James Benitez

Cloud Platform Engineer

(703) 555-0186 james.benitez.cloud@example.com
linkedin.com/example/jamesbenitez Alexandria, VA 22314

SUMMARY

Cloud Platform Engineer with 11 years of experience building and operating secure **cloud infrastructure** for federal health programs serving HHS, NIH, and FDA stakeholders. Delivers multi-cloud landing zones across Azure, AWS, and **Google Cloud Platform** through Terraform, Bicep, CloudFormation, **GitHub Actions**, CI/CD, policy as code, and DevSecOps controls. Brings hands-on judgment across identity-first access, network guardrails, DNS, certificates, **secrets management**, telemetry, Zero Trust, compliance reviews, and production support. Known for turning architecture standards into dependable platforms, resolving difficult escalations, and leaving clear runbooks behind. Ready to support Northstar Federal Systems with practical engineering, disciplined governance, and care for mission-critical public services.

EXPERIENCE

Senior Cloud Platform Engineer

HarborPoint Digital Services January 2022 - Present Bethesda, MD

Owns production cloud platform operations for an NIH research services program. Leads landing zone delivery across Azure, AWS, and Google Cloud, translating enterprise architecture standards into secure, repeatable environments. Partners with security, identity, device, and application teams while guiding platform decisions, remediation work, and operational readiness.

- Operated Azure, AWS, and Google Cloud landing zones for NIH workloads, balancing automated provisioning, service availability, **identity-first controls**, **network security**, and agency baselines.
- Standardized Terraform and Bicep modules for subscriptions, accounts, identity roles, network segments, logging, and policy guardrails, giving delivery teams auditable builds without console changes.
- Built GitHub Actions **CI/CD** workflows with linting, unit validation, Terraform plan review, policy checks, and **automated security testing** before production promotion.
- Implemented **Azure Virtual Desktop** host pools for clinical research and administrative personas, linking conditional access, device compliance, profile storage, and least-privilege groups.
- Connected Azure Monitor, AWS CloudTrail, and Google Cloud audit telemetry with SIEM and SOAR workflows, helping teams identify risky changes and suspicious access patterns earlier.
- Directed quarterly reviews against **NIST 800-53**, FedRAMP, and CIS benchmarks, turning findings into remediation plans and refreshed baselines, runbooks, and operating procedures.

Cloud Infrastructure Engineer

CivicCloud Engineering Group June 2019 - December 2021 Rockville, MD

Delivered cloud infrastructure for an HHS modernization program spanning platform foundations, network connectivity, identity integration, release automation, and production recovery. Worked with engineering, cybersecurity, endpoint, and service operations partners to replace manual builds with controlled, reviewable delivery patterns.

- Delivered **Azure** and **AWS** landing zones with hub-and-spoke networking, private endpoints, centralized identity, encryption, and policy enforcement for HHS application teams.
- Replaced ticket-driven builds with Terraform and CloudFormation pipelines, creating reusable modules and approval gates across development, test, and production environments.
- Automated **DNS-as-code** through Route 53, **Azure DNS**, certificate workflows, and Git-managed configuration, reducing release inconsistencies across agency services.
- Developed API and SDK integrations for account provisioning, secrets rotation, monitoring registration, and event notifications using scoped credentials, retry handling, and structured logs.
- Partnered with identity, endpoint, and cybersecurity teams to align **conditional access**, **device compliance**, privileged access, and cloud policy within a practical Zero Trust model.
- Resolved escalated incidents involving routing, identity federation, failed deployments, and certificate expiration, then documented root causes and recovery steps for operations teams.

Cloud Operations Engineer

BlueMesa Federal Technologies August 2017 - May 2019 Falls Church, VA

STRENGTHS

Production judgment
During a difficult identity outage, traced failure across federation and policy layers, restoring access and giving leaders a clear recovery path.

Automation first
Manual builds caused drift on an earlier program. Reusable Terraform modules and review gates became a trusted delivery habit.

Security partnership
Peers sought help aligning device compliance, conditional access, and least privilege when Zero Trust decisions affected delivery.

Clear operations
Runbooks written after recurring incidents helped service desk teams act with confidence instead of waiting for a platform engineer.

Cross-cloud delivery
A shared landing zone pattern kept Azure, AWS, and Google Cloud decisions consistent for teams with different workload needs.

SKILLS

Cloud engineering, Landing zones, Terraform, Bicep, CloudFormation, DevSecOps, CI/CD, Zero Trust, Azure Virtual Desktop, Policy as code, Compliance as code

Incident response

Secrets management

Cloud governance | Federal IT

LANGUAGES

English — Native

Spanish — Proficient

MY CAREER

- Senior Cloud Platform Engineer at HarborPoint Digital Services (4.6 Years)
- Cloud Infrastructure Engineer at CivicCloud Engineering Group (2.5 Years)
- Cloud Operations Engineer at BlueMesa Federal Technologies (1.8 Years)
- Cloud Systems Administrator at Redwood Systems Consulting (2 Years)

Supported production Azure and AWS platforms for an FDA data service, with responsibility for reliable operations, infrastructure automation, security evidence, monitoring, and service desk enablement. Contributed implementation work under established engineering and security direction, keeping platform changes controlled and supportable.

