

Aerospace Startup Provisions its AWS GovCloud Security, Compliance, Growth

START DATE

March 4, 2021

END DATE

March 30, 2021

CHALLENGE

A growing aerospace startup requested assistance maintaining ITAR compliance and anticipating the need to scale processing efforts on short notice in the middle of a test campaign. Although an AWS GovCloud account was approved, the next steps – maintaining its existing compliance posture and configuring AWS GovCloud – were complicated by the lack of personnel required to work with massive data sets.

SOLUTION

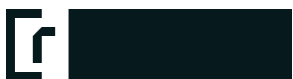
To overcome security infra-structure challenges of a rapidly scaling startup, this aerospace company partnered with [redacted] to leverage its team of elite security and IA experts. [redacted] started the engagement by investigating the company's security policies, resources, and compliance requirements.

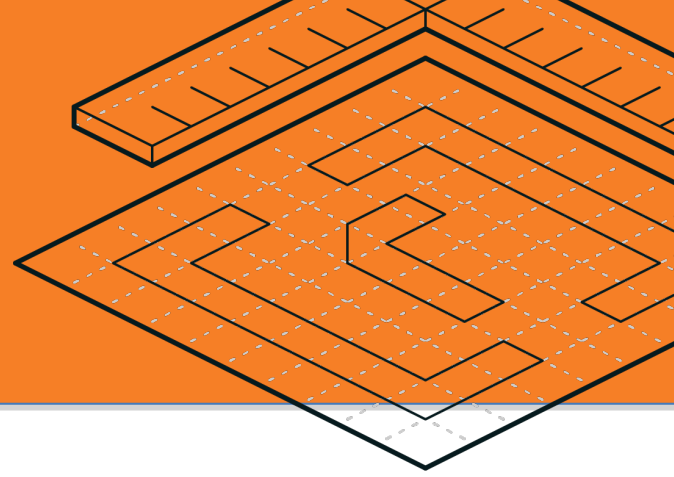
[redacted] provided detailed technical advice to meet these requirements and direct support to implement and validate the startup's AWS GovCloud environment. [redacted] helped get the startup's efforts aloft, allowing it to address immediate data processing needs and begin longer term AWS GovCloud tenancy maintenance/disaster recovery.

Because of the volume of data requiring processing and sensitivity of the data, [redacted] used an AWS

Snowball as a component of the solution to provide ITAR-compliant data transfer into the cloud. This allowed for a smooth transfer between cloud and on-premise resources, keeping the company's network connected for its ongoing work.

"[redacted] has been nothing but professional and has gotten us the detailed, security-focused advice we needed." - CIO





[redacted] Security Engineering Solution

INTEGRATING AWS BEST PRACTICES AND ITAR COMPLIANCE

While AWS provides several deployment templates to constitute a security system from the ground up, the challenge is to leverage existing efforts and policies to enable a path forward.



AWS GovCloud is a FedRAMP High- and Moderate baseline capability that enables ITAR compliance.



AWS Identity and Access Management is a powerful tool to implement roles and role separation and is a fundamental component of meeting regulatory compliance.



AWS CloudTrail established the required auditing trail guaranteeing visibility into all accounts for compliance and security.



AWS S3 to provide secure storage, specific to properly (and securely) manage encryption keys and access roles.



AWS Snowball provided a high-bandwidth, secure upload capability that effectively shipped itself.

NAVIGATE SHARED RESPONSIBILITY

Much of the ability to provide secure, compliant solutions was a function of leveraging the AWS Shared Responsibility Model. In this way, the aerospace startup was able to further benefit from the resources it was paying for by using them in an already approved- and recommended manner, additionally easing compliance.

OUTCOME DELIVERED ON TIME

In this case study, there was an immediate need to process data for answers, an issue that faces many aerospace companies. Processing needs climb and descend rapidly – often in the middle of a major testing campaign – and the solution outlined was delivered efficiently, torn down efficiently, and remains ready for the next campaign without having to keep and to maintain expensive resources.

I appreciate having [redacted] as part of the team and I'm looking forward to getting [redacted] more integrated.
- CIO

