SOPHOS

La confianza cero desmitificada

La era del perímetro de seguridad único y de red corporativa está llegando a su fin. Los usuarios trabajan cada vez más de forma remota y realizan su trabajo a través de la Internet pública. El auge de las aplicaciones de software como servicio (SaaS), las plataformas en la nube y otros servicios basados en la nube ha reducido la eficacia del uso de la red como principal elemento para proteger un recurso. Ya no podemos depender de una única red corporativa cerrada ni permitirnos confiar en todos los sistemas que residen dentro de ella, ya que ahora los límites entre redes son difusos.

Aquí entra la confianza cero, una filosofía de ciberseguridad sobre cómo pensar sobre la seguridad y cómo ejecutarla. La confianza cero se basa en el principio de que no se debe confiar en nada y que se debe comprobar todo, en que hay que centrarse en proteger los recursos independientemente de dónde estén física o digitalmente y no confiar nunca en nada por defecto.

No existe un único proveedor, producto o tecnología que pueda hacerle llegar a la confianza cero. Lo que se necesita es un cambio cultural y un montón de soluciones distintas para modificar los paradigmas por los que protegemos nuestros recursos.

En este monográfico se explica el concepto de la confianza cero, se detallan las ventajas de implementar un modelo de confianza cero y se ofrece orientación en cuanto a los pasos que deben seguir las empresas para su transición hacia ella.

Los tiempos han cambiado

"Confianza" es una palabra peligrosa en el campo de la tecnología de la información, sobre todo cuando esta confianza es implícita, es decir, cuando es incondicional o incuestionable.

Se ha demostrado una y otra vez que crear un gran perímetro de seguridad de red corporativo precintado y confiar en todo lo que se encuentra en su interior es una estrategia condenada al fracaso. Este interior tierno y cremoso es el sueño de todo hacker. Una vez dentro, suelen ser invisibles. Propagarse por la red y acceder a sistemas importantes, por ejemplo, es sencillo, porque los controles de seguridad y las comprobaciones más sólidas solo tienen lugar en el perímetro.

Tanto si nos gusta como si no, el perímetro se ha debilitado.

Los usuarios quieren trabajar de forma remota en redes que no son de confianza, como las redes Wi-Fi públicas de las cafeterías. Quieren guardar sus datos en la nube para poder acceder a ellos siempre que lo necesiten. Quieren utilizar sus propios dispositivos personales para acceder a los datos y los recursos corporativos. Nuestros usuarios nos exigen disponer de un acceso libre para poder trabajar cuando, donde y como deseen.

El uso de aplicaciones de software como servicio (SaaS), plataformas en la nube y otros servicios basados en la nube deja los datos fuera del perímetro corporativo, y el uso de plataformas en la nube pública significa que muchos de los dispositivos o servicios que antes se ejecutaban dentro del perímetro corporativo ahora se ejecutan fuera de él. Nuestras cargas de trabajo se están trasladando allá donde sea más rentable procesarlas, lejos de las redes de confianza que nos pertenecen y controlamos.

Todo está en todas partes. El antiguo modelo de "red corporativa" con defensas estáticas no da a las empresas la capacidad de adoptar soluciones como la nube al tiempo que protegen sus datos, usuarios y clientes. Es necesario un cambio de paradigma.

El modelo de confianza cero

La confianza cero es un enfoque holístico a la seguridad que hace frente a estas amenazas y cambios en el modo de trabajar de las empresas. Se trata de un modelo y una filosofía para saber cómo pensar sobre la seguridad y cómo ejecutarla.

Nada ni nadie es digno de una confianza automática, ni dentro ni fuera de la red corporativa, ni siquiera la propia red. La confianza implícita basada en la ubicación de la red, con defensas estáticas como un firewall tradicional, debe limitarse.

En última instancia, es necesario confiar en algo, pero con la confianza cero, esta confianza es temporal y se establece dinámicamente a partir de múltiples fuentes de datos, más de las que se hayan usado nunca en el pasado, y se reevalúa de forma constante. Entre las fuentes de datos se incluyen la información sobre la propia solicitud de acceso, la información del usuario, la información del sistema, la información de los requisitos de acceso y la información sobre amenazas. Además, el acceso a los datos y a los recursos solo se concede cuando es necesario, determinándose conexión a conexión.

