CTAC Managed Services for a Federal Multi-Tenant Cloud Enclave

CTAC Managed Services for a Federal Multi-Tenant Cloud Enclave

Customer Overview:

CTAC was contracted to support a federal health agency which is charged with producing evidence to make healthcare safer, higher quality, more accessible, equitable, and affordable. The agency supports a diverse portfolio of research programs, data platforms, digital tools, and public-facing information systems that serve policymakers, researchers, clinicians, and the public.

To support this mission, the agency operates multiple digital platforms and applications that vary in scale, sensitivity, and usage patterns, including public websites, research data systems, analytics platforms, and internal collaboration tools. These systems must operate securely and reliably while meeting federal cybersecurity, privacy, and accessibility requirements. Many of these workloads are subject to heightened scrutiny due to the nature of healthcare data, research integrity, and federal compliance obligations.

The agency required a cloud operating model that could support **multiple independent programs and systems simultaneously**, while maintaining strong security boundaries, centralized governance, and consistent operational oversight. This necessitated a managed services approach capable of scaling across tenants without duplicating infrastructure, tooling, or operational effort.

Customer Challenge:

The agency faced the challenge of operating and securing a growing portfolio of cloud-based systems across multiple programs, each with distinct requirements, stakeholders, and lifecycle timelines. Traditional, siloed hosting approaches increased operational complexity, duplicated tooling, and made it difficult to enforce consistent security and compliance controls across environments.

The agency required a solution that could provide centralized security and governance while allowing individual programs to operate independently within isolated environments. This included the need for strong ingress controls, identity and access management, network inspection, and compliance enforcement aligned with federal standards such as FISMA, the NIST Risk Management Framework, and agency specific security policies.

The agency required continuous operations, proactive monitoring, and disciplined change management to support production systems without service disruption. The agency needed a long-term partner capable of operating a shared, multi-tenant AWS environment, delivering 24×7 managed services, and supporting ongoing modernization without increasing operational risk or administrative burden on program teams.

Proposed Solution:

CTAC serves as a trusted partner for AWS hosting and full-lifecycle managed services, operating a secure, multi-tenant cloud enclave designed to support multiple federal programs within a single, governed AWS environment. CTAC provides end-to-end responsibility for the platform, including infrastructure operations, security and compliance management, shared services, and continuous optimization.

The solution is built around a **centralized security enclave and shared services model**, with individual federal program workloads deployed into isolated tenant VPCs. This approach

enables CTAC to apply consistent security controls, monitoring, and operational processes across all tenants, while preserving strict separation between systems.

CTAC operates and maintains the enclave as a continuously available service, supporting onboarding of new tenants, day-to-day operations, system enhancements, and compliance activities without disrupting existing workloads. This model allows the agency to scale its cloud footprint efficiently while maintaining strong governance and operational consistency.

The agency's AWS environment is implemented using a **hub-and-spoke, multi-account architecture** anchored by a centralized security enclave. Ingress traffic is routed through Zscaler and Okta for identity, authentication, and secure access, followed by inspection through Palo Alto firewalls deployed within the enclave. AWS Transit Gateway provides controlled routing between the enclave and individual tenant VPCs, enabling centralized enforcement of network and security policies.

Each federal program operates within its own tenant accounts, attached to the enclave through dedicated Transit Gateway attachments. This design ensures strong isolation between tenants while allowing shared access to centralized services such as monitoring, logging, security tooling, and DevSecOps capabilities.

From a tenant perspective, application workloads are deployed across multiple Availability Zones using private Application Load Balancers, Auto Scaling Groups, and AWS-managed services. Public access is provided through Amazon CloudFront with AWS WAF protection, while application and administrative access remains restricted to private networks.

Managed Services Delivery:

The agency's multi-tenant enclave leverages AWS-native services to deliver scalability, security, and operational visibility across all hosted systems. CloudFront and AWS WAF provide secure, globally distributed access to public-facing applications, while private Application Load Balancers route traffic to application tiers within tenant VPCs.

Compute workloads are deployed using Amazon EC2 within Auto Scaling Groups to support elasticity and high availability. Shared storage and state management are provided through services such as Amazon EFS, Amazon RDS configured for Multi-AZ availability, and in-memory data services where appropriate. Static content, logs, and backups are stored in Amazon S3 with encryption and lifecycle policies.

Centralized monitoring and security visibility are achieved through services including Amazon CloudWatch, AWS CloudTrail, AWS Config, GuardDuty, and AWS Security Hub, which aggregate telemetry across the enclave and tenant environments. CI/CD pipelines leverage GitHub and Amazon ECR to support standardized build and deployment processes across tenants.

This AWS architecture enables CTAC to operate multiple independent systems within a single, governed environment while maintaining availability, security, and compliance at scale by leveraging IaC and Terraform.

CTAC provides **24×7×365 managed services** for the federal enclave and all tenant environments, assuming full responsibility for ongoing operations, maintenance, and continuous improvement. Services are delivered through standardized service management processes designed to ensure consistent availability, security, and compliance across all tenants.

Operations are supported through CTAC's deployed Engineering Team, which provides centralized monitoring, alerting, incident response, and coordination. Infrastructure, application performance, logs, and security telemetry are monitored continuously, enabling proactive detection and resolution of issues before they impact federal systems or users.

Incident response follows escalation paths, and change control procedures to minimize risk and service disruption.

Routine operational activities include operating system and application patching, vulnerability remediation, configuration management, backup and recovery operations, and capacity planning. CTAC also manages tenant onboarding and lifecycle activities, ensuring new systems can be introduced into the enclave efficiently and securely without impacting existing workloads.

DevSecOps and Continuous Improvement:

CTAC applies DevSecOps practices to integrate security, reliability, and operational controls throughout the lifecycle of systems hosted within the enclave. Infrastructure and application components are managed using Infrastructure as Code and automated CI/CD pipelines, enabling consistent provisioning, controlled deployments, and auditable change management across tenants.

Security and compliance requirements are embedded into delivery workflows through configuration validation, vulnerability scanning, and defined promotion gates between development, staging, and production environments. Operational telemetry, incident data, and security findings are reviewed regularly and incorporated into backlog prioritization, infrastructure tuning, and process improvements.

This continuous improvement model enables CTAC to evolve the enclave and tenant environments in response to changing security requirements, workload demands, and agency priorities, while maintaining stability and compliance.

Results and Outcomes:

Through its managed services engagement, CTAC has enabled the agency to operate a **secure, scalable, and resilient multi-tenant cloud environment** that supports a diverse portfolio of healthcare research and digital systems. The shared enclave model has reduced infrastructure duplication, improved consistency of security controls, and simplified operational management across programs.

Centralized monitoring, standardized operations, and disciplined change management have strengthened system stability and security posture while supporting ongoing compliance with agency specific and federal requirements. The ability to onboard and operate multiple tenant systems within a single governed environment has improved operational efficiency and reduced time to deploy new capabilities.

Most importantly, CTAC's managed services model allows the agency's program teams to focus on research, data analysis, and mission outcomes, while CTAC ensures that the underlying cloud platform remains reliable, secure, and continuously optimized.

Conclusion:

The agency's multi-tenant AWS enclave represents a complex, high-value cloud operating environment that demands continuous availability, strong security, and disciplined governance. Through its role as an AWS Managed Service Provider, CTAC delivers the operational rigor, security expertise, and cloud engineering capabilities required to operate this environment at scale.

This engagement demonstrates CTAC's ability to deliver **full-lifecycle AWS managed services** across multiple tenants and programs, combining centralized security and shared services with isolated, high-availability application environments to support long-term mission success.