La nube segura para los datos:

6 beneficios básicos de una nube segura

Cambios en el abordaje de la seguridad en la nube

Si bien la seguridad siempre será tema de conversación en relación con la nube, la manera de abordarla está cambiando.

En un principio, las preocupaciones de los clientes giraban en torno a si la nube en sí era o no segura: ¿Podemos confiarle nuestros datos a la nube? ¿Migrar datos a la nube incrementará nuestra exposición a los riesgos?

Sin embargo, con el correr del tiempo, el abordaje cambió. Las preocupaciones ya no se relacionan con si la nube es segura o no, sino con cuál es la mejor manera de proteger los datos en la nube.

Los clientes quieren saber: ¿Qué tipo de controles se encuentran disponibles para poder saber quién obtiene acceso a mis datos y cuándo? ¿De qué manera puedo obtener acceso a los datos y auditarlos para saber si cumplo las normas correspondientes? ¿Cómo puedo proteger un entorno en la nube híbrida?

Los primeros líderes en realizar estas preguntas fueron pioneros en lo que resultó ser un cambio cultural y, al mismo tiempo, una actualización tecnológica. Hoy en día, un mayor número de organizaciones han percibido que, de una u otra manera, su futuro está vinculado con la nube y están buscando la mejor manera de proteger sus datos con el proveedor de nube correcto.

A medida que aumenta la confianza en la nube pública, también observamos un crecimiento en el volumen de aplicaciones que se ejecutan en infraestructuras compartidas. Ese fenómeno nos suministra un mayor número de diferentes casos de uso que revelan los beneficios y las prácticas recomendadas para una nube segura para los datos.

51%

El 51 por ciento de los gerentes de TI dijo que el nivel de seguridad de los datos es mejor en la nube que en sus centros de datos.

58%

El 58 por ciento dijo que la nube pública era la solución más segura, flexible y rentable para sus organizaciones.[1]

2020

El nivel de confianza es tan elevado que, según Gartner, para el 2020 se venderá más capacidad informática a través de la nube de la que se implementa en los centros de datos locales de los clientes.[2]

1 Encuesta sobre la nube pública de SADA Systems
2 Gartner, Predicts 2016: Cloud Computing to Drive Digital Business, diciembre de 2015

6 beneficios de la seguridad en la nube

Uno de los desafíos de migrar a la nube es lidiar con varias partes interesadas dentro de una organización con diferentes niveles de interés en relación con el proceso de adopción de la nube.

Conocer los beneficios únicos de una nube segura es el primer paso en pos de abordar las preocupaciones de los profesionales de las áreas de seguridad y conformidad de su organización.

El proveedor que logre demostrar estos seis beneficios puede ayudarlo a transformar el funcionamiento de su organización, lo que permite liberar recursos para que se enfoquen en el negocio principal. Además, todo esto se alcanza mientras su organización se hace más segura.

01

Herede controles de conformidad y seguridad sólidos

02

Ajuste su escala con niveles optimizados de visibilidad y control

03

Proteja su privacidad y sus datos

04

Encuentre soluciones y socios de seguridad fiables

05

Use la automatización para mejorar el nivel de seguridad y ahorrar tiempo

06

Mejore continuamente con características de seguridad innovadoras

01

Herede controles de conformidad y seguridad sólidos

Cuando elija un proveedor de nube, recuerde que heredará muchos de los controles de seguridad de este en sus propios programas de conformidad y certificación. Si son los correctos, pueden disminuir radicalmente los costos de sus estrategias de control de seguridad. Para asegurarse de seleccionar al proveedor correcto, busque validaciones de terceros: certificaciones y prácticas recomendadas sobre seguridad con reconocimiento internacional, además de certificaciones específicas del sector.

