comforte

CASE STUDY

GROSSER US-AMERIKANISCHER VERSICHERUNGSANBIETER WÄHLT COMFORTE FÜR NACHA-COMPLIANCE

UNTERNEHMENSPROFIL

Dieser Fortune-500-Krankenversicherungsanbieter gehört zu den größten und am schnellsten wachsenden Schadens- und Versicherungsgruppen in den Vereinigten Staaten. Neben der Schadens- und Unfallversicherung bietet das Unternehmen auch Lebensversicherungen, Rentenversicherungen, Altersvorsorge, Hausratversicherungen, Kfz-Versicherungen und Arbeiterunfallversicherungen sowie Beratungs- und Investitionsdienstleistungen an.

Das Unternehmen verfügt über eine komplexe Datenumgebung mit einer Mischung aus Cloud- und On-Premises-Anwendungen und ist dabei, auf Cloud Native DevOps umzustellen. Die Kernanwendung für die Schadensregulierung läuft vor Ort und führt täglich Millionen von Transaktionen aus, während sie mit Dutzenden anderer Anwendungen interagiert. Aufgrund ihrer Wachstumsstrategie haben Fusionen und Übernahmen zu einer komplexen Architektur mit einer Vielzahl verschiedener Datenbanken geführt, die sie zu harmonisieren versuchen.

HERAUSFORDERUNGEN

Dieser große Versicherer verfügt über eine komplexe Datenumgebung mit Legacy-Tools und benötigte eine moderne Datenschutzlösung, die es ihm ermöglicht, sensible Daten zu schützen, während er auf einen modernen DevOps- und Cloudfirst-Ansatz in der IT umstellt. Aufgrund der schnellen Expansion, die durch Übernahmen vorangetrieben wurde, ist die IT-Umgebung des Unternehmens sehr dynamisch und ändert sich häufig. Um dieses Ziel zu erreichen, standen sie vor drei großen Herausforderungen.

NACHA-Compliance

Zusätzlich zu den bevorstehenden Datenschutzgesetzen auf staatlicher Ebene näherte sich eine harte Frist für neue NACHA-Anforderungen. NACHA ähnelt in mancher Hinsicht dem PCI DSS, geht aber über die Daten von Karteninhabern hinaus und erfordert den Schutz zusätzlicher personenbezogener Daten, die nicht mit Zahlungskontoinformationen zusammenhängen.

Das Schadenbearbeitungs- und Angebotssystem des Versicherers speicherte Millionen von Datensätzen mit personenbezogenen Daten, darunter Führerscheine, Bankkontoinformationen, Versicherungspolicen, SSNs und andere sensible Daten in strukturierten und halbstrukturierten Freitextfeldern. Diese Daten waren zwar bereits mit verschiedenen Mitteln geschützt, einschließlich einer bestehenden Tokenisierungslösung, aber der Versicherer benötigte eine flexiblere und skalierbarere Lösung, da er zu cloudbasierten Anwendungen für maschinelles Lernen und Analysen überging. Die Fähigkeit, halbstrukturierte sensible Daten in Freitextfeldern zu erkennen und zu schützen, war eine wichtige Anforderung.

PRODUCTS

- SecurDPS Enterprise
- SecurDSP Discover & Classify
- SecurDPS Connect

QUICK FACTS

- Erfüllt die neuesten NACHA Datenschutzanforderungen und ist auf zukünftige Vorschriften vorbereitet
- Ermöglicht Datenwissenschaftlern, Betrug effektiver zu erkennen, ohne PII preiszugeben
- Automatisierte und agentenlose Datenerkennung für hocheffiziente Data Governance
- Cloud-native Sicherheit ermöglicht die Umstellung auf DevOps-Methodik
- Implementierung der Lösung in einem Bruchteil der Zeit, die konkurrierende Lösungen benötigen

Datenanalyse, KI und maschinelles Lernen mit sensiblen Daten

Das Data-Science-Team des Unternehmens benötigte größere Datenmengen für tiefgreifendere Analysen unter Verwendung einer Mischung aus Amazon Cloud (AWS) und Google BigQuery in der Google Cloud. Dazu war es erforderlich, das Risiko für personenbezogene Daten zu verringern und sie gleichzeitig in einem verwendbaren Format zu halten, das die Nutzung größerer Datensätze ermöglicht.

So wurden beispielsweise Daten aus dem firmeneigenen Ökosystem zur Aufbereitung in AWS und anschließend in eine GCP- und BigQuery-Umgebung für automatisierte Analyseprozesse zur Risikoverwaltung, Risikominderung und Vorhersage übertragen. Bei dieser Art von Datenbewegung war es absolut entscheidend, dass die Sicherheit während des gesamten Workflows mit den Daten einherging.

Der Workflow endete mit geschäftskritischen Analysen auf der Grundlage von Data Science, und der gesamte Workflow war darauf ausgerichtet, bei der Gewinnung von Erkenntnissen eine hohe Agilität zu erreichen. Die größte Herausforderung bestand darin, sensible Daten so zu schützen, dass sie dennoch für Datenanalysen mit hohem Volumen, hoher Geschwindigkeit und großer Vielfalt verwendet werden konnten.

Der Versicherer arbeitete mit einem Legacy-Ökosystem für die herkömmliche Schadensbearbeitung, das auf die Zeit vor der Transformation ausgerichtet war, aber der Kunde migrierte seine Anwendungen schnell in die Cloud für maschinelles Lernen und KI-basierte Analysen. Schnelllebige Datenökosysteme bergen das Potenzial für die Offenlegung von Daten, was dazu führt, dass nicht alle benötigten Daten genutzt werden können, da herkömmliche Schutzmethoden automatisierte Workstreams für maschinelles Lernen und KI-Anwendungen behindern können.

Leider konnte die vorhandene Datenmaskierungslösung keine Daten für die skalierte KI- und Umgebung für maschinelles Lernen bereitstellen, da sie in den Anwendungsentwicklungsprozessen des Unternehmens zu Warnmeldungen führte. Die bestehende Lösung funktionierte in einer Testumgebung, versagte jedoch in einer maschinellen Lern- und KI-gesteuerten Analyseumgebung, da sie Live-Daten offengelegt hätte und ein Risiko für Datenschutzverletzungen durch versehentliche Offenlegung, Insider-Bedrohungen oder externe Angriffe dargestellt hätte.

Sensible Daten müssen geschützt und gleichzeitig in einem Format aufbewahrt werden, das die Verarbeitung durch maschinelles Lernen und KI-basierte Anwendungen ermöglicht.

Zero Trust Data Transfer und Umstellung auf SaaS-Anwendungen

Die zentrale Kundendatenbank des Unternehmens enthielt eine Mischung aus nicht sensiblen Daten und personenbezogenen Daten, die von Offshore-Teams verwaltet wurden. Im Sinne einer Zero-Trust-Methode sollten alle sensiblen Daten so weit wie möglich geschützt werden, um das Risiko interner und externer Datenlecks zu verringern.

Darüber hinaus sollten in naher Zukunft SaaS-Anwendungen eingeführt werden, was ebenfalls eine Lösung erforderte, die verhindert, dass personenbezogene Daten unnötigerweise in der Cloud oder bei der Übertragung in die Cloud offengelegt werden. Leider stammen die traditionellen Kontrollen, die mit modernen Cloud-Plattformen einhergehen, meist aus einer früheren Generation von Zugangskontrollen für gespeicherte Daten und in Bewegung befindliche Daten sowie von Perimeter-basierten Kontrollen. In vielen Fällen schützen diese Kontrollen die Daten erst, nachdem sie bereits in die Cloud gelangt sind, was eine große Sicherheitslücke darstellt.

SICHERN SIE IHR WACHSTUM MIT COMFORTE

Mit mehr als 20 Jahren Erfahrung in der Datensicherung auf wirklich unternehmenskritischen Systemen ist comforte der perfekte Partner für Unternehmen, die ihr wertvollstes Gut schützen wollen: Daten.

SecurDPS, die Data Protection Suite von comforte, wurde von Grund auf entwickelt, um die Datensicherheit in einer Welt zu gewährleisten, die von digitalen Geschäftsinnovationen, mündigen Kunden und ständigen technologischen Veränderungen geprägt ist. Wir helfen Ihnen, Ihr Wachstum zu sichern, indem wir Ihnen Fachwissen, eine innovative Technologie-Suite und lokalen Support bieten.

Wenn Sie mehr erfahren möchten, nehmen Sie noch heute Kontakt mit einem comforte-Mitarbeiter auf: www.comforte.com/contact/.

Erschwerend kam hinzu, dass das Unternehmen eine fusionierte IT-Infrastruktur (aus 13 Unternehmen) von einem rechenzentrumszentrierten Modell auf ein verteiltes Cloud-Modell umstellen wollte, was einen wesentlich leistungsfähigeren Datenermittlungsmechanismus erforderte, als er bisher eingesetzt wurde.

LÖSUNG

Kontinuierliche und agentenlose Datenermittlung

Der erste Schritt zur Schließung von Datensicherheitslücken und zur Beseitigung von Risiken besteht darin zu wissen, wo alle sensiblen Daten gespeichert sind. Wir ersetzten die vorhandenen Erkennungstechnologien durch eine automatisierte, kontinuierliche Lösung, die in der Lage ist, unbekannte Datenarchive zu erkennen und einen weitaus effizienteren und effektiveren Datenerkennungsprozess zu ermöglichen. Dies bedeutet nicht nur, dass sensible Daten gefunden werden können, sondern auch, dass man weiß, wofür die Daten verwendet werden, wo sie verwendet werden und welche Anwendungen sie verarbeiten. All dies kann nun auf automatisierter Basis im gesamten Unternehmen und bis hin zu den Cloud-Ökosystemen durchgeführt werden. Dadurch erhielten sie ein klares Bild davon, wo Risiken bestehen und wo zusätzliche Kontrollen erforderlich sind, um neue Compliance- und Risikominderungsvorgaben zu erfüllen.

Darüber hinaus ist die Data-Discovery-Lösung agentenlos, d. h. sie belastet die Server nur wenig, sodass große Datenmengen in relativ kurzer Zeit gescannt werden können.

Skalierbarer End-to-End-Datenschutz

Das Problem der Vermischung sensibler Daten mit unkritischen Daten in Freitextfeldern stellte für das Unternehmen eine große Herausforderung dar. Unsere Lösung meisterte diese Herausforderung, indem sie automatisch sensible Datenelemente innerhalb des Freiformtextfeldes aufspürte und auf der Grundlage der Unternehmensrichtlinien die entsprechende Form des Schutzes anwandte. Wenn beispielsweise die letzten vier Ziffern der Sozialversicherungsnummer oder eine Bankkontonummer nicht geschützt werden müssen, können sie im Klartext belassen werden, während der Rest pseudonymisiert oder maskiert wird. Selbst wenn die Daten geschützt wurden, können sie in einem erkennbaren Format belassen werden, um maschinelles Lernen undAnalysen von Stimmungslagen zu ermöglichen.

Als Nächstes entfernten wir isolierte Datenschutzlösungen, um einen einheitlichen, kontinuierlichen und iterativen Workflow innerhalb des Unternehmens zu schaffen. Wir integrierten die Datensicherheit als Service in das DevOps-Programm und ermöglichten es dem Unternehmen, geschützte Produktionsdaten mit datenzentrierter Sicherheit in diesen Live-Umgebungen zu nutzen. Wir schützen Daten durchgängig von der Erfassung über den Betrieb bis hin zu Data-Science-Plattformen in jeder Cloud. Unser cloudnativer, DevOps-freundlicher Ansatz, bei dem die Infrastruktur auf Kubernetes laufen kann, löste dieses Problem, was wir im PoC (proof of concept) demonstrierten.

Dieser ganzheitliche Ansatz reduziert die Offenlegung personenbezogener Daten, ermöglicht Offshore-Datenmanagement, ohne die Daten offenzulegen, und schafft dennoch die Möglichkeit, all diese Daten zu verarbeiten, was sehr interessante Analysen und Einblicke für alle Arten von Prognostischen Analyseb und Kundenmeinungsbildern ermöglicht.

Transparente Integration

Eine der wichtigsten Anwendungen war Informatica MDM/360, die keine APIs für die Integration von Drittanbieter-Verschlüsselung hat. Im Gegensatz zum API-Ansatz ihrer bestehenden Lösung konnte unsere Lösung in einem Bruchteil der Zeit und mit einem Bruchteil des Aufwands implementiert werden.

