

**Government
Business
Council**

Federal Cloud in Focus: Five Things You Need to Know About the Federal Cloud Environment

**PRESIDIO[®]
FEDERAL**

Think Mission.

vmware[®]

Introduction

Across the federal government, agencies are undergoing a large-scale digital transformation. Evolving needs have compelled agencies to modernize their IT infrastructure and embrace the latest technology innovations. Cloud computing in particular is a widely desired tool that empowers digital modernization. With the potential for greater scalability, increased efficiency, reduced costs, and more, cloud capabilities are understandably appealing to the federal government. Despite the importance of cloud to the future of federal IT, there is little clarity on what is actually being done to leverage cloud or what progress has been made. This ambiguity leaves many confused about the federal government's cloud implementation and what constitutes an agency's cloud environment. This report provides answers and clarity to the five things you need to know about the federal cloud environment.

Defining Cloud

Given that the term “cloud” is often broadly used to describe any technology provided to the federal government by an outside vendor, it's worthwhile to provide a definition of cloud. The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources — such as networks, servers, storage, applications, and services — that can be rapidly provisioned and released with minimal management effort or service provider interaction.¹ In summary, cloud computing constitutes convenient, flexible access to a broad range of computing resources over a network. Cloud computing is essential to the government for a variety of reasons beyond just offering an alternative to physical servers. According to a Congressional Research Service report, the advantages of cloud adoption include reduced IT costs, improved efficiency, greater accessibility, increased collaboration, faster innovation, more reliability, and enhanced security.²



Top 5 “Need to Know” Factors about the Federal Cloud Environment

1

What are agencies doing to develop cloud environments?

The federal government is already using various forms of cloud computing solutions today. The federal government has been shifting its data storage needs to cloud-based services and away from agency-owned, in-house data centers since 2009.³ The Office of Management and Budget’s latest plan to drive cloud adoption in federal agencies is the 2019 [Cloud Smart](#) strategy. This long-term, high-level strategy has provided agencies with guidance on how to implement and leverage cloud-based technologies. With three key pillars to successful cloud adoption – security, procurement, and workforce – Cloud Smart includes [22 action items](#). These action items constitute a work plan aimed at creating and updating programs, policies, and resources the entire government will use to advance the Cloud Smart agenda.⁴ In accordance with the Cloud Smart strategy, federal agencies are encouraged to seek the environments and solutions, cloud or otherwise, that best enable them to achieve their mission goals while being good stewards of taxpayer resources.⁵ Under the Cloud Smart strategy, each agency’s cloud implementation journey is unique and necessitates a change in mentality where cloud is part of the day-to-day business of technology.



2



How far along are agencies in cloud development?

In April 2019, the Government Accountability Office (GAO) published a [report](#) that examined the status of cloud adoption at 16 federal agencies. According to the report, all 16 agencies made progress in implementing cloud services. However, the extent of their progress varied. Between fiscal years 2016 through 2019, 10 agencies reported an increase in the use of cloud services, four reported a slight decrease, and two reported no change.⁶

Change in Investments Using Cloud Services between FY 2016-2019		
INCREASED <ul style="list-style-type: none">• General Services Administration• Social Security Administration• Department of Agriculture• Department of Commerce• Department of Health and Human Services*• Department of Justice• Department of State• Department of the Treasury• Department of Transportation*• Small Business Administration	NO CHANGE <ul style="list-style-type: none">• Department of Energy**• Department of Labor**	DECREASED <ul style="list-style-type: none">• Department of Defense• Department of Education*• Department of Homeland Security• Department of Veterans Affairs

* agency did not have guidance for assessing all investments for cloud services

** agency had guidance but did not assess all investments for cloud

A more recent [GAO study](#) in June 2022 looked specifically at the Defense Department’s cloud implementation progress and found that the department fully addressed 11 of the 14 key IT cloud requirements established by the Office of Management and Budget. The remaining three requirements concern workforce planning and software application modernization.⁷

According to the Office of the Chief Information Officer, 17 of the 22 action items in the government-wide Cloud Smart strategy have been completed.⁸ The remaining five action items are in progress and scheduled to be completed in the next 6 to 18 months.

