comforte

IM FOKUS: DATENSICHERHEIT
FÜR CLOUD & PII

WICHTIG FÜR IHRE DATEN:

Schutz von sensiblen Daten in Ihrer Cloud-Umgebung

Eine Cloud-basierte Infrastruktur und der Einsatz eines Cloud-orientierten Geschäftsmodells bieten enorme technische und wirtschaftliche Vorteile. Datensicherheit ist jedoch nicht unbedingt eine Selbstverständlichkeit.

> Sicherheit darf kein untergeordneter Aspekt sein. Doch leider beschäftigen sich viele Unternehmen nicht ausreichend mit einem sehr relevanten Thema: der Datensicherheit.

Sie denken vielleicht, dass sich Ihr Cloud-Anbieter um Ihre Datensicherheit kümmert, richtig? Cloud-Anbieter können Ihnen zwar viel bieten, aber die Verantwortung für die Datensicherheit liegt immer noch bei Ihnen selbst. Zudem steigt mit anspruchsvolleren Cloud-Implementierungen (Hybrid-Cloud, Multi-Cloud) auch die Komplexität Ihrer Daten-Workflows. Damit ist es schwieriger, Aspekte wie Datensicherheit über diese Bereiche hinweg zu managen. Die Einhaltung von Industriestandards sowie eine konsequente und zielgerichtete Ausrichtung auf die Sicherheit sollten ganz oben auf Ihrer Liste stehen.

Wortwolke zum Thema Cloud-Risiken

Hier sehen Sie auf einen Blick unterschiedliche Aspekte der Cloud-basierten Datensicherheit, die für IT-Organisationen problematisch sind:

Wir wissen, dass es für Sie wichtig ist, Geschwindigkeit und Agilität für Ihr Unternehmen mit der Notwendigkeit in Einklang zu bringen, Ihre sensiblen Daten vor absichtlicher und unabsichtlicher Offenlegung zu schützen. Wir wissen auch, dass dies ein Balanceakt ist. Aber diese beiden Schlagworte sollten Sie keineswegs abschrecken. Wir haben eine Lösung.

Wunsch wird Wirklichkeit

Stellen Sie sich vor, wie sich Ihr Sicherheitsgefühl (Ihr Seelenfrieden) verändern würde, wenn Sie Folgendes gewährleisten könnten:

- **Schutz sensibler personenbezogener Daten**, auch wenn sie in die falschen Hände geraten? Für die meisten Unternehmen ist es nur eine Frage der Zeit, bis es passiert. Falls es bei Ihnen eintritt, wäre es dann eine andere Situation, wenn Sie sicher sein könnten, dass sensible Informationen nicht preisgegeben werden?
- **Sensible, personenbezogene Daten verarbeiten und analysieren,** ohne dass der Schutz dieser Daten beeinträchtigt wird? Wie viele andere Unternehmen auch, lebt Ihr Unternehmen von der Datenanalyse. Doch damit sind Sie einem erheblichen Risiko ausgesetzt. Warum sollten Sie nicht einfach sowohl Datensicherheit als auch höchste Produktivität haben können?
- **Vermeidung** von Überprovisionierung, **Eliminierung** von Abhängigkeiten von konventionellen Anwendungen und **Orientierung** an agilen IT/Ops-Prozessen. Die Verwaltung der Datensicherheit in Ihrer Cloud-Umgebung muss nicht kompliziert sein oder sogar ein Hindernis für Produktivität und Agilität darstellen. Zumindest nicht mit der Datensicherheitsplattform von comforte.
- **Reduzierung** der Implementierungskomplexität und Vermeidung einer engen Kopplung, die zu einer Anbieterbindung oder langwierigen Programmierintegrationen führt, wann immer möglich. Mit Snap-In-Implementierungsfunktionen lässt sich unsere Datensicherheitsplattform einfach in Ihre Infrastruktur integrieren.

