Conquer Your Share of Security in Government Cloud Migration

In June 2019, the Office of Management and Budget released Cloud Smart, an update to the Government's Legacy Federal Cloud Computing Strategy, known as Cloud First. The purpose of this updated strategy is to offer agencies a roadmap to cloud implementation through insights from public and private sector use cases. In an effort to support the Administration's efforts to modernize Federal IT, the strategy outlines three pillars necessary for successful cloud adoption: security, procurement, and workforce. While Cloud Smart and FedRAMP have set standards to help mitigate cloud barriers and accelerate IT modernization, significant security and workforce roadblocks persist.

The solution? A shared security model with custom capabilities to align with your agency's unique needs. The shared security model sets clear responsibilities for both the cloud service provider and the customer – leaving no room for confusion or gaps in security. This paired with training, management, and monitoring offerings from cloud service partners makes cloud migration a sensible solution.

What's stopping agencies from reaping the benefits of cloud computing and how can the shared security model alleviate cloud concerns?

Cloud Concerns – Improved but Not Perfect

As a pillar to cloud success, security remains a major concern for agencies. The public sector is working tirelessly to discover and implement solutions that will help agencies handle their growing data sets while combatting evolving cyber threats. Historically, agencies have relied on the security of costly legacy on-premise systems and strategies that struggle to keep pace with Federal IT modernization efforts. Some fear the transition from data centers to cloud will result in less access and protection of agency data. Now, the Cloud Smart strategy is encouraging agencies to add protections into the data, network, and physical infrastructure layers. This defense-in-depth approach makes it harder for modern cyber adversaries to access sensitive and mission critical data and increases the operational burden.

Additionally, agencies who are embracing the cloud are faced with an added and unavoidable challenge – the workforce skills gap. The problem is twofold: reskilling the existing internal cyber workforce and developing a program to attract the next-gen cyber ready workforce. Current employees often lack tailored knowledge to facilitate and support the migration to the cloud. As a result, agencies must spend their limited time and resources developing a skills gap analysis to identify possible deficiencies – and implementing skill development plans – further delaying cloud implementation.

From Interest to Action – Operationalizing Shared Responsibility and Hybrid Cloud

Now more than ever, the public sector is embracing hybrid cloud environments and the shared security model. The proof is in the numbers – 93% of government IT professionals report taking steps towards data center modernization[1]. However, there is no one size fits all approach to public sector cloud use, especially when organizations find themselves at varying stages of implementation and experience. The process of building custom solutions that fit an organization's unique needs and mission goals is anything but simple.

The shared security model's collaborative approach establishes clear responsibilities – the provider, such as AWS, monitors and supports its infrastructure to ensure total security of the "cloud" itself, composed of the hardware, compute, storage, networking, and facilities. But Federal agency customers are fully responsible for the security of their platforms, applications, and most critically, the data itself. Agencies aiming to manage these responsibilities with a defense-in-depth approach must custom-fit capabilities to suit their specific environment. But with the myriad solutions available, many agencies are left wondering how to do exactly that – and operationalize shared security. What capabilities and services need to be built in to their architecture and why?

The AWS Marketplace, a digital catalog with thousands of software offerings available to test, buy, and deploy, has streamlined procurement and supported joint domain solutions on the AWS cloud. Agencies can easily browse solutions while enjoying flexible pricing options and multiple deployment methods. As a Premier Consulting Partner and Public Sector Distributor, customers can purchase software solutions directly from DLT in the AWS Marketplace.

Red Hat Solutions offerings, for example, create efficiencies, eliminate vendor lock-in, and improve service delivery. Red Hat OpenShift helps agencies centralize systems, even in cases where they are operating on both physical servers and virtual machines. A key challenge for agencies in the days ahead will be designing modern hybrid architectures, making sure IT services run efficiently no matter the workload, and providing for seamless integration between operating systems and multiple cloud and on-premise environments. Open cloud solutions like Red Hat on AWS help the public sector remain in control and optimize performance across all clouds.

Returning to the ultimate prerogative – security – as the threat landscape widens and endpoints further proliferate, a greater share of responsibility falls on the agency. Fully capitalizing on cloud-native technologies can provide immediate benefits. Tools like Elasticsearch, available on AWS Marketplace, enable advanced threat hunting capabilities. Centrify's fully-integrated mobile device and app management capabilities track, secure, and manage all devices used to access the cloud. And Veritas NetBackup solutions provide resiliency for sensitive data.

This is just a small section of the cloud services puzzle agencies are tasked with piecing together. No organization can do it alone. Partnering with a government solutions aggregator that leverages deep cross-domain expertise empowers agencies to take advantage of this vast array of cloud-native technologies, tailored specifically to the customer.

[1] https://www.meritalk.com/study/outdated-data-center/

Shared Security Model

Cloud Service Provider Security Responsibilities:

- Facilities
- Compute
- Storage
- Database
- Networking

Agency Security Responsibilities:

- Data
- Platform, Apps, Users
- Operating System
- Configurations
- Encryption

DLT + AWS = The Path Forward

No matter where you are in your cloud journey, whether just starting or born in the cloud, DLT has the knowledge and insights to guide public sector organizations to success. DLT and its industry partners aid customers in designing, implementing, securing, and managing cloud environments that specifically meet mission needs — no matter how small or large the project. DLT offerings are built to complement AWS' proven framework, increasing customer benefit, satisfaction, and productivity.

DLT's team of AWS-certified technical experts bring unmatched industry experience with more than 5,000+ cases a year and sport a 98% customer satisfaction rating. Their premier technical services deliver a cloud environment that fits the unique needs of any customer with the ability to rapidly procure IT services, scale up/down as needed, and release when finished.

To learn more, please visit:
https://www.dlt.com/government-products/amazon-web-services#tab-771-3.