CASE STUDY

Transform System Security, Streamline Processes, and Automate CI/CD Flow with AWS

softserve

Build a FedRAMP compliant environment, enhance security protocols, improve multi-account setup, and automate processes using Landing Zone, AWS Control Tower, and AWS Organizations.

While cloud security is essential to any company working in the cloud, it's especially paramount for healthcare. If you're dealing with people's sensitive personal and health data, you want to ensure that your system is secure. Our client—a global virtual healthcare technology company—wanted to expand its business into the governmental sector. To do that, they needed to ensure an even higher level of cloud security protocols than before.

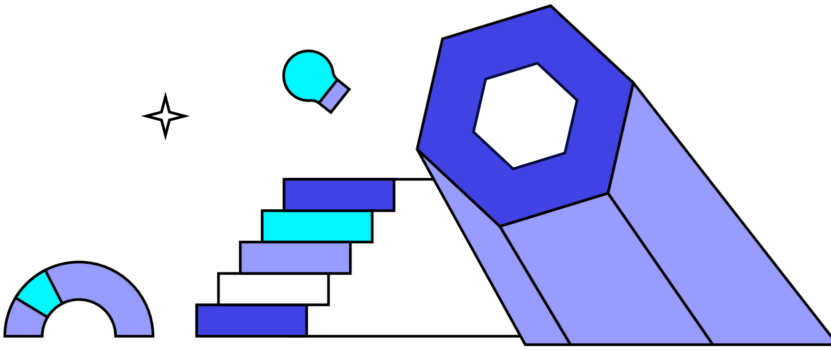
When working with the government and providing cloud-based services, one of the best ways to meet their high level of standards and security is to obtain a FedRAMP Authorization. FedRAMP is a U.S. government program that "provides a standardized security framework for all cloud products and services" and is recognized by all federal agencies within the executive branch.

To ensure their solutions and services met this standard, our client approached SoftServe to help build a FedRAMP-compliant cloud environment and CI/CD flow. The client also wanted to improve overall multi-account and multi-region usability, repeatability, and consistency, as well as create centralized networking, security, and logging solutions.

Having previously designed and implemented greenfield concepts to enhance security, automate and standardize processes, and improve customer workloads, our SoftServe team was confident that they could handle this project.

Our experts knew that this type of setup required a Landing Zone—a well-architected AWS Organization structure that allows multiple customizable AWS accounts and organizational units. They also knew that AWS Control Tower was the best way to create this Landing Zone. To deliver on the client's goals, such an environment also required a hybrid cross-region network setup with on-premises data centers and a large set of guardrails and Service Control Policies (SCP). Lastly, the client needed a centralized AWS security services-integrated logging solution to best comply with the FedRAMP security program protocols.

Once our SoftServe team understood the size and scope of this project, they divided it into three phases.



In the first phase, SoftServe built out the greenfield multi-account AWS environment. This ensured that the framework complied with the FedRAMP security standards from the very beginning. To start, our experts created a Landing Zone managed by AWS Control Tower. Using the Control Tower customization orchestrator, CloudFormation templates, and AWS security control policies, our team customized the Landing Zone baseline to provide each new AWS account enrollment a set of AWS resources and services.

Having routinely partnered with AWS, our experts know that AWS Organizations—a service that lets you centrally manage multiple accounts—is the foundation of a well-architected multi-account environment. The Landing Zone built by the SoftServe team required a proper AWS Organization and nested accounts structure that included centralized logging, security, and networks, a management account, and more.

As the SoftServe engineers were constructing these elements, they realized that the client needed a complex network topology as well. At the time, the client's network account contained shared VPCs and was meant to centrally manage the network components. In order to improve security and usability, our team of experts established complex network connections between AWS VPCs, branch offices, and on-premises servers using AWS Transit Gateway (TGW), VPN, VPC endpoints, edge routers, and multiple other components.

Since the highest levels of security were needed to meet the FedRAMP standards, SoftServe integrated numerous components into the Landing Zone that would automatically deploy with each new AWS account. First, the AWS Security Hub and AWS GuardDuty services were set up on the AWS Organization with an administrator/member relationship. AWS Security acts as an administrator and serves as a central place for security management. All other accounts are considered member accounts and therefore cannot disassociate themselves from the administrator account, ensuring the same level of security throughout.

Next, an AWS Logging account was provided as a central place for storing various logs from different accounts, such as AWS data and management logs like AWS CloudTrail, VPC flow logs, DNS, and more. A set of SCPs that met the FedRAMP requirements were also implemented, meaning the system would deny unused regions and services or non-compliant parameters and options as security measures.

