LSA DIGITAL
Lean Scaled Architects

CASE STUDY

ZERO-TRUST CLOUD SERVICES FOR USER FRIENDLY, FASTER RESEARCH

CONTEXT

The US Air Force Research Labs needed a secure Hybrid Multi-Cloud solution to do everything from basic office document sharing to supporting faster research and data-intensive experiment analysis, and wanted to see fast results to show value for their investment.

CLIENT CHALLENGE

In the case of USAF Research Labs, there were key use cases that demanded various cloud environments:

- Existing CloudONE and DoD Microsoft Office environments allowed workloads at various security levels (e.g., IL5/ITAR, IL6, TS, etc.) but were not flexible enough to support more flexible collaboration tools between researchers, for basic 6-1 research.
- Researchers wanted to do fast experiments that needed secure cloud scaling capabilities using IL/4 data, with the option to spin up Virtual Private Clouds (VPC's) as needed for lower-level infrastructure support
- Cloud developers needed a way to build and deploy secure infrastructure to deliver researcher services - preventing both security vulnerabilities and configuration mistakes

SNAPSHOT

Hybrid Multi-Cloud, Zero Trust & Google Cloud

US Dept of Defense

GCP native tools, GitOps, Terraform

PAIN POINTS

- Researchers needed a way to perform fast, flexible research experiments, up to "petabyte events"
- Zero-trust security assurance was needed to safeguard information, both inside and outside the perimeter

RESULTS

- Improved collaboration both inside and outside AFRL, using Zero-Trust context-based security controls
- A better UX for researchers with "service-oriented" landing zones
- Declarative infrastructure configuration approach for traceability and fewer "mistakes"
- Automated, secure DevSecOps with GitOps

LSA DIGITAL
Case Study

WHAT WE DID

Multi-Cloud Landing Zone Ecosystem. At a high level, working towards a zero-trust principled approach, we used DoD Zero Trust Reference Architecture guidance to architect a flexible (but not over-built) HMC solution. We conducted UX research to understand the needs of researchers, and — working with other contractors responsible for cloud environments — we focused on high-level HMC authentication & authorization frameworks and approaches, paired with landing zones to present a more user-friendly "service" perspective that researchers needed. Researchers could use common, lower-cost services when necessary, and then had options for leveraging cloud environments that could accommodate their specific workloads.

Change Management & Governance. At a more detailed level, we architected, designed, implemented, and maintained a Google Cloud Platform (GCP) for researchers to accommodate basic 6-1 research and flexible collaboration services (first at IL/4, then scaling to IL/5 when sufficient security controls were in place and approved). We accomplished this with automated Infrastructure-as-Code (IaC) that uses a declarative Terraform configuration, rather than imperative approach (i.e., manually changing configuration at runtime). This declarative approach ensures that configuration changes are approved according to a governed process within the configured code base -- instead of relying on humans to manually change configuration, which can result in small configuration mistakes, or big mistakes from mis-interpreted policy. This ensures accountability and – at the same time, built-in documentation for the entire cloud infrastructure, to track changes over time.

GitOps Secure Continuous Delivery Pipeline. The GCP terraform code and other components were managed in a fully automated GitLab pipeline (including with automated code & container scanning), leveraging the GCP API for automated infrastructure code deployment.

Zero Trust. In TIC 3.0, it is recognized that the definition of "trust" may vary across specific computing contexts and that agencies have different risk tolerances for defining trust zones. The TIC 3.0 Security Capability Handbook recognizes Policy Enforcement Point (PEP) Security network-level capabilities can be applied to multiple PEPs. For example, for the GCP cloud platform, we leveraged PEP capabilities to implement the following NIST 800-207 use case: A single headquarters and one or more geographically dispersed locations that are not joined by an enterprise-owned physical network connection. Employees may be teleworking or in a remote location and using enterprise-owned or personally owned devices.