snowflake

Cloud Data Warehouse Security

HOW SNOWFLAKE SETS THE STANDARD

WHITEPAPER

The threat of a data security breach, someone gaining unauthorized access to an organization's data, is what keeps CEOs and CIOs awake at night. Such a breach can quickly turn into a public relations nightmare and result in lost business and steep fines from regulatory agencies. This is why Snowflake is committed to setting the industry standard for data warehouse security. All aspects of Snowflake's cloud data warehouse as a service — its architecture, implementation and operation — are designed to protect customer data in transit and at rest against both current and evolving security threats. At Snowflake, we lose sleep over data security so you don't have to.

SNOWFLAKE SECURITY FRAMEWORK

Snowflake has been designed to deliver end-to-end data security. We follow best-in-class, standards-based practices for the controls and processes that secure our service. As part of our overall security program, we leverage 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.

Snowflake comprises 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.

Security for compliance requirements

Snowflake is a multi-tenant service that implements isolation at multiple levels. It runs inside a virtual private cloud (VPC), a logically isolated network section within the Amazon Web Services (AWS) cloud. The VPC enables Snowflake to isolate and limit access to its internal components. Customers can choose from five editions that vary by available features and level of security. For customers who have HIPAA, PCI or other compliance requirements, Snowflake offers its Enterprise for Sensitive Data (ESD) service, which provides customers with additional security features. The edition that comprises the highest level of security, Virtual Private Snowflake (VPS), includes ESD and a dedicated version of Snowflake. For additional details about the five editions, see the later section, "Five Levels of Snowflake Security."

Snowflake also isolates query processing, which is performed by one or more compute clusters virtual warehouses. These are multi-node compute clusters created by customers using Snowflake-provided interfaces. Each customer's virtual warehouses are isolated from other customers' virtual warehouses. In addition, virtual warehouses are visible and accessible only to the users within a customer account and 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

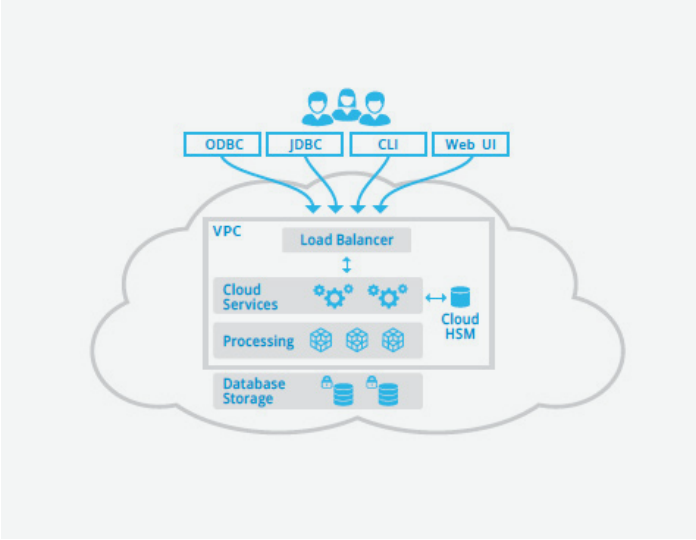
Snowflake also isolates data storage. Each customer's data is always stored in an independent directory and encrypted using customer-specific keys, which are accessible only by that customer.

EXTERNAL INTERFACES

Customers access Snowflake service via the Internet using secure protocols. Customers use the following drivers and tools to connect 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 Internet communication between users and the Snowflake service is secured and encrypted using TLS 1.2 or higher. Snowflake also supports IP address whitelisting to enable customersto restrict access to the Snowflake service by only trusted networks.



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

ACCESS CONTROL

Authentication

Snowflake employs robust authentication mechanisms. Every request to Snowflake must be authenticated. User password hashes are securely stored, strong password policy is enforced and various mechanisms are deployed by Snowflake to thwart brute-force attacks. Snowflake also offers built-in multi-factor authentication (MFA) and MFA for users with administrative privileges. For customers who want to manage the authentication mechanism to their account, and whose providers support SAML 2.0, Snowflake offers federated authentication.

Authorization

Snowflake provides a sophisticated, role-based access control (RBAC) authorization framework to ensure 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 a user's ability to both view and operate on database objects.

In Snowflake's access control model, users are assigned one or more roles, each of which can be assigned different access privileges. For every access to database objects, Snowflake validates that the necessary privileges have been granted to a role assigned to the user.

Customers can choose from a set of built-in roles or create and define custom roles within the role hierarchy defined by Snowflake.

Data Storage

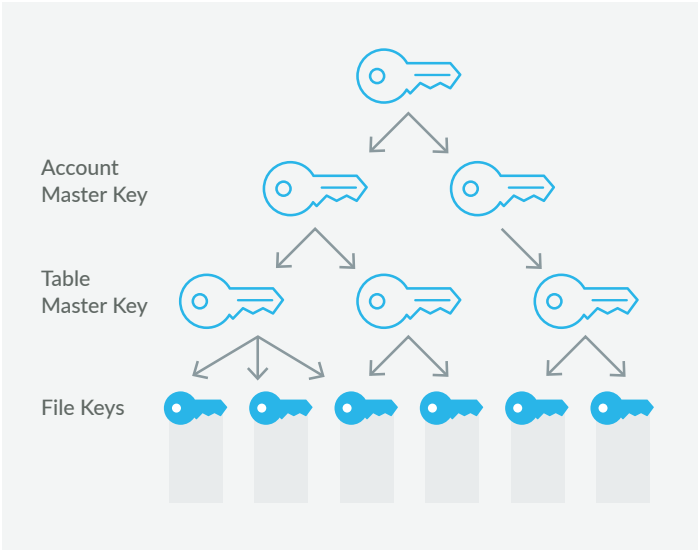
We protect all data stored in Snowflake from unauthorized access and from data loss by incorporating data encryption, access restrictions and data protection mechanisms.

Encryption Everywhere

In Snowflake, all customer data is always encrypted when stored on disk. Data is encrypted when it's moved into a Snowflake-provided staging location for loading into Snowflake. Data is also encrypted when it is stored within a database object in Snowflake, when it is cached within a virtual warehouse and when Snowflake stores a query result. For data stored in a customer-provided staging location, Snowflake recommends the customer store the data. If that data is not encrypted, Snowflake will immediately encrypt it when loaded into Snowflake.

Key Management

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. Snowflake automatically rotates account and table keys on a regular basis. Data encryption and key management are entirely transparent to the customer and require no configuration or management.



Snowflake employs a hierarchical key model to securely encrypt data

Data Protection

Snowflake also protects data from accidental or intentional destruction due to user errors, system failures or malicious acts. Using Snowflake's Time Travel feature, customers can instantly restore or query any previous version of data in a table or database within a specified retention period. By default, the retention period is one day, but longer periods are available based on the 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.

File Integrity Monitoring Tools (FIM)

FIM tools are used to ensure that critical system files, such as important system and application executable files, libraries and configuration files, have not been tampered with. These integrity checks identify any suspicious system alterations, which include owner or permissions changes to files or directories, the use of alternate data streams to hide malicious activities and 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. Alerts automatically notify Snowflake security personnel when malicious or anomalous activity is detected.

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

Physical Security

Snowflake is hosted in Amazon Web Services (AWS) data centers and is available in multiple AWS regions. AWS data centers are certified as ISO 27001 and PCI/DSS Service Provider Level 1. They employ many physical security measures, including biometric access controls and 24-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 validate and maintain 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.

FIVE LEVELS OF SNOWFLAKE SECURITY

Snowflake offers five editions of its data warehouse-as-a-service, with varying levels of security. Each subsequent version contains all the capabilities of the preceding versions. For example, the Enterprise version includes everything the Premiere version offers.

Enterprise

All data is re-encrypted annually. Federated authentication is also available so users can access Snowflake with a secure single sign-on. Snowflake's unique data protection feature, Time Travel, enables deleted or modified data to be restored to its original state for up to 90 days. Cross-region replication is also available in the Enterprise edition, making it possible to add additional redundancy to Snowflake's standard in-region replication.

Enterprise for Sensitive Data (ESD)

ESD is Snowflake's solution for customers with specific compliance requirements. It includes HIPAA support, is PCI compliant and features an enhanced security policy.

ESD enables customers to utilize Tri-Secret Secure: split encryption keys for multiple layers of data security.

When using Tri-Secret Secure, access to a customer's data requires the combination of the Snowflake encryption key, the customer encryption key (which is wholly owned by the customer) and valid customer credentials with role-based access to the data.

Because the data is encrypted with split keys, it is impossible for anyone beyond the customer, including Amazon, to gain access to the underlying data. Snowflake can gain access to the data only if the customer key and access credentials are provided to Snowflake. This ensures that only the customer can respond to demands for data access, regardless of where they come from.

Virtual Private Snowflake (VPS)

VPS represents the most sophisticated solution for customers with sensitive data. It differs from other Snowflake editions in a number of important ways.

With VPS, all of the servers that contain in-memory encryption keys are unique to each customer.

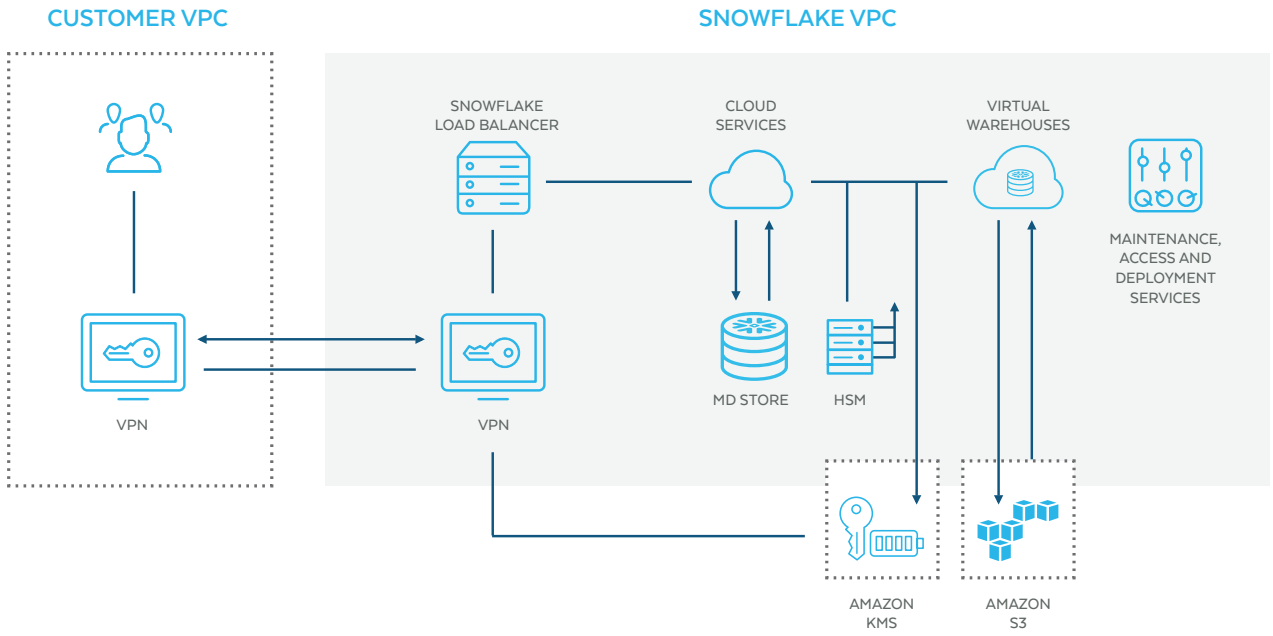
Each VPS customer has their own dedicated virtual servers, load balancer and metadata store.

STANDARD	PREMIER	ENTERPRISE	ENTERPRISE FOR SENSITIVE DATA	VIRTUAL PRIVATE SNOWFLAKE (VPS)
• Complete SQL data warehouse • Business hour support M-F • 1 day of time travel • Always-on enterprise grade encryption in transit and at rest • Customer dedicated virtual warehouses	Standard + • Premier support 24 x 365 • Faster support response time • SLA with refund for outage	Premier + • Multi-cluster warehouse • Up to 90 days of time travel • Federated authentication • Annual rekey of all encrypted data • Audit log (H2 2017) • Cross region replication (H2 2017)	Enterprise + • HIPAA Support • PCI Compliance • Data encryption everywhere • Enhanced security policy • Customer managed encryption keys	Enterprise for Sensitive Data + • Customer dedicated virtual servers wherever the encryption key is in-memory • Customer dedicated metadata store • VPN or VPC bridge to customer VPC or on-premises data center • Business critical support
	Business Critical Support (BCS)	• Named Technical Account Manager • Integration with customer operations • Query validation before upgrades • Access to Snowflake service data		

There are also dedicated VPNs or VPC bridges from a customer's own VPC to the Snowflake VPC. These dedicated services ensure the most sensitive components of the customer's data warehouse are completely separate from those of other customers. However, the VPS is designed to preserve Snowflake's unique ease of use and low burden of management.

Even with VPS, Snowflake's hardware security module, along with maintenance, access and deployment services, are still shared services. These components are secure by design, even in a multi-tenant model. For instance, the hierarchical security module (HSM) is configured with a completely separate partition dedicated to the customer. All data is stored in S3 within a separately provisioned AWS account.

This design makes it possible for even the most security conscious customers to trust VPS as a comprehensively secure solution for their data.



CONCLUSION

Across all editions, Snowflake provides a secure and protected environment for customer data, protecting data in-transit and at rest from current and evolving threats. The features built into Snowflake deliver enterprise-class security by default, without the additional burdens of complexity and management that traditional solutions force customers to endure. Snowflake is an SQL data warehouse designed from the ground up for the cloud and for modern data analytics. Built with a unique new architecture, and provided as an enterprise-class software-as-a-service (SaaS) offering, Snowflake delivers cloud elasticity, native support for diverse data and differentiated price performance.

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, the elasticity of the cloud and live data sharing at a fraction of the cost of traditional solutions. Snowflake: Your data, no limits. Find out more at snowflake.net.