La confianza *cero* se convierte en un factor **clave en la gestión del riesgo** en la era digital

Managed secure IT | no matter what

En los viejos tiempos, antes de que golpeara la pandemia, los profesionales de la seguridad discutian los méritos relativos de los métodos de confianza cero frente a las estrategias más amplias de gestión de riesgos digitales. Pero en un mundo que se enfrenta al ritmo acelerado de la transformación digital, lo que comenzó como un debate filosófico ha adquirido mayor urgencia y claridad. En una época de proyectos e iniciativas digitales en rápida evolución, así como crisis, incertidumbre y cambios agudos sin precedentes, ahora es el momento ideal para adoptar una mentalidad de confianza cero y adoptar muchos de sus ingredientes clave para avanzar en una estrategia más amplia de gestión de riesgos digitales.

¿Cómo llegamos aquí?

¿Por qué la confianza cero se convirtió en el nuevo mantra de seguridad?

La respuesta breve a cómo la confianza cero llegó a ser tan ampliamente aceptada es que **COVID-19 obligó a las empresas a adaptar sus agendas de transformación digital.**

Si bien muchos líderes de riesgos y seguridad ingresaron a la nueva década con planes de ejecución detallados que respaldan estrategias de gestión de riesgos digitales bastante sofisticadas, 2020 tenía otros planes. De repente se suspendieron los presupuestos, se cancelaron los proyectos. **La atención se centró en clasificar y mitigar las interrupciones que estaban experimentando las operaciones, los empleados, los socios y los clientes. Acelerar rápidamente y de forma segura determinadas soluciones digitales se convirtió en la tarea de 2020.** Cuando nos enfrentamos a la inevitable pregunta "¿Cómo vamos a conseguir esto?" ... la confianza cero ha surgido como una respuesta expedita y aparentemente irrefutable.

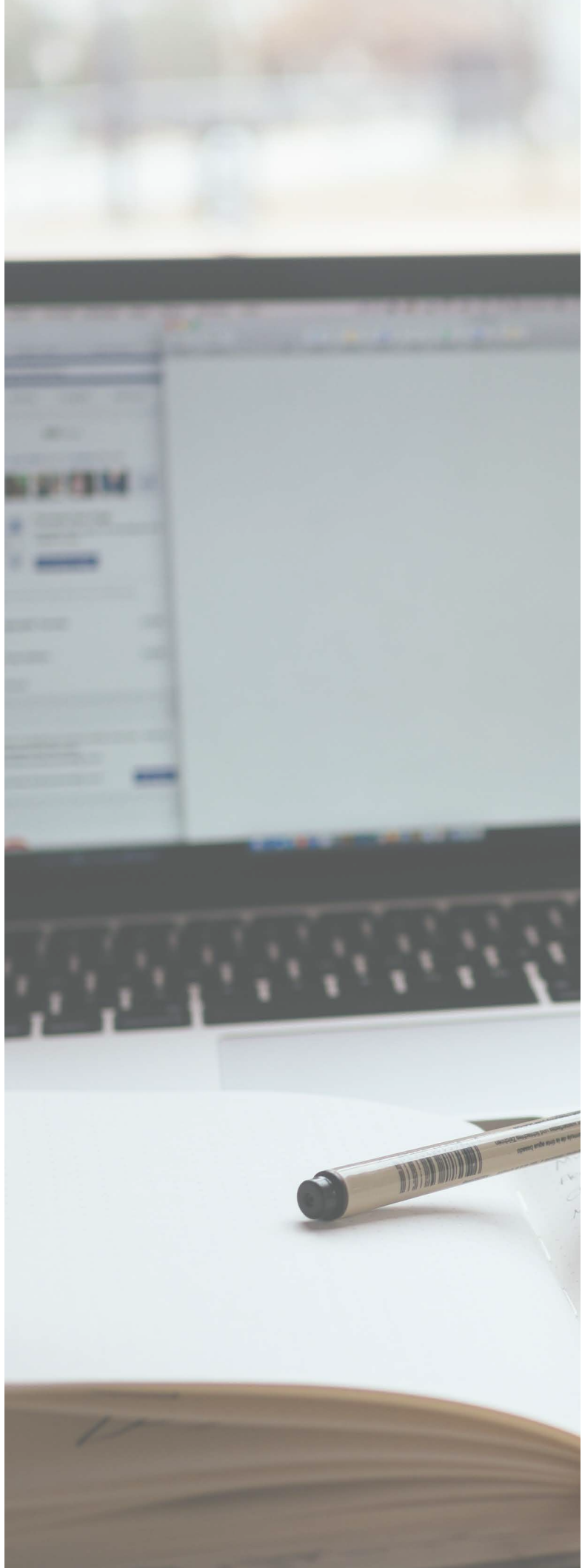
Los principios clave de la confianza cero, tal como los definió Forrester hace una década, parecen lo suficientemente simples de comprender y prescribir cuando se agrega rápidamente inventario digital

Se accede a todos los recursos de manera segura, independientemente de la ubicación (implica autenticación y cifrado sólidos y de múltiples factores).
El control de acceso se basa en la necesidad de conocer y se aplica estrictamente (implica aplicar principios de acceso con privilegios mínimos, gobernanza de identidad, VLAN, infraestructura definida por software, microsegmentación, etc.)

Inspeccione y registre todo el tráfico (implica que los SIEM examinen los registros y paquetes que atraviesan puntos finales, IoT, nube, SaaS, PaaS, etc.)

Pero cuando se considera completamente la amplitud del ecosistema digital empresarial, los desafíos de escalar este enfoque en su totalidad pueden volverse desalentadores. **¿Es realmente posible "No confiar nunca" en todos los dispositivos? ¿Es realmente posible "Verificar siempre" el acceso a toda la infraestructura? En realidad, probablemente no.** Este fue el quid del argumento de la gestión de riesgos digitales frente a la confianza cero del pasado.

Aceptemos que la implementación amplia de confianza cero puede llevar algún tiempo. Aceptemos también que, ahora más que nunca, **los equipos de seguridad deberán priorizar proyectos clave para mantener la continuidad del negocio y proteger sus operaciones. Incluso un cambio inmediato o gradual a la confianza cero puede tener grandes beneficios:**



1. El primer paso para adoptar la confianza cero es identificar los elementos fundamentales necesarios para hacerlo realidad.

La implementación de los componentes lógicos para la confianza cero no debería obligar a una gran actualización de la infraestructura de seguridad empresarial, siempre y cuando las plataformas IAM y SIEM existentes ofrezcan las capacidades necesarias.

Fuente de información:
www.rsa.com