CSO

Microsoft Security

CONTENIDO PATROCINADO

Seguridad de Confianza cero: **Lecciones de los primeros usuarios**

CSO Microsoft Security

Tabla de contenido

CSO Microsoft Security

Introducción

Los últimos dos años de interrupción han sacudido los modelos tradicionales de TI y seguridad. Como resultado, la seguridad de Confianza cero ha pasado rápidamente de ser un concepto interesante a convertirse en una base de la seguridad empresarial moderna.

En una nueva investigación de Foundry, se descubrió que el 52 % de las organizaciones está ejecutando pilotos o ha implementado arquitectura de Confianza cero, así como que otro 15 % está investigando modelos de Confianza cero. Estos usuarios informan que sus implementaciones tienen múltiples beneficios, que incluyen la protección mejorada de datos de clientes, la reducción de la complejidad y la entrega de acceso seguro y confiable a recursos corporativos.

En este eBook, exploraremos los resultados de un estudio de Foundry, que recalca la importancia de una estrategia de Confianza cero para ayudar a los CISO a proteger sus organizaciones contra diversos riesgos de numerosos vectores de ataque. También se incluye orientación sobre cómo implementar Confianza cero para quienes inician su recorrido.

Acerca de la encuesta

En los meses de febrero y marzo de 2022, Foundry encuestó a negocios estadounidenses para explorar el estado actual de la adopción de Confianza cero. Los encuestados debían ser gerentes de TI o tener un puesto superior en una empresa con más de 500 empleados, además de tener un rol en la compra de productos y servicios de ciberseguridad.

Un total de 250 personas respondieron la encuesta de 23 preguntas.

CSO Microsoft Security

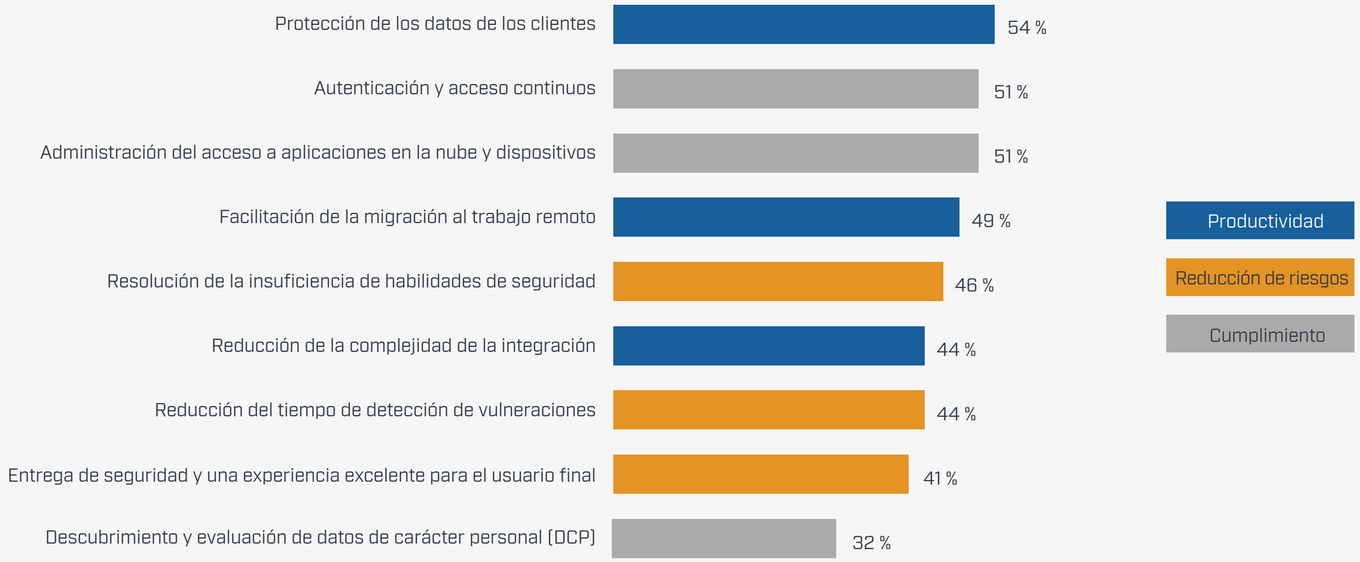
Confianza cero está aquí y está ofreciendo valor

A partir de los resultados de la encuesta y de las entrevistas en profundidad realizadas a ejecutivos de TI y seguridad, queda claro que Confianza cero es una prioridad en la mayoría de las organizaciones. Y quienes han implementado diferentes componentes de esta ya observan los beneficios.

