comforte

SOLUTION BRIEF

COMFORTE Connect

SCHUTZ VON DATEN WÄHREND IHRES GESAMTEN LEBENSZYKLUS IN JEDER ANWENDUNG

Schnelle Implementierung für eine raschere Einhaltung von Vorschriften

Zahlreiche gesetzliche Vorschriften machen den Datenschutz zu einer absoluten Notwendigkeit, aber viele Anwendungen bieten nur minimale oder gar keine Datensicherheitsmaßnahmen. Datenverarbeitungsvorschriften legen Mindeststandards für den Schutz von Informationen fest. Ihre Einhaltung ist für Unternehmen, die in bestimmten Bereichen und Gerichtsbarkeiten tätig sind, verpflichtend. Unternehmen müssen die sensiblen, personenbezogenen Daten von Patienten und Kunden unter allen Umständen schützen. Dabei ist zu beachten, dass das Unternehmen, das die Daten sammelt, verarbeitet und speichert, die Verantwortung für den Datenschutz trägt!

Um die Compliance-Ziele schneller und nachhaltiger zu erreichen, müssen die Daten über ihren gesamten Lebenszyklus hinweg geschützt werden. Ein wichtiger Schritt in diesem Prozess ist die Berücksichtigung von Daten, die über web- und cloudbasierte Anwendungen, SaaS, COTS und Datenbankanwendungen erzeugt, verarbeitet und übertragen werden. Diese äußerst nützlichen Unternehmenstools bieten oft nur ein Minimum an Datensicherheitsfunktionen, und da die von ihnen erzeugten Daten sehr mobil sind, ist ein robusterer Schutz erforderlich.

SecurDPS Connect von comforte beschleunigt den datenorientierten Schutz von strukturierten, halbstrukturierten und unstrukturierten Daten in modernen Anwendungen und gehosteten Anwendungsworkflows und reduziert so schnell die potenzielle Gefährdung und die damit verbundenen Risiken. Die Implementierung von SecurDPS Connect kann innerhalb von Stunden statt Tagen oder Wochen erfolgen, sodass Sie schnell das richtige Maß an Sicherheit für Ihre Unternehmensanwendungen erreichen können.

MEHR ALS **3 /4** der von McAfee befragten Unternehmen gaben an, dass sie sensible Daten in öffentlichen Cloud-Umgebungen speichern.

MEHR ALS **50%** aller Unternehmen verlassen sich auf Cloud-Services, bei denen bereits sensible Daten gestohlen wurden.

Laut einem Bericht von IBM belaufen sich die durchschnittlichen Kosten für eine Datenschutzverletzung im Jahr 2020 auf

$3,86 Millionen USD

Zudem können Unternehmen mehr als

280 TAGE

benötigen, um eine Datenschutzverletzung zu erkennen, einzudämmen und zu entschärfen.

SecurDPS Connect schützt Ihr Unternehmen vor diesen Auswirkungen.

ALLE IHRE ANWENDUNGEN ERFORDERN AGILEN DATENSCHUTZ

Aber viele Anwendungen werden übersehen

Ihre Anwendungen müssen datenorientiert geschützt werden, unabhängig davon, ob sie vor Ort, als as-a-Service (aaS) oder in einer Cloud-Umgebung gehostet werden. Was wäre, wenn Sie Ihre Daten unabhängig davon, welche Anwendungen auf sie zugreifen, schützen könnten?

SecurDPS Connect schützt alle sensiblen Daten und Informationen, mit denen Ihre Benutzer in diesen Anwendungen arbeiten. Alle Sicherheitsmechanismen der Plattform entsprechen den Industriestandards. Auf der Grundlage Ihrer geschäftlichen und rechtlichen Anforderungen bietet SecurDPS Connect eine Vielzahl von Datenschutzoptionen, darunter Tokenisierung, formaterhaltende Verschlüsselung, klassische Verschlüsselung und Datenmaskierung.

Der entscheidende Punkt ist: Sie entscheiden, wie Sie Ihre Daten schützen möchten. Sie entscheiden, welche Felder geschützt werden sollen, z. B. Name, Adresse, Notizen, Identifikationsnummern wie Sozialversicherungsnummern oder Kontonummern. Dazu nutzen Sie eine vorlagenbasierte Methode zur Definition der zu schützenden Informationsfelder und Dateien. Der Vorteil ist, dass autorisierte Benutzer nicht erkennen, dass die Daten zusätzlich geschützt werden, da sie ihnen im Klartext angezeigt werden. Für alle anderen, die sie sehen könnten, sind die Daten vollständig verschleiert, sodass die geschützten sensiblen Informationen nicht kompromittiert oder missbraucht werden können.

