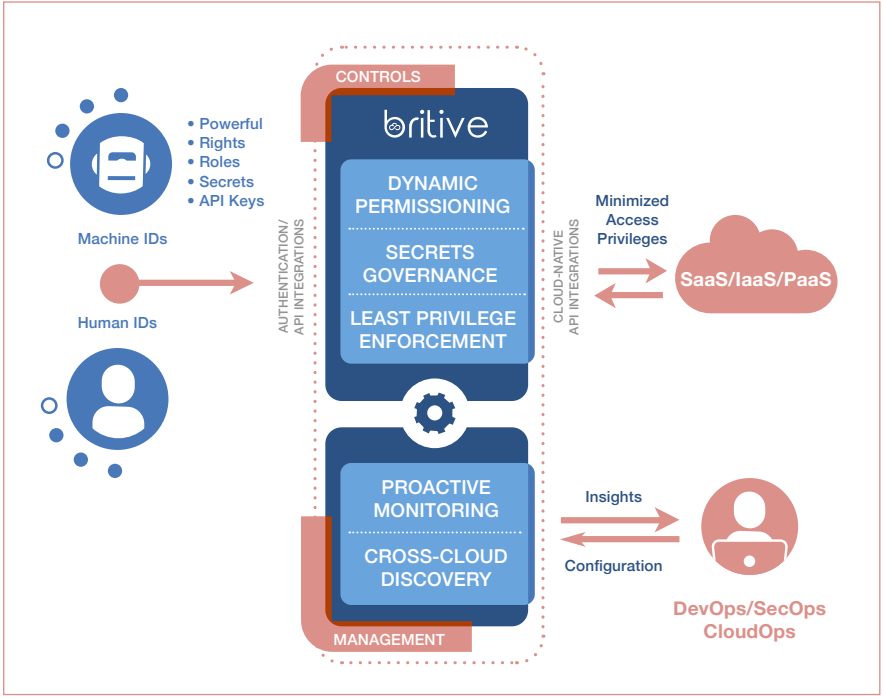
DYNAMIC PERMISSIONING PLATFORM

CLOUD IS VULNERABLE TO PRIVILEGED ACCESS ATTACKS

- Thousands of cloud applications with different access models
- No visibility into who has which cloud privileges, and how they are being used
- Over-provisioned cloud privileges go unused and can be exploited
- Static access policies in cloud applications leave organizations vulnerable
- Available products for managing privileges stand in the way of cloud operations and administration
- Compliance challenges escalate
- Access violations and threats are lost across thousands of cloud applications

The Britive Dynamic Permissioning Platform is built with scalability and security in mind. It is designed for privileged users whose access levels in cloud systems 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 across multiple cloud environments.



DYNAMIC PERMISSIONING PLATFORM

Dynamic Permissioning

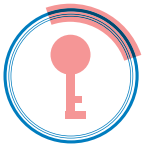
- Automated granting and expiration of Just In Time (JIT) permissions
- Maintenance of Zero Standing Privileges (ZSP)
- Centralized and scalable management of human and machine IDs

Cross-Cloud Discovery

- Single pane of glass cross cloud (x-cloud)
- Automated discovery and auditing of accounts and privileges
- Reporting from a unified x-cloud access model

Least Privilege Enforcement

- Privilege right sizing
- Discovery and elimination of excess privileges



Secrets Governance

- Automated granting of dynamic secrets for human and machine processes

Proactive Monitoring

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

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

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 from Britive's unified x-cloud access model
- 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