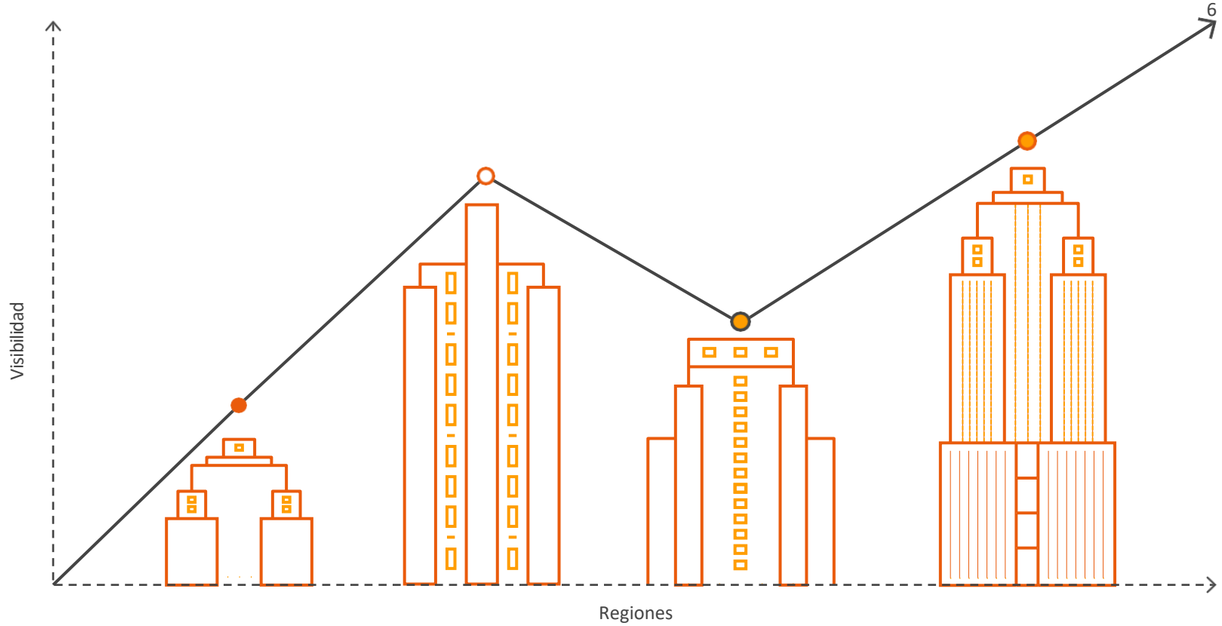
Ejemplos de estos controles son las certificaciones y las prácticas recomendadas de seguridad con reconocimiento internacional, como ISO 27001, ISO 27017 para seguridad en la nube, ISO 27018 para privacidad en la nube, y SOC 1, SOC 2 y SOC 3. El proveedor correcto también ofrecerá servicios para ayudarlo a cumplir con HIPAA o PCI-DSS. Además, contará con muchas certificaciones destinadas al sector público mediante FedRAMP y la SRG del DoD SRG en EE.UU., C5 en Alemania, IRAP en Australia y MTCS nivel 3 en Singapur.

"Un nivel de seguridad sólido en un entorno minorista es fundamental para nosotros debido a nuestra gran cantidad de operaciones minoristas. Mediante el uso de las prácticas recomendadas de seguridad de AWS, pudimos eliminar una gran cantidad de tareas de conformidad que anteriormente consumían mucho tiempo y dinero".

Brian Mercer, arquitecto de software sénior, Delaware North

02

Ajuste su escala con niveles optimizados de visibilidad y control



Los datos que almacena en la nube no están

ocultos ni fuera de control. Debe saber en todo momento dónde se encuentran y quién obtiene acceso a ellos. Esta información debe estar disponible casi en tiempo real independientemente de dónde se encuentre y sin importar en qué lugar del mundo estén almacenados sus datos. Imagínese si pudiera recibir información sobre su infraestructura y datos con una simple llamada de programación de software. No podría lograr este tipo de visibilidad con un centro de datos local.

Asegúrese de tener el control que necesita.

Para ello, busque características clave, como los controles de acceso e identidad pormenorizados combinados con servicios de monitoreo de actividades que detecten cambios de configuración y seguridad en todo su ecosistema.

Estos controles no solo le permitirán reducir los riesgos, sino también ajustar la escala de su organización de una manera más eficiente. Idealmente, estos servicios y controles basados en la nube incluso se integrarán con soluciones existentes para simplificar las operaciones y la generación de informes de conformidad.

