britive

Dynamic Access Governance for Google Cloud Platform

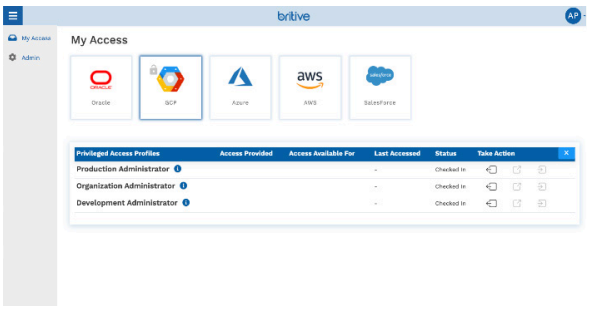
GCP Requires a New Approach for Privileged Access Governance

- Managing access within GCP requires managing the GCP organization, folders and projects
- Difficult to gain complete visibility into who has what level of access in GCP and how it's being used
- Static user privileges has exposed GCP to higher risks of security breaches
- Traditional access governance models and tools cannot adapt to the highly dynamic nature of DevOps
- Existing threat monitoring solutions fall short of providing valuable identity and policy context for user activities

Secure GCP with Dynamic Cloud Privileged Access Governance

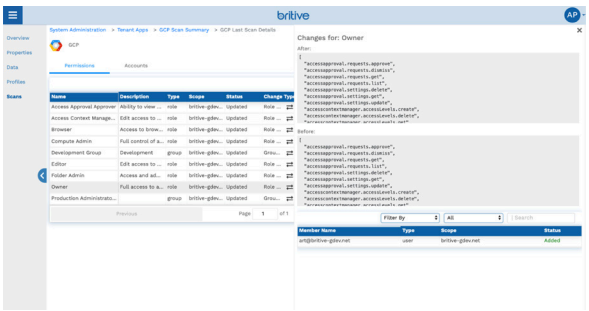
Visibility & Control

- Automatically discover, audit & control existing users and access levels across GCP organizations, folders and projects
- Categorize users and access to enforce least privilege



Policy & Governance

- Implement consistent privileged access policies across GCP organizations, folders and projects
- Eliminate static privileges for GCP resources
- Dynamically enforce access policies to minimize impact on DevOps



Monitoring & Detection

- Centralize auditing & policy compliance monitoring
- Apply machine learning to generate risk profile and enrich with identity data, access policy, and behavioral analytics
- Build a comprehensive risk dashboard to help prioritize internal/external threats

450 N. Brand Blvd., Ste. 600
Glendale, California, 91203