3

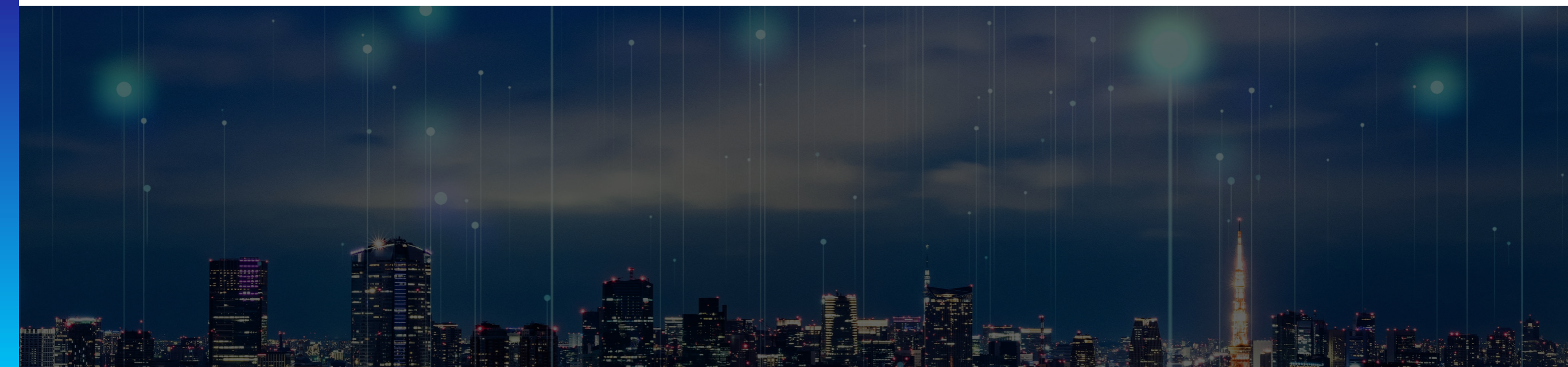
What do agencies' cloud environments actually look like?

Federal agencies use a variety of cloud deployments and cloud services depending on their mission needs. Federal agencies can receive cloud services from providers similarly to how individuals receive utilities from private companies. The type of service depends on the extent to which resources are managed by the cloud service provider or the agency itself. There are three main types of cloud services provided to federal agencies:

- **Infrastructure as a Service (IaaS):** Vendors provide the infrastructure and hardware.
- **Platform as a Service (PaaS):** Vendors provide a managed environment for the agency's application.
- **Software as a Service (SaaS):** Vendors provide a fully managed application and the agency need only supply their data.

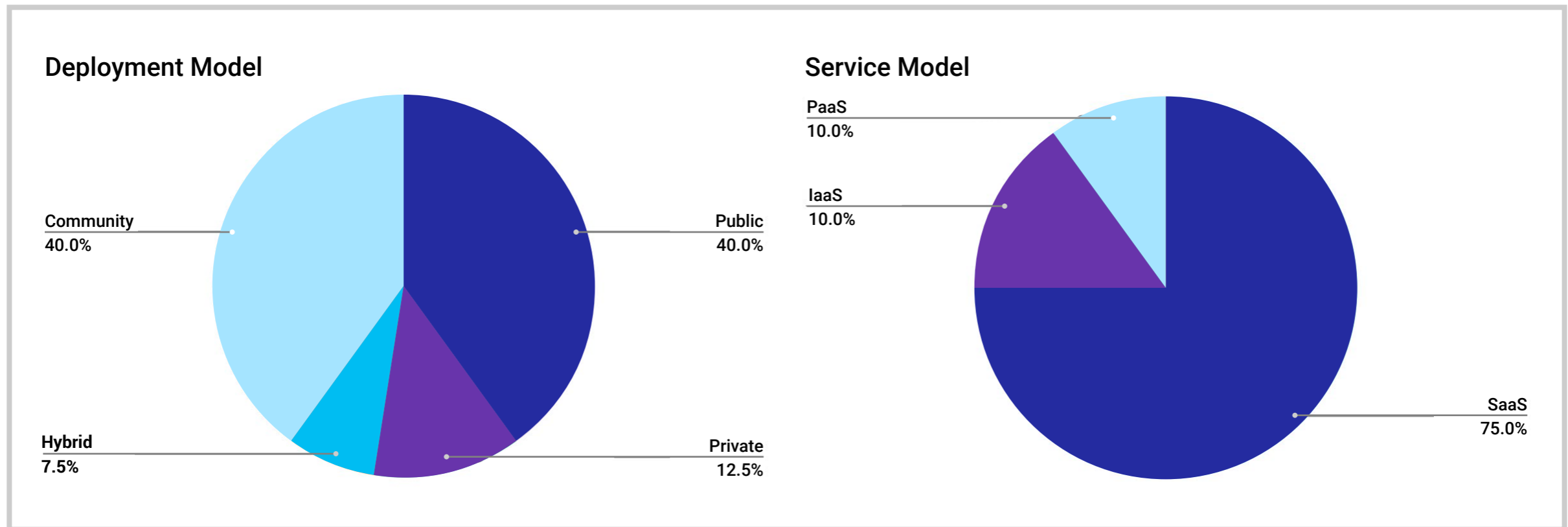
There are four main types of cloud deployments: public cloud, private cloud, hybrid cloud, and community cloud. Each deployment model is defined according to where the infrastructure for the environment is located.

