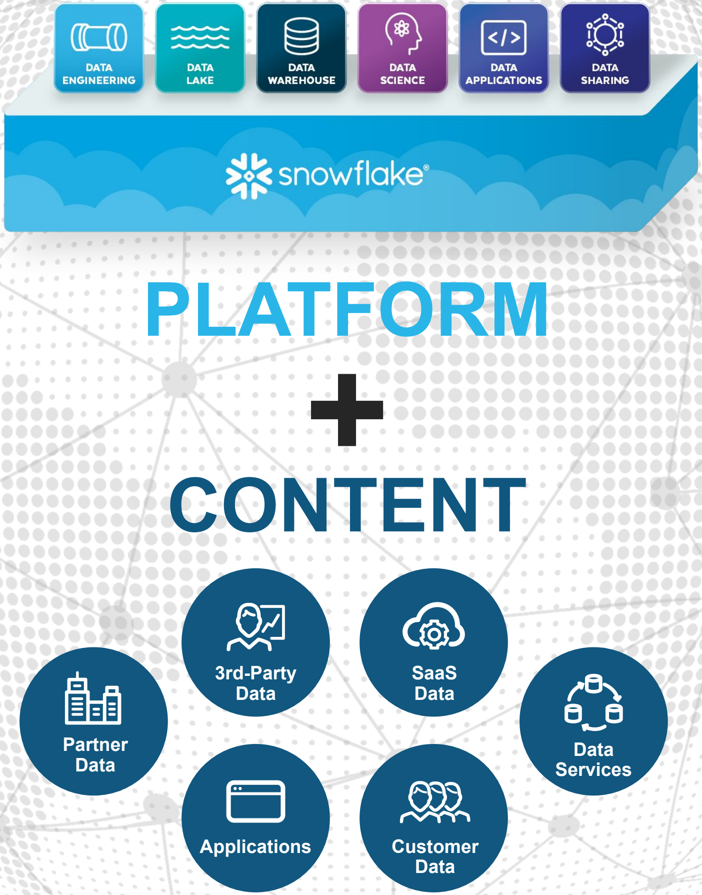
THE DATA CLOUD IS A GLOBAL NETWORK

One global, unified system connecting companies and
data providers to the most relevant data for their business

ELEMENTS OF THE DATA CLOUD



DATA ENGINEERING

DATA LAKE

DATA WAREHOUSE

DATA SCIENCE

DATA APPLICATIONS

DATA SHARING

snowflake

PLATFORM

+

CONTENT

Partner Data

3rd-Party Data

SaaS Data

Data Services

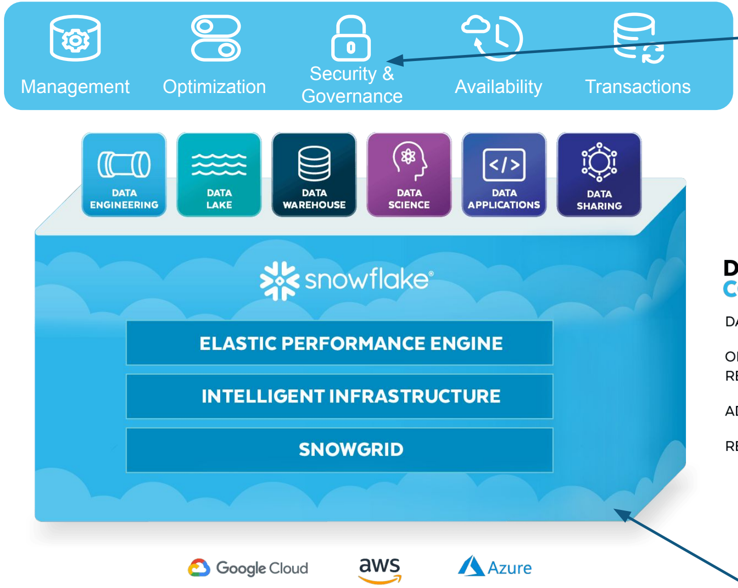
Applications

Customer Data

THE SNOWFLAKE PLATFORM

Customers, for example:

- *Create & manage users*
- *Load data*
- *Execute commands*
- *Export data*



DATA SOURCES

OLTP DATABASES

ENTERPRISE APPLICATIONS

THIRD-PARTY

WEB/LOG DATA

IoT

DATA CONSUMERS

DATA MONETIZATION

OPERATIONAL REPORTING

AD HOC ANALYSIS

REAL-TIME ANALYTICS

- Orchestrated security built in to the fabric of the platform
- Automated controls in place for all functions
- Constant monitoring
- Analysis to detect and mitigate threats quickly

Snowflake, for example:

- *Processes requests*
- *Maintains security*
- *Manages capacity*

Built-in security & governance features protect the data you load and use in Snowflake

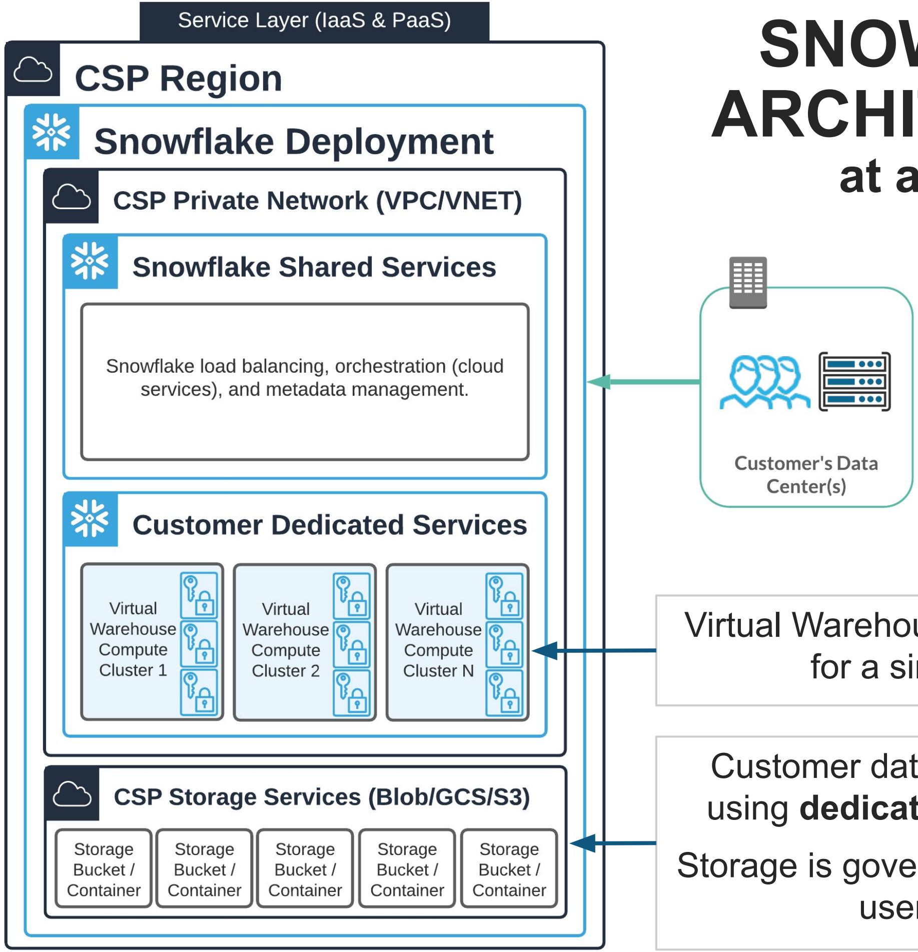
- Snowflake uses the industry-standard “shared responsibility” model
- Snowflake personnel do not have unauthorized access to customer data
- Snowflake personnel do not *collect*, *delete*, *update*, *disclose*, or *use* customer data

Snowflake uses sophisticated mechanisms to keep the platform safe and stable

SNOWFLAKE ARCHITECTURE

at a Glance

- Customers never have direct access (*e.g.*, "SSH") to the Snowflake VPC/VNET
- All access to customer data is through the Snowflake Service application layer
- Customer data is decrypted only in memory on dedicated Virtual Warehouse VMs:
  - Only the data **required to process the command is decrypted**
  - Virtual Warehouses are **ephemeral**, meaning they run only when needed


Service Layer (IaaS & PaaS)
CSP Region
Snowflake Deployment
CSP Private Network (VPC/VNET)
Snowflake Shared Services
Snowflake load balancing, orchestration (cloud services), and metadata management.
Customer Dedicated Services
Virtual Warehouse Compute Cluster 1
Virtual Warehouse Compute Cluster 2
Virtual Warehouse Compute Cluster N
CSP Storage Services (Blob/GCS/S3)
Storage Bucket / Container
Storage Bucket / Container
Storage Bucket / Container
Storage Bucket / Container
Storage Bucket / Container
Customer's Data Center(s)

Virtual Warehouses only process data for a single customer.

Customer data is encrypted at rest using **dedicated encryption keys**.

Storage is governed by dedicated IaaS user principals.

SNOWFLAKE SECURITY & GOVERNANCE AT A GLANCE

1 Network Controls

- All communication secured using TLS 1.2 with HSTS enforced for all client communications, and controlled by Network Policies (IP Allowlisting)
- Integration with CSP Private Networking
  - GCP Private Service Connect
  - AWS Privatelink
  - AWS VPC ID S3 policies
  - Azure Private Link
  - Azure cross-VNet rules for Blob access
- Choose from any of the Snowflake-supported cloud regions

2 Identity & Access

- SCIM user management
- Native Snowflake credentials
  - Password policies
  - Multi-Factor Authentication
  - Key Pair Authentication
- Federated Identity
  - SAML 2.0-based SSO
  - OAuth 2.0 delegated authorization
- Session control through policies

3 Data Governance

- Built-in Features & partner integrations
- RBAC & DAC
- Column-level security
  - Using views & UDFs
  - Dynamic data masking
  - External tokenization
- Row access policy
- Tagging
- Classification
- Anonymization

4 Encryption

- Customer data always encrypted in flight
- Data-at-rest always encrypted using a hierarchical key model
  - Rooted in the CSP's HSM
  - Automated key rotation & re-keying
  - BYOK with "Tri-Secret Secure"

5 Data Protection

- Account, region, cloud, and data-level recovery & failover
  - Fail-Safe
  - Time Travel
  - Cross-cloud & region replication & failover
  - AWS, Azure, GCP redundancy

6 Auditing

Comprehensive audit trail for all activities by all users from login

7 Compliance & Legal

AICPA SOC

SOC 2 Type II
12 Month Coverage Period

SOC 1 Type II
6 Month Coverage Period

HIPAA

HITRUST Certified

PCI Security Standards Council

irap

ISO 27001 CERTIFIED A-LIGN

FedRAMP

Moderate (Available from OMB MAX)

- Snowflake security policy
- https://www.snowflake.com/legal/ for DPA (GDPR), acceptable use, support, and more

INFOSEC & COMPLIANCE
at a Glance

All reports, attestations, documentation, and certifications

Third-Party Reports & Certifications

- Snowflake SOC 2 Type II Report
- Snowflake SOC 1 Type II Report
- Snowflake PCI-DSS-AOC-Final Report
- HIPAA/HITRUST Reports (proving ability to enter into BAA)
- Snowflake's ISO 27001 Certificate
- FedRAMP Moderate (on OMB MAX)
- IRAP Protected
- CyberGRX Report
- Penetration Test Results

ISO/IEC 27001

PCI-DSS

HIPAA

HITRUST Certified

FedRAMP Moderate

(Available from OMB MAX)

SOC 2 Type II

12 Month Coverage Period

SOC 1 Type II

6 Month Coverage Period

IRAP

Snowflake's Policy Documentation

- Snowflake Security Policy
- https://www.snowflake.com/legal/ for Acceptable Use, Support, and more

Snowflake Internal Controls & Testing

- DRP, BCP, and Information System Contingency Plans
- Security Incident Process
- Staff Training, Onboarding, and Access Policies

