Guía empresarial sobre los aspectos básicos de la seguridad en la nube

Forcepoint

Folleto

Qué contiene:

Descripción general del panorama: seguridad en la nube y migración a la nube

Si cree que la nube está cada vez más generalizada, está en lo cierto. Pero, ¿qué es lo que impulsa esta aceleración rápida y furiosa de todas las cosas hacia la nube? En realidad, es el consumismo. Sí, del tipo B2C (de la empresa al consumidor).

La manera en que las personas utilizan la nube cada día impulsa a las empresas a adoptar y proteger la nube.

La seguridad en la nube está impulsada por las personas.

La nube representa un acceso instantáneo.

Y se espera contar con la nube.

Con acceso constante a contenido, aplicaciones, dispositivos, todos conectados entre sí, sin interrupciones y todo el tiempo, la nube es una parte inextricable de nuestras vidas diarias. Está profundamente arraigada a la manera en que la persona moderna funciona y opera en forma inconsciente. Por eso, en el trabajo, la expectativa es la misma. Usted desea usar lo que necesita, cuándo lo necesita. Y desea tener una experiencia fluida que no obstaculice su productividad, sino todo lo contrario. ¿Cómo puede incrementar su productividad con la nube? ¿Cómo puede hacer más con menos? Porque, en realidad, la nube representa comodidad. Pero también es una vulnerabilidad.

En definitiva, los trabajadores son consumidores. La manera en que las empresas protegen sus organizaciones, y resguardan sus datos y personal, debe coincidir con la misma expectativa y experiencia que tenemos todos los días en nuestras tareas diarias. Y la seguridad debe evolucionar para permitir esa fluidez, a la vez que debe proteger el panorama de amenazas en constante expansión que acompaña esa libertad y comodidad.

Esta es la cultura general de la nube. Pero, ¿cuáles son las circunstancias específicas que incitan a la acción y alientan a las organizaciones a repensar su enfoque hacia la nube y la seguridad como un todo? Algunas de ellas son:

- El camino hacia la transformación digital, comenzando con la adopción e implementación de O365
- Trasladar las aplicaciones heredadas o personalizadas a la nube, como los sistemas EHR o ERP
- Personas que trabajan más allá de los confines de una oficina, fuera de la red corporativa o bajo otras protecciones
- Empresas globales que operan dentro de entornos altamente distribuidos, que abarcan sitios que requieren el mismo nivel de seguridad que las oficinas centrales, sin la necesidad de recrear una huella costosa y cargada de hardware en cada ubicación con concentración de tráfico
- Esfuerzos de optimización, ya sea para consolidar las capas de seguridad, optimizar los flujos de trabajo de los equipos o simplemente reducir los gastos de capital/gastos operativos
- Trasladar la infraestructura a nubes públicas como AWS o Azure

El camino correcto hacia la nube

La seguridad en la nube significa algo diferente para cada persona. Y cambia constante y rápidamente. Entonces, ¿cómo puede mantenerse actualizado? ¿Cómo puede garantizar que su método sea holístico y efectivo? Para proteger satisfactoriamente a su organización, la seguridad en la nube debe ser inclusiva.

Analicemos los componentes clave de la nube:

Datos en la nube | **Usuarios** en la nube | **Aplicaciones** en la nube | **Conectividad** en la nube | **Infraestructura** en la nube | **Seguridad** en la nube

En esencia, de esto se trata la seguridad en la nube. Y es necesario considerar, gestionar y proteger todos los componentes de la nube para evitar fugas de seguridad y para mantener a los usuarios y los datos seguros. Si bien la seguridad en la nube no tiene una definición estática, existe un camino correcto hacia la "nube".

Bien, ¿cómo es eso?