La mayor parte de los encuestados que han implementado Confianza cero (87 %) señalan que la arquitectura entrega los resultados esperados o resultados que superan los objetivos originales de implementación, adopción e integración.

“[Confianza cero] se ha convertido en un procedimiento operativo estándar para nosotros. No nos veo regresando a como

Beneficios obtenidos a partir de la implementación de Confianza cero



12 % de los encuestados indicó obtener *todos* estos beneficios

Fuente: Zero Trust Adoption Survey, marzo de 2022, Foundry. Base: 250

éramos antes", señala el director de TI de un minorista mundial (se mantuvo el anonimato de los encuestados a cambio de que estos pudieran hablar libremente sobre sus planes de seguridad). Además, alrededor del 44 % de los encuestados informó que Confianza cero redujo la complejidad inherente de la implementación de una arquitectura de seguridad integrada. "Dado que se trata de un marco y se trabaja con este, hace que las cosas sean menos complicadas", señala el CISO de una empresa de centro de llamadas con 3.500 empleados.

Un VP y CISO de una empresa de servicios financieros con 17.000 empleados indica que la autenticación multifactor que su empresa implementó como parte de Confianza cero ha sido un éxito con los empleados. "Ha aumentado la satisfacción de los empleados, porque ahora no tienen que ir a un equipo proporcionado por la empresa y usar un cliente de VPN, pueden acceder a los recursos desde cualquier lugar", afirma.

El concepto de acceso con privilegios mínimos también ha rendido frutos, señala el CISO. "Hemos tenido menos errores catastróficos de los administradores del sistema debido a la implementación de ese sistema de acceso con privilegios", afirma. "Tienen sus privilegios para cosas específicas y por períodos específicos, lo que significa que las posibilidades de cometer errores son menores".

Dado el aumento de la prevalencia de la suplantación de identidad (phishing) y de otros ciberataques, el director de TI de la empresa minorista resume los beneficios de Confianza cero de esta manera: "Si no tuviéramos estos tipos de herramientas, probablemente en este momento estaríamos en una situación difícil y haciendo pagos en bitcoins a alguien".

CSO Microsoft Security

Impulsores de la implementación de Confianza cero

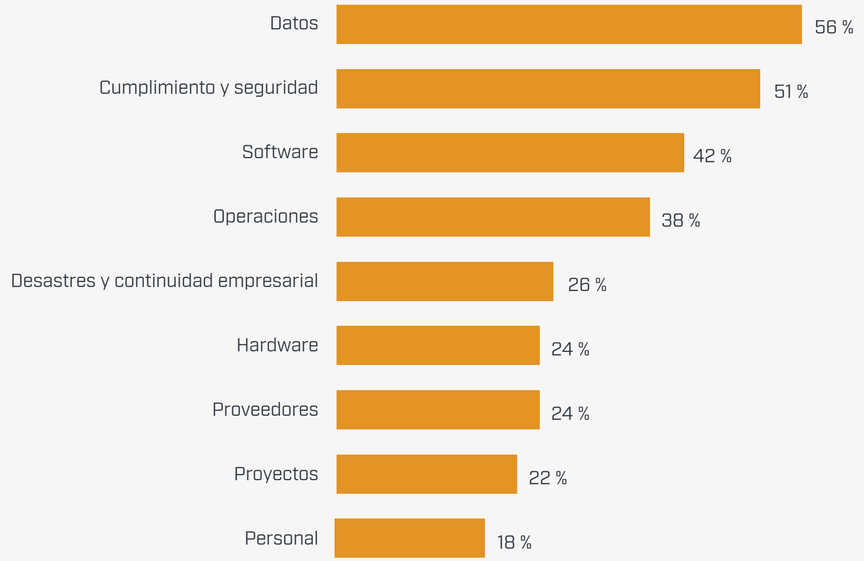
Una confluencia de eventos está impulsando a las empresas a, al menos, considerar una arquitectura de Confianza cero. En lo más alto de la lista se encuentra la necesidad de administrar riesgos para una gran cantidad de recursos contra múltiples amenazas. Los encuestados atribuyeron el valor de un año de incidentes de seguridad a diversas causas, lideradas por las vulnerabilidades de seguridad de personas u organizaciones externas. Entre otras causas se incluyeron:

- Riesgos inesperados para el negocio
- Configuración errónea de servicios o sistemas
- Ataques internos malintencionados
- Errores no malintencionados de los usuarios, como convertirse en víctimas de suplantación de identidad (phishing)
- Identidades vulneradas
- Software sin parches
- Credenciales robadas

Estos incidentes conllevan diversos riesgos, dirigidos por datos.

Para muchas organizaciones, el cambio repentino al trabajo remoto provocado por la pandemia aceleró la adopción de planes de Confianza cero, ya que los modelos de seguridad tradicionales basados en el perímetro quedaron obsoletos. Muchas organizaciones ya habían adoptado esa dirección, ya que habían migrado más aplicaciones e infraestructura

Principales categorías en riesgo de amenazas de ciberseguridad



Fuente: Zero Trust Adoption Survey, marzo de 2022, Foundry. Base: 250

CSO Microsoft Security

de TI a la nube, pero la pandemia le dio un remezón adicional. Por ejemplo, el CISO de una empresa de tecnología médica con 1.700 empleados señala que la nube y la pandemia impulsaron la adopción de Confianza cero, que ahora proporciona una base segura para cualquier modelo de lugar de trabajo que se les presente.

"Los impulsores del negocio fueron el hecho de que éramos una empresa basada en la nube que debía ser capaz de proteger su entorno", indica. "También tuvimos que proveer trabajadores remotos capaces durante la pandemia. [Confianza cero] nos ha permitido reducir drásticamente nuestra huella de bienes inmuebles y es probable que mantengamos al menos el 60 % de nuestra empresa de forma remota y virtual".

CSO Microsoft Security

No hay escasez de amenazas

Las necesidades de cumplimiento también han impulsado modelos de seguridad más sólidos. “Los reguladores nos observan y esperan que sigamos mejorando nuestro marco de seguridad”, señala el SVP de seguridad global de la información de una empresa de servicios financieros con 290.000 empleados.

Algunas organizaciones han tomado medidas proactivas hacia Confianza cero para evitar que una vulneración de alto perfil los ponga en el centro de atención por los motivos equivocados. “La idea era ser proactivos e intentar mantenernos alejados de los noticiarios”, indica el CIO de una institución de educación superior con 3.500 empleados. “Hay algunas historias de terror de otras instituciones locales de tamaño similar al nuestro que no pudieron funcionar durante mucho tiempo”.

Otros ya han experimentado un incidente de ciberseguridad grave, lo que los incita a revisar rápidamente su estrategia de seguridad. Después de que una compañía de seguros con 6.000 empleados sufriera un ataque de ransomware que paralizó la red corporativa por dos semanas, la instrucción de adoptar Confianza cero llegó directamente del CEO. “Aceleramos la implementación”, indica el VP de desarrollo de TI de la compañía. “Al comienzo, su implementación fue sin duda un procedimiento recomendado, pero después del ataque de ransomware realmente se aceleró mucho”.

Un catalizador basado en la nube

El VP y CISO de una importante empresa de servicios financieros señala que su equipo reconoció hace varios años la necesidad de una nueva arquitectura de seguridad, cuando comenzaron a adoptar más recursos basados en la nube y aumentó la movilidad de los usuarios.

“Nos dimos cuenta de que la arquitectura de seguridad tradicional en la que habíamos confiado en el pasado no nos protegería de los avances de los atacantes”, señala.

Esa realidad se hizo mucho más evidente a comienzos de 2020, cuando la empresa descubrió que en algún momento del año anterior un atacante había penetrado en su perímetro y se había movido lateralmente dentro del entorno sin ser detectado. “Necesitábamos una nueva arquitectura donde pudiéramos proteger y autenticar el uso de esos recursos en cualquier lugar en que se encontraran, y Confianza cero es una arquitectura diseñada para hacer eso”

CSO Microsoft Security

Obstáculos de adopción de Confianza cero

Para muchas organizaciones, Confianza cero representa un cambio fundamental en la estructura, el proceso y la mentalidad de seguridad, lo que explica algunos de los obstáculos que deben sobrellevar después de adoptarla.

“Comenzamos a eliminar muchos espacios aislados diferentes dentro de la organización”, indicó el CISO del centro de llamadas, que explicó que los equipos de servidor, red y base de datos tenían su propio contingente de servidores web y herramientas. “Eso nos complicó porque todo el mundo tenía ideas diferentes de hacia dónde ir y cómo hacerlo”.

¿Qué le impide adoptar Confianza cero?

Fuente: Zero Trust Adoption Survey, marzo de 2022, Foundry. Base: 250

CSO Microsoft Security

De acuerdo con Anthony Mocny, gerente sénior de marketing de productos de Confianza cero de Microsoft, descubrir esos problemas puede ser un efecto secundario positivo de Confianza cero. “Como arquitectura, Confianza cero está diseñada para eliminar los espacios aislados de los equipos de seguridad que se encuentran dentro de los pilares de la tecnología y ayudan a los equipos a trabajar en conjunto de forma coherente”, afirma. “También puede significar un cambio cultural, en términos de la forma en que los equipos trabajan juntos”.

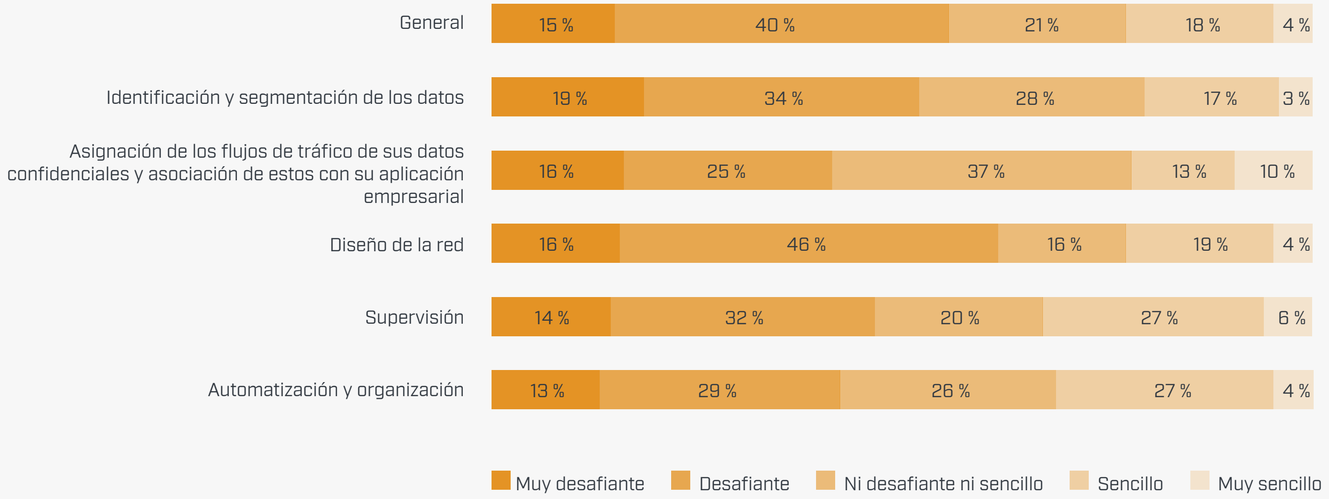
Para el VP/CISO de servicios financieros, las aplicaciones heredadas fueron un obstáculo a superar en el camino hacia Confianza cero. “Se tienen que adaptar con tecnología moderna de autenticación”, señala. “Dependiendo de cuál sea su antigüedad, es posible que no sea muy fácil hacerlo”.

CSO Microsoft Security

Desafíos de implementación

Una vez que las empresas se embarcan en un recorrido de Confianza cero, también pueden surgir una variedad de desafíos de implementación. Más de la mitad de los encuestados (56 %) reconoció que la implementación de Confianza cero fue desafiante o muy desafiante. Específicamente:

¿Qué tan desafiante es la implementación de Confianza Cero?



