COMFORTE DATENSCHUTZ FÜR SNOWFLAKE

ÜBERNEHMEN SIE DIE VOLLE KONTROLLE ÜBER IHRE DATEN

DIE LÖSUNG IM ÜBERBLICK

- Permanenter Schutz sensibler* Daten (Data at Rest, Data in Motion & Data in Use) innerhalb und außerhalb von Snowflake
- Formaterhaltende Verschlüsselung (FPE) auf operativer Ebene sowie Tokenisierung
- Granulare Zugriffskontrolle
- Analysen geschützter Datensätze ohne Leistungsverluste
- Behalten Sie Ihre eigenen Schlüssel für die volle Kontrolle Ihrer eigenen Daten
- Nachhaltiger Datenschutz unter Einhaltung gesetzlicher Vorschriften

EINLEITUNG

Organisationen auf der ganzen Welt nutzen die Snowflake Data Cloud, um neuen Mehrwert für ihr Unternehmen zu erschließen.

Die Verlagerung von lokal gespeicherten Daten und Anwendungen in die Cloud, stellt jedoch aufgrund von Sicherheitsbedenken und der Einhaltung von gesetzlichen Vorschriften oft eine Herausforderung dar.

Comforte's Data Protection für Snowflake bietet die Möglichkeit sensible Daten richtig zu schützen, um gesetzliche Auflagen zu erfüllen und gleichzeitig die Nutzbarkeit für Geschäftsprozesse, Anwendungen und Analysen zu gewährleisten.

WIE SNOWFLAKE DATEN SCHÜTZT

Snowflake arbeitet mit dynamischer Datenmaskierung, um sensible Daten vor unbefugten Nutzern zu verbergen. Es handelt sich dabei um eine Funktion auf Spaltenebene, die spezifische Maskierungsrichtlinien verwendet. Dabei werden Klartext Daten in Tabellen und Ansichtsspalten zur Abfragezeit, an jeder Stelle an der die Spalte erscheint, selektiv maskiert. Abhängig von der Maskierungsrichtlinie für die jeweilige Rolle können Nutzer den Klartext Wert (“John Smith”), einen teilweise maskierten Wert (“Jxxx Sxxxx”) oder den vollständig maskierten Wert (“xxxx xxxxx”) sehen. Die Daten müssen jedoch im Vorfeld als Klartext auf Snowflake hochgeladen werden. Zusätzlich muss eine Datenbank und ein Schema vorhanden sein, bevor eine Maskierungsrichtlinie auf Spalten angewendet werden kann. Das bedeutet, dass nach wie vor ein hohes Risiko für Fehlkonfigurationen und Offenlegungen von Daten existiert, da die Daten auf Datenbankebene und bei der Verwendung in externen Anwendungen ungeschützt bleiben.

MULTICLOUD-DATENSCHUTZ AUF IHRE BEDÜRFNISSE ZUGESCHNITTEN - END-TO-END

Comforte bietet einen robusten Datenschutz, der die integrierten Funktionen von Cloud-basierten Datenspeichern übertrifft. Durch Hybrid- und Multicloud datenbasierte Ökosysteme sind Unternehmen dazu in der Lage strukturierte und semi-strukturierte Daten innerhalb und außerhalb von Snowflake zu schützen. Dies hilft Kunden bei der Bereitstellung eines Self-Service Zugangs, der die Verarbeitung und Analyse von Daten ermöglicht, die zuvor auf Grund von Datenschutz- oder Sicherheitsbedenken nicht realisierbar waren. Cloud-native Architektur und Integrationsfunktionen helfen den Kunden eine datenzentrierte Sicherheit schnell zu implementieren, Daten so früh wie möglich im gesamten Lebenszyklus zu schützen und Sicherheitsrichtlinien konsequent anzuwenden.

Comforte bietet mehrere Datenschutzmethoden an, um spezifische Anforderungen und Anwendungsfälle abzudecken. Techniken wie Datenmaskierung, formaterhaltendes Hashing, Tokenisierung sowie formaterhaltende Verschlüsselung (FPE) ermöglichen die Pseudonymisierung oder vollständige Anonymisierung von Daten.

Während bei der Anonymisierung die Sensibilität der Daten vollständig entfernt und unbrauchbar wird (z. B. für fortgeschrittene Analysen), schützen Pseudonymisierungsmethoden - wie FPE - die Daten so, dass sie weiterhin in Analyse- oder BI-Tools verwendet werden können; dabei bleiben das Format der Daten, die referenzielle Integrität und weitere Aspekte erhalten.

