Un Manual Básico de Seguridad en Nube

WHITE PAPER

Contenido

A pesar de la rápida proliferación de la computación en nube, no existe sólo un modelo estándar para la manera en que las empresas están implementando y utilizando modelos de nube. Las organizaciones están utilizando las nubes privadas y públicas, y a menudo la combinación de las dos en nubes híbridas. Están desplegando modelos de software como servicio (SaaS), infraestructura como servicio (IaaS) y plataforma como servicio (PaaS). Algunos equipos de TI están entregando las aplicaciones críticas de negocios en una única nube privada; otros están utilizando múltiples nubes para los mismos tipos de aplicaciones. Algunos están aprobando iniciativas de TI oculta; otros las desalientan.

Sin importar qué tan diverso pueda ser su entorno de nube, si usted está involucrado en la supervisión o el despliegue de servicios de nube en su organización, hay un axioma inviolable que debe tener en mente siempre: No importa qué tan sencillos o complejos sean sus despliegues de nube, nunca debe permitir que la seguridad de sus datos o aplicaciones se ponga en riesgo de alguna manera. Si ocurre una brecha o un ciberataque donde sus datos son expuestos, o si las agencias reguladoras lo citan por estar en no conformidad, no le servirá de mucho echar la culpa al proveedor de nube pública. A final de cuentas, usted es responsable de su propia seguridad, Incluso si su proveedor de nube pública tiene un modelo de "responsabilidad compartida".

En esta época de diversos despliegues de nube, ¿qué significa eso? Conforme los datos y aplicaciones fluyen a través de múltiples nubes privadas, públicas e híbridas, ¿cómo puede garantizar la protección en todo momento? Cuando usted está utilizando una nube pública, ¿dónde está su responsabilidad por la seguridad final y dónde comienza la del proveedor? ¿Puede asegurar que no haya lagunas en la protección de datos y aplicaciones cuando dejan su perímetro de red? Conforme adopte nuevas

intel Security

TechTarget Custom Media

A TECHTARGET WHITE PAPER

No importa qué tan sencillos o complejos son sus despliegues de nube, nunca debe permitir que la seguridad de sus datos o aplicaciones se pongan en riesgo de alguna manera.

tecnologías para nubes privadas, tales como un centro de datos definido por software (SDDC), ¿qué es lo que debe saber acerca de la exposición al riesgo adicional?

Este documento describe los desafíos de seguridad de los distintos modelos de nube que usted puede estar implementando o considerando. También proporcionamos guías para ayudar a asegurar que la protección no se vea en riesgo, sin importar qué tan diverso o complejo se vuelva en su uso de los modelos de nube. Por último, ofrecemos una breve descripción de algunas de las tecnologías fundamentales que forman una sólida base de seguridad para la era de la nube.

Desafíos de Seguridad de los Diferentes Modelos de Nube

No es una exageración decir que la nube lo cambia todo, especialmente cuando se trata de la seguridad. La computación en nube presenta desafíos de seguridad que son bastante diferentes de los desafíos del pasado, incluso en el pasado reciente. Para los profesionales de la seguridad, no trata sólo acerca de la protección del perímetro, crear una zona desmilitarizada (DMZ) o utilizar los últimos productos de antivirus o antimalware: trata acerca de tener una estrategia de seguridad de principio a fin que permita nuevos niveles de visibilidad, percepción, control y protección, especialmente a medida que las aplicaciones y los datos se mueven cada vez más a lo largo de entornos heterogéneos. Aquí mostramos los principales desafíos presentados por cada uno de los distintos modelos de nube:

Nube Híbrida

La nube híbrida es un entorno de computo en nube que utiliza una mezcla de instalaciones de nube privada y nube pública de terceros con orquestación de servicios entre las dos plataformas[1]. Las organizaciones están utilizando cada vez más los modelos de nube híbrida porque proporcionan a TI modelos flexibles de despliegue. Algunas de las aplicaciones críticas de negocios pueden permanecer bajo el control de TI en una nube privada. Otras aplicaciones pueden prestarse a modelos de nube pública para aprovechar ventajas como la escalabilidad elástica, ahorros o aprovisionamiento de autoservicio.

