Superar los desafíos de la seguridad de los datos en un mundo híbrido multinube

Proteja sus datos dondequiera que residan con la plataforma de protección de datos IBM Security Guardium

IBM **Security**

IBM

Contenido

Desplegar en un entorno híbrido multinube

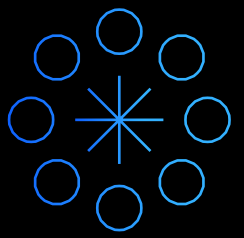
Seamos realistas, la computación en la nube está evolucionando a un ritmo rápido. Hoy en día, existe una variedad de opciones para mover aplicaciones y datos a la nube que incluye varios modelos de despliegue, desde tipos de servicios de nube pública y privada hasta híbrida.

Como parte de una estrategia digital más amplia, las organizaciones buscan formas de utilizar múltiples nubes. Con un enfoque multinube, las empresas pueden evitar el bloqueo de proveedores y aprovechar las mejores tecnologías, como la inteligencia artificial (IA) y blockchain. Los beneficios comerciales son claros: flexibilidad y agilidad mejoradas, costos más bajos y un tiempo de comercialización más rápido.

Según una encuesta del IBM Institute for Business Value a 1.106 ejecutivos de negocios y tecnología, para el 2021, el 85 % de las organizaciones ya estarán operando entornos multinube. El 98 % planea usar múltiples nubes híbridas para 2021. Sin embargo, solo el 41 % tiene una estrategia de gestión de multinube.[1]

Cuando se trata de elegir soluciones en la nube, hay una gran cantidad de opciones disponibles. Resulta útil observar las diferencias entre los distintos tipos de despliegue en la nube y modelos de servicios en la nube.

85 %
de las organizaciones ya están operando en entornos multinube.[1]



98 %
de las organizaciones planean usar múltiples nubes híbridas para 2021.[1]

Comprender los modelos de despliegue en la nube

Durante la última década, la computación en la nube ha madurado de varias maneras y se ha convertido en una herramienta para la transformación digital en todo el mundo. Generalmente, las nubes toman uno de los tres modelos de despliegue: público, privado o híbrido.

Nube pública
Una nube pública es aquella en la que los servicios se prestan a través de una internet pública. El proveedor de la nube posee, administra y mantiene completamente la infraestructura y la alquila a los clientes en función del uso o la suscripción periódica, por ejemplo, Amazon Web Services (AWS) o Microsoft Azure.

Nube privada
En un modelo de nube privada, la infraestructura de nube y los recursos se despliegan on premises para una sola organización, ya sea administrada internamente o por un tercero.

Con las nubes privadas, las organizaciones controlan todo el paquete de software, así como la plataforma subyacente, desde la infraestructura de hardware hasta las herramientas de medición.

Nube híbrida
Ofrece lo mejor de ambos mundos. Una infraestructura de nube híbrida conecta la nube privada de una empresa y la nube pública de terceros en una única infraestructura para que la empresa ejecute sus aplicaciones y cargas de trabajo.

Con el modelo de nube híbrida, las organizaciones pueden ejecutar cargas de trabajo confidenciales y altamente reguladas en una infraestructura de nube privada y ejecutar las cargas de trabajo temporales y menos confidenciales en la nube pública. Sin embargo, migrar aplicaciones y datos a la nube, más allá de los firewalls, los expone a riesgos.

Ya sea que sus datos se encuentren en una nube privada o en un entorno híbrido, los controles de seguridad y protección de datos deben estar implementados para proteger los datos y cumplir con los requisitos de conformidad del gobierno y sector.

Se estima que el mercado de la nube híbrida representa una **oportunidad de 1,2 billones de dólares**.[2]

Pero persisten las preocupaciones sobre la conformidad y protección de datos.

El costo de la filtración de datos está aumentando.

En promedio, las empresas tardan **279 días** en detectar y contener una filtración de datos.[3]

Tipos de modelos de servicios en la nube

La seguridad de los datos difiere según el modelo de servicio en la nube que se utilice. Hay cuatro categorías principales de modelos de servicios en la nube: infraestructura como servicio (IaaS), plataforma como servicio (PaaS), software como servicio (SaaS) y base de datos como servicio (DBaaS), que es una opción de PaaS.

IaaS permite a las organizaciones mantener sus plataformas de software físico y middleware existentes, y aplicaciones comerciales en la infraestructura proporcionada y administrada por el proveedor de servicios. Las organizaciones se benefician de este enfoque cuando quieren aprovechar rápidamente la nube mientras minimizan el impacto y utilizan las inversiones existentes.

PaaS permite a las empresas utilizar la infraestructura, así como el middleware o software proporcionado y administrado por el proveedor de servicios. Esta flexibilidad elimina una carga significativa para una empresa desde una perspectiva de TI y le permite concentrarse en desarrollar aplicaciones comerciales innovadoras.

