Moving Intelligently Toward the Cloud

Bryce Petty, EVP of Software Development for SAP NS2, highlights the value of FedRAMP-certified clouds and suggests how organizations can securely take advantage of multi-cloud and hybrid cloud environments.

How is cloud use evolving in state and local government, especially regarding advanced analytics and other emerging capabilities?

The cloud helps lower the barrier of entry into advanced analytics. In the past, organizations had to stand up their own environment and compute center to take advantage of these capabilities. Now, with today's extensive cloud marketplace, they can easily obtain software-as-a-service (SaaS) offerings to rapidly take advantage of a whole set of advanced analytics features — whether that's AI, machine learning or some other emerging technology. At the same time, the cloud introduces new security concerns. Once data moves into the cloud, it's very important to have a good understanding of how it's being used and secured.

What are the challenges of moving business operations to the cloud and managing hybrid environments?

The biggest challenges include security, cost, having the technical expertise to successfully migrate into these hybrid environments and understanding which applications are best suited to run there. Organizations often spend a lot of time and money and introduce security vulnerabilities because they try to move applications that are not designed to run in a cloud environment. With the pandemic, organizations are under pressure to rapidly move their workforce into cloud environments. There can be a tendency to cut corners to save time, but these sacrifices can also create vulnerabilities.

How can the right cloud platform help organizations integrate on-premises and cloud applications?

One of the great things about the cloud is its inherent flexibility. You can establish a cloud account and be up and running very quickly. The right cloud platform can also spin up a near infinite amount of hardware and resources, as needed, to fulfill a solution requirement. It lets agencies try new ideas, fail fast and continuously improve — with less risk than traditional approaches. The key to success is understanding the capabilities of the various cloud platforms and the tools that are available in those clouds, and then quickly taking advantage of them.

How can organizations better protect data and workloads in a multi-cloud environment?

Protecting data is an extremely important consideration in cloud migration. Each cloud environment — Amazon, Azure, Google and so on — is constructed differently, and each cloud provider uses different security terminology and approaches. When you bring these different clouds into a multi-cloud environment, it's very complex to manually combine information from all the clouds, understand how each cloud implements security policies and rules, and determine whether your organization has a viable security posture. Even if an organization has a highly trained staff, I recommend investing in a commercial cloud security posture management (CSPM) application. The right CSPM tools can make it substantially easier to understand your organization's overall security posture, and help enforce compliance across a multi-cloud environment.

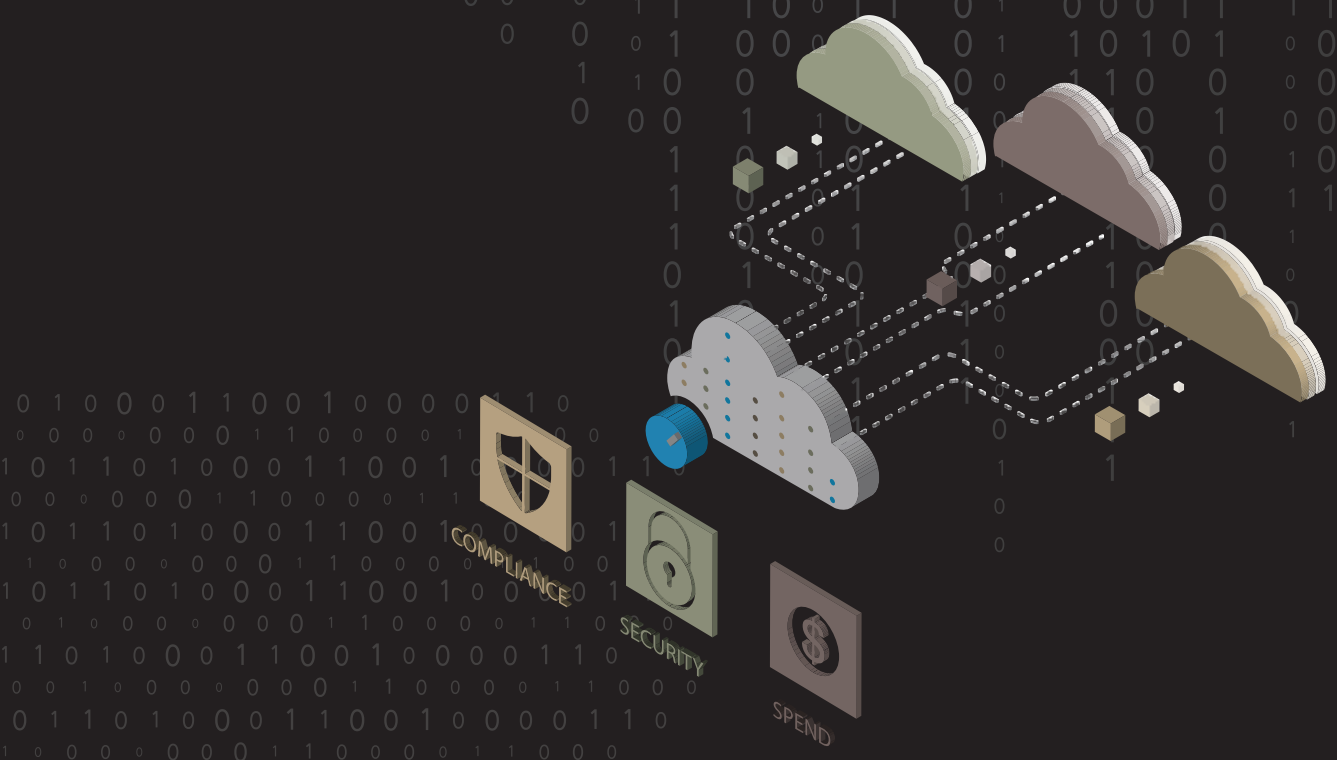
When using FedRAMP certification as guidance for selecting a cloud vendor, what should organizations keep in mind?

In the FedRAMP world, at a minimum, cloud environments must meet the third-party security assessment, authorization and continuous monitoring requirements. This can be challenging for organizations that are new to the process, and they should partner with a cloud provider that has an existing FedRAMP-certified cloud. It's important to understand that doing things to comply with FedRAMP requirements is not the same as having FedRAMP authorization. Vendors may say they're building their environments around FedRAMP or their software tools are compliant. But it doesn't necessarily mean they've succeeded in all the auditing rigor to become certified. Only a handful of cloud providers are actually certified.

With remote work increasing, what suggestions do you have for secure teleworking?

You don't want to make the environment so hard to use that productivity and the user experience are affected. It's really an art of finding the right balance between implementing a strong security posture and making the system easy to use. Organizations can begin by establishing a detailed written policy around remote access. This plan can be refined over time, but starting with the strictest policy first may save headaches in the future. Then organizations can take advantage of commercial cloud security tools to ensure their cloud is adhering to best practices and standards. As time and budget permits, it's also worthwhile to have a third party assess your organization's cloud security posture.

Control costs and manage security on your multi-cloud environment



Do you and your team have a full picture of your cloud spend today and in the future? What about your continuously evolving security and compliance posture? We can help.

CloudMixr from NS2 tackles your security, compliance management, and cost optimization challenges.

CLOUD MIXR

Learn more **sapns2.com/cloudmixr/**

SAP NS2 NATIONAL SECURITY SERVICES