comforte

SOLUTION BRIEF

CONNECT

PROTEJA LOS DATOS DURANTE TODO SU CICLO DE VIDA EN CUALQUIER APLICACIÓN

Implementación rápida para un cumplimiento normativo más rápido

Los diversos requisitos reglamentarios hacen que la protección de datos sea una necesidad absoluta, pero muchas aplicaciones ofrecen medidas mínimas de seguridad de datos, si es que acaso ofrecen alguna. Las regulaciones de procesamiento de datos especifican estándares mínimos de protección de la información y exigen el cumplimiento a las empresas que operan dentro de dominios y jurisdicciones específicos. Las empresas deben proteger los datos confidenciales e identificables de personas, pacientes y clientes en todas las condiciones. ¡Tenga en cuenta que la empresa que recopila, procesa y almacena esos datos, es la que tiene la responsabilidad de proteger dichos datos!

Para cumplir con los objetivos de cumplimiento normativo de manera más rápida y duradera, debe proteger los datos durante todo su ciclo de vida. Un paso crítico en el proceso es abordar los datos generados, procesados y transmitidos a través de aplicaciones web y basadas en la nube, SaaS, COTS y aplicaciones de bases de datos. Estas herramientas empresariales altamente convenientes a menudo tienen capacidades mínimas de seguridad de datos, y debido a que los datos que generan son altamente móviles, necesitará una protección más sólida.

SecurDPS Connect de Comforte acelera la protección centrada en datos, de datos estructurados, semiestructurados y no estructurados en aplicaciones modernas y flujos de trabajo de aplicaciones alojadas, reduciendo rápidamente la exposición potencial y los riesgos asociados con ella. SecurDPS Connect facilita la implementación en horas en lugar de días o semanas, para que pueda implementar rápidamente el nivel adecuado de seguridad para sus aplicaciones empresariales.

MÁS DE **3/4** partes de las empresas encuestadas por McAfee indicaron que almacenan datos confidenciales en entornos de nube pública.

MÁS DE **50%** de todas las empresas confían en los servicios en la nube que han experimentado el robo de información confidencial.

Un informe de IBM muestra que el costo promedio de una violación de datos en 2020 es de

$3,86 millones USD

Además las empresas pueden tomar más de

280 DÍAS

para identificar, contener y mitigar una violación de datos.

SecurDPS Connect protege a su organización contra estas repercusiones

TODAS SUS APLICACIONES NECESITAN UNA PROTECCIÓN DE DATOS ÁGIL

Pero muchas aplicaciones son pasadas por alto

Sus aplicaciones necesitan protección centrada en datos, ya sea que las tenga de manera local, alojadas como servicio (aaS) o en un entorno de nube. ¿Qué pasaría si pudiera proteger los datos sin importar que aplicación esté trabajando con ellos?

SecurDPS Connect proteje todos los datos confidenciales y la información con la que trabajan sus usuarios en dichas aplicaciones. Todos sus mecanismos de seguridad cumplen con los estándares de la industria. En función de sus necesidades comerciales y reglamentarias, SecurDPS Connect ofrece una variedad de opciones de protección de datos que incluyen tokenización, cifrado con preservación de formato, cifrado clásico y enmascaramiento de datos.

El punto es que usted puede decidir cómo proteger sus datos. Usted selecciona qué campos deben protegerse (nombre, dirección, notas, números de identificación como números de seguro social o números de cuenta) a través de un enfoque basado en plantillas para definir los campos y archivos informativos que se protegerán. Lo mejor de todo es que los usuarios autorizados no reconocen que se está aplicando seguridad adicional a los datos, que se les muestran en texto sin formato. Para todos los demás que puedan verlo, los datos están completamente ofuscados, lo que mantiene la información confidencial protegida a salvo de ser comprometida y aprovechada.

SECURDPS EN POCAS PALABRAS

SecurDPS Connect aplica una variedad de mecanismos de seguridad para información a nivel de los campos y de archivos antes de que se almacenen esos datos en sus aplicaciones, asegurándose de que la seguridad efectiva viaje con los datos a medida que se mueven entre entornos.

