

FORTUNE 500 VERSICHERUNGSGESELLSCHAFT AUTOMATISIERT DIE ERKENNUNG UND KLASSIFIZIERUNG VON SENSIBLEN DATEN

Dieses Fortune-500-Versicherungsunternehmen für Sach- und Unfallversicherungen hatte erhebliche Investitionen in mehrere Datenschutz- und Sicherheitslösungen getätigt, um sein riesiges Portfolio an Sach- und Unfallversicherungen und anderen Beständen ordnungsgemäß verwalten, schützen und nutzen zu können.

Ohne eine vollständig autonome Lösung zur Erkennung und Klassifizierung sensibler Daten war das Unternehmen jedoch besorgt, dass unvollständige und ungenaue Daten nicht nur die Wirksamkeit der verwendeten Tools beeinträchtigen, sondern auch, dass die Existenz dunkler Daten für das Unternehmen ein großes Risiko darstellte.

BRANCHENKONTEXT

Schaden- und Unfallversicherer haben einzigartige Anforderungen, die robuste, vollautomatische Datenerkennungs- und Klassifizierungsfunktionen erfordern:

- ▶ **Datenkonsolidierung:** Fusionen und Übernahmen führen dazu, dass disparate Datensätze unter einer gemeinsamen Unternehmensstruktur zusammengeführt werden. Das Auffinden aller persönlich identifizierbaren Informationen (PII) in allen Datenquellen und die ordnungsgemäße Klassifizierung der gefundenen Daten ist für die Datenkonsolidierung von entscheidender Bedeutung.
- ▶ **Identifizierung unstrukturierter Daten:** PII Daten können als strukturierte, halbstrukturierte oder unstrukturierte Daten vorhanden sein. Eine erfolgreiche Governance hängt davon ab, dass alle Daten unabhängig von ihrer Form identifiziert, gekennzeichnet und geschützt werden können. Dies kann besonders schwierig sein, wenn es sich um unstrukturierte PII Daten handelt, die informell erfasst und aufgezeichnet werden.
- ▶ **Datensegmentierung:** Große Unternehmen können mehrere Tochtergesellschaften haben, die unter einem einzigen Unternehmensdach operieren. Die Segmentierung ist für den Datenschutz, die Sicherheit und die Einhaltung von Vorschriften von entscheidender Bedeutung. Daher benötigen Sachversicherer eine genaue Datenerkennung und -klassifizierung mit klarem Geschäftskontext, um sicherzustellen, dass sich keine Daten in Netzwerken oder Datenquellen befinden, die nicht der jeweiligen Tochtergesellschaft gehören.

HAUPTANWENDUNGSFÄLLE UND ERFOLGSKRITERIEN

Abgesehen von den oben beschriebenen allgemeinen Anforderungen der Branche hatte das Unternehmen spezifische Anwendungsfälle im Sinn, um die Effizienz der comforte SecurDPS Discover & Classify-Lösung zu testen.

- ▶ **Automatisierte Datenermittlung:** Demonstration der Vorteile von comforte gegenüber einem statischen Regex-Pattern-Scan-Ansatz durch Anwendung der automatisierten Erkennung von strukturierten, semistrukturierten und unstrukturierten Daten sowohl in Cloud- als auch On-Premise Datenquellen.
- ▶ **Microsoft Office 365 E5-Integration:** Erweiterung der Sicherheits- und Compliance-Lösungen, die die Microsoft E5-Lizenzanwendungssuite umfassen.

QUICK FACTS

- ▶ Automatisierte Erkennung und Klassifizierung sensibler Daten mit Integration in bestehende DLP- und GRC-Lösungen zur Konsolidierung und Stärkung des Master-Katalogs mit sensiblen personenbezogenen Daten.
- ▶ Proof-of-Concept (POC) wurde innerhalb von 30 Tagen entwickelt, implementiert und abgeschlossen.
- ▶ Comforte SecurDPS Discover & Classify setzt den Standard für Datenerkennung- und Klassifizierung im Unternehmen.

SICHERN SIE IHR WACHSTUM MIT COMFORTE

Mit mehr als 20 Jahren Erfahrung in der Datensicherheit auf unternehmenskritischen Systemen ist die comforte AG der perfekte Partner für Unternehmen, die ihr wertvollstes Gut schützen wollen: Daten. Die Data Security Plattform von comforte wurde von Grund auf entwickelt, um die Datensicherheit in einer Welt zu gewährleisten, die von digitalen Geschäftsinnovationen und ständigen technologischen Veränderungen geprägt ist. Wir helfen Ihnen, Ihr Wachstum zu sichern, indem wir Ihnen Expertise, eine innovative Technologie-Plattform und lokalen Support bieten. Wenn Sie mehr erfahren möchten, nehmen Sie noch heute Kontakt mit unserem Team auf: www.comforte.com/contact



- ▶ **DLP, Datenschutz, Governance-Katalysator:** Nutzung und Verbesserung bestehender Investitionen, die der Kunde bereits in Lösungen für Governance, Risikomanagement und Compliance (GRC) sowie Data Loss Prevention (DLP) getätigt hat, darunter OnSpring, CyberArk, Alation und Cortex XDR. Erhöhen Sie den Wert bestehender Lösungen durch eine tiefere Erkennung von "unbekannten Unbekannten" und eine effektivere Klassifizierung aller Daten. Durch die Integration ermöglicht SecurDPS Discover & Classify das Tagging von Dateien in der E5 DLP-Lösung. Dies ermöglicht Unternehmen die Durchsetzung von Richtlinien.

