DETAILS
BY: MERITALK STAFF
NOV 30, 2020
9:00 AM

Executive Q&A: Rackspace Technology Talks FedRAMP and Speeding the Path to ATO

Build once, use many times is a framework designed to bring efficiency and innovation to a wide variety of practices. In Federal government IT, perhaps the best known example is the Federal Risk and Authorization Management Program (FedRAMP), which endeavors to adopt this approach to standardize security and compliance of cloud solutions at work in the Federal government. It's a worthy goal that is well underway.

The time and cost associated with the FedRAMP process is declining, and the number of authorized solutions continues to increase. But Federal IT still has a long way to go in embracing the build-once, use-many-times framework. At the same time, the FedRAMP program management office (PMO) continues to improve and evolve the process, and Congress may soon codify FedRAMP into law. MeriTalk sat down with Lorenzo Winfrey, senior product manager, and Brad Schulteis, senior director, global government solutions at Rackspace Technology, to discuss the successes of the program to date and what's next.

MeriTalk: In what ways have you seen FedRAMP enable agencies to take advantage of innovation through SaaS and other cloud services?

Schulteis: FedRAMP has nailed its mission of providing a standardized approach to security and risk assessment in the cloud. Agencies can now use a cloud service without doing all the heavy lifting themselves. They can reuse an authorization and be operating in the cloud in days.

MeriTalk: The FedRAMP program continues to evolve. The liaison program and continuous monitoring capabilities are two recent examples. Do you think the FedRAMP program is doing enough to provide an easy and less intimidating process for companies interested in entering the public sector cloud services marketplace?

Winfrey: The FedRAMP Program Management Office (PMO) has done some really good work over the last couple of years to make the process easier for companies that want to get into the space. We think more can be done. A deeper focus in the FedRAMP training for software-as-a service (SaaS) providers about how to mature their security posture before beginning the authority to operate (ATO) process will have a very positive effect.

SaaS providers often underestimate what it takes to build a solid security foundation within their application before they enter the FedRAMP process. When we do a gap assessment, they often find out that key components in their application architecture will not be compliant with FedRAMP guidelines. Then they have to make significant modifications that require additional development or refactoring of existing features. That could take six months to a year, if not longer. Being better educated upfront will save SaaS providers a lot of time and a lot of money.

Agencies need education, as well. One of the things the liaison program wants to address is what's really involved in being an agency sponsor. Since FedRAMP began, a lot of government agencies have been hesitant to commit to being a sponsor because they aren't clear on exactly what will be required of them. That is a gap we need to close, helping them to understand clearly what their responsibilities are and how their increased participation as a whole can help them accelerate mission across the entire Federal government. The lack of agency sponsors fluent in the process is perhaps the largest reason that so few SaaS solutions have been authorized. More than 12,000 SaaS solutions exist today, but if you don't have an agency sponsor or you don't get into the Joint Authorization Board (JAB) process, you can't get authorized. If we can get the agencies to come to the table as sponsors more often, we can get more solutions authorized, faster.

MeriTalk: The FY21 National Defense Authorization Act includes a provision to codify FedRAMP into law. It would establish a presumption of adequacy for FedRAMP authorized cloud services and encourage further automation of the FedRAMP process. Will codifying FedRAMP encourage agency use of cloud services?

Winfrey: Codifying FedRAMP into law will be a big deal for the program. A GAO report last year found 15 of 24 agencies surveyed did not always use the program for authorizing cloud services. One agency reported that it used 90 cloud services that were not authorized, and the other 14 agencies reported using a total of 157 cloud services that were not authorized through the program. That gets away from the Cloud Smart concept. If FedRAMP is codified into law, it will increase the pool of solutions that government could utilize.