Para proteger y conectarse a la nube, las organizaciones deben:

- Resguardar el acceso al contenido web y a las aplicaciones en la nube para cualquier usuario, en cualquier parte y en cualquier dispositivo
- Tener visibilidad y control sobre la organización para impulsar la estrategia de seguridad en la nube
- Proteger los datos a medida que se mueven desde y hacia la nube
- Habilitar la conectividad directa a la nube para los usuarios y sitios sin concentración del tráfico
- Optimizar la infraestructura y el flujo de trabajo
- Protegerse contra las amenazas avanzadas, incluidas las vulnerabilidades del día cero

Muy bien, entonces ahora que sabe lo que tiene que hacer, ¿cómo puede hacerlo? Es posible que muchas organizaciones cuenten con productos que puedan desempeñar algunas capacidades clave, o empleen a diferentes equipos que son responsables de ciertos elementos de la seguridad en la nube. Pero lo que toda organización de seguridad quiere evitar es abrumar a sus ya agobiados equipos de seguridad al implementar varios productos que no están integrados y no se comunican entre sí. Lo que realmente necesitan las organizaciones es una solución singular, no una mezcla de productos de diversos proveedores. Sí, las dependencias existen, como la necesidad de tener visibilidad para tener control, o la necesidad de migrar la seguridad web en las instalaciones hacia la nube para proteger a los usuarios fuera de la red. En su estado óptimo, la seguridad en la nube es una solución unificada que gira en torno a los datos, el acceso web, el acceso a la nube y los datos en la nube, y la conectividad. Sirve para aliviar los puntos problemáticos de su equipo de seguridad y evitar brechas en la seguridad. Ya sea que eso se logre con uno o tres proveedores, las empresas deben garantizar que tienen lo que desean dónde lo desean para estar en sintonía a fin de obtener resultados comerciales clave.

Inquietudes sobre la nube

Trasladar los datos a la nube es un esfuerzo considerable, y si se siente preocupado al respecto, no es el único. ¿Cómo puede mantener la propiedad y el control? ¿Cómo puede seguir manteniendo las amenazas a raya? ¿Cómo garantiza el rendimiento?

Resolvamos algunos de los temas comunes en cuestión.

Latencia

La cobertura es crítica para reducir la latencia. Una huella amplia con muchos PoP en todo el mundo ofrecerá una latencia baja, así como otros beneficios que aumentan la productividad como la localización de contenido. **Las redes de nivel 1 y los centros de datos de nivel 4** ayudan a garantizar un alto grado de alcance, redundancia, conectividad y calidad ideales para aplicaciones sensibles a la latencia.

Visibilidad

No puede proteger lo que no puede ver. Y no puede hacer cambios o establecer una política sin saber qué cosas afectará. Combinar una **puerta de enlace web en la nube** con un **firewall** brinda visibilidad y aplicación constantes para los usuarios y las ubicaciones, lo que incluye la implementación de políticas y el control de la Shadow IT. Y la funcionalidad **CASB** ayuda a proteger a las empresas al brindar visibilidad respecto de lo que hacen en la nube los usuarios de aplicaciones autorizadas y no autorizadas para comprender los riesgos y proteger a los usuarios y los datos.

Cumplimiento

Certificaciones de programas confiables: no simplemente el cumplimiento auditado por el mismo proveedor. Es probable que los estándares relevantes para su organización incluyan:

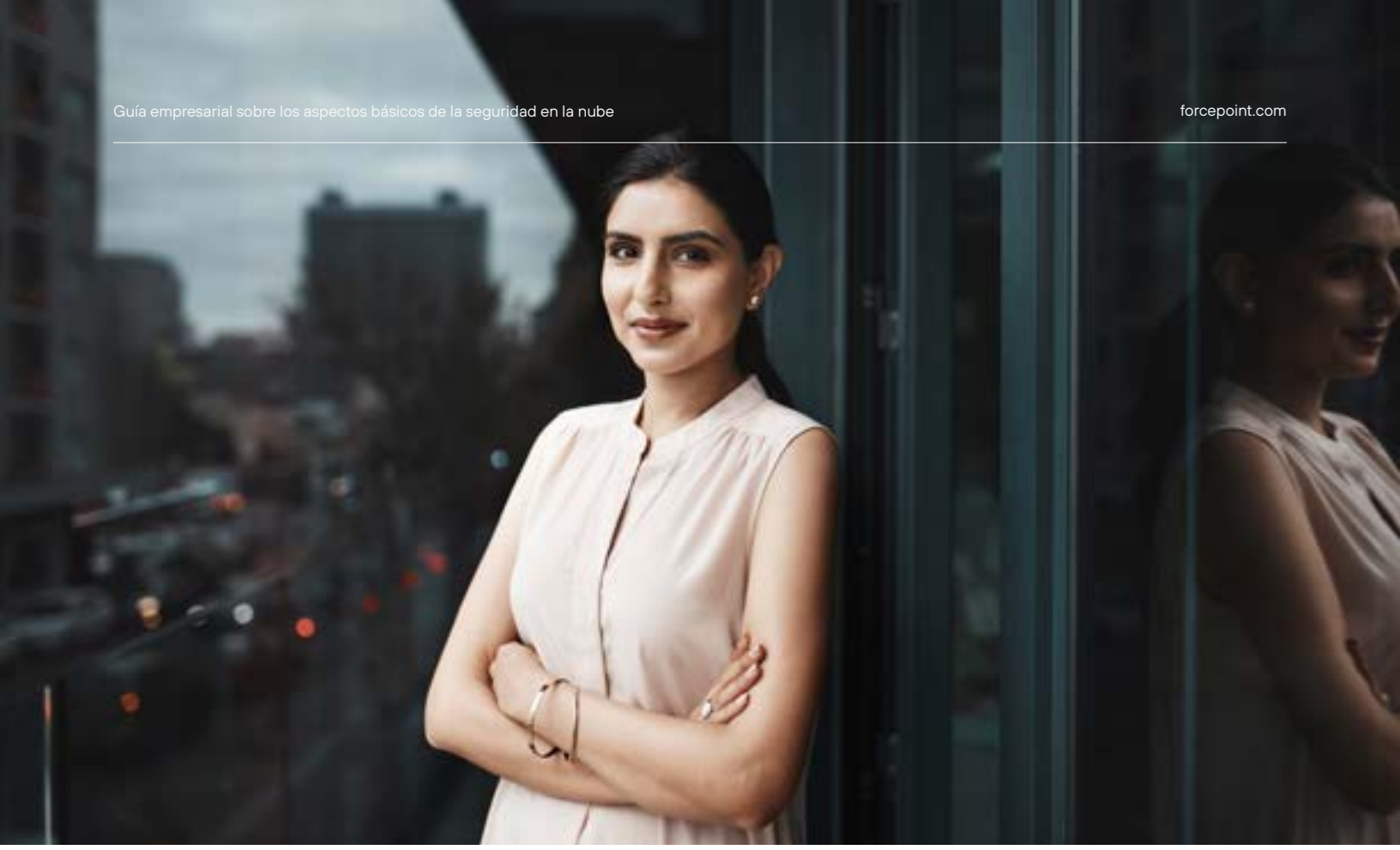
- **ISO 27018**, que rige la información de identificación personal (PII)
- **ISO 27001**, una certificación de varios sitios para operaciones de desarrollo, control de calidad, implementación y soporte
- **CSA**, que rige la seguridad del software y las operaciones interdisciplinarias en un entorno de nube (y se basa en el Código de conducta de la Normativa General de Protección de Datos (GDPR))
- **SOC2**, que se centra en los controles de redacción de informes no financieros relacionados con la seguridad, la disponibilidad, la integridad del proceso, la confidencialidad y la privacidad, además de la evaluación de los centros de datos y la efectividad operativa

Soberanía de datos

Si bien la nube en sí no tiene límites concretos, no está exenta de las consecuencias legales de las fronteras y los límites geográficos. Los datos digitales están sujetos a las leyes de los lugares en donde residen esos datos. Utilizar **centros de datos en la nube ubicados en las regiones en las que opera su empresa** es fundamental para cumplir con las leyes y normas locales, así como para el rendimiento.

Pérdida de datos

Un enfoque unificado es el más exitoso. Con **soluciones de protección de datos** integradas, puede extender sus medidas de seguridad de las instalaciones a la web, el correo electrónico, los dispositivos finales, las redes y la nube. Aproveche sus políticas existentes para resguardar los datos en reposo en la nube y los datos en tránsito.



Traiga su propio dispositivo (BYOD)

En la actualidad, la fuerza laboral depende de diversas aplicaciones en la nube autorizadas y no autorizadas, en dispositivos administrados y no administrados. Cuando se protege a los usuarios remotos e itinerantes, las defensas del perímetro de la red y la protección de los dispositivos finales simplemente no alcanzan. Debe distinguir entre los dispositivos administrados y los BYOD, al utilizar **políticas de seguridad granular** para brindar a los empleados la flexibilidad necesaria para usar sus propios dispositivos sin que esto presente un riesgo adicional. **Los controles ampliados** ofrecen seguridad para aquellos usuarios remotos que utilizan dispositivos de la compañía tanto para el trabajo como para uso personal.

