COMFORTE DATENSCHUTZ FÜR DIE GOOGLE CLOUD UND BIG QUERY

BRINGEN SIE IHRE EIGENE VERSCHLÜSSELUNG IN DIE GOOGLE CLOUD

DIE LÖSUNG AUF EINEN BLICK

- Bring Your Own Encryption (BYOE) Schutz für die Google Cloud, hybride Umgebungen und Multi-Cloud-Setups
- Konsistente, datenzentrierte Sicherheit für komplexe Umgebungen
- Granulare Datenzugriffskontrollen
- De-Identifizierung von Daten für Cloud-basierte Analysen durch Tokenisierung oder format-preserving encryption (FPE)
- Cloud-native Integration für schnelle Implementierung
- Nahtlose Integration mit Google BigQuery

EINLEITUNG

Die Nutzung der Cloud birgt erhebliche Risiken in Bezug auf Sicherheit und Datenschutz. Um diese Bedenken auszuräumen, bietet comforte mit datenschutz für die google cloud eine umfassende Lösung, die sich nahtlos in BigQuery integriert und einen starken Schutz sensibler Daten gewährleistet. Dieser Ansatz ermöglicht es Unternehmen nicht nur, gesetzliche Auflagen zu erfüllen, sondern auch, dass die Daten für wichtige Geschäftsprozesse, Anwendungen und Analysen zugänglich bleiben.

WIE GOOGLE CLOUD DATEN SCHÜTZT

Für einige Unternehmen erfüllen die integrierten Sicherheitsfunktionen von Google ihre Anforderungen, da die native Verschlüsselung in BigQuery robuste Sicherheitsmaßnahmen für Daten im Ruhezustand und bei der Übertragung bietet.

Google Cloud Platform (GCP) verschlüsselt Kundeninhalte, die im Ruhezustand gespeichert sind, standardmäßig, ohne dass der Kunde etwas unternehmen muss. Dies ist möglich, wenn die Daten auf GCP und nicht anderswo gespeichert sind. Wenn Daten außerhalb der Google-Umgebung verschoben werden sollen, z. B. zu einem anderen Cloud-Service-Anbieter oder zu Datenanalysetools, kann es erforderlich sein, die Daten vor der Anwendung einer neuen Schutzmethode erneut zu identifizieren.

Für Unternehmen, die in stark regulierten Branchen tätig sind, werden oft zusätzliche Sicherheitsmaßnahmen von den Aufsichtsbehörden vorgeschrieben. Hier kann eine zusätzliche Ebene der datenzentrierten Sicherheit erforderlich sein.

COMFORTE-DATENSCHUTZ FÜR GOOGLE BIGQUERY: WIE ES FUNKTIONIERT

Comforte Data Protection für Google Cloud und BigQuery pseudonymisiert sensible Daten (PII, PHI, PCI) mittels Tokenisierung oder FPE auf Feldebene, wobei das Datenelement vollständig durch ein Token in der Datenbank ersetzt wird. Der Token selbst bewahrt die Kompatibilität und Nutzbarkeit für Analysetools, gibt aber keine sensiblen Informationen preis. Dies ermöglicht die Verwendung von BigQuery oder anderen BI-Tools, 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. Obwohl Token bei Bedarf für geschäftliche Zwecke wieder in ihren ursprünglichen Wert umgewandelt werden können, trägt diese Methode durch die strikte Trennung von Datenbank und Schutzmechanismus zur Einhaltung von Datenschutzbestimmungen bei und verringert die Risiken im Zusammenhang mit Datenschutzverletzungen immens, da tokenisierte Daten keinen Wert für potenziellen Datenmissbrauch haben.

BRINGEN SIE IHREN EIGENEN SCHUTZ

Beim BYOE-Konzept hat der Kunde einer öffentlichen Cloud die Freiheit, seine bevorzugten Verschlüsselungs- und Schutztechnologien zu verwenden, unabhängig von den spezifischen Angeboten des Anbieters der öffentlichen Cloud. Dadurch hat der Kunde die vollständige Kontrolle über die Generierung aller “protection secrets”, wie z. B. “encryption keys” oder “tokenization secrets”. Somit werden nur geschützte Daten in der öffentlichen Cloud gespeichert.

Comforte geht über die integrierten Funktionen von Cloud-basierten Datenbanken hinaus und bietet umfassenden End-to-End-Datenschutz für hybride und Multi-Cloud-Umgebungen. Es bietet die datenzentrierte Fähigkeit, Daten zu sichern, bevor sie in der Cloud gespeichert werden, und gewährleistet einen kontinuierlichen Schutz während ihrer Bewegung und Verarbeitung durch Anwendungen und Benutzer.

Zu den De-Identifizierungsverfahren gehören “data masking“, format-preserving hashing, Tokenisierung und format-preserving encryption (FPE). Sie ermöglichen den Prozess der Pseudonymisierung oder vollständigen Anonymisierung von Daten. Bei der Anonymisierung werden sensible Informationen eliminiert, wodurch die Daten für erweiterte Analysen ungeeignet sind. Pseudonymisierungsmethoden wie Tokenisierung oder FPE hingegen erhalten die Nutzbarkeit der Daten für Analysezwecke und gewährleisten die Datenintegrität.

Dieser datenzentrierte Ansatz kann das Sicherheitsmanagement in komplexen Umgebungen vereinfachen und ermöglicht einen sicheren Self-Service-Zugriff, die Bewegung zwischen Cloud-Diensten oder die Verwendung in Analyse-Tools, ohne den Datenschutz und die Sicherheit zu beeinträchtigen.

VORTEILE

- **Verbesserte Sicherheit für Cloud-basierte Analysen** - Wahrung der Privatsphäre und Schutz der Daten
- **Bring Your Own Encryption (BYOE) in die Cloud** - Erhöhte Flexibilität für Multi-Cloud-Setups
- **Cloud-native integration** - Schnelle Implementierung zum Schutz der Daten von Anfang an
- **Durchführung von Analysen mit geschützten Datensätzen** - Ermöglicht die sichere Nutzung sensibler Daten
- **Schutz der Privatsphäre und Erreichen von Compliance** - Pseudonymisierte Daten sind vollständig mit den Datenschutzbestimmungen konform

OPTIONEN FÜR DIE IMPLEMENTIERUNG

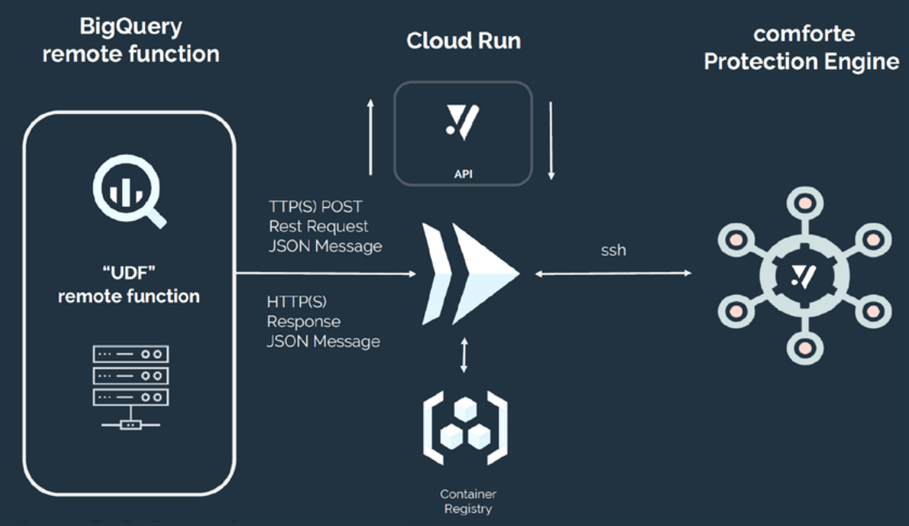
1

Präventiver Datenschutz, bevor die Daten BigQuery erreichen: comforte bietet eine Reihe von transparenten Integratoren und APIs, die Datenschutzmaßnahmen in den frühesten Stadien des Datenlebenszyklus ermöglichen. Dies bedeutet, dass sensible Daten in verschiedenen Stadien während ihrer Aufnahme in BigQuery geschützt werden können. Durch den Schutz sensibler Daten vor der Aufnahme in die Cloud, d. h. bevor sie überhaupt in den Google-Speicher gelangen, wird sichergestellt, dass keine sensiblen Informationen in der Cloud gespeichert werden, wodurch die mit der Cloud-Speicherung verbundenen potenziellen Risiken gemindert werden.

2

Remote-Funktion innerhalb von BigQuery: Verwenden Sie Cloud-Funktionen und Cloud-Run, indem Sie APIs nutzen, um sensible Daten zu schützen, die sich bereits in BigQuery befinden. Rollenbasierte Zugriffskontrollen ermöglichen eine granulare Verwaltung des Datenzugriffs. Datenanalysten können beispielsweise Daten im Original abrufen, während andere Benutzer nur geschützte Daten sehen dürfen.

[Sie können diese Methode unten sehen]



Kontaktieren Sie uns für weitere Informationen