cpl.thalesgroup.com

THALES

Las bases para la protección de datos sensibles en cualquier organización

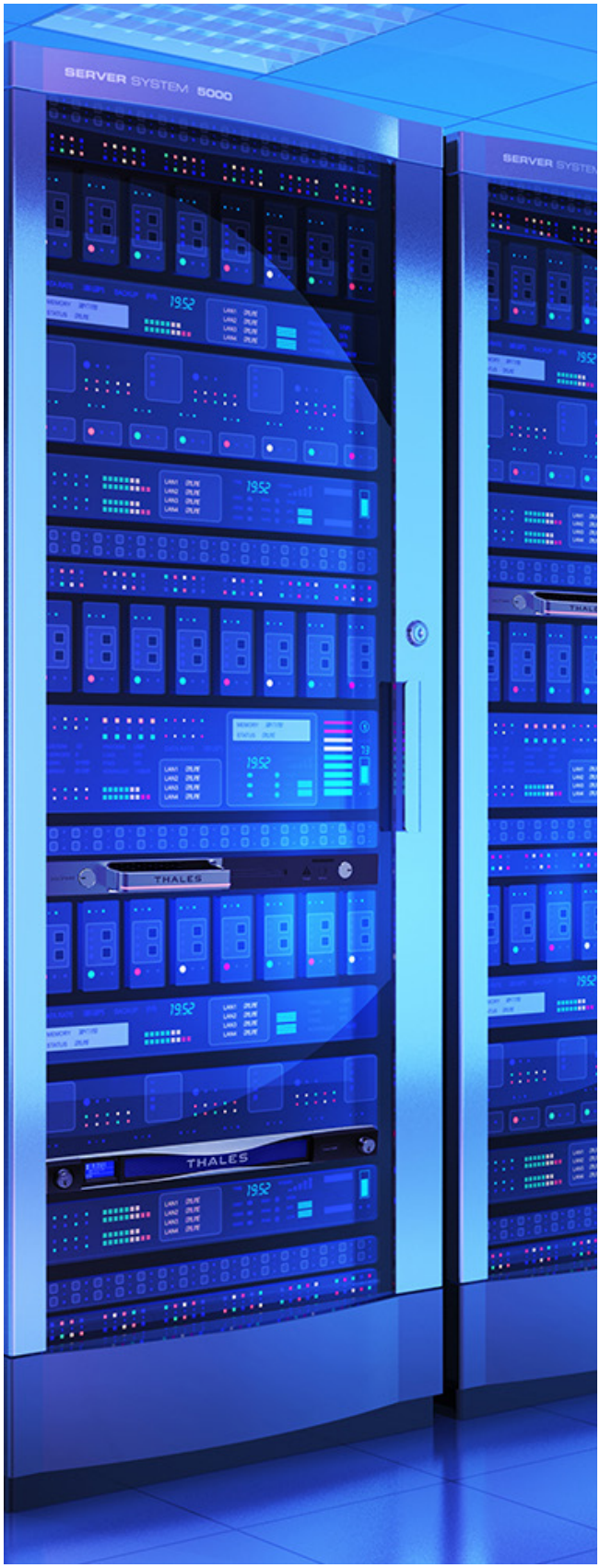
Libro blanco

Índice

Panorama general

Tradicionalmente las organizaciones han centrado la seguridad informática principalmente en la defensa del perímetro, construyendo muros para impedir que las amenazas externas entren en la red. Esto, aunque es importante, no es suficiente. Los ciberdelincuentes a menudo superan las defensas de los perímetros y se encuentran con datos que residen libremente en la nube sin defensas. Es por esto que las organizaciones deben implementar una estrategia de seguridad centrada en los datos para protegerlos allá donde estén. Con la proliferación de datos en la actualidad, el auge de los reglamentos de privacidad a nivel regional y mundial, el aumento en el uso de la nube y la persistencia de amenazas avanzadas, una seguridad centrada en los datos permite que las empresas tengan el control de sus datos sin importar dónde estén y evita que los ladrones de datos los puedan leer. Pero, para ser efectiva, esta protección debe actuar automáticamente sin depender de la intervención del usuario.

Este libro blanco se centra en los desafíos que supone la seguridad de los datos en esta era de proliferación de datos. También ofrece estrategias para localizar y clasificar sus datos críticos y aplicarles una seguridad centrada en los datos.



Proliferación de datos, incremento de los reglamentos y ciberdelincuentes más hábiles

Muchas de las arquitecturas de seguridad de datos se construyeron bajo el supuesto de que los datos se alojan en un centro de datos y se consumen in situ. El entorno de TI tradicional lo controlaba plenamente del departamento de TI. El equipo de TI era responsable de operar las infraestructuras, la seguridad y las aplicaciones, lo que le concedía una enorme visibilidad y control sobre datos y usuarios. Todo el acceso a datos y aplicaciones pasaba por capas de seguridad de perímetro, como cortafuegos, cortafuegos de nueva generación, VPN, antivirus, sistemas de prevención de intrusión, etc.

Seguridad más allá del perímetro para defender lo que más importa

Arquitectura tradicional de seguridad de datos

Seguridad basada en perímetro de confianza

Arquitectura de seguridad centrada en los datos

Seguridad que protege sus datos en cualquier lugar

Sin embargo, estos controles ya no existen en las organizaciones modernas. Con independencia de la robustez del perímetro del centro de datos, la seguridad que ofrece es solo conceptual, dado que:

1. **La seguridad del perímetro no se puede escalar en línea con la transmisión y proliferación de los datos**

El uso generalizado de servicios en la nube, entornos de macrodatos y tecnologías de IoT hace que las organizaciones transmitan grandes cantidades de datos con gran rapidez, a menudo a infraestructuras de terceros y socios. Esto conlleva una serie de desafíos:

- Datos en diversos formatos, incluyendo estructurados, semiestructurados y no estructurados.
- Cuellos de botella en la seguridad del perímetro, que ralentizan el rendimiento, lo que hace incumplir acuerdos de nivel de servicio (ANS) y provoca que los usuarios tengan a menudo acceso directo a servicios en la nube.
- Acceso interno desde fuera: no solo sus empleados pueden acceder a sus datos desde dentro del perímetro. Ahora sus datos están en manos de contratistas, proveedores de servicio y otras organizaciones externas. Estas personas con acceso interno son individuos que no ha examinado, no puede supervisar y no controla.

2. **Normativa y complejidad operativa**

La migración de datos a la nube, los contenedores, las tecnologías de big data y las diversas herramientas de multitud de vendedores añaden complejidad al asunto. Con perímetros de seguridad empresarial cada vez menos definidos, las organizaciones presentan dificultades a la hora de costear, implementar y gestionar políticas de acceso unificadas y coherentes para los recursos de TI distribuidos. Todas las organizaciones cuentan con una combinación de plataformas heredadas y nuevas.

Este crecimiento explosivo de datos se complica aún más con el creciente número de reglamentos en materia de privacidad a nivel regional y mundial con distintos requisitos de cumplimiento. Para cumplirlos con efectividad, las empresas ya no pueden confiar en enfoques aislados y tradicionales para mantener sus datos a salvo.

Todo esto se suma a que los entornos de datos actuales son cada vez más complejos. No es una sorpresa, pues, que las empresas piensen en la complejidad operativa como el principal obstáculo a la hora de implementar la protección de sus datos. Los directores de seguridad de la información y los directores de datos reconocen cada vez más la necesidad de establecer soluciones exhaustivas e integradas de seguridad de datos que ofrezcan protección completa de datos sensibles sin importar dónde se almacenen o usen.

Dado que las arquitecturas tradicionales de seguridad de datos no pueden lidiar con muchas de las características de este mundo moderno centrado en los datos, dichas arquitecturas no pueden proteger a las empresas de brechas de datos sofisticadas de ciberdelincuentes cada vez más determinados. Si los actuales directores de seguridad de la información y directores de datos quieren romper el ciclo reaccionario de medidas y contramedidas, deben comenzar a ver la seguridad con un enfoque completamente nuevo.

