CLOUDFLARE

DOCUMENTO TÉCNICO

La esperanza en el horizonte: Cómo mejorar la postura de ciberseguridad durante la incertidumbre económica

Contenido

Resumen ejecutivo

Las organizaciones afrontan la incertidumbre económica mientras las perspectivas son cada vez mas imprevisibles. Esta incertidumbre (que se refleja a menudo en presupuestos cada vez más pequeños) implica aún más presión sobre los directores de informática y los responsables técnicos para que encuentren nuevos caminos a seguir.

Por suerte, aquellos que desarrollen estrategias para capear el temporal mediante la adaptación proactiva de los presupuestos, la redefinición de los procesos para mejorar la eficacia y la planificación continuada del crecimiento sin un incremento considerable de los recursos pueden seguir encontrándose bien posicionados cuando el clima de incertidumbre se disipe.

En las siguientes secciones, definiremos y ampliaremos los diversos factores que propician estas circunstancias y condiciones de mercado. A partir de estos conocimientos, definimos cinco medidas que los responsables de TI pueden adoptar para buscar oportunidades a fin de mejorar la eficiencia de sus prácticas de seguridad sin poner en riesgo su postura de seguridad. Al adaptar la estrategia de la infraestructura de TI al nuevo entorno económico, pueden garantizar el éxito de sus organizaciones a largo plazo.

Introducción

Durante los últimos años, los responsables de TI se han tenido que enfrentar a una crisis tras otra mientras planificaban y ejecutaban su estrategia. Han tenido que reaccionar a una pandemia global y a sus efectos secundarios, a desabastecimientos en la cadena de suministro, a la escalada bélica en Europa oriental, y a lo que podría llegar a ser una recesión. En palabras de Paul Romer, economista de Stanford, "Es terrible desperdiciar una crisis" (fuente). Las decisiones que tomen los directores de informática para ayudar a sus trabajadores remotos tendrán beneficios imprevistos y a largo plazo para que sus lugares de trabajo sean más atractivos para permitir el trabajo remoto. Ahora, de la misma forma, cuando los responsables de TI afrontan unas perspectivas económicas cada vez peores, las decisiones que tomen acerca de la seguridad, la red, el acceso remoto, el almacenamiento, el desarrollo y la infraestructura les ayudarán a salir fortalecidos y mejor posicionados para un crecimiento seguro y sostenible en el futuro.

El auge del trabajo remoto vino acompañado por el incremento de las amenazas de ransomware y otras sofisticadas ciberamenazas, que marcaron nuevos referentes en lo que respecta al impacto en los ingresos, la escala y la sofisticación (fuente). La desaparición de lo que quedaba del perímetro de red, junto con incrementos históricos de la rotación de empleados, conllevó vulnerabilidades de seguridad y retrasos en proyectos de TI estratégicos. Esto obligó a las organizaciones a reconsiderar su enfoque no solo de la contratación y la retención, sino también de cómo controlar el acceso a sus sistemas y máquinas. La pandemia generó un drástico crecimiento de los crímenes electrónicos (fuente). Sin embargo, también abrió los ojos a las organizaciones y a sus directivos acerca de la necesidad urgente de una ciberseguridad eficaz. Ahora es el momento de que las organizaciones adopten un enfoque más estratégico a la carrera de fondo que representa la implementación de una infraestructura de trabajo híbrido segura, productiva y disponible.

A continuación, te proponemos cinco medidas que puedes adoptar para eliminar el riesgo de tu empresa sin salirte de tu presupuesto, y para mejorar la capacidad de tu organización para gestionar las nuevas amenazas en el horizonte:

1. Audita las herramientas de seguridad existentes para descubrir las funcionalidades que se solapan

Las organizaciones pueden conseguir importantes ventajas si consolidan sus proveedores de seguridad. Aunque ninguna herramienta por sí sola nunca será la solución "milagrosa" que les gustaría tener a los directores de seguridad de la información, muchos operadores de seguridad han expresado su convicción de que su empresa está malgastando dinero en demasiadas herramientas que no les ofrecen una protección óptima. La compatibilidad con múltiples herramientas de distintos proveedores significa que tus empleados dedican un tiempo valioso a la adquisición, la implementación y la resolución de problemas, así como al soporte de un gran número de sistemas desconectados, en lugar de dedicarse a proteger tu infraestructura y tus datos. De hecho, una encuesta de junio de 2022 realizada en la conferencia anual de RSA reveló que "la mitad (53 %) de las empresas encuestadas creían que habían desperdiciado más del 50 % de su presupuesto en ciberseguridad y que aún no habían solucionado las amenazas. El 43 % de los encuestados indicaron que su principal desafío en materia de detección y corrección de amenazas es una sobreabundancia de herramientas, mientras que el 10 % de las organizaciones carecen de las herramientas eficaces para corregir las amenazas de ciberseguridad" (fuente). Si prescindieras de solo algunas de esas herramientas, podrías mejorar la seguridad, al mismo tiempo que ahorrarías un valioso tiempo de los empleados.

Si pasas de invertir en gastos de capital a invertir en gastos operativos, también puedes obtener mejoras inmediatas del flujo de caja a corto plazo, y evitar depender de inversiones de capital mutianuales que obstaculizan la agilidad empresarial. Una forma de simplificar es reducir la dependencia del hardware tradicional. El cambio de módulos heredados por soluciones como servicio puede ayudar a garantizar que tus iniciativas de mayor prioridad sigan recibiendo financiación, incluso si tu presupuesto se reduce. Si adquieres un modelo como servicio, también te beneficias de ciclos de innovación de software inherentemente más rápidos y eliminas los inevitables quebraderos de cabeza que supone el hardware heredado, al que es necesario aplicar parches con frecuencia. Si liberas a tus equipos de la carga que supone la aplicación de parches y la innovación, pueden centrar su atención en actividades que realmente marquen la diferencia para tu empresa. En tiempos de incertidumbre, la simplificación y la consolidación estratégicas pueden ayudarte a lograr el éxito a largo plazo.

2. Centra tu atención en los datos, no solo en las herramientas

Los equipos directivos deben considerar la opción de empezar a centrar su atención en la integración no solo de las herramientas, sino también de los datos, de todo su conjunto de herramientas de seguridad, a fin de descubrir los patrones y las anomalías existentes. Históricamente, los equipos de seguridad han seguido añadiendo cada vez más herramientas a lo largo del tiempo, sin considerar las consecuencias a largo plazo de tener demasiados conjuntos de datos en demasiadas ubicaciones. A menudo, el resultado es una amalgama de productos con poca o ninguna interoperabilidad y sin transparencia de datos. Esto genera conocimientos más deficientes y niveles más bajos de precisión, puesto que crea nuevas oportunidades de errores humanos. Por no hablar de que la gran cantidad de tiempo que puede necesitar el equipo para obtener los distintos conjuntos de datos, fusionarlos y ejecutar las consultas supone no solo una pérdida de tiempo, sino también un desperdicio de recursos. En su lugar, estos recursos podrían centrarse en iniciativas empresariales más estratégicas.

Es posible que los equipos puedan encontrar soluciones creativas para resolver los desafíos de la interoperabilidad, como por ejemplo la fusión manual de los conjuntos de datos o la importación y la exportación de los archivos CSV. Sin embargo, es importante considerar que, al margen de la eficiencia, el valor de las herramientas de seguridad radica en los datos que estos sistemas consumen, crean y ponen a disposición de los responsables de la protección. Si tus datos están en todas partes (sin clasificar, sin protección y sin una gestión adecuada), pueden crear sesgos en lo que de otra forma podrían haber sido conocimientos de gran impacto derivados de dichos datos, en especial si hay datos en instancias de Shadow IT que es posible que hayan quedado completamente olvidados. Si consolidas las herramientas y reflexionas acerca de la interoperabilidad de tu conjunto de soluciones de seguridad, puedes reducir los errores humanos y proteger mejor tus datos. Porque, incluso si has invertido en las mejores herramientas disponibles actualmente, los conjuntos de datos aislados y los "datos en la sombra" generan conocimientos más deficientes.