- Maintained Azure and AWS subscriptions, virtual networks, identity assignments, backup configurations, and diagnostic **logging** for an FDA data platform.
- Created **Terraform** modules and **CloudFormation** templates for compute, storage, security groups, and monitoring patterns, improving consistency across six application environments.
- Added GitHub Actions checks for formatting, static security rules, secret scanning, and peer-reviewed promotion through CI/CD pipelines.
- Integrated Azure Monitor **alerts**, AWS CloudWatch events, and service desk notifications, improving triage for capacity, availability, and policy issues.
- Reviewed cloud configurations against **CIS benchmarks** and federal control evidence requirements, recording exceptions and coordinating corrective actions with system owners.
- Maintained diagrams, **configuration baselines**, support procedures, and incident runbooks so service desk staff could resolve routine access and platform issues safely.

Cloud Systems Administrator

Redwood Systems Consulting | July 2015 - July 2017 | McLean, VA

Administered Azure and AWS infrastructure for federal public health applications, supporting identity, networking, virtual machines, storage, backups, monitoring, and secure remote administration. Built early automation practices and supplied migration analysis, troubleshooting, documentation, and change-control support for engineering and security stakeholders.

- Administered **Azure** and AWS infrastructure for public health applications, maintaining virtual networks, virtual machines, storage, backups, **identity** assignments, and secure remote access.
- Introduced **Terraform** and Azure Resource Manager templates for repeatable virtual network, resource group, and monitoring deployments, reducing variation across environments.
- Configured DNS records, TLS **certificates**, firewall rules, and routing changes through documented change controls, supporting reliable application releases.
- Assessed cloud migration options by mapping legacy workloads to managed services, identifying dependencies, and preparing implementation plans for engineering and security review.
- Investigated authentication, connectivity, deployment, and monitoring incidents through **platform logs**, command-line tools, and vendor documentation, restoring service within support procedures.
- Updated architecture diagrams and knowledge articles while applying least-privilege permissions and secure credential handling during daily administration.

PROJECTS

Federal Multi-Cloud Landing Zone Baseline | 2024

Created a reusable reference baseline for Azure, AWS, and Google Cloud landing zones. Combined Terraform, Bicep, CloudFormation, identity controls, network guardrails, policy as code, logging, and compliance evidence into a consistent delivery model.

Zero Trust Telemetry Automation | 2023

Connected cloud audit data, platform alerts, and risk signals with SIEM and SOAR workflows. Added scoped credentials, event handling, structured logs, and response automation for suspicious access and configuration drift.

LEADERSHIP & AWARDS

- Received HarborPoint Digital Services Cloud Engineering Recognition for dependable NIH platform delivery and clear operational ownership.
- Selected by federal program leadership as a trusted contributor during quarterly compliance reviews and production recovery efforts.
- Led peer knowledge sessions on Terraform modules, cloud guardrails, incident runbooks, and secure CI/CD practices.

EDUCATION

Bachelor of Science in Information Technology

George Mason University GPA: 3.6 2014 Fairfax, VA

Coursework: *Cloud infrastructure, Network security, Database systems, Systems analysis, Information assurance*

CERTIFICATIONS

- Microsoft Certified: Azure Administrator Associate 2021
- AWS Certified SysOps Administrator - Associate 2020
- Google Cloud Professional Cloud Engineer 2023
- HashiCorp Certified: Terraform Associate 2022

TECHNICAL SKILLS

- **Cloud Platforms:** Microsoft Azure, Amazon Web Services, Google Cloud Platform
- **Infrastructure as Code:** Terraform, Bicep, CloudFormation
- **DevSecOps Delivery:** GitHub Actions, CI/CD pipelines, automated security testing
- **Identity and Access:** IAM, conditional access, privileged access management
- **Virtual Desktop:** Azure Virtual Desktop, host pools, profile storage
- **Network Services:** Hub-and-spoke networking, private endpoints, virtual networks
- **DNS and Certificates:** Azure DNS, Route 53, TLS certificates
- **Monitoring and Telemetry:** Azure Monitor, AWS CloudWatch, Google Cloud audit logs
- **Security Operations:** SIEM, SOAR, alert automation
- **Integration Development:** APIs, SDKs, webhooks, event streams
- **Secrets and Data Protection:** Secrets management, encryption, credential rotation
- **Compliance Standards:** NIST 800-53, FedRAMP, CIS benchmarks
- **Zero Trust Frameworks:** CISA Zero Trust guidelines, device compliance, least privilege
- **Automation Languages:** Python, PowerShell, JSON
- **Documentation and Operations:** Architecture diagrams, runbooks, configuration baselines

PROFESSIONAL AFFILIATIONS

- Member, Cloud Security Alliance, with focus on secure cloud architecture and shared responsibility.
- Member, Association for Computing Machinery, supporting continued practice in infrastructure engineering and systems design.

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST