snowflake

Snowflake for sensitive data

THE MOST SECURE CLOUD DATA WAREHOUSE

CHAMPION GUIDES

What's inside

snowflake

Meeting the needs of today's enterprise

More data, more insight and far better security

Organizations that collect, analyze and share sensitive data have been cloud hesitant. This has been a barrier to them capitalizing on the many compelling benefits of true data-driven analytics. Across 13 industries, only 19 percent of companies had a cloud-only approach in 2016. But financial services, manufacturing and retail remain below the average. Insurance had the lowest cloud-only approach with just nine percent.[1]

Organizations that deal with sensitive data are paradoxically finding themselves under pressure to make that data more accessible to authorized stakeholders and to find more practical and seamless ways to share it securely with users inside and outside the organization. The cloud addresses all of these issues but only if the particular cloud solution is the right one.

For securing data, there has long been a bias toward on-premises solutions, based on the assumption that an organization's data center is more secure than the cloud. However, the biggest data breaches in recent history involved on-premises data centers. Cloud storage options have proven to be considerably more secure since they first emerged, and they continue to evolve.

In addition, legacy data warehouse solutions, whether they're located on-premises or in the cloud, struggle to meet the needs of today's organizations to store, analyze and share more data with others than ever before. Companies also want a powerful solution that's simple to use with minimal overhead.

A solution that meets all of these needs exists: Snowflake's built-for-the-cloud data warehouse. The most secure cloud data warehouse available.

[1] Source: "Building Trust in a Cloudy Sky: The state of cloud adoption and security," McAfee, January 2017.

What organizations with sensitive data truly need

What should a secure cloud data warehouse comprise? Five essentials, plus the inherent qualities of a truly modern data warehouse:

1. END-TO-END ENCRYPTION

Data must be stored and transmitted in encrypted form. At no point, when data is at rest or in-transit, should the data exist in an unencrypted format.

2. GOVERNANCE

The organization must have complete control over the data at all times. No one outside the organization should be able to grant access to others. People within the organization should be able to access the data only after being given proper authority, and access must be easy to revoke whenever circumstances demand.

3. RESILIENCY

The data must be impossible to physically lose, whether it be from a cyber attack, power outage, hard drive crash, natural disaster or accidental deletion.

4. NO MANAGEMENT

Security has to be baked into the core product, without the need for customer configuration or ongoing management.

5. ISOLATION

An individual organization's data warehouse must be able to be partitioned in its own secure cloud environment, a requirement of particular importance to satisfy strict corporate standards and comply with stringent privacy and security regulations.

6. POWER AND FLEXIBILITY

A cloud data warehouse must also provide the power, simplicity and limitless concurrency needed to analyze all your data types, from all your data sources, amalgamating all data silos into a single location for a single source of truth.

The principles of securing data in today's environment

How traditional data warehouses fall short

The trouble with legacy technology

Legacy technology, primarily used in on-premises solutions, does not address many of the critical elements outlined above. Redundancy can be a major challenge. While RAID and drive mirroring are commonplace, avoiding data loss due to larger-scale problems can be problematic. Natural disasters pose a special risk for an in-house storage solution unless the organization has multiple mirrored locations in different parts of the world—a costly and uncommon infrastructure.

Encryption, key management, key rotation and many other critical security features are typically available as options or provided as a set of building blocks that the customer has to assemble and manage, which can delay your time to market. In addition, internal IT teams spend their valuable time on these monumental tasks instead of focusing on high value projects to help streamline operations and better serve customers through data-driven analytics.

On-premises solutions become even more of a challenge when scaling for more data and more users. Organizations must plan ahead and buy hardware, software and a host of other products and services for their projected highest usage period, which may only be a day, week or month each year. They must also employ large teams of highly technical, dedicated staff who can be difficult to find.

CHALLENGES WITH TRADITIONAL CLOUD-HOSTED DATA WAREHOUSING

Cloud services offer solutions to many of the problems inherent in on-premises solutions. But these services are merely on-premises solutions migrated to the cloud. Therefore, they present the same security issues. Primarily, the level of security can vary widely from provider to provider. Secure data may not be isolated from non-secure data (or other users), encryption is widely variable (and often not end-to-end) and access controls can be weak. Many cloud data warehouses provide a simple password as a means of security, which is insufficient for a truly sensitive-data environment.