Unsere Datensicherheitsplattform ermöglicht eine “Snap-in”-Integration in Prozesse, die bei der Datenermittlung als risikoreich identifiziert wurden. In vielen Fällen kann der Datenschutz erreicht werden, ohne dass die jeweilige Anwendung geändert werden muss. Auch für Dateien, Streams, Datenbanken und Pipes steht eine transparente Integration zur Verfügung, die von JDBC-Abschnitten bis zu nativen Integrationsoptionen (z. B. Apache Kafka) reicht. So können sensible Daten bereits bei der Erfassung und damit über ihren gesamten Lebenszyklus hinweg effektiv gesichert werden.

GESCHÄFTSVORTEILE

Wie bei vielen Unternehmen, die sich auf dem Weg in die Cloud, DevOps, maschinelle Intelligenz und Automatisierung befinden, können Datenschutzbestimmungen und das Risiko von Datenschutzverletzungen ein großes Hindernis darstellen. Wir ermöglichen diesem Versicherer einen Sprung nach vorn und die Fortsetzung seines Wachstumskurses an die Spitze der Versicherungsrangliste und einen Aufstieg in der Fortune 250-Rangliste.

Agiler Schutz für Datenschutzbestimmungen

Die Daten werden durchgängig gemäß NACHA und vielen anderen Datenschutzbestimmungen geschützt, da ein starker Datenschutz eine allgemeine Anforderung ist. Um die Nachhaltigkeit zu gewährleisten, kann unsere skalierbare Lösung problemlos so konfiguriert werden, dass sie zusätzliche Datenelemente enthält, die in den Anwendungsbereich künftiger Vorschriften fallen könnten.

Effektivere Betrugsaufdeckung und Geschäftseinblicke

Einer der größten Vorteile der formatbewahrenden Datensicherung besteht darin, dass Data-Science-Teams viel größere Datensätze nutzen können, ohne sensible Daten preiszugeben. Das bedeutet, dass sie effizienter wertvolle Erkenntnisse gewinnen können, beispielsweise bei der Aufdeckung von Betrugsfällen.

Effiziente Data Governance und Risikoreduzierung

Eine der größten Herausforderungen bei der Data Governance besteht darin, die Datenlandschaft zu verstehen und zu bestimmen, ob entdeckte Daten als sensibel und wertvoll eingestuft werden sollten und daher eine Risikominderung erforderlich ist. Dieser Prozess ist nun vollständig automatisiert, was viel Zeit und Ressourcen spart und das Risiko deutlich reduziert.

Sie haben nun ein klares Bild davon, wie ihre Daten gespeichert, verarbeitet und weitergegeben werden, und das nahezu in Echtzeit. Sie können die gesamte Nutzung von Daten und deren Herkunft automatisch aufspüren und analysieren, ohne sich auf bereits vorhandenes Wissen über das Vorhandensein oder den Speicherort von Daten verlassen zu müssen.

Mit diesem Wissen können sie wirksame Schutzrichtlinien erstellen und geeignete Sicherheitskontrollen implementieren. Sie können sensible Daten identifizieren, sie angemessen schützen und dann die laufenden Änderungen im Datenökosystem überwachen.

Unsere Discovery and Classification Lösung setzt bessere Datenschutz-, Sicherheits- und Governance-Maßnahmen durch, indem sie ein Inventar des Master Data Katalogs erstellt. Die Verknüpfung aller Teile zu einem umfassenden Informationsbild erleichtert die Identifizierung von Compliance-Risiken und die Verwaltung von Zugriffsanfragen von Datensubjekten - einschließlich des Rechts auf Löschung, Aktualisierung oder Weitergabe von Datenänderungen.

> *Comforte bietet einen tadellosen Support, der dazu beigetragen hat, dass der Implementierungsprozess reibungslos verlief. Wann immer wir uns an Comforte wenden, erhalten wir eine prompte Antwort von erfahrenen Technikern, die alle Probleme schnell diagnostizieren und lösen können, so dass die Projekte, Themen und Prozesse weitergehen können.*
>
> *– Datensicherheitsingenieur bei einem großen US-Versicherungsanbieter*