Las soluciones DBaaS son entornos de base de datos alojados y totalmente gestionados por un proveedor de nube. Por ejemplo, una empresa puede suscribirse a Amazon RDS para MySQL o Microsoft Azure SQL Database.

SaaS es un modelo de servicio que subcontrata toda la TI y permite a las organizaciones centrarse más en sus principales puntos fuertes en lugar de gastar tiempo e inversión en tecnología. Ofrece SaaS a los usuarios finales. En este modelo de servicio en la nube, un proveedor de servicios aloja aplicaciones y las pone a disposición de las organizaciones.

Con cada paso, desde IaaS a PaaS, a SaaS y a DBaaS, las organizaciones renuncian a cierto nivel de control sobre los sistemas que almacenan, administran, distribuyen y protegen sus datos confidenciales. Este aumento de la confianza depositada en terceros también presenta un aumento del riesgo para la seguridad de los datos.

Independientemente de la arquitectura elegida, en última instancia, es responsabilidad de su organización garantizar que existan medidas de seguridad de datos adecuadas en todos los entornos.

Modelos de servicios en la nube: diferencias clave

IaaS	**PaaS**	**SaaS**	**DBaaS**
Mantiene un control completo de la gestión de la infraestructura	Permite la subcontratación de infraestructura, mantenimiento de software y middleware	Evita gastos de capital en software	Evita gastos de capital en infraestructura y hardware de base de datos
Es independiente de la plataforma	Permite que el personal de TI tenga tiempo para concentrarse en el desarrollo de aplicaciones	Entrega la gestión completa al proveedor de servicios	Entrega la gestión completa al proveedor de servicios
Ofrece un modelo de precios de pago por uso	Carece de control completo sobre la infraestructura de TI	Carece de control sobre los datos y la seguridad	Reduce el control sobre los datos y la seguridad

Desafíos de seguridad de datos para su entornode nube

Lo más probable es que ya esté en su trayectoria hacia la nube.

Si su organización es como la gran cantidad de empresas, sus datos confidenciales residen en ubicaciones que no puede controlar y son administrados por terceros que pueden tener acceso sin restricciones.

La investigación del Instituto Ponemon ha descubierto que las amenazas internas están aumentando significativamente en frecuencia y costo. Según las conclusiones del instituto, "el costo global promedio de las amenazas internas aumentó en un 31 por ciento en dos años alcanzado USD 11,45 millones y la frecuencia de incidentes aumentó en un 47 por ciento en el mismo período de tiempo". [4] Las organizaciones encuestadas tenían un personal global de 1.000 empleados o más.

USD 11,45 millones

es el costo promedio global de una amenaza interna.[4]

Determinar la mejor forma de almacenar los datos es una de las decisiones más importantes que puede tomar una organización. La nube es especialmente adecuada para el almacenamiento de datos a largo plazo a nivel empresarial que permite a las organizaciones beneficiarse de enormes economías de escala, lo que se traduce en menores gastos. Y esta característica a menudo hace que los centros de datos basados en la nube sean un lugar más inteligente para almacenar información crítica para el negocio que una pila de servidores en el pasillo.

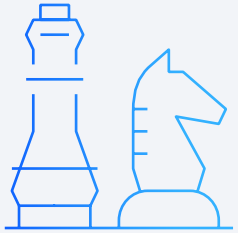
Incluso cuando los gastos de adquisición de almacenamiento disminuyen, pueden ser costosos a largo plazo, debido al mayor uso comercial y la cantidad de personal que administra los sistemas de almacenamiento. Sin embargo, si bien poner el almacenamiento de datos en manos de proveedores de servicios externos puede ayudar a ahorrar dinero y tiempo, también puede plantear serios desafíos de seguridad y crear nuevos tipos de riesgo.

Los despliegues en la nube funcionan con un modelo de responsabilidad compartida entre el consumidor y el proveedor de la nube. En el caso de un modelo IaaS, el consumidor de la nube tiene espacio para implementar medidas de seguridad de datos muy parecidas a las que normalmente desplegaría on premises y ejercer controles más estrictos.

Por otro lado, para los servicios SaaS, los consumidores de la nube en su mayor parte deben confiar en la visibilidad proporcionada por el proveedor de la nube que, básicamente, limita su capacidad para ejercer controles más detallados.

Es importante comprender que cualquiera que sea su modelo de despliegue o tipo de servicio en la nube, la seguridad de los datos debe ser una prioridad. Lo que es más preocupante es que sus datos confidenciales ahora se encuentran en muchos lugares, tanto dentro como fuera de su empresa. Y sus controles de seguridad deben estar junto con sus datos.