Tenemos mucha experiencia con las redes que no son de confianza a través de nuestro uso diario de Internet. Los ordenadores expuestos a la Internet pública se protegen de forma muy distinta a la de aquellos que se encuentran dentro del perímetro tradicional, ya que requieren más análisis y capas de defensa para protegerlos de amenazas externas.

El modelo de confianza cero le lleva a tratar todos los dispositivos como si estuvieran abiertos a Internet y, en lugar de tener un único perímetro, debe crear muchos microperímetros (o microsegmentos) y aplicar comprobaciones y controles en torno a todo y entre todo.

Ventajas clave de adoptar la confianza cero

Adoptar un modelo de confianza cero reporta incontables beneficios, así que, para ponérselo más fácil, hemos seleccionado algunos de las más fundamentales.

Controlar toda la infraestructura de TI

Desde el interior de la oficina hasta las plataformas en la nube que utilice. Se acabaron la falta de control fuera del perímetro corporativo y las dificultades con los usuarios remotos.

Gestionar y proteger a todos los usuarios de la misma forma

Cuando se deja de hacer la distinción entre fuera y dentro del perímetro corporativo, se puede tratar a todos los usuarios de la misma manera. Esto simplifica la seguridad TI al tiempo que garantiza un trato equitativo de todos los dispositivos y usuarios.

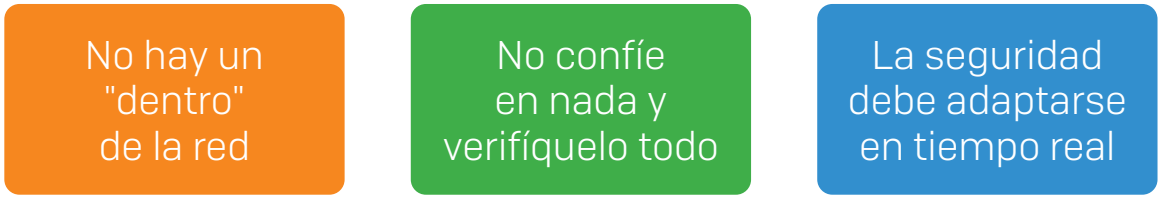
Mantener la seguridad incluso cuando la infraestructura en uso no es suya o no tiene control total sobre ella

Al utilizar la supervisión y el análisis de la identidad, la ubicación, el estado del dispositivo, la AMF y la superposición, puede seguir contando con una sólida seguridad en cualquier tipo de entorno, plataforma o servicio.

Reducir drásticamente el movimiento del malware o los atacantes

Los atacantes, en lugar de tener vía libre en toda la red una vez que entran, solo tienen acceso al mínimo indispensable de sistemas a los que tiene acceso el usuario comprometido. Al considerarse que el usuario autenticado sigue sin ser de confianza, se establecen comprobaciones entre esos sistemas, lo que limita aún más su capacidad de propagarse.

Resumen de la confianza cero



La confianza cero es una gran idea, y existe mucho debate en torno a ella. Esencialmente, podemos resumir los principales conceptos de la confianza cero en varias máximas que debe observar a lo largo de su camino.

No hay un "dentro" de la red

Actúe como si estuviera operando toda su empresa desde una ubicación no segura, como la red Wi-Fi pública de una cafetería, y como si todos sus dispositivos estuvieran conectados directamente a la más peligrosa de todas las redes: la Internet pública. Si imaginamos que esta es nuestra realidad, nos obligaremos a aplicar unas medidas de seguridad para las que no se presuponga que nos encontramos dentro de un perímetro corporativo tradicional.

Siempre habrá redes "de confianza" corporativas para la administración y los sistemas internos, pero el objetivo es mantener a los usuarios normales fuera de estas redes, usando servidores proxy de aplicaciones u otras tecnologías, con el fin de reducir drásticamente la superficie de ataque.

