CLOUDFLARE

DOCUMENTO TÉCNICO

Un horizonte esperanzador

Cómo posicionarse mejor en cuanto a la ciberseguridad en tiempos de incertidumbre económica

Contenido

Resumen ejecutivo

Las organizaciones están enfrentando un período de incertidumbre económica a medida que el panorama se vuelve cada vez más impredecible. Esta incertidumbre — a menudo representada por presupuestos más reducidos — presiona a los directores de información y a los directivos técnicos para que encuentren nuevas salidas.

Afortunadamente, los directivos que tienen estrategias para sortear el temporal mediante el reajuste del presupuesto, la redefinición de procesos para lograr mayor eficiencia y la continuidad de un crecimiento planificado sin un aumento sustancial de los recursos aún pueden estar bien posicionados una vez que pase el período de incertidumbre.

En las siguientes secciones, definiremos y ampliaremos los diversos factores que propician estas circunstancias y las condiciones de mercado. A partir de estas ideas, delineamos cinco pasos que los directivos pueden seguir para buscar oportunidades que mejoren la eficiencia en las prácticas de seguridad sin arriesgar su postura de seguridad. Al alinear la estrategia de infraestructura de TI para el nuevo entorno económico, los directivos pueden preparar a sus organizaciones para tener éxito en el futuro.

Introducción

En los últimos años, los directivos de TI han estado lidiando con una crisis tras otra en la planificación y ejecución de sus estrategias. Han tenido que reaccionar ante una pandemia a nivel mundial y sus efectos secundarios, fallas en la cadena de suministro, un conflicto creciente en Europa del este y lo que puede evolucionar como una recesión. Según el economista de Stanford Paul Romer, “Nunca se debe desperdiciar una crisis” (fuente). Las decisiones que tomaron los directores de información (CIO) para apoyar el trabajo remoto tendrán beneficios duraderos e imprevistos para hacer que el lugar de trabajo sea atractivo. De igual modo ahora que los directivos enfrentan un panorama económico cada vez peor, las opciones que elijan en cuanto a seguridad, redes, acceso remoto, almacenamiento, desarrollo e infraestructura les ayudarán a emerger con mayor solidez y a estar mejor posicionados para lograr un crecimiento seguro y sostenible en el futuro.

El aumento del trabajo remoto trajo aparejado un auge de ransomware y de sofisticadas amenazas cibernéticas que establecieron nuevos parámetros en cuanto al impacto en los ingresos, escala y sofisticación (fuente). La desaparición de lo que quedaba del perímetro de la red, junto con el histórico aumento de la rotación de empleados, generó fallas en la seguridad y demoras en los proyectos de TI estratégicos. Esto obligó a las organizaciones a repensar no solo su método para contratar y retener personal, sino también el método para controlar el acceso a sus sistemas y equipos. Si bien debido a la pandemia aumentó considerablemente el nivel de ciberdelito (fuente), la situación también alertó a las organizaciones y a sus juntas en cuanto a la necesidad urgente de contar con un sistema de ciberseguridad efectivo. Ahora es el momento de que las organizaciones consideren un enfoque más estratégico a largo plazo para tener una infraestructura de trabajo segura, productiva e híbrida

A continuación, te ofrecemos cinco consejos para reducir el riesgo de tu negocio sin gastar demasiado dinero y mejorar la capacidad de la organización para lidiar con las amenazas que se avizoran en el horizonte:

1. Auditar las herramientas de seguridad existentes para descubrir funciones que se superponen

Las organizaciones tienen mucho para ganar si consolidan a los proveedores de seguridad. Si bien ninguna herramienta individual será nunca la "solución milagrosa" que a los directivos de seguridad de la información (CISO) les gustaría tener, muchos operadores de seguridad creen que sus compañías está desperdiciando dinero en demasiadas herramientas que no les ofrecen una protección óptima. Tener múltiples herramientas de varios proveedores significa que tus empleados deben desperdiciar un tiempo valioso en la adquisición, implementación, gestión, resolución de problemas y soporte de una gran cantidad de sistemas desconectados – en lugar de proteger tu infraestructura y tus datos. En realidad, una encuesta de junio de 2022 que se llevó a cabo en la Conferencia Anual de RSA reveló que "la mitad (53 %) de las empresas que respondieron creen que han desperdiciado más del 50 % de su presupuesto de ciberseguridad y siguen sin poder resolver el problema de las amenazas. Cuarenta y tres por ciento de los que respondieron la encuesta dijeron que el principal desafío que enfrentan en cuanto a la detección y solución de amenazas es el exceso de herramientas, mientras que el 10 % de las organizaciones carece de herramientas efectivas para solucionar las amenazas de ciberseguridad" (fuente). Si tuvieras que eliminar incluso unas cuantas de esas herramientas, podrías mejorar la seguridad y al mismo tiempo ahorrar un tiempo valioso para los empleados.