SECURDPS
AUF DEN PUNKT GEBRACHT

SecurDPS Connect nutzt zahlreiche Sicherheitsmechanismen für Informationen auf Feld- und Dateiebene, bevor diese Daten in Ihren Anwendungen gespeichert werden, und stellt so sicher, dass die Daten bei der Übertragung zwischen verschiedenen Umgebungen wirksam geschützt sind.

CLOUD-ANBIETER TUN VIEL

Immer wenn ein Unternehmen sensible Daten in einer SaaS-Anwendung oder einem Cloud-Service ablegt, ist das Unternehmen selbst dafür verantwortlich, diese Daten zu schützen und die vertraulichen Informationen der Personen zu sichern, nicht der SaaS- oder Cloud-Anbieter. Jedes Unternehmen ist letztlich für seine eigene Datensicherheit verantwortlich, auch wenn Tools oder Anwendungen von Drittanbietern zur Verarbeitung und Speicherung dieser Daten verwendet werden. Und die Aufsichtsbehörden wissen das!

DATENORIENTIERTE SICHERHEIT ALS LÖSUNG

Nachlässigkeit bei herkömmlichen Datenschutzmethoden oder den von SaaS- oder Cloud-Anbietern angebotenen grundlegenden Sicherheitsservices kann zu weiteren Risiken und Gefährdungen führen. Die klassischen Sicherheitsansätze beruhen auf der Erkennung von Eindringlingen, dem Passwortschutz und anderen zugangsbasierten Maßnahmen. Die Branche hat jedoch immer wieder festgestellt, dass Eindringlinge immer einen Weg zu den Daten finden, die sie suchen. Daher entscheiden sich immer mehr Unternehmen für Lösungen, mit denen die eigentlichen Daten und nicht die Umgebung dieser Daten geschützt werden. Der Schlüssel dazu liegt in einer **datenorientierten** Sicherheit, die folgende Punkte berücksichtigt:

1/ Sensible Daten schützen, sobald Sie in den Workflows Ihres Unternehmens darauf zugreifen.

2/ Den Schutz nur dann aufheben, wenn es unbedingt notwendig ist, und zwar in einer sehr kontrollierten Umgebung, oder besser überhaupt nicht.

Datenorientierte Sicherheit konzentriert sich auf die Daten selbst, nicht auf die virtuellen Grenzen um diese Daten herum. Sie schützt die Daten auch dann, wenn sie sich außerhalb eines geschützten Bereichs bewegen, d. h. sie schützt Daten in Bewegung und Daten im Ruhezustand, ganz gleich, welche Anwendung diese Daten verarbeitet.

SO FUNKTIONIERT SECURDPS CONNECT

SecurDPS Connect arbeitet wie ein Gateway. Es sitzt zwischen den Anwendungen und den Benutzern in Ihrem Unternehmen, die mit diesen Anwendungen Daten sammeln, verarbeiten, übertragen und speichern. SecurDPS Connect fängt Datenströme ab und schützt diese Daten gemäß den rechtlichen Anforderungen des Kunden, die durch flexible Vorlagen definiert sind. So schützt SecurDPS Connect vor unberechtigtem Zugriff, egal welche Anwendung mit den Daten in Berührung kommt.

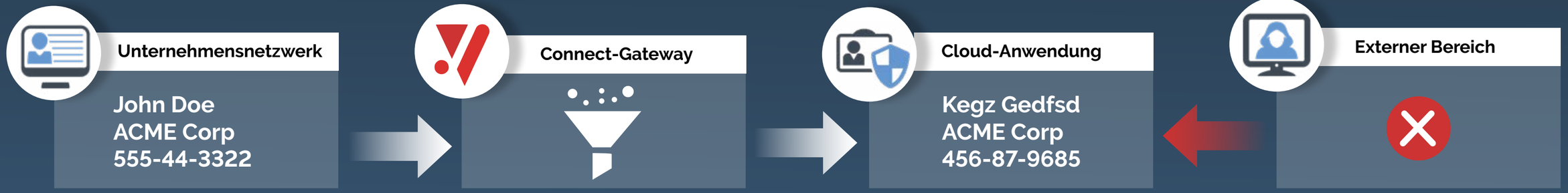
Intelligente Datensicherheit für eine schnelle Implementierung

Mit SecurDPS Connect können Benutzer individuelle Vorlagen entwickeln, mit denen die Lösung trainiert wird, sensible Daten zu erkennen und durch verschlüsselte oder tokenisierte Daten zu ersetzen, bevor diese Informationen in der Anwendung oder in der Cloud gespeichert werden. Mit diesen Vorlagen kann definiert werden, welche Arten von Informationen sensibel sind. Außerdem kann die Art des Schutzes für jedes einzelne Datenfeld festgelegt werden.