La complejidad operativa es el principal obstáculo a la hora de implementar la seguridad de los datos

Estrategia de tres puntos para proteger los datos sensibles de su empresa

Las arquitecturas de seguridad tradicionales han fallado mucho, dado que reflejan pensamientos obsoletos sobre cómo las empresas interactúan con sus datos. La seguridad de datos de hoy en día debe reconocer que los datos no solo son el activo más importante de una empresa, sino que también crecen a ritmo exponencial.

La seguridad centrada en los datos protege los datos, en lugar de solo proteger los puntos finales, las redes y las aplicaciones entre los que se mueven dichos datos. En consecuencia, los datos se protegen para que las empresas puedan transmitirlos según sus necesidades sin que el riesgo aumente. En vez de ralentizar el progreso e inhibir la proliferación de datos, la seguridad centrada en los datos permite a la empresa aprovechar al máximo sus datos dondequiera que se almacenen y usen.

Este gráfico muestra los tres pilares principales de la seguridad centrada en los datos.

Los tres pilares principales de la seguridad de datos

Nº1
Localizar y clasificar los datos sensibles

- Localizar y clasificar datos sensibles de forma eficiente
- Entender los datos y sus riesgos de forma clara

Nº2
Proteger los datos sensibles

- Proteger los datos sensibles con cifrado, controles de acceso y tokenización
- Hacer que sean ilegibles e inútiles en caso de robo o filtración

Nº3
Controlar las claves de cifrado

- Centralizar la gestión de claves
- Gestionar el ciclo de vida de las claves
- Gestión unificada de claves y políticas de cifrado

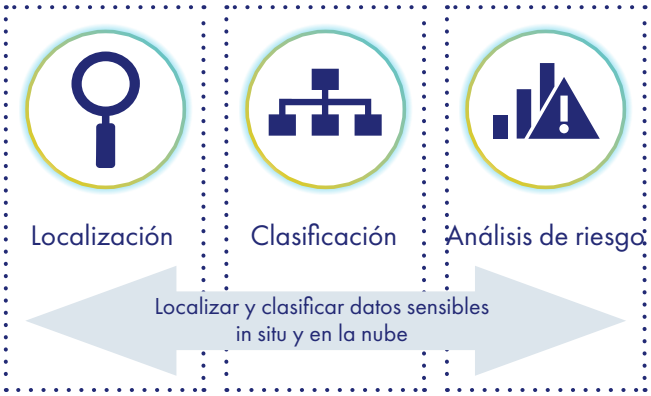
El ADN de una empresa debe incluir un enfoque de seguridad basada en los datos. Este enfoque holístico se basa en la experiencia de Thales tras colaborar con cientos de directores de seguridad de la información, directores de datos y directores informáticos, así como arquitectos al frente de la seguridad y protección de los datos, así como en las mejores prácticas requeridas por numerosos reglamentos y normativas sectoriales. Para adoptar este enfoque de seguridad de los datos, las empresas deben hacer lo siguiente:

1. Localizar y clasificar los datos sensibles

Se pueden encontrar datos sensibles por toda la empresa, la nube y más allá. Normalmente, la seguridad de TI cuenta con visibilidad limitada respecto a dónde se almacenan los datos y quiénes tienen acceso a estos. Los riesgos asociados a tener los datos distribuidos varían, desde brechas hasta incumplimientos normativos. Comience por identificar dónde se encuentran sus activos de datos más sensibles en su centro de datos local y luego pase a un entorno ampliado, como la nube y servicios alojados. Comience buscando sus servidores de almacenamiento y de archivos, aplicaciones, bases de datos y máquinas virtuales. Busque los datos por toda la empresa allá donde residan, y clasifique su grado de sensibilidad e importancia en base a las políticas internas y a los reglamentos externos.