Las nubes híbridas presentan desafíos de seguridad muy específicos porque los datos y las aplicaciones puedan entrar y salir de diversos entornos de nube: desde su centro de datos, hacia las nubes públicas, y luego de regreso hacia la red. Cuando sus aplicaciones y datos fluyen hacia la infraestructura de un proveedor de nube pública, usted corre el riesgo de perder visibilidad y control. Esto puede convertirse en un punto de inserción para el malware. El desafío no es sólo ampliar la visibilidad a lo largo de todos los recursos de cómputo, en las instalaciones y en la nube pública, sino también aplicar monitoreo, protección, presentación de informes y corrección constantes en todo el entorno de nube híbrida de principio a fin.

Lo que usted necesita para nube híbrida es una estrategia de seguridad de principio a fin que amplíe la visibilidad y el control. Usted necesita aplicar fácilmente protecciones y políticas para todas las máquinas virtuales (VMs), sin importar donde estén ubicadas, dentro de su nube privada o dentro de la infraestructura de un proveedor de nube pública como parte de su entorno de nube híbrida.

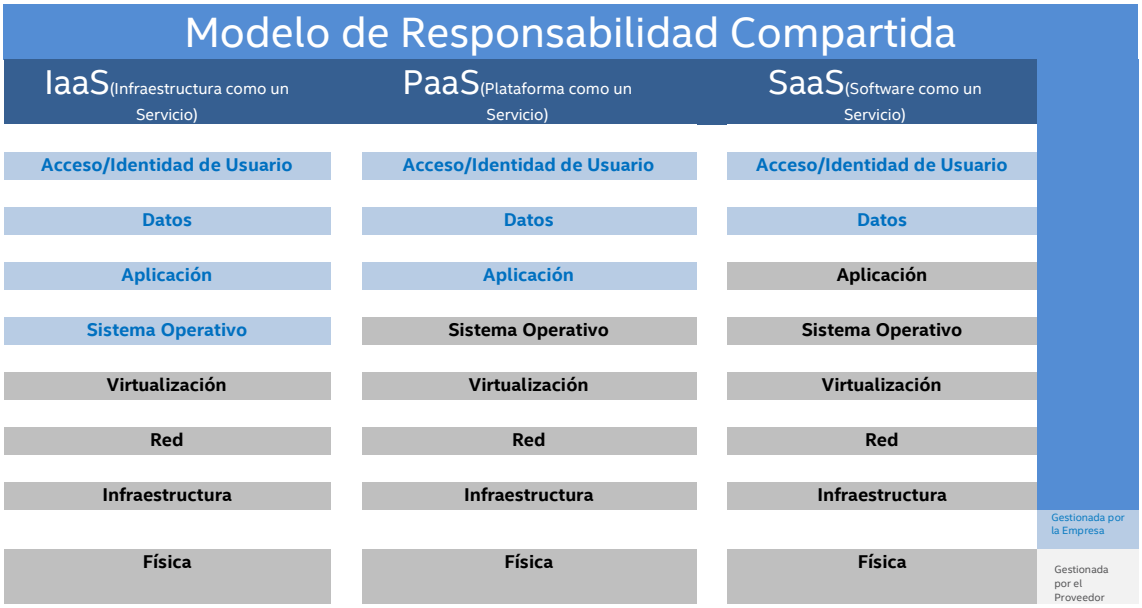
Nube Pública

Una nube pública es una infraestructura en nube que está abierta para su uso por parte del público en general. Es propiedad, se gestiona y opera por un negocio u organización gubernamental o académica, o alguna combinación de ellos. Existe en las instalaciones del proveedor de nube[2]. Desde un punto de vista de la seguridad, la nube pública plantea muchos de los mismos desafíos que acabamos de discutir en la sección sobre nube híbrida. Sus datos y aplicaciones se mueven hacia afuera de su visibilidad y control, hacia la infraestructura de un proveedor de nube pública. Debe saber dónde terminan sus responsabilidades y dónde comienzan las responsabilidades de su proveedor de nube pública.

Usted no puede simplemente abdicar de la responsabilidad por la seguridad y el cumplimiento, y dejarla a los proveedores de nube pública, asumiendo que se harán cargo de ella. Usted tiene que estar consciente del modelo de responsabilidad compartida de cada proveedor de servicios de nube por cada uno de los distintos modelos de nube que usted despliegue: SaaS, PaaS y/o IaaS. La mayoría de los principales proveedores de nube pública, tales como Amazon, Google o Microsoft, detallan sus modelos de responsabilidad compartida en sus sitios Web. Tómese el tiempo para comprender estos modelos y aplicarlos a los diferentes tipos de modelos de despliegue que pueda estar utilizando. Y, antes de firmar cualquier contrato, asegúrese de que las responsabilidades se detallen en cada caso por separado para cada tipo de servicio.