Nur autorisierte Benutzer können ungeschützte Daten anzeigen und bearbeiten. Für unbefugte Benutzer sind sensible Informationen völlig unverständlich, sodass der Datenschutz gewahrt bleibt und die Einhaltung von gesetzlichen Bestimmungen und Branchenvorschriften gewährleistet ist.

IMPLEMENTIERUNG VON SECURDPS CONNECT

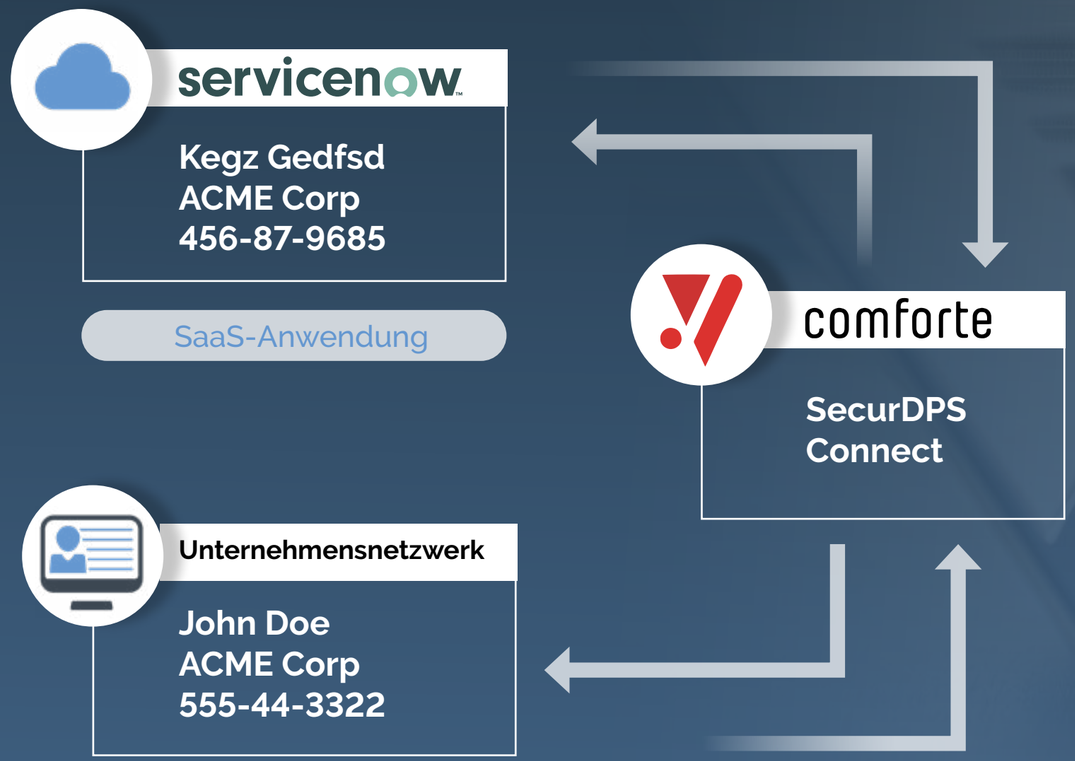
SecurDPS Connect-Proxys werden zwischen den Unternehmensbenutzern und den Anwendungen und Services eingesetzt, auf die sie zugreifen. Diese Proxys werden von einer Engine gesteuert, die anhand zuvor festgelegter Vorlagen bestimmt, welche Informationen geschützt werden müssen (und wie sie zu schützen sind), bevor sie an die Anwendung oder den Service weitergeleitet werden. Folgende Cloud-Anwendungen werden unterstützt: Salesforce, ServiceNOW, Microsoft Sharepoint, Microsoft Dynamics 365, Hubspot, Xing/LinkedIn und Tableau. Außerdem wird eine API-basierte Integration über REST-, JDBC- und ODBC-Verbindungen unterstützt.



SecurDPS Connect bietet Gateway-Funktionalität und dient als Proxy zwischen autorisierten Benutzern innerhalb des Unternehmens und Cloud-Services sowie Anwendungen.

BEISPIELWORKFLOW MIT SERVICENOW

Ein autorisierter Benutzer, der Informationen in ServiceNOW aktualisiert (z. B. ein Support-Ticket), kann den Nachnamen des Kontakts sehen (in diesem Fall Doe). SecurDPS Connect fängt diese Information jedoch ab, bestimmt die Vertraulichkeitsstufe des Feldes anhand der definierten Vorlage und schützt das Feld entsprechend, bevor es mit der Cloud-Anwendung interagiert. Für unbefugte Benutzer ist der Nachname des Kontakts durch die definierte Methode (Verschlüsselung, Tokenisierung oder Maskierung) geschützt und somit unverständlich.



EINE LÖSUNG, VIELE WICHTIGE VORTEILE

Unternehmen können insbesondere mit SaaS und Cloud-basierten Anwendungen schnell und wesentlich kostengünstiger auf den Markt kommen als mit Infrastrukturservices im Unternehmen vor Ort. Die Kostenvorteile der Cloud sind unbestreitbar.