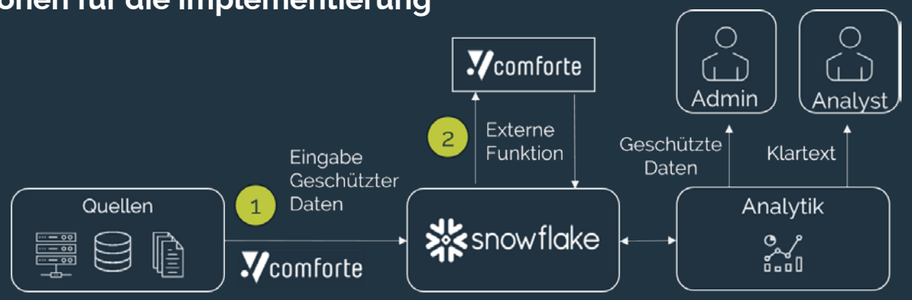
*(PII, PCI oder PHI)

WIE DIE LÖSUNG FUNKTIONIERT

Comforte's Datenschutz für Snowflake pseudonymisiert sensible Daten (PII, PHI, PCI) mittels Tokenisierung oder formaterhaltende Verschlüsselung (FPE) auf Feldebene. Anstatt die Werte nur zu maskieren, wird das Datenelement in der Datenbank vollständig durch ein Token ersetzt. Der Token selbst kann auf das ursprüngliche Datenelement zurückgeführt werden, gibt aber keine sensiblen Informationen preis. Der größte Vorteil der Tokenisierung gegenüber der klassischen Verschlüsselung ist ihre formaterhaltende Eigenschaft. Token behalten das Format und die Länge der ursprünglichen Datenelemente bei, wodurch sie für Geschäftsanwendungen und Analysen nutzbar bleiben. So können sie von jedem Abfrage- oder BI-Tool verwendet werden, ohne dass die SQL-Syntax geändert werden muss. Außerdem erfordert die Verarbeitung von Token keine großen Rechenressourcen, was eine hohe Leistung und geringe Latenzzeiten ermöglicht. Da der Datenspeicher und die Schutz-Engine strikt voneinander getrennt sind, trägt diese Methode zur Einhaltung von Datenschutzbestimmungen bei und reduziert die Risiken im Zusammenhang mit Datenschutzverletzungen immens, da tokenisierte Daten keinen Wert für potenziellen Missbrauch haben.

Die fortschrittlichen Schutztechnologien von comforte sind in der Lage, sich an jedem Punkt der Datenumgebung zu integrieren, von den Quellen bis zu den Analysetools. Dies ermöglicht die Umwandlung von Daten auf der Grundlage feingranularer Richtlinien, so dass auf einfache Weise definiert werden kann, welche Benutzerrollen welche Datenelemente in welcher Form sehen können und beispielsweise nur Datenanalysten vollständigen Zufriff auf die Daten in Klartext haben.

Optionen für die Implementierung



1. Schutz der Daten, bevor sie Snowflake erreichen. Diese Option wird empfohlen, wenn keine sensiblen Daten auf Snowflake gespeichert werden sollen. Die Daten werden entweder in der Cloud-Aufnahme-Phase geschützt - bevor sie mit Speichern wie Amazon S3 in Berührung kommen - oder in der Abfangphase, wenn die Daten in Snowflake selbst geladen werden. Dies geschieht durch die Nutzung der Fähigkeit von comforte, Daten transparent abzufangen und Tokenization on the fly anzuwenden, indem es als Proxy zwischen der Datenquelle und der Datenbank arbeitet (siehe Abbildung oben).

2. Externe Tokenisierungsfunktion von Snowflake, die eine Rest-API nutzt. Diese Option wird empfohlen, wenn Sie nach einer Lösung suchen, mit der Sie Ihre sensiblen Daten besser schützen und den Zugriff über die rollenbasierten dynamischen Datenmaskierungsrichtlinien von Snowflake steuern können. Dadurch können bestimmte Rollen, wie z. B. Datenanalysten, Daten im Klartext abrufen, während andere nur geschützte Daten sehen.

VORTEILE

- Beschleunigen Sie datenbasierte Geschäftsinitiativen
  - Migration in die Cloud unter Wahrung der Datensicherheit
- Durchführung von Analysen auf geschützten Datensätzen
  - Sichere Nutzung der Daten für Analysen ermöglichen
- Schutz der personenbezogenen Daten und Einhaltung gesetzlichen Vorschriften
  - Pseudonymisierte Daten sind vollständig mit den Datenschutzbestimmungen konform
- Vereinfachung der Datensicherheit und Verwaltung
  - Durchgängiger Schutz von Daten über verschiedene Tools, komplexe Architekturen, Umgebungen und sogar separate Cloud-Anbieter hinweg

Beispielarchitektur