Determinar la mejor forma de almacenar los datos es una de las decisiones más importantes que puede tomar una organización.



Mantenga sus datos confidenciales seguros esencialmente en todas partes

¿Quién tiene acceso a los datos confidenciales en su organización? ¿Qué tan seguro está de que su personal o que los usuarios con privilegios no han accedido de manera inapropiada a los datos confidenciales de los clientes?

En otras palabras, no puede proteger lo que no sabe. Es posible que simplemente bloquear el acceso a la red no sea la solución. Después de todo, los colaboradores confían en esta red para acceder y compartir datos. Este acceso significa que la efectividad de la seguridad de sus datos está en gran parte en manos de sus colaboradores, algunos de los cuales ya no trabajan directamente para su empresa, pero aún mantienen el acceso. El descubrimiento, la clasificación y el monitoreo automatizados de sus datos confidenciales en todas las plataformas es crucial para hacer cumplir políticas de seguridad efectivas y en contexto, así como para ayudar a abordar el cumplimiento de las normas.

Generalmente, en entornos de nube, los proveedores de servicios en la nube (CSP) tienen la capacidad de acceder a sus datos confidenciales, lo que convierte a los CSP en una nueva frontera en las amenazas internas. Además, los ciberdelincuentes saben que los CSP almacenan grandes cantidades de datos importantes, lo que convierte a estos entornos en los principales objetivos de los ataques. Para contrarrestar estas amenazas, se deben utilizar sofisticadas herramientas basadas en análisis que verifiquen el acceso normal y autorizado.

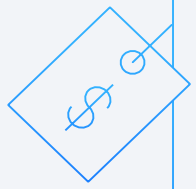
Más información →

95 % más alto

costo promedio de filtración de datos en organizaciones sin automatización de seguridad en 2019.[3]

USD 5,16 millones

fue el costo **sin automatización**.[3]



USD 2,65 millones

fue el costo **con automatización completamente desplegada**.[3]

Considere la encriptación para el almacenamiento en la nube

Con el almacenamiento en la nube, sus datos pueden moverse a un lugar diferente, en un medio diferente, al de su ubicación actual. Lo mismo ocurre con la virtualización. No solo los datos basados en la nube, sino también los recursos informáticos basados en la nube pueden cambiar rápidamente en términos de ubicación y bases de hardware. La naturaleza cambiante de la nube significa que su enfoque de seguridad debe abordar diferentes tipos de almacenamiento basado en la nube. Su enfoque también debe tener en cuenta las copias, ya sean las copias de seguridad a largo plazo o las copias temporales creadas durante la migración de datos.

Para abordar estos desafíos, debe desplegar soluciones multiplataforma y emplear una encriptación sólida para ayudar a garantizar que sus datos no puedan ser utilizados por personas no autorizadas en caso de que se manejen incorrectamente.

Incluso si sus datos no se almacenan principalmente en la nube, tanto la forma en que los datos salen y regresan a su empresa como la ruta que toman los datos son preocupaciones importantes. Los datos son tan seguros como el eslabón más débil de la cadena de procesamiento. Por lo tanto, incluso si los datos se mantienen principalmente encriptados y detrás de un firewall presencial, si se transmiten a una copia de seguridad externa o para procesamiento de terceros, los mismos pueden quedar expuestos.

La detección de malware o el análisis de comportamiento que está diseñado para detectar actividades sospechosas puede ayudar a prevenir una filtración de datos interna o externa y cumple funciones valiosas por derecho propio.

Sin embargo, la encriptación ayuda a proteger los datos dondequiera que estén, ya sea en reposo o en movimiento.

La seguridad eficaz del almacenamiento en la nube es más que simplemente realizar una copia de seguridad de los archivos. Se trata de proteger sus datos con medidas preventivas contra el uso no autorizado.

Mejores prácticas de seguridad de almacenamiento en la nube

- Bloqueo de acceso a puertos no aprobados
- Evaluación proactiva de vulnerabilidades
- Escaneo continuo en busca de acceso a datos sospechosos
- Cifrar sus datos confidenciales, realizar un buen mantenimiento de las claves de encriptación y almacenar las claves on premises en una red separada de los datos encriptados
- Uso de una plataforma unificada que integra la información de seguridad en entornos híbridos multinube.

Desafíos organizativos para su entorno de nube

Con el crecimiento de los datos a un ritmo exponencial, las organizaciones se enfrentan a una lista cada vez mayor de leyes y regulaciones de protección de datos. ¿Qué está en riesgo? La información personal de los clientes, como la información de la tarjeta de pago, direcciones, números de teléfono y números de seguro social, por nombrar algunos. Para tener una solución de seguridad eficaz, las organizaciones deben adoptar un enfoque basado en riesgos para proteger los datos de los clientes en todos los entornos.

