Google Cloud | Deloitte.

Speed, Security, and Value – Assessing Cloud Options for Federal Agencies

Federal agencies are at a crossroads with cloud computing. The need for a secure, fast, and economical cloud is evident, and the question is how can agencies cross the bridge from legacy, lethargic data operations to a more nimble and scalable future state?

The impetus for change owes to a convergence of factors. The 2020 pandemic created a sense of urgency for government agencies to spin up critical services and offer just in-time assistance, including for remote workers. Meanwhile, in 2022, the Office of Management and Budget released a federal strategy for implementing a Zero Trust approach toward cybersecurity in government agencies. This injects new considerations for government cloud strategy and questions around whether a cloud provider's offering can meet Zero Trust expectations. There is also a growing focus on the new discipline of FinOps and the importance of managing and optimizing cloud spend.

These factors come alongside the need for safe data exchange between agencies and facilities, a low tolerance for latency, and the importance of setting the stage for a data-driven future leveraging artificial intelligence (AI) and emerging technologies. No surprise then that CIOs are motivated to enhance their cloud strategies and ecosystems, whether it is by selecting or expanding work with a single cloud service provider (CSP) or taking a multi-cloud approach.

Whatever the path ahead, the soundest decisions and investments need to address three central questions surrounding an effective and valuable cloud offering. Which networks are best suited to rapidly transfer data between geographically dispersed agencies and data centers? How is the network and cloud offering secure and aligned with regulations and standards? And what is the best fiscal choice in an era of FinOps?

> Answering these questions sets agencies on a path to making the best decisions for their cloud needs and ambition.

How do you rapidly move data to where it needs to be?

Agencies and government workforces are dispersed across the country and the world, and the volumes of data with which they contend are only growing. This raises the fundamental challenge of accessing network infrastructure to rapidly share data between stakeholders and partners. Regulatory agencies, for example, use vast datasets created and held at facilities and labs across the country. The challenge is to move that data to other facilities and to the cloud where it can be analyzed and the insights extracted. In this, the technology enables the mission, and for mission-critical data sharing, the outcomes can be a matter of public health, even life and death.

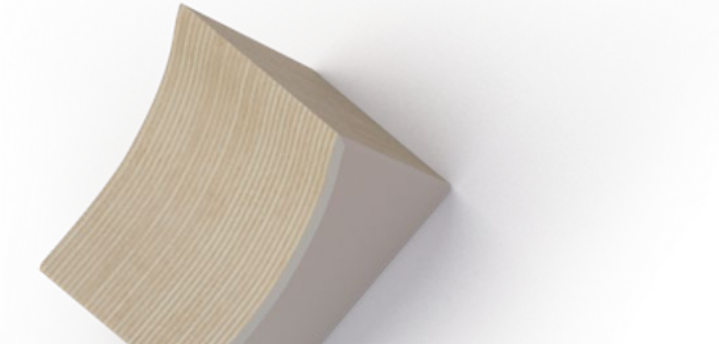
Consider a hypothetical example wherein there are reports of an illness suspected to be stemming from romaine lettuce. To promote public health, a regulatory agency needs to identify and isolate the farm where the produce is grown, so as to locate and recall any other potentially contaminated goods. Yet, challenges and delays can arise when attempting to connect lab environments in different locations, which can impede data sharing and analysis. Ultimately, the longer it takes to trace the source of contamination, the longer the public health threat persists.

When data is siloed and cannot be shared at the necessary speed, simplicity, or volume, it could hinder the mission. Different CSPs offer a range of capabilities, and one important factor is the fiber network itself. On this point, the Google network in particular is unique. It is one of the largest privately managed networks in the world, spanning 37 regions and 112 zones, and 187 edge locations. The same infrastructure that underpins the modern web and fuels billions of exchanges of e-mails, documents, and other media is the same infrastructure underlying the Google Cloud offering. What this means is federal agencies can access data speed commensurate with commercial users while also meeting the rigorous standards for government cloud use.

Taking the contaminated lettuce example, consider a lab in California using on-premise hardware for data storage and compute. To quickly identify the source of the contamination, the lab needs to share data with a lab on the East Coast while also analyzing the datasets in the cloud. With the Google network as the data superhighway, the California lab and the East Coast lab each connect to an edge point of presence and because the traffic does not touch a public network, both labs enjoy a fast, secure, and compliant way to connect the data.

This foundational capability is complimented with software that allows agencies to route a request to any free output port without interfering with other traffic. Users can also rely on a software-defined network providing functional and performance isolation that can burst thousands of stateful machines online in minutes or deploy firewall rules across thousands of machines without chokepoints.

Bottomline: When exploring and evaluating cloud offerings, investigate the capabilities of the network that makes secure data sharing and analytics possible.



How do you meet security and compliance standards in the cloud?

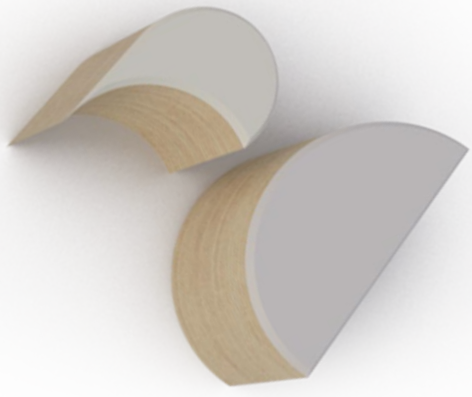
The Zero Trust federal strategy for cybersecurity mandates an agency prioritization of security requirements. The essence is that no user or device is trusted implicitly based on its network location. Instead, there is an assumption that users, devices, applications and networks may not be trustworthy, and data access is granted based on the identity of the user and device.

