britive

Improve Visibility with Britive Dynamic Privileged Access Governance

Introduction & Problem Description

As businesses have replaced on-premise software and infrastructure with cloud applications and infrastructure-as-a-service (IaaS), identity and access management has become more and more difficult for companies to control.

While implementing Single Sign-On (SSO), Multi-Factor Authentication (MFA) and identity provisioning are good first steps to strengthen and secure the authentication process at cloud services, these tools do little to provide visibility and control for granted privileges in cloud services.

Once a user has authenticated, few tools provide visibility into privileges that are used by the user. Identity Governance and Administration (IGA) tools can map users to groups and roles but lack capability to show effective access levels. Additionally, information mapped between users, groups and privileges is typically stale because the information is refreshed periodically rather than in real time.

As cloud use grows and scales, complexities in groups and roles mask access to privileges which make companies vulnerable to privilege exploitation. For example, accidentally assigning AWS S3 administrator privileges to a user can result in data loss across the entire AWS environment.

Combining the lack of deep visibility into user, group, and role privileges with the dynamic nature of cloud infrastructure results in very little oversight and control over the activities of users within cloud infrastructure and applications. Companies are at risk of giving too many privileges to too many people and losing control of critical business data managed and stored in cloud environments.

britive

DISCOVER

Britive scans cloud applications for existing users, groups, roles, and granted privileges down to the resource level. Each user, group, role and privilege are categorized to identify and verify that privilege users have the appropriate levels of access. Clear concise access reports outline users and groups with the most privilege and the highest risk.

AUDIT

Britive tracks and reports levels of privilege as well as all activity associated with those privileges. Britive will also generate privileged access reports for consumption by internal and external auditors to ensure compliance with regulatory and other requirements such as SOX, GDPR, HIPAA, GLBA, PCI-DSS, ISO 27001, SOC 2, FedRAMP etc.

MONITOR

Britive monitors privileged access across all cloud applications. Applied behavior analysis identifies privilege abuse and abnormal activities from users. Additionally, Britive detects and alerts administrators if users circumvent Britive to get direct privileged access to cloud services.

BRITIVE SOLUTION SUMMARY

Britive's Dynamic Privilege Access Governance automatically scans and retrieves the users, roles and privileges from each cloud system. Britive correlates this information with the company user identity information. Privileged users are identified and flagged for review to ensure the right people have the right levels of access to work efficiently.

After users, groups, and roles are reviewed, privileged access governance can be shifted to Britive. Britive will dynamically grant cloud application administrative privileges to users based on policy authorization. This ensures that each user adheres to the principle of least privilege while still easily getting the privileges needed to complete their work.

Britive ensures that cloud identity security scales as cloud adoption grows within an organization. User privileged access doesn't get lost in a complex set of roles and groups. As complexity grows, Britive continues to scan and review each cloud service to ensure that permissions and privileges are used appropriately by users who require elevated permissions to support applications and the business.

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