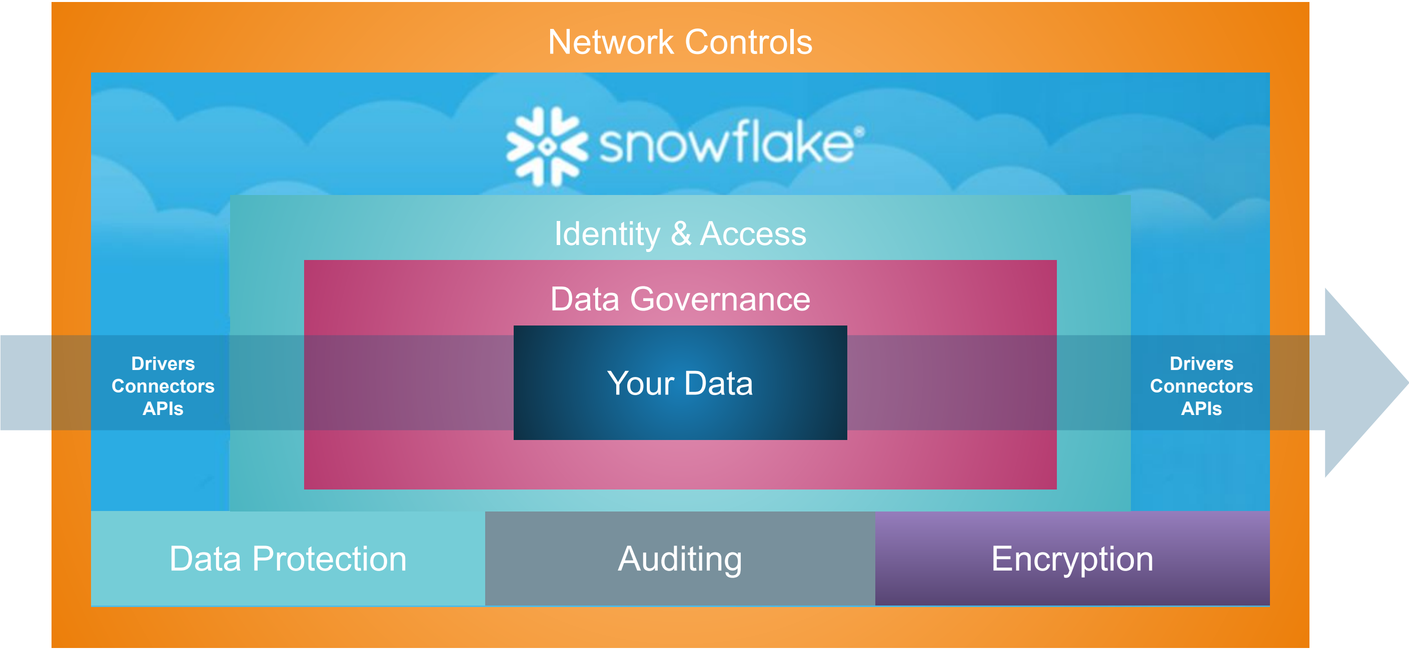
Snowflake Self-Assessment Reports

- CAIQ
- SIG Lite
- Red Team Pen Tests

SNOWFLAKE SECURITY & GOVERNANCE AT A GLANCE

DATA
SOURCES

- SECURITY EVENTS
- CMDB
- THREAT INTEL
- OLTP DATABASES
- ENTERPRISE
- APPLICATIONS
- THIRD-PARTY
- WEB/LOG DATA
- IoT

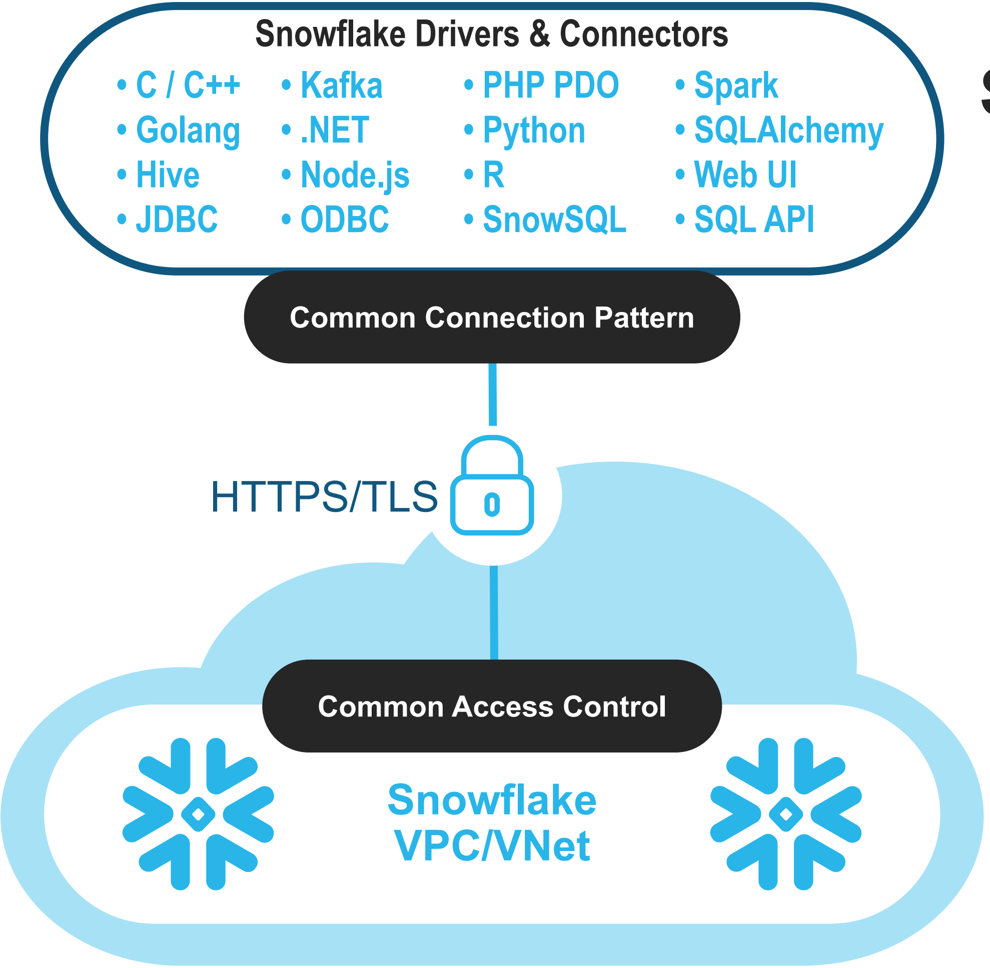


DATA
CONSUMERS

- SIEM
- XDR
- SOAR
- BI TOOLS
- DATA MONETIZATION
- OPERATIONAL
- REPORTING
- AD HOC ANALYSIS (JAVA UDF, SQL, Search)
- REAL-TIME ANALYTICS

Achieve: Compliance benchmarks, Privacy goals

NETWORK CONTROLS – SECURE COMMUNICATION



Common Connection Pattern for Drivers & Connectors

- Every driver & connector connects the same way
- All communication encrypted end-to-end
  - All customer data flows solely over HTTPS
  - Connections encrypted using TLS 1.2 from client through to the Snowflake Service
  - HSTS enforced for all client communications
- Data encrypted at rest

Common Access Control for all Sessions

- IP allowlisting available to restrict client communication to specific IP addresses using customer-configured Network Policies
- Authentication required for all connections

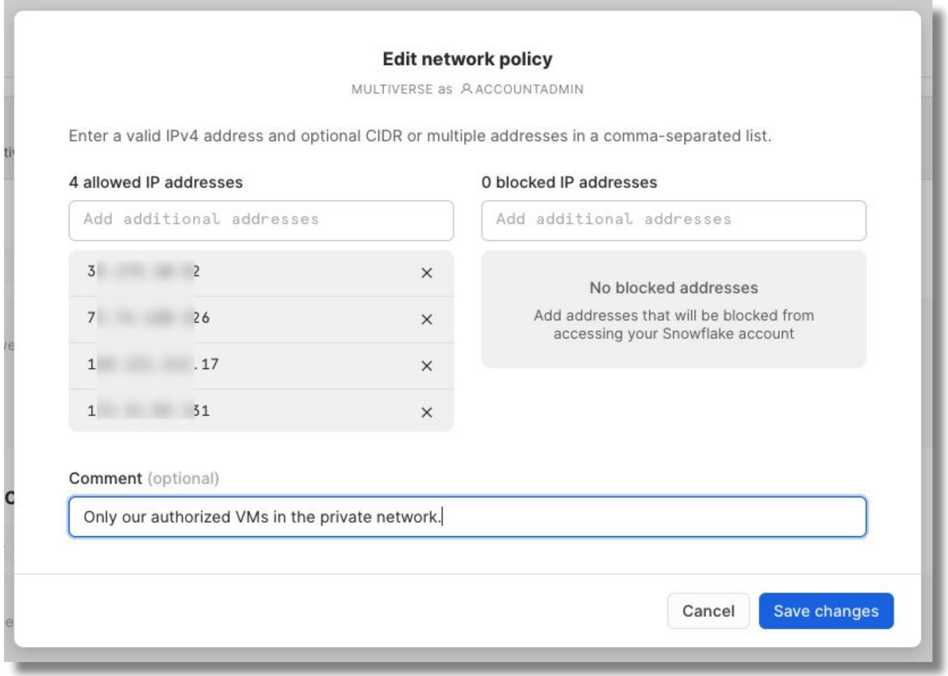
NETWORK CONTROLS – NETWORK POLICIES

- **Network Policies encapsulate an IP allowlist and an IP blocklist**
- **Customer-configured Network Policy**

Network policies can be applied at three levels

1. **Snowflake Account**
   - All traffic will use this policy, unless there is a more specific one.
   - Control is applied at authentication time.
2. **Outside Integration**
   - Applies to traffic at the integration endpoint only. For example: SCIM or OAuth security integrations.
3. **User Specific**
   - Applies to the specific user only.
   - Best practice for users used as service accounts.

The most specific policy always wins.



Edit network policy

MULTIVERSE as ACCOUNTADMIN

Enter a valid IPv4 address and optional CIDR or multiple addresses in a comma-separated list.

4 allowed IP addresses

Add additional addresses

3[redacted]2 ×

7[redacted]26 ×

1[redacted].17 ×

1[redacted]31 ×

0 blocked IP addresses

Add additional addresses

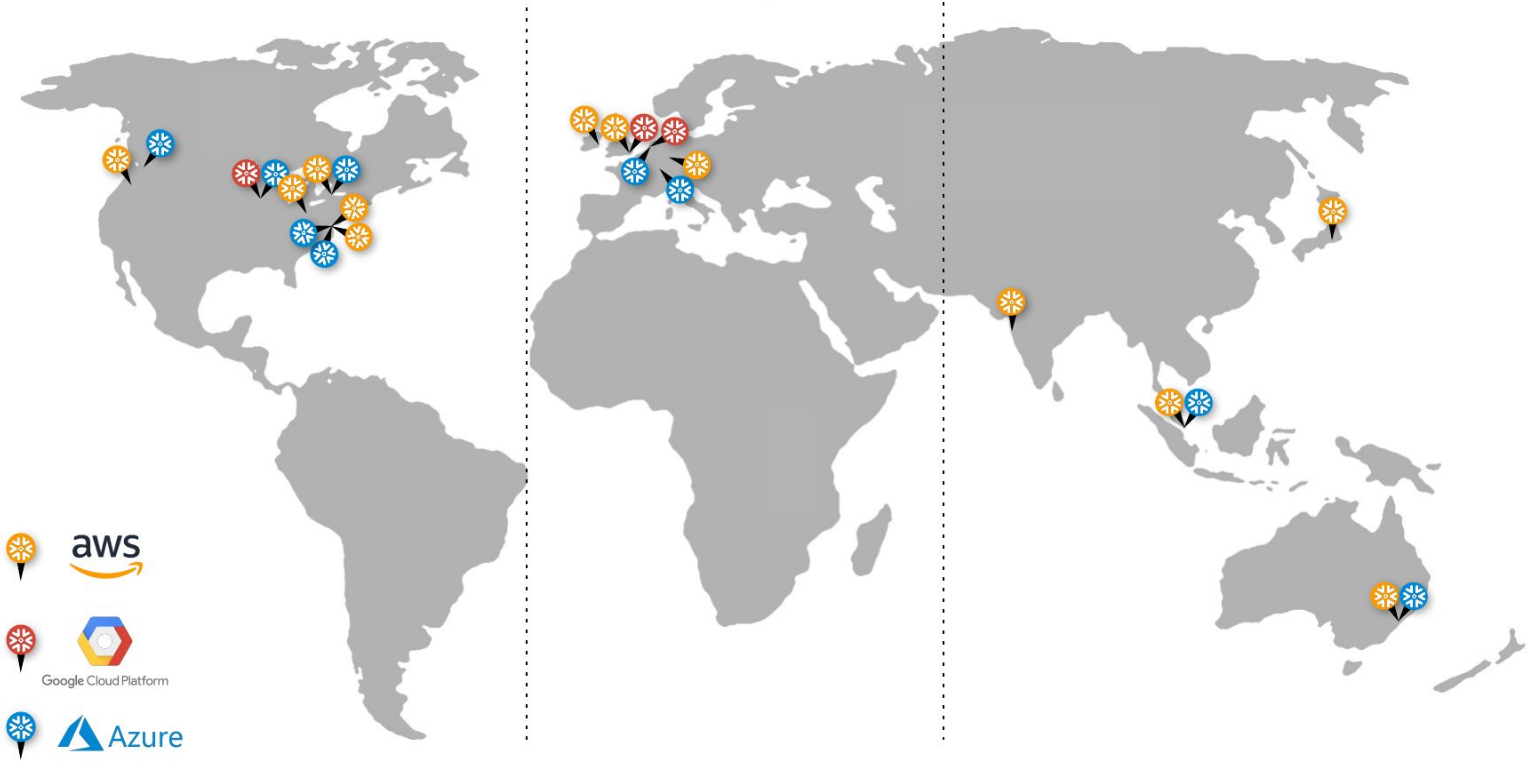
No blocked addresses

Add addresses that will be blocked from accessing your Snowflake account

Comment (optional)

Only our authorized VMs in the private network.