In addition, agencies face the requirement to use the Federal Risk and Authorization Management Program (FedRAMP) when evaluating, authorizing, and monitoring cloud services. Security controls for CSPs must enable the protection of sensitive information, the prevention of data deletion or modification, and reliable data availability. FedRAMP High requirements place hundreds of security controls around the CSPs offering when dealing with highly sensitive or mission-critical data.

To meet FedRAMP requirements, some CSPs have taken the approach of building dedicated U.S. Government Clouds. In this, the cloud exists in isolated environments, including physically separate data centers. On the one hand, this does deliver a level of security federal agencies are seeking for data transfer and compute. Yet, a government cloud often does not offer the robust capabilities of a commercial cloud. In addition, workloads are not easily migrated between U.S. Government Clouds, and authorizing new services can take as long as a year. There is also the challenge that the United States is the only country that uses U.S. Government Clouds, which can lead to compatibility issues across multiple geographies. Finally, legacy Government Clouds struggle to maintain parity of patching and features with their commercial cloud equivalents.

Here again it is important to point out a difference in how Google Cloud meets Zero Trust and FedRAMP requirements. A government cloud is a destination, a place where agencies can securely share and analyze data. Google Cloud does not segregate commercial and government cloud users into distinct environments because by design, the entire private network is inherently secure. For example, all data is encrypted by default at rest, and all service-to-service traffic is encrypted by default as well. These kinds of qualities are what Google refers to as “Assured Workloads,” and allows agencies to leverage the power of the commercial cloud while enjoying the security of a government cloud.

Every cloud platform needs to meet agency requirements for FedRAMP, as well as security regulations and standards like HIPAA and PCI DSS. Some CSPs offer some FedRAMP High and other compliant services. Google in this respect is ahead of the market, in that its solution offers FedRAMP High and other services at the level federal agencies need to be compliant and secure today.



How do you think about your cloud strategy from a fiscal perspective?

Every organization, whether in the public or private sector, seeks to maximize the value of their investments and paid services. For private companies, this may be motivated by cost avoidance, but with federal agencies, the challenge is to use a finite budget to access the most value from cloud offerings, whether it is with one provider or several.

A philosophy of FinOps moves in this direction. The cloud landscape is complex, with a multitude of cloud architectures, vendors, and pricing. One consequence of this complexity is that traditional IT financial management models may not deliver the cloud spend optimization federal agencies are seeking. What's needed is a deeper understanding of cost across platforms and vendors and a strategy that reduces cloud spend waste and aligns usage, capabilities, cost, and ROI.

Ultimately, agencies are called upon to think fiscally about their cloud platform decisions, and in this, Deloitte can help. Our Cloud FinOps Services help federal clients drive cost efficiency in the cloud. Working with Deloitte, we help you understand your cloud needs and spend, develop a customized cloud FinOps model to guide your decisions and investments, and align your FinOps maturity with broader agency strategy and goals. As a result, agencies can improve resource visibility across a multi-cloud environment, enjoy visibility into cost allocation at the resource level, and identify new opportunities for cloud and cost efficiency.

The path ahead for federal cloud computing

The data future for federal agencies is in the cloud, and the three pillars of a mission-enabling, value-driving CSP can help organization leaders sort through their needs and make clear-eyed decisions on which platforms are best suited to their priorities for speed, security, and budget. Deloitte works with a range of hyperscale cloud providers, and Google Cloud is one trusted solution.

Importantly for federal customers, the Google Cloud network can accommodate a multi-cloud strategy, leveraging its network backbone to fuel a variety of services and tools from across the cloud marketplace. From a budgetary perspective, it is worth noting that Google offers a straightforward onramp for its cloud platform services, with flexible service pricing for cloud adoption.

Whether you select Google Cloud as your primary provider or as part of a multi-cloud approach, Deloitte brings the people and capabilities that can help you succeed in transforming to a modern cloud. Our government cloud services help agencies meet the challenges and opportunities in data modernization, workforce transformation, cloud migration, multi-cloud management, and data security and compliance. With deep domain knowledge, systems integration, and tax and audit services, we help government clients identify the key priorities and challenges in their cloud strategy, take a fiscally minded approach to evaluating CSPs, and position the agency for cloud computing that is fast, secure, and in line with budgetary realities.

Deloitte's services include support and trusted advice in areas including:

Moving to the cloud

We help you assess your IT and data infrastructure to create a migration and transformation strategy that minimizes risk and disruption. As a part of this, we help you manage and configure your environment for either a single- or multi-cloud solution.

Multi-cloud strategy

Maximizing value in a multi-cloud environment takes a strategic approach anchored in efficiency, security, and compliance. We help you establish a unified approach for managing multiple clouds, and we can supplement your capacity with cybersecurity and compliance monitoring.

Change management

We help you identify the skills and capacity you need to use the cloud in a compliant and secure way. This includes learning plans and upskilling programs that prioritize future capability sets.

Security and regulatory excellence

Agencies face different priorities and goals with their data. We help you develop an integrated cloud security strategy with controls built into the platform.

Federal agencies have an opportunity today to chart their cloud journey and transform to a truly data-driven organization.

The advantages and ROI, the expectations for security, and the capacity to work with growing data volumes are all compelling forces for change. With a robust network and cloud platform, like Google, the path to a modern data environment is within reach.

Contacts

Paul Baliff
Managing Director
Deloitte Consulting LLP
pbaliff@deloitte.com

Michael Coene
Senior Manager
Deloitte Services LP
mcoene@deloitte.com

Aaron Weis
Managing Director
Google Public Sector
Contact here