britive

Why 'IAM User' Doesn't Work at Scale

As you grow, creating and managing accounts on AWS quickly becomes unmanageable.

- Manual & time-intensive, IAM User requires ongoing maintenance of keys to meet compliance or organizational policy
- Access keys stored in plain text are open to attacks
- Does not support least privilege, especially at scale
- Lack of governance, audit trails, & workflow approvals

Britive orchestrates admin & management of AWS access through Just-in-Time (JIT) permissioning

- **Support least privilege**
  JIT reduces the number of high-risk privileges and standing permissions on Day 1.
- **Save resources**
  Slash the time and cost required to manage the growing demands of DevOps' requests.
- **Automate processes**
  Gain efficiency by granting ephemeral keys & automating workflow approvals.

Overly complex security layers impedes growth in the cloud. Our API-driven platform is easy to deploy, integrates seamlessly with existing tools, and maximizes ROI with a cross-cloud platform that scales with your organization.

IAM Management

- Easily manage identity privileges & entitlements on AWS–and across your entire cloud landscape.
- Grant & revoke priivleges and entitlements on the fly.
- Eliminate longlived credentials stored in plain text.

Operations

- JIT permissioning for human and synthetic identities on AWS delivers the control and speed you need to manage access requests efficiently.
- When DevOps has the access they need, cloud app delivery is expedited.

Security & Governance

- Support a least-privilege security posture at scale without compromising user experience.
- Gain visibility into workflow approvals and access management to always meet compliance and maintain auidt trails

Britive saves valuable time and resources so you can scale securely.

CYBER SECURITY EXCELLENCE AWARDS WINNER 2022

CLOUD SECURITY ALLIANCE Trusted Cloud Provider CSA

Book a Meeting

www.britive.com