03

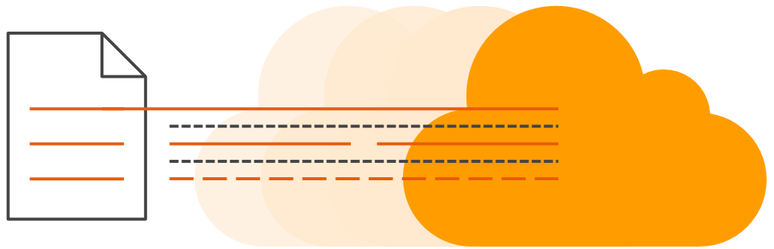
Proteja su privacidad y sus datos

Cuando transfiere datos a la nube, estos continúan siendo de su propiedad. Además, no debe perder la capacidad de cifrarlos, transferirlos ni de administrar la retención. Busque un proveedor que sea cuidadoso en relación con su privacidad y que ofrezca herramientas que le permitan cifrar fácilmente sus datos en tránsito y en reposo, para ayudarlo a garantizar que solo usuarios autorizados puedan obtener acceso a los datos.

Además, cuando trabaje con una infraestructura en la nube global, debe asegurarse de poder conservar el control pleno sobre las regiones en las que se almacenan físicamente sus datos. Esto será clave para sus reguladores, ya que lo ayudará a cumplir las regulaciones y las leyes de privacidad de datos locales y regionales, además de los requisitos de residencia de datos.

"[Usar un proveedor con una región en Sídney] es muy importante para nosotros desde una perspectiva de desempeño de producto y latencia. Nuestros clientes se encuentran en Australia y Nueva Zelanda y la soberanía de los datos también era una preocupación. También queríamos usar una gama de servicios en la nube flexibles para optimizar la capacidad del sistema para satisfacer las necesidades de los clientes".

Trevor Leybourne, director de entrega, Mind Your Own Business



“Nuestros datos están hospedados en Europa, lo que resulta fundamental para nosotros desde una perspectiva de seguridad. Con AWS, tenemos control pleno de dónde y cómo se almacenan los datos, además de quién tiene acceso a ellos.
Este control, junto con la amplia capacidad de cifrado, hace que nos sintamos seguros. Sabemos que los datos de Trust están protegidos”.

Martin Brambley,
director de MSP Sirocco Systems,
que trabaja con The National Trust, Reino Unido

04

Encuentre soluciones y socios de seguridad fiables

Una de las principales ventajas de trabajar con un proveedor de nube líder es tener acceso a sus socios y a los servicios de asesoramiento y las soluciones de seguridad en la nube que ofrecen.
Existen miles de servicios de asesoramiento y tecnología en seguridad, pero saber cuáles son los correctos para su caso de uso en particular, dónde obtener acceso a ellos y cómo administrar dichas interacciones puede ser una tarea ardua.

¿De qué manera pueden ayudarlo los socios de seguridad en la nube correctos?

1. El socio correcto tendrá una amplia experiencia y éxito comprobado en la etapa del proceso de adopción de la nube en el que se encuentre, lo que le permitirá encontrar la ayuda correcta en el momento correcto. También puede encontrar socios con habilidades en migraciones híbridas o completas.
2. Use las soluciones que ya conoce y en las que confía. Muchos socios de seguridad en la nube ofrecen las mismas herramientas y servicios que actualmente usa localmente, lo que suministra a su equipo y a los datos una transición directa a la nube.
3. Para entornos con un nivel alto de regulación, puede encontrar socios que cumplan requisitos de seguridad estrictos y que tengan experiencia en crear, implementar y administrar los tipos de cargas de trabajo que desea migrar a la nube.
4. El proveedor de nube correcto inclusive lo ayudará a simplificar asuntos de facturación con precios de socios de pago por uso y facturación consolidada, para que tenga solo una factura para todos los gastos relacionados con la nube.

05

Use la automatización para mejorar el nivel de seguridad y ahorrar tiempo

La automatización es un componente fundamental en cualquier programa de seguridad en la nube, no solo para gestionar comprobaciones de alta escala de manera eficiente, lo que libera a su equipo y permite que se enfoque en áreas más importantes del negocio, sino también para reducir los errores de configuración humanos.

También debería poder automatizar las comprobaciones de seguridad de las aplicaciones y la infraestructura siempre que se implemente código nuevo, a fin de imponer sus controles de seguridad y conformidad para ayudar a garantizar la confidencialidad, integridad y disponibilidad en todo momento.

"Con AWS, el departamento de TI es más ágil que nunca y logra alcanzar el ritmo de los negocios".

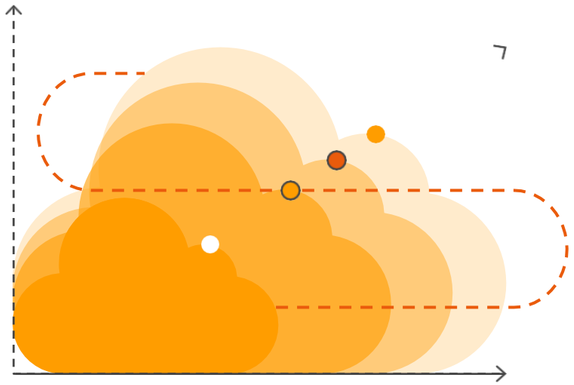
Balakrishna Rao, director de información de Manipal Global Education

0

Mejore continuamente con características de seguridad innovadoras

Durante mucho tiempo, algunos consideraron la seguridad como un impedimento para la innovación que disminuía el ritmo de los negocios. Con las herramientas y los servicios correctos en la nube, puede proteger los datos con mayor velocidad y agilidad. Además, su equipo de seguridad puede considerarse un área promotora de la innovación en toda la organización.

Para lograr este tipo de transformación, la escala sí importa. Un proveedor de nube con experiencia que trabaje con millones de clientes de todo el mundo debe contar con un equipo de ingenieros con experiencia y amplios conocimientos de las tendencias globales que les den una visibilidad destacada acerca de los nuevos desafíos de seguridad. Este conocimiento, sumado a los comentarios de los clientes, debería incorporarse en su infraestructura y en sus servicios. Estos comentarios y mejoras continuos deberían mejorar los servicios de seguridad básicos, como la administración sólida de identidades y acceso, el registro y el monitoreo, el cifrado y la administración de claves, la segmentación de redes y la protección contra ataques DDoS. De esta manera, todos se benefician.



Consejos para una buena mentalidad enfocada en la nube

En la actualidad, los CISO abordan la seguridad y los riesgos de una nueva manera. Tan solo unos pocos años atrás, inclusive considerar una migración a la nube era un asunto controversial.

Recientemente, hubo un cambio de abordaje y el foco pasó a estar en la gobernanza y de qué manera los líderes pueden guiar a su organización a través del cambio para maximizar de forma segura las nuevas oportunidades, al mismo tiempo que se conservan los controles necesarios.

También estamos observando los comienzos de una verdadera integración de la planificación de la seguridad en la estrategia en la nube. Anteriormente, los clientes empresariales podrían haberles solicitado a los proveedores que los ayudasen a escribir una estrategia de seguridad en la nube. En la actualidad, están percibiendo que una pregunta más útil es “¿Cuál es mi estrategia de seguridad general y cómo puedo incorporar la nube en ella como un modelo de implementación?”

Incorporar una mentalidad correcta puede ayudar a su organización a adaptarse a lo nuevo en seguridad en un entorno en la nube. Estos son algunos consejos a tener en cuenta.

Cree sobre lo que ya tiene.
No piense en su estrategia de seguridad en la nube de manera aislada. Por el contrario, observe su estrategia de seguridad más amplia y piense en cómo incorporar la nube sin perder de vista sus marcos de control.

Recuerde los principios básicos.
En su mayor parte, se trata de conservar la limpieza y estos principios podrán implementarse independientemente de si tiene un entorno local, híbrido o completamente hospedado en la nube.

Es un camino trillado.
Sus colegas ya recorrieron el camino. Hoy en día, no enfrenta el riesgo de ser una de las primeras organizaciones en migrar cargas de trabajo sensibles a la nube. El 84 por ciento de los gerentes de TI informó ya estar usando infraestructura en la nube pública.[3]

El verdadero asunto sobre la seguridad es el liderazgo.
Para tener éxito en la nube, muchas organizaciones eligen transformar su funcionamiento. Su equipo de líderes debe estar preparado para definir de qué manera guiará a su organización a través del cambio. ¿Quién será responsable de la seguridad y la conformidad? En caso de que sea necesario, ¿de qué manera deben modificarse las habilidades de los trabajos y los roles?

3 Encuesta sobre la nube pública de SADA Systems

Invierta en la seguridad en la nube de la misma manera que lo hace en la nube.

Pruebe nuevas maneras de resolver los desafíos relacionados con la seguridad y la conformidad.

La nube le ofrece un modelo flexible que le permite probar antes de comprar o probar mientras compra que también le otorga el beneficio de una mayor responsabilidad por parte del proveedor. De esta manera, puede empezar con poca escala, probar y después crear en función de sus necesidades.