BESTEHENDE HERAUSFORDERUNGEN

Um sein umfangreiches Portfolio an Sach- und Unfallversicherungen und anderen Beständen ordnungsgemäß zu verwalten, zu schützen und zu nutzen, hatte das Unternehmen erhebliche Investitionen in verschiedene Datenschutz- und Sicherheitslösungen getätigt. Ohne eine vollständig autonome Lösung zur Erkennung und Klassifizierung sensibler Daten, die die optimale Leistung dieser verschiedenen Lösungen steuert, war das Unternehmen jedoch sehr besorgt darüber, dass unvollständige und ungenaue Daten nicht nur die Wirksamkeit der verwendeten Tools beeinträchtigten, sondern auch, dass es durch die Existenz dunkler Daten einem erheblichen Risiko ausgesetzt war.

Effizienz und Genauigkeit der Datenermittlungs- und Klassifizierungslösung waren ein großes Problem: Das Unternehmen hatte sich für die Datenerkennung und -klassifizierung auf eine etablierte Lösung verlassen. Der hochgradig manuelle und statische Regex-Prozess, der von der etablierten Technologie verwendet wurde, beschränkte die Datenerkennung auf die bereits bekannten Datenquellen. Die unzureichende Möglichkeit, den gefundenen Daten einen geschäftlichen Kontext hinzuzufügen, führte dazu, dass die Mitarbeiter des Unternehmens die gefundenen Daten manuell klassifizieren und kennzeichnen mussten, was sehr zeitaufwändig und mühsam war.

Über die automatische Erkennung und Klassifizierung hinaus war die Integration mit der Microsoft 365 E5-Suite und einer Reihe anderer Sicherheits- und Compliance-Lösungen, in die der Kunde investiert hatte, unerlässlich. Jedes Unternehmen stellt sich die Frage wie am nachhaltigsten investiert werden kann, und dieses Unternehmen war zu Recht besorgt, dass die etablierte Lösung es ihm nicht ermöglichte, genug Nutzen aus den getätigten Investitionen zu erlangen. Die Demonstration des API-first-Ansatzes von comforte zur Verbindung mit Lösungen anderer Anbieter - darunter Proofpoint, Microsoft 365, OnSpring, CyberArk, Alation und Cortex XDR - lieferte den unwiderlegbaren Beweis, dass es eine wesentliche und offensichtliche Geschäftsentscheidung war, sich auf SecurDPS Discover & Classify als Motor für die Datenschutz- und Sicherheitstools zu verlassen, die der Kunde bereits eingesetzt hatte.

Kein Unternehmen, vor allem nicht in der stark regulierten Schaden- und Unfallversicherungsbranche, kann es riskieren, blind für dunkle Daten zu sein. Der Kunde verstand, dass "unbekannte Unbekannte" eine große Schwachstelle darstellen, und durch das anfängliche Projekt erkannte er, dass SecurDPS Discover & Classify seine Gefährdung stark minimieren konnte.

ERGEBNISSE

- ▶ Der POC wurde innerhalb von 30 Tagen durchgeführt. Die Geschwindigkeit, mit der Comforte in der Lage war, in das Projekt einzusteigen und es zu beenden, half dabei, das den starken Nutzen zu demonstrieren, den SecurDPS Discover & Classify bietet. Comforte SecurDPS Discover & Classify is now installed as the engine to drive the client's data security and governance toolset for superior outcomes in data governance, security, and privacy.
- ▶ Comforte SecurDPS Discover & Classify wird nun als Motor für die Datensicherheit und das Governance-Tools des Kunden angesehen, und zeigt klar auf, dass damit bessere Ergebnisse in den Bereichen Data Governance, Sicherheit und Datenschutz erzielt werden.

GESCHÄFTSVORTEILE

- ▶ **Die kontinuierliche und umfassende Suche von SecurDPS** nach unbekanntem sensiblen Daten im Unternehmen brachte eine Vielzahl von dunklen Daten ans Licht, so dass damit verbundene Risiken besser eingeschätzt und kontrolliert werden konnten.
- ▶ **Die Automatisierung**, die SecurDPS bei der Erkennung und Klassifizierung von Daten einsetzt, spart Zeit und Energie und erlaubt es, sich mit wertvolleren Dingen zu befassen. So kann sich das Unternehmen auf Wachstum statt auf Regulierung konzentrieren.
- ▶ **Die kontinuierliche Daten-Erkennung** durch comforte SecurDPS Discover & Classify gewährleistet die Anwendung globaler Datenschutz-, Governance- und Sicherheitsrichtlinien für strukturierte und unstrukturierte Daten, die sich überall in Unternehmensnetzwerken befinden.
- ▶ **Basierend auf einem innovativen und einzigartigen Ansatz** reduziert SecurDPS Discover & Classify „False Positives“ massiv, erhöht die Genauigkeit und reduziert den manuellen Aufwand für die Erkennung und Klassifizierung insgesamt.

DURCH DEN API FIRST-ANSATZ VON COMFORTE KANN SECURDPS DISCOVER & CLASSIFY MIT DEN LÖSUNGEN ANDERER ANBIETER EINFACH INTEGRIERT WERDEN

 Microsoft 365

 CYBERARK®

 proofpoint.

 CORTEX®

 Onspring

 Alation