A continuación, cinco desafíos que podrían afectar la estrategia de seguridad de su organización:

- Asegurar la conformidad
- Asegurar la privacidad
- Mejorar la productividad
- Supervisar los controles de acceso
- Abordar las vulnerabilidades

La plataforma de protección de datos IBM Security™ Guardium® está diseñada para ayudar a su organización a enfrentar estos desafíos con capacidades de protección de datos más inteligentes en todos los entornos.

Manténgase al día con la conformidad

La realidad de la computación y almacenamiento basados en la nube significa que sus datos confidenciales en sistemas de multinube híbrida podrían estar sujetos a las regulaciones gubernamentales y del sector.

Si sus datos están en una nube pública, debe saber cómo planea el CSP proteger sus datos confidenciales. Por ejemplo, de acuerdo con el Reglamento general de protección de datos (RGPD) de la Unión Europea (UE), la información que revela el origen racial o étnico de una persona se considera confidencial y podría estar sujeta a condiciones de procesamiento específicas.[5] Estos requisitos se aplican incluso a empresas ubicadas en otras regiones del mundo que poseen y acceden a los datos personales de los residentes de la UE.

Comprender dónde residen los datos de una organización, de qué tipo de información se componen y cómo se relacionan en toda la empresa puede ayudar a los líderes empresariales a definir las políticas adecuadas para proteger y encriptar sus datos.

Además, también podría ayudar a demostrar el cumplimiento de las normas, como:

- Sarbanes-Oxley (SOX)
- Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)
- Protocolo de automatización de contenido de seguridad (SCAP)
- Ley federal de gestión de seguridad de la información (FISMA)
- Ley de tecnología de la información sanitaria para la salud económica y clínica (HITECH)
- Ley de portabilidad y responsabilidad del seguro médico (HIPAA)
- Ley de privacidad del consumidor de California (CCPA).

Las soluciones IBM Security Guardium están diseñadas para monitorear y auditar la actividad de datos en bases de datos, archivos, despliegues en la nube, entornos de mainframe, contenedores y repositorios de big data. El proceso se optimiza con la automatización, lo que reduce los costos y el tiempo de cumplimiento de los requisitos.

Más información →

"Guardium tiene una gran cantidad de funciones e informes incorporados ahora, centrándose en cosas como RGPD. Por lo tanto, podemos aprovechar esa funcionalidad incorporada para darnos un comienzo más rápido, sin tener que construir cosas desde cero".

Una organización de seguros especialista senior en gobernanza, en un estudio de Forrester del impacto económico total (TEI).[6]

Lea el estudio TEI de Guardium →

Aborde los problemas de privacidad

Con la multiplicación de smartphones, tablets y relojes inteligentes, administrar la privacidad y los controles de acceso puede convertirse en una tarea difícil. Uno de los desafíos para los administradores de seguridad es garantizar que solo las personas con una razón comercial válida tengan acceso a la información personal. Por ejemplo, los médicos deben tener acceso a información confidencial, como datos de síntomas y pronóstico del paciente, mientras que un empleado de facturación solo necesita el número de seguro y la dirección de facturación del paciente.

Sus clientes esperan que usted considere su privacidad una prioridad. Empiece por desarrollar una política de privacidad, describiendo la información que recopila sobre sus clientes y lo que piensa hacer con ella.

IBM Security Guardium Insights proporciona a los equipos de seguridad opiniones y alertas basadas en riesgos, así como análisis avanzados basados en tecnología patentada de aprendizaje automático (ML) para ayudarlos a descubrir amenazas ocultas en grandes volúmenes de datos en entornos híbridos.

Más información →

Escuche a Kevin Baker, Director de seguridad de la información de Westfield, sobre los desafíos de privacidad de los datos que enfrenta su organización y su enfoque para abordarlos a través de la información y la automatización necesarias, mientras escala para respaldar la innovación con IBM Security Guardium Insights.

Ver video →

Mejore la productividad

Las políticas de seguridad y privacidad deben permitir y mejorar, no interferir con las operaciones comerciales. Las políticas deben integrarse en las operaciones diarias y funcionar sin problemas dentro y en todos los entornos (en entornos privados, públicos, on premises e híbridos) sin afectar su productividad. Por ejemplo, cuando se despliegan nubes privadas para facilitar las pruebas de aplicaciones, considere usar encriptación o tokenización para mitigar el riesgo de exponer esos datos confidenciales.

Las soluciones IBM® Guardium pueden ayudar a sus equipos de seguridad a monitorear la actividad de los usuarios y responder a las amenazas en tiempo real. Este proceso se simplifica con controles automatizados y centralizados, lo que reduce el tiempo dedicado a las investigaciones y permite que los administradores de bases de datos y especialistas en privacidad de datos tomen decisiones más informadas.

