sequoia
Classified Cloud Experts

RGS
Rancher Government Solutions

Solving Cloud Migration Challenges for Classified Environments

Migrating applications across the air-gap to classified cloud environments is not a simple lift-and-shift operation. Software written for commercial cloud environments often fails when deployed to classified clouds due to technical barriers, security policies, and workforce limitations.

Sequoia Holdings, LLC. (Sequoia) provides a sandbox environment through its Combine solution that emulates classified cloud regions, proactively identifying code violations and accelerating secure migration. Rancher Government Solutions (RGS) delivers secure-by-default Kubernetes management for seamless containerized deployment. Together, Sequoia and RGS provide a trusted, scalable, and mission-ready solutions for the Department of Defense, Intelligence Community, and civilian agencies.

The Cloud Migration Challenge

Development teams may rigorously test software in a commercial cloud only to find that it fails upon deployment to a classified region. Identity and access management (IAM) policies vary, critical services are missing or restricted, and strict security controls prevent external dependencies. Without early visibility into these differences, agencies and contractors waste valuable time troubleshooting, refactoring code, and working through compliance issues.

Unlike commercial clouds, classified environments are air-gapped, preventing access to the internet, external APIs, or cloud-based authentication services. Service parity is also inconsistent, with missing or modified services impacting functionality. Endpoint structures differ, requiring costly and manual configuration to align with high-side constraints. Without an accurate pre-production environment, agencies risk:

- Costly deployment failures
- Security vulnerabilities
- Significantly delays in mission operations

The Sequoia + RGS Advantage

Sequoia and Rancher Government Solutions bring together decades of expertise in classified cloud migration and Kubernetes management. Sequoia Combine acts as a digital twin, replicating classified environments in a commercial setting so developers can test and fix issues before deployment. RGS powers secure Kubernetes with government-grade security for seamless operations and workload orchestration across commercial and classified clouds.

Together, they solve a problem no other tool can—ensuring cloud applications built in commercial environments can deploy successfully in air-gapped, classified regions without last-minute failures or security risks.

Without Sequoia Combine, teams deploying to classified environments are forced to throw code over the fence and hope it works. Combine eliminates the guesswork so teams can migrate with confidence.

Core Capabilities

- **IAM Policy & Access Control Replication** – Simulates classified IAM structures, including role-based access controls (RBAC), CAP API integration, and hierarchical user permissions.
- **Service Parity Enforcement** – Restricts development environments to only those services and configurations available in classified cloud regions.
- **Air-Gapped CI/CD Support** – Enables DevSecOps pipelines without reliance on external internet access, mirroring software repositories and enforcing security constraints through Rancher Government Hauler for fully isolated software deployment.
- **Software Supply Chain Security** – Integrates Rancher Government Carbide™ for automated vulnerability scanning and generation of SBOMs to protect against threats.

- **Endpoint Emulation & API Compatibility** – Replicates classified cloud endpoints, intercepts misconfigured API calls, and allows for proper government certificate authority integration.
- **Day-2 Kubernetes Operations** – Automates certificate rotation, encryption key management, snapshot rollbacks, and cluster scaling through STIGATRON, a tool within Rancher Government Carbide™, simplifying the lifecycle management, including Amazon EKS integration.
- **STIG-Compliant Kubernetes** – Deploys Rancher RKE2 and K3s clusters that meet DISA STIG and federal compliance mandates out-of-the-box.
- **Multi-Cloud & Hybrid Ready** – Supports AWS C2S, SC2S, Azure Secret, Oracle OCI, and hybrid on-premise/cloud environments.
- **Zero Trust Integration** – Enforces strict authentication and network segmentation.

Mission Use Cases

- **Multi-Cloud Deployment** – Enable secure workload portability across C2E, JWCC, and hybrid cloud environments.
- **Low-to-High DevOps Pipelines** – Develop in commercial cloud, then deploy to classified cloud securely.
- **Edge Computing for Defense** – Supports tactical deployments, AI/ML workloads, and DevSecOps at the edge.
- **Day 2 Kubernetes Operations** – Automates certificate rotation, encryption key management, scaling, and security compliance.
- **Air-Gapped DevSecOps** – Secure deployment & compliance automation in classified, isolated environments.

Accelerate Your Software Delivery to Restricted Cloud Regions

Sequoia Combine and Rancher Government Solutions deliver unmatched security and automation for classified cloud migrations. With Sequoia's digital twin environment and RGS's government-grade Kubernetes management, agencies can confidently deploy mission-critical applications.

Ready to accelerate your cloud migration? Let's talk.

Contact our team at info@ranchergovernment.com or 844.RGS.7779 to learn more.

Why RGS & Sequoia Combine?

Built for National Security

Trusted by DOD, IC, and Federal agencies.

End-to-End DevSecOps

Securely migrate, deploy, and manage mission applications.

Cloud-Agnostic & Secure

Multi-cloud support for AWS, Azure, and Oracle classified regions.

Continuous Compliance

Rancher Government Carbide™ locks down software supply chain security.

RGS Rancher Government Solutions | sequoia Classified Cloud Experts