COMFORTE DATA PROTECTION FOR SNOWFLAKE

TOME EL CONTROL COMPLETO DE SUS DATOS

SOLUCIÓN A SIMPLE VISTA

- Protección consistente de datos confidenciales (PII, PCI o PHI) en reposo, en movimiento y en uso, dentro y fuera de Snowflake
- Formato de nivel de campo que preserva el cifrado (FPE) y la tokenización
- Control de acceso granular
- Análisis de conjuntos de datos protegidos sin problemas de rendimiento
- Mantenga su propia llave para mantener el control total de sus datos
- Privacidad sostenible y cumplimiento normativo

INTRODUCCIÓN

Organizaciones de todo el mundo utilizan Snowflake Cloud Data Platform para generarle valor a sus negocios. Sin embargo, mover los datos de las tiendas en sitio y aplicaciones locales a la nube suele ser un desafío debido a problemas de seguridad y cumplimiento normativo. Comforte Data Protection para Snowflake brinda la capacidad de proteger adecuadamente los datos confidenciales para cumplir con las obligaciones reglamentarias y mantenerlos utilizables para procesos comerciales, aplicaciones y análisis.

CÓMO SNOWFLAKE PROTEGE LOS DATOS

Snowflake proporciona enmascaramiento dinámico de datos para mantener los datos confidenciales ocultos a usuarios no autorizados. Es una función a nivel de columna que utiliza políticas de enmascaramiento para enmascarar de forma selectiva los datos de texto sin formato en la tabla y ver las columnas en el momento de la consulta, en cada ubicación donde aparece la columna. Por lo tanto, dependiendo de la política de enmascaramiento para su función particular, los usuarios pueden ver el valor de texto sin formato (“John Smith”), el valor parcialmente enmascarado (“Jxxx Sxxxx”) o el valor completamente enmascarado (“xxxx xxxxx”). Sin embargo, los datos deben de cargarse en Snowflake en texto claro, y debe existir una base de datos y un esquema antes de que se pueda aplicar una política de enmascaramiento a una columna. Esto significa que todavía existe un alto riesgo de mala configuración y exposición de los datos, ya que los datos aún permanecen desprotegidos a nivel de la base de datos y cuando se utilizan en aplicaciones externas.

PROTECCIÓN DE DATOS MULTINUBE ADAPTADA A SUS NECESIDADES DE EXTREMO-A-EXTREMO

Comforte brinda una sólida protección de datos que supera las capacidades integradas de los almacenes de datos basados en la nube. Permite a las organizaciones proteger datos estructurados y semiestructurados no solo dentro sino también, fuera de Snowflake y mantenerlos protegidos mientras fluyen en ecosistemas de datos híbridos y de múltiples nubes. Esto le ayuda a los clientes a proporcionar acceso de autoservicio a los datos, lo que permite el procesamiento y el análisis que antes eran imposibles debido a problemas de privacidad o seguridad. La arquitectura nativa de la nube y las capacidades de integración, ayudan a los clientes a implementar rápidamente la seguridad centrada en los datos (data-centric security), proteger los datos lo antes posible y aplicar políticas de seguridad de manera consistente para mantener los datos seguros durante todo su ciclo de vida.

Comforte proporciona múltiples métodos de protección de datos para abordar necesidades y casos de uso específicos. Las técnicas como el enmascaramiento de datos, el hash con preservación de formato o la tokenización y el cifrado con preservación de formato (FPE), permiten la seudonimización o la anonimización completa de los datos. Si bien la anonimización elimina por completo la sensibilidad de los datos y los hace inutilizables (por ejemplo, para análisis avanzados), los métodos de seudonimización, como el FPE (cifrado con preservación de formato), protegen los datos de una manera que aún se pueden utilizar en herramientas de análisis o BI; preservando el formato de los datos, la integridad referencial y más.

CÓMO FUNCIONA LA SOLUCION

Comforte Data Protection para Snowflake seudonimiza los datos confidenciales (PII, PHI, PCI) mediante tokenización o el cifrado con preservación de formato (FPE) a nivel de campo. En lugar de simplemente enmascarar los valores, el elemento de datos se reemplaza completamente por un token en la base de datos. El token en sí mismo puede volver a mapear al elemento de datos original, pero no expone ninguna información sensible. La mayor ventaja que tiene la tokenización sobre el cifrado clásico es su propiedad de preservación del formato. Los tokens preservan el formato y la longitud de los elementos de datos originales, lo que los mantiene utilizables para aplicaciones comerciales y análisis. Esto permite el uso de cualquier consulta o herramienta de BI sin necesidad de cambiar la sintaxis SQL. Además, los tokens no requieren muchos recursos computacionales para procesarse, lo que permite un alto rendimiento y una baja latencia. Dado que el almacén de datos y el motor de protección están estrictamente separados, este método ayuda a lograr el cumplimiento de las normas de privacidad y protección de datos y reduce enormemente los riesgos relacionados con las filtraciones de datos, ya que los datos tokenizados no tienen valor para un posible uso indebido.

Las tecnologías de protección avanzada de Comforte tienen la capacidad de integrarse en cualquier punto del entorno de datos, desde las fuentes hasta las herramientas de análisis. Esto permite la transformación de datos basada en políticas granulares finas, lo que hace posible definir fácilmente qué roles de usuario pueden ver qué elemento de datos, en qué forma y, por ejemplo, proporcionar acceso a los datos en claro solo a los analistas de datos.

Opciones de implementación

1. Protegiendo los datos antes de que lleguen a Snowflake. Esta opción se recomienda si no se deben almacenar datos confidenciales en Snowflake. Los datos estarán protegidos ya sea en la etapa de ingesta en la nube - antes de que toque almacenes como Amazon S3 - o en la etapa de intercepción cuando los datos se cargan a Snowflake. Esto se logra aprovechando la capacidad que tiene comforte para interceptar datos de manera transparente y aplicar tokenización sobre la marcha, trabajando como un proxy entre la fuente de datos y la base de datos (consulte el diagrama anterior).

2. Función de tokenización externa de Snowflake que aprovecha una API REST. Esta opción es recomendada si está buscando una solución para agregar protección avanzada a sus datos confidenciales y controlar el acceso a través de las políticas de enmascaramiento de datos dinámicas basadas en las funciones de Snowflake.

BENEFICIOS

- Acelere las iniciativas empresariales basadas en datos
  - Muévase a la nube mientras mantiene los datos seguros
- Ejecute análisis en conjuntos de datos protegidos
  - Habilite el uso seguro de datos para análisis
- Proteja la privacidad y logre el cumplimiento
  - Los datos seudonimizados cumplen totalmente con las normas de privacidad
- Simplifique la seguridad y la gestión de datos
  - Protección consistente de datos a través de diferentes herramientas, arquitecturas complejas, entornos e incluso proveedores de nube distintos

Ejemplo de la arquitectura