NETWORK CONTROLS – ANY SUPPORTED REGION

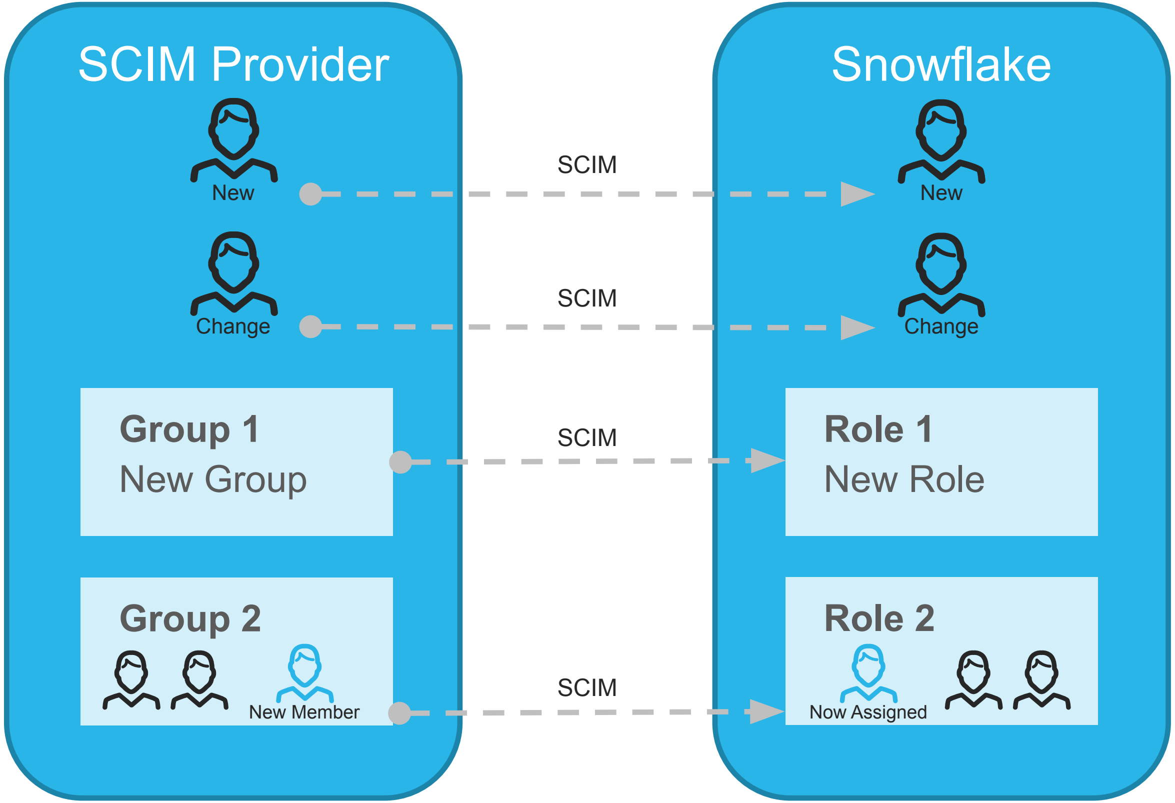


[Most up-to-date list of Snowflake regions]

USER PROVISIONING WITH SCIM

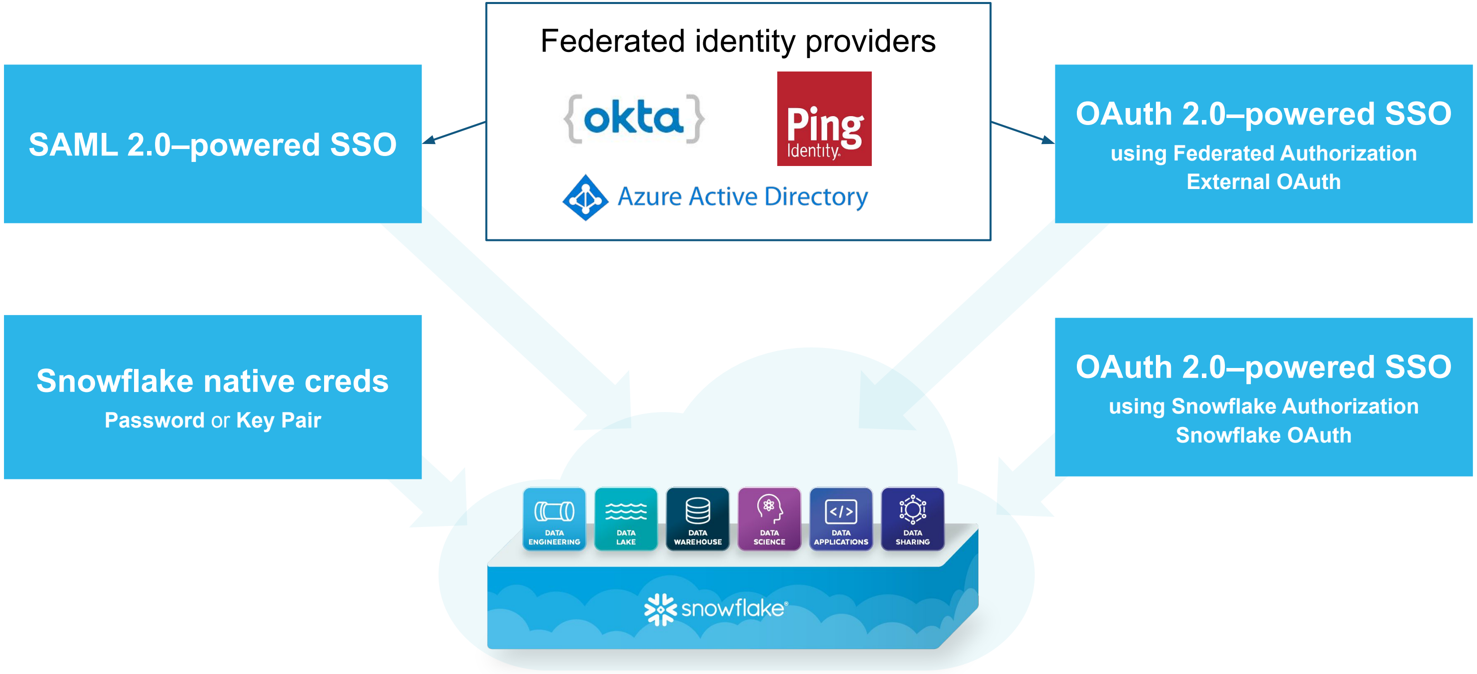
Authoritative Directory in Control

- User creation, changes, & deletes
- Roles driven by group membership
- Use Okta, Azure AD, or any system that speaks SCIM, *or...*
- Any system that can use SQL



SNOWFLAKE AUTHENTICATION

How to do Authentication & Delegated Authorization for Snowflake



Federated identity providers

SAML 2.0–powered SSO

Snowflake native creds
Password or **Key Pair**

OAuth 2.0–powered SSO
using Federated Authorization
External OAuth

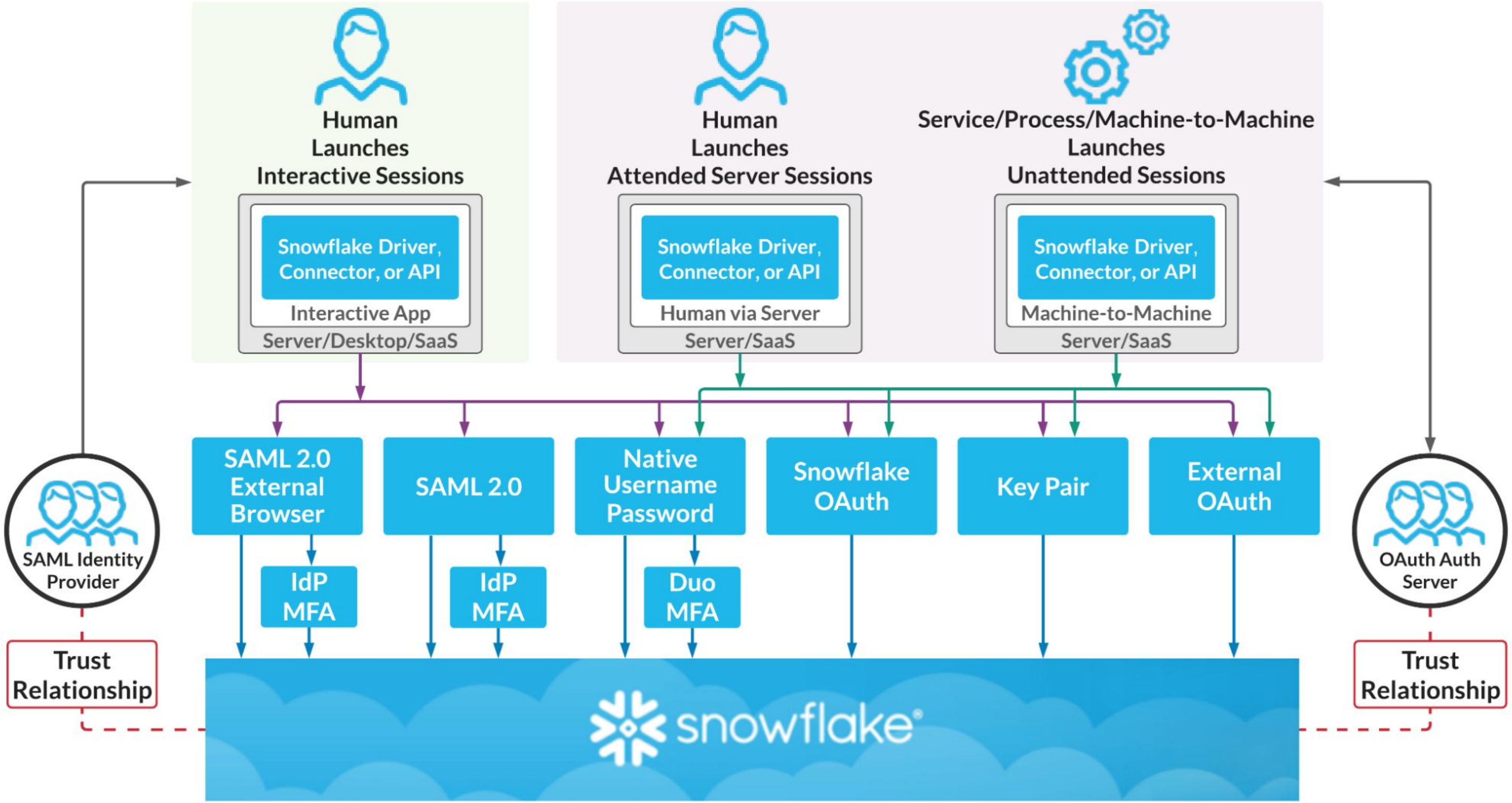
OAuth 2.0–powered SSO
using Snowflake Authorization
Snowflake OAuth

- Users may have multiple authN & authZ methods all configured at once
- “External Browser” mode can bring SSO to desktop apps that do not natively support it
- Integrate easily with a secrets management platform like Hashicorp Vault

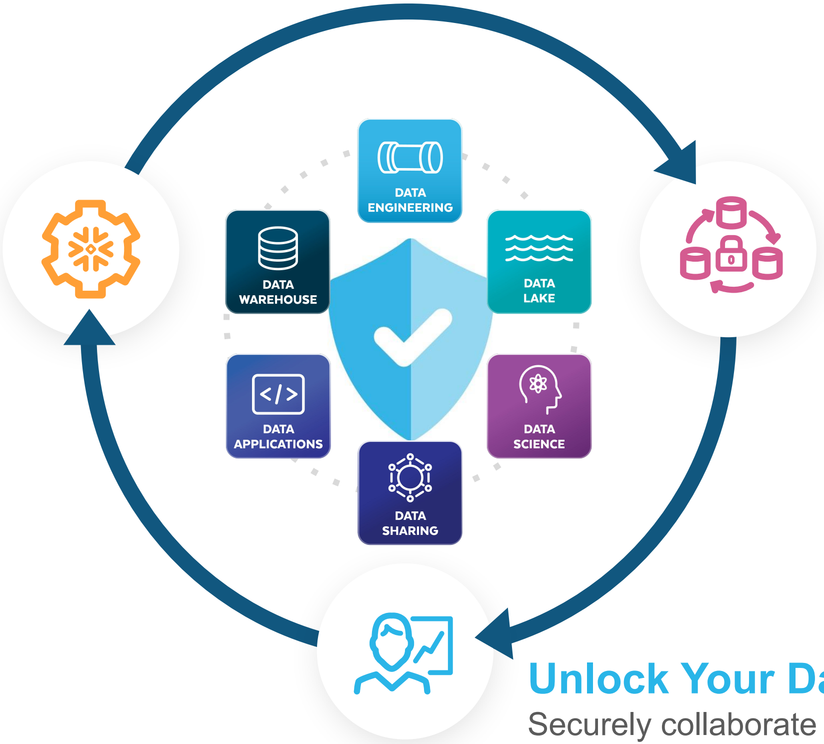
Please note: Partners shown are a sample list and not the full list of supported platforms.

SNOWFLAKE AUTHENTICATION

How to do Authentication & Delegated Authorization for Snowflake



SNOWFLAKE GOVERNANCE



Know Your Data

Understand, classify, and track data and its usage

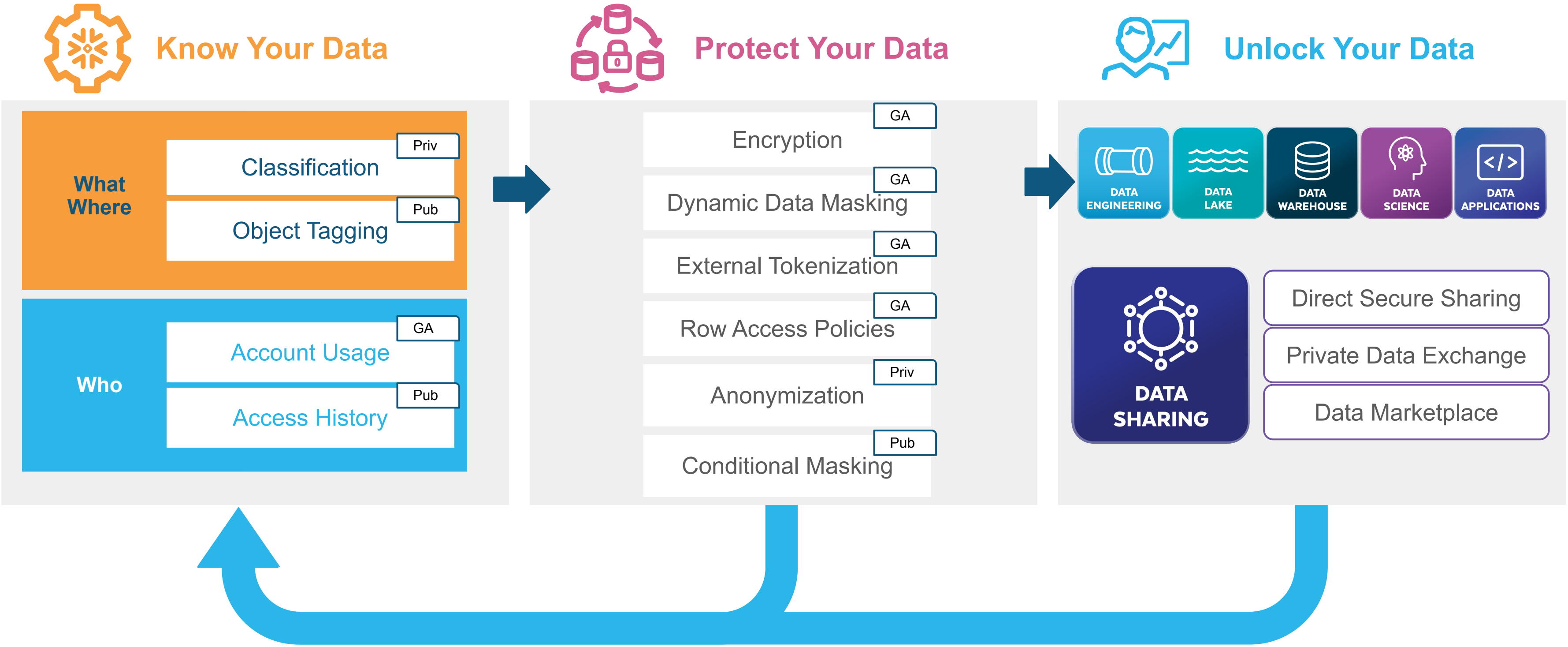
Protect Your Data

Secure sensitive data with policy-based access controls

Unlock Your Data

Securely collaborate and share data across teams

SNOWFLAKE GOVERNANCE CAPABILITIES



Know Your Data

What Where
- Classification — Priv
- Object Tagging — Pub

Who
- Account Usage — GA
- Access History — Pub

Protect Your Data

- Encryption — GA
- Dynamic Data Masking — GA
- External Tokenization — GA
- Row Access Policies — GA
- Anonymization — Priv
- Conditional Masking — Pub

