SOLUTION BRIEF

COMFORTE – Discovery and Classification

Nachhaltige Datenerkennung für Datenschutz, Datensicherheit und Governance
Angesichts der zunehmenden Komplexität moderner Netzwerke und Datenspeicherumgebungen ist es nahezu unmöglich, eine ständige Transparenz sensibler Daten im gesamten Unternehmen zu gewährleisten. Die Systeme sind stärker miteinander verbunden als je zuvor, und die jüngsten Angriffe auf Daten zeigen, dass für eine wirksame Umsetzung von Datenschutzmaßnahmen eine genaue Kenntnis der Datenlandschaft erforderlich ist.

Mit manuellen Snapshots und Analysen kommt man nicht weit
Die Datennutzung ist unglaublich dynamisch und entwickelt sich ständig weiter. Sie haben keine Möglichkeit, jederzeit alle Orte zu kennen, an denen sensible Daten abgelegt sind, insbesondere wenn Sie auf reaktive manuelle Prozesse angewiesen sind und ein umfangreiches Daten-Ökosystem nutzen.

Vollständige Kontrolle über sensible Daten
Mit der Lösung **Data Discovery and Classification** von comforte können Unternehmen die gesamte Verwendung von Daten und deren Herkunft erkennen und analysieren, ohne auf Kenntnisse über Vorhandensein oder Speicherort dieser Daten angewiesen zu sein.
Und das Beste ist: Dieser Prozess ist vollständig automatisiert! Durch die Automatisierung ist es wesentlich einfacher, sich ein klares Bild davon zu machen, wie Ihre Daten in Echtzeit gespeichert, verarbeitet und weitergegeben werden.

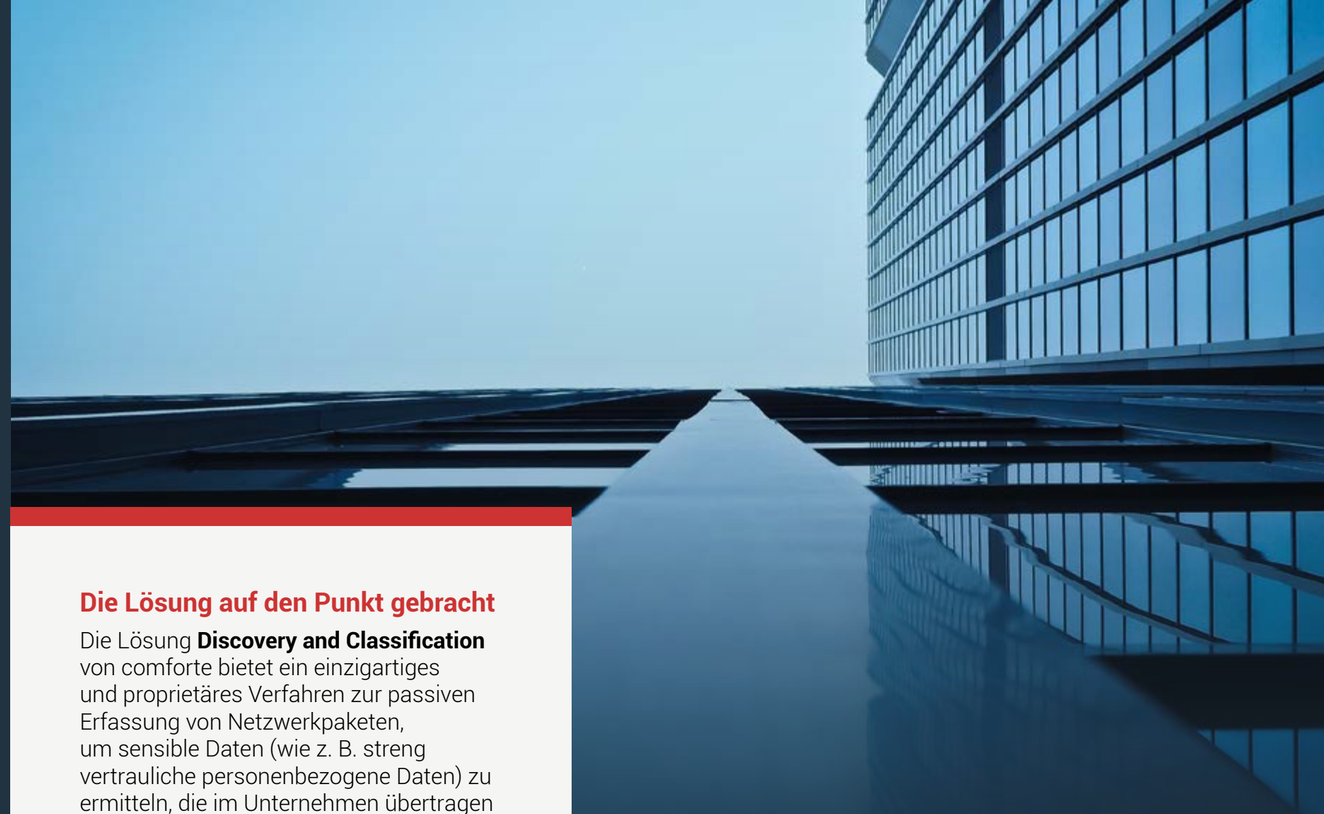
> Der Schutz von Daten setzt voraus, dass man weiß, wo sich die Daten befinden, und dass man weiß, worum es sich dabei handelt. Man kann nicht schützen, was man nicht kennt.

Verschiedene gesetzliche Bestimmungen legen Mindeststandards für den Datenschutz fest und verlangen von Unternehmen die vollständige Einhaltung dieser Standards. Diese Bestimmungen machen den Datenschutz zu einer absoluten Notwendigkeit für Ihr Unternehmen. Dabei ist zu berücksichtigen, dass das Unternehmen, das diese Daten erfasst, verarbeitet und speichert, aus Sicht der zuständigen Aufsichtsbehörden die Hauptverantwortung für den Datenschutz trägt!

Um das Risiko möglichst effektiv zu begrenzen, müssen Unternehmen **unbekannte sensible Daten in der gesamten Datenlandschaft erfassen**.

- Nahezu **in Echtzeit die Herkunft sensibler Daten** und den geschäftlichen Kontext jedes sensiblen Datenelements in Ihrer Umgebung verstehen
- **Vollständige Transparenz** über die Verwendung der Informationen jeder betroffenen Person
- Nachvollziehen, wenn sensible Produktionsdaten außerhalb von Produktionsumgebungen gefunden werden
- Automatische Erstellung eines vollständigen Master-Katalogs mit sensiblen Daten nahezu in Echtzeit
- Implementierung von Mess-, Überwachungs- und Kontrollinstrumenten zur Steuerung der Nutzung sensibler Daten
- Nachvollziehen, aus welchen unterschiedlichen Quellen sich die individuellen Datensätze für jede betroffene Person zusammensetzen

96% der Unternehmen in den USA betrachten *unbekannte Datenspeicher und -flüsse als Risiko*



Die Lösung auf den Punkt gebracht

Die Lösung **Discovery and Classification** von comforte bietet ein einzigartiges und proprietäres Verfahren zur passiven Erfassung von Netzwerkpaketen, um sensible Daten (wie z. B. streng vertrauliche personenbezogene Daten) zu ermitteln, die im Unternehmen übertragen werden. Aufgrund der Transparenz dieser Datenflüsse ist unsere Lösung in der Lage, Repositories (Datenbanken, Anwendungen, Dateisysteme und Protokolldateien) zu erkennen, in denen sich sensible Daten befinden. Die Lösung führt dann einen gründlichen Scan dieser Repositories durch, um einen umfassenden Einblick in die gesamte Datenlandschaft zu erhalten. Außerdem werden die bei diesen Scans identifizierten Daten analysiert und in einer Struktur konsolidiert, mit deren Hilfe Benutzer die Datenherkunft erkennen, auf Zugriffsanfragen betroffener Personen reagieren, Produktionsdaten an Speicherorten außerhalb von Produktionsumgebungen identifizieren und viele andere Aufgaben in den Bereichen Datenschutz, Sicherheit und Data Governance erfüllen können.

> “Sensible Daten und ihre Verwendung entdecken, und zwar auch solche, von denen Sie nicht wussten, dass sie in Ihrer Umgebung existieren.

Haben Sie alle Daten erfasst – und auch alles, was wichtig ist?

Ihr Datenökosystem ist dynamisch. Die Informationen darin ändern sich ständig. Daher müssen Sie diese Veränderungen kontinuierlich überwachen und das damit verbundene Risiko bewerten.

- Kontinuierliche Überwachung Ihres Netzwerks und Identifizierung von Netzwerkelementen
- Ausgangspunkt ist die vollständige Unkenntnis über den Inhalt Ihrer Daten
- Ermitteln von bekannten wie auch unbekannten Datenquellen
- Nutzung eines einzigartigen und proprietären Verfahrens zur passiven Erfassung von Netzwerkpaketen

> Fortlaufende Aktualisierung des Datenbestands mit minimalem manuellen Aufwand.

Praxisbeispiel

Eine Hotelkette hat beispielsweise 25 Millionen Kunden in 2.500 Datenspeichern. Kein Unternehmen kann diese Datenmenge manuell verwalten, ganz gleich, wie viele Mitarbeiter für diese Aufgabe abgestellt werden. Und da das erfolgreiche DevOps-Team fast jede Woche neue Produkte und Anwendungen einführt, sind diese Datenspeicher sehr dynamisch und ändern sich ständig. Ein einmaliges – oder auch nur gelegentliches – Scannen dieser Datenspeicher deckt nicht das gesamte potenzielle Risiko auf. Dieses Datenökosystem muss kontinuierlich gescannt werden, um auf dem Laufenden zu bleiben, was sich wirklich darin befindet.

Nur scannen, was wichtig ist

Aber wie entscheidet man, was wichtig ist?

Unsere Lösung erkennt sensible Datenelemente und Repositories, die mit manuellen Prozessen oder beschränkten Erkennungslösungen einfach nicht gefunden werden können. Warum sollten Sie unbekannte sensible Daten übersehen, die Ihr Unternehmen einem Risiko aussetzen?

> Eine der größten Sicherheitsherausforderungen in der Cloud bewältigen.

Die Lösung **Discovery and Classification** von comforte lässt sich mit einer Vielzahl von Datenquellen, zentralen Dateisystemen, branchenüblichen Datenbanken, NoSQL- und SaaS-Lösungen und sogar Amazon S3-Buckets verbinden.

Praxisbeispiel

Nicht alle Informationen sind im gleichen Maße von Interesse oder sensibel. In unserem Praxisbeispiel kann eine enorme Menge an Daten in den 2.500 Datenspeichern vorhanden sein, die überhaupt nicht sensibel sind. Und doch müssen Sie wissen, wo all die personenbezogenen Daten gespeichert sind, die wie kleine Perlen an einem riesigen Sandstrand liegen.
Sie brauchen eine Lösung, die erkennen kann, welche personenbezogenen Daten als Kundendaten gespeichert und verarbeitet werden (es gibt möglicherweise 50 bis 60 Felder mit solchen Daten, darunter Kreditkartendetails, Daten zur Kundentreue, zur Buchungshistorie, zu Vorlieben und Präferenzen, Reisepassdaten, ID von Mobilgeräten, Reiseversicherungspolicen, Flugdaten und Bank- oder Finanzdaten). Hier liegt das eigentliche Risiko für das Unternehmen.

Sensible Daten unabhängig von ihrer Art verstehen

Nicht alle Daten sind gleich.

Ihre Unternehmensdaten sind wahrscheinlich sowohl strukturiert als auch unstrukturiert und reichen von stark strukturierten Datenbanken bis zu formlosen Dokumenten wie PDFs und TXT-Dateien. Sie müssen alle Daten aufspüren, unabhängig von ihrem Typ oder Format. Die Aufsichtsbehörden werden keinen Unterschied machen, nur weil eine bestimmte Art von sensiblen Daten schwer zu finden oder zu bearbeiten ist.

- Daten vor Ort oder in der Cloud finden, sowohl strukturierte als auch unstrukturierte, und zwar unabhängig davon, ob sie in Bewegung sind oder nicht
- Datenbanken, Dateisysteme und andere Repository-Typen analysieren
- Machine-Learning-Funktionen nutzen, die Ihre Daten „lesen und verstehen“

Praxisbeispiel

In unserem Praxisbeispiel ist ein Großteil der Informationen in den 2.500 Repositories in bekannten Datenbanken strukturiert. Informationen wie die 50 bis 60 Felder mit personenbezogenen Daten (Kreditkartendaten, Treuedaten, Buchungsdaten) stammen definitiv aus bekannten Datenbanken. Einige kundenbezogene Informationen können jedoch auch in unstrukturierten Daten enthalten sein. Dazu gehören beispielsweise die Korrespondenz von Kunden, Datenanalyse-Informationen in verschiedenen Berichtsformaten (Word-Dokumente, PowerPoint-Präsentationen) und andere nicht aus Datenbanken stammende Informationen. Sie können nicht einfach davon ausgehen, dass alle personenbezogenen Daten in bekannten strukturierten Datenbanken gespeichert sind – eine solche Annahme führt zu weiteren Risiken und Gefahren.

Die ermittelten Daten organisieren

Ordnen Sie Ihre Daten den Personen oder Einrichtungen zu, die diese Daten verwenden. Bestimmen Sie, was wirklich Ihre Daten sind, und erstellen Sie dann eine einheitliche Ansicht:

- Verknüpfen von sensiblen Daten aus unterschiedlichen Quellen in einem Datensatz für jede betroffene Person
- Vergleichen des entsprechenden Datensatzes mit der bekannten geschäftlichen Nutzung, um bekannte, verwaltete personenbezogene Informationen zu bestätigen

Praxisbeispiel

In diesem Beispiel geht es um 25 Millionen Kunden. Um das Risiko vollständig zu minimieren, müssen Sie so viel wie möglich über diese einzelnen Kunden wissen. Sie benötigen also ein System, das in der Lage ist, herauszufinden, 1) was ein Kunde ist, 2) wer die Kunden bis hin zu den einzelnen Personen oder Unternehmen sind und 3) wo sich die Kundendaten verstreut haben und wo sie vervielfältigt wurden. Ein Kunde kann beispielsweise John Smith heißen, und seine Handy-ID und E-Mail-Adresse befinden sich in den Datensätzen für mobile Transaktionen. Seine Buchungshistorie befindet sich sowohl in der DB2-Masterdatenbank als auch in einem Cloud Data Lake sowie in 86 CSV-Dateien in 14 Dateispeichern, die mit AWS S3 verbunden sind. Die Daten von John Smith werden von 36 verschiedenen Anwendungen verarbeitet und sind in das CRM eingespeist. Sie befinden sich im Fluss und sind ungeschützt gespeichert. Außerdem gibt es Kopien der Daten in 25 ruhenden Datenbanken. Sie sehen also: Es wird kompliziert. Daten sind ziemlich viel unterwegs!

Den Weg Ihrer Daten verstehen

Verknüpfen Sie alle Teile zu einem aussagekräftigen Gesamtbild Ihrer Daten – ihre Quelle, ihre Verwendung und ihre Veränderung im Laufe der Zeit.

- *Datenherkunft* und *Datenfluss* verstehen
- Datensätze und Verweise mithilfe von entdeckten personenbezogenen Informationen aktualisieren
- Beziehung(en) der entsprechenden betroffenen Personen zu Ihrem Unternehmen bestimmen
- Sensible Daten identifizieren, die mit Dritten geteilt werden

Praxisbeispiel

Diese umfangreichen, dynamischen und sich ständig verändernden Daten müssen von Ihren Mitarbeitern gebündelt und genutzt werden. Sonst sind sie völlig wertlos! Sie müssen in der Lage sein, diese Daten visuell zu untersuchen und zu bewerten, wo sich diese Daten verteilt haben. Dies dient der Risikobewertung, der Festlegung von Prioritäten für die Risikominderung und dem angemessenen Datenschutz (z. B. Tokenisierung von Daten im Data Lake, da es sich hierbei um die umfangreichsten, am wenigsten geschützten und am häufigsten gemeinsam genutzten Informationen handelt).

Ermittelte Risiken nutzen, um optimale Kontrollmaßnahmen festzulegen

Erstellen Sie einen umfassenden virtuellen Katalog sensibler Daten, einschließlich der Angaben, wem sie gehören und wo sie verarbeitet, gespeichert und verwendet werden. Diese Datenelemente können mit Tags (wie beispielsweise *Compliance*, *Kunde*, *Geschäftszweig* und *Prozess*) versehen werden. So können die Daten abgerufen, analysiert, geordnet, sortiert und für Risikobewertungen im Hinblick auf Compliance-Lücken, Datenvolumen und Datentypen verarbeitet werden.

Darüber hinaus erkennt unsere Lösung Prozesse, in denen sensible Daten fließen, die ein Risiko für ein Datenleck darstellen können:

- Berichtsdaten in bisher unbekannten, ruhenden Datenbanken, Dateien, Speichern oder Freigaben
- Prozesse, die Daten mit einer Cloud teilen
- Unerwartete Dateispeicher, wie z. B. Auszüge aus einer Datenbank, die in SharePoint in Office 365 eingehen
- Prozesse, die nicht von den Dateneigentümern verwaltet werden (wie Kopien in Data Lakes)

Dank der Transparenz und der gewonnenen Erkenntnisse können Sie entscheiden, welche Daten geschützt oder gelöscht werden sollen, und das alles unter Einhaltung von Vorschriften und Auflagen. Die Plattform von comforte bietet Ihnen zahlreiche Schutzmechanismen. So kann Ihr Unternehmen sensible Daten vor dem Risiko von versehentlichem Verlust, Offenlegung oder versehentlichen Datenlecks aufgrund von Fehlkonfigurationen schützen und stets die richtigen Maßnahmen für die gefundenen Daten treffen.

> Hardware oder keine Hardware – das ist die eigentliche Frage

Durch die skalierbare, verteilte Architektur von comforte können Sie so viele Erkennungsinstanzen einsetzen, wie für die Zusammenführung der Daten erforderlich sind. Diese Analyseinstanzen können als physische oder virtuelle Instanz installiert werden (die in AWS innerhalb Ihrer VPC bereitgestellt werden kann).

Einblick in Datenbedrohungen oder -risiken

Verschaffen Sie sich nahezu in Echtzeit ein klares Bild davon, wie Ihre Daten gespeichert, verarbeitet und weitergegeben werden.

Erkennen und analysieren Sie automatisch die gesamte Datennutzung und die Herkunft der Daten, ohne dass Sie auf die bereits vorhandenen Kenntnisse Ihres Unternehmens über das Vorhandensein oder den Speicherort der Daten angewiesen sind.

Risiko reduzieren

Mit diesen Erkenntnissen können Sie wirksame Schutzstrategien erstellen und Sicherheitskontrollen implementieren, die auf Ihre geschäftlichen Anwendungsfälle abgestimmt sind. Sie können sensible Daten identifizieren, sie angemessen schützen und dann die laufenden Änderungen in Ihrem gesamten Datenökosystem überwachen.

Einhaltung von Datenschutzbestimmungen

Die Lösung **Discovery and Classification** von comforte gewährleistet bessere Datenschutz-, Sicherheits- und Governance-Maßnahmen durch die Erstellung eines *Stammdatenkatalogs*. Durch die Verknüpfung aller Teile zu einem umfassenden Informationsbild Ihrer Daten können Sie Compliance-Risiken identifizieren und Zugriffsanfragen von betroffenen Personen verwalten – einschließlich des Rechts auf Löschung, Aktualisierung oder Weitergabe von Datenänderungen.

Verwaltung sensibler Daten im gesamten Unternehmen

Die Lösung **Data Discovery and Classification** von comforte bietet eine umfassende Plattform für die Erkennung der Datenherkunft für alle personenbezogenen Daten in einem stetig wachsenden Unternehmen mit einer schnellen Zuordnung von Datenspeicherung, -verarbeitung und -verwendung. Unsere Lösung eignet sich ideal für die Erkennung von Daten, deren Zweck und Verwendung und ist auf die modernen Anforderungen an die Einhaltung von Datenschutzbestimmungen in datenintensiven Branchen abgestimmt.

Das gewünschte Ergebnis für unsere Kunden ist eine automatisierte Erkennung von Datenrisiken als kontinuierlicher Prozess, im Gegensatz zu einem einmaligen Prozess oder einem personalintensiven manuellen Prozess, der mit Fehlalarmen behaftet ist. Unsere Lösung gewährleistet ein schnelles und effizientes Aufdecken von unbekannten Risiken, die Ihrem Unternehmen, Ihrer Marke und Ihrem Ruf ernsthaften Schaden zufügen könnten.

In Kombination mit den Datenschutzprodukten von comforte sorgt unsere Lösung dafür, dass Datenrisiken aufgedeckt und Datenschutzverletzungen verhindert sowie gesetzliche Vorschriften eingehalten werden.

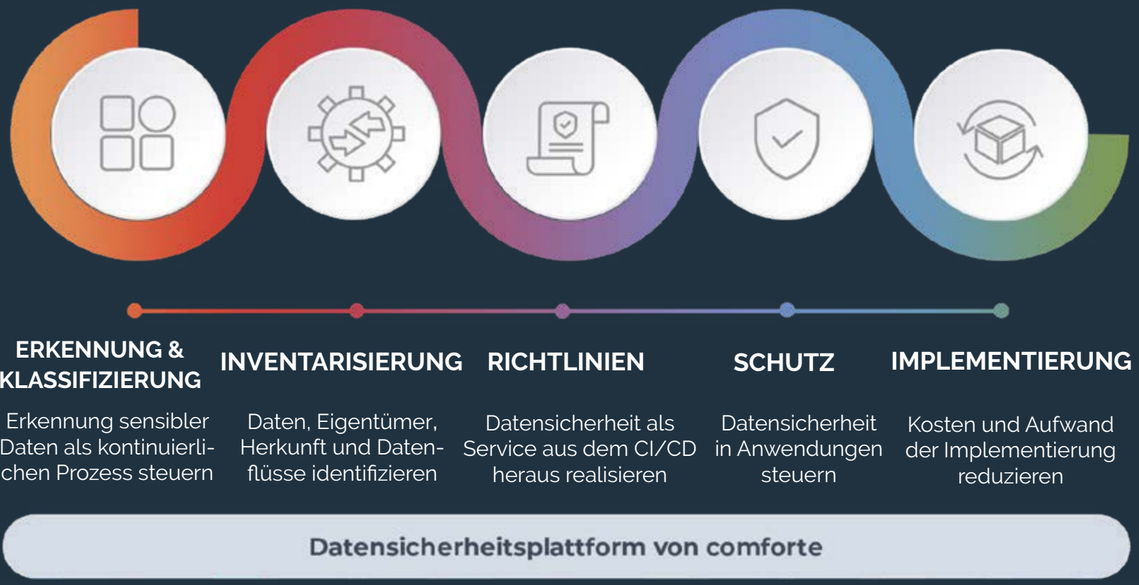
Zusammenfassung

Die Datenerkennung ist keine Selbstverständlichkeit. Bei komplexen und dynamischen Datenökosystemen, insbesondere in stark regulierten Branchen wie Finanzdienstleistungen, Gesundheitswesen und Versicherungen, funktioniert die manuelle Erkennung potenziell sensibler Informationen einfach nicht. Warum also ein derartig hohes Risiko eingehen?

Eine umfassende Lösung

Für die Implementierung datenorientierter Sicherheit ist eine Plattform erforderlich, die das Ermitteln, Schützen und Verwalten sensibler Daten ermöglicht. Außerdem muss diese Plattform in der Lage sein, diese Funktionen schnell und einfach in Ihre Unternehmensanwendungen und Ihre bestehende Cybersicherheitsinfrastruktur zu integrieren.

Die Datensicherheitsplattform von comforte bietet Ihnen dabei eine umfassende End-to-End-Datensicherheitsstrategie. So schützen unsere Kunden Millionen von Zahlungstransaktionen, sensible Gesundheitsdaten, Versicherungsdaten und vieles mehr, die alle zuverlässig in geschäftskritischen Umgebungen genutzt werden.



Die nächsten Schritte

Gerne zeigen wir Ihnen unsere Discovery and Classification Lösung in Aktion. Setzen Sie sich mit uns in Verbindung, um eine Demo oder ein Beratungsgespräch zu vereinbaren.

www.comforte.com

comforte

www.comforte.com