How to close the Service Account security gap in GCP and Snowflake

Many security and IT teams are concerned about a substantial security gap in their data warehouses such as GCP's BigQuery and Snowflake.

By now they understand that there are probably hundreds, if not thousands, of service accounts that are currently connecting their data warehouses to other cloud-services. Some of them are third-party cloud services, which may not be necessarily trustworthy.

These service accounts, which are essentially very powerful credentials, are usually created by employees like data analysts and DevOps practitioners in order to increase process automation and interconnectivity between systems. However, these app-to-app connections are created and granted powerful permissions under the radar of the security teams, and often increase organizations' attack surface.

So what is exactly this attack surface and how can you minimize it with the help of Astrix?

Let's start from the basics.

What are service accounts?

We are all familiar with the concept of user accounts. These accounts are specific to individuals, and allow us to sign in using our own credentials or identities to computers, networks, applications and services. There is a wide range of identity platforms out there that organizations can use to help them manage their user accounts - Okta and Duo being two noteworthy examples.

Similar to humans having user accounts, services and applications can have service accounts. These accounts are designed to complete tasks on behalf of a particular application or automated service - without human involvement. As such, service accounts are a popular tool for connecting core systems to each other and to third-party applications.

Consider the following common use cases:

- A data engineer creates a service account and uses it to connect the organization's database to a third-party data transformation tool, such as Fivetran or dbt, giving it access to read and modify data.
- A business analyst creates a service account and uses it to connect to some third-party BI platform, such as Tableau or Power BI, giving it access to read sensitive data.
- A DevOps engineer uses a service account to connect the comapany's database to an internally created automated backup service, giving the service account full read access to the database.

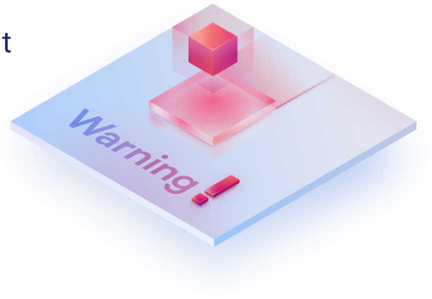
Each of the above examples involves creating a service account and granting it sensitive permissions. This service account is then handed over to an application or service, either internal or external, that then uses the service account to access the database.

What makes service accounts an attractive attack target?

Many service accounts require high exposure permissions, granting them **access to read and modify sensitive data**, and oftentimes even change configurations in your environment. These powerful credentials make these accounts a popular target of attacks; a single leaked service account can give a malicious actor access to vast resources, thus having catastrophic consequences for an organization.

While most companies have become quite competent at managing their user accounts, the increasing use of service accounts introduces some unique challenges that security practitioners often struggle to cope with.

How big is the attack surface?



Considering the increasing number of cloud applications and services that companies use nowadays (a large enterprise uses on average 1,400), the number of service accounts in an organization can easily match or even exceed the number of user accounts.

In fact, in typical cloud-first customers we see up to 5 times more service accounts than human accounts. This fact emphasizes the importance of proper visibility and management of service accounts.

What are the cyber risks posed by service accounts?

Service accounts, just like OAuth and API keys, provide programmable access to your organization's most critical systems. Improperly secured app-to-app connections massively increase the likelihood of supply chain attacks, data breaches, and compliance violations.

The recent attacks listed below reveal a new generation of supply chain attacks, in which attackers take advantage of the access granted to third-party cloud services as a backdoor into the companies' most sensitive core systems.

- **Microsoft's OAuth breach (Sep 22, 2022)**
  Malicious OAuth applications were deployed on compromised cloud tenants and then used to control exchange servers and spread spam (Read more).