Unlock Your Data

- DATA ENGINEERING
- DATA LAKE
- DATA WAREHOUSE
- DATA SCIENCE
- DATA APPLICATIONS

DATA SHARING
- Direct Secure Sharing
- Private Data Exchange
- Data Marketplace

Start with a Table

name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357

We start with a table

- The table has been instantiated from the encrypted, at-rest files (micro-partitions)
- The information in the table is opaque to Snowflake
- This table contains data “in the clear,” but you might load data that’s been modified in some way to protect it as well

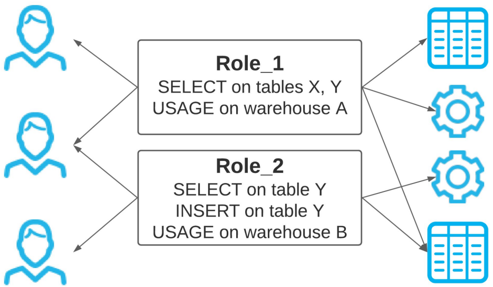
RBAC, DAC, Views, UDFs

RBAC & DAC

Views & UDFs

name	age	zip_code
J Smith	3-	790**
J Doe	5-	770**
M Taylor	4-	770**
M Gaines	7-	790**

name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357



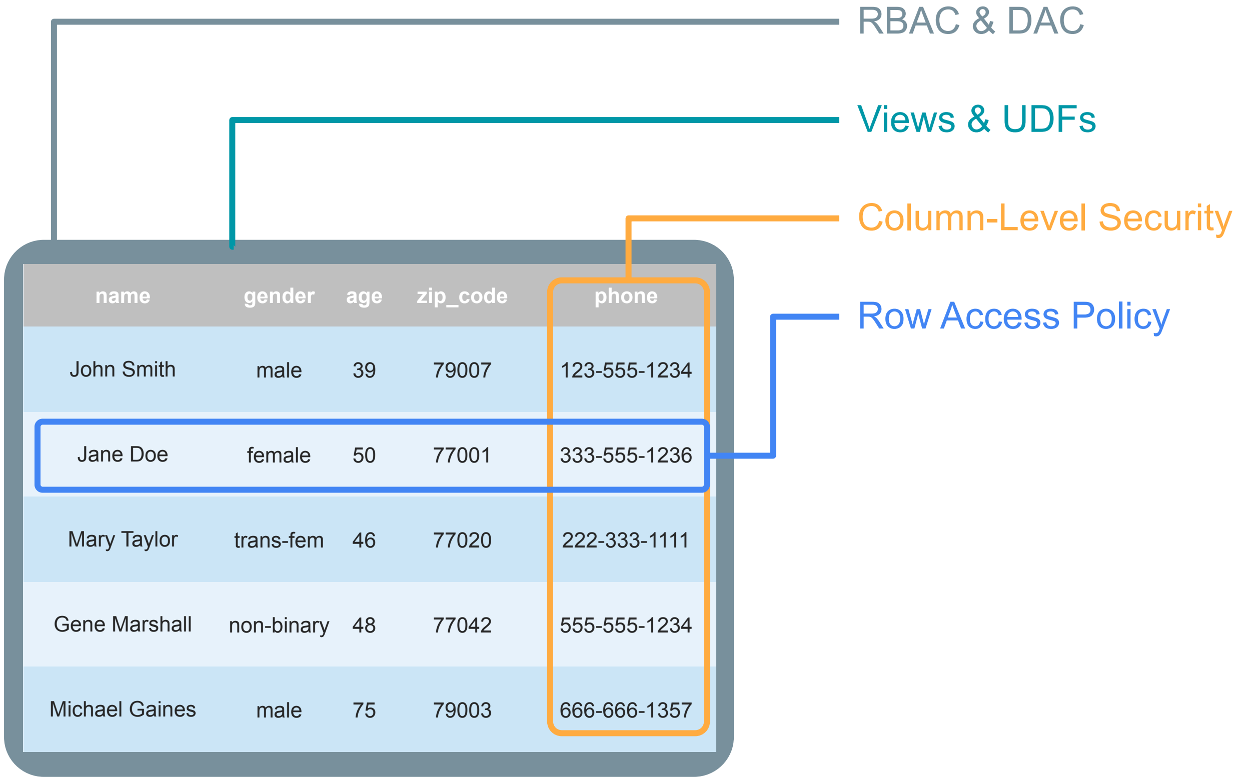
RBAC & DAC Protect the table

- Every object in Snowflake is subject to these controls, and they are at the whole-object level
- RBAC inheritance and other RBAC features apply
- The customer controls RBAC completely
- DAC (Discretionary Access Control) applies to the role that owns the object, unless the object is subject to Managed Schema Access

You may also create Views & UDFs

- These are mostly used to redact or transform rows, columns, or even cells, and create a new object
- The new object has RBAC and DAC controls

CLS & RAP



RBAC & DAC

Views & UDFs

Column-Level Security

Row Access Policy

name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357

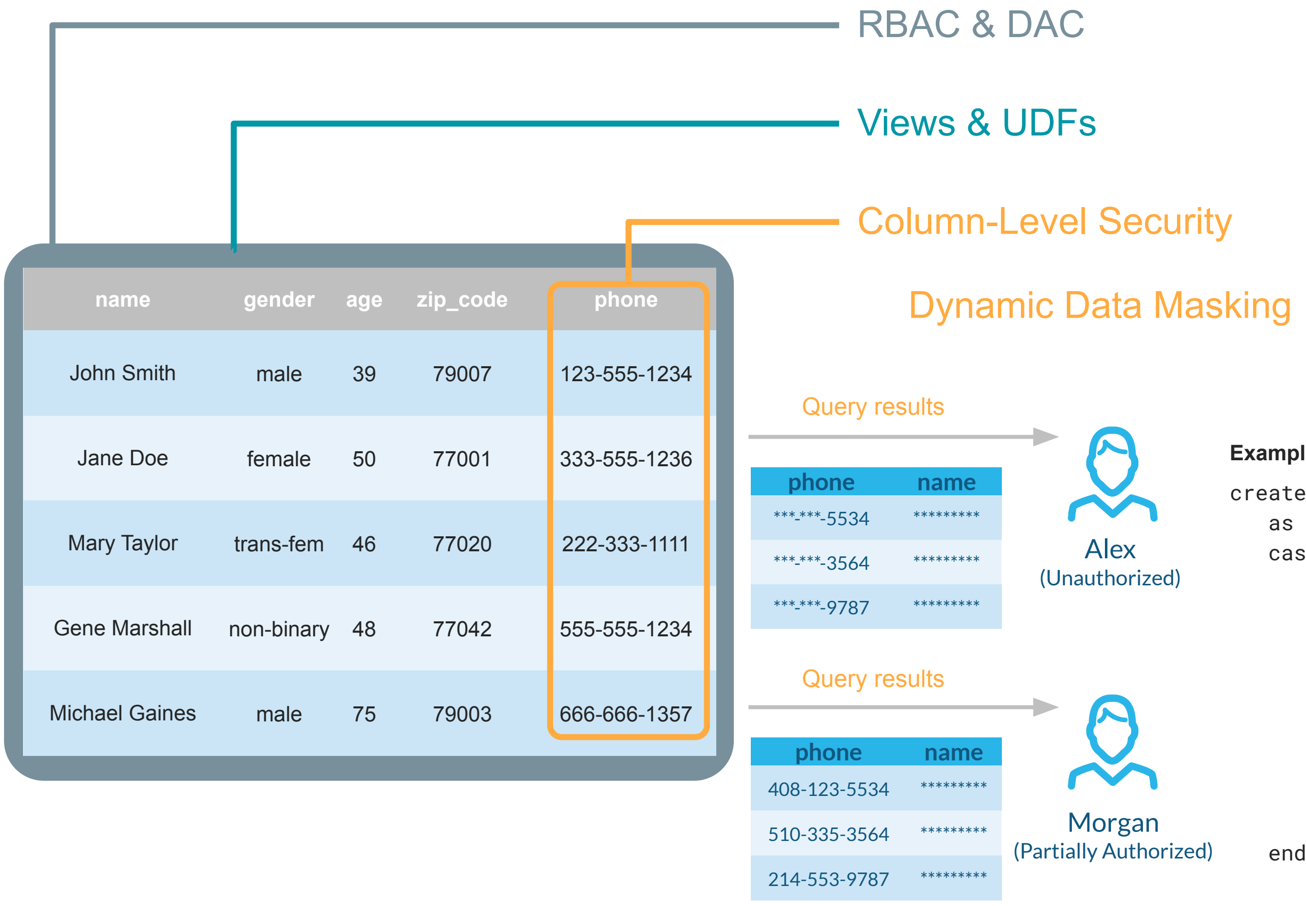
We can use Policy controls for Columns and Rows

- Prevent View/UDF explosion
- Table/View owners and privileged users (such as ACCOUNTADMIN) unauthorized to data by default
- Ensure controls are applied in any context where the object's data is used

We get more ease of management

- Centrally manage policies
- Apply a single policy to multiple tables
- Built-in separation of duty: policy admins assign and users are subject to policy controls
- All application and use is fully audited

Dynamic Data Masking



name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357

phone	name
--5534	*********
--3564	*********
--9787	*********

phone	name
408-123-5534	*********
510-335-3564	*********
214-553-9787	*********

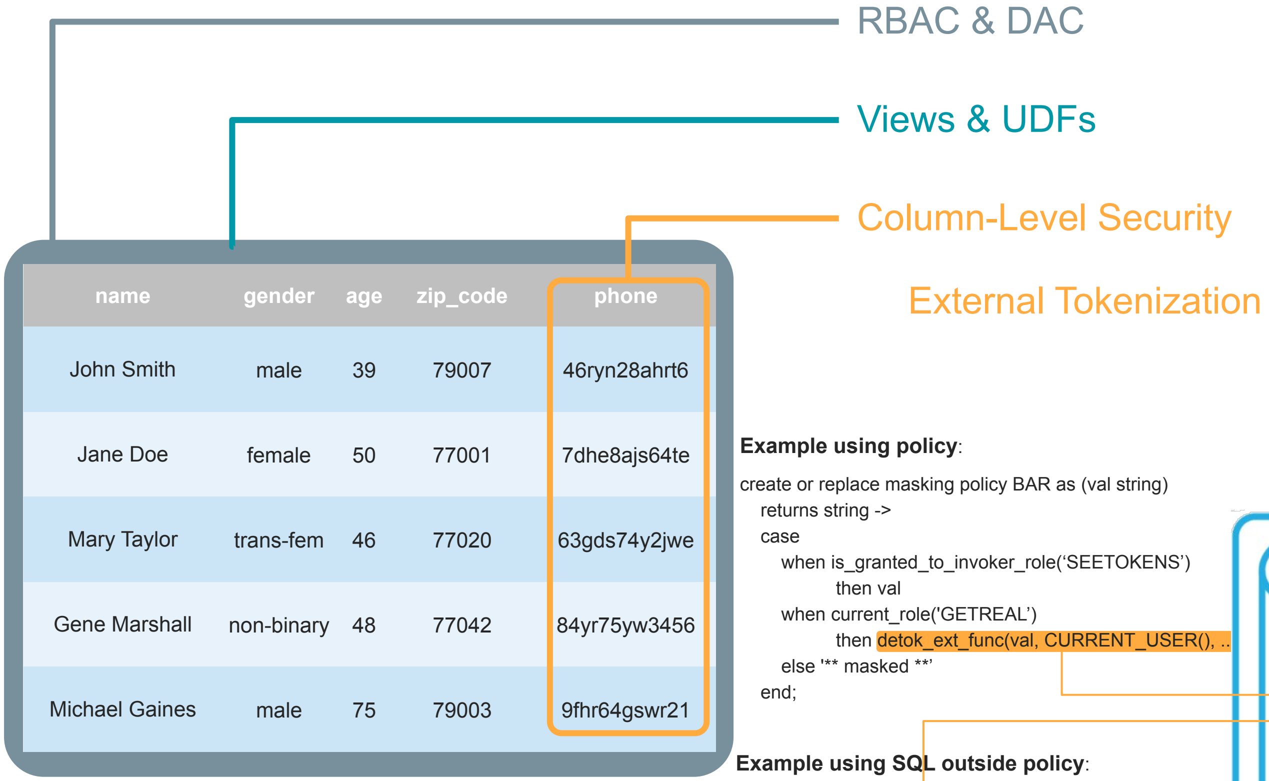
We can leverage Column-Level Security to dynamically mask data at query time