Fuente: Zero Trust Adoption Survey, marzo de 2022, Foundry. Base: 168

CSO Microsoft Security

Los desafíos en torno a la segmentación y la microsegmentación aparecieron con frecuencia en las entrevistas en profundidad.

“Se segmenta la red hasta el host individual”, señala el VP/CISO de servicios financieros. “Es como colocar un pequeño firewall entre cada host de la red interna para que pueda ver todo el tráfico y controlarlo hasta la máquina individual. Tiene enormes beneficios para la seguridad, pero es súper difícil de implementar porque ahora tiene que, básicamente, administrar decenas de miles de firewalls”.

La asignación de flujos de tráfico puede ser otro proceso que tome varios meses. Para el CTO de una empresa editorial y de medios de comunicación con 5.000 empleados, después de definir los datos críticos, la aplicación y los servicios de red que debían proteger, “asignamos flujos de transacción a lo largo de la red e intentamos entenderlos como grupos de información”, señala. “[Luego] segmentamos partes de esa información y la forma en que se traspasa a la red, incluso a paquetes únicos de información”. En ese punto, la empresa aplicó directivas de Confianza cero a cada tipo de flujo de tráfico. “También incorporamos nuevas capacidades para supervisar y mantener nuestra red”.

A pesar de los desafíos, muchos encuestados consideran que Confianza cero finalmente simplifica las operaciones del día a día. Con las tecnologías tradicionales, “hacer cambios toma días; tiene que implementarlos en todos los componentes de hardware y software, y para ello se usan muchos recursos”, señala el SVP de servicios financieros de seguridad global de la información. “Cuando observamos Confianza cero, realmente se minimiza la complejidad arquitectónica en el largo plazo y se reduce el número de empleados que necesitamos que hagan el mismo tipo de trabajo”.

Procedimientos recomendados para implementar Confianza cero

A medida que aumenta la cantidad de empresas que implementan una arquitectura de Confianza cero, se desarrollan planes de desarrollo y procedimientos recomendados para que otros los sigan. A continuación, le presentamos cinco aspectos que debe considerar al planificar una implementación.

No abarque tanto al comienzo

Diseñar una estrategia de Confianza cero puede ser abrumador si solo ve el contexto amplio de tener que modificar directivas y protecciones en redes, datos, aplicaciones, identidades, puntos de conexión e infraestructura. “Al comienzo solo veíamos esta enorme montaña que debíamos escalar y nos preguntábamos si lo lograríamos”, señala el CIO de educación superior. “Simplemente tiene que ir un paso a la vez”.

El CIO y su equipo finalmente adoptaron un enfoque de “seguir al dinero”, en el que priorizaron la segmentación de las aplicaciones de finanzas y nómina en una red independiente.

De acuerdo con Mocny, la identificación de los activos cuya protección es más crítica es un buen enfoque. “Sea consciente del motivo por el que está implementando Confianza cero en primer lugar”, indica.

Cuando tenga dudas, comience con la autenticación multifactor

Al priorizar la pila de seguridad, muchos CISO y proveedores de seguridad recomiendan centrarse inicialmente en la autenticación y otras protecciones basadas en la identidad. “Si no tiene un punto de partida en mente, la autenticación multifactor es un buen lugar para considerar”, señala Mocny. Microsoft calcula que la autenticación multifactor puede evitar más del 90 % de los ataques basados en la identidad. El VP/CISO de servicios financieros está de acuerdo. “La autenticación es un elemento fundamental de la implementación de una arquitectura de Confianza cero. Ninguno de los demás componentes funcionará si no puede validar la identidad del usuario final, por lo que comenzamos por ahí”.

A continuación, el VP/CISO de servicios financieros abordó el componente de redes, que proporcionó beneficios inmediatos para apoyar a los trabajadores remotos. El equipo dejó la microsegmentación para otro momento del recorrido porque no es fácilmente visible para el negocio en general. “Cuando haya terminado, la seguridad será mucho mejor, pero nadie notará la diferencia”, señala.