No confíe en nada y verifíquelo todo

Asuma que hay atacantes tanto dentro de sus redes como fuera y que están ahí todo el tiempo, atacando constantemente. No se debe confiar automáticamente en ningún usuario ni dispositivo, y estos deben autenticarse ellos mismos antes siquiera de que pueda considerarse una conexión. Si imagina que está bajo ataque constante desde todas direcciones, se verá en la obligación de posibilitar una autenticación y una autorización de gran robustez para sus recursos, organizar sus defensas en capas, y supervisar y analizar constantemente todo lo que ocurre en todos sus entornos.

La seguridad debe adaptarse en tiempo real

Las políticas de seguridad que implemente para llegar a la confianza cero deben ser dinámicas y cambiar automáticamente en función de la información recibida de todas las fuentes de datos y mediante todas las tecnologías posibles. Una política estática como "ESTE USUARIO" en "ESTE DISPOSITIVO" puede acceder a "ESTE RECURSO" no le protegerá si ese dispositivo se ha visto comprometido mientras ese usuario lo estaba utilizando. Si su política también tuviera en cuenta el estado de seguridad del dispositivo, como la identificación de comportamientos maliciosos, la política podría usar esto para adaptarse dinámicamente a la situación sin ningún esfuerzo de ningún administrador.

Esto ha formado parte de la estrategia y la filosofía de Sophos en cuanto a la ciberseguridad desde hace mucho tiempo. Seguramente lo conozca como Seguridad Sincronizada, un sistema por el que nuestros productos pueden compartir datos únicos entre sí. Esto nos permite tener políticas dinámicas y adaptativas y sacar provecho de todas estas informaciones para que una política no sea nunca estática y no pueda esquivarse fácilmente.

Muchas de estas cosas son simplemente buenas políticas de seguridad y prácticas recomendadas que posiblemente ya está aplicando y, si se ha preparado para el RGPD, ya habrá hecho gran parte de este trabajo.

Principios de la confianza cero

No confíe en nada. Nunca. Porque si no confía en nada, no le queda más remedio que buscar medidas de seguridad relevantes donde sea que haya riesgo.

Verifíquelo todo. No dé por descontado que superar un control aporta confianza. Que alguien tenga credenciales no significa que sea fiable. Solo significa que tiene credenciales. Y las credenciales pueden robarse.

Podemos desglosar esta cuestión en cuatro sencillos principios que debemos tener en cuenta.

Identificar siempre

Necesita una fuente de identidad específica y fidedigna y utilizarla en todas partes con el inicio de sesión único (SSO). Es necesario autenticar todo mediante la autenticación multifactor (AMF). Independientemente de dónde esté el usuario y a lo que esté intentando acceder, valide sus credenciales, compruebe que tiene su segundo (o tercer) factor y exija que se reautentique regularmente.

Si las credenciales son robadas o algún sistema ha sido secuestrado, la AMF y la reautenticación periódica frenarán rápidamente al atacante.

Controlar siempre

Aplique controles y comprobaciones donde se necesiten y adopte y aplique el principio del mínimo privilegio: los usuarios solo deben tener acceso a lo mínimo indispensable necesario para realizar su trabajo. Si existe un sistema de recursos humanos que solo utiliza el personal alemán, entonces solo debe ser accesible para el personal alemán. Nadie más debe tener acceso, ni siquiera si el riesgo de tener acceso se considera bajo.

Analizar siempre

Que una autenticación se realice con éxito o que se conceda acceso a un usuario o dispositivo no implica que sea fiable. Tanto amenazas internas como ciberdelincuentes pueden obtener acceso a credenciales válidas. Registre toda la actividad del sistema y de la red, y analícela e inspecciónela regularmente para verificar qué ocurre después de la autenticación. Las soluciones SIEM (información de seguridad y gestión de eventos), EDR (detección y respuesta para endpoints) y MDR (detección y respuesta gestionadas) han surgido precisamente para responder a esta necesidad.

Proteger siempre

Utilice un enfoque "de dentro a fuera" a la ciberseguridad. Debe centrarse en sus datos importantes y trabajar hacia fuera, identificando puntos de vulnerabilidad en el recorrido de sus datos dentro de la red desde el momento en que se crean hasta el momento en que se destruyen.