Datenorientierte Sicherheit im Mittelpunkt

Ihre Cloud-Daten sind dynamisch und mobil

Schützen Sie Ihre Daten, bevor Sie diese in Ihren Cloud-Anwendungen verwenden. Datenorientierte Sicherheit schützt die Daten selbst, egal wo sie hingehen. Sie müssen also nicht in einem geschützten Bereich liegen, um vollkommen sicher zu sein. Und wenn Sie die Daten bereits bei der Erfassung, Verarbeitung und Speicherung schützen, sind sie bereits gesichert, bevor Ihre Anwender in Ihren Cloud-Anwendungen mit ihnen arbeiten oder sie von Ihrem Dev-Ops-Team in einen Container eingebunden werden.

Native Cloud-Anwendungen in Ihrem Unternehmen nutzen

Bessere Agilität verschafft Ihnen einen Vorsprung. Dev-Ops-Teams müssen so agil wie möglich sein, um Innovationen mit schnellen, iterativen Ergebnissen zu erzielen. Traditionelle Sicherheitsarchitekturen sind oft nicht mit modernen Cloud-nativen Einsatzbedingungen, Automatisierung, Programmiersprachen und Orchestrierungs-Frameworks wie Kubernetes kompatibel. Außerdem ist infrastrukturorientierte Sicherheit häufig eine nur bruchstückhafte Lösung, die nicht mit Cloud-first-Strategien und -Architekturen vereinbar ist.

Datensicherheit in Cloud- und Cloud-nativen Plattformen ist sehr konventionell aufgebaut

Die Sicherheit in Cloud- und Cloud-nativen Plattformen ist abhängig von der zugrunde liegenden Kerninfrastruktur. Oft implementieren Unternehmen klassische Sicherheitskonzepte wie die „Isolierung“ von Containern zur Reduzierung der „Blast Zone“ sowie Schwachstellen-Scans und Verhaltensüberwachung, Zugriffskontrolllisten (RBAC) und teilweise auch Data-at-Rest-Verschlüsselung. All diese Ansätze sind veraltet und mit Risiken behaftet. Zudem bieten diese Gegenmaßnahmen keine Datensicherheit über den gesamten Lebenszyklus Ihrer Daten hinweg, und sie helfen sicherlich nicht bei der Einhaltung von Datenschutzbestimmungen. Ebenso wenig verhindern sie versehentliche Datenverluste durch Fehler und die Ausnutzung von Schwachstellen.

Die meisten vorhandenen Datensicherheitslösungen sind nicht für moderne Cloud-Architekturen ausgelegt

AGILITÄT OHNE ABSTRICHE BEI DER SICHERHEIT

Setzen Sie auf Cloud-Initiativen und sichern Sie zuerst Ihre sensiblen Unternehmensdaten, damit Sie die Einschränkungen von Vorschriften und Risiken überwinden können. Steigen Sie schneller auf eine Cloud-native DevOps-Strategie um.

Datenorientierte Sicherheit – was bedeutet das?

Die beste Möglichkeit, Datenschutzbestimmungen einzuhalten und gleichzeitig Technologien wie As-a-Service (aaS) und Cloud-native Lösungen zu nutzen, besteht darin, datenorientierte Sicherungsmaßnahmen für alle sensiblen Informationen in Ihrem Datenökosystem zu implementieren. Genau das tun viele Unternehmen bereits heute.

> Datenorientierte Sicherungsmaßnahmen schützen die Daten selbst, unabhängig davon, wo sie sich befinden.

Datenorientierte Sicherheit konzentriert sich auf den Schutz der Daten selbst und nicht auf Perimeter, Grenzen, Zugriffskontrolle auf Daten oder Speichermechanismen im Umfeld dieser Daten.

Um eine umfassende Datensicherheit zu gewährleisten, sind bestimmte technische Voraussetzungen erforderlich, die über den reinen Schutz (z. B. die Verschlüsselung der Daten) hinausgehen. Unternehmen müssen zunächst in der Lage sein, sensible Daten über verschiedene Systeme, Speicher und Plattformen hinweg zu finden und zu klassifizieren. Mit diesem Wissen können sich Unternehmen ein klares Bild von ihrer Datenlandschaft und den damit verbundenen Risikoebenen machen. Mit Blick auf den Schutz aller sensiblen Daten können Unternehmen nun Richtlinien erstellen und die geeigneten Datenschutzmechanismen bereitstellen, die tatsächlich zu ihren geschäftlichen Ausrichtungen und Datentypen passen.

