Britive Joins Snowflake To Develop Identity-Centric Data Lakes

britive

Identity-Centric Data Lakes

The recently announced partnership between Britive and Snowflake ushers in an exciting new era for organizations looking to optimize their multi-cloud privileged access management (PAM) capabilities.

For too long, maintaining user privilege visibility across cloud platforms has been a vexing problem. Additionally, managing thousands of human and machine users is a Sisyphean task made more difficult by the need for DevOps teams to build at the speed of automation – without privilege grant delays – in multi-cloud environments. across the entire landscape of cloud platforms and apps, in addition to policy enforcement and threat monitoring.

Now, Britive's multi-cloud privileged access management platform can help Snowflake customers analyze and right-size cloud infrastructure privileges together with their security data lake.

Joint customers can normalize and analyze their Identity Access Management (IAM) data to obtain insights into identity-borne risks, recommendations for eliminating overly permissive access, and gaining visibility into access spread to allow automatic remediation of issues.

Manage Access Permissions Across Cloud Infrastructure

Utilizing identity-centric data lakes represents an important breakthrough in effectively managing access permissions across cloud infrastructure. In addition, this model allows for the ingestion of historical identity and access data for analysis and the enablement of users to proactively monitor their data for changes going forward.

As a result, joint Britive and Snowflake customers can quickly gain essential insights into user permissions and issue recommendations applicable to their data lake.

The Britive platform dramatically reduces the complexity and time to secure identities and permissions across multi-cloud environments, including IaaS, PaaS, SaaS, and DaaS services. The platform provides enterprise organizations with the ability to automatically grant Just-In-Time (JIT) permissions, auto-expire permissions, enforce least-privilege access, right-size broad permissions, and more.

As the Snowflake customer base continues to expand, Britive anticipates playing a vital role in accelerating cloud infrastructure management while reducing an organization's overall attack surface due to over-privileged or standing permissions.

The graphic below demonstrates the workflow. Identity data, drawn from an organization's various cloud data sources, flows to the Britive solution, which explores the data, grants right-size privileges, and assesses overall risk. Britive enforces JIT permissions through rigorous access control, ensuring the data stored and searched within Snowflake is appropriately vetted by powerful visualization so it can securely pass to its intended data platform.

Snowflake + Britive

The Britive/Snowflake partnership establishes identity-centric data lakes that are manageable, systematic, and designed to augment an organization's privileged access management. Made for the cloud, Britive requires no agents or proxies, and features built-in integrations with the most popular IaaS, PaaS, SaaS, and DaaS services. Britive presents a flexible cloud package that easily scales as your DevOps pipeline expands along with your business growth. It enables you to dramatically reduce the time required and the level of expertise needed to securely manage your data, apps and resources in the cloud.

britive

About Britive

Britive (www.britive.com) is a cloud-native security solution built for the most demanding cloud-forward enterprises. The Britive platform empowers teams across cloud infrastructure, DevOps, and security functions with dynamic and intelligent privileged access administration solutions for multi-cloud environments.

The Britive platform helps organizations implement cloud security best practices like just-in-time (JIT) access and zero standing privileges (ZSP) to prevent security breaches and operational disruptions, while increasing efficiency and user productivity.