



Building a scalable turnkey solution for multi-cloud PAM governance

Our multi-cloud PAM solution for a cabinet-level agency delivered significant results and established a scalable model for the federal government.

Background

Easy Dynamics partnered with a cabinet-level agency (CLA) to address one of its most complex modernization challenges: Securing privileged access across a rapidly-expanding multi-cloud ecosystem supporting more than 100,000 users. Workload migrations and new builds across disparate cloud environments had fragmented privileged access, intensified compliance demands, and decentralized identity governance. The agency needed more than just a tool; it required an enterprise shared service capable of enforcing NIST SP 800-53, FISMA High, and CISA SCuBA requirements while accelerating cloud adoption. With no consistent PAM baseline in place, our team set out to design a unified architecture aligned to CLA's ICAM strategy and zero trust objectives.

The Challenges

Fragmented Multi-Cloud Privileged Access

CLA had a growing multi-cloud environment across Azure, AWS, GCP, OCI, and on-prem VMware, but privileged access was decentralized and inconsistent.

Manual, Inconsistent Compliance

Compliance relied heavily on manual configuration, manual validation, and after-the-fact evidence gathering.

Configuration Drift and Inconsistent Security Baselines

CLA lacked the ability to launch a cloud environment with secure, pre-hardened, repeatable configurations.

Slow Onboarding and Duplicated PAM Efforts

Organizations across the agency were burdened with building or maintaining their own separate, secure PAM capability.

Our Solution

Working across CLA's governance bodies, cloud working groups, and the CIO Council, Easy Dynamics helped drive consensus around a hub-and-spoke architecture anchored in Microsoft Entra ID and integrated with the agency's existing ICAM investments, including SailPoint-based identity governance. The resulting solution – Easy Dynamics' Obsidian platform – consolidates provisioning, monitoring, and policy enforcement into a centralized control plane across cloud providers. Unlike traditional PAM implementations that rely on manual configuration, Obsidian embeds security and compliance directly into automated CI/CD pipelines using modular IaC, alongside CISA's SCuBAGear validation tooling. We designed Obsidian for enterprise-wide implementation, deploying consistent security controls across multiple Entra ID tenants, as well as GCP and OCI – providing application teams with inheritable controls they could easily consume and benefit from.

The Measurable Results

Accelerated Deployment Times

Automated Infrastructure-as-Code and CI/CD pipelines reduced privileged environment deployment timelines by

60–70%, accelerating secure cloud adoption across the agency.

Strengthened System Reliability

Standardized baselines and embedded continuous validation delivered >90% reduction in security compliance configuration drift incidents, strengthening system reliability and audit readiness.

Reduced Manual Workloads

Replaced up to 90% of manual configuration and hardening tasks using automation, freeing technical staff to focus on mission delivery rather than compliance administration.

Consistent Security Posture

Reduced average detection time of unauthorized configuration drift of monitored cloud identity systems from multiple weeks to less than one business day.

Supported Continuous Authorization

Real-time dashboards and automated SCuBA compliance validation reduced audit preparation effort by up to 70%, supporting continuous authorization models.

Delivered A Scalable Turnkey Solution

Obsidian established a repeatable model for enterprise-wide, multi-cloud PAM governance that can be adopted and scaled across the federal government.

CONTACT US

Greg Gordon
Chief Delivery Officer
ggordon@easydynamics.com

JJ Harkema
VP Solutions & Partnerships
jharkema@easydynamics.com

FEDERAL EXPERIENCE

- Department of Agriculture
- Department of Homeland Security
- Defense Information Systems Agency
- Defense Logistics Agency
- Naval Special Warfare Command
- Federal Law Enforcement Training Center
- National Institute of Standards and Technology
- Cybersecurity and Infrastructure Security Agency
- Internal Revenue Service
- General Services Administration
- Department of the Treasury
- Health & Human Services
- Social Security Administration
- Department of Education

CORE CYBERSECURITY CAPABILITIES

- Enterprise ICAM
- Cloud Modernization
- Automation
- Zero Trust
- Risk Management