Durch geeignete Sicherungsmechanismen wie die Nutzung von Tokens für strukturierte Daten ist der entsprechende Schutz unabhängig von Anwendungen, Datenbanken und Containern – im Ruhezustand, in Bewegung oder bei der Verwendung– stets mit den Daten verbunden. Dadurch haben Unternehmen die vollständige Kontrolle über ihre sensiblen Daten (Kontrolle des Benutzerzugriffs in Echtzeit und auf granularen Ebenen unter Nutzung von Verhaltensanalysen, Berichten über die Datennutzung und Sicherheitsereignissen) und können so die Compliance-Kosten senken und das Risiko von Datenschutzverletzungen deutlich reduzieren.

ERKENNUNG & KLASSIFIZIERUNG	INVENTARISIERUNG	RICHTLINIEN	SCHUTZ	IMPLEMENTIERUNG
Erkennung sensibler Daten als kontinuierlichen Prozess steuern	Daten, Eigentümer, Herkunft und Datenflüsse identifizieren	Datensicherheit als Service aus dem CI/CD heraus realisieren	Datensicherheit in Anwendungen steuern	Kosten und Aufwand der Implementierung reduzieren

Datensicherheitsplattform von comforte

UNSERE OBEN DARGESTELLTE DATENSICHERHEITSPLATTFORM BIETET DURCHGÄNGIGE DATENERKENNUNG, -KLASSIFIZIERUNG UND -SCHUTZ MIT EINFACHER INTEGRATION UND CLOUD-NATIVE SUPPORT.

Die Datensicherheitsplattform von comforte

Wir haben unsere Plattform von Grund auf speziell für moderne, agile Unternehmen entwickelt. Mit diesem Ansatz sind robuste, datenintensive Unternehmen in der Lage, Datenschutz und Sicherheit für ihre Kunden per Design zu gewährleisten. Wir sorgen dafür, dass sich der Datenschutz in Anwendungen, Datenprozesse und Arbeitsabläufe problemlos eingliedern lässt. Unsere Plattform kann integriert werden, ohne das Datensatzformat der ursprünglichen Daten zu verändern und verhindert dadurch kostenintensive Entwicklungsanpassungen. Somit eignet sich unsere Datensicherheitsplattform optimal sowohl für hybride IT als auch für Cloud-native Infrastrukturen.

Entwickelt für Cloud-first-Unternehmen

Mit der Einführung einer modernen DevSecOps-Strategie und der erhöhten Entwicklungsgeschwindigkeit, die DevOps für ein Unternehmen mit sich bringt, entsteht die Notwendigkeit einer ebenso agilen Datensicherheit. Dies setzt voraus, dass Sicherheitsprozesse und insbesondere die Datensicherheit in die Entwicklung und QA integriert werden. Die Umsetzung ist jedoch nicht immer einfach.

Unsere API-first Cloud-native Plattformarchitektur wird der modernen Infrastructure-as-Code-Strategie gerecht und ermöglicht ein echtes „Data-Security-as-Code“ Modell zur Bereitstellung für agile Unternehmen. Im Gegensatz zu Lösungen, die vor der Cloud und vor dem Datenschutz entwickelt wurden, ist die Plattform von comforte so konzipiert, dass sie innerhalb moderner operativer DevOps-Prozesse betrieben und genutzt werden kann, in die CI/CD- und Robotik-Prozesse integriert ist und die Vorteile moderner Anwendungsorchestrierungssysteme, einschließlich Kubernetes, für die automatisierte Skalierung, den Betrieb und das Management voll ausschöpft.

Datenschutz in jeder Anwendung

Die Datensicherheitsplattform von comforte gewährleistet den Schutz all Ihrer sensiblen Daten und Informationen für Anwendungen durch den Einsatz von Standardprotokollen. Dies ist insbesondere hilfreich für aaS-Anwendungen. Alle Sicherheitsmechanismen der Plattform entsprechen den Industriestandards.

