COMFORTE DATA PROTECTION PARA GOOGLE CLOUD Y BIGQUERY

TRAIGA SU PROPIO CIFRADO A GOOGLE CLOUD

LA SOLUCIÓN EN UN VISTAZO

- Protección Traiga su propio cifrado (BYOE) (del inglés Bring Your Own Encryption) para Google Cloud, entornos híbridos y configuraciones multinube.
- Seguridad coherente centrada en los datos para entornos complejos.
- Controles de acceso de datos granulares.
- Desidentificación de datos para los análisis en la nube por medio de la tokenización avanzada o la encriptación de preservación del formato (FPE).
- Integración nativa de la nube para una implementación rápida.
- Integrada perfectamente a Google BigQuery.

INTRODUCCIÓN

Trabajar en la nube acarrea una serie de riesgos de seguridad y privacidad. Para abordar dichos problemas, la Data Protection para Google Cloud de comforte proporciona una amplia solución que se integra perfectamente a BigQuery, lo que asegura así una sólida protección de los datos confidenciales. Este enfoque no solo permite a las organizaciones cumplir con sus obligaciones normativas, sino también que los datos sean sigan siendo accesibles para los procesos, aplicaciones y analíticas empresariales esenciales.

PARA QUÉ UNA PROTECCIÓN DE DATOS ADICIONAL

Para algunas organizaciones, las funciones de seguridad que trae Google de fábrica serán suficientes, ya que el cifrado nativo en BigQuery proporciona medidas fuertes de seguridad para los datos almacenados y los datos en tránsito.

Google Cloud Platform (GCP) cifra por defecto el contenido del cliente almacenado en reposo, sin que el usuario tenga que hacer nada. Esto es posible si los datos están únicamente en la GCP. Por ejemplo, para trasladar los datos fuera del entorno de Google a otro proveedor de servicio en la nube o herramientas de análisis de datos, será necesario volver a identificar los datos antes de aplicar un método nuevo de protección.

Para organizaciones que trabajan en industrias estrictamente reguladas, los organismos reguladores suelen exigir medidas de seguridad adicionales. En este caso, se pedirá una capa de seguridad centrada en los datos adicional.

COMFORTE DATA PROTECTION PARA GOOGLE BIG QUERY: CÓMO FUNCIONA

Comforte Data Protection para Google Cloud y BigQuery seudonimiza los datos confidenciales (PII, PHI, PCI) por medio de la tokenización o FPE sobre el terreno; los datos se remplazan completamente por un token en la base de datos. El mismo token guarda la compatibilidad y la usabilidad para las herramientas de análisis, pero no filtra información confidencial. Esto permite usar BigQuery o cualquier otra herramienta BI sin necesidad de cambiar la sintaxis SQL.

Además, los tokens no necesitan de muchos recursos computacionales para que puedan procesar, lo que permite un rendimiento elevado y tiempos de espera bajos. Aunque, si por fines empresariales los token tienen que volver al valor original, será posible gracias a que el almacenamiento de datos y el motor de protección están bien separados, lo que permite cumplir con las normativas de privacidad y protección de datos y, además, reduce significativamente el riesgo de filtración de datos, ya que los datos tokenizados no tienen valor para un posible uso indebido.

SU PROPIA PROTECCIÓN DE DATOS PARA GOOGLE CLOUD

La idea del BYOE es que el usuario de una nube pública tenga libertad para utilizar la tecnología de cifrado y protección que prefiera, independientemente de lo que ofrezca el proveedor público de la nube. Esto permite al usuario tener un control sobre la generación de toda la protección de secretos como claves de cifrado o tokenización de secretos. Como consecuencia, en la nube pública solo se guardan los datos protegidos.

Comforte va más allá de las funciones de fábrica de los almacenamientos en la nube al ofrecer protección de datos coherente e integral para entornos híbridos y de multinube. Proporciona la capacidad centrada en datos para asegurar los datos antes de almacenarlos en la nube y garantiza una protección continua en todos los movimientos y procesos de las aplicaciones y los usuarios.

