britive

Secure Dynamic Access Governance

Cloud is Vulnerable to Privileged Access Attacks

- Thousands of cloud applications with different access models
- No visibility into cloud privileged user access to know who has what access, and how it's used
- Available privilege products inhibit cloud operations and administration
- Static access policies in cloud applications make organizations more vulnerable
- Access violations and threats are lost across thousands of cloud applications

Centralize Cloud Privilege Access Security

Visibility & Control

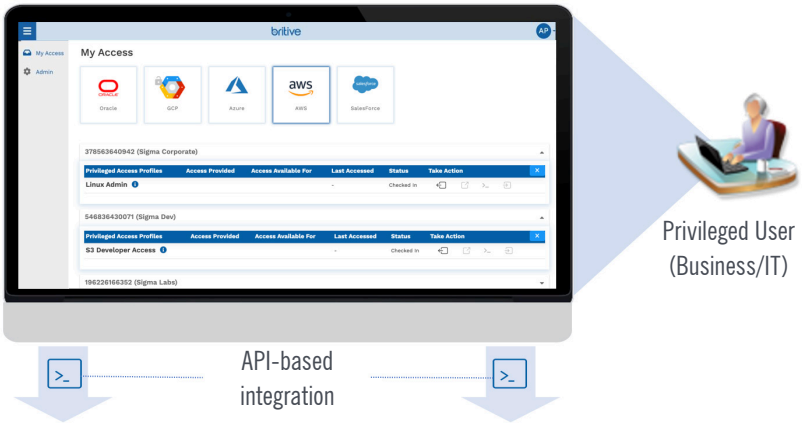
- Central access model for cloud applications
- Discover, audit & control existing access levels and users
- Categorize users and access to enforce least privilege

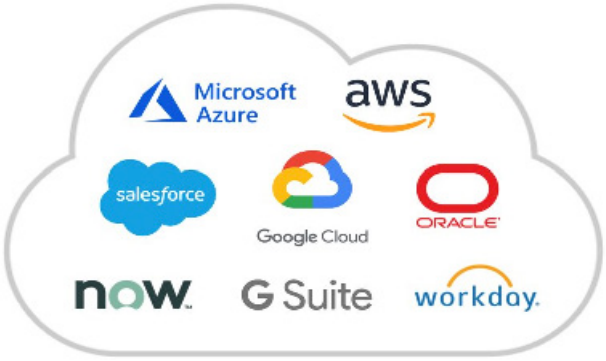
Policy & Governance

- Implement cloud policy & enforcement for cloud apps
- Dynamically expand cloud privilege with time-based expiration
- Centralize auditing & policy compliance monitoring

Monitoring & Detection

- Integrate with existing identity & security ecosystem (SSO/MFA, IGA, SIEM, UEBA)
- Threat monitoring with machine learning





End-User Features

- Context-based Multi-Factor Authentication
- Policy-based Access Profiles
- Visibility & Access Policy Enforcement
- Threat Analytics and Policy Monitoring

Architecture

- Multi-tenanted SaaS Built on AWS
- Pre-integrated with Major Enterprise IaaS & SaaS
- Secure & Scalable API-based Integration

Britive's solution is built with the cloud scalability and security requirements in mind. It is designed for privileged business and IT 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.

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