

Dissecting the federal cloud 'forecast'

The new capabilities, applications and business models unlocked by cloud adoption are expected to have an outsized effect on the business of government.

Cloud service adoption among federal agencies has changed significantly since it first kicked off more than a decade ago. Cost-savings and enhanced capabilities, while certainly still motivators, have given way to more targeted incentives. Cloud services, for example, provide collaborative tools that enable hybrid work environments. They facilitate data collection that can help agencies make better decisions about everything from workplace efficiency to cybersecurity. Finally, they've helped federal agencies hone in on customer experience, delivering more efficient and personalized services for constituents.



CHALLENGES OF CLOUD ADOPTION

Of course, there have been challenges along the way; data sovereignty, transportation and storage have mostly been worked out at this point, especially through the introduction of government-specific and even classified cloud instances.

However, service-level agreements have been a weak point. On the latest [Federal Information Technology Acquisition Reform Act](#) scorecard, most agencies received failing grades when it came to meeting the Office of Management and Budget's requirements for the Federal Cloud Computing Strategy. The GAO report backs that up, noting "specifically, agencies' service level agreements did not consistently define performance metrics, including how they would be measured, and the enforcement mechanisms."

Security has been particularly challenging, as well. The proliferation of online threats from bad actors has made manual monitoring nearly impossible, putting data and network infrastructure at risk. For example, a [2023 Government Accountability Office report](#) found that of 15 systems across four departments examined, the departments had only implemented continuous monitoring in three of those systems. However, artificial intelligence may present the solution to this particular struggle.



THE FEDERAL CLOUD "FORECAST"

AI is one of the emerging technologies expected to have a major impact in the near future, enabled by cloud services. In a survey, Gartner found that 87% of organizations expect to adopt AI by 2025, and federal agencies are no exception. Currently, agencies are at varying points in figuring out how to integrate AI into their existing processes. Developing strategies for responsible and ethical AI that emphasizes accountability, transparency and fairness, is another hurdle agencies will have to clear before they can fully adopt the technology.

However, once they do, AI – including generative AI and large language models – can be trained on the massive amounts of security data agencies have been collecting thanks to their cloud investments, making continuous monitoring not only easier, but cheaper and more effective

as well. AI-enhanced tools can also be used to help shift security left, making development processes more secure.

Further, generative AI can help agencies speed up their content generation and deliver new applications and services. AI-enhanced analytics tools can improve decision-making based on data. Large language models can help deliver better customer experience.

Agencies can also leverage automation through cloud service adoption, making employees more effective by reducing the number of manual tasks they are required to perform. It will save time, as employees will be required to do less data entry between disparate systems and tasks. Automation of manual tasks can also help reduce the effect of human error, yielding cleaner data for better decision making.

Cloud adoption is also making edge computing more common, enabling agencies to collect, store and process data in the field for faster and better decision making. That will lead to better outcomes in time-sensitive fields like law enforcement and military applications, as well as allowing scientists and researchers to process more of their data in the field. In addition, edge computing contributes to both network security and cost effectiveness by reducing the need for transference of large amounts of data.

And cloud services themselves are expected to grow significantly as agencies turn to more as-a-service offerings to help them accomplish their missions. Gartner expects the global public cloud services market to grow to \$501.3 billion in 2024, up from \$364.1 billion in 2022. This will likely be driven by increased adoption of multi-cloud strategies, which will help agencies reduce vendor lock-in, improve their flexibility and resilience, and optimize performance by choosing the best tool for the need, rather than relying on a single vendor for all their cloud services.

This will also drive an increase in interoperability and portability, allowing agencies to transfer data and workloads from one platform and environment to another, provider notwithstanding. That flexibility will allow agencies to further optimize costs and efficiencies through strategic planning and management.

Finally, cloud-managed networking solutions will give agencies increased visibility across these platforms, environments and services. Combined with the government wide push to adopt zero trust security, agencies will be better equipped to protect their own networks and data, as well as the data of their customers.



For all of these reasons and more, the new capabilities, applications and business models unlocked by increased cloud adoption are expected to have an outsized effect on the business of government within the next few years.

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