Según el Instituto Ponemon, las soluciones IBM Guardium pueden ayudar a que los equipos de seguridad de TI sean más eficientes.[7] Antes de desplegar la solución Guardium, un 61 % del tiempo de los equipos de seguridad de TI encuestados se dedicaba a identificar y solucionar problemas de seguridad de datos. Después del despliegue, el porcentaje promedio del tiempo dedicado a tales actividades fue del 40 %, una disminución del 42 %.

Antes del despliegue de la solución Guardium, un

61 %

del tiempo se dedicó anualmente a identificar y solucionar problemas de seguridad de datos.[7]

Después del despliegue de Guardium, el

40 %

del tiempo se dedicó anualmente a identificar y solucionar problemas de seguridad de datos.[7]

Supervise los controles de acceso

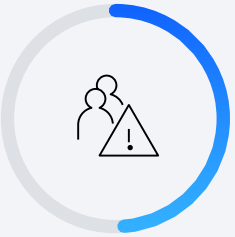
El ciclo de vida de una filtración de datos se está alargando, afirma un estudio del Instituto Ponemon. De hecho, la investigación del instituto descubrió que el 49 % de las filtraciones de datos estudiadas se debieron a errores humanos, incluidas fallas del sistema y "personal interno inadvertido" que pueden verse comprometidas por ataques de phishing o que sus dispositivos se infecten, se pierdan o se los roben". [3]

Los ciberdelincuentes pueden variar desde individuos hasta hackers patrocinados por el estado con intenciones disruptivas. Pueden ser científicos informáticos deshonestos que intentan mostrarse o hacer una declaración política, o pueden ser intrusos organizados y difíciles. Pueden ser empleados descontentos o incluso hackers patrocinados por un estado extranjero que quieren recopilar información de inteligencia de organizaciones gubernamentales.

Las filtraciones también pueden ser accidentales, como el robo de credenciales, errores humanos o configuraciones incorrectas, por ejemplo, cuando los permisos se configuran incorrectamente en una tabla de base de datos o cuando las credenciales de un colaborador se ven comprometidas. Una forma de evitar este problema es otorgar a los usuarios finales, tanto con privilegios como a los comunes, los "menores privilegios posibles" para minimizar errores y el abuso de privilegios. Las organizaciones deben proteger los datos de ataques tanto internos como externos en entornos de nube físicos, virtuales y privados.

Las defensas perimetrales son importantes, pero lo más importante es proteger los datos confidenciales dondequiera que residan. De esta manera, si se viola el perímetro, los datos confidenciales permanecerán seguros e inutilizables para un ladrón. Los perímetros en declive hacen que la protección de los datos en su origen sea crucial.

Una solución de seguridad de datos segmentada puede ayudar a los administradores a examinar los modelos de acceso a los datos y los comportamientos de los usuarios beneficiados para comprender lo que sucede dentro de su entorno de nube privada. El desafío es implementar soluciones de seguridad sin obstaculizar la capacidad de la empresa para crecer y adaptarse, brindando, por lo tanto, acceso y protecciones de datos adecuados para garantizar que los datos se administren según la necesidad, donde sea que residan.



49 %

Casi la mitad de las filtraciones de datos se debieron a filtraciones inadvertidas por errores humanos y fallas del sistema.[3]

Aborde las evaluaciones de vulnerabilidad

Cuando se trata de defenderse de los atacantes, lo que funcionó en el pasado puede que no funcione hoy. Muchas organizaciones dependen de diversas tecnologías de seguridad que podrían estar operando en silos. Según un estudio de Forrester Consulting, en promedio, las organizaciones administran 25 productos o servicios de seguridad diferentes de 13 proveedores.[8]

El número de vulnerabilidades del repositorio de datos es enorme y los delincuentes pueden aprovechar incluso la ventana de oportunidad más pequeña. Algunas de estas vulnerabilidades incluyen parches faltantes, configuraciones incorrectas y configuraciones predeterminadas del sistema que podrían dejar brechas que los ciberdelincuentes esperan. Esta complejidad es cada vez más difícil de controlar y administrar a medida que los repositorios de datos se virtualizan.

Además, las empresas que se trasladan a la nube a menudo tienen dificultades para hacer evolucionar sus prácticas de seguridad de datos de una manera que les permita proteger los datos confidenciales mientras disfrutan de los beneficios de la nube. Cuantos más servicios en la nube utilice su organización, más control necesitará para administrar los diferentes entornos.

Piense en el uso de herramientas propias que existen actualmente para la seguridad de los datos. ¿Funcionarán mañana las herramientas propias que utiliza hoy? Por ejemplo, con las rutinas de enmascaramiento de datos o los scripts de monitoreo de la actividad de la base de datos, ¿se requerirán cambios de codificación para que funcionen en una base de datos virtual? Es probable que se requiera una inversión significativa para actualizar estas soluciones propias. En resumen, las organizaciones necesitan un enfoque de seguridad centrado en los datos en el que las estrategias de seguridad estén integradas en la estructura de sus entornos híbridos multinube.