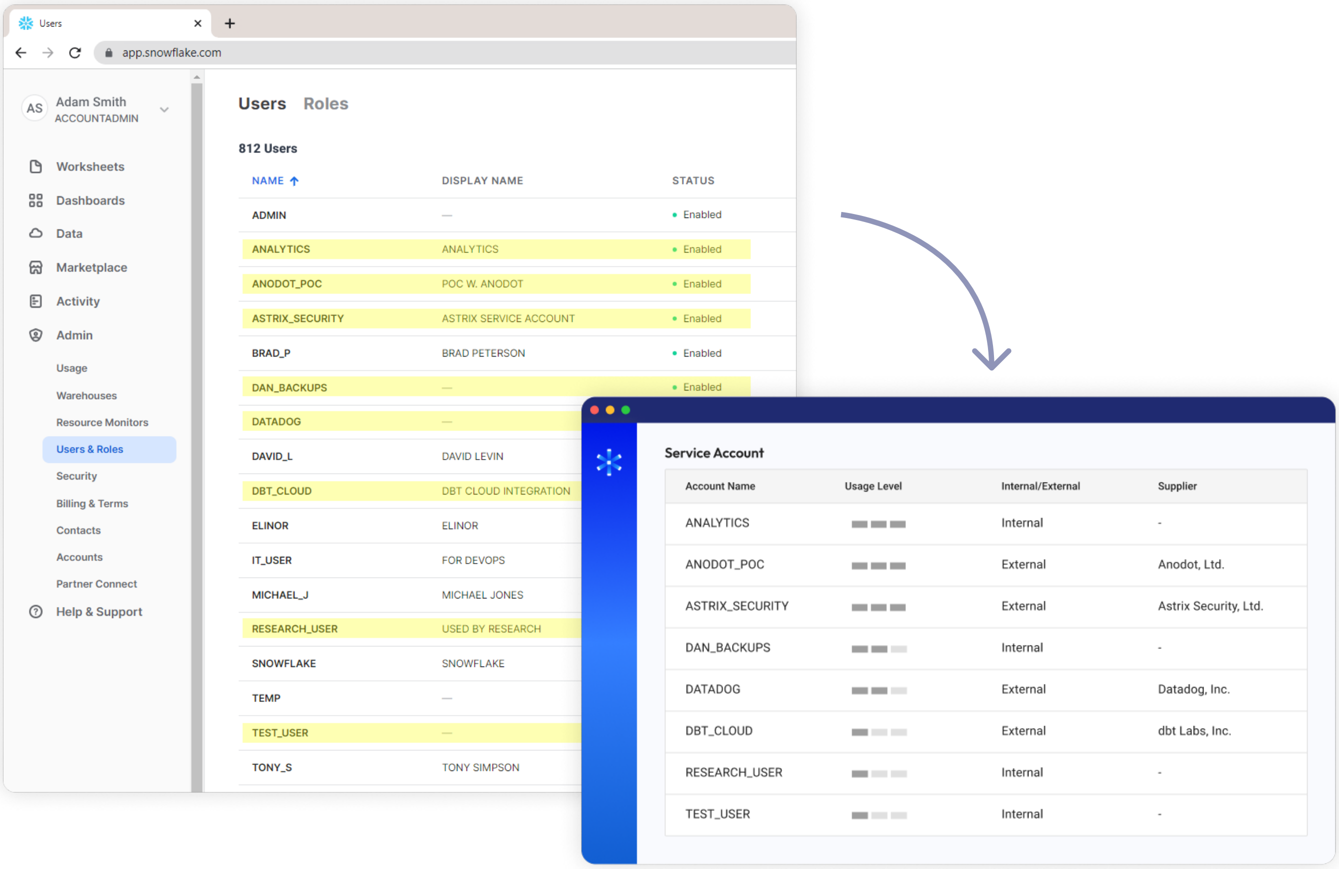
- **GitHub OAuth breach (April 28, 2022)**
  Attacker Breaches 'Dozens' of GitHub Repos Using Stolen OAuth Tokens (Read More).

- **Mailchimp breach (April 4, 2022)**
  Hundreds of customer accounts were compromised using stolen API keys (Read More).

How can Astrix help?

Our researchers at Astrix put their minds to this very problem, and developed engines that help you keep your service accounts in check. Astrix helps security teams take control of their tangled web of service accounts, by answering each of the following key questions:

#1 Which of these hundreds of service accounts belong to humans, and which of them are actually service accounts? In certain platforms, like Snowflake, user accounts and service accounts "look" exactly the same. Distinguishing between the two is crucial, since these are very different "creatures" that call for different management methods and security practices.



812 Users

NAME ↑	DISPLAY NAME	STATUS
ADMIN	—	● Enabled
ANALYTICS	ANALYTICS	● Enabled
ANODOT_POC	POC W. ANODOT	● Enabled
ASTRIX_SECURITY	ASTRIX SERVICE ACCOUNT	● Enabled
BRAD_P	BRAD PETERSON	● Enabled
DAN_BACKUPS	—	● Enabled
DATADOG	—	
DAVID_L	DAVID LEVIN	
DBT_CLOUD	DBT CLOUD INTEGRATION	
ELINOR	ELINOR	
IT_USER	FOR DEVOPS	
MICHAEL_J	MICHAEL JONES	
RESEARCH_USER	USED BY RESEARCH	
SNOWFLAKE	SNOWFLAKE	
TEMP	—	
TEST_USER	—	
TONY_S	TONY SIMPSON	

