10 CARACTERÍSTICAS CLAVE

de un buen proveedor de soluciones de seguridad en la nube

Buscar un proveedor de seguridad en la nube puede ser una tarea desconcertante. A primera vista, da la sensación de que muchos proveedores son idénticos, ya que ofrecen métricas y promesas semejantes. Lo cierto es que, si quiere hacer una comparación válida, deberá formular una serie de preguntas e indagar en datos que los proveedores de servicios en la nube no siempre ponen a su disposición abiertamente.

Sírvase de esta lista para seleccionar un proveedor de seguridad en la nube que le ofrezca los elementos clave que le permitan proteger su organización de ciberataques maliciosos.

1. **Experiencia.** ¿Cuánto tiempo lleva el proveedor en el sector de la seguridad en la nube? ¿Con cuántos clientes cuenta actualmente en el marco de la seguridad en la nube en todo el mundo? (Los datos sobre los vectores de ataque globales son muy interesantes). ¿Puede satisfacer las necesidades de su empresa?

2. **Capacidad y escalabilidad.** Muchos proveedores de seguridad en la nube sostienen que ofrecen suficiente escalabilidad, pero es importante saber cómo la miden. Deberá confirmar si pueden ofrecérsela justo cuando la necesita. Para ello, conviene hacerles las siguientes preguntas: ¿Cuál es el tamaño del mayor ataque distribuido de denegación de servicio (DDoS) al que podrían hacer frente? ¿Pueden demostrarlo? ¿Han tenido ataques similares en su red?

3. **Rendimiento, distribución y disponibilidad.** ¿Ofrecen soluciones de seguridad en la nube totalmente integradas que dispongan de una red global de servidores respaldados por sistemas de automatización y algoritmos basados en datos? ¿Permiten elegir barrido de DDoS, redes CDN o ambas opciones?

4. **Inteligencia colectiva.** ¿Cuenta el proveedor con la escala y el volumen de tráfico global necesarios para extraer información relevante? ¿Está preparado para llevar a la práctica esta experiencia acumulada de modo que toda su base de clientes pueda aprovecharla en el caso de que se produzca un ataque, tanto antes de la amenaza como en el trascurso de la misma? ¿Dispone de un motor de análisis integral de big data para identificar a atacantes concretos que puedan tener un impacto en otros clientes?

5. **Reputación de IP.** ¿Qué fuentes usa el proveedor de seguridad en la nube para asignar una puntuación por reputación a las direcciones IP? Algunos productos que miden la reputación de las direcciones IP tienen distintos grados de calidad y emplean una puntuación de tipo binario para el riesgo, clasificada en "atacante" o "no atacante", en lugar de una variedad de puntuaciones en función de la actividad maliciosa registrada a lo largo del tiempo.

6. **Precisión.** Interpretar lo que cada proveedor de firewall de aplicaciones web (WAF) sostiene que ofrece no es tarea sencilla. No tiene sentido comparar los índices de precisión de dos proveedores distintos a menos que se apliquen los mismos criterios. Por tanto, deberá conocer qué es lo que se evalúa, quién lo evalúa y cuántas pruebas conforman el resultado final. En conclusión, asegúrese de no comparar peras con manzanas.

7. **Mejora continua.** La clave de la precisión reside en optimizar las reglas con regularidad para que se mantengan al día con respecto al tráfico en constante evolución. Averigüe con qué frecuencia evalúa el proveedor de seguridad en la nube su infraestructura de seguridad. ¿Lo hace mensual, semanal o diariamente? ¿Cuánto tráfico usa a efectos de pruebas?

8. **Tiempo de mitigación.** ¿Refleja el acuerdo de nivel de servicio (SLA) del proveedor un compromiso con la velocidad y la calidad de la mitigación, o solo un tiempo de respuesta? La mayoría de proveedores pueden prometer una respuesta en cuestión de minutos, pero eso solamente hace referencia a la investigación del problema. Los SLA que ofrecen una mitigación específica, garantizada contractualmente, son una buena métrica tangible en la que basarse para comparar la protección de forma más precisa.

9. **El factor humano (centros de operaciones de seguridad).** Muchos proveedores afirman poder protegerle con sus centros de operaciones de seguridad (SOC) de asistencia ininterrumpida. Sin embargo, es crucial saber exactamente cuántas instalaciones de seguridad en la nube tienen, dónde se encuentran y de qué personal disponen. ¿Cuántas personas están disponibles de forma simultánea? ¿Qué protocolos usan para garantizar cobertura entre turnos en el curso de un ataque?

10. **Defensa multicapa/defensa en profundidad.** Ninguna solución de seguridad es 100 % eficaz por sí sola. Si se combinan herramientas desarrolladas con la misma tecnología o hardware subyacente, se consiguen varias capas con las mismas debilidades o deficiencias de las que los atacantes pueden aprovecharse. El enfoque ideal consiste en superponer las mejores tecnologías, una sobre otra.

Cada vez son más las organizaciones que confían en la nube para protegerse en Internet. La seguridad basada en la nube ofrece mayor escalabilidad, más precisión y mejor rendimiento que las soluciones in situ por sí mismas. Para elegir una solución de seguridad en la nube que funcione correctamente con su infraestructura de seguridad existente deberá entender qué es lo que se le ofrece realmente.

Obtenga más información en el ebook gratuito de Akamai "Why Cloud? The Buyer's Guide to Cloud Security" (¿Por qué la nube? Guía de seguridad en la nube para compradores).