- **Public cloud:** A third-party vendor supplies one or more cloud-computing services to a group of independent organizations over the public internet.
- **Private cloud:** Operates similarly to public cloud, but on a private network controlled and used by a single organization.
- **Hybrid cloud:** Uses a combination of public and private cloud services.
- **Community cloud:** A group of organizations with similar requirements share cloud infrastructure.

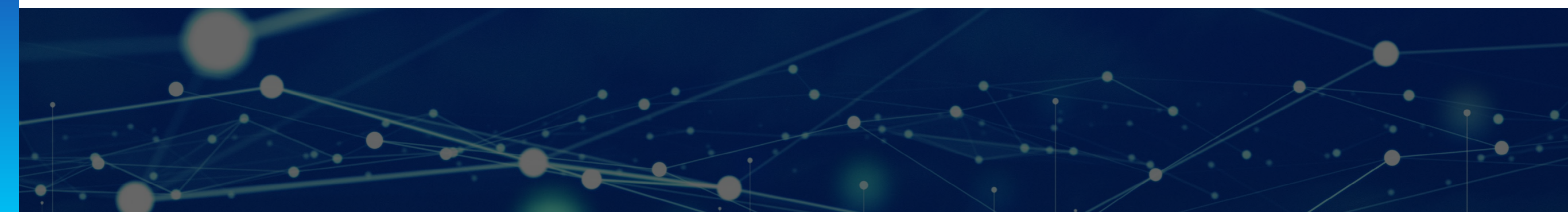




Agency Example: **Department of Energy (DoE)**
2018 DoE investments related to spending on cloud services of at least \$1 million or more in life-cycle costs.⁹



Several agencies also employ a **multi-cloud** strategy – the integration of services from multiple cloud service providers in a single architecture. In a multi-cloud strategy, agencies select multiple cloud providers that are best suited for their data and applications. This strategy allows agencies to leverage the desired benefits from different cloud providers depending on the agency’s mission needs while also avoiding vendor lock-in.



