comforte

CASO DE ESTUDIO

IMPORTANTE PROVEEDOR DE SEGUROS DE EE. UU. ELIGE COMFORTE PARA EL CUMPLIMIENTO DE NACHA

PERFIL DE LA EMPRESA

Este proveedor de seguros de salud del Fortune 500 se encuentra entre los grupos de seguros de propiedad/accidentes más grandes y de más rápido crecimiento en los Estados Unidos. Además de seguros de propiedad y accidentes, ofrecen seguros de vida, anualidades, inversiones para la jubilación, seguros de hogar, automóviles y compensación laboral, así como servicios de asesoramiento y servicios de inversión.

Tienen un entorno de datos complejo con una combinación de aplicaciones locales y en la nube y, están en proceso de transformación a DevOps nativos en la nube. Su aplicación principal de reclamos se ejecuta de manera local con millones de transacciones diarias mientras interactúa con docenas de aplicaciones. Debido a su estrategia de rápido crecimiento, las fusiones y adquisiciones han dado como resultado una arquitectura compleja con una multitud de bases de datos diferentes que están tratando de armonizar.

RETOS

Esta importante aseguradora tiene un entorno de datos complejo con herramientas heredadas y necesitaba una solución moderna de protección de datos, que les permitiera mantener protegidos los datos confidenciales mientras se transforman a un enfoque moderno de DevOps y de TI que prioriza la nube. Debido a la rápida expansión impulsada por las adquisiciones, su entorno de TI es muy dinámico y cambia con frecuencia. Se enfrentaron a tres grandes desafíos para lograr ese objetivo.

Cumplimiento NACHA

Además de la inminente legislación de privacidad de datos a nivel estatal, se acercaba una fecha límite difícil para los nuevos requisitos de NACHA. NACHA es similar a PCI DSS en algunos aspectos, pero va más allá de los datos del titular de la tarjeta y requiere protecciones para formas adicionales de datos personales no relacionados con la información de la cuenta de pago.

El sistema de cotización y procesamiento de reclamos de la aseguradora almacenó millones de registros de PII, incluidas licencias de conducir, información de cuentas bancarias, información de pólizas, Números de Seguro Social y otros datos confidenciales dentro de campos de texto libre, tanto estructurados como semiestructurados. Si bien estos datos ya estaban protegidos con varios medios, incluida una solución de tokenización existente, la aseguradora necesitaba una solución más ágil y escalable a medida que se trasladaban a aplicaciones basadas en la nube para el aprendizaje automático y el análisis. La capacidad de descubrir y proteger datos confidenciales semiestructurados dentro de campos de texto libre era un requisito clave.

PRODUCTOS

- SecurDPS Enterprise
- SecurDSP Discover & Classify
- SecurDPS Connect

DATOS RELEVANTES

- Cumplió con los últimos requisitos de protección de datos de NACHA y se preparó para futuras regulaciones
- Permitió a los científicos de datos detectar el fraude de manera más efectiva sin exponer la PII
- Descubrimiento de datos automatizado y sin agentes para una gobernanza de datos altamente eficiente
- Seguridad nativa en la nube que permite la transformación a la metodología DevOps
- Solución implementada en una fracción del tiempo que demandan las soluciones de la competencia

Análisis de datos, IA y Aprendizaje Automático con Datos Confidenciales

Su equipo de ciencia de datos requería mayores volúmenes de datos para un análisis más profundo, utilizando una combinación de la nube de Amazon (AWS) y Google BigQuery en Google Cloud. Esto requería eliminar el riesgo de la PII y mantenerla en un formato utilizable que les permitiera hacer uso de conjuntos de datos más grandes.

Por ejemplo, tenían datos que se trasladaban operativamente desde su ecosistema local a AWS para su preparación, y luego se trasladaban hacia un entorno de GCP y Big Query para procesos de análisis automatizados para la gestión de riesgos de seguros, la reducción de riesgos y la predicción. Con datos en movimiento como este, era absolutamente crítico que los datos viajaran seguros a lo largo del flujo de trabajo.

El flujo de trabajo finalizó con un análisis crítico para el negocio basado en la ciencia de datos, y todo el flujo de trabajo se orientó para lograr una hiperagilidad mientras se obtenía información. El principal desafío aquí fue mantener los datos confidenciales protegidos, pero en un estado en el que aún podrían usarse para análisis de datos con gran volumen, alta velocidad y gran variedad.

La aseguradora estaba trabajando con un ecosistema para el procesamiento tradicional de reclamos heredado que se basaba en la transformación previa, pero el cliente estaba migrando rápidamente sus aplicaciones a la nube para el aprendizaje automático y el análisis basado en IA. Los ecosistemas de datos que se mueven rápidamente tienen el potencial de exponer los datos, lo que resulta en la incapacidad de utilizar todos los datos que necesita porque los métodos de protección tradicionales pueden tropezar con el aprendizaje automático automatizado y los flujos de trabajo de las aplicaciones de IA.

Desafortunadamente, su solución de enmascaramiento de datos existente no pudo entregar datos al entorno de aprendizaje automático y a la IA escalada, ya que creó señales de alerta en sus procesos de desarrollo de aplicaciones. La solución existente funcionó en un entorno de prueba, pero falló en un entorno de análisis basado en inteligencia artificial y aprendizaje automático, ya que habría expuesto datos en vivo y creado un riesgo de filtración por exposición accidental, amenazas internas o ataques externos.

Los datos confidenciales tendrían que protegerse y mantenerse en un formato que permitiera procesarlos mediante el aprendizaje automático y las aplicaciones basadas en IA.

Transferencia de Datos Zero Trust y Transferencia a Aplicaciones SaaS

Su centro de datos de clientes contenía una combinación de datos no confidenciales y PII que era administrado por equipos en el extranjero. De acuerdo con una metodología de Zero Trust (cero confianza), querían proteger todos los datos confidenciales siempre que fuera posible para reducir el riesgo de fugas de datos tanto internas como externas.

Además, incorporarian aplicaciones SaaS en un futuro próximo, lo que también requería una solución que evitara que la PII quedara expuesta innecesariamente en la nube o mientras se transfería a ella. Desafortunadamente, los controles tradicionales que vienen con las modernas plataformas en la nube tienden a ser de una generación anterior de controles de acceso de datos en reposo y datos en movimiento y, controles basados en el perímetro. En muchos casos, estos controles solo protegen los datos una vez que ya han ingresado a la nube, lo que presenta una gran brecha de seguridad.

Para complicar aún más el asunto, querían mover una infraestructura de TI fusionada (de 13 empresas) de un modelo centrado en el centro de datos, a un modelo distribuido en la nube, lo que requería un mecanismo de descubrimiento de datos mucho más poderoso que el que habían estado ejecutando.

SOLUCIÓN

Descubrimiento de Datos Continuo y Sin Agentes

El primer paso para cerrar las brechas de seguridad de los datos y eliminar el riesgo, es saber dónde se almacenan todos los datos confidenciales. Reemplazamos las tecnologías de descubrimiento existentes que tenían, con una solución continua y automatizada que puede descubrir repositorios desconocidos y permite un proceso de descubrimiento de datos mucho más eficiente y efectivo. Esto significa que no solo se pueden localizar datos confidenciales, sino también, saber para qué se usan, dónde se usan y qué aplicaciones los procesan. Todo esto ahora se puede hacer de forma automatizada en toda la empresa y en los ecosistemas de la nube. Esto les dio una imagen muy clara de dónde están los riesgos y dónde se necesitaban controles adicionales para cumplir con los nuevos mandatos de cumplimiento y reducción de riesgos.

Además, la solución de descubrimiento de datos no tiene agentes, lo que significa que impone muy poca carga a los servidores, por lo que se pueden escanear grandes volúmenes de datos en un período de tiempo relativamente corto.

Protección de Datos Escalable y de Extremo-a-Extremo

El problema de los datos confidenciales mezclados con datos no confidenciales en campos de texto de forma libre fue un desafío serio para la empresa. Nuestra solución superó ese desafío al ubicar automáticamente elementos de datos confidenciales dentro del campo de texto de forma libre y aplicar la forma adecuada de protección según sus políticas. Si, por ejemplo, no es necesario proteger los últimos cuatro dígitos del Número de Seguro Social o un número de cuenta bancaria, se pueden dejar en texto sin cifrar, mientras que el resto se seudonimiza o enmascara. Incluso cuando se ha aplicado protección, los datos pueden conservarse en un formato reconocible para permitir el aprendizaje automático y el análisis de sentimientos.

Después, eliminamos las soluciones de protección de datos en silos para crear un flujo de trabajo único, continuo e iterativo dentro de la empresa. Instrumentamos la seguridad de los datos como un servicio en su programa DevOps y permitimos que la empresa consuma datos de producción protegidos con seguridad centrada en los datos aplicada en estos entornos en vivo. Protegemos los datos de extremo-a-extremo, desde la adquisición hasta las operaciones y las plataformas de ciencia de datos en cualquier nube. Nuestro enfoque compatible con DevOps y nativo de la nube en el que la infraestructura se podía ejecutar en Kubernetes, resolvió este problema que demostramos en la Prueba de Concepto.

Este enfoque holístico reduce la exposición de los datos personales, permite la gestión de datos a distancia sin exponerlos y, aun así, crea la capacidad de manejar y procesar todos estos datos, lo que permite el análisis de información muy interesante para todo tipo de análisis predictivos y sentimiento del cliente.

Integración transparente

Una de las aplicaciones clave en el alcance fue la de Informática MDM/360, que no tiene API para integrar el cifrado de terceros. A diferencia del enfoque API de su solución existente, nuestra solución podría implementarse en una fracción del tiempo y con una fracción del esfuerzo.

Nuestra plataforma de seguridad de datos permite la integración “complementaria” a los procesos identificados como de alto riesgo durante el descubrimiento de datos. En muchos casos, la protección de datos se puede lograr sin tener que cambiar la aplicación respectiva. La integración transparente también está disponible para archivos, flujos, bases de datos y canalizaciones que van desde intercepciones de JDBC hasta opciones de integración nativas (es decir, Apache Kafka). Esto permite que los datos confidenciales se protejan de manera efectiva sobre la marcha en el momento de la captura y, por lo tanto, durante todo su ciclo de vida.

BENEFICIOS DE NEGOCIO

Al igual que muchas empresas en su camino de transformación hacia la nube, DevOps, inteligencia artificial y automatización, el telón de fondo de las regulaciones de privacidad y el riesgo de incumplimiento pueden ser un gran obstáculo - estamos habilitando a esta aseguradora para que avance y continúe su viaje de crecimiento hacia la cima de las clasificaciones de seguros y para que ascienda en la clasificación del Fortune 250.

Protección Ágil para las Normas de Privacidad de Datos

Los datos están protegidos de extremo-a-extremo de acuerdo con NACHA, así como con muchas otras regulaciones de privacidad de datos, ya que la protección sólida de datos es un requisito común. Para garantizar la sostenibilidad, nuestra solución escalable se puede configurar fácilmente para incluir elementos de datos adicionales que pudieran estar dentro del alcance de futuras regulaciones.

Detección de Fraude e Información Comercial Más Eficaces

Uno de los mayores beneficios de la protección de preservación de formato, es que los equipos de ciencia de datos pueden utilizar conjuntos de datos mucho más grandes sin exponer datos confidenciales. Esto significa que pueden obtener información valiosa de manera más eficaz, tal como la detección de fraudes.

Gobernanza Eficiente de Datos y Reducción de Riesgos

Uno de los principales desafíos para la gobernanza de datos es comprender el panorama de datos y determinar si los datos descubiertos deben clasificarse como confidenciales y valiosos y, por lo tanto, requieran mitigación de riesgos. Este proceso ahora está completamente automatizado, lo que ahorra una gran cantidad de tiempo y recursos y, reduce el riesgo.

Ahora tienen una imagen clara de cómo se almacenan, procesan y comparten sus datos casi en tiempo real. Pueden descubrir y analizar automáticamente todo el uso de los datos y su linaje sin tener que depender del conocimiento preexistente de la presencia o ubicación de los datos.

Con este conocimiento de descubrimiento, pueden crear políticas de protección efectivas e implementar controles de seguridad apropiados. Pueden identificar datos confidenciales, protegerlos adecuadamente y luego monitorear los cambios en curso en el ecosistema de datos.

Nuestra solución de Descubrimiento y Clasificación aplica mejores medidas de privacidad, seguridad y gobernanza mediante la creación de un inventario de Catálogo de Datos Maestros. La vinculación de todas las piezas en una imagen informativa integral facilita la identificación del riesgo de cumplimiento y la gestión de las solicitudes de acceso de los interesados - incluyendo el derecho a borrar, actualizar o compartir cambios de datos.

> *Comforte ofrece un soporte impecable que ha ayudado a que el proceso de implementación transcurra sin problemas. Cada vez que nos comunicamos con ellos, recibimos una respuesta rápida de ingenieros experimentados que pueden diagnosticar y resolver rápidamente cualquier problema para que las cosas puedan seguir avanzando.*
>
> *– Ingeniero de Seguridad de Datos en el Principal Proveedor de Seguros de EE. UU.*