Value of FedRAMP Enterprise Solution Portfolio

Agencies need comprehensive cloud solutions

With the increasing importance of data to mission and operations, mounting cybersecurity concerns, and IT operations that are both on-premises and off, federal civilian agencies need comprehensive solutions that can adapt to those shifting conditions.

Software solutions provider SAP's National Security Services (NS2) has streamlined adoption of its cloud solution with a deployment model that meets FedRAMP requirements, said Kevin Gallagher, cloud product launch lead for SAP NS2 at the recent Carahsoft FedRAMP Headliner Summit.

"We're taking SAP cloud solutions across the portfolio and including them in a FedRAMP-certified platform-as-a-service (PaaS) and software-as-a-service (SaaS) environment," he said.

Cybersecurity threats are ever evolving and becoming more virulent and easier to perpetrate, according to Gallagher. A ten-year-old child can create and distribute a virus that works using common tools available on the internet and on smart phones and other devices, he said.

That growing danger runs up against how agencies and the workforce at large are evolving to more open, increasingly remote workplaces where there are potentially more avenues for attacks.

"There are obvious advantages to bringing workloads and capabilities into the cloud," Gallagher said, since it provides a centralized place for increasing amounts of data.

However, more data can mean more problems if it's not secured properly, according to Gallagher. He notes that the next optimal solution in a FedRAMP landscape is the ability to deliver a portfolio of solutions, within that secure boundary. The federal government is taking steps to allow agencies to quickly respond and address changing technology and shifting threat landscapes through programs such as FedRAMP.

According to Gallagher, the move to the cloud has been particularly useful in keeping up with technologies, as well as addressing threats. FedRAMP's consistent, standardized approach to security requirements can level very different security approaches in technology.

To secure their data, agencies need to understand where that data resides and who can access it, Gallagher advised. Additionally, having a centralized governance such as FedRAMP helps maintain a stable, secure environment.

To keep that data within appropriate boundaries, SAP's cloud facilities "reside in the U.S. and stay in the U.S.," said Gallagher, emphasizing the importance of that domestic residency to federal agencies. "That is a critical mechanism to help decrease the number of international entryways into your data and into your landscape," he said.

Who has access to data is always a fluid situation that has to be monitored closely. Over time, however, that process must be maintained to keep it sharp. "You have to patch it and ensure you're looking at current threats, but also predict future threats," he said.

FedRAMP ensures that vendors continue to meet baseline security requirements over time, including on-going federal monitoring, reporting and remediation compliance requirements.

SAP and SAP NS2's portfolio of cloud solutions is the only one that can be deployed within FedRAMP, SaaS and PaaS Provisional Authority to Operate (P-ATO) and Authority to Operate (ATO) environments, according to Gallagher.

"It's the entire portfolio of your business solutions," he said. SAP works with its customers, its FedRAMP technology partners, FedRAMP's third party assessment organizations (3PAO) that assess security, and with network infrastructure providers to hone its cloud data security services, said Gallagher.

The cloud provides enormous benefits for data functionality and accessibility, he said. "Cloud continues to change the way we operate our businesses and organizations. There's an inherent risk with that. Threats will continue to change and adapt."

SAP NS2 recognized that challenge and gave customers a way to adopt cloud solutions in a consistent portfolio, secured to the highest standards through U.S. data sovereignty, and the company's compliance techniques.

"We've allowed the customer to adopt cloud portfolio in a way that they would not have been able to do before," he said.

> "Cloud continues to change the way we operate our businesses and organizations. There's an inherent risk with that. Threats will continue to change and adapt.
>
> **KEVIN GALLAGHER**
> Cloud Product Launch Lead, SAP NS2