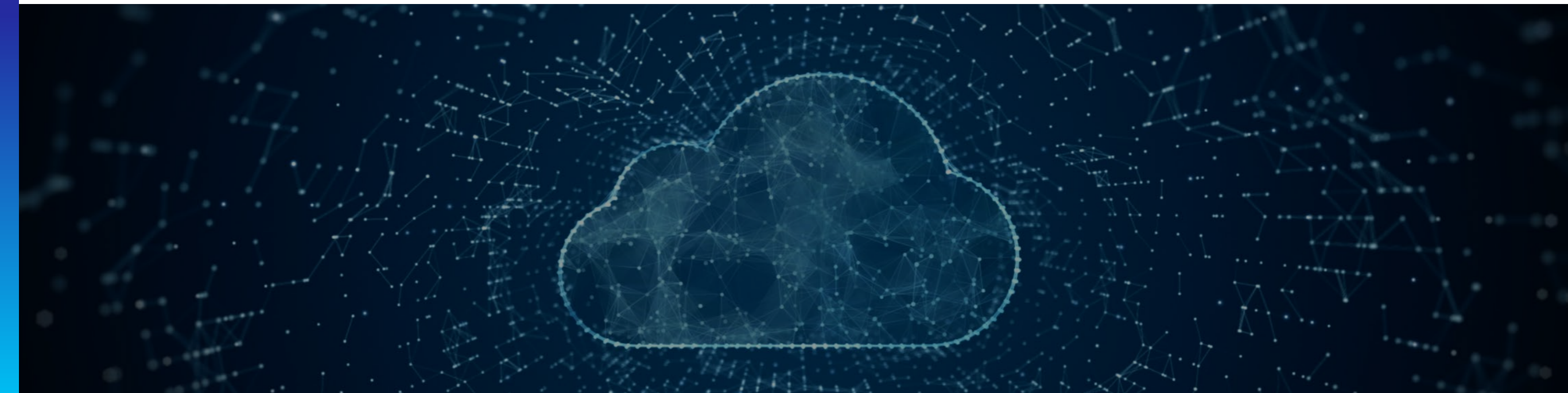
4

How are agencies successfully leveraging cloud?

Implementing the Cloud Smart strategy and transitioning the majority of the federal government's stored data to the cloud is a lengthy process, to say the least. Fortunately, this process has been streamlined through partnership with private industry. Through this partnership, agencies are able to harness new capabilities, expand existing abilities, and deliver services to the public faster. To partner with federal agencies, cloud service providers must be approved through the Federal Risk and Authorization Management Program ([FedRAMP](#)).

Industry Partnership Example: **US Air Force's Cloud One**¹⁰

Cloud One is a cloud hosting service and platform for the Air Force and Defense Department. Cloud One is a multi-cloud environment leveraging several private industry partners to provide secure access to commercial cloud services, hardened cloud environments, and managed cloud capabilities.



5

What areas of cloud are still evolving?

Cloud computing has come a long way since its inception. However, continued evolution of cloud computing is needed in order to meet the expanding needs of its users. For example, cybersecurity is commonly cited as the principal concern with cloud computing. This is because the security perimeter of a cloud network is expanded out to all devices connected to the cloud, meaning that every remote endpoint can be a point of entry for a cyber attack. This concern has elevated the importance of defending endpoints such as desktops, laptops, and mobile devices from malicious activity, also known as endpoint protection. Cloud-based endpoint detection services offer the capability to continuously monitor an agency's networks and analyze cyber threat data. Cloud-based endpoint protection allows a system administrator to configure settings, install patches, approve devices, audit users, and more from anywhere there's internet access.¹¹

Another key way in which cloud computing is evolving is through the incorporation of artificial intelligence (AI) and machine learning (ML). The integration of AI and ML in cloud services presents several benefits, including automation of redundant tasks, a reduced workload for IT staff, and less risk of human error. In addition to streamlining the data management process, AI and ML integration can also curb potential data leaks, eliminate security loopholes, and prevent data theft, ultimately improving cybersecurity.



Industry Perspective



Think Mission.

While the federal government was driving innovation in technology 40-50 years ago, private industry is now evolving its products and services at a rapid pace and has proven the value of cloud computing. Today, private industry offers a streamlined pathway to embracing cloud computing and federal agencies can leverage IT infrastructure as an instant commodity.

In addition, the private sector can share many of the lessons learned with the federal government to help ensure success in their cloud journey. There are many applications and platforms required to support any agency's mission. Each application or platform has its own lifecycle and requirements. Not every application or platform is right for public cloud, nor is refactorization. There are many cloud solutions to deploy applications – such as private, public, or

hybrid – many various tiers for consumption – such as IaaS, PaaS, or SaaS – and endless locations offering these different cloud services.

With so many choices and so many solutions to integrate, it's important for any organization, private or public, to have a technology partner like Presidio Federal that will help navigate through the integration of all the many disparate cloud platforms.

In partnership with private industry, the federal government can start normalizing their applications and resolving technical debt, all while maximizing taxpayer dollars and minimizing their environmental footprint.