Tenga también en cuenta el riesgo sobre todo lo demás, no el cumplimiento ni la normativa. Aplicar medidas de seguridad meramente para satisfacer una comprobación del cumplimiento o un requisito normativo es peligroso. Los requisitos de cumplimiento no saben qué hay en su red, los flujos y las cargas de trabajo, los sistemas y las tecnologías. No conocen los riesgos relacionados con cada posible elemento de su red. Para garantizar que sabe dónde reforzar o relajar la seguridad y dónde crear microsegmentos, debe considerar el riesgo y modelar las amenazas a las que se enfrenta su empresa.

El paso a la confianza cero

¿Cómo pasamos a la confianza cero y sacamos partido de todas las ventajas que ofrece?

Defina su superficie e identifique recursos | Trace rutas estándar y con privilegios | Diseñe una red de confianza cero | Cree políticas de confianza cero | Supervise y mantenga sus perímetros

Defina su superficie e identifique recursos

Primero, debe definir qué superficie tiene la intención de proteger, controlar y supervisar. ¿Cuáles son todos los recursos, servicios, aplicaciones y dispositivos que se utilizan en su negocio? Tener una visión clara de todo lo que se está utilizando en toda la red le ayudará posteriormente a aplicar nuestra nueva mentalidad de confianza cero a todo ello.

Trace rutas estándar y con privilegios

Una vez que lo haya examinado todo, debe trazar rutas estándar: ¿qué flujos, comportamientos y relaciones existen entre todos los elementos que sean estándar y esperados? Este grupo de usuarios accederá a esta aplicación, este dispositivo se conectará a esa red, este servicio utiliza aquel almacén de datos y así sucesivamente, pero también ¿cuáles son las rutas con privilegios? Este administrador querrá conectarse a esta consola de administración y utilizar el protocolo de acceso remoto (RDP) para acceder a ese servidor que aloja datos confidenciales, por ejemplo. Con toda probabilidad, las rutas con privilegios requerirán la aplicación de seguridad o controles adicionales.

Diseñe una red de confianza cero

Ahora que conoce los elementos en juego y las relaciones entre todos ellos, puede empezar a aplicar la filosofía de confianza cero a todo ello. Identificar qué medidas de seguridad y controles de acceso necesita aplicar y dónde, qué tecnología mitigará mejor qué riesgo, etcétera.

Cree políticas de confianza cero

A continuación, debe implementar políticas de confianza cero que se servirán del mayor número posible de fuentes de datos distintas para añadir contexto a cualquier conexión o solicitud.

Supervise y mantenga sus perímetros

Por último, y quizás lo más importante, es necesario que implemente una supervisión detallada de absolutamente todo para que pueda mantener sus perímetros recién creados.

Este es uno de los mayores retos a los que se enfrentan los administradores. Donde antes se instalaba y configuraba un antivirus y nunca se volvía a mirar la consola, con la confianza cero, es necesario cambiar de hábitos.

Debe supervisar los eventos que tienen lugar, utilizando herramientas como la EDR para entender la causa raíz de la irrupción de una amenaza en el entorno, y los eventos que han ocurrido antes de una detección o después de una posible filtración.

En este sentido, servicios como la MDR pueden ser realmente útiles, ya que permiten que expertos en ciberseguridad le ayuden con la supervisión de su red, e incluso pueden encargarse de destruir amenazas por usted.

La pila tecnológica de la confianza cero

Se necesitan muchas tecnologías para proteger todos los recursos y los activos que residen en una red. No existe un único proveedor, producto o tecnología que vaya a solucionar todos sus problemas.

Una pila tecnológica de confianza cero debe cubrir dos áreas principales: la administración de la confianza cero y la seguridad y el control de sus distintos recursos y activos.

La **administración** se divide en tres subáreas:

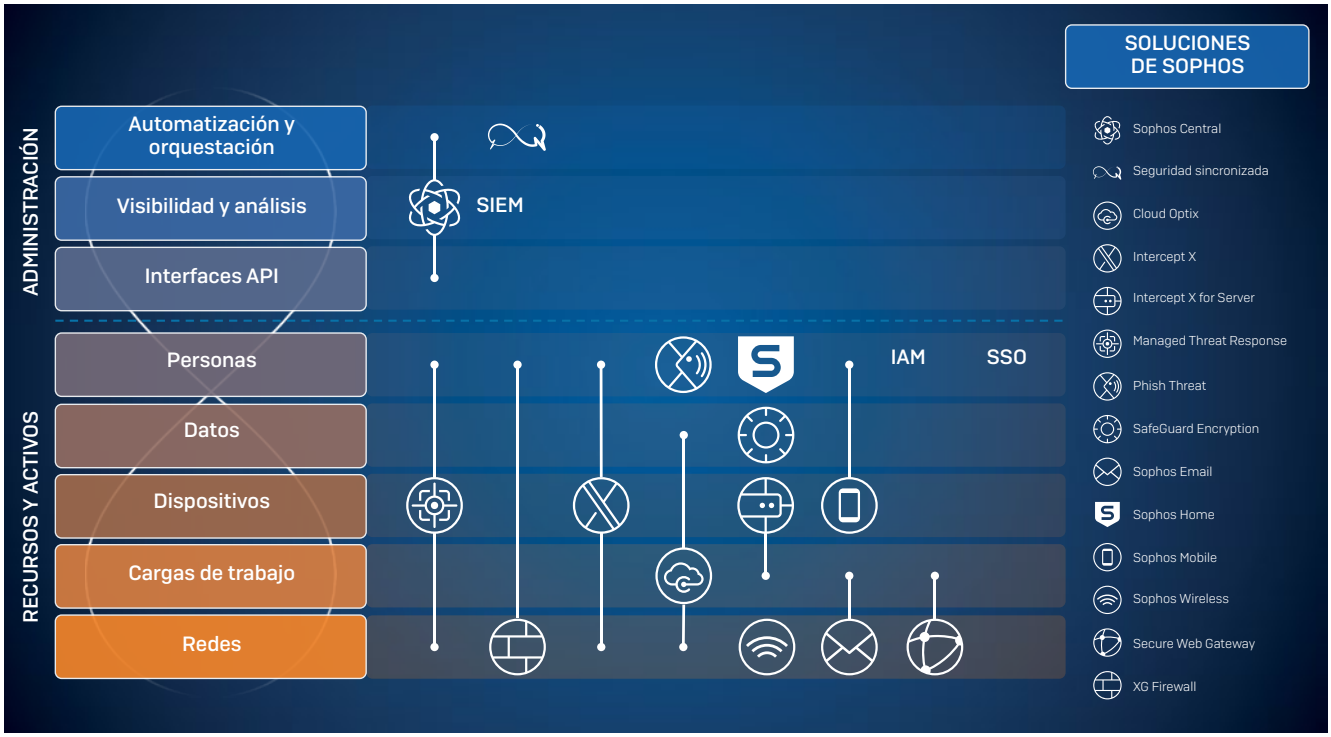
1. Automatización y orquestación: para definir políticas dinámicas, coordinar las distintas tecnologías y ponerlo todo en práctica.
2. Visibilidad y análisis: para mantener el control de la red y asegurarse de que todo está funcionando, además de identificar amenazas y filtraciones si ocurren y cuando ocurran.
3. Interfaces API: para integrar sus distintas tecnologías a fin de extraer datos de un sistema y suministrarlos a otro.

Los **recursos y activos** se dividen en cinco subáreas:

1. Personas: los usuarios, administradores, etc. que trabajan para o con su empresa.
2. Datos: el elemento vital de todas las empresas y quizás el recurso más importante que proteger.
3. Dispositivos: los servidores, portátiles, equipos virtuales, etc. que utiliza para operar su negocio.
4. Cargas de trabajo: los servicios y las aplicaciones que utiliza para procesar datos, realizar cálculos, generar informes, etc.
5. Redes: los canales de comunicación por los que fluyen los datos, la Web, redes Wi-Fi, Internet, etc.

Cómo puede ayudar Sophