QBurst | A High AI-Q™ Company

Streamlining Multi-Cloud Employee Offboarding with Unified Automation

Enhancing internal security posture by replacing manual, multi-platform access revocation with a centralized, one-click automated dashboard.

Overview

We developed a unified dashboard that allows CloudOps teams to check and revoke employee access across AWS, Azure, and GitLab using a single email-based search.

- Eliminated the operational bottleneck of manual per-platform logins, drastically reducing the time required for secure employee de-provisioning.
- Strengthened data integrity and security by implementing a secure, one-click deletion function and centralized secret management for multi-cloud credentials.

Client Profile

The client operates large-scale CloudOps environments that support distributed engineering teams, cloud-native platforms, and continuous delivery pipelines across multiple cloud providers. With extensive usage of AWS, Azure, Kubernetes, GitLab, and cloud automation frameworks, the organization maintains a strong focus on operational security, infrastructure reliability, and enterprise-grade access governance.

Challenges: Manual Inefficiency and Security Gaps

As the organization grew, the existing offboarding workflow became a liability:

- **Operational Latency:** Admins had to log into each cloud platform (AWS, Azure, GitLab) individually to check and remove user permissions.

- **High Error Margin:** Manual de-provisioning increased the risk of "stale" accounts, where former employees might retain access due to an overlooked platform.
- **Credential Sprawl:** Managing the various access keys and secrets required to interface with multiple cloud providers posed its own security challenge.
- **Access Control Bottlenecks:** No centralized way to track which internal admins were authorized to perform these sensitive offboarding tasks.

Solution: Centralized Access Governance Dashboard

We engineered a unified web-based application to serve as a single point of truth for employee access management. The solution interfaces with multiple cloud providers through a secure backend, providing real-time "found or not found" status for any comma-separated list of email IDs.

The architecture prioritizes security and simplicity:

- **Unified Interface:** Built with Python and Jinja, the dashboard simplifies complex API interactions into a user-friendly form input.
- **Multi-Cloud Integration:** Uses platform-specific access keys for AWS and Azure, orchestrated through a Kubernetes environment.
- **Hardened Secret Management:** Credentials and environment variables are stored in AWS SSM Parameter Store and fetched into Kubernetes using the External Secrets Operator (ESO) and Reloader for secure, real-time updates.
- **OAuth-Based Security:** Dashboard access is strictly controlled via GCP OAuth, ensuring only admin-authorized members can log in.

Technical Highlights

- **One-Click Deletion:** A secure function that allows logged-in admins to instantly remove identified users from specific AWS accounts.
- **Batch Processing:** Support for comma-separated email inputs to handle multiple offboarding requests in a single action.

- **Secrets Abstraction:** Complete decoupling of cloud credentials from the application code, leveraging AWS-native secret stores for ITAR-compliant security levels.
- **Dynamic Access Control:** Admin-defined environment variables govern who can access the dashboard, managed externally for maximum security.

Impact

- **Enhanced Security Posture:** Automated revocation ensures that access is removed consistently across all platforms, effectively eliminating the risk of unauthorized data breaches.
- **Operational Efficiency:** The CloudOps team has transitioned from manual, repetitive checks to high-value strategic initiatives, thanks to the reduction in offboarding time.
- **Improved Data Integrity:** Removing human error from the de-provisioning cycle ensures that 100% of necessary access is revoked accurately every time.
- **Simplified Administration:** Centralizing management for AWS, Azure, and GitLab into one dashboard has streamlined internal governance and audit readiness.