Para los profesionales de seguridad, no sólo trata acerca de la protección del perímetro, creando una zona desmilitarizada (DMZ) o utilizando los últimos antivirus o productos antimalware: Trata acerca de tener una estrategia de seguridad de principio a que permita alcanzar nuevos niveles de visibilidad, conocimientos, control y protección.

Un ejemplo del modelo de responsabilidad compartida de nube pública puede verse en el gráfico siguiente, en el que las capas de la pila están diferenciadas por quién es el responsable de esos ítems.



Uno de los mayores desafíos de seguridad con una nube pública es que es muy fácil de desplegar. Un gerente de línea de negocios, o incluso un usuario individual, puede simplemente ir a una página Web del proveedor de nube pública y suscribirse a un servicio con unos pocos clics y una tarjeta de crédito. Este tipo de despliegue de "TI oculta" puede exponer a la organización a riesgos de seguridad adicionales. El equipo de TI podría incluso no enterarse de ello, y el usuario puede no estar familiarizado con los tipos de controles de seguridad necesarios para mantener la seguridad de la compañía.

Uno de los desafíos adicionales en relación con la nube pública es saber quién en su organización está utilizando los servicios en la nube pública, qué tipos de servicios está utilizando - SaaS, PaaS o IaaS- y cómo y cuándo los está utilizando. Una vez que sea capaz de lograr este conocimiento, usted necesita utilizar soluciones tecnológicas que le permitan ejercer cierto grado de control sobre ellos, que variarán en función del tipo de servicios en uso. Al hacer referencia al modelo de seguridad compartida, es evidente que el acceso, el control de la identidad y la protección de datos deben ser cosas prioritarias para la seguridad en la nube, especialmente con los servicios SaaS. Para entornos de IaaS, busque un producto de seguridad que permita el control y monitoreo de integridad de archivos, que prohíba la instalación de software no autorizado y monitoree cualquier cambio realizado. También, asegúrese de utilizar una solución basada en host que proporcione visibilidad hacia todas sus aplicaciones.

Nube Privada

Usted no puede simplemente abdicar de la responsabilidad por la seguridad y la conformidad y dejarla a los proveedores de nube pública.

Una nube privada es un tipo de cómputo en nube que ofrece ventajas similares a la nube pública, incluyendo escalabilidad y suministro de autoservicio, pero a través de una arquitectura propia. A diferencia de las nubes públicas, que ofrecen servicios a múltiples organizaciones, una nube privada está dedicada a una única organización[3].

La nube privada mantiene los datos y aplicaciones bajo el control de su organización, para que no tengan que desplazarse hacia afuera de su perímetro, hacia otro proveedor de infraestructura. En apariencia, esto parecería hacer que la seguridad sea mucho más sencilla que en despliegues públicos o híbridos. Esto puede ser cierto de alguna manera, pero, como se señaló anteriormente, la nube lo cambia todo.

Las nubes privadas exigen nuevos modelos de despliegue para los centros de datos, que extienden la virtualización a lo largo de toda la infraestructura y permiten a las organizaciones utilizar capacidades de nube, agrupación de recursos, escalabilidad elástica, capacidades de autoservicio y contracargos automáticos. Esto permite al negocio beneficiarse de un modelo de TI más centrado en servicios. Sin embargo, este modelo puede traer riesgos de seguridad adicionales que deben preverse y planificarse.

Las soluciones de seguridad deben estar incorporadas en el entorno de TI general y no ser agregadas como una ocurrencia tardía. Los equipos de TI y de seguridad deben utilizar herramientas y tecnologías que han sido diseñadas específicamente para satisfacer los desafíos de la era de la nube.

Un ejemplo: A medida que la virtualización se expande dentro de su centro de datos más allá de los servidores y hacia redes y almacenamiento, la cantidad del tráfico este/oeste que fluye entre las máquinas virtuales (VMs) aumentará drásticamente. Las tecnologías anteriores que se enfocaban en el perímetro no tenían visibilidad de este tráfico y no serán capaces de proporcionar protección para ellas. Usted necesita la capacidad para aplicar controles de seguridad con inspección de paquete profunda a todo este tráfico intra-VM.