A diferencia de una solución puntual, IBM Security Guardium Insights admite la integración heterogénea con otras soluciones de seguridad líderes del sector. La protección de datos de Guardium también proporciona la mejor integración de su clase con las soluciones de seguridad de IBM, como IBM QRadar® SIEM para la protección proactiva de datos.

Más información →

"Guardium toma los diferentes sistemas de gestión de bases de datos y los consolida en una sola herramienta en lugar de que necesitemos usar sistemas separados para Oracle, para el servidor SQL y similares. Podemos ver toda la información en una sola ventana".

Vicepresidente de gestión de seguridad cibernética, servicios fi, estudio TEI[6]

Lea el estudio TEI de Guardium →

Un enfoque de seguridad de datos más inteligente

A medida que la nube madura y se escala rápidamente, debemos darnos cuenta de que **la seguridad efectiva de los datos no es una carrera corta, sino un maratón**—un proceso constante que continúa durante la vida de los datos.

Si bien no existe un enfoque único para la seguridad de los datos, es fundamental que las organizaciones busquen centralizar la seguridad de los datos y los controles de protección que puedan funcionar bien juntos. Este enfoque puede ayudar a los equipos de seguridad a mejorar la visibilidad y el control de los datos en la empresa y en la nube.

¿Qué constituye una estrategia eficaz de seguridad en la nube?

Descubra y clasifique sus datos confidenciales estructurados y no estructurados, online y offline, independientemente de dónde residan y clasifique la IP confidencial y los datos sujetos a regulaciones, como PCI, HIPAA, Ley general de protección de datos (LGPD), CCPA y RGPD.

Proteja las fuentes de datos confidenciales basándose en un conocimiento profundo de los datos que tiene, quién tiene y debería tener acceso a ellos. Los controles de protección deben adaptarse a los diferentes tipos de datos y perfiles de usuario dentro de su entorno. Las políticas de acceso flexibles, la encriptación de datos y la gestión de claves de encriptación deberían ayudar a mantener protegidos sus datos confidenciales.

Responda a amenazas en tiempo real. Una vez que se le alerta sobre posibles vulnerabilidades y riesgos, necesita la capacidad de responder rápidamente. Las acciones pueden incluir bloquear y poner en cuarentena una actividad sospechosa, suspender o cerrar sesiones de usuario o acceso a datos y enviar alertas procesables a los sistemas de operaciones y seguridad de TI.

Evalúe el riesgo con información y análisis contextuales. ¿Cómo se protegen sus datos críticos? ¿Los derechos de acceso están de acuerdo con los requisitos reglamentarios y del sector? ¿Son los datos vulnerables al acceso no autorizado y los riesgos de seguridad debido a la falta de controles de protección?

Supervise el acceso a los datos y los modelos de uso para descubrir rápidamente actividades sospechosas. Una vez que se hayan implementado los controles adecuados, debe recibir una alerta rápida sobre actividades sospechosas y desviaciones de las políticas de acceso y uso de datos. También debe poder ver de forma centralizada la seguridad de sus datos y la posición de conformidad en varios entornos de datos sin depender de varias consolas inconexas.

Simplifique la conformidad y sus informes. Debe poder demostrar la seguridad y conformidad de los datos tanto a partes internas como externas y realizar las modificaciones adecuadas en función de los resultados. Demostrar la conformidad con los mandatos regulatorios a menudo requiere almacenar y generar informes sobre los datos de auditoría y la seguridad de los datos durante años. Los informes de conformidad y seguridad de los datos deben ser completos y tener en cuenta todo el entorno de datos.

Cifre datos en entornos híbridos multinube

Dado que ya no podemos confiar en el perímetro para proteger los datos confidenciales de una organización, es fundamental que los líderes empresariales actuales envuelvan los datos en protección.

IBM Security Guardium Data Encryption es un conjunto de soluciones modulares, integradas y altamente escalables de encriptación, tokenización, gestión de acceso y gestión de claves de encriptación que se puede desplegar esencialmente en todos los entornos. Estas soluciones codifican su información confidencial y proporcionan un control detallado sobre quién tiene la capacidad de decodificarla.

Más información →

La encriptación sólida es una respuesta común al desafío de proteger los datos confidenciales dondequiera que residan. Sin embargo, la encriptación plantea problemas complicados de portabilidad y garantía de acceso. Los datos son tan sólidos como la seguridad y confiabilidad de las claves que los protegen. ¿Cómo se hacen copias de seguridad de las claves? ¿Cómo pueden moverse los datos de manera transparente entre proveedores de nube, o compartirse entre el almacenamiento basado en la nube y el almacenamiento local?

