britive

Dynamic Access Governance for Microsoft Azure

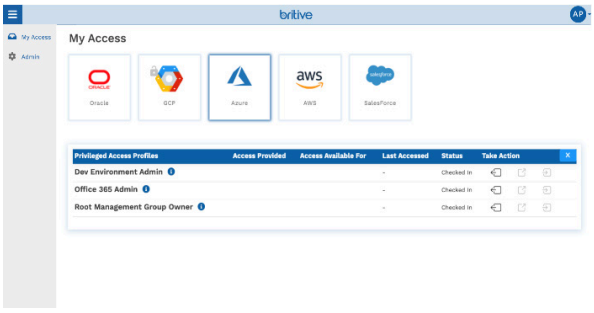
Azure Requires a New Approach for Privileged Access Governance

- Managing access within Azure requires managing both Azure AD and Azure Resources
- Difficult to gain complete visibility into who has what level of access in Azure and how it's being used
- Challenges in enforcing consistent access policies across multiple Azure management groups, subscriptions, resource groups and resources
- Use of static privileges has exposed Azure environments to higher risks of security breaches
- Traditional access governance models and tools cannot adapt to the highly dynamic nature of DevOps

Secure Azure with Dynamic Cloud Privileged Access Governance

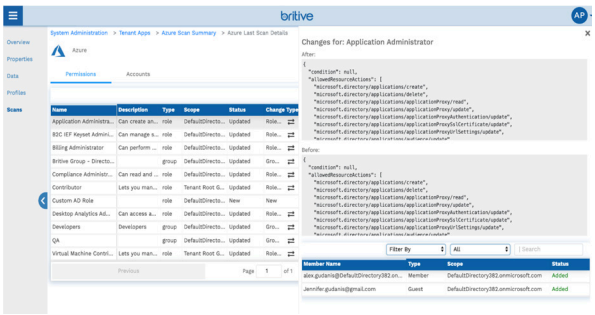
Visibility & Control

- Automatically discover, audit & control existing users and access levels across Azure AD directories, management groups, subscriptions, resource groups and resources
- Categorize users and access to enforce least privilege



Policy & Governance

- Implement consistent privileged access policies across Azure directories, management groups, subscriptions, resource groups and resources
- Eliminate static access for Azure directories and resources
- Dynamically enforce access policies to minimize impact on DevOps



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