CSO Microsoft Security

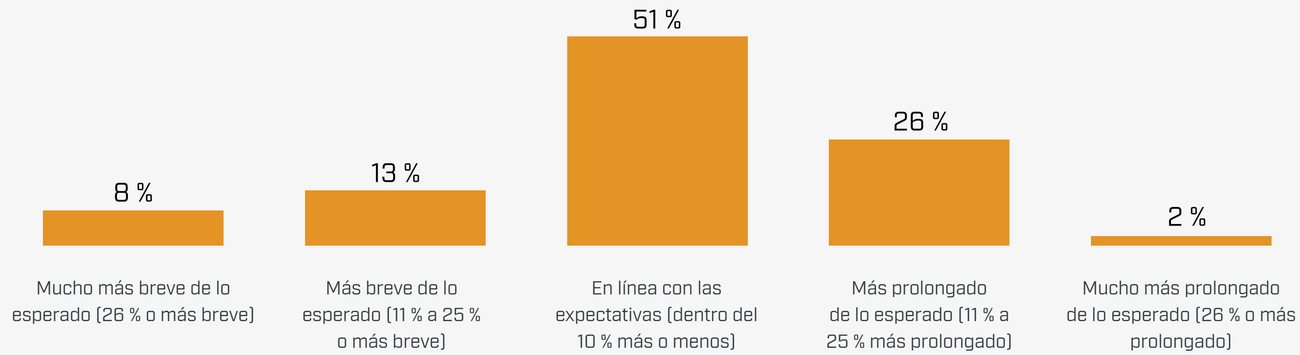
Propóngase plazos realistas

Es importante que los CISO establezcan expectativas realistas con relación a la implementación de Confianza cero. “La implementación de una arquitectura de Confianza cero es un programa, no un proyecto”, afirma el VP/CISO de servicios financieros. “Este fue un cambio enorme. Hacerlo bien conlleva numerosos proyectos y es probable que dure años; no existe una implementación fácil y rápida de la arquitectura de Confianza cero”.

Su SVP de finanzas está de acuerdo. “No creo que termine alguna vez, porque siempre aparece nueva tecnología, siempre aparece nuevo malware, siempre aparecen nuevas amenazas”, afirma.

La mayoría de los encuestados (72 %) indicó que sus plazos de implementación iban según lo planeado o adelantados, mientras que el resto señaló que la implementación estaba tardando más de lo que esperaban.

¿Confianza cero cumple con sus objetivos de plazos?