En términos de eficiencia, es importante considerar que, en la era de Zero Trust ("Nunca confíes, verifica siempre"), más herramientas significa que los equipos también deben dedicar más tiempo a iniciar sesión, autenticarse y obtener acceso en los sistemas antes de poder empezar realmente a realizar su trabajo. Cuantos menos sistemas deban utilizar los empleados, más tiempo ahorrarán y más rápido podrán moverse. Es primordial tener en cuenta que los datos en estos sistemas, así como a cuántos sistemas deben acceder para completar una tarea determinada, es, en ultima instancia, lo que permitirá o impedirá a los equipos responder, en lugar de reaccionar, a las amenazas de manera oportuna.

3. Considera utilizar modelos en la nube y como servicio para maximizar la innovación y minimizar la complejidad

Todas las empresas necesitan innovar para seguir siendo competitivas, pero aquellas que no se dedican específicamente a la ciberseguridad no tienen el tiempo, el presupuesto o los recursos para mantenerse al día sobre los últimos CVE, las tendencias de ataques y los parches fundamentales para proteger toda su infraestructura. La adopción de modelos como servicio, allí donde sea posible, permite a los responsables de TI beneficiarse de la innovación continua sin tener que preocuparse acerca de las contrapartidas o de decisiones difíciles relacionadas con la deuda técnica.

También es importante considerar que algunos servicios de seguridad cobran sobrecargos cuando se sobrepasan las limitaciones de tráfico, y algunos cobrarán tarifas de ancho de banda. Considera analizar detalladamente lo que paga tu organización mensual o anualmente para comprender si estás pagando más de lo que crees. Si es así, puedes aprovechar esa oportunidad para buscar otras soluciones que no cobren tarifas adicionales y que te ayuden no solo a ahorrar dinero, sino también a tener un gasto más previsible a lo largo del tiempo, lo que permitirá a tu equipo una mejor planificación de cara al futuro.

Este tipo de servicios proporcionados en la nube también permite que tu organización adapte su crecimiento a las necesidades, sin compromisos de hardware caro ni todas las dificultades de la gestión del ciclo de vida que esto implica. En tiempos de incertidumbre, las empresas deben mantenerse ágiles y responder rápidamente a las condiciones cambiantes del mercado. Cuando el flujo de caja es una preocupación, la capacidad de minimizar los costes o de eliminarlos por completo es una ventaja estratégica que puede marcar la diferencia entre apenas sobrevivir y progresar, independientemente de las condiciones del mercado.

4. Mejora la experiencia de tus empleados

Según Forbes, "Nuestra encuesta reveló que los procesos de inicio de sesión complejos y de varios pasos frustran a los trabajadores, les hacen perder el tiempo, obstaculizan la productividad y les impulsan a abandonar tareas laborales fundamentales... La gran ironía es que casi el 40 % de los trabajadores declararon que habían aplazado, delegado u omitido por completo configurar nuevas aplicaciones de seguridad en el trabajo debido a los engorrosos procesos de inicio de sesión. Es como si proteges tu casa con la verja más sólida, alta y segura que puedes comprar (fortificada con dragones que lancen rayos láser por la boca) pero la dejas abierta por la noche". Para los responsables de la protección, el seguimiento de qué herramienta contiene qué función es ineficaz y difícil. Además, para cualquier organización, demasiados paneles de control y demasiadas ubicaciones de datos pueden crear mayores riesgos de seguridad y deficiencias de visibilidad. Las empresas que deseen anticiparse a las amenazas de ciberseguridad deben tener presente que cada clic y cada pulsación de tecla requiere un tiempo valioso y energía, y desvía la atención de la respuesta a los eventos críticos. Para crear una experiencia mejor y más simplificada para los empleados, es fundamental que los directivos analicen detalladamente cuántas herramientas necesitan utilizar los responsables de la seguridad para realizar su trabajo con eficacia, así como de qué pueden prescindir o qué pueden consolidar para reducir el tiempo necesario para responder, no solo reaccionar, a un evento de seguridad crítico.

Cuando se trata de empleados no técnicos o de aquellos que no desempeñan roles de protección, también es importante valorar que los empleados remotos desean acelerar su productividad personal. Pueden recurrir a Shadow IT o a métodos alternativos. Aunque los controles Zero Trust han proporcionado un prometedor camino a seguir para el desarrollo de organizaciones más seguras, especialmente en un entorno remoto, es evidente que no todos los enfoques Zero Trust se crean de la misma forma. Cuanto más complejo sea para un empleado acceder a lo que necesita, más probable es que encuentre una forma de sortear los controles de seguridad. Los responsables de TI deben comprender no solo la eficacia de los productos de seguridad, sino también considerar la facilidad de uso, puesto que si no prestas atención a la experiencia de los empleados, aumentas el riesgo global de tu organización.

