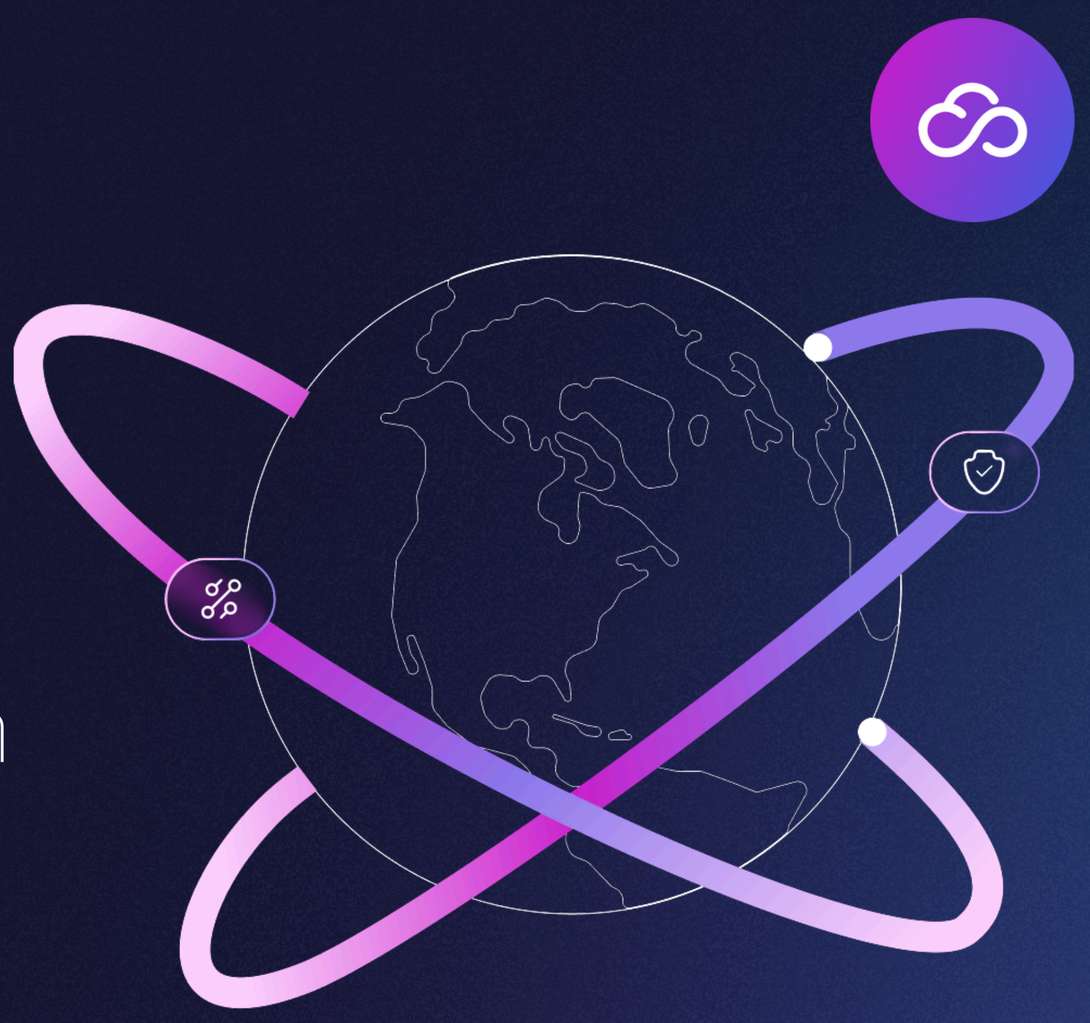
britive

>_ SOLUTION BRIEF

Cloud Privileged Access Management

for Google Cloud Platform (GCP)



Britive's platform is built with scalability and security in mind. Our cloud-native design is suited to handle privileged users whose access levels in GCP require more granular security controls. Easily enforce these controls with minimal impact on users while reducing the risk associated with standing access.

Simple to deploy and use, the Britive Platform features a flexible, API-first architecture that enables even enterprise-level organizations to get up and running quickly.

Britive's patented ephemeral, dynamic JIT permissioning is specifically designed for the modern cloud environment. We secure organizations employing CI/CD and IaC strategies in cloud infrastructure providers like GCP, as well as across other cloud applications, data services, and other solutions.

The platform also handles hybrid and private cloud for customers using Kubernetes—both self-managed or as part of a cloud service such as Google Kubernetes Engine (GKE). We standardize privilege management across cloud solutions, making it simpler and easier while maintaining the flexibility and controls provided by the native cloud providers.

GOOGLE CLOUD IS VULNERABLE TO PRIVILEGED ACCESS ATTACKS

- Excessive standing privileges among human and non-human accounts are extremely difficult to manage and maintain at scale.
- Teams have limited visibility into what identities have access to which resources, and how they're being used.
- Managing audits and compliance is difficult across siloed tools and fragmented processes.
- Over-provisioned privileges go unused and can be exploited for lateral movement across the environment.
- Static access policies in applications leave your organization vulnerable as part of a growing attack surface.
- Products available for managing privileges impede cloud operations and administration, introducing unnecessary friction.
- Teams quickly lose visibility into access violations and threats across thousands of applications.

HOW BRITIVE SECURES & ENHANCES GCP

DYNAMIC PERMISSIONING

- Grant and revoke permissions just-in-time (JIT) according to security policy
- Eliminate standing permissions and achieve zero standing privileges (ZSP)
- Centralized, scalable access management for all identities both human and non-human

ACCESS DATA ANALYTICS

- Query engine to flatten access views
- Exportable data via API to external solutions and data visualization tools
- Identity-centric data enrichment for analysis

PROACTIVE MONITORING

- Gain visibility into access changes
- Quick identification of unusual behavior
- Support post-incident investigation of identity-based incidents

ACCESS TO RESOURCES & APPLICATIONS

- Single platform to easily manage privileges and entitlements across AWS services
- Centralized management for all requests, policies, and configuration
- Request and check out permissions via existing tools & workflows

ZERO-TRUST & LEAST PRIVILEGE ENFORCEMENT

- Eliminate excess standing privileges
- Enforce principle of least privileges at time of new, self-service access requests
- Enforce zero standing privileges (ZSP)

SECRETS GOVERNANCE

- Automated granting of ephemeral, time-bound secrets for human and automated processes
- Secure, ephemeral vault access for any required static secrets

KEY CUSTOMER BENEFITS

Rapid, API-First Deployment

Agent-less, proxy-less, and API-first design allows for rapid deployment and integration across the environment. Get Britive up and running in a matter of hours or days.

Enhance Cloud Security Posture

Dynamic, policy-based granting and revoking of permissions just-in-time ensures that there are no static privileges. Minimize the attack surface and adhere to Zero Trust approaches such as Zero Standing Privileges and Least Privileged Access.

Balance Speed and Security

Secure privileged access without slowing teams down. Simplify access requests and provisioning into a single platform, minimizing time-consuming back-and-forth for new access configurations.

TRUSTED BY LEADERS

TOYOTA Forbes ThermoFisher SCIENTIFIC GAP