LOS PROVEEDORES DE LA NUBE HACEN MUCHO

Cada vez que una empresa coloca datos confidenciales en una aplicación SaaS o en un servicio en la nube, la empresa misma tiene la responsabilidad de proteger esa información y mantener segura la información privada de las personas, no el SaaS ni el proveedor de la nube. Cada empresa es responsable en última instancia de la seguridad de sus propios datos, incluso si se utilizan herramientas o aplicaciones de terceros para procesar y almacenar esa información. ¡Y los reguladores lo saben!

DATA-CENTRIC SECURITY (SEGURIDAD CENTRADA EN DATOS) EN LA RESPUESTA

La complacencia en los métodos tradicionales de seguridad de datos o los servicios básicos de seguridad ofrecidos por SaaS o, los proveedores de la nube en realidad pueden generar más riesgos y exposición. Los enfoques de seguridad tradicionales dependen de la detección de intrusos basada en el perímetro, la protección de contraseña y otras medidas basadas en el acceso. Sin embargo, la industria ha visto una y otra vez que los actores de amenazas siempre encuentran la forma de obtener los datos que buscan. Esta es la razón por la que cada vez más empresas recurren a soluciones que protegen los datos reales en lugar de los bordes alrededor de esa información. La respuesta es centrarse en el **data-centric security (seguridad centrada en datos)** teniendo en cuenta lo siguiente:

1/ Proteja los datos confidenciales tan pronto como los toque dentro de sus flujos de trabajo corporativos.

2/ Solo desprotéjalo cuando sea absolutamente necesario dentro de un entorno muy controlado, o mejor aún, no lo desproteja en absoluto.

El Data-centric security (seguridad centrada en datos) se centra en los datos en sí, no en los bordes virtuales que los rodean. También protege los datos incluso si esos datos se salen de un perímetro protegido, por lo que protege los datos en movimiento y los datos en reposo, sin importar qué aplicación los toque.

LA MANERA EN LA QUE FUNCIONA SECURDPS CONNECT

SecurDPS Connect funciona como una tecnología de puerta de enlace. Reside entre las aplicaciones y los usuarios de su empresa que recopilan, procesan, transmiten y almacenan datos utilizando esas aplicaciones. Intercepta flujos de datos y los protege en función de los requisitos reglamentarios del cliente definidos a través de plantillas flexibles. De esta manera, SecurDPS Connect protege contra el acceso no autorizado sin importar qué aplicación lo toque

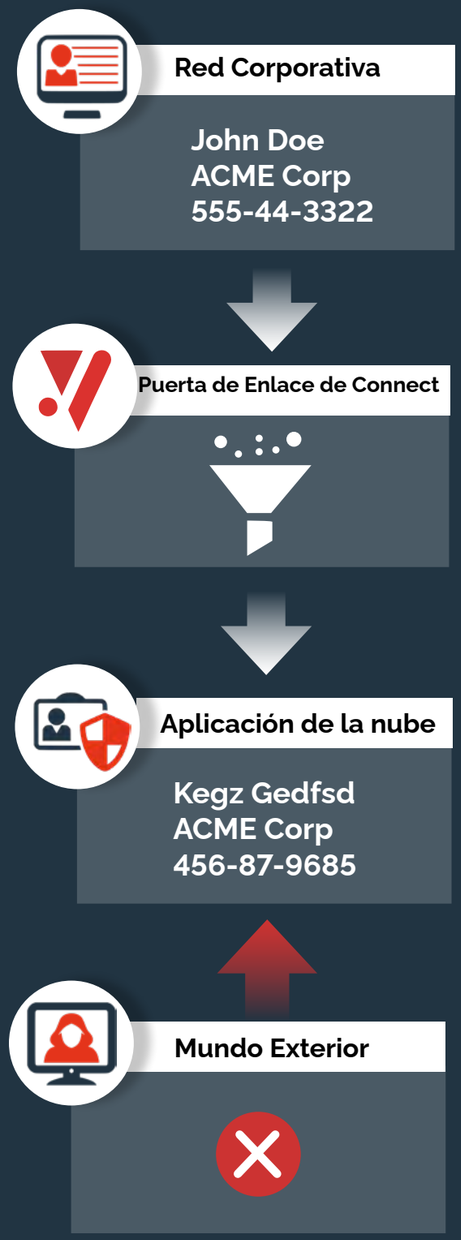
La seguridad de datos inteligente permite una implementación rápida

SecurDPS Connect permite a los usuarios desarrollar plantillas personalizadas que entrenan a la solución a detectar y reemplazar datos confidenciales con datos cifrados o tokenizados antes de que esa información se almacene en la aplicación o servicio en la nube. Estas plantillas proporcionan el mecanismo para definir qué tipos de información son confidenciales y guían el tipo de protección para cada campo de datos.

