SAIC AWS Migration

Public Reference Case Study 2

Our customer develops and maintains a mission-critical, multi-tier web application for tracking communications assets used for emergency response planning. The customer deployed the application using an on-premise technology silo, and the application runs on legacy hardware and software. After a compliance review, the customer needed to address security findings in order to continue operating the application. In addition, a new FISMA compliance policy required a FedRAMP-certified data center with NIST SP 800-53 Moderate security controls to host the application.

Given the quick turnaround to fix the security findings and meet new policy requirements, SAIC proposed a migration strategy to rehost the application in AWS GovCloud and refactor it to take advantage of cloud-native services and line it up with a long-term technology vision. We also helped our customer obtain the needed Authority to Operate (ATO).

We used our Cloud Migration Edge (CME) reference framework and AWS Architecture best practices to assess, architect, design, and implement the application migration effort. CME provides migration process guidelines, industry best practices, and repeatable tools and techniques that accelerate cloud migration efforts at lower risk and cost while providing value-added outcomes.

SAIC successfully migrated the customer's application to AWS GovCloud on time and within budgetary expectations. After obtaining the ATO, we helped the client gain operational efficiencies by incorporating cloud automation techniques for the application.

SAIC
Redefining Ingenuity