britive

SOLUTIONS BRIEF

Just-In-Time Access for Snowflake

Britive integrates with Snowflake to provide JIT temporary access to Snowflake Roles

Mitigate risks to sensitive data in Snowflake by granting and revoking privileges as needed. Human and synthetic user requests are approved or denied based on policy. JIT permissions expire in the minimum amount of time required to accomplish their tasks or users can manually end them sooner.

Programmatic JIT access ensures data scientists and DevOps teams have the access they need. When static access is removed, the risk associated with a data lake breach is significantly reduced.

Challenge

Snowflake helps customers gain access to data services, data governance, and use data to drive business forward, which is why it's critical to have visibility and control into which permissions roles can access.

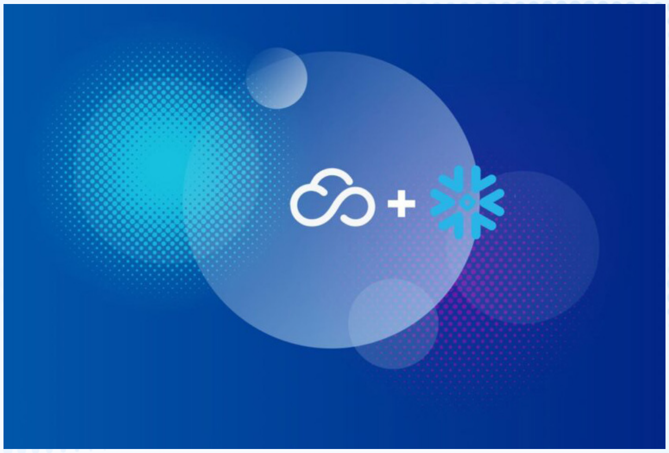
Establishing best practice policies is one thing; enforcing them without impeding workflows is another.

Organizations often struggle to implement JIT permissioning in ways that are cohesive, streamlined, and data driven.

A Closer Look

Static access puts data at risk:

- The #1 cloud risk concern for security leaders is having too many standing privileges
- 51% of organizations have static access to high-risk privileges
- 43% of organizations not currently employing JIT principles to privileged access plan to implement it in the next 12 months



Solution: JIT access for Snowflake

It is difficult to enforce policies when visibility is limited. But when roles are clearly defined, and visibility into users is total, enforcing best practice security policies is attainable. Data is accessible and protected—always.

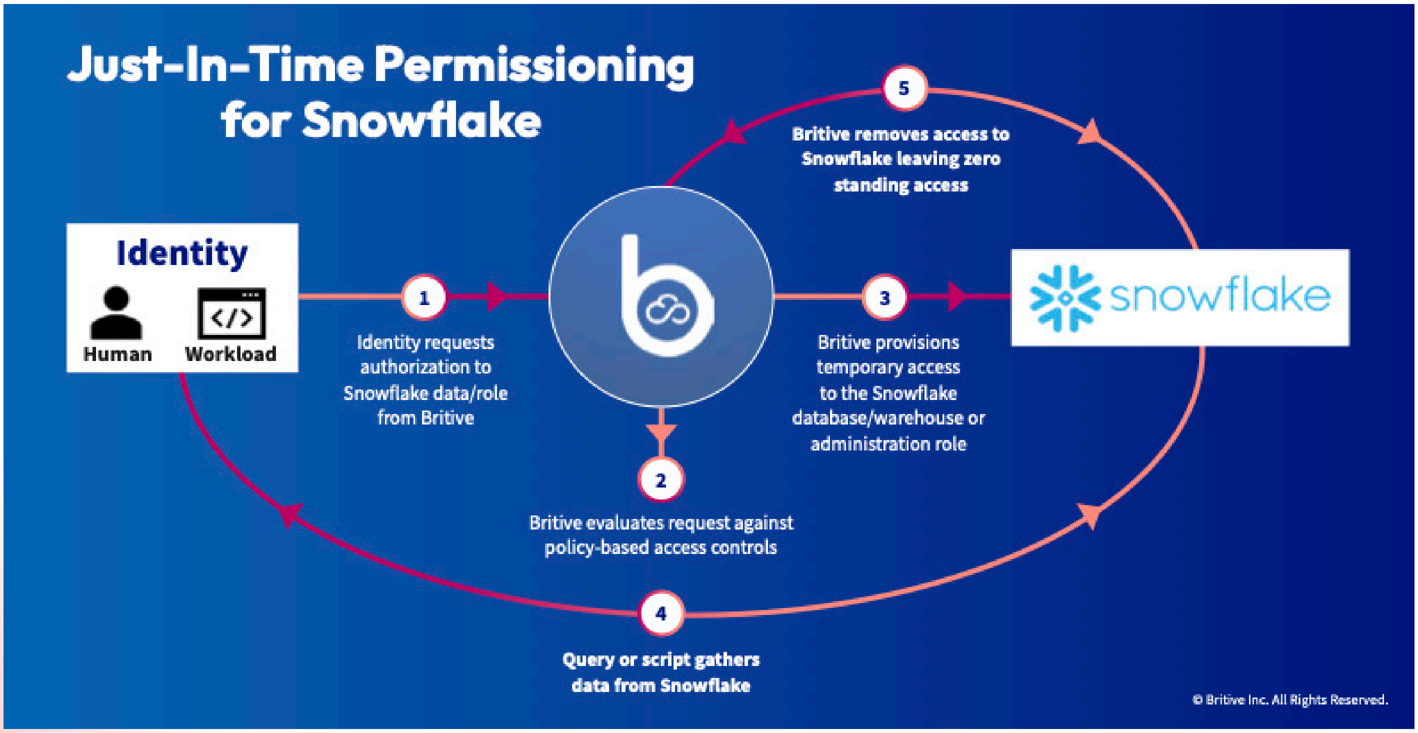
Britive provides Just-in-Time (JIT) temporary access for Snowflake administrative roles and databases, which delivers the visibility and control you need to secure data access and eliminate standing privileges.

Programmatic JIT in Snowflake

Britive JIT access seamlessly integrates with programmatic tooling—such as Python, Jupyter Notebook, etc.— used by data scientists and DevOps teams. Programmatic JIT access detaches roles from identities, removes static access, and keeps data lakes secure. Teams can quickly scale up using a single role checkout.

HERE'S HOW IT WORKS:

1. Britive's My Access page shows the Snowflake profiles that are designated for specific permission sets
2. Click 'checkout' to gain access for a predetermined period of time
3. Access is granted automatically
4. The Snowflake console opens
5. 'Checkin' the permission when the task is complete, or, when the allotted time expires, the


Just-In-Time Permissioning for Snowflake
5
Britive removes access to Snowflake leaving zero standing access
Identity
Human
Workload
1
Identity requests authorization to Snowflake data/role from Britive
3
Britive provisions temporary access to the Snowflake database/warehouse or administration role
snowflake
2
Britive evaluates request against policy-based access controls
4
Query or script gathers data from Snowflake
© Britive Inc. All Rights Reserved.

CAPITALIZE ON SNOWFLAKE'S POWERFUL DATA CAPABILITIES AND SUPPORT KEY BUSINESS DRIVERS THROUGH TEMPORARY, JIT PERMISSIONING. VISIT BRITIVE.COM TO LEARN MORE.

About Britive

Britive manages identities and privileges in multi-cloud and hybrid organizations. Control privileged entitlements and secrets management for human and machine identities, make business decisions based on activity analytics, and stay in front of threats with real-time reporting. We help secure your identities and