Localizar, identificar y clasificar sus datos sensibles es el primer paso clave del proceso, pero esto se debe hacer con capacidad de repetibilidad y con independencia de la tecnología y de la situación geográfica. Las soluciones actuales de localización y clasificación de datos ofrecen paneles visuales y exploraciones que le permiten conocer con claridad qué clase de datos sensibles posee, dónde se encuentran y su clasificación de riesgo. Las clasificaciones de riesgo combinan varios parámetros, como nivel de protección, número de elementos encontrados, localización, cantidad de datos sensibles, etc., y permiten que las empresas conozcan el grado de sensibilidad de elementos particulares, como archivos y bases de datos. De esta forma, las empresas pueden proteger sus datos y mitigar los riesgos, por ejemplo, al dar prioridad a la mitigación o al tomar decisiones fundamentadas a la hora de compartir datos con terceros o migrar a la nube.

La localización y clasificación de datos es el primer paso hacia una seguridad de datos efectiva



2. Proteger sus datos sensibles

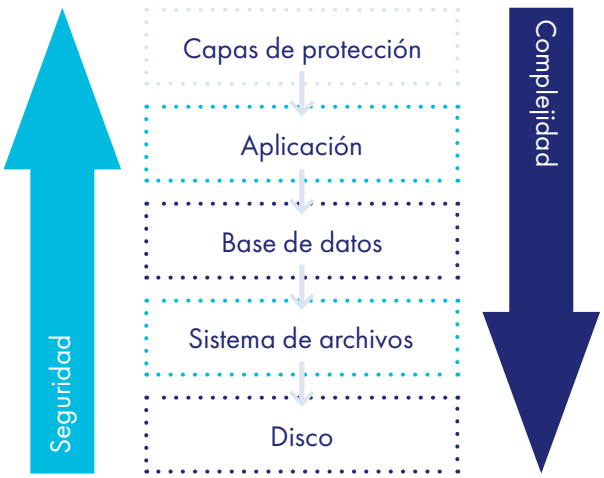
Lo ideal es que, para proteger los datos sensibles, haya establecido una estrategia básica de cifrado en toda su empresa, la cual mitiga los riesgos de filtración de datos y de divulgación de brechas.

Una vez haya localizado y clasificado sus datos, puede determinar el riesgo que estos entrañan para su empresa, y dar prioridad a cómo y dónde usar controles de acceso y mecanismos de ocultación, como el cifrado a nivel de archivo con controles de acceso granular y la tokenización con enmascaramiento dinámico de datos. Esto permite proteger los datos dificultando que usuarios no autorizados accedan a ellos y dejándolos ilegibles e inútiles en caso de robo o filtración.

Actualmente, el cifrado es uno de los métodos de seguridad de datos más populares y eficaces que utilizan las organizaciones. El cifrado de datos transforma los datos a otro formato (texto cifrado), de manera que solo los usuarios autorizados pueden acceder a los datos como texto legible. Mientras el cifrado transforma los datos con un algoritmo específico, la tokenización protege los datos sensibles sustituyendo los datos no sensibles. La tokenización crea una forma tokenizada irreconocible de los datos que mantiene el formato origen. Estos datos tokenizados también se pueden almacenar con el mismo tamaño y formato que los originales. De esta forma, los datos tokenizados no requieren cambios en los esquemas o procesos de la base de datos. Si los datos almacenados no tienen este tipo de estructura (por ejemplo, archivos de texto, PDF, MP3, etc.), la tokenización no es la forma ideal de ocultación. En este caso, sería apropiado un cifrado a nivel de archivo-sistema. Este cambiaría el bloque original de datos por una versión encriptada de los datos.