Las mejores soluciones de seguridad en la nube están diseñadas para la agilidad y la automatización.

Las soluciones en la nube ofrecen a los usuarios la libertad para probar e iterar, con la posibilidad de hacer mejoras sobre la marcha. Pruebe una nueva solución de seguridad y, si no le gusta, puede hacer cambios pequeños y controlados para adecuarla, o bien puede retrotraerla, sin quedar bloqueado.

Probablemente ya esté en la nube en alguna parte.

Si hoy cuenta con un centro de datos, probablemente ya esté usando la informática en la nube en alguna parte de dicha cadena de suministro. Puede aprovechar este hecho con su equipo de líderes para empezar a migrar más cargas de trabajo sensibles a la nube.

Lograr que la conformidad deje de ser un obstáculo y se convierta en un factor habilitador

Uno de los principales obstáculos para la adopción de la nube es la preocupación en torno al cumplimiento de requisitos de conformidad y riesgo estrictos, que a menudo son específicos de un sector o país. Encontrar un proveedor de nube con amplia experiencia en la creación de entornos seguros para la mayoría de las organizaciones sensibles al riesgo es solo el primer paso. Idealmente, encontrará un proveedor que pueda ayudarlo a demostrar ante las personas internas y externas interesadas en el riesgo que sus datos están seguros y que cumplen los requisitos de marcos de control externos correspondientes.

En AWS, tenemos una mentalidad diferente en relación con la seguridad y la conformidad.
Como todo en Amazon, nuestro éxito se mide principalmente en función de un factor: el éxito de nuestros clientes. Cuando se trata de la seguridad y la conformidad, nuestros clientes orientan nuestra cartera de informes de conformidad, acreditaciones y certificaciones que respaldan sus estrategias para ejecutar un entorno en la nube seguro y en conformidad.

Con AWS, puede:

- Heredar muchos controles de seguridad que utiliza AWS, lo que le da la oportunidad de fortalecer sus propios programas de conformidad y certificación.
- Obtener acceso a herramientas que lo ayudarán a reducir el costo de mantener y ejecutar sus requisitos de control de seguridad específicos.
- Ahorrar tiempo con AWS Artifact, nuestra herramienta de informes de conformidad automatizada, que permite revisar y descargar informes y detalles sobre miles de nuestros controles de seguridad.
- Comience con confianza con nuestras prácticas recomendadas de configuración de seguridad descritas en nuestras guías de inicio rápido, que ofrecen una base sólida para cumplir requisitos de conformidad globales.
- Combine características de seguridad aptas para auditorías y enfocadas en gobernanza con estándares de auditorías o regulaciones de conformidad de seguridad aplicables.
- Con AWS Compliance, puede basarse en sistemas heredados y ayudar a los clientes a definir un entorno con control de seguridad de AWS y a ejecutar operaciones en él.

Compartir con su proveedor de nube las responsabilidades vinculadas con la seguridad

Un asunto que ha surgido en relación con la nube es quién es responsable de la seguridad.

¿Cómo se desglosa la responsabilidad en relación con la seguridad en su organización y cómo se divide entre usted y el proveedor?

Una conjetura sorpresivamente común entre quienes compran servicios en la nube es que una vez que migran a la nube, toda la responsabilidad asociada con la seguridad queda a cargo del proveedor. Eso no sucede con ningún proveedor. En AWS, nuestra estrategia de priorización del cliente define la manera en la que compartimos la responsabilidad por la seguridad y la conformidad con nuestros clientes.

El modelo de responsabilidad compartida de AWS

Nuestro modelo diferencia claramente entre la seguridad de la nube y la seguridad en la nube.

01

La seguridad de la nube

se refiere a las medidas que nosotros, como el proveedor de servicios en la nube, implementamos y usamos.

02

Seguridad en la nube

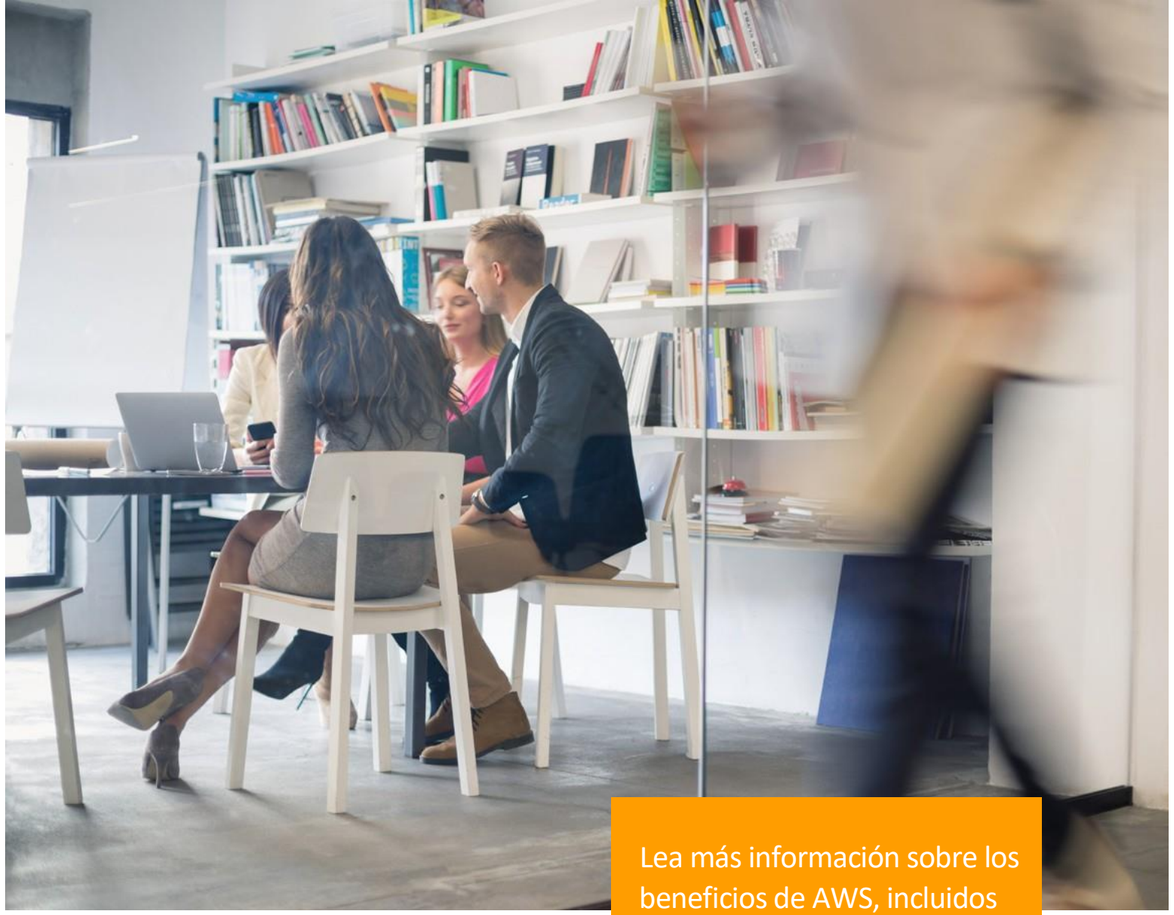
se refiere a aquellas medidas que el cliente implementa y usa, y se relaciona con la seguridad del contenido y las aplicaciones del cliente que usan los servicios de AWS.

Ayuda al cliente a compartir la responsabilidad sin entregar las riendas. Las organizaciones conservan la visibilidad y el control sobre las medidas de seguridad que deciden implementar para proteger su contenido, plataforma, aplicaciones, sistemas y redes, sin diferencias en relación con las aplicaciones de un centro de datos local.

Para leer información más detallada sobre la seguridad y la nube (y, en última instancia, hasta dónde llega la responsabilidad de cada uno), consulte este Libro electrónico sobre el modelo de responsabilidad compartida de AWS.

Su próxima movida

Tendrá muchos recursos disponibles cuando esté listo para empezar a usar los servicios de AWS:



1. Siga las prácticas recomendadas sobre seguridad descritas en nuestro marco de adopción de la nube (CAF).
2. Aproveche nuestra completa red de socios de AWS (APN), conformada por socios y servicios de seguridad que probablemente conozca y use actualmente, y consulte las soluciones disponibles a través de AWS Marketplace.
3. Entre en contacto con nuestro equipo de servicios profesionales para agilizar su migración a la nube y para que lo ayuden en cada paso relacionado con la protección de su entorno en la nube.

Lea más información sobre los beneficios de AWS, incluidos detalles sobre nuestra infraestructura y seguridad, y las características de conformidad en nuestro sitio web aws.amazon.com/security.