britive

Enforce and Control Access with Britive Dynamic Privileged Access Governance

Introduction & Problem Description

Cloud adoption has simplified many responsibilities of IT teams across all company sizes. However, Infrastructure as a Service (IaaS) and cloud applications made identity and access security more difficult by splintering access authorization and privilege management. Each cloud offering has their own complex access and privilege administration. IT administrators must learn the nuances of each cloud application in order to secure users and company data. With the added complexity and the differences in systems, most administration activities are difficult to automate. As a result, granting user access to cloud environments takes days or weeks due to the complex resource models, and control approvals needed to provision static accounts.

These complex privilege models in cloud platforms often leave companies vulnerable to breaches and data loss because of misconfiguration. Since each cloud platform has different controls, each platform is manually administered. Manual configuration takes more time, costs more money and leads to misconfiguration. Users end up with critical privileges that, when misused or abused, lead to a security incidents. Cloud environments are left exposed to privilege exploit and critical data losses.

These vulnerabilities often continue for months or years because privilege grants are static (“always on”). Once a user has been granted privileges, very rarely are those privileges revoked. Even when users change roles within a company, they will keep the privileges associated to their previous role. If a user loses control of their account, those privileges are vulnerable to abuse. This problem is exacerbated with the default settings of most cloud applications and platforms. Users are granted, by default, broad access to all objects and resources. Additionally, most companies see additional licensing costs for users with over-provisioned privileges.

SIMPLIFY

Britive simplifies privilege administration and accelerates cloud access provisioning with recommended policies derived from existing cloud application configurations. Administrators work with policies that apply to all cloud applications. Rather than struggling with the privilege model for each cloud application, Britive applies extensive knowledge and experience with cloud environments to recommend the correct set of access policies.

ENFORCE

Britive enforces zero privilege rule because users don't need privileges all the time. When a user needs a privilege to accomplish a task, Britive dynamically adds only the necessary privileges to the user's account for a limited time. Privileges are removed when the user completes the task or when the grant time expires.

PROTECT

Britive protects companies and users by assigning privileges based on policy. Privileges are assigned with fine-grained control based on the task. Privileges are removed to ensure that privileges are not inadvertently misused or, if an account is stolen, exploited to gain access to critical information or infrastructures. Britive monitors the use of privileged access with behavioral analytics and machine learning to alert administrators when users perform unexpected or unauthorized actions.

BRITIVE SOLUTION SUMMARY

Britive's Dynamic Privileged Access Governance simplifies privilege configuration, dynamically manages cloud privileges through automation, and enforces access policies for all cloud applications. Britive provides a single pane of glass for configuring and controlling privileges across multiple cloud environments.

Britive simplifies privilege configuration by scanning, correlating and analyzing granted user privileges. Based on a comprehensive understanding of privilege models for each cloud service, Britive recommends policies appropriate for each type of user.

Britive also protects a company and encourages least privilege by dynamically removing user privileges and enforcing privilege authorization based on the policy associated with the user. These policies are common across all the different cloud applications and can be applied to corporate users, groups or roles.

Using the policy-based privilege model, Britive accelerates the ability to grant access to cloud environments for users to be productive from "Day One", with the right resource models across cloud environments.

When a user is approved to use a privilege, Britive dynamically adds the privilege to the user in the cloud application on demand (just-in-time (JIT) privilege provisioning). The privilege is dynamically removed when the user has completed the action or when a time limit is reached. At that point, the privilege is removed from the user account, protecting both the company and user from privilege abuse (zero standing privileges (ZSP)).