- No change to the stored data
- Mask or partially mask using constant value, hash, and custom functions
- Unmask for authorized users only

Example:

```
create or replace masking policy FOO
   as (val string) returns string ->
   case
      when is_granted_to_invoker_role(‘SEECLEAR’)
           then val
      when current_role('ONLYPART')
           then regexp_replace(val, '[0-9]', '*', 7)
      when is_role_in_session('CRYPTO')
           then decrypt_raw(val, KEY, IV, ...)
      when is_role_in_session('BESPOKE')
           then user_defined_Func(val, baz, ...)
      else '** masked **’
   end;
```

External Tokenization



RBAC & DAC

Views & UDFs

Column-Level Security

External Tokenization

name	gender	age	zip_code	phone
John Smith	male	39	79007	46ryn28ahrt6
Jane Doe	female	50	77001	7dhe8ajs64te
Mary Taylor	trans-fem	46	77020	63gds74y2jwe
Gene Marshall	non-binary	48	77042	84yr75yw3456
Michael Gaines	male	75	79003	9fhr64gswr21

Ingest protected (PII/PHI) data as Externally Tokenized

- Using tokenization provider functionality upstream from Snowflake

De-tokenize for authorized users at query time

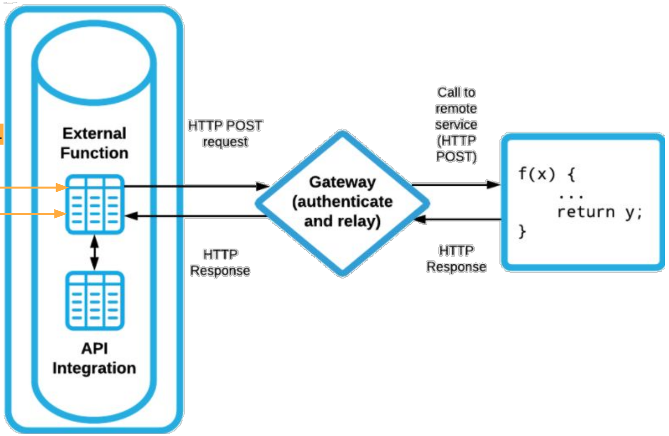
- Tokenization provider called using a Snowflake External Function to de-tokenize data
- For unauthorized users, third-party service is not called
- Can be used in policy or outside

Example using policy:

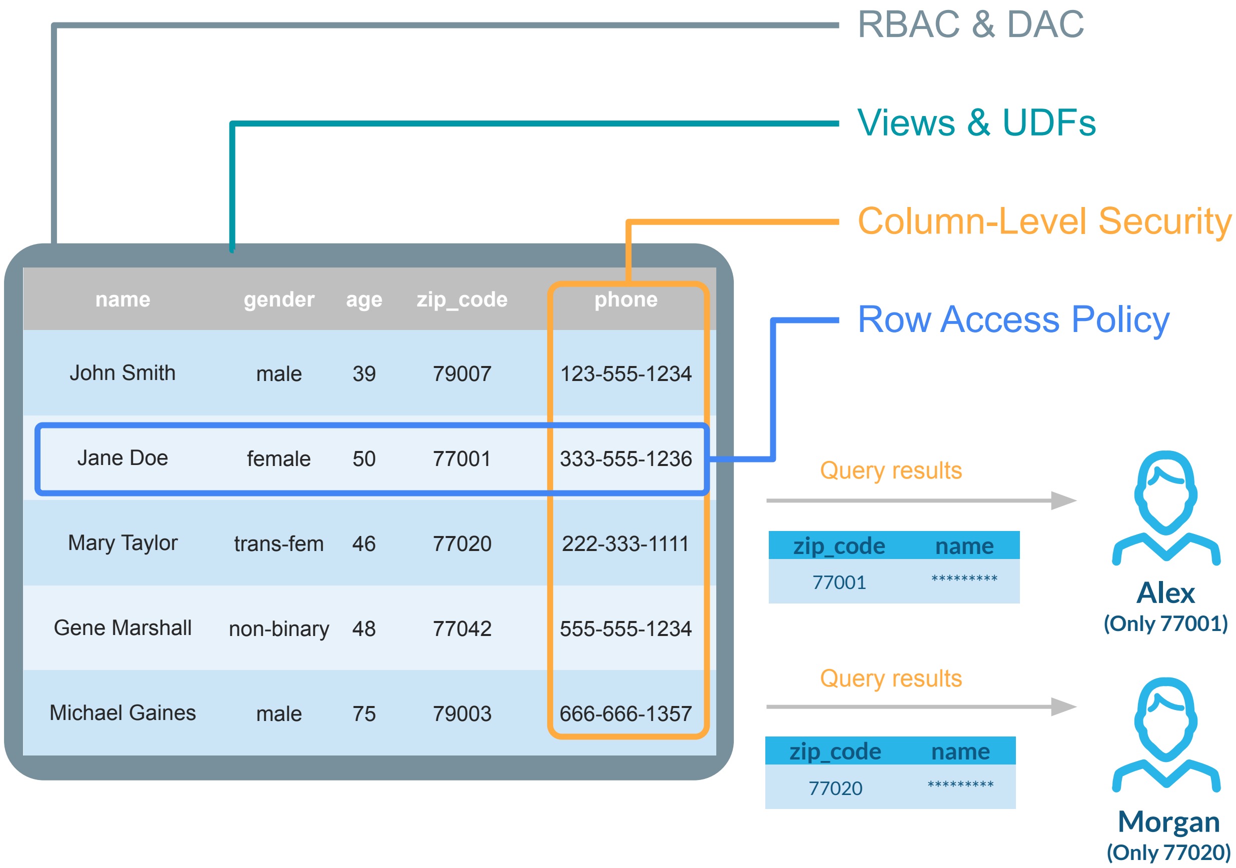
```
create or replace masking policy BAR as (val string)
  returns string ->
  case
    when is_granted_to_invoker_role(‘SEETOKENS’)
           then val
    when current_role('GETREAL’)
           then detok_ext_func(val, CURRENT_USER(), ..
    else '** masked **’
  end;
```

Example using SQL outside policy:

```
SELECT detok_ext_func(T1.phone) AS REAL_PHONE
    ,T1.GENDER
    ,T2.ZIP
 FROM T1
    JOIN T2
      ON T2.PHONE = T1.PHONE
;
```



Row Access Policy



name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357

zip_code	name
77001	*********

zip_code	name
77020	*********

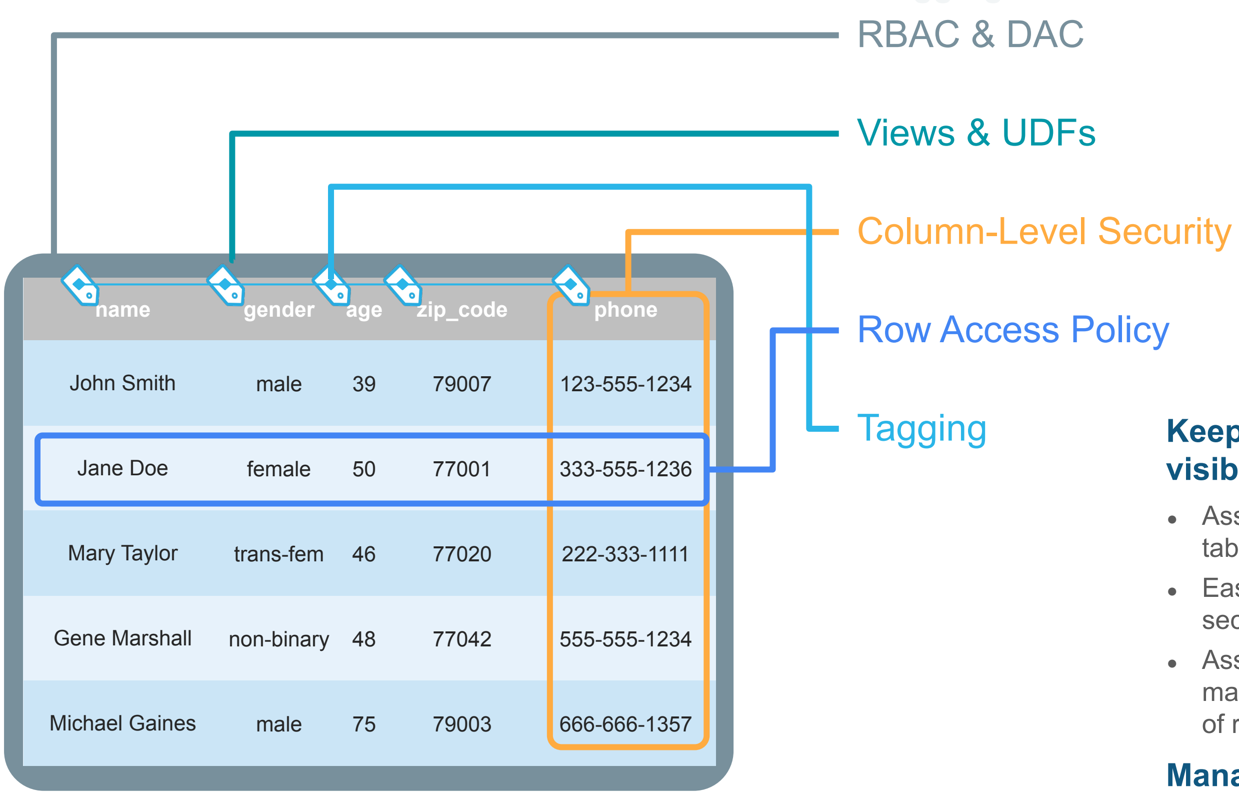
Filter rows at query time based on user role and lookup table

- Policy contains condition(s) to allow or filter out rows
- Policy is applied to one or more table, view, or external table in an account
- Dynamically generated predicate filters out rows the user is not authorized to see at query time
- Can be combined with other controls

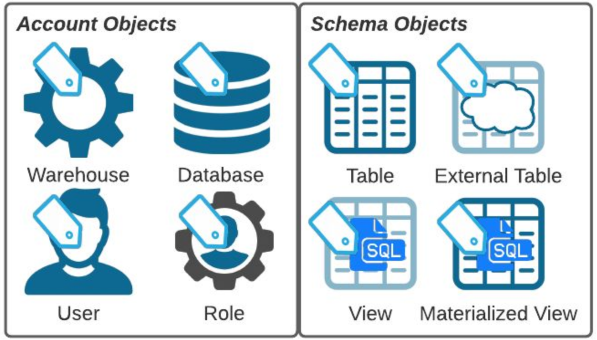
Example:

```
create or replace row access policy FOO
   as (this_zip varchar) returns boolean ->
       'all_seeing_role' = current_role()
       or
       exists (
           select 1 from zip_mapping_table
           where info_reader = current_role()
           and zip_code = this_zip
       )
;
```

Tagging



name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357



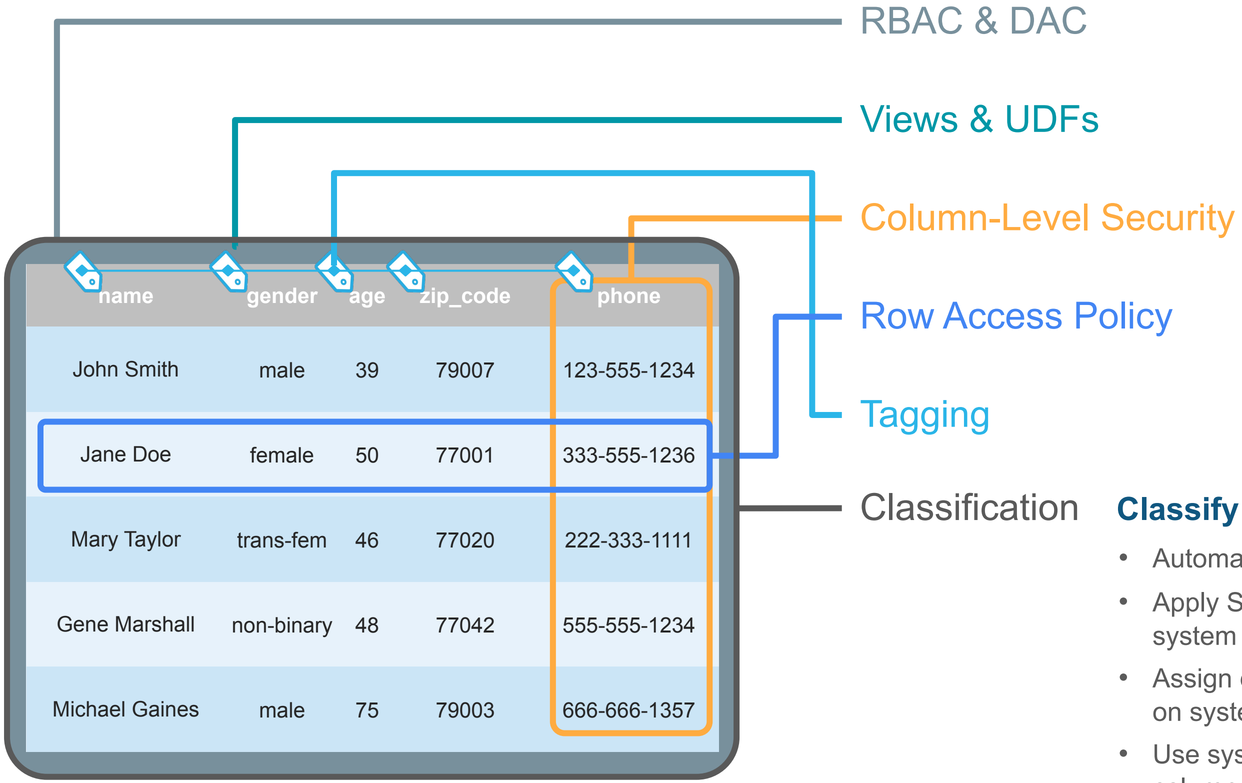
Keep track of sensitive data for visibility and compliance

