41% of respondents say they don't know what their security budgets will be for the upcoming year. Richberg attributed this to the cumbersome federal budget process.

"It's really the nature of the procurement cycle; there's always a time lag, so I wasn't surprised that they didn't know what the budget was," said Richberg. "The five-year development program (FDYP) we have in parts of the federal government doesn't have a parallel in the private sector. A well-funded company that is focused on securing its operations may have gone through multiple generations of products and technologies in that five years."

On the other hand, Richberg added that federal agencies can expect more cybersecurity spending based on the recent Biden administration executive order and Congress passing $1 billion in tech modernization targeted for cybersecurity.

"While there will be more money coming to cyber, the government is running a deficit, so I wouldn't be surprised if eventually the budget flattens," he said.

The message to federal agencies, according to Richberg, is to take advantage now while the Congress and the Administration are focusing on cyber. These next couple of years could be the best opportunities agencies have had to meet their cybersecurity goals in a generation.