Industrial-Strength Security

THE SNOWFLAKE ELASTIC DATA WAREHOUSE

WHITEPAPER

The Snowflake Elastic Data Warehouse is a completely new SQL data warehouse designed from the ground up for the cloud and modern data analytics. Snowflake's data warehouse was built with a unique new architecture to deliver cloud elasticity, native support for diverse data, and differentiated price:performance. Snowflake is delivered as an enterprise-class software-as-a-service (SaaS) offering running in the cloud.

Security is fundamental to the architecture, implementation, and operation of Snowflake's service. Every aspect of Snowflake is designed and operated to protect customer data. This philosophy and approach permeates Snowflake—from the CEO to every individual within the Snowflake team, security is a top priority.

SNOWFLAKE SECURITY FRAMEWORK

Snowflake has been designed to deliver end-to-end protection of data. We follow best-in-class, standards-based practices for the controls and processes that secure our service. As part of our overall security program, Snowflake leverages NIST 800-53 and the CIS Critical Security Controls, a set of controls created by a broad consortium of international security experts to identify the security functions that are effective against real-world threats.

The Snowflake service employs a multi-layered security architecture to protect customer data and access to that data. This architecture addresses the following:

- External interfaces
- Access control
- Data storage
- Physical infrastructure

This security architecture is complemented by the monitoring, alerts, controls, and processes that are part of Snowflake's comprehensive security program

Snowflake is a multi-tenant service that implements isolation at multiple levels.

The Snowflake service runs inside a virtual private cloud (VPC), a logically isolated network section within the Amazon Web Services (AWS) cloud. The VPC allows Snowflake to isolate and limit access to the internal components of the Snowflake service.

Snowflake also isolates query processing. Query processing is performed by one or more virtual warehouses, multi-node compute clusters created by customers using Snowflakeprovided interfaces. Each customer's virtual warehouses are dedicated to that customer and are isolated from other customers' virtual warehouses and from each other. In addition to being visible and accessible only to the customer that created them, virtual warehouses are visible and accessible only to the users within a customer account who have been granted access.

> "We came to the conclusion that we achieved better security with Snowflake than we could ever do on our own."
>
> — Bob Asensio, CIO, CapSpecialty

Snowflake also isolates data storage. Each customer's data is always stored in an independent directory structure, encrypted using customer-specific keys, and accessible only by that customer.

For customers who have HIPAA, PCI or other compliance requirements, Snowflake also offers its Enterprise for Sensitive Data (ESD) service. ESD provides customers with additional security features that help them meet these compliance requirements.

EXTERNAL INTERFACES

The Snowflake service is accessed via the Internet using secure protocols. Snowflake provides the following drivers and tools for connecting to the service:

- Standard ODBC and JDBC drivers
- The Snowflake command-line interface (CLI) client
- Snowflake's web-based user interface
- The Snowflake Python connector

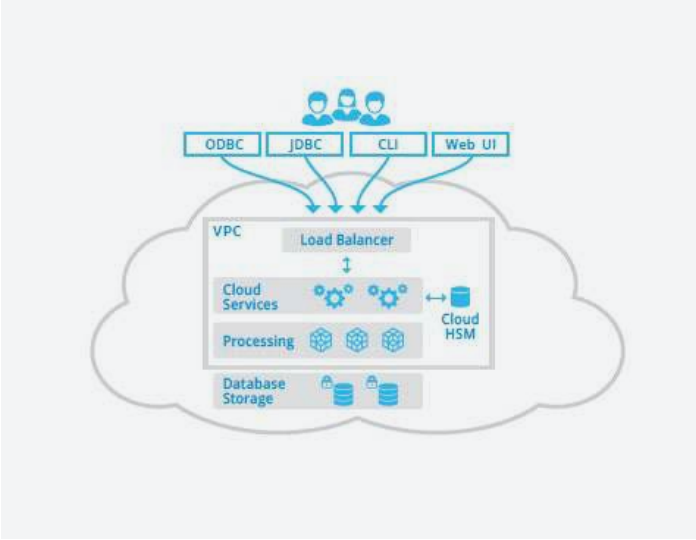
All communication across the Internet between users and the Snowflake service is secured and encrypted using TLS 1.2 or higher. Snowflake also supports IP address whitelisting to allow customers to restrict access to the Snowflake service to only trusted networks. Snowflake is a multi-tenant service that implements isolation at multiple levels.

ACCESS CONTROL

Authentication

Snowflake employs robust authentication mechanisms to control access to the Snowflake service.
Every request to the Snowflake service must be authenticated. User password hashes are securely stored, strong password policy is enforced, and various mechanisms are deployed by Snowflake to thwart bruteforce attacks. Snowflake also offers multi-factor authentication (MFA) as a built-in part of the Snowflake service and strongly recommends use of MFA for users with administrative privileges.

Additionally, for customers who who want to manage the authentication mechanism to their Snowflake account, Snowflake offers federated authentication for customers whose providers support SAML 2.0.



Snowflake ensures end-to-end security of data and access.

Authorization

The Snowflake service provides a sophisticated, role-based access control (RBAC) authorization framework to ensure that data and information can only be accessed by authorized users within an organization. Access control is applied to all database objects including tables, schemas, and virtual warehouses. Access control grants determine users' ability both to view and to operate on database objects.

In Snowflake's access control model, users are assigned one or more roles, and access privileges on objects are granted to roles. For every access to database objects, the Snowflake service validates that the necessary privileges have been granted to a role assigned to the user.