Conformarse con algo suficientemente bueno

Ansiosas por ser más ágiles, eficientes, etc., a menudo las compañías emplean un enfoque de "lo resolveremos después" cuando se trata de la nube. Sin embargo, hacer lo mínimo necesario a menudo perjudica tanto la seguridad como la eficacia. Por ejemplo, el filtrado de URL por sí solo no brinda seguridad, de la misma manera una solución de DNS recursiva no reemplaza una puerta de enlace web completa. No puede obtener una protección integral con un solo elemento de una solución. Además, el enfoque de "solo lo indispensable" coloca a la seguridad en una posición en la que debe reaccionar, en lugar de actuar en forma proactiva. Asegúrese de que tanto la **seguridad como las redes trabajen en forma conjunta y tengan un rol destacado** a medida que su empresa crea su estrategia para la transformación digital; de esa manera, trabajarán siguiendo los objetivos de la empresa y evitarán quedarse atrás.

Cómo tener éxito en un mundo conectado a la nube

Establecimos al comienzo que la seguridad en la nube está impulsada por las personas. Es por eso que debe estar centrada en las personas.

Gracias a la nube, **las personas son el nuevo perímetro.**

Cuando los usuarios, socios y clientes acceden a los datos de su empresa desde cualquier parte del mundo, el muro artificial que protege los datos ya no es suficiente.

La seguridad heredada centrada en la infraestructura que agrupa a usuarios confiables en el interior y a individuos no confiables en el exterior ya no es relevante.

La confianza inherente no puede ser parte de su capa de seguridad.

Y su capa de seguridad es fundamental, y no auxiliar, para su transformación digital.

Para acelerarla y protegerla, le presentamos algunos principios fundamentales a tener en cuenta:

La nube a su propio ritmo
Roma no se construyó en un día. Y la migración a la nube no se realizará de la noche a la mañana. La mayoría de las empresas operan en entornos de TI híbrida/nubes múltiples, y seguirán haciéndolo en un futuro previsible. Asegúrese de que su puerta de enlace web segura tenga opciones flexibles de implementación que le permitan realizar la migración conforme a lo que necesite su organización hoy, y mañana. Esto le permitirá realizar la migración en sus propios términos, cuando esté listo, y a la vez podrá mantener la seguridad general.

Amplíese a medida que crece
Proteja su nube, red y dispositivos finales para satisfacer sus necesidades en constante cambio. Una plataforma convergente con bajo nivel de hardware con capacidades de seguridad modular ofrece a las organizaciones altamente distribuidas la extensibilidad y agilidad que necesitan para sacar provecho de los nuevos avances, evitar los puntos ciegos y conectar las ubicaciones, en forma segura y gestionable.

Zero Trust: conocimiento absoluto
"Nunca confíe, siempre verifique" es un principio fundamental del marco Zero Trust, y significa que la manera de proteger los datos de su organización es evaluar el acceso a esos datos durante la interacción entre el usuario y el dispositivo. Esto lo ayuda a comprender "quién" y "cómo". Comprender el "por qué" es lo que le ayudará a pasar de la conciencia a la prevención. Básese en un análisis conductual para comprender la intención.

¿Listo para ver lo que viene en el camino hacia la seguridad en la nube escalable?

› Lea nuestro libro electrónico, Protegiendo la fuerza laboral cuándo sea, dónde sea.

Forcepoint

forcepoint.com/contact

Acerca de Forcepoint

Forcepoint es la compañía líder en seguridad cibernética de protección de datos y usuarios, encargada de proteger a organizaciones a la vez que impulsa la transformación digital y el crecimiento. Las soluciones de Forcepoint se adaptan en tiempo real a la manera en que las personas interactúan con los datos, y proporcionan un acceso seguro a la vez que permiten que los empleados generen valor. Con sede en Austin, Texas, Forcepoint crea entornos seguros y fiables para miles de clientes en todo el mundo.