- Assign tags to sensitive columns, tables, external tables, or views
- Easily audit sensitive objects without appropriate security policies
- Assign tags to virtual warehouses, Snowpipe, materialized views, and clustered tables to keep track of resource usage for cost visibility and attribution

Manage tags with flexible administration models

- Centralized tag creation and assignment for centrally managed governance
- Decentralized tag assignment controlled by privileges for object owner-supplied tag value

Classification



RBAC & DAC

Views & UDFs

Column-Level Security

Row Access Policy

Tagging

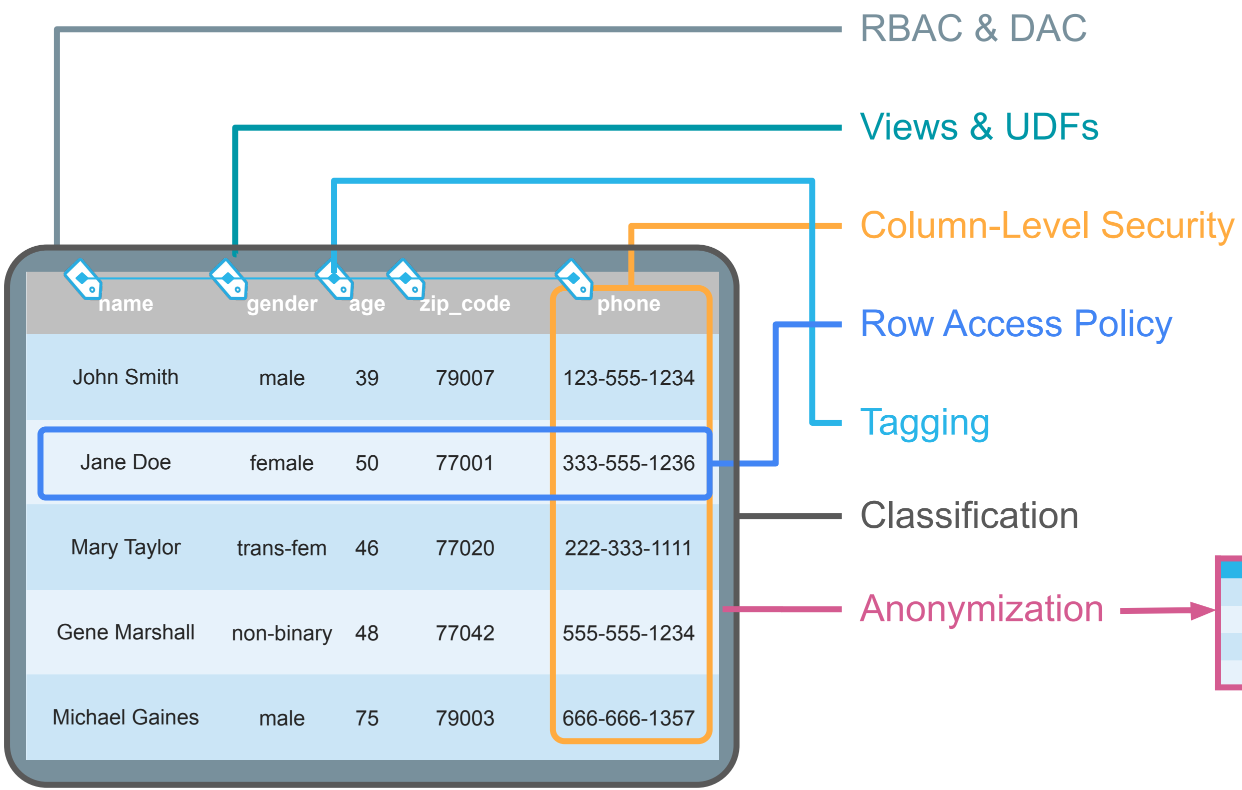
Classification

name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357

Classify columns containing personal data

- Automatically detect columns with personal data
- Apply Snowflake-defined semantic and privacy category system tags
- Assign data access policies to columns based on system tags
- Use system tags to audit personal data among millions of columns
- Seamlessly integrates across Snowflake's governance capabilities and Data Sharing
- Populate and manipulate tags using third-party GRC, MDM, and other classification solutions

Anonymization



name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357

Protect personal data and retain analytical value

- Set level of protection to meet your internal policies
- Optimize for your analytic use case
- Help comply with privacy regulations

Maintain protection during updates

- Dynamically applied
- Role-based controls dictate who can view personal data at query time

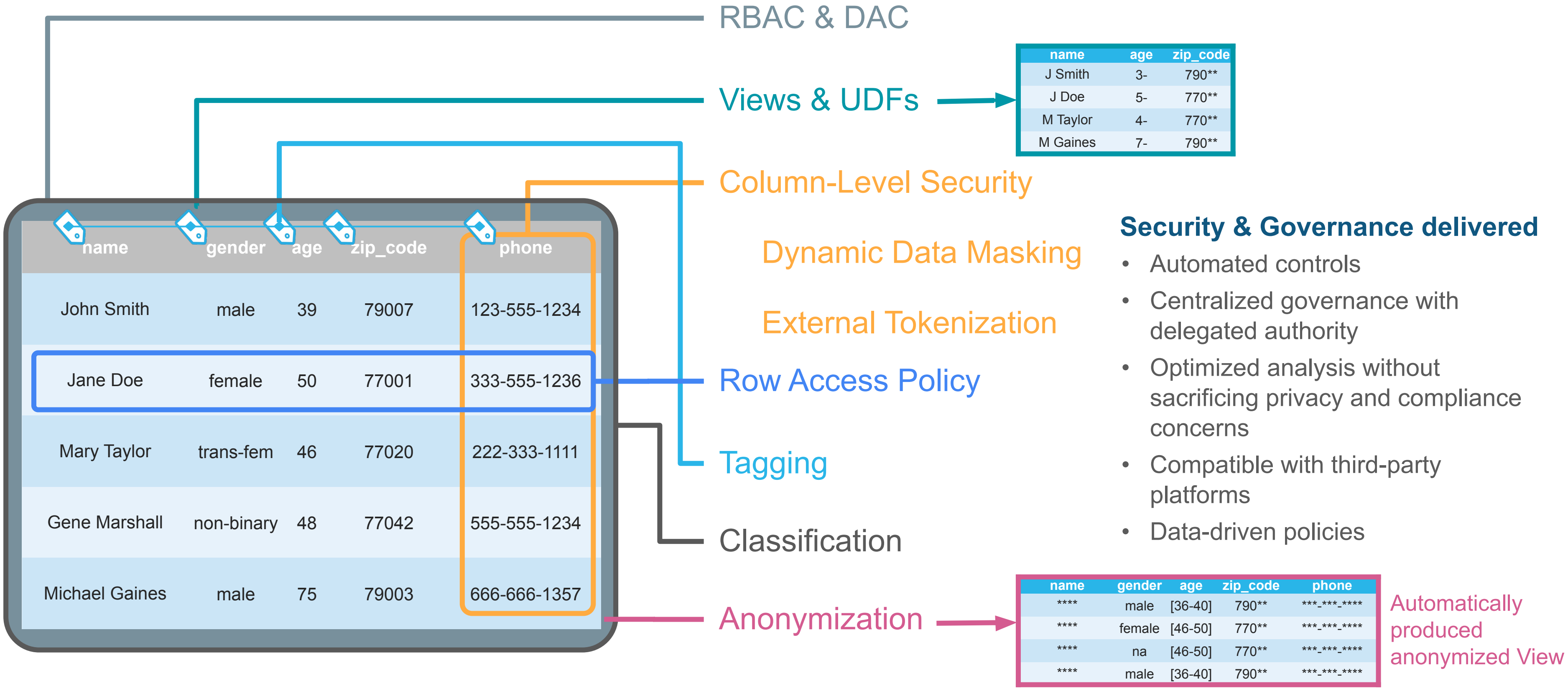
name	gender	age	zip_code	phone
****	male	[36-40]	790**	***_***_****
****	female	[46-50]	770**	***_***_****
****	na	[46-50]	770**	***_***_****
****	male	[36-40]	790**	***_***_****

Automatically produced anonymized View

Industry standard built for Snowflake

- Utilize native k-Anonymity algorithm
- Integrated, centralized access controls
- Share data internally and externally while protecting personal information

All Data Gov Features



name	gender	age	zip_code	phone
John Smith	male	39	79007	123-555-1234
Jane Doe	female	50	77001	333-555-1236
Mary Taylor	trans-fem	46	77020	222-333-1111
Gene Marshall	non-binary	48	77042	555-555-1234
Michael Gaines	male	75	79003	666-666-1357

name	age	zip_code
J Smith	3-	790**
J Doe	5-	770**
M Taylor	4-	770**
M Gaines	7-	790**

name	gender	age	zip_code	phone
****	male	[36-40]	790**	***_***_****
****	female	[46-50]	770**	***_***_****
****	na	[46-50]	770**	***_***_****
****	male	[36-40]	790**	***_***_****

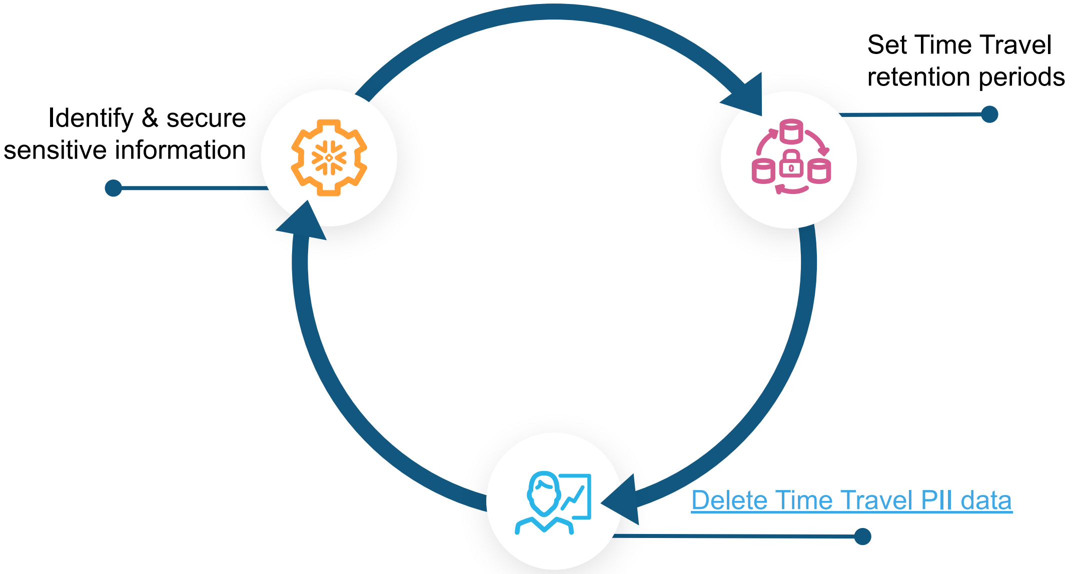
Automatically produced anonymized View

Security & Governance delivered

- Automated controls
- Centralized governance with delegated authority
- Optimized analysis without sacrificing privacy and compliance concerns
- Compatible with third-party platforms
- Data-driven policies

TIME TRAVEL & FAIL-SAFE

GDPR, CCPA, and other emerging regulations allow individuals to request the deletion of their personal information, unless exceptions apply. This means your Snowflake recovery policies must properly align to your organization's compliance policies.



Identify & secure sensitive information

Set Time Travel retention periods

Delete Time Travel PII data

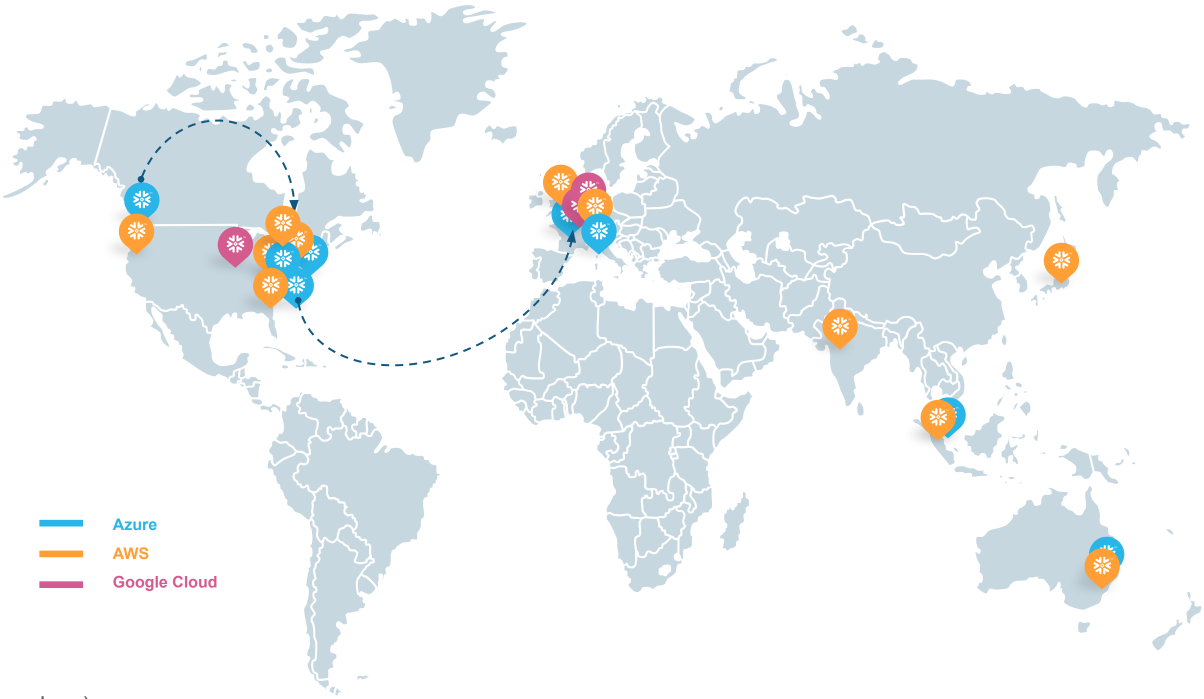
Snowflake provides product features for customers to meet the demands of data privacy regulations.