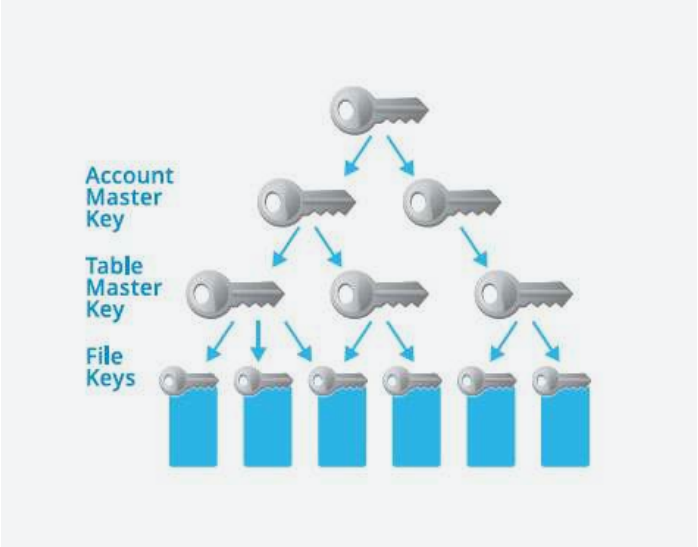
Snowflake provides a set of built-in roles for each customer and allows customers to create and define custom roles within the role hierarchy defined by Snowflake.

Data Storage

We protect all data stored in Snowflake from unauthorized access and from data loss by incorporating data encryption, access restrictions, and data protection mechanisms.

Data Encryption

In Snowflake all customer data is always encrypted when stored on disk. Data is encrypted when it is moved into a Snowflakeprovided staging location for loading into Snowflake, while it is stored within a database object in Snowflake, when it is cached within a virtual warehouse, and when we store a query result. For data stored in a customer-provided staging location, Snowflake recommends that the data be encrypted by the customer, but if that data is not encrypted Snowflake will immediately encrypt the data when it is loaded into a Snowflake database.



Snowflake employs a hierarchical key model to securely encrypt data

Snowflake uses strong AES 256 bit encryption with a hierarchical key model rooted in a cluster of Hardware Security Modules. Each customer account has a separate key hierarchy of account level, table level, and file level keys. Account and table keys are automatically rotated on a regular basis by the Snowflake service. Data encryption and key management is entirely transparent to the customer and requires no configuration or management.

Data Protection

Snowflake also protects data from accidental or intentional destruction due to user errors, system failures, or malicious acts. Snowflake's Time Travel feature makes it possible to instantly restore or query any previous version of data in a table or database within a specified retention period. Snowflake provides a one-day retention period by default, however longer periods are available for customers based on their chosen service agreement.

For more information, please refer to our: Continuous Data Protection whitepaper.

Security Monitoring and Alerting

Snowflake uses multiple security tools and processes to monitor security and raise alerts when necessary. Among the tools in use are file integrity monitoring tools (FIM), which are used to ensure that critical system files (e.g. important system and application executable files, libraries, and configuration files) have not been tampered with. These integrity checks identify any suspicious system alterations such as owner or permissions changes to files or directories, alert on the use of alternate data streams which could be used to hide malicious activities, and detect the introduction of new files.

Security events are centrally stored in a tamper-resistant Security Information and Event Management (SIEM) product where they are automatically analyzed and permanently stored for future forensic purposes. Alerting mechanisms automatically notify Snowflake security personnel in the event of detection of malicious or anomalous activity.

Snowflake offers daily security reports for customers who want to review who has accessed their Snowflake environment.

Physical Security

The Snowflake service is hosted in Amazon Web Services (AWS) datacenters and is available in multiple AWS regions. AWS data centers are certified as ISO 27001 and PCI/DSS Service Provider Level 1 and employ many physical security measures (including biometric access controls, twentyfour-hour armed guards and video surveillance) to ensure that no unauthorized access is permitted. As a standard AWS security measure, neither Snowflake personnel nor Snowflake customers have access to these data centers.

SECURITY COMPLIANCE

Snowflake works with certified third party auditors to attain, maintain, and validate Snowflake security.

- SOC 2, Type II: Snowflake has completed attestation and audit.
- HIPAA: Snowflake is HIPAA compliant and is eligible to enter into a BAA with a covered entity.
- PCI: Snowflake is certified PCI DSS compliant

Snowflake also engages third parties to perform annual penetration testing against its environment and platform.

CONCLUSION: BUILT IN ENTERPRISE-CLASS SECURITY

All of these capabilities are built into the Snowflake Elastic Data Warehouse service to protect our customers' data and access to that data. Building these features into the Snowflake service makes it possible to deliver enterprise-class security by default, without the additional burdens of complexity and management that traditional solutions force customers to take on. The Snowflake Elastic Data Warehouse is a completely new SQL data warehouse designed from the ground up for the cloud and modern data analytics. Snowflake's data warehouse was built with a unique new architecture to deliver cloud elasticity, native support for diverse data, and differentiated price:performance. Snowflake is delivered as an enterprise-class software-as-a-service (SaaS) offering running in the cloud.

Security is fundamental to the architecture, implementation, and operation of Snowflake's service. Every aspect of Snowflake is designed and operated to protect customer data. This philosophy and approach permeates Snowflake—from the CEO to every individual within the Snowflake team, security is a top priority.

Snowflake is the only data warehouse built for the cloud. Snowflake delivers the performance, concurrency and simplicity needed to store and analyze all of an organization's data in one solution. Snowflake's technology combines the power of data warehousing, the flexibility of big data platforms and the elasticity of the cloud at a fraction of the cost of traditional solutions. Snowflake: Your data, no limits. Find out more at snowflake.net.

WP_SEC_1_7_052017