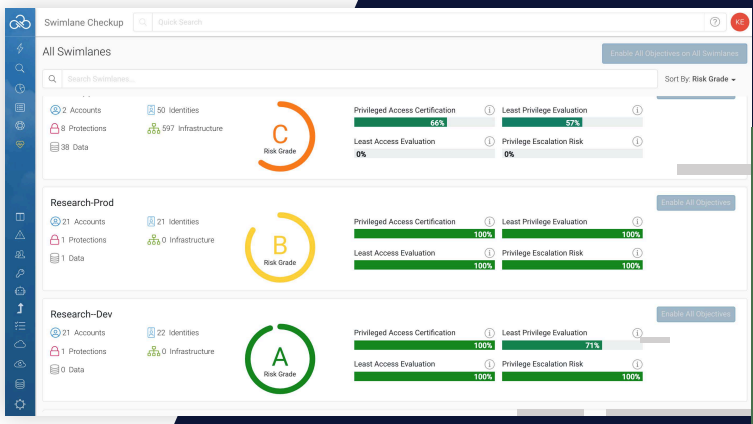
sonraí SECURITY

Sonrai Dig on Google Cloud



Who Can and Has Accessed GCP Resident Data, Resources, and Infrastructure?

Organizations building applications on Google Cloud quickly discover how important identity and access management (IAM) is to securing data resident in the public cloud. A poor Google Cloud configuration can expose corporate data to potential breaches by an external actor or an over-permissioned insider. Sonrai Dig, our identity and data governance platform, helps organizations understand and monitor Google Cloud to eliminate weak or accidental configurations that if left unchecked, will inevitably lead to a disaster.

Increase Visibility into Google Cloud Workloads

- Cross-project configuration checks for possible data exposure from poor usage of configuration and trust relationships
- Automated alerts for over-privileged identities and compute
- Timely notification of high risk IAM, network, and resource configurations

Address Identity and Data Governance Concerns

- Who has accessed Google Cloud resources and data?
- Who can access Google Cloud workload data and their components?
- Does the Google Cloud configuration properly protect data if a credential is stolen or misused?

Assess GCP Policy Change Risk Auto-remediation

- Continually monitor configuration drift against an approved baseline
- Integrated use of GCP resource tags to align risk with workload classifications
- Strong audit capabilities of changes to configuration and data access

Secure Google CloudData Stores & Support More Services

- Data stores including Cloud SQL, Big Table, and more
- Compute including Compute Engine, BigQuery, and more
- Other services including key management, networks, load balancers, firewalls, and more

Ready to graph, identify, and monitor identities and data inside your Google Cloud ?
Request a demo today.

Google Cloud

sonraísecurity.com | info@sonraísecurity.com | 646.389.2262

sonraí SECURITY