Las técnicas de desidentificación incluyen enmascaramiento de datos, función hash de preservación del formato, tokenización y encriptación de preservación del formato (FPE). Todo esto permite el proceso de seudonimización o anonimización completa de los datos. La anonimización elimina la información confidencial, lo que hace que los datos no se presten a análisis avanzados. Por el contrario, los métodos de seudonimización como la tokenización o la FPE conservan la usabilidad de los datos con fines analíticos y para garantizar la integridad de los datos.

Este enfoque centrado en los datos simplifica la gestión de la seguridad en ambientes complejos, permitiendo así el acceso seguro al autoservicio, la movilidad entre servicios de nube o el uso de herramientas de análisis sin comprometer la privacidad y la seguridad.

VENTAJAS

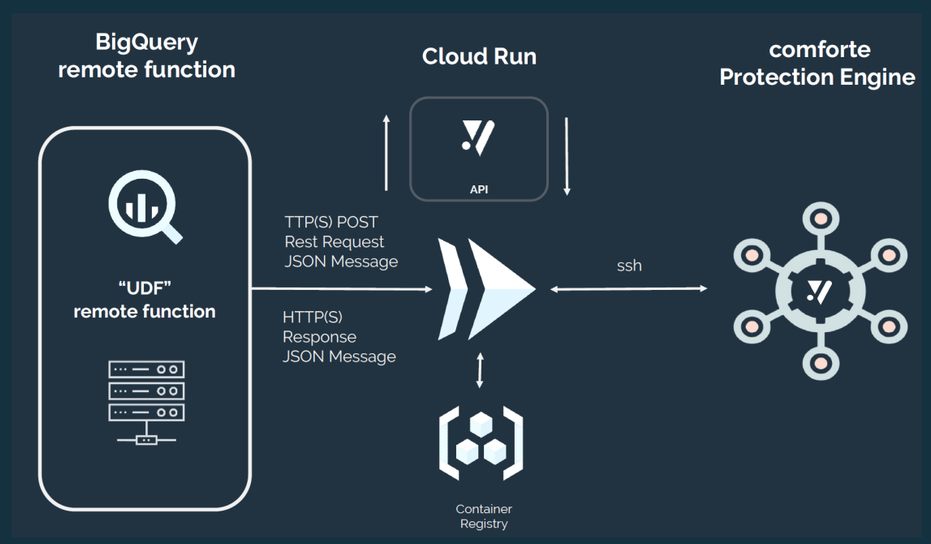
- **Mayor seguridad para los análisis basados en la nube** - Preservar la privacidad y proteger los datos
- **Lleve su propio cifrado (BYOE) a la nube** - Mantenga el control y aumente la flexibilidad para las configuraciones en varias nubes
- **Integración nativa de la nube** - Implementación rápida para la protección de datos desde el primer momento
- **Ejecuta análisis en datos protegidos** - Permite el uso seguro de datos confidenciales
- **Protege la privacidad y cumple con las normativas** - Los datos seudonimizados cumplen completamente con las normativas de privacidad

OPCIONES DE IMPLEMENTACIÓN

1. **Protección de datos preventiva antes de que lleguen a BigQuery:** comforte proporciona integradores transparentes y varias API que permiten las medidas de protección de datos desde el inicio del ciclo de la vida de los datos. Esto significa que los datos confidenciales están protegidos en diferentes fases durante la ingesta de datos a BigQuery. Proteger los datos confidenciales antes de la ingesta a la nube, incluso antes de que llegue al almacenamiento de Google, asegura que ninguna información confidencial se almacene en la nube, lo que mitiga posibles riesgos relacionados con el almacenamiento en la nube.

2. **Función a distancia desde BigQuery:** utilice Cloud Functions y Cloud Run aprovechando las API para proteger los datos confidenciales que están ya en BigQuery. Los controles de acceso basados en rol permiten el acceso a la gestión granular de los datos. Los análisis de datos, por ejemplo, pueden recuperar los datos en su forma original, mientras que otros usuarios solo pueden visualizar los datos protegidos.

   [véase el diagrama de abajo]



Escríbanos y hablemos