- Time Travel & Fail-safe have data retention implications
- Up to 90 days (Time Travel)
- 7 days (Fail-safe)
- For PII erasure requests, you must consider Time Travel and its setting.

More on Time Travel & Fail-safe

DATABASE REPLICATION & FAILOVER

1. **Cross-Cloud & Cross-Region Replication**
   - Business continuity & disaster recovery
   - Secure data sharing across regions/clouds
   - Data portability for account migrations
2. **Zero Performance Impact on Primary**
   - Asynchronous replication
3. **Reduced Data Loss**
   - Incremental refreshes
4. **Instant Recovery**
   - Read: Readable secondary databases
   - Write: Database failover
5. **Secure**
   - Data encrypted at-rest & in-transit
   - Tri-Secret Secure compatible
6. **Cost Effective**
   - Replication costs: Data transfer & compute (serverless)
   - Control which databases to replicate



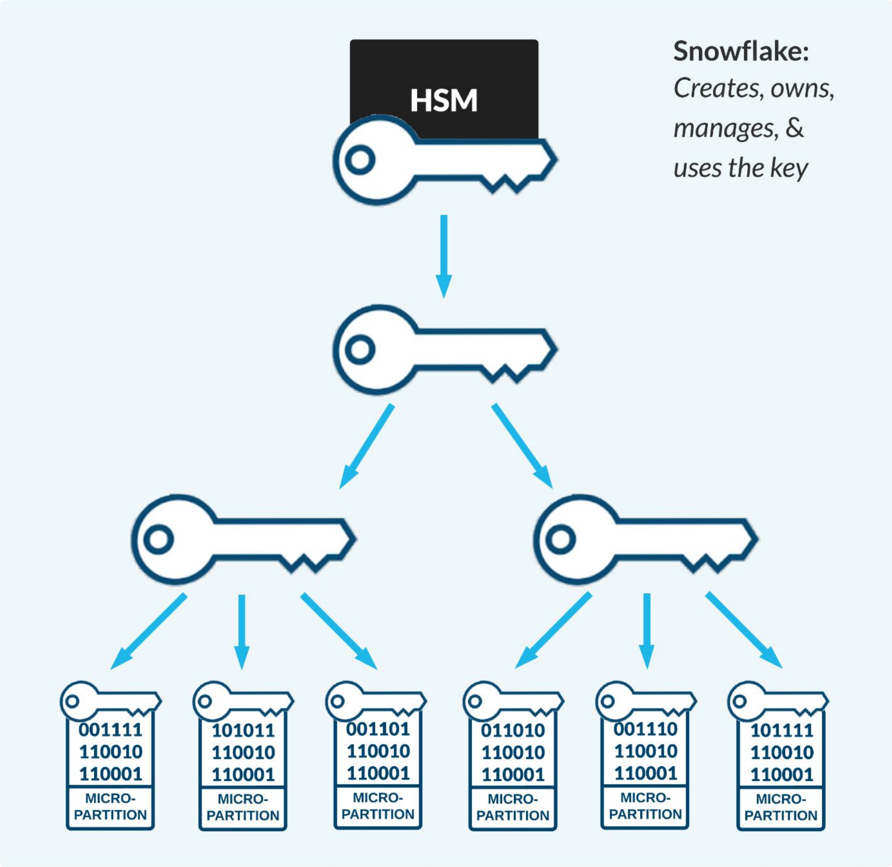
More about Database Replication & Failover

HIERARCHICAL KEY MODEL

Account Master Key

Object Master Keys (*e.g.* Table Master Keys, Result Master Keys, Stage Master Keys)

File Keys



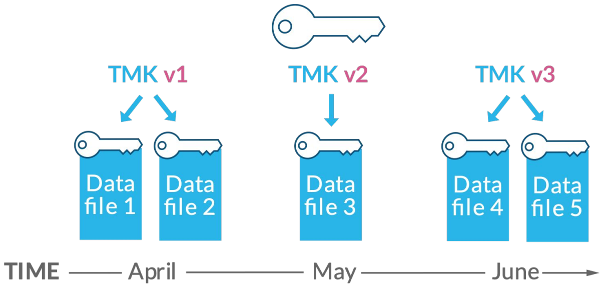
Snowflake:
Creates, owns, manages, & uses the key

Hierarchical Key Model

- Hierarchical key model rooted in the CSP’s HSM
  - GCP: Cloud HSM
  - AWS: Cloud HSM
  - Azure: Dedicated HSM
- All data at rest is encrypted by default, with no configuration required

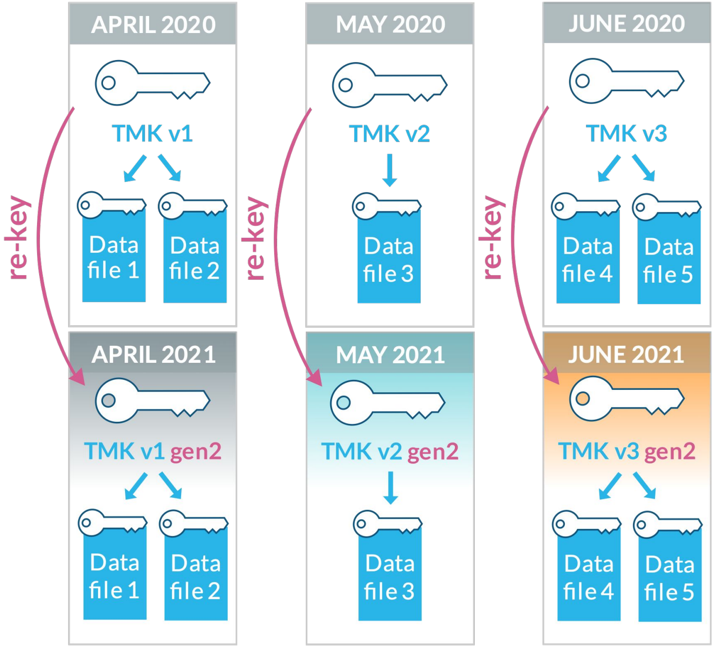
More resources on Key Management

KEY ROTATION & RE-KEYING



Key Rotation

- Snowflake rotates keys every 30 days
- Process is transparent to customer and queries

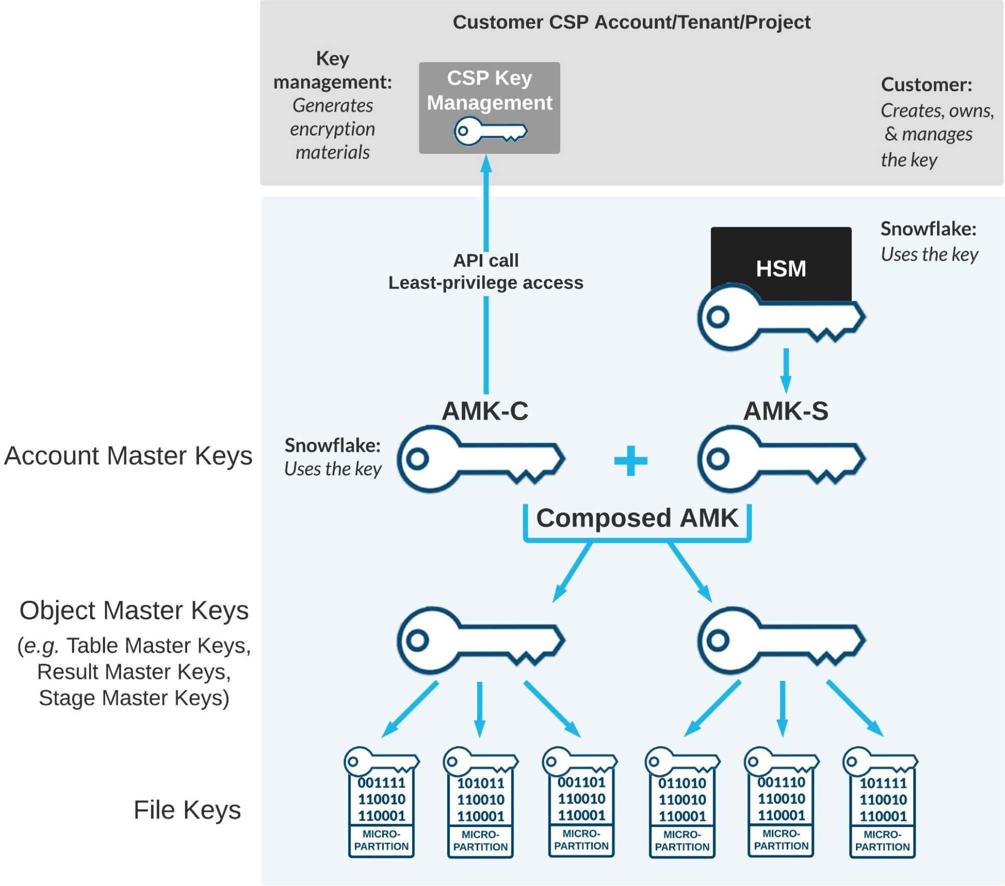


Key Re-Keying

- Yearly re-keying re-encrypts data on the key's birthday
- Re-keying requires Enterprise Edition or better
- Process is transparent to customer and queries

More resources on Key Management

TRI-SECRET SECURE KEY MODEL


Customer CSP Account/Tenant/Project
Key management: *Generates encryption materials*
CSP Key Management
Customer: *Creates, owns, & manages the key*
API call
Least-privilege access
HSM
Snowflake: *Uses the key*
AMK-C
AMK-S
Snowflake: *Uses the key*
+
Composed AMK
Account Master Keys
Object Master Keys
(*e.g.* Table Master Keys, Result Master Keys, Stage Master Keys)
File Keys
001111 110010 110001 MICRO-PARTITION
101011 110010 110001 MICRO-PARTITION
001101 110010 110001 MICRO-PARTITION
011010 110010 110001 MICRO-PARTITION
001110 110010 110001 MICRO-PARTITION
101111 110010 110001 MICRO-PARTITION

Hierarchical Key Model using Tri-Secret Secure

- Hierarchical key model adds a hybrid HYOK & BYOK model to give the customer control
- Customer holds key in their CSP Key Management and brings key materials to Snowflake to be part of the key-encrypting key (the Account Master Key or *AMK*)
- CSP-supported key managers:
  - GCP: Cloud KMS
  - AWS: AWS KMS
  - Azure: Key Vault

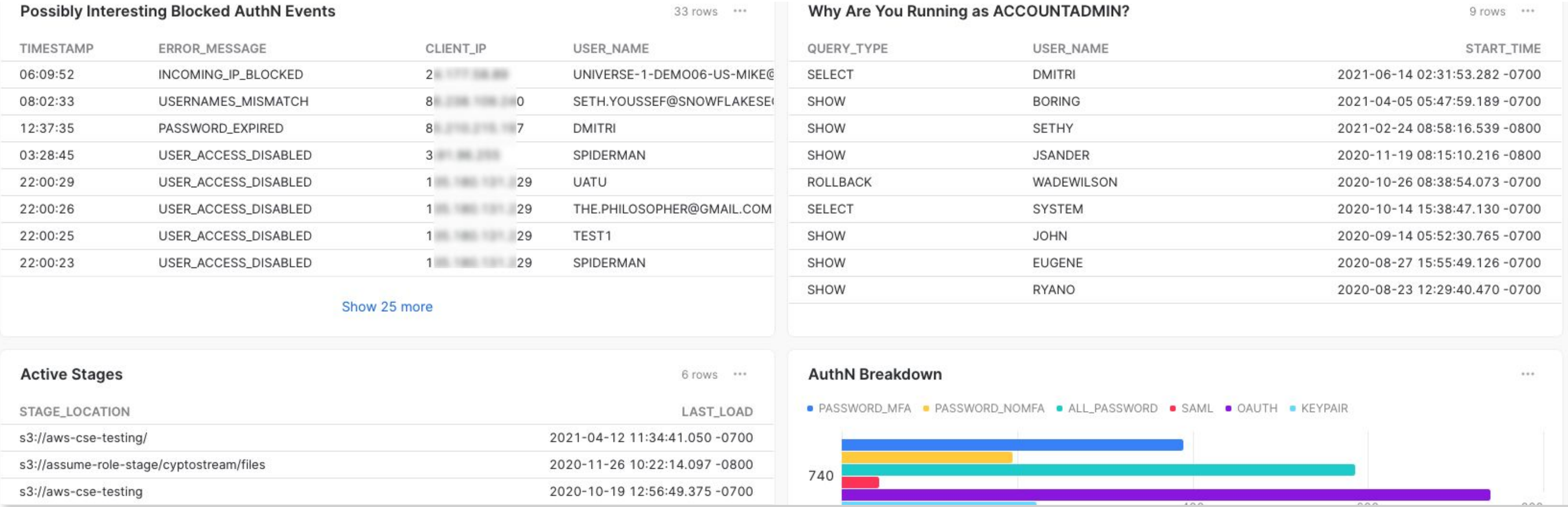
More resources on Key Management

AUDIT LOGGING – ACCOUNT USAGE

Auditing tracks every user's activity at all times in full detail

Kept in a tamper-proof area of your account for 365 days

All supplied drivers and connectors also have extended logging



Possibly Interesting Blocked AuthN Events

33 rows ···

TIMESTAMP	ERROR_MESSAGE	CLIENT_IP	USER_NAME
06:09:52	INCOMING_IP_BLOCKED	2[redacted]	UNIVERSE-1-DEMO06-US-MIKE@
08:02:33	USERNAMES_MISMATCH	8[redacted]0	SETH.YOUSSEF@SNOWFLAKESE(
12:37:35	PASSWORD_EXPIRED	8[redacted]7	DMITRI
03:28:45	USER_ACCESS_DISABLED	3[redacted]	SPIDERMAN
22:00:29	USER_ACCESS_DISABLED	1[redacted]29	UATU
22:00:26	USER_ACCESS_DISABLED	1[redacted]29	THE.PHILOSOPHER@GMAIL.COM
22:00:25	USER_ACCESS_DISABLED	1[redacted]29	TEST1
22:00:23	USER_ACCESS_DISABLED	1[redacted]29	SPIDERMAN

Show 25 more

Why Are You Running as ACCOUNTADMIN?

9 rows ···

QUERY_TYPE	USER_NAME	START_TIME
SELECT	DMITRI	2021-06-14 02:31:53.282 -0700
SHOW	BORING	2021-04-05 05:47:59.189 -0700
SHOW	SETHY	2021-02-24 08:58:16.539 -0800
SHOW	JSANDER	2020-11-19 08:15:10.216 -0800
ROLLBACK	WADEWILSON	2020-10-26 08:38:54.073 -0700
SELECT	SYSTEM	2020-10-14 15:38:47.130 -0700
SHOW	JOHN	2020-09-14 05:52:30.765 -0700
SHOW	EUGENE	2020-08-27 15:55:49.126 -0700
SHOW	RYANO	2020-08-23 12:29:40.470 -0700

Active Stages

6 rows ···

STAGE_LOCATION	LAST_LOAD
s3://aws-cse-testing/	2021-04-12 11:34:41.050 -0700
s3://assume-role-stage/cyptostream/files	2020-11-26 10:22:14.097 -0800
s3://aws-cse-testing	2020-10-19 12:56:49.375 -0700

AuthN Breakdown

···

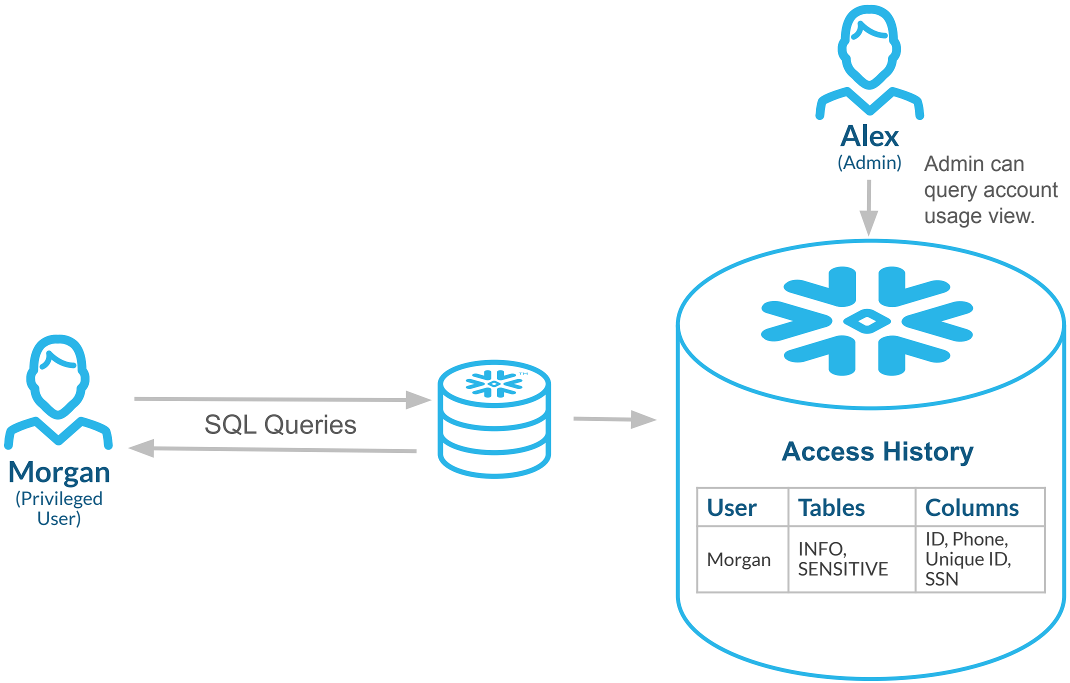
AUDIT LOGGING – ACCESS HISTORY

Access History supplies audit data access to comply with regulatory requirements and data governance initiatives.

- Access log of the tables, views, and columns each query accesses
- Includes base objects (*e.g.* table serving a view) indirectly accessed by the query
- Data access history available for easy reporting as a Account Usage View

Discover unused data to determine whether to archive or delete the data.

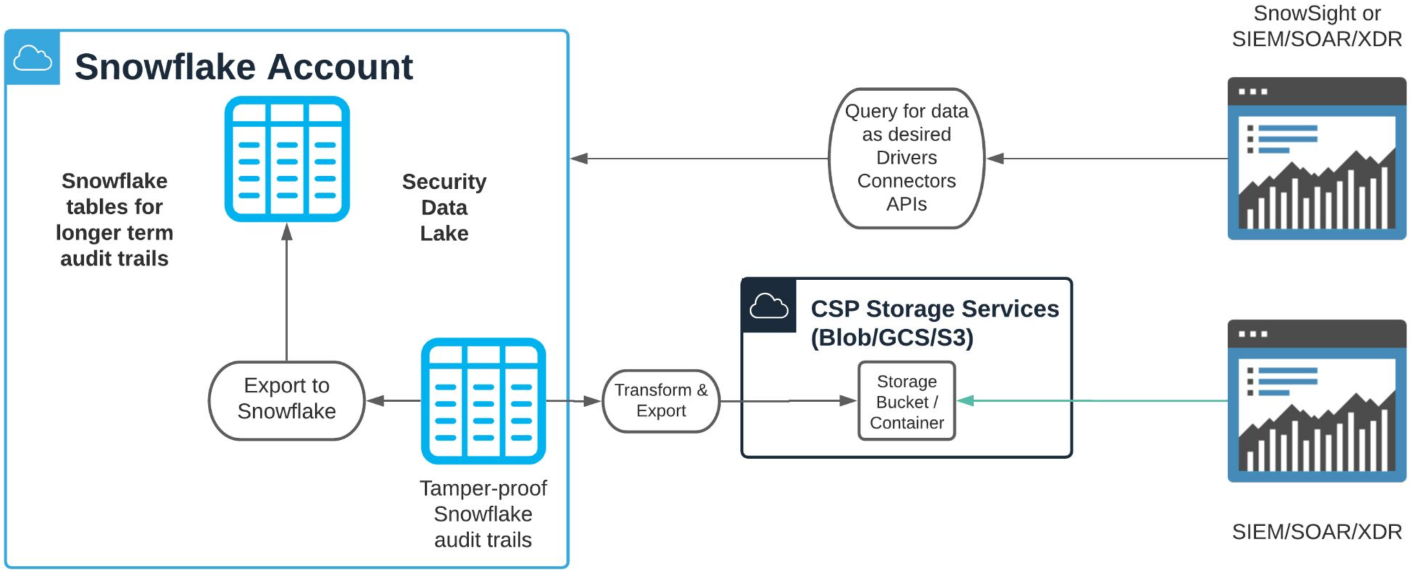
Notify users prior to altering a table, view, or column.



User	Tables	Columns
Morgan	INFO, SENSITIVE	ID, Phone, Unique ID, SSN

AUDIT LOGGING – EXPORTING AUDIT LOGS

- Results can be further filtered using SQL predicates
- Export through JDBC or as JSON for use in SIEM


SnowSight or SIEM/SOAR/XDR
Snowflake Account
Snowflake tables for longer term audit trails
Security Data Lake
Query for data as desired Drivers Connectors APIs
CSP Storage Services (Blob/GCS/S3)
Export to Snowflake
Transform & Export
Storage Bucket / Container
Tamper-proof Snowflake audit trails
SIEM/SOAR/XDR

INFRASTRUCTURE SECURITY & MONITORING

How is the Snowflake Infosec Team monitoring the service?

Snowflake's internal Critical Security Controls dashboard provides real-time risk visibility

- Access Control, Security Assessment & Authorization, Configuration Management, Security Awareness, *etc*. all represented on a single Dashboard
- Real-time monitoring of data loaded into Snowflake from internal and other relevant data sources

Snowflake uses CIS benchmark templates for configuration hardening

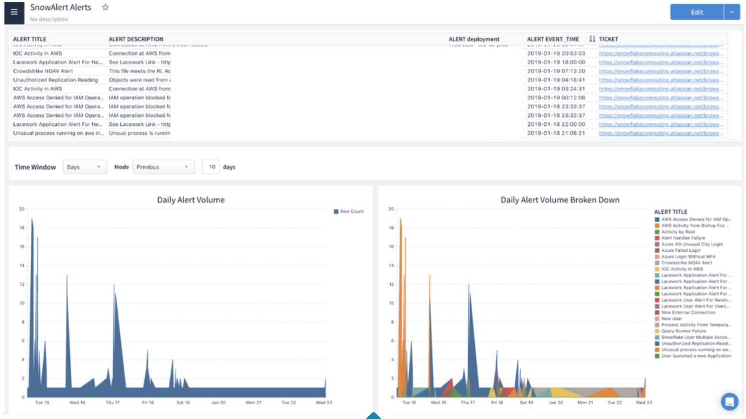
- Service configuration information is collected centrally in Snowflake
- Continuously and automatically tracked—unplanned changes cause alerts
- Part of the Snowflake Security Compliance Team's dashboard

Snowflake undergoes independent pentests

- Comprehensive Web Application Penetration Test – Annually
- Internal Network Penetration Test – Annually
- Major Functionality Penetration Tests – As major functionality is released as part of the SDLC

Snowflake performs weekly vulnerability scans on infrastructure

- Vulnerabilities are remediated per Security Policy
- Remediation trends tracked using Snowflake



SnowAlert Alerts ☆

No description

ALERT TITLE	ALERT DESCRIPTION	ALERT deployment	ALERT EVENT_TIME	TICKET
IOC Activity in AWS	Connection at AWS from		2019-01-19 20:53:03	https://snowflakecomputing.atlassian.net/brows...
Lacework Application Alert For Ne...	See Lacework Link - http		2019-01-19 18:00:00	https://snowflakecomputing.atlassian.net/brows...
Crowdstrike NGAV Alert	This file meets the RL Ac		2019-01-19 07:13:20	https://snowflakecomputing.atlassian.net/brows...
Unauthorized Replication Reading	Objects were read from a		2019-01-19 04:18:41	https://snowflakecomputing.atlassian.net/brows...
IOC Activity in AWS	Connection at AWS from		2019-01-19 03:24:31	https://snowflakecomputing.atlassian.net/brows...
AWS Access Denied for IAM Opera...	IAM operation blocked fc		2019-01-19 00:12:06	https://snowflakecomputing.atlassian.net/brows...
AWS Access Denied for IAM Opera...	IAM operation blocked fc		2019-01-18 23:33:37	https://snowflakecomputing.atlassian.net/brows...
AWS Access Denied for IAM Opera...	IAM operation blocked fc		2019-01-18 23:33:37	https://snowflakecomputing.atlassian.net/brows...
Lacework Application Alert For Ne...	See Lacework Link - http		2019-01-18 22:00:00	https://snowflakecomputing.atlassian.net/brows...
Unusual process running on aws in...	Unsual process is runnin		2019-01-18 21:06:21	https://snowflakecomputing.atlassian.net/brows...

Time Window: Days · Mode: Previous · 10 days

Edit
Daily Alert Volume
Row Count
0
2
4
6
8
10
12
14
16
18
20
Tue 15
Wed 16
Thu 17
Fri 18
Sat 19
Jan 20
Mon 21
Tue 22
Wed 23
Daily Alert Volume Broken Down
ALERT TITLE
AWS Access Denied for IAM Op...
AWS Activity from Bishop Fox ...
Activity by Root
Alert Handler Failure
Azure AD Unusual City Login
Azure Failed Login
Azure Login Without MFA
Crowdstrike NGAV Alert
IOC Activity in AWS
Lacework Application Alert For ...
Lacework Application Alert For ...
Lacework Application Alert For ...
Lacework Application Alert For ...
Lacework User Alert For NewIn...
Lacework User Alert For UserL...
New External Connection
New User
Process Activity From Tempora...
Query Runner Failure
Snowflake User Multiple Acces...
Unauthorized Replication Readi...
Unusual process running on aw...
User launched a new Application

GDPR – GENERAL DATA PROTECTION REGULATION

What is it?

- GDPR is an EU regulation that went into effect on May 25, 2018
- Governs the protection and processing of EU personal data

What does it mean in the context of Snowflake?

Different requirements apply to different types of entities:

- **Controller** – Snowflake customers are responsible for complying with GDPR independently from Snowflake
- **Processor** – Snowflake is responsible for the following:
  - Putting data processing addendums in place with our customers and our vendors
  - Only using our customers' EU personal data to provide our service to them
  - Being transparent about how we handle and process our customers' EU personal data on their behalf and keeping accurate records
  - Securing customers' EU personal data in our service
  - Facilitating our customers' compliance with data subject requests
  - Notifying customers about changes to our list of subcontractors

Snowflake responsibilities are documented in a Data Processing Addendum (DPA on snowflake.com/legal).

Available for signature now

USEFUL LINKS

- Snowflake Security Overview and Best Practices
- Snowflake Security Product Documentation
- Managing Governance in Snowflake

THANK YOU