IBM Security Guardium Key Lifecycle Manager puede ayudar a los clientes que necesitan una protección de datos más estricta. La solución ofrece almacenamiento sólido de claves y altamente seguro, servicio de claves y gestión del ciclo de vida de las claves para soluciones de almacenamiento de IBM y de otras marcas que utilizan el protocolo de interoperabilidad de gestión de claves de OASIS (KMIP). Con la gestión centralizada de las claves de encriptación, las organizaciones podrán cumplir con las normas, como PCI DSS, SOX y HIPAA.

Descubra más →

La plataforma IBM Security Guardium fue nombrada líder en Forrester Wave: Proveedores de portafolio de seguridad de datos, segundo trimestre de 2019. Según el informe, la plataforma Guardium es una "buena opción para los compradores que buscan reducir y gestionar de forma centralizada los riesgos de datos en entornos de bases de datos dispares".

Lea el informe →

Descubra un nuevo enfoque para la seguridad de los datos

En el centro de la protección de un entorno híbrido multinube, está la necesidad de que las organizaciones adopten soluciones que ofrezcan la máxima visibilidad y continuidad empresarial y ayuden a cumplir con la conformidad y confianza del cliente.

seguridad de los datos. Además, la solución es compatible con una amplia gama de entornos en la nube, incluidas nubes públicas y privadas, en entornos PaaS, IaaS y SaaS, para operaciones y seguridad continuas.

El Instituto Ponemon realizó una encuesta de organizaciones que utilizan la solución Guardium para monitorear y defender los datos y bases de datos de su empresa. La misma descubrió que el 86 % de los encuestados dijo que la capacidad de usar la solución Guardium para gestionar el riesgo de datos en entornos de TI complejos, como un ecosistema de nube híbrida o multinube, es muy valiosa. De manera similar, el aprendizaje automático y la automatización son un beneficio significativo en la gestión de riesgos de datos en toda la empresa.[7]

Con la solución Guardium, su equipo de seguridad puede elegir la arquitectura del sistema que mejor se adapte a su empresa. Por ejemplo, su equipo puede desplegar todos los componentes de Guardium en la nube, o elegir mantener algunos de esos componentes, como un administrador central, on premises. Esta flexibilidad permite a los clientes existentes extender fácilmente su estrategia de protección de datos a la nube sin afectar los despliegues existentes.

Más información →

Características clave de IBM Security Guardium:

Descubra y clasifique automáticamente datos confidenciales.

Encripte los datos en todos los entornos.

Identifique los datos en riesgo y obtenga recomendaciones de corrección.

Utilice información y análisis contextuales.

Simplifique los informes de seguridad y conformidad.

Obtenga una perspectiva empresarial sobre el riesgo de los datos.

Supervise el acceso y proteja los datos.

Conclusión

Dado el panorama de amenazas en evolución, las organizaciones deben adoptar un enfoque coherente y unificado para la seguridad de datos híbridos multinube. Puede considerar las siguientes preguntas:

- ¿Qué datos permanecen on premises?
- ¿Qué datos se trasladan a la nube?
- ¿Cómo se puede monitorear el acceso a los datos?
- ¿Qué tipos de vulnerabilidades deben considerarse?
- ¿Cómo podemos demostrar la conformidad con los requisitos normativos y de seguridad de los datos?

Al elegir las soluciones de protección y seguridad de datos, seleccione soluciones que sean escalables en distintas infraestructuras de TI, protegiendo los entornos físicos, virtuales y en la nube de ataques externos maliciosos, fraude, acceso no autorizado y filtraciones internas. Estas soluciones deben funcionar en un entorno de nube sin configuraciones complejas y costosas. Este enfoque proporcionará una plataforma eficiente para la seguridad de los datos y entrega de privacidad, lo que lo ayudará a administrar los costos al reducir los recursos y brindar mayor agilidad y flexibilidad.

El software Guardium proporciona una solución integral para infraestructuras físicas, virtuales y en la nube a través de controles de seguridad automatizados y centralizados en entornos heterogéneos. La solución ayuda a optimizar la conformidad, reduce el riesgo y es compatible con las principales plataformas en la nube, incluidas IBM Cloud®, Microsoft Azure y AWS, y opera en entornos Microsoft Windows, UNIX y Linux®.