Solo los usuarios autorizados pueden ver y trabajar con datos desprotegidos. Para los usuarios no autorizados, la información confidencial es completamente incomprensible, lo que preserva la privacidad de la información y mantiene el cumplimiento de las normas y los mandatos de la industria.

CÓMO ESTA IMPLEMENTADO TODO EL SECURDPS CONNECT

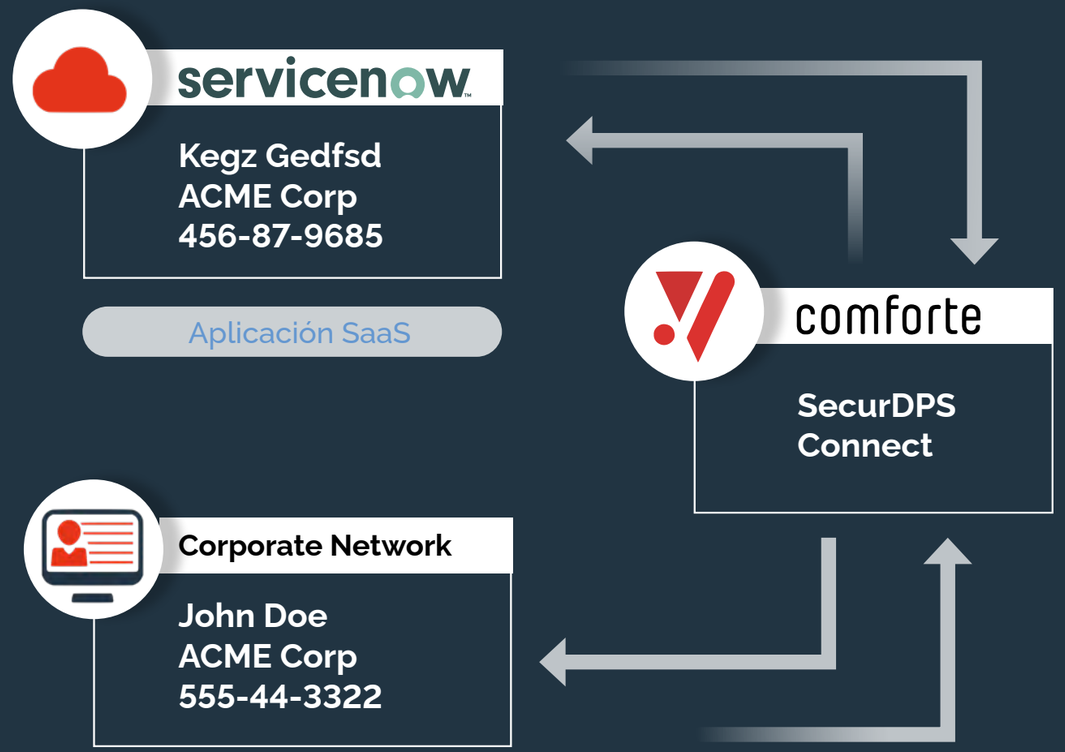
Los proxies de SecurDPS Connect residen entre los usuarios empresariales y las aplicaciones y servicios a los que acceden. Estos proxies son impulsados por un procesador que determina, en base a plantillas predefinidas, qué campos de información deben protegerse (y cómo protegerlos) antes de enviar esa información a la aplicación o servicio. Las aplicaciones en la nube admitidas incluyen Salesforce, ServiceNOW, Microsoft Sharepoint, Microsoft Dynamics 365, Hubspot, Xing/LinkedIn y Tableau. También es compatible con la integración basada en API a través de conexiones REST, JDBC y ODBC.



SECURDPS CONNECT PROPORCIONA FUNCIONALIDAD DE PUERTA DE ENLACE, SIRVIENDO COMO UN PROXY ENTRE LOS USUARIOS AUTORIZADOS DENTRO DE LA EMPRESA Y LOS SERVICIOS Y APLICACIONES EN LA NUBE.