Al decidir qué solución de cifrado de datos puede satisfacer mejor con sus requisitos, hay varias cuestiones a tener en cuenta. A un alto nivel, los tipos de cifrado de datos se pueden clasificar en función de dónde se usan en la pila tecnológica. Existen cuatro niveles en la pila tecnológica en los que normalmente se usa cifrado de datos: disco, sistema de archivos, base de datos y aplicación. En general, cuanto más abajo se emplee el cifrado en la pila, más fácil y menos intrusiva será la implementación. Sin embargo, el número y los tipos de amenazas que estos cifrados de datos pueden abordar son reducidos. Por otro lado, al usar cifrado en partes más altas de la pila, las empresas pueden disfrutar normalmente de niveles más altos de seguridad y mitigar más amenazas.

La seguridad aumenta pero también lo hace la complejidad del desarrollo al realizar cambios en las partes altas de la pila



3. Controlar las claves de cifrado

La seguridad de los procesos de cifrado depende de la seguridad de las claves usadas para cifrar los datos. Si las claves usadas para encriptar o tokenizar los datos son robadas junto con los datos cifrados o tokenizados, estos ya no son seguros puesto que se pueden descifrar y hacer legibles. Para que el cifrado o la tokenización protejan con éxito sus datos sensibles, las claves criptográficas deben estar protegidas, gestionadas y controladas por su empresa, y no por un tercero o un proveedor en la nube.

Con el uso de cada vez más soluciones de cifrado aislado, las empresas comienzan a gestionar políticas inconsistentes, distintos niveles de protección y mayores costes. La solución más simple a este enredo es la transición a un modelo centralizado de gestión de claves. La gestión de las claves de cifrado conlleva administrar el ciclo de vida completo de estas y protegerlas frente a su pérdida o uso indebido. Las claves tienen un ciclo de vida: se crean, viven vidas útiles y se retiran. La gestión del ciclo de vida de las claves incluye: generar, utilizar, almacenar, distribuir, archivar y borrar las claves. Algunos de los beneficios de una gestión centralizada de claves son:

- Gestión unificada de claves y políticas de cifrado
- Revocación de claves en todo el sistema
- Reducción del riesgo de error humano a la hora de ajustar permisos administrativos y de usuario
- Alta disponibilidad y escalabilidad
- Validación FIPS 140-2 segura
- Ahorro de costes con la automatización
- Datos de auditorías consolidados
- Copias de seguridad y recuperaciones simplificadas
- Seguridad mejorada con separación exhaustiva de funciones

Gestiones sus claves de cifrado de manera centralizada

Beneficios de una seguridad eficiente centrada en los datos

Con una solución de seguridad eficiente y centrada en los datos, podrá lidiar con los desafíos de seguridad resultantes de la proliferación de los datos y la creación de reglamentos de privacidad a nivel regional y mundial, así como preparar a su empresa para un futuro más seguro.

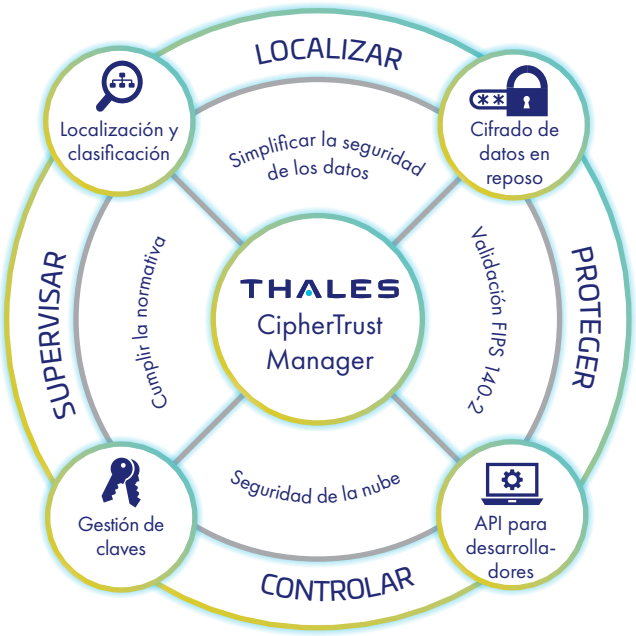
Una solución de seguridad centrada en los datos implementada de forma correcta:

- Ayuda a las empresas a mitigar riesgos y reducir costes. Las empresas pueden reducir costes empleando la infraestructura existente a una escala global, reduciendo los procesos manuales que pueden ser intensivos, repetitivos y propensos a errores, y garantizando su inversión en el futuro mediante la adopción de nuevas tecnologías.
- Ofrece una visión exhaustiva y continua de todos los datos y facilita la gestión de las políticas de seguridad y del control.
- Ayuda a las empresas a conocer sus datos y sus riesgos, así como a dar prioridad a la mitigación.
- Protege los datos para poder transmitirlos entre diversos entornos in situ y de nube, al tiempo que se mantiene su nivel de protección.
- Garantiza que los datos quedan protegidos frente a usuarios maliciosos y amenazas avanzadas continuas, que intentan robar información sensible.
- Reduce las sanciones y ayuda a las empresas a cumplir los reglamentos gubernamentales, empresariales y sectoriales. Las empresas pueden controlar las infracciones y aplicar políticas y reglas de seguridad, al tiempo que crean informes automatizados y auditan procedimientos de seguridad.
- Crea una posición jurídica defendible frente a una brecha de datos o a un problema de auditoría.

¿Cómo puede ayudarle Thales a implementar una estrategia de seguridad de tres puntos?

Thales es líder mundial en protección de datos. Ofrecemos todo lo que una empresa necesita para localizar, proteger y gestionar sus datos, identidades y propiedad intelectual: localización y clasificación de datos, encriptado, gestión avanzada de claves, tokenización, autenticación y gestión de acceso. CipherTrust Data Security Platform de Thales unifica la localización, la clasificación, la protección de datos y unos controles de acceso granular sin precedentes mediante una gestión centralizada de las claves, todo ello desde una única plataforma. Esto se traduce en menos recursos dedicados a las operaciones de seguridad de datos, controles de cumplimiento omnipresentes y una reducción significativa del riesgo en toda su empresa.

CipherTrust Data Security Platform



Capacidades clave de CipherTrust Data Security Platform

- Localización y clasificación de datos
  - Análisis de riesgos con visualización de los datos
- Técnicas de protección de datos
  - Cifrado transparente para archivos, bases de datos, macrodatos y contenedores
  - Protección de datos de aplicaciones
  - Tokenización con enmascaramiento dinámico de datos
  - Cifrado que mantiene el formato
  - Enmascaramiento de datos estáticos
  - Controles de acceso a usuarios con privilegios
- Gestión centralizada de claves de empresas
  - Cumplimiento FIPS 140-2
  - Gestión de claves multi-cloud
  - Ecosistema de socios para integraciones KMIP sin igual
  - Gestión de claves de cifrado de bases de datos (Oracle TDE, macrodatos, MS SQL, SQL Server Always Encrypted, etc.)
- Supervisión y elaboración de informes
- Consola de gestión centralizada

Beneficios de CipherTrust Data Security Platform

Simplificar la seguridad de los datos

Localice, proteja y controle los datos sensibles en cualquier lugar gracias a la protección de datos unificada de última generación. CipherTrust Data Security Platform simplifica la gestión de seguridad de los datos con una consola de gestión centralizada en un "panel único" que ofrece a las empresas herramientas potentes destinadas a localizar y clasificar datos sensibles, combatir amenazas externas, defenderse de abusos internos y establecer controles continuos, incluso cuando sus datos se almacenan en la nube o en cualquier otra infraestructura de un proveedor externo. Las empresas podrán detectar y solucionar estos puntos ciegos de privacidad, dar prioridad a la protección y fundamentar sus decisiones relativas a mandatos de privacidad y seguridad antes de emprender una transformación digital.

