britive

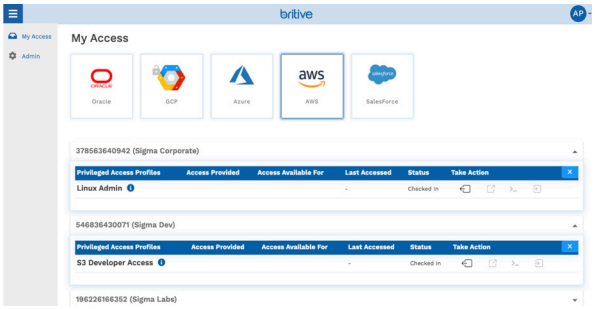
Dynamic Access Governance for Amazon Web Services

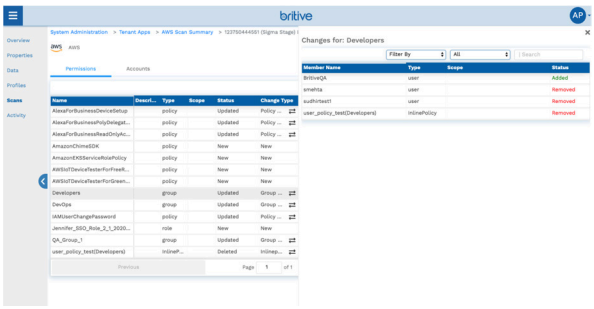
britive + aws

AWS Requires a New Approach for Privileged Access Governance

- Difficult to gain complete visibility into who has what level of access in AWS and how it's being used
- Challenges in enforcing consistent access policies across multiple AWS accounts within an organization
- Use of static credentials and access keys has exposed AWS environments to higher risks of security breaches
- Traditional access governance models and tools cannot adapt to the highly dynamic nature of DevOps

Secure AWS with Dynamic Cloud Privilege Access Governance





Visibility & Control

- Automatically discover, audit & control existing users and access levels across multiple AWS accounts
- Categorize users and access to enforce least privilege

Policy & Governance

- Implement consistent privileged access policies across all AWS accounts within an organization
- Dynamically enforce access policies to minimize impact on DevOps
- Eliminate static credentials and access keys for AWS console and API access through the use of policy-based temporary keys

Monitoring & Detection

- Centralize auditing & policy compliance monitoring
- Apply machine learning to generate risk profile and enrich with identity data, access policy, and behavioral analytics
- Build a comprehensive risk dashboard to help prioritize internal/external threats

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