Probleme entstehen jedoch, wenn sich Unternehmen auf die geringen Sicherheitsvorkehrungen von Cloud-Anbietern und SaaS-Angeboten verlassen. Daraus resultierende Datenschutzverletzungen können katastrophale Auswirkungen auf das Unternehmensergebnis und die Marke haben. Stellen Sie daher sicher, dass Sie die gesetzlichen Anforderungen übertreffen und somit das Risiko reduzieren, indem Sie SecurDPS Connect zwischen Ihren Benutzern und den Anwendungen auf die sie sich verlassen, implementieren.

Multi-Cloud-Schutz:

SecurDPS Connect bietet hochsicheren Schutz für zahlreiche Cloud-Services, darunter Salesforce, Microsoft Sharepoint und Dynamics 365, ServiceNow, Xing/ LinkedIn, Oracle Sales Cloud und viele mehr.

Gateway-Sicherheit:

SecurDPS Connect ist ein Gateway, das Datenströme von einem ICAP-fähigen Proxy analysiert und Daten auf der Grundlage kundenspezifischer Compliance-Regeln schützt. Dieser Ansatz bietet einen starken Schutz gegen unbefugten Zugriff.

Schutz-Mechanismus:

SecurDPS Connect ist sehr vielseitig. Wir unterstützen viele datenorientierte Schutzmechanismen, darunter starke Verschlüsselung, formatbewahrende Verschlüsselung, dynamische Schlüsselgenerierung, Tokenisierung und Pseudonymisierung.

Multi-Channel-Schutz:

SecurDPS Connect unterstützt mehrere Protokolle (wie HTTP, SMTP, OFTP und ICAP), Inhaltstypen (wie JSON, PDF, DOCX, XLS und CVS) und die Integration über mehrere APIs (einschließlich REST, JDBC und binär). Flexibilität ist entscheidend!

Vorlagenbasierter Schutz:

SecurDPS Connect nutzt Vorlagen, um sensible Daten in Datensätzen zu erkennen und diese Daten dann durch einen ausgewählten Schutzmechanismus zu schützen. Die Vorlagen werden mit unserer eigenen Domain Specific Language (DSL) erstellt.

NICHT NUR EINEN TEIL DES PROBLEMS LÖSEN

Unsere Kunden versuchen, das Problem der Datensicherheit nicht nur mit einem einzigen Schutzverfahren zu lösen, sondern mit einer End-to-End-Lösung, die ihnen hilft, ihre Daten zu kennen, zu verstehen und dann zu schützen – ganz gleich, wo sie sich befinden – und zwar mit dem am besten geeigneten datenorientierten Verfahren.

Unsere Datensicherheitsplattform hilft Ihnen, Ihr Ökosystem so zu optimieren, damit Sie wirklich wissen, wo die sensiblen Daten sind. Das erleichtert Audit- und Compliance-Maßnahmen.
Die Plattform besteht aus drei integrierten Services, die eine umfassende End-to-End-Datensicherheitsstrategie gewährleisten: SecurDPS Discovery & Classification, SecurDPS Enterprise für den Datenschutz und SecurDPS Connect als ideale Lösung für SaaS-basierte und On-Premise-Anwendungen.

ERKENNUNG & KLASSIFIZIERUNG

Erkennung sensibler Daten als kontinuierlichen Prozess steuern

INVENTARISIERUNG

Daten, Eigentümer, Herkunft und Datenflüsse identifizieren

RICHTLINIEN

Datensicherheit als Service aus dem CI/CD heraus realisieren

SCHUTZ

Datensicherheit in Anwendungen steuern

IMPLEMENTIERUNG

Kosten und Aufwand der Implementierung reduzieren

Datensicherheitsplattform von comforte

DAS SAGEN ANALYSTEN ÜBER UNS

Analysten haben unsere SecurDPS Connect-Lösung mehr als ein **Dutzend Mal** als herausragendes Beispiel für eine ideale, effektive Datenschutzlösung für Cloud-basierte Anwendungen und Services angeführt.

ÜBERZEUGEN SIE SICH SELBST

Schauen Sie sich SecurDPS Connect in der Praxis an! Bei der Arbeit mit realen Anwendungen und repräsentativen sensiblen Daten können wir demonstrieren, wie verschiedene Benutzer (sowohl autorisierte als auch nicht autorisierte) die Datenfelder sehen und wie die Lösung anhand von Eingaben aus Vorlagen funktioniert. Setzen Sie sich unter **www.comforte.com/contact** mit uns in Verbindung und vereinbaren Sie noch heute einen Demo-Termin.

comforte

www.comforte.com

Secure Your Growth