Service Account

Account Name	Usage Level	Internal/External	Supplier
ANALYTICS	■■■	Internal	-
ANODOT_POC	■■■	External	Anodot, Ltd.
ASTRIX_SECURITY	■■■	External	Astrix Security, Ltd.
DAN_BACKUPS	■■□	Internal	-
DATADOG	■■□	External	Datadog, Inc.
DBT_CLOUD	■□□	External	dbt Labs, Inc.
RESEARCH_USER	■□□	Internal	-
TEST_USER	■□□	Internal	-

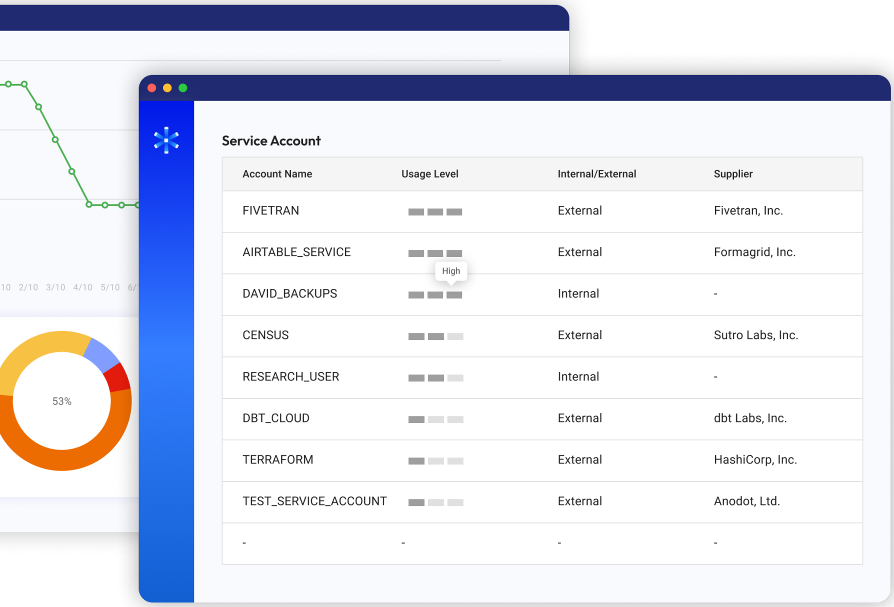
Astrix automatically distinguishes between user accounts and service accounts in Snowflake. Distinguishing between the two types of accounts is crucial, since they are very different "creatures" that call for different management methods and security practices.

#2 Which of these accounts are in use, and which are no longer needed? Many service accounts are created to address specific and timely needs, such as a POC or a trial, but remain connected even after they are no longer necessary and needlessly expand the attack surface.

#3 Which of these service accounts are used by third-party cloud services, and which are used by an internal system? Consider a DevOps engineer creating an automated process that uses a service account to backup your database, and write the backups to some internal storage bucket. This service account is not as exposed to supply chain attacks as one that is handed over to a third-party service, and the two should be treated differently.

#4 Which third-party cloud service uses this service account? Can the vendor behind this service be trusted?

#5 Has this service account been granted with the minimal permissions it needs to get the job done, or is it over-privileged?



Service Account

Account Name	Usage Level	Internal/External	Supplier
FIVETRAN	■■■	External	Fivetran, Inc.
AIRTABLE_SERVICE	■■■	External	Formagrid, Inc.
DAVID_BACKUPS	■■■	Internal	-
CENSUS	■■□	External	Sutro Labs, Inc.
RESEARCH_USER	■■□	Internal	-
DBT_CLOUD	■□□	External	dbt Labs, Inc.
TERRAFORM	■□□	External	HashiCorp, Inc.
TEST_SERVICE_ACCOUNT	■□□	External	Anodot, Ltd.
-	-	-	-

Astrix analyzes static and dynamic metadata from the monitored platforms to generate insights on each of your service accounts:

1. Astrix determines which of the service accounts are in use and which are not, and can therefore be removed.
2. Astrix identifies each of the service accounts as either internal (i.e. used only inside the organization) or external (i.e., used by a 3rd party service).
3. For each of the external service accounts, Astrix pinpoints the 3rd party service that uses it.

By answering the above questions, Astrix helps you make sense of your "service account jungle". Astrix first differentiates between user accounts and service accounts in places where such a distinction is not immediate. Astrix then determines which of your service accounts are exposed to third-parties, and finally identifies over-privileged or unused service accounts. Astrix' recommendations help you keep your service accounts in check, minimizing your attack surface dramatically.

About Astrix

From Salesforce and Office 365 to GitHub, and Snowflake, Astrix security platform ensures your XaaS core systems securely connect to third-party cloud services. Astrix's agentless, easy-to-deploy solution provides you with holistic visibility into all app-to-app connections and automatically detects and remediates over-privileged, unnecessary, and malicious integrations exposing you to supply chain attacks, data leakage, and compliance violations.

Learn more at www.astrix.security