At Presidio Federal; we think mission, and we will invest our experience into your mission.



*Trevor Patch,
Principal Architect –
Cloud & DevOps
Adoption, Presidio
Federal*



Across the Federal government, a hybrid cloud implemented on the right platform enables agencies to tap into the unique benefits of each cloud option.

Public cloud provides unique, innovative, or differentiated services to build new applications. The on-demand consumption models allow for flexible pay-for-use economics. In addition, the elastic capacity, rapid scalability, and the speed with which capacity is provided in public cloud are difficult to match for many public sector organizations.

Private cloud provides a degree of elasticity and resilience with which public sector organizations can complement their existing on-premises infrastructure. In certain instances, organizations have massive amounts of data or data residency requirements that prevent them from migrating to public cloud. In this case, local cloud delivers

the benefits of public cloud to the data center, including modern technologies to transform existing applications.

In most situations, organizations have on-premises infrastructure that they built over many years. They have invested in hardware, software, skills, and processes that haven't been fully depreciated and want to use that infrastructure as long as possible. Often this infrastructure has specialized hardware or software not available in other cloud options, or the organization wants to stay in full control of every aspect of the infrastructure and applications. For these reasons and many others, Federal organizations want to leverage the right cloud for the right application. A hybrid cloud delivers consistent infrastructure and operations across all these environments for all applications.



*Mike Wilkerson,
Federal VMC on
AWS Specialist,
VMware*

Final Considerations

It's important to remember that each agency's cloud journey is different.

While some have taken to cloud services faster than others, all are making progress toward a more cloud-centric future. Much progress and investment have already been made, yet there is still more work to be done.

Fortunately, the future of federal cloud is promising. Through continued private-sector partnerships, federal agencies will soon, if not already, be able to leverage the latest advancements in AI and ML while also enhancing endpoint protection cybersecurity measures. While timelines may yet be up in the air, the future is certainly in the cloud.

Government Business Council

About GBC:

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of *Government Executive's* 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision-makers from across government to produce intelligence-based research analysis.

For more information, email us at research@govexec.com or visit our website at <https://www.govexec.com/insights/?org=gbc>.

PRESIDIO[®]
FEDERAL

Think Mission.

About Presidio Federal:

Presidio Government Solutions, branded Presidio Federal, is a dominant provider of communications, technology and security solutions in support of federal mission outcomes. We are a wholly-owned subsidiary, and fully independent entity of Presidio Network Solutions, dedicated to servicing the needs of federal customers through expert knowledge centers in automation, augmentation, cloud, cyber security, collaboration, data center, and digital infrastructure.

Learn more at <https://presidiofederal.com/>

vmware[®]

About VMware:

VMware is helping federal government agencies such as the U.S. Air Force and IRS accelerate the delivery of critical services across data center, cloud, and edge environments. For more than 20 years, VMware has helped government organizations use the latest R&D innovations to drive greater efficiency, security, and reliability. Our integrated capabilities are designed to make the most of legacy technical investments, while also enhancing the organizational culture. With VMware, your agency can build, run, manage, connect, and protect any application. And this continuous delivery lifecycle works with any cloud and any device.

Learn more at <https://www.vmware.com/solutions/industry/federal-government-it-solutions.html>

Sources

1. <https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published#:~:text=According%20to%20the%20official%20NIST,and%20released%20with%20minimal%20management>
2. <https://sgp.fas.org/crs/misc/R46119.pdf>
3. <https://sgp.fas.org/crs/misc/R46119.pdf>
4. <https://cloud.cio.gov/strategy/#cloud-at-a-glance>
5. <https://cloud.cio.gov/strategy/#cloud-at-a-glance>
6. <https://www.gao.gov/assets/gao-19-58.pdf>
7. <https://www.gao.gov/assets/gao-22-104070.pdf>
8. <https://cloud.cio.gov/strategy/actions/>
9. <https://www.gao.gov/assets/gao-19-58.pdf>
10. <https://www.cloud.mil/Cloud-One/>
11. <https://www.selecthub.com/endpoint-security/cloud-endpoint-security/#:~:text=Cloud%20endpoint%20protection%20allows%20your,IT%20staff%20in%20one%20office.>