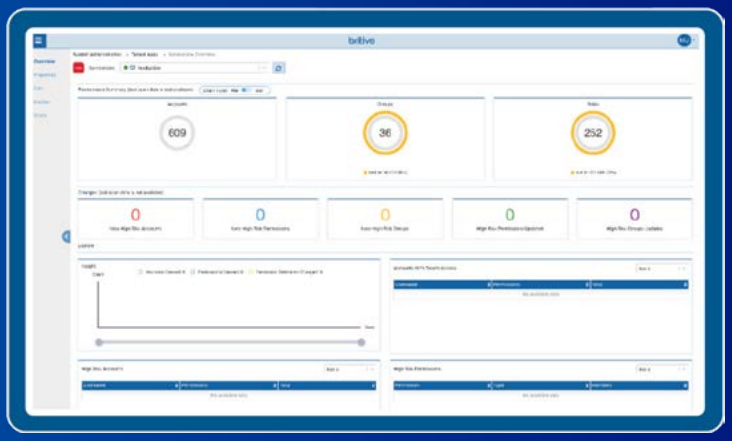
britive

SOLUTIONS BRIEF

Just-In-Time (JIT) Permissioning for Google Cloud Platform

Google Cloud is Vulnerable to Privileged Access Attacks

- Excessive standing privileges among human and machine IDs are extremely difficult to manage and maintain in a systematic way
- Limited visibility into who has which privileges, and how they are being used
- Over-provisioned privileges go unused and can be exploited
- Static access policies in applications leave your organization vulnerable
- Available products for managing privileges impede cloud operations and administration
- Compliance challenges escalate
- Access violations and threats are lost across thousands of applications



Only Britive Delivers JIT Permissioning for GCP

The Britive Multi-Cloud Privilege Management Platform is built with scalability and security in mind. It is designed for privileged users whose access levels in GCP require stronger security controls. Our platform enforces these controls with minimum impact on users, while substantially reducing the risks of privileged access breaches.

Simple to deploy and use, the Britive Platform features an API-only architecture that enables even enterprise level organizations to get up and running within 15 minutes or less. The only solution providing Just–In-Time Permissioning and Secrets Governance, Britive is specifically designed to secure organizations employing continuous integration / continuous delivery development (CI/CD) strategies in specific cloud environments – such as GCP – as well as across multiple cloud environments.

The platform transforms visibility into access – for both human and service accounts; it turns visibility into enforcement with JIT via console and command line interface (CLI). Finally, the platform also integrates with Ping to enforce MFA and covers – at a minimum – human use cases.

Secure Google Cloud with Least Privilege Access & Secrets Governance

Dynamic Permissioning

- Automated granting and expiration of Just In Time (JIT) permissions
- Maintenance of Zero Standing Privileges (ZSP)
- Centralized and scalable management of human and machine IDs

Advanced Data Analytics

- Access map visualizing access and authorization
- Query engine to flatten access views
- Exportable data via API to external systems

Least Privilege Enforcement

- Privilege right sizing
- Discovery and elimination of excess privileges

Custom URL Pages for GCP Integration

- Users can log in to GCP via Britive, where credentials will be encoded and delivered as a token
- The token grants JIT access to the user, and the custom URL takes users directly to the application they need

Proactive Monitoring

- Analysis of access changes and policy drift
- Identification of risky behavior
- Post incident investigation of identity based incidents

Secrets Governance

- Automated granting of dynamic secrets for human and machine processes

KEY CUSTOMER BENEFITS:

- Grant and revoke JIT secrets on the fly – ideal for quick provisioning of temporary cloud services
- Enforce Least Privilege Access (LPA) to eliminate over-privileged accounts and minimize your attack surface
- Get insights into risky identities and privileges
- Integrate Britive with your UEBA/SIEM technologies to gain centralized insight into cloud privileges and activity
- Simple to use and deploy, even enterprise-level organizations can get up and running within 15 minutes or less
- Empower DevOps, SecOps, and CloudOps teams for speed and security
- Secure your CI/CD pipeline in minutes, not days or weeks

THE BRITIVE PLATFORM IS CLOUD-NATIVE AND API-FIRST, MAKING INTEGRATIONS SEAMLESS AND COST-EFFICIENT

Get a closer look at how Britive secures Google Cloud Platform without disrupting workflow:

SCHEDULE A DEMO