Auf der Grundlage Ihrer geschäftlichen und gesetzlichen Anforderungen bietet unsere Plattform verschiedene Schutzmechanismen, um die in Anwendungen gespeicherten Daten zu sichern. Autorisierte Benutzer erkennen nicht, dass zusätzliche Sicherheit auf die Cloud-basierten Daten angewendet wird, die ihnen im Klartext angezeigt werden. Für alle anderen, die die Daten sehen könnten, sind sie vollständig verschleiert.

Entwickelt für Cloud-first-Unternehmen. Eine Plattform für End-to-End-Datensicherheit. Automatisierte Abläufe mit transparenter Integration.

Das spricht für sich.

Keine Unterbrechung Ihres Geschäftsbetriebs

Sichern Sie all Ihre sensiblen Daten und Informationen, die für die Cloud bestimmt sind, ohne Ihre Geschäftsprozesse und Arbeitsabläufe zu unterbrechen.

Schneller Wechsel zur Cloud-Agilität

Die einfache Implementierung sorgt für einen schnelleren Wechsel. Zu viele Cloud-Projekte scheitern schon zu Beginn an der komplexen Implementierung. Und selbst wenn Sie die erste Implementierung geschafft haben, können zunehmend komplexere Abläufe zu Problemen und Ineffizienzen führen.

Datenschutz und -sicherheit gehören zu Ihrer Cloud-Strategie

Datenschutzbestimmungen machen den Schutz von Daten zu einer absoluten Notwendigkeit. Implementieren Sie strenge Maßnahmen zum Schutz von Cloud-Daten, bevor diese in Ihr Cloud-Ökosystem gelangen, und stellen Sie gleichzeitig sicher, dass wertvolle Analysen und Datenverarbeitung möglich sind. Bringen Sie Datennutzung, Datenschutz, Kundendatenwert und Sicherheit auf einer einzigen integrierten und intelligenten Plattform in ein optimales Gleichgewicht.

Reduzieren Sie die unternehmerische Haftung

und vermeiden Sie die unbeabsichtigte Offenlegung von Daten, indem Sie unverschlüsselte sensible Daten durch verschleiernde Werte ersetzen, die bei Offenlegung keinerlei Bedeutung haben.

Halten Sie gesetzliche Vorschriften ein

reduzieren Sie die Haftung und vermeiden Sie gleichzeitig teure Geldstrafen, die sich auch negativ auf den Ruf Ihres Unternehmens auswirken können.

Reduzieren Sie den Umfang von Prüfungen

denn ein System, das keine zugänglichen sensiblen Informationen enthält, erfordert nicht den gleichen Prüfumfang wie ein System mit sensiblen Informationen. Ein geringerer Umfang bedeutet eine deutlich weniger kostspieliges Prüfung.

Sorgen Sie für Multi-Cloud-Schutz

durch einen einheitlichen, interoperablen Ansatz für die Datensicherheit in Cloud-Anwendungen über verschiedene Cloud-Service-Anbieter hinweg. Vereinfachen Sie die Prozesse durch einen einzigen, einheitlichen Ansatz und nutzen Sie gleichzeitig alle Vorteile, die Cloud-Anwendungen Ihrem Unternehmen bieten.

IHR NÄCHSTES ZIEL

Unsere Datensicherheitsplattform unterstützt Unternehmen seit Jahren bei der Erkennung wertvoller und sensibler personenbezogener Daten, bei der sicheren Einführung neuer Anwendungen und Daten-Workflows in ihre Abläufe sowie bei der Nutzung der Cloud und der Umstellung auf Cloud Native-Anwendungen – und das alles unter Wahrung der Datensicherheit und der Einhaltung gesetzlicher Datenschutzbestimmungen.

Informationen über unser Angebot sowie interessante Fallstudien finden Sie auf unserer Website

www.comforte.com

Hier können Sie auch gerne eine Produktdemonstration anfordern.

www.comforte.com/contact