The SoftServe team also created a custom AWS Config Conformance Pack that included both FedRAMP and Control Tower rules and deployed it across the entire organization. Lastly, they integrated the AWS Single Sign-On (AWS SSO) service with the client's OKTA identity provider. This synchronized with the client's Active Directory and enabled a single user management system at the organization level, allowing only SSO users login access to the AWS Console.

After all of these services and systems were built and implemented, the second phase of this project focused on enhancing and automating the client's CI/CD approaches and pipelines. Using the Infrastructure as Code guiding principles, our SoftServe experts established the necessary application infrastructure resources with Terraform code in conjunction with Terragrunt. In addition, they introduced a specific Terraform/Terragrunt repository structure.

The client's CI/CD was then improved using GitOps practices and immutability principles and orchestrated using Jenkins pipelines and Terraform code. The Jenkins pipeline bakes Packer AMI images and then uses AWS KMS keys to distribute them across different AWS accounts. It also creates docker images which Terraform delivers, deploying them into AWS EKS as Helm charts.

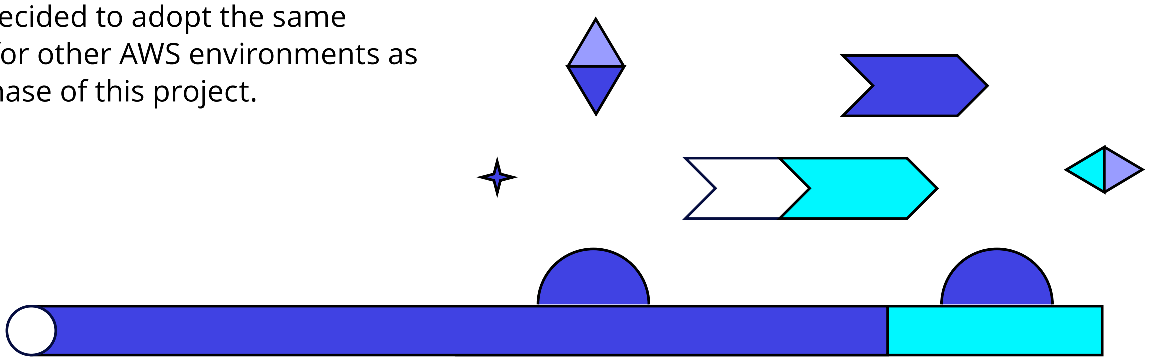
Lastly, our SoftServe engineers enhanced the security of the client's Kubernetes services by introducing AWS IRSA model (IAM Roles for Service Accounts) on AWS EKS clusters.

After all of that, the client was so impressed with the process and systems improvements and the enhanced security, that they decided to adopt the same principles for other AWS environments as the final phase of this project.

Ultimately, SoftServe successfully customized AWS Control Tower and delivered a complex yet well-defined AWS Organization and account structure. This structure included greenfield repeatable environments based on the Landing Zone concept and best practices. Our experts designed and implemented network components, configured AWS security services, and centralized security controls, ensuring all information was safe and secure. Finally, we improved our client's CI/CD workflows and GitOps practices. Each of these elements led to our client having a FedRAMP compliant AWS setup, paving their way to achieve the FedRAMP certification for their products as they venture into the government sector.

SoftServe's experience and expertise combined with AWS products and services meant that our client could expand and scale their global virtual healthcare technology business, reassured that their environment met the highest security requirements.

LET'S TALK about how SoftServe can help meet your toughest inventory challenges using AI/ML, big data, and cloud solutions.



ABOUT SOFTSERVE

We are a digital authority made up of advisors, engineers, and designers who deliver innovation, quality, and speed to elevate and accelerate our clients' digital journeys.

Our approach is built on a foundation of empathetic, human-focused experience design that ensures value and continuity from concept to release.

WE IDENTIFY WHERE YOU ARE.

WE PREPARE YOU FOR THE ROAD AHEAD.

WE TAKE YOU WHERE YOU NEED TO GO.

Visit our **website**, **blog**, **LinkedIn**, **Facebook**, and **Twitter** pages.

NORTH AMERICAN HQ

201 W 5th Street, Suite 1550
Austin, TX 78701
USA +1 866 687 3588 (USA)
+1 647 948 7638 (Canada)

EUROPEAN HQ

30 Cannon Street
London EC4M 6XH
United Kingdom
+44 333 006 4341

info@softserveinc.com
www.softserveinc.com

softserve