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

Lo que puede marcar la diferencia no es solo las herramientas, sino también cómo las configuras y gestionas. Considera la posibilidad de que tus equipos lleven a cabo una auditoría de las configuraciones y las personalizaciones actuales para descubrir oportunidades que puedan ayudar a mejorar el rendimiento. Si no es posible mejorar el rendimiento, valora buscar soluciones desarrolladas desde cero para el rendimiento, puesto que el rendimiento como idea de última hora raramente logra los objetivos que se desea. Cuando se trata del rendimiento de la red, es importante tener presente que no es posible rediseñar el código de una arquitectura deficiente. Al igual que hay pocas oportunidades de rediseñar los planos de un edificio una vez que ya se han construido los cimientos, para lograr el mejor rendimiento es necesario rediseñar las redes desde cero.

Aprovechando la eficacia de una red perimetral global que procesa y gestiona los datos más cerca del origen, las organizaciones tendrán una ventaja estratégica hoy y en el futuro. Según MIT Technology Review, "El proceso de volúmenes de datos puede conllevar problemas de rendimiento. Como respuesta, muchas organizaciones están adoptando el proceso perimetral, que procesa los datos cerca del origen para permitir un análisis y una respuesta rápidos y en tiempo real, al mismo tiempo que mantiene los requisitos de privacidad y seguridad" (fuente). Si optas estratégicamente por soluciones ya desarrolladas sobre las arquitecturas del mañana, puedes proporcionar a tus equipos la ventaja estratégica de un mejor rendimiento de la red sin sacrificar los aspectos fundamentales de privacidad y seguridad.

En resumen, las medidas que puedes adoptar para desarrollar una postura de ciberseguridad mejor durante los tiempos de incertidumbre son:

1. **Audita las herramientas de seguridad existentes para descubrir las funcionalidades que se solapan**
   - Consolida las herramientas que se solapan.
   - Pasa de invertir en gastos de capital a invertir en gastos operativos.
2. **Centra tu atención en los datos, no solo en las herramientas**
   - La interoperabilidad de las herramientas da como resultado conjuntos de datos mejores y más precisos.
   - Los conjuntos de datos más precisos y la elaboración de informes generan mejores conocimientos, esenciales para lograr los objetivos empresariales.
3. **Considera utilizar modelos en la nube como servicio para maximizar la innovación y minimizar la complejidad**
   - Si tu empresa no se dedica específicamente a la ciberseguridad, obtendrás importantes ventajas si trasfieres la aplicación de parches, el mantenimiento y las actualizaciones a soluciones como servicio.
   - Los modelos en la nube y como servicio ofrecen la flexibilidad que necesitas para lograr agilidad en el fluctuante entorno económico.
4. **Mejora la experiencia de tus empleados**
   - Demasiadas herramientas en demasiadas ubicaciones pueden crear puntos ciegos de seguridad así como frustración en los empleados. La consolidación y la simplificación te ayudarán a optimizar su experiencia.
   - La optimización de la facilidad de uso para los empleados ayudará con la retención de los empleados y evitará que recurran a Shadow IT para llevar a cabo su trabajo.
5. **Busca los costes ocultos y oportunidades de mejora del rendimiento en tu conjunto actual de soluciones de ciberseguridad**
   - Audita las herramientas existentes para descubrir oportunidades para optimizar el rendimiento, pero ten presente que no puedes optimizar una arquitectura deficiente.
   - La adopción de herramientas desarrolladas a escala global más cerca de la ubicación donde esperas que estén tus clientes permitirá a tu organización proporcionarles una experiencia mejor y más segura.

Cómo puede ayudar 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 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.

