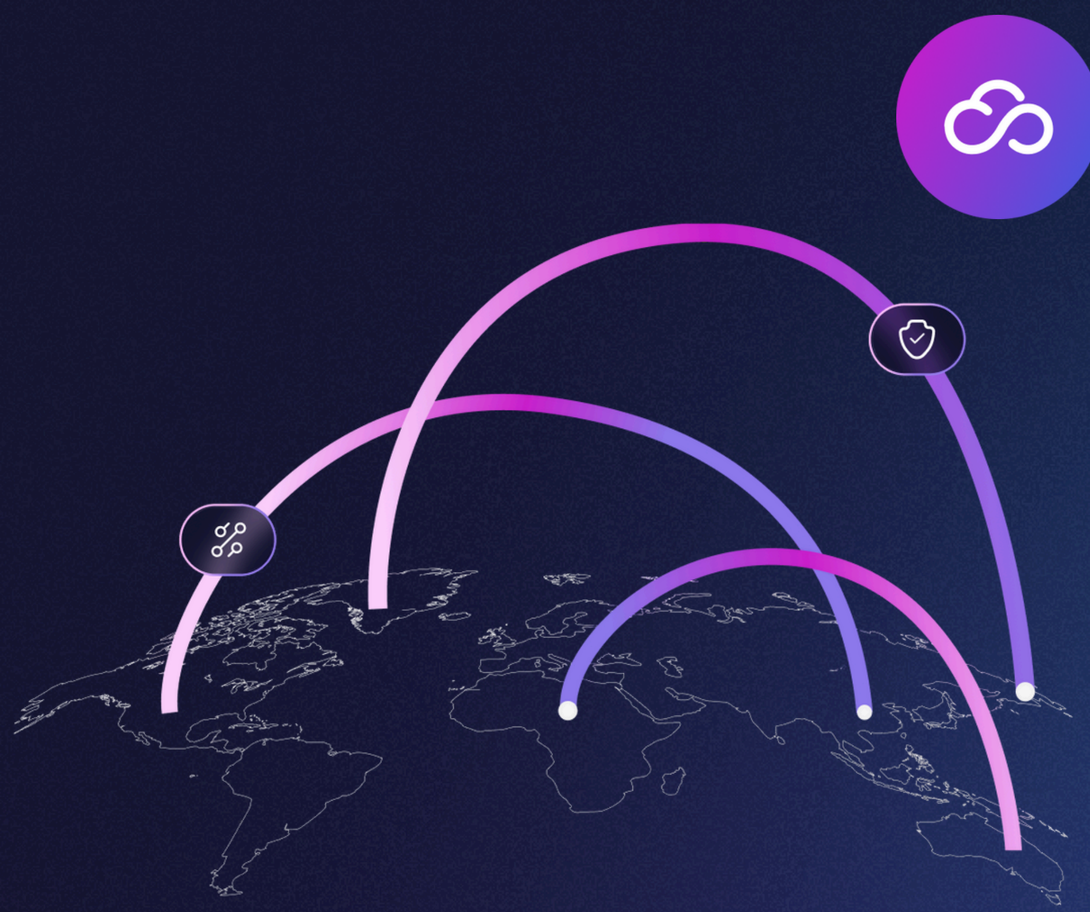
britive

>_ SOLUTION BRIEF

Cloud Privileged Access Management

for Amazon Web Service (AWS)



Britive is the first dynamic cloud privileged access management (CPAM) platform purpose-built for security, cloud oeprations, and development teams operating in AWS.

Our platform unifies access control across AWS environments, eliminating complexity and reducing risk. True Just-in-Time (JIT) ephemeral permissions eliminate static credentials and overprivileged accounts. Teams can enforce fine-grained access controls in AWS with true Zero Standing Privileges (ZSP), ensuring static access cannot be exploited while enabling cloud agility.

Our agent-less, proxy-less, API-first architecture makes deployment fast and frictionless, allowing enterprise-scale organizations to integrate seamlessly with AWS infrastructure and services, hybrid cloud, and multi-cloud environments.

Standardize privileged access across AWS and beyond for a consistent, scalable approach to securing cloud identities, applications, and data services.

ENHANCING SECURITY AND SCALABILITY CHALLENGES IN AWS

- Manual & time-intensive ongoing maintenance of keys to maintain compliance with internal and external policies and standards.
- Excessive standing privileges across human and non-human accounts is difficult to manage and maintain long-term.
- Lack comprehensive visibility into who has access to what and how it's being used.
- Over-provisioned privileges and static access policies sit unused, leading to large attack surface and increased risk of potential exploitation.
- Existing privileged and identity access solutions slow down cloud operations and administration, leading to friction and delays.
- Native IAM solution lacks governance, audit trails, and workflow approvals to facilitate workflows and audits.
- Teams lack visibility into access violations and threats across hundreds or thousands of applications, making risk remediation and reduction difficult.

HOW BRITIVE SECURES & ENHANCES AWS

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, 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 changes in access
- 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