Otro ejemplo: Conforme las nuevas máquinas virtuales son pobladas, usted puede experimentar brechas de seguridad si las políticas y protecciones no se aplican a ellas inmediatamente. Usted no puede permitir que esto suceda, así en la nube privada, usted debe buscar aplicar seguridad mediante un modelo virtualizado o definido por software que aproveche la automatización y orquestación de políticas de seguridad. Esto limitará el tiempo y los riesgos involucrados en el suministro y despliegues manuales. Si y cuando la VM se mueve, todas las configuraciones y protecciones de seguridad deberían moverse con ella.

Un tercer ejemplo: La naturaleza dinámica de suministrar máquinas virtuales y su carga general en servidores en un entorno de nube privada, puede dificultar la planificación de la capacidad. Si está ejecutando una solución antivirus que no está diseñada para los entornos virtuales dentro de una nube privada, puede ser una tarea casi imposible. Aunque los tradicionales antivirus se ejecutan en estas máquinas virtuales, el impacto en el rendimiento acumulativo en la infraestructura será muy alto. Esto afectará directamente a cuántas VMs se pueden ejecutar en un servidor, lo que impacta la relación diseñada VM-servidor, así como a los retornos operacionales. Una solución de antivirus virtual optimizada se adapta mejor para proteger este entorno elástico sin alterar el rendimiento y la escalabilidad.

Emprendiendo el Siguiente Paso

El cambio hacia el cómputo en nube es una de las iniciativas de TI más importantes de nuestros tiempos. IDC ha dicho: "'La Nube Primero' se convertirá en el nuevo mantra para la TI empresarial"[4]. Según un reciente informe del Estado de la Adopción de la Nube de Intel Security, un 80% de los presupuestos de TI se destinarán a los servicios de computo en nube durante los próximos 16 meses, y el 96% de las organizaciones aumentarán sus inversiones en la nube[5]. Además, las compañías están utilizando un promedio de 43 diferentes servicios de nube, y 40% ya procesan o almacenan datos confidenciales en la nube. Y aunque el 77% de los encuestados dijeron que confían en la nube más que hace un año, el 66% también dijeron creer que los altos directivos no comprenden totalmente los riesgos de almacenar datos confidenciales en la nube.

Para los profesionales de seguridad, la nube requiere un nuevo abordaje. La seguridad en la nube es un desafío de principio a fin donde las soluciones deben ser integradas en el entorno general de TI y no agregadas como una idea adicional. Los equipos de TI y de seguridad deben utilizar herramientas y tecnologías que han sido diseñadas específicamente para satisfacer los desafíos de la era de la nube. Por último, estas tecnologías y herramientas deben desplegarse como parte de un sistema integrado de modelo de despliegue. Usted desea asegurarse de que la protección sea consistente en todos los entornos de nube. Las funcionalidades tales como la detección y prevención de intrusiones deben ser entregadas en tiempo real para proteger a toda la organización en todo momento, sin importar dónde están ubicados los datos y las aplicaciones.

En la construcción de su estrategia de seguridad en la nube, es importante trabajar con un proveedor que ofrezca un modelo integrado para la seguridad en la nube, así como un conjunto diverso de soluciones específicas para la nube. Las tecnologías críticas que usted necesitará implementar incluyen un controlador de seguridad definido por software; una plataforma de seguridad de red virtual; protección antimalware virtual; Protección de nube pública basada en host; inteligencia de amenazas avanzada; y gestión centralizada.

Estas soluciones integradas entre sí, forman la base de su estrategia de seguridad en la nube para ahora y para el futuro. Y, como siempre parece ser el caso en la TI empresarial, el futuro ya está al alcance de la mano.

Si está listo para dar el siguiente paso para garantizar la seguridad de sus entornos de nube, póngase en contacto con Intel Security en **www.mcafee.com/cloudsecurity**.

intel Security

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

1 "Hybrid Cloud," SearchCloudComputing, TechTarget

2 "The NIST Definition of Cloud Computing," Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, septiembre de 2011

3 "Private Cloud," SearchCloudComputing," Tech Target

4 "IDC Predicts the Emergence of 'the DX Economy' in a Critical Period of Widespread Digital Transformation and Massive Scale Up of 3rd Platform Technologies in Every Industry," IDC, 4 de noviembre de 2015

5 "Blue Skies Ahead? The State of Cloud Adoption," Intel Security, abril de 2016