Reducir el tiempo necesario para lograr el cumplimiento normativo

Los organismos reguladores y los auditores requieren que las empresas controlen los datos normativos y sensibles, y cuenten con informes probatorios. Las funciones de CipherTrust Data Security Platform (como la localización y clasificación de datos, el cifrado, los controles de acceso, los registros de auditoría, la tokenización y la gestión de claves) contribuyen a dar respuesta a los requisitos ampliados en materia de seguridad y privacidad de los datos. Estos controles se pueden añadir con rapidez a nuevas implementaciones o adaptar a los cambios en los requisitos de cumplimiento. La naturaleza centralizada y ampliable de esta plataforma permite que se añadan con rapidez nuevos controles mediante la incorporación de licencias y la implementación de los conectores necesarios para adaptarse a nuevos requisitos de protección de datos.

Migraciones seguras a la nube

CipherTrust Data Security Platform ofrece soluciones de cifrado avanzado y de gestión centralizada de claves que permiten que las empresas almacenen con seguridad los datos sensibles en la nube. La plataforma ofrece soluciones avanzadas de tipo "traiga su propio cifrado" (Bring Your Own Encryption o BYOE) multinube para evitar que el cifrado dependa de un proveedor de la nube y garantizar la movilidad de los datos para protegerlo con múltiples proveedores y con una gestión independiente y centralizada de claves de cifrado. Las empresas que no puedan utilizar su propio cifrado pueden seguir las mejores prácticas del sector y gestionar sus claves de forma externa usando CipherTrust Cloud Key Manager. CipherTrust Cloud Key Manager acepta escenarios de tipo "traiga su propia clave" (Bring Your Own Key o BYOK) en múltiples infraestructuras de nube y aplicaciones SaaS. CipherTrust Data Security Platform emplea las medidas de protección más potentes para proteger los datos sensibles y las aplicaciones en la nube de las empresas, ayudándolas a cumplir los requisitos de cumplimiento y a controlar más sus datos, con independencia de dónde se crean, utilizan o almacenan.

Reducción de los costes totales de propiedad

CipherTrust Data Security Platform puede reducir los costes totales de propiedad en empresas de todos los tamaños simplificando la seguridad de los datos, reduciendo los tiempos para alcanzar su cumplimiento, y ofreciendo seguridad y control multinube. La plataforma, construida sobre una infraestructura ampliable, permite que sus departamentos de TI y seguridad localicen, clasifiquen y protejan los datos en reposo de su empresa de manera uniforme y repetible. Usar un enfoque tradicional puede requerir productos dedicados y caros que pueden necesitar una mayor integración y más personal para gestionarlos, invalidando cualquier ahorro potencial. La amplia gama de productos disponibles en CipherTrust Data Security Platform se puede usar individualmente o en combinación, y preparan a su empresa frente a futuros desafíos en materia de seguridad o cumplimiento normativo con el menor coste total de propiedad. Al integrar localización de datos, clasificación, análisis de riesgo, protección de datos e informes desde una única plataforma, la solución CipherTrust libera de carga al personal de TI y libera presupuesto para tareas más estratégicas, al tiempo que permite adoptar una actitud abierta y tener la libertad de colaboración que las empresas actuales necesitan sin poner en riesgo la seguridad.

Resumen

Los ataques a los datos se están volviendo más sofisticados porque estos datos son cada vez más valiosos, por lo que las empresas deben proteger su información más sensible y defender su reputación. La seguridad centrada en los datos es el único enfoque que aporta a la ciberseguridad actual tanto cumplimiento normativo como protección de calidad. Las estrategias efectivas de seguridad centrada en los datos basadas en los tres pilares de localización y clasificación de datos, protección de datos y gestión centralizada de claves de cifrado permiten que las empresas extraigan valor de forma segura de los datos sensibles y adopten de manera segura tecnologías de transformación digital.

Con soluciones centradas en los datos como Thales, puede proteger de forma eficiente y económica los datos sensibles estructurados y no estructurados en su empresa.

THALES

Póngase en contacto con nosotros

Para conocer la ubicación de las oficinas y nuestros datos de contacto, visite cpl.thalesgroup.com/es/contact-us

> cpl.thalesgroup.com <