Al hacer un cambio en las inversiones, de gastos de capital a gastos operativos, también puedes lograr mejoras inmediatas para obtener un flujo de caja a corto plazo y evitar quedar atrapado en inversiones de capital de varios años que entorpecen la agilidad del negocio. Una forma de simplificar es depender menos del hardware tradicional. El cambio de módulos heredados a soluciones como servicio puede ayudar a garantizar que tus iniciativas de mayor prioridad sigan recibiendo financiación, incluso si tu presupuesto se reduce. Adquirir el modelo como servicio también significa que te beneficias de manera intrínseca con los ciclos de innovación más rápidos de software y eliminas las molestias inevitables de los frecuentes parches del hardware heredado. Deshacerse de los parches y de las actualizaciones permite que tus equipos se concentren en las actividades que marcan realmente una diferencia en tu negocio. Para hacer frente a la incertidumbre, la simplificación estratégica y la consolidación ayudan a lograr el éxito a largo plazo.

2. Concentrarse en los datos, no solo en las herramientas

Los equipos directivos deben considerar un cambio de enfoque para integrar mejor no solo las herramientas sino también los datos en todas las herramientas de seguridad para detectar mejor los patrones y las anomalías. Históricamente, los equipos de seguridad han seguido agregando cada vez más herramientas sin considerar los impactos en el largo plazo de tener tantos conjuntos de datos en demasiados lugares. El resultado suele ser un conjunto fragmentado de productos con prácticamente nada de interoperabilidad y con opacidad en los datos, lo que da como resultado una información menos valiosa, con menores niveles de precisión y mayores oportunidades de errores humanos. Por no mencionar todo el tiempo que le lleva al equipo extraer múltiples conjuntos de datos, combinarlos y ejecutar búsquedas, que no solo es una pérdida de tiempo sino también de recursos. Esos recursos, podrían utilizarse para iniciativas comerciales más estratégicas.

Si bien los equipos pueden encontrar soluciones alternativas creativas para resolver los desafíos de interoperabilidad, como la fusión manual de conjuntos de datos o la importación y la exportación de CSV, es importante considerar que, dejando la eficiencia de lado, el valor de las herramientas de seguridad está en los datos que estos sistemas asimilan, crean y ponen a disposición para la protección. Si tus datos están en todas partes - no clasificados, sin protección y no se gestionan con cuidado - puede haber desviaciones que de otro modo podrían habría sido información de gran impacto obtenida de estos datos, especialmente si hay datos en instancias de shadow IT que podría haber sido totalmente omitida. Al consolidar los conjuntos de herramientas y al considerar cuidadosamente la interoperabilidad de tus herramientas de seguridad, tienes la capacidad para reducir los errores humanos y proteger mejor tus datos. Porque aunque hayas invertido en las mejores herramientas que están disponibles en la actualidad, los conjuntos de datos en silos y los conjuntos de datos shadow dan como resultado información menos valiosa.

En cuanto a la eficiencia, es importante considerar que en la era del Zero Trust (“nunca confiar, siempre verificar”), una mayor cantidad de herramientas significa que los equipos dedican más tiempo a iniciar sesión, autenticar y obtener acceso a los sistemas antes de comenzar a hacer su trabajo. Cuanto menos sistemas un empleado debe tocar, más tiempo ahorra y más rápido se puede mover. Es de una importancia fundamental considerar que los datos dentro de estos sistemas, y la cantidad de sistemas a los que deben acceder para completar una determinada tarea, es lo que en última instancia permitirá o impedirá a los equipos responder, en lugar de reaccionar, ante las amenazas de manera inmediata.

3. Considerar a la nube como modelo de servicio para maximizar la innovación y minimizar la complejidad

Todos los negocios deben innovar para mantener la competitividad, pero las empresas que no están en el negocio de la ciberseguridad no tienen el tiempo, el presupuesto ni los recursos para mantenerse al tanto de lo más actualizado en cuanto a vulnerabilidades y exposiciones comunes (CVE), de las tendencias de ataques y de los parches críticos que se necesitan para mantener la seguridad de toda su infraestructura. La adopción de los modelos como servicio, donde sea posible, permiten a los líderes beneficiarse de las innovaciones constantes sin tener que preocuparse de elegir las soluciones más adecuadas o de tomar decisiones difíciles en cuanto a la deuda técnica.

También es importante tener en cuenta que algunos servicios de seguridad cobran cargos por excedente si se sobrepasan las limitaciones de tráfico y algunos cobran cargos por ancho de banda. Considera hacer un análisis exhaustivo de lo que tu organización está pagando por mes o por año para saber si estás pagando demasiado. Si estás pagando demasiado, puedes aprovechar la oportunidad para buscar otras soluciones que no cobren cargos por excedente, para que no solo te permita ahorrar dinero, sino también a tener un gasto más previsible en el largo plazo, lo que permite a tu equipo planificar mejor para el futuro.

Los servicios de esta naturaleza ofrecidos en la nube también permiten que tu organización pueda ampliarse o reducirse según sea necesario, sin tener que arriesgar gabinetes de hardware costosos y sin tener que pasar por la compleja gestión del ciclo de vida útil que esto trae aparejado. En tiempos de incertidumbre, los negocios deben mantenerse ágiles y atentos a las condiciones cambiantes del mercado. Cuando el flujo de caja es una preocupación, la habilidad de minimizar costos o eliminarlos de raíz es una ventaja estratégica que puede marcar la diferencia entre apenas sobrevivir y progresar, independientemente de las condiciones del mercado.

4. Mejorar el nivel de experiencia de tus empleados

Según Forbes, "Nuestra encuesta reveló que los procesos de inicio de sesión complejos y de muchos pasos frustran a los trabajadores, les hacen perder tiempo, entorpecen la productividad y hacen que no cumplan con tareas esenciales relacionadas con el trabajo...Y la gran ironía es que casi el 40 % de los trabajadores dijo haber aplazado, delegado u omitido completamente la configuración de nuevas aplicaciones de seguridad en el trabajo debido a los engorrosos procesos de inicio de sesión. Es como querer proteger tu casa con la puerta más sólida, más alta y más segura que puedas comprar—reforzada con dragones que emiten rayos láser—y la dejas sin llave por la noche". No solo resulta ineficiente y difícil para la protección hacer un seguimiento de qué herramientas tienen cada función, sino que demasiados paneles de control y demasiados lugares con datos almacenados pueden generar mayores riesgos de seguridad y brechas de visibilidad para la organización. Las compañías que quieren ir un paso por delante de las amenazas de ciberseguridad deben tener en cuenta que cada clic y cada tecla pulsada implican un tiempo valioso, energía y distracción que no permite responder adecuadamente ante eventos críticos. Para que los empleados tengan una experiencia más optimizada y simplificada, es fundamental que los directivos analicen bien cuántas herramientas de protección necesitan para hacer su trabajo de manera efectiva y también qué se puede eliminar o consolidar para reducir el tiempo que la protección tarda en responder, no solo reaccionar, ante un hecho de seguridad crítico.

Cuando se trata de empleados no técnicos o empleados que no están en roles de protección, también es importante tener en cuenta que a medida que los trabajadores remotos tratan de acelerar su productividad personal, es probable que recurran al shadow IT o a métodos de soluciones alternativas. Si bien los controles Zero Trust han ofrecido un camino prometedor para el futuro para construir organizaciones más seguras, especialmente en entornos remotos, no se puede negar que no todos los enfoques Zero Trust son iguales. Cuanto más complejo resulta para un empleado acceder a lo que necesita, más probabilidades hay de que busque una manera de esquivar los controles de seguridad en lugar de cumplir con esos controles. Los directivos deben tratar de entender no solo la efectividad de los productos de seguridad, sino que también deben tener en cuenta cuán fáciles son de usar, ya que no tener en cuenta la experiencia del empleado aumenta el riesgo de la organización en general.

5. Buscar servicios de seguridad que no pongan en riesgo el rendimiento de la red

No solo se trata de las herramientas, sino de cómo las configuras y las gestionas para poder marcar la diferencia. Pide a tus equipos que hagan una auditoría de las configuraciones y de los ajustes actuales para detectar oportunidades que puedan ayudar a mejorar el rendimiento. Si no es posible mejorar el rendimiento, considera la posibilidad de buscar soluciones que se centren desde un principio en el rendimiento – ya que tener en cuenta el rendimiento como algo adicional en raras ocasiones permite que los directivos logren los objetivos que desean. Cuando se trata del rendimiento de la red, es importante tener en cuenta que una arquitectura deficiente no puede ser descodificada. Al igual que los planos de un edificio tienen oportunidades limitadas para el rediseño, una vez que se han establecido las bases, las redes deben ser diseñadas desde cero para obtener un máximo rendimiento.

La posibilidad de aprovechar el poder de una red perimetral global que procese y gestione los datos lo más cerca posible del origen brindará a las organizaciones una ventaja estratégica, tanto en la actualidad como en el futuro. Según MIT Technology Review, “El procesamiento de volúmenes de datos puede generar problemas de rendimiento. Como respuesta, muchas organizaciones están recurriendo al edge computing, que procesa los datos cerca del origen para permitir análisis y respuestas rápidos y en tiempo real, y al mismo tiempo mantener las privacidad y cumplir con los requisitos de seguridad” (fuente). Al elegir de manera estratégica soluciones que ya están integradas en las arquitecturas del futuro, puedes dar a tus equipos la ventaja estratégica de un mejor rendimiento de red sin arriesgar los elementos críticos de la privacidad y la seguridad.

En resumen, estos son los pasos que puedes seguir para posicionarte mejor en cuanto a la ciberseguridad en tiempos de incertidumbre económica:

1. **Auditar las herramientas de seguridad existentes para descubrir funciones que se superponen**
   - Consolidar las herramientas que se superponen
   - Cambiar las inversiones de gastos de capital a gastos operativos
2. **Concentrarse en los datos, no solo en las herramientas**
   - La interoperabilidad de las herramientas permite obtener conjuntos de datos mejores y más precisos
   - Los conjuntos de datos y los informes más precisos permiten obtener mejor información, lo cual es fundamental para lograr los objetivos comerciales
3. **Considerar a la nube como modelo de servicio para maximizar la innovación y minimizar la complejidad**
   - Si no estás en el negocio de la ciberseguridad, puedes obtener muchas ventajas si te deshaces de los parches, del mantenimiento y de las actualizaciones de las ofertas como servicio
   - La nube y los modelos como servicio ofrecen la flexibilidad que necesitas para actuar de manera ágil en un entorno económico fluctuante
4. **Mejorar el nivel de experiencia de tus empleados**
   - Demasiadas herramientas en demasiados lugares pueden crear puntos ciegos en cuanto a la seguridad y generar frustración entre los empleados - la consolidación y la simplificación ayudarán a optimizar sus experiencias
   - La optimización para facilitar el uso del sistema a los empleados ayudará a retener los empleados y evitará que recurran al shadow IT para completar sus trabajos
5. **Buscar costos ocultos y oportunidades para mejorar el rendimiento dentro de la variedad de tus herramientas de ciberseguridad actuales**
   - Auditar las herramientas existentes para detectar oportunidades que permitan optimizar el rendimiento, pero se debe tener en cuenta que no se puede optimizar una arquitectura deficiente
   - La adopción de herramientas a escala global que están lo más cerca posible de los clientes permitirá que tu organización ofrezca una experiencia al cliente superior y segura

Cómo puede ayudarte Cloudflare

Cloudflare se lanzó en 2010, tras la crisis económica de 2008, para liderar la transformación de la infraestructura local hacia la nube. Diseñamos la plataforma de Cloudflare con un osado objetivo: ayudar a mejorar Internet. La oferta de productos de Cloudflare protege y acelera cualquier recurso que esté conectado a Internet sin necesidad de añadir hardware, instalar software o cambiar líneas de código.

El tráfico web de las propiedades de Internet que utilizan tecnología de Cloudflare se enruta a través de nuestra red global inteligente que aprende de las solicitudes que recibe. Ayudamos a nuestros clientes a trabajar de manera más inteligente, diseñar mejor, funcionar con mayor rapidez y crecer de manera segura. En la actualidad, Cloudflare protege y acelera millones de propiedades de Internet.

Control

Benefíciate de la eficacia de una red global integrada que ofrece conectividad, seguridad y procesos integrales otorgándote el control de las políticas.