Schulteis: That's true, but that same report quoted an agency official who said it was too expensive for the providers to become compliant with FedRAMP. Many of these technologies are from startups that may have annual revenue of $1 million or $10 million. Expecting them to front the cost of FedRAMP – which could be more than $2 million to start – is not realistic. If grants or investment can become part of the FedRAMP law, that would be huge. The entry cost for FedRAMP can be disqualifying. And if a company can't make the investment in the short term, there's no way it can pay for the continuous monitoring component. That's a million dollars a year to maintain. Ashley Mahan (director of FedRAMP in the General Services Administration) has been talking about bringing more automation and streamlining the process, which ideally will drive down some of the costs.

MeriTalk: NIST and FedRAMP are working to add automation to the review of security documentation with the machine-readable Open Security Controls Assessment Language (OSCAL). What are your thoughts on that, and what other efficiencies do you think FedRAMP can realize?

Winfrey: What they've been doing with OSCAL – coming up with a standard that can be applied to the publication and assessment of security controls – is definitely a step in the right direction. It probably would behoove them to partner with some folks who already operate in this space and build on the things they've already done.

Schulteis: I don't know that they're going to be able to eliminate most of the paperwork by automating the authorization process. Getting in the front door to FedRAMP is one thing, but then you have the continuous monitoring requirement, which is directly incumbent upon the agency that is authorizing the cloud. That piece is the most burdensome and needs strong automation.

MeriTalk: Rackspace helps agencies and vendors get to FedRAMP ATO – and thus mission enablement – with a couple of unique pieces to the FedRAMP puzzle. Can you talk a bit about inherited security controls and cloud security-as-a-service?

Schulteis: When customers use Rackspace Inheritable Security Controls, we document and manage approximately 80 percent of the security and compliance requirements within the cloud environment to help them receive a FedRAMP ATO.

Winfrey: Using inheritable controls means that the cloud solution has already been assessed for compliance and it is continuously monitored, so agencies can accept it. The concept aligns directly with FedRAMP's build-once, use-many-times inheritance model. Agencies have access to all of the authorized vendors and their entire body of evidence. They can assess their work without requiring that it be done again. The effective use of the inheritable controls model in FedRAMP is perhaps the biggest factor related to reducing time and costs to deliver.

Schulteis: Many of our FedRAMP customers are other solution providers from industry, but government agencies can inherit our controls, as well. If the typical government customer wants to use Amazon Web Services (AWS) today, for example, they can put it on their credit card, but they still need to manage and secure in the cloud. We can secure the cloud for them and give them a path to ATO with all of our documentation. We provide that in a monthly bill, the same way the agency would buy AWS and get a monthly bill for services.

MeriTalk: What's on your wish list for the FedRAMP program?

Winfrey: We've seen FedRAMP authorizations double in the last few years. If the program can maintain that momentum, agencies will benefit from a larger selection of innovative and mission-relevant capabilities. As the FedRAMP program continues to evolve, perhaps there's a categorization for solutions in high-need or high-demand areas across the Federal government, like artificial intelligence, DevSecOps, and machine learning, which helps accelerate their journey to FedRAMP compliance. The Federal government's ability to leverage these technologies and approaches will be critical to our country's ability to deliver technical capability when and where the mission demands. Otherwise, short of FedRAMP being codified into law, agencies will continue to seek those types of solutions and authorize them outside of the program. And then we are going backwards a little bit.

READ MORE ABOUT
INDUSTRY NEWS

RECENT
CDM Program Manager Discusses Higher Funding Baseline for FY 2022
Census Bureau Must Ensure Transparency on Apportionment Data
More Complete Data on Promotions Can Help Address Federal Pay Gap

MORE TOPICS
CIO BRIEFING ROOM
CIVILIAN AGENCIES
CONGRESS
DEFENSE & INTELLIGENCE
EDUCATION
EMERGING TECH
INDUSTRY NEWS
JUDICIARY
WHITE HOUSE
WORKFORCE ISSUES

ABOUT
MERITALK STAFF
TAGS
FedRAMP