Similarly, these systems can be difficult to manage. The user may be tasked with maintaining the server and applying updates and other patches, and scaling can be difficult if the provider has a hard cap on storage space or the number of users. You may also have to push your own legacy security tools (such as encryption systems) to the cloud if you want an extra layer of protection, only to find out they don't work the same way online as they do offline.

Snowflake: The data warehouse built for the cloud

All the security to protect your data

There's a solution to all these challenges: Snowflake, a truly secure data warehouse with all the flexibility and power of the cloud.

SECURITY FROM THE START

Snowflake has been architected with security baked into the product. You don't have to install extra software to make Snowflake secure. Enterprise-grade security is always on for every user. To ensure security, penetration testing is performed continuously to detect any way an unauthorized user might gain entry. Other cloud companies may perform penetration testing only once a year.

VALIDATED SECURITY

Snowflake is certified by third-party auditors to ensure the highest level of compliance with various regulations, including Health Insurance Portability and Accountability Act (HIPAA) regulations, and is certified as compliant with the Payment Card Industry Data Security Standard (PCI DSS) Level 1 Service Provider, a key standard for organizations that handle credit card information. Snowflake's staff are highly trained on all of these security protocols—as are Snowflake's subcontractors and other vendors.

ENCRYPTION EVERYWHERE

Encryption is the centerpiece of Snowflake's security infrastructure, and the system is built so each user has total control over data at all times. Data is encrypted when it's at rest on Snowflake's servers and when it is in-transit to and from the user. At no point can anyone access or understand the data without the appropriate encryption key.

TRI-SECRET SECURE

This new feature ensures customer control and protection of data by combining a customer-provided encryption key with a Snowflake-provided encryption key and user credentials.

- **Customer encryption key.** Owned by the customer, this "kill-switch" can disable an attempted data decryption attack by instantly rendering data unreadable.
- **Snowflake encryption key.** This key is securely maintained by Snowflake and combined with the customer key to create a master key to decrypt data. Without both keys, data will remain encrypted and unreadable.
- **User credentials.** Each Snowflake account is protected by a unique user name and password, so each user accessing the system is authenticated before even reaching the encrypted data store.

RESILIENCY AND DATA RECOVERY

Data stored in Snowflake is also safe from accidental deletion, hardware failure, natural disaster or any other unforeseen occurrence. All data is stored on the Amazon Web Services (AWS) S3 platform, where multiple redundant systems ensure customer information is safe at all times. S3 automatically replicates data across multiple locations, protecting data in the event of a data loss at any one location.

TIME TRAVEL

This feature of Snowflake provides additional data security by keeping copies of historical data at various points in time. So, if a file is mistakenly changed or deleted, it can be recovered after the fact. A retention period of 1-90 days is available for Snowflake customers.

VIRTUAL PRIVATE SNOWFLAKE (VPS)

For organizations that need a dedicated stack of Snowflake in the cloud, the VPS version of Snowflake is maintained as a dedicated service, in its own AWS Virtual Private Cloud (VPC).

Beyond security

The utmost in flexibility and ease of use

Solid security is only part of the equation. Snowflake is powerful and easy to use, offering customers maximum flexibility and usability.

ZERO MAINTENANCE

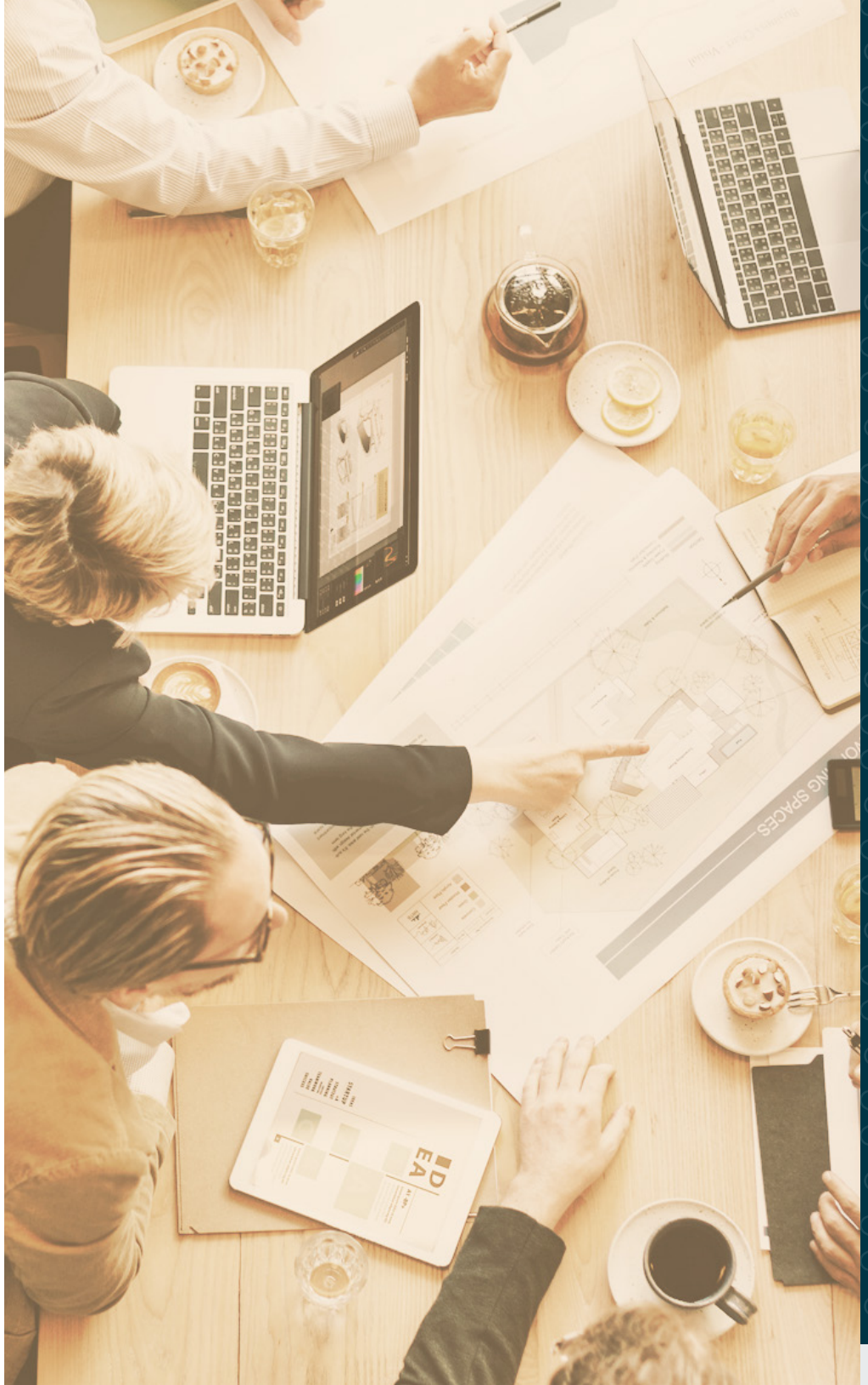
Snowflake's built-in security reduces complexity, so there's no labor-intensive process to install, configure and manage security measures that may not meet today's standards for thwarting cyber attacks.

ALL YOUR USERS

As your organization grows, and as your data analytics needs expand and contract, Snowflake can instantly scale up and down to match capacity with demand. Snowflake's multi-cluster architecture also supports limitless numbers of concurrent users.

ALL YOUR DATA

Snowflake customers can analyze multiple petabytes of structured and semi-structured data (JSON, XML, AVRO) to quickly extract critical insight. Snowflake natively ingests semi-structured data, stores it efficiently and then accesses it quickly using simple extensions to standard SQL.



Snowflake at work: CapSpecialty

"Snowflake allows us to focus on finding answers and addressing the business problem, versus spending time worrying about infrastructure,"

CapSpecialty is a leading provider of specialty insurance for small to mid-sized businesses in the US, and is a provider of commercial property insurance and casualty, professional liability, surety and fidelity products.

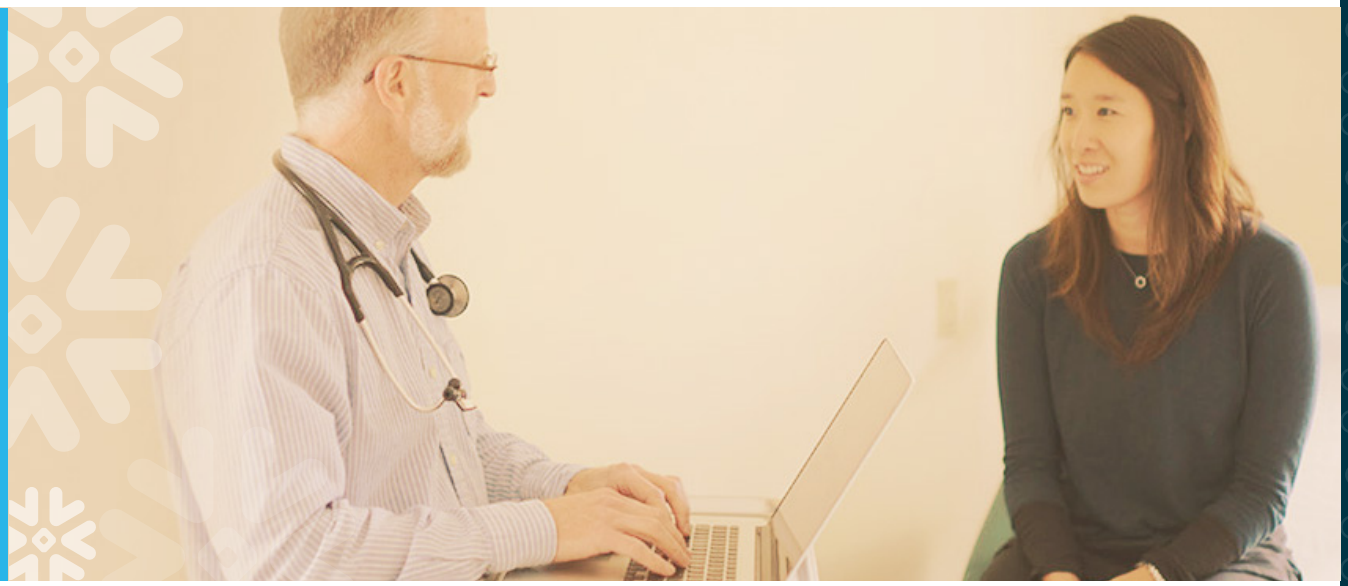
CapSpecialty deals in large volumes of sensitive information and requires end-to-end encryption and compliance with HIPAA. "We did a lot of digging with our IT security guys and the Snowflake team to make sure our data was going to be safe," CapSpecialty data team manager, Ken Wood says. This included scrutinizing encryption at rest and in-transit, as well as extensively testing the HIPAA security configuration before CapSpecialty was assured Snowflake was truly secure. Today, the company runs its reports in a matter of minutes, confident that the data being analyzed is completely safe.

CapSpecialty also made the move to Snowflake because it could no longer afford to lose an entire day running a single report. With Snowflake, the results were immediate—a performance boost that made its analytics run 20 to 200 times faster. "We were blown away by that," Wood says. "The speed gives us huge scalability advantages."

CapSpecialty has also realized performance benefits because the system is entirely in the cloud. "Snowflake allows us to focus on finding answers and addressing the business problem, versus spending time worrying about infrastructure," Wood says.

Snowflake at work: athenahealth

After migrating to Snowflake, the company saw a 50 percent improvement in the time it took to run reports, with a reduction of time spent on overhead and maintenance, as well.



athenahealth is a cloud-based provider of software and services to doctors and hospitals. The company's service captures everything from doctor's notes to receipts for purchases, and it's all tracked in databases that collectively store petabytes of data.

Over time, the company found that its legacy platform could no longer scale to handle the massive amounts of data. After investigating the options, athenahealth made the move to Snowflake.

Security was a key consideration for athenahealth. Since all of its data is health care data, athenahealth needed a data warehouse that was HIPAA-compliant, fault tolerant and provided end-to-end encryption.

After migrating to Snowflake, the company also saw a 50 percent improvement in the time it took to run reports, with a reduction of time spent on overhead and maintenance, as well.

Snowflake: The truly secure data warehouse

A business that requires a secure data warehouse no longer needs to develop an in-house solution. Snowflake's data warehouse security is best-in-class, with security built into its foundation. With enterprise-grade encryption, multi-factor authentication, automatic key management and robust intrusion detection baked in, Snowflake offers an incredible suite of security features and removes the concern over data security and the burden of maintaining a secure data warehouse in an environment of constantly evolving threats.

With Snowflake, your business can free up all those resources previously devoted to security management, letting you focus on doing the work that really matters: solving business problems.

About Snowflake Computing

Snowflake is the only data warehouse built for the cloud. Snowflake delivers the performance, concurrency and simplicity needed to store and analyze all data available to an organization in one location. 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 www.snowflake.net