Flexibilidad

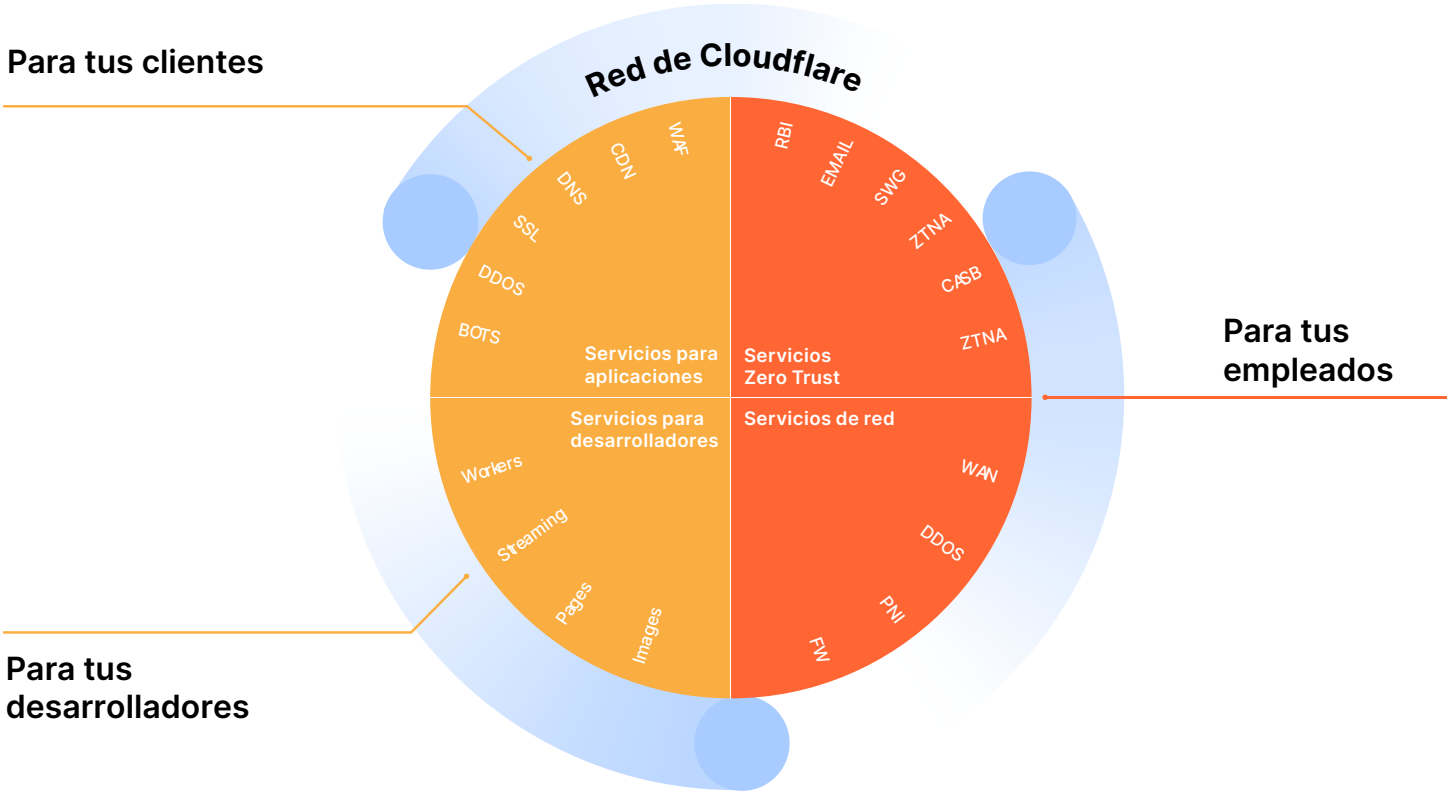
Con los servicios nativos en la nube, no necesitas hacer inversiones iniciales de gasto de capital. Incrementa o disminuye fácilmente el uso en consonancia con las fluctuaciones de tu negocio.

Previsibilidad

Facturación previsible – sin costos inesperados, como tasas de salida ilimitadas. Sin necesidad de invertir ahora en hardware que se entregará el año próximo.

La red global de Cloudflare garantiza la seguridad, la privacidad, la rapidez y la fiabilidad de todo lo que conectes a Internet.

- Protege tus sitios web, API y aplicaciones de Internet
- Protege tus redes corporativas, empleados y dispositivos
- Escribe e implementa el código que se ejecuta en el perímetro de la red



Acerca de Cloudflare

Cloudflare se lanzó en 2010 para liderar la transformación de la infraestructura local hacia la nube. Diseñamos la plataforma de Cloudflare desde cero con una comprensión total de nuestro osado plan: ayudar a mejorar Internet. Nuestra oferta de productos protege y acelera cualquier aplicación de Internet sin necesidad de agregar hardware, instalar software o cambiar líneas de código.

El tráfico web de las propiedades de Internet que utilizan tecnología de Cloudflare se enruta a través de una red global inteligente que aprende de las solicitudes que recibe. Ayudamos a nuestros clientes a trabajar de manera más inteligente, diseñar mejor, funcionar con mayor rapidez y crecer de manera segura. En la actualidad, Cloudflare protege y acelera millones de propiedades de Internet.

Para obtener más información, visita www.cloudflare.com

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/

REV:BDES-4327.2023MAR10