P0 SECURITY

CNA takes control of service account sprawl with continuous access governance

CNA

About CNA Insurance

CNA is one of the largest commercial property and casualty insurance companies in the United States, offering a broad range of standard and specialized insurance products and services.

The company helps businesses manage risk and protect their people, assets, and operations, delivering solutions tailored to the unique needs of its clients

Overview

CNA Insurance has over 1000 live projects in GCP on average. Within which, developers had created tens of thousands of service accounts over time.

The sprawl of service accounts (40,000+, growing 5% monthly) and static keys (30,000+) presented a security risk for CNA and made effective governance near impossible.

Challenge

CNA's service account sprawl became unmanageable, but their existing IGA, CSPM, and native GCP tooling was unable to provide relief. Lacking scalable, proactive governance for NHIs that led to:

- **Lack of ownership:** Without accountable users tied to service accounts, effective governance was impossible
- **Lack of visibility:** Posture, usage, and permissions were unclear, making remedial action risky
- **Manual overhead:** Homegrown fixes across 40,000+ accounts were cumbersome and error-prone, requiring significant FTE effort and custom tooling

The sprawl of service accounts (40,000+, growing 5% monthly) and static keys (30,000+) presented risky governance gaps for CNA.

Per a 2025 CyberArk report, at least 42% of machine identities hold privileged access.

Why it matters

With P0, CNA went from 40,000+ unmanaged GCP service accounts to eliminating 100% of static keys and overly permissive access.

CNA now has a sustainable program to proactively manage non human identities, drastically reducing security risk and operational overhead across their entire cloud environment.

Solution

CNA partnered with P0 Security to transform sprawling GCP service accounts into comprehensive, continuous access governance. In a single deployment, they connected 1,000+ projects and began managing 40,000+ NHIs with full visibility and automated operational workflows.

Key features:

- Comprehensive discovery of all human and non-human identities
- Risk assessment and guided remediation of over-privileged accounts and unused keys
- Key rotation and permissions removal using P0-managed service accounts
- Seamless just-in-time access workflows for developers

Results

P0 Security's deployment was straightforward and consisted of connecting CNA's GCP APIs to P0 and adding all 1000+ projects via a script in P0's web GUI. Deployment took less than an hour, with no additional infrastructure required.

Out of the box, P0 provided visibility into all privileged access in their GCP. Over a period of a few weeks, CNA's security team began managing 40,000+ service accounts via P0, thereby eliminating 100% of static keys and overly permissive access.

With vaults or bastions, time to value would have taken several months and resulted in only partial risk reduction of about 70%. More importantly, CNA can now operationalize a continuous governance program, ensuring that new service accounts are short-lived and least privileged by default.