Control

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

Flexibilidad

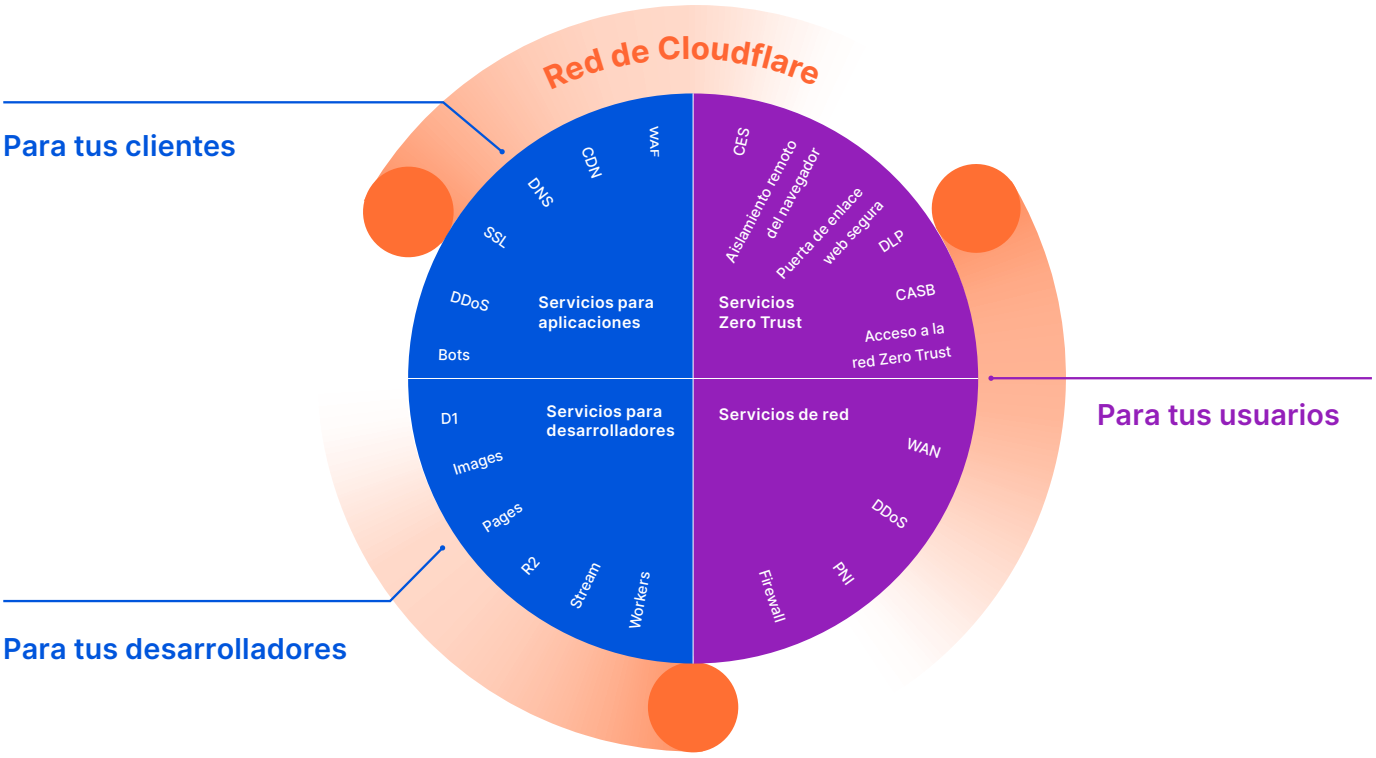
Con los servicios nativos de nube no necesitas adelantar inversiones de gasto de capital. Incrementa o disminuye fácilmente el uso en consonancia con las fluctuaciones de tu negocio.

Previsibilidad

Facturación previsible, sin costes inesperados, como tarifas 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, usuarios y dispositivos.
- **Escribe** e **implementa** el código que se ejecuta en el perímetro de la red.



Nuestra plataforma

Acerca de Cloudflare

Cloudflare se puso en marcha en 2010 para liderar la transformación de la infraestructura local a la nube. Desarrollamos la plataforma de Cloudflare desde cero teniendo presente un plan audaz: ayudar a mejorar Internet. Nuestra cartera de productos protege y acelera cualquier aplicación de 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 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.

Si deseas más información, visita www.cloudflare.com/es-es/

CLOUDFLARE

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-4327.10MAR2023