EJEMPLO DE FLUJO DE TRABAJO UTILIZANDO SERVICENOW

Un usuario autorizado que actualiza la información en ServiceNOW (como un ticket de soporte) puede ver el apellido del contacto (en este caso, Doe). Sin embargo, SecurDPSConnect intercepta esa información, determina el nivel de sensibilidad del campo en función de la definición de la plantilla y protege el campo en consecuencia antes de interactuar con la aplicación en la nube. Para cualquier usuario no autorizado, el apellido del contacto está protegido por el método definido (cifrado, tokenización o enmascaramiento) y es incomprensible



"TOME EL CONTROL COMPLETO DE SUS DATOS CONFIDENCIALES CON EL MÍNIMO ESFUERZO"

UNA SOLUCIÓN, MUCHOS RESULTADOS VALIOSOS

Especialmente con SaaS y aplicaciones basadas en la nube, las empresas pueden llegarle al mercado de forma rápida y mucho más rentable que con los servicios de infraestructura en las instalaciones. Los beneficios de los costos de la nube son innegables.

Sin embargo, los problemas surgen cuando las empresas dependen de la seguridad mínima proporcionada por los proveedores de la nube y las ofertas de aaS. Las filtraciones de datos resultantes pueden ser catastróficas para el resultado final y para la marca. ¿Por qué no asegurarse de superar los requisitos reglamentarios, reduciendo así el riesgo, mediante la implementación de SecurDPS Connect entre sus usuarios y las aplicaciones de las que dependen?

Protección Multinube:

SecurDPS Connect ofrece una protección altamente segura en una gran cantidad de servicios en la nube, incluidos Salesforce, Microsoft Sharepoint y Dynamics 365, ServiceNow, Xing/Linkedin. Oracle Sales Cloud y muchos más.

Seguridad de la Puerta de Enlace:

SecurDPS Connect es una tecnología de puerta de enlace que analizó los flujos de datos de un proxy habilitado para ICAP y protege los datos según las reglas de cumplimiento especificadas por el cliente. Este enfoque proporciona una fuerte protección contra el acceso no autorizado.

Mecanismo de Protección:

SecurDPS Conect no es un mago de un solo truco. Mantiene muchos mecanismos de protección centrados en datos, incluido el cifrado sólido, el cifrado con preservación de formato, la generación dinámica de llaves, la tokenización y la seudonimización.

Protección Multicanal:

SecureDPS Connect admite múltiples protocolos (como HTTP, SMTP, OFTP e ICAP), tipos de contenido (como JSON, PDF, DOCX, XLS y CVS) e integración a través de múltiples API (incluidos REST, JDBC y binario). ¡La flexibilidad es clave!

Protección de Bases de Plantillas:

SecurDPS Connect aprovecha las plantillas para descubrir datos confidenciales dentro del contenido y luego los protege a través del mecanismo de protección elegido. Las plantillas se crean a través de nuestro propio lenguaje específico de dominio (DSL por sus siglas en inglés).

¿NO DEBERIA RESOLVER TODO EL PROBLEMA EN VEZ DE SOLO UNA PARTE?

Nuestros clientes están tratando de resolver el problema de la seguridad de los datos no solo con un único método de protección, sino con una solución de extremo-a extremo que los ayude a conocer, comprender y luego proteger sus datos, donde sea que estén, con un método lo más data-centric (centrado en datos) posible. ¿No deberías tú también? Nuestra plataforma de seguridad de datos ayuda a optimizar su ecosistema de datos para que sepa dónde están realmente los datos confidenciales. Esto facilita las actividades de auditoría y cumplimiento de las normas. La plataforma comprende tres servicios integrados para permitir una estrategia integral de seguridad de datos de extremo-a-extremo: SecurDPS Discovery & Classification, SecurDPS Enterprise para protección de datos y SecurDPS Connect, que es ideal para aplicaciones locales y basadas en SaaS.

DESCUBRE & CLASIFICA
Instrumentación sensible para la búsqueda de datos confidenciales como un proceso

INVENTARIO
Identifica datos, propietario, linaje y flujos

POLÍTICAS
Habilite la Seguridad de Datos como un Servicio del CI/CD

PROTEJA
Seguridad de datos instrumental en aplicaciones

IMPLEMENTE
Reduzca el costo y esfuerzo de la implementación. Sin código con muy poco código.

Plataforma Comforte Data Security

Secure Your Growth

www.comforte.com