

4 elementos críticos que debe tener su próxima solución de seguridad



■ La seguridad es esencial para el éxito de cualquier negocio digital. Pero hay una cosa con la que siempre se debe contar: las amenazas relacionadas con la seguridad son inevitables. Y los resultados pueden ser devastadores. Las violaciones de seguridad erosionan la confianza y dañan la reputación.



Como CIO, CISO u otro líder en seguridad TI, es primordial mitigar el riesgo digital.

El objetivo, por tanto, consiste en encontrar la solución de seguridad más eficaz para cada empresa, una tarea que es más fácil decir que hacer.

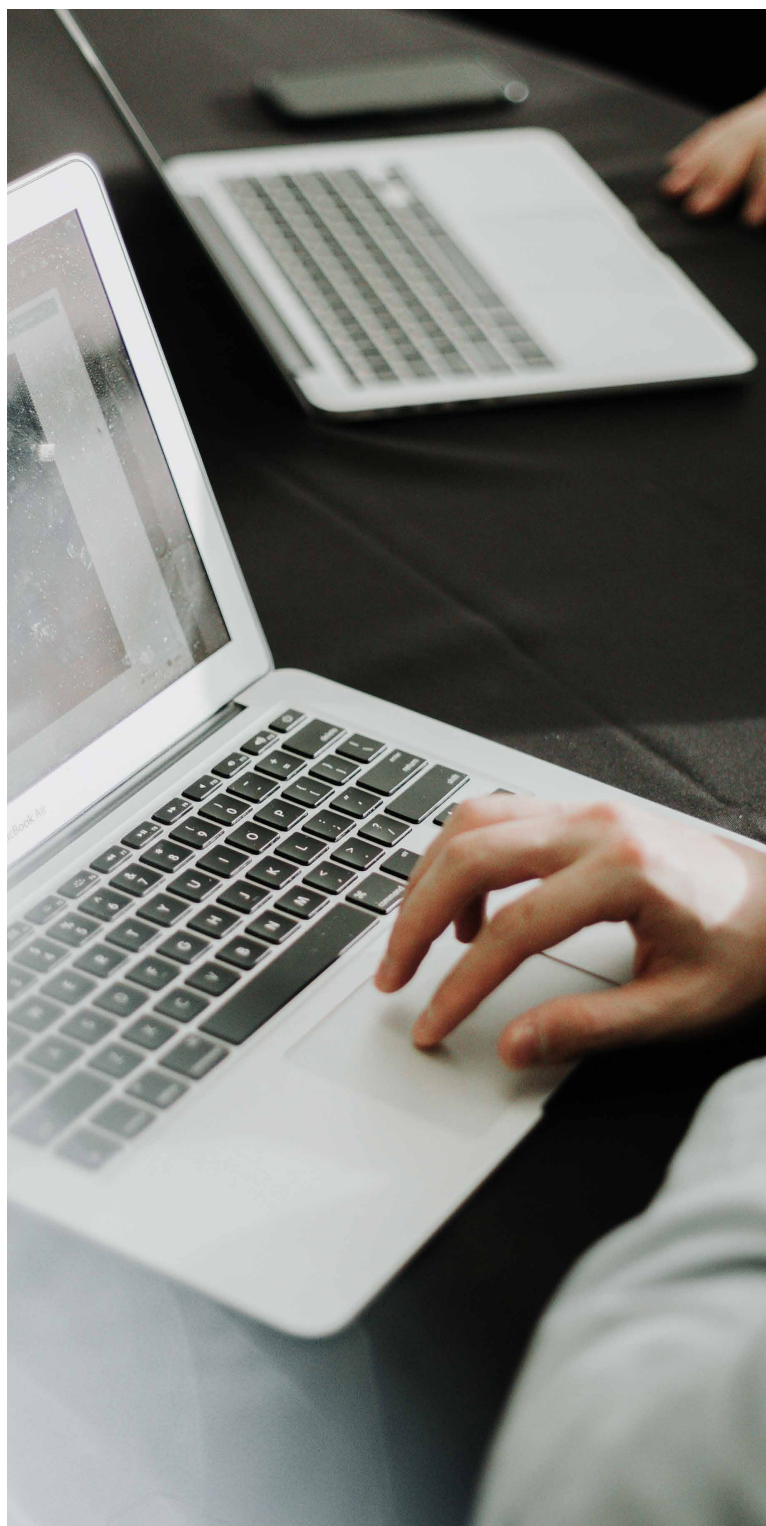
Al comenzar esta búsqueda, debemos concentrarnos en esos 4 elementos críticos que cualquier plataforma de seguridad de calidad debe ofrecer:



La Plataforma: El valor de una plataforma de seguridad depende de nosotros y de las necesidades de nuestro negocio. Debemos hacernos las siguientes preguntas para poder determinar los elementos críticos que una plataforma debe proporcionarnos: ¿Qué significa la plataforma de seguridad para mí, como líder en seguridad? ¿Qué capacidades me ofrece? ¿Me permite moverme más rápido? ¿Cómo está asegurando nuestros activos? ¿Es fácil (o difícil) de gestionar?

Servicio y asistencia: Nuestro proveedor debe contar con expertos en seguridad altamente capacitados que proporcionen un profundo análisis de amenazas y estrategias personalizadas. Para muchas organizaciones, la protección contra amenazas de seguridad de gran alcance y en constante evolución requiere algo más que tecnología.

Frente a objetivos comerciales muy competitivos y un presupuesto de TI limitado, es posible que simplemente no dispongamos del tiempo, los recursos o el personal experto necesarios para proporcionar la mejor seguridad para nuestros sitios web, aplicaciones y API. Los servicios de seguridad bien gestionados podrían ayudar a reducir el tiempo de respuesta y aumentar la calidad de la mitigación al aprovechar un enfoque colectivo entre nosotros y el proveedor.



Cumplimiento: Hay que asegurarse de que cualquier proveedor que estemos considerando cumpla estrictamente todas las regulaciones apropiadas para nuestro sector como por ejemplo el Reglamento General de Protección de Datos (RGPD) de la UE.

Por último, ¿la solución cubre todas las bases? Hay ciertas funciones que cualquier proveedor de seguridad debe dominar y dirigir para cubrir sus necesidades. Estos son los requisitos básicos que debemos tener en mente cuando nos sumerjamos en el proceso de seleccionar un proveedor:

Protección DDoS, seguridad de las aplicaciones y APIs, protección contra la suplantación de identidad (phishing), credential stuffing, protección contra bots, acceso seguro a aplicaciones y protección contra malware.

Los líderes en seguridad deben ayudar a dotar a su negocio digital de la mentalidad, los recursos y la planificación necesarios para hacer frente a las inevitables amenazas. La seguridad ya no es simplemente un centro de coste por tanto tenemos la responsabilidad de ayudar proactivamente a la transformación digital, y consolidarnos como la base del negocio y de la innovación en nuestra organización.

Fuente de información:
cybersecuritynews