Fuente: Zero Trust Adoption Survey, marzo de 2022, Foundry. Base: 168

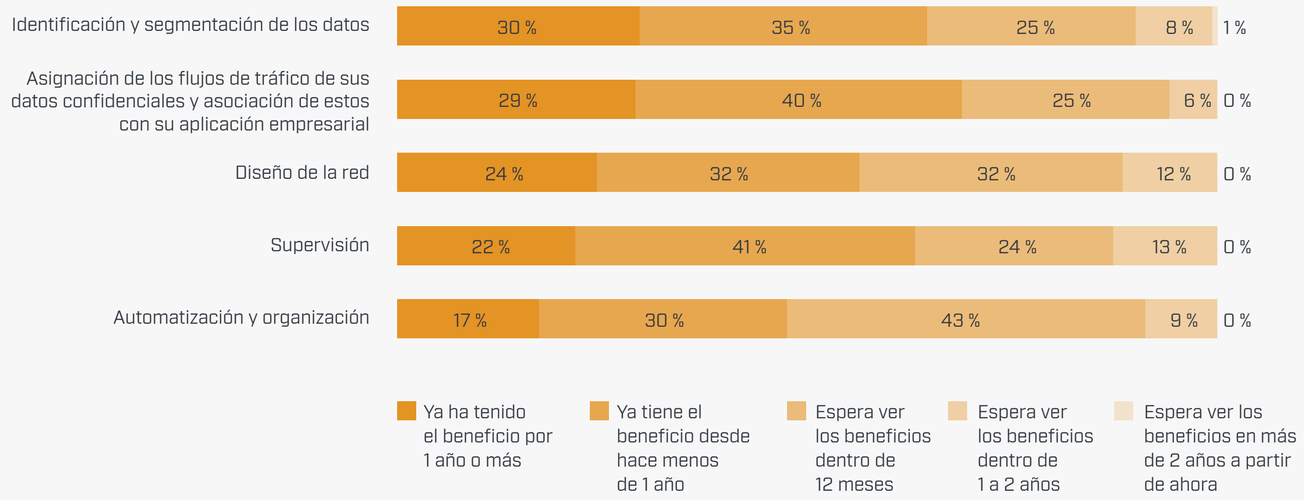
CSO Microsoft Security

Mida a medida que progresa

Mientras está en curso la implementación de Confianza cero, los CISO pueden y deben crear hitos para así poder medir el progreso. Es una buena señal que alrededor de dos tercios de los encuestados dijeran que obtenían beneficios de la mayoría de los aspectos de sus proyectos en un período de un año, y que aproximadamente otra cuarta parte o más espera obtenerlos dentro de 12 meses, en actividades clave que incluyen la identificación y segmentación de datos, la asignación de flujos de tráfico y la arquitectura de la red.

“Confianza cero es un recorrido, esto se debe a la evaluación continua que debe hacer para defenderse de la naturaleza cambiante de los ataques”, afirma Mocny. “Siempre debe estar atento a las mejoras”.

Plazos para obtener los beneficios de Confianza cero



Fuente: Zero Trust Adoption Survey, marzo de 2022, Foundry. Base: 103

Enfóquese en las personas, no solo en la tecnología

El amplio alcance del modelo de seguridad de Confianza cero afecta a todos los empleados, incluidos los equipos de TI y seguridad que están a cargo de la tarea de implementarlo. Es por eso que, al igual que con cualquier proyecto de tecnología, es importante asegurarse de que las implementaciones estén sincronizadas con los nuevos procesos, así como con los cambios en los procesos de administración, para garantizar una puesta en marcha exitosa y sin problemas.

"Además de un cambio en la tecnología, también hay un cambio cultural", afirma Mocny. "Si tiene varios equipos que abordan la seguridad, incluidos arquitectos o expertos en identidad, también debe cambiar la forma en que esos equipos trabajan juntos. Debe eliminar los espacios aislados para garantizar que, con la tecnología, todos trabajen juntos de forma coherente".

La eliminación de los espacios aislados implica lograr que los equipos de todas esas disciplinas participen estrechamente en proyectos de ejecución de pilotos y prueba de concepto (POC). El director de sistemas de TI de una empresa de telecomunicaciones con aproximadamente 2.000 empleados aprendió esa lección después de tener dificultades con varios puntos de error únicos durante la implementación, incluidos servicios que no podían autenticarse y, de un momento a otro, "no eran de confianza", lo que provocaba que estos y algunos sistemas no estuvieran disponibles.

"La implementación de un servicio puede tener un efecto dominó y hacer fallar otros", indica. Luego de esto, "tenemos mucho más cuidado, más tiempo de POC, más revisiones y más revisiones arquitectónicas de expertos antes de la implementación".

Retorno de la inversión (ROI) de Confianza cero

Un **estudio Forrester Consulting Total Economic Impact™** encargado realizado en 2021 cuantifica los ahorros de costos y los beneficios empresariales de las soluciones de Confianza cero de Microsoft. De acuerdo con las cinco empresas que entrevistó Forrester, una organización compuesta observó un retorno de la inversión de tres años del 92 % mediante la implementación de una arquitectura de Confianza cero con Microsoft.

Esta organización compuesta también ahorró en promedio USD 20 por empleado, al mes, al eludir la necesidad de contar con herramientas de seguridad que se volvieron redundantes con Confianza cero, incluida la administración de puntos de conexión, los antivirus y las soluciones antimalware.

CSO Microsoft Security

¿En qué lugar de la ruta hacia Confianza cero se encuentra?

Como lo indica la encuesta, los beneficios de un modelo de seguridad de Confianza cero claramente superan a algunos de los desafíos de implementación que enfrentan los CISO y sus equipos de seguridad. Hacer frente a estos desafíos con un plan bien pensado puede ayudar a su organización a mejorar rápidamente las protecciones, reducir el riesgo y comenzar a ofrecer valor en el negocio.

Para evaluar el nivel de madurez de Confianza cero de su organización y consultar más recursos prácticos de implementación, realice la **Evaluación del modelo de madurez de Confianza cero** de Microsoft.