¿Qué es lo que sigue?
Descubra cómo las soluciones de IBM Security Guardium pueden ayudarlo a adoptar un enfoque más inteligente e integrado para proteger los datos críticos en sus entornos híbridos multinube. Visite ibm.com/security/data-security/guardium

El estudio TEI de Forrester muestra estos beneficios comerciales clave habilitados por la plataforma IBM Security Guardium: [6]

343 % de ROI

USD 3,3 millones en beneficios generales

Recuperación en **<6 meses** en promedio

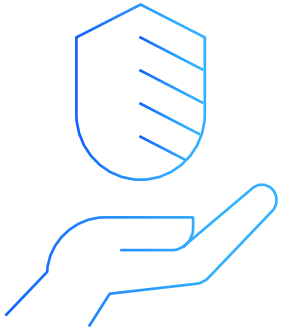
Lea más →

¿Por qué soluciones de IBM Security?

Las soluciones de IBM Security ofrecen uno de los portafolios más avanzados e integrados de productos y servicios de seguridad empresarial. El portafolio, respaldado por la investigación y el desarrollo del mundialmente reconocido IBM X-Force®, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger de manera integral a sus personas, infraestructuras, datos y aplicaciones. Ofrece soluciones para la gestión de identidades y de acceso, seguridad de bases de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de terminales, seguridad de red y más.

Estas soluciones permiten a las organizaciones gestionar riegos de forma efectiva e implementar seguridad integrada para dispositivos móviles, nubes, redes sociales y otras arquitecturas comerciales empresariales.

IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, monitoreando más de 60 mil millones de eventos de seguridad por día en más de 130 países y la corporación posee más de 3.700 patentes de seguridad.



IBM Corporation
New Orchard
Road Armonk, NY 10504

Producido en los Estados Unidos de América
en junio de 2020

Este documento se actualizó por última vez en la fecha de su publicación y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Los ejemplos de cliente y datos de rendimiento mencionados fueron presentados solamente para propósitos ilustrativos. Los resultados reales de rendimiento pueden variar dependiendo de configuraciones específicas y condiciones de operación. Es responsabilidad del usuario evaluar y verificar la operación de cualquier otro producto o programa con los productos y programas de IBM. LA INFORMACIÓN DE ESTE DOCUMENTO ES SUMINISTRADA "COMO ESTÁ" SIN NINGUNA GARANTÍA, EXPRESA O IMPLÍCITA, NO INCLUYE NINGUNA GARANTÍA DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO ESPECÍFICO Y NINGUNA GARANTÍA O CONDICIÓN DE NO INFRACCIÓN. Los productos de IBM están garantizados de conformidad con los términos y condiciones de los contratos en virtud de los cuales se suministran.

El cliente es responsable de asegurar la conformidad con las leyes y los reglamentos aplicables. IBM no proporciona asesoría legal, ni representa ni garantiza que sus servicios o productos aseguren que el cliente cumple con cualquier ley o regulación.

Declaración de buenas prácticas de seguridad: La seguridad de los sistemas de TI implica proteger los sistemas y la información mediante prevención, detección y respuesta al acceso indebido dentro y fuera de su empresa. El acceso inadecuado puede dar lugar a la modificación, destrucción, apropiación indebida o utilización indebida de la información, así como también a daños a sus sistemas o a la utilización indebida de éstos, incluso para su uso en ataques a otros. Ningún producto o sistema de TI deberá considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente eficaz en la prevención de la utilización o el acceso indebidos. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un enfoque de seguridad legal e integral, el cual necesariamente involucrará procedimientos operativos adicionales y puede requerir otros sistemas, productos o servicios para contar con el máximo de eficacia. IBM NO GARANTIZA QUE NINGÚN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE, O HAGA A SU EMPRESA INMUNE, A LA CONDUCTA MALINTENCIONADA O ILEGAL DE CUALQUIER TERCERO.

1 "Assembling your cloud orchestra." *IBM Institute for Business Value*, octubre de 2018. ibm.com/thought-leadership/institute-business-value/report/multicloud/#

2 Jim Comfort, "How a Hybrid Multicloud Strategy Can Overcome the Cloud Paradox." *IBM*, 5 de noviembre de 2019. ibm.com/blogs/think/2019/11/how-a-hybrid-multicloud-strategy-can-overcome-the-cloud-paradox/

3 "Cost of a Data Breach Report 2019." *IBM Security.* databreachcalculator.mybluemix.net/executive-summary

4 "2020 Cost of Insider Threats Global Report", *Ponemon Institute, ObserveIT*. observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf

5 "What personal data is considered sensitive?" *European Commission*. ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

6 "The Total Economic Impact Of IBM Security Guardium." *Forrester*, abril de 2018. ibm.com/downloads/cas/QA8XWPBA

7 "Ponemon Report: Client Insights on Data Protection with Guardium." *Ponemon Institute*, agosto de 2019. ibm.com/account/reg/us-en/signup?formid=urx-40683

8 "Complexity In Cybersecurity Report 2019." *Forrester Consulting*, mayo de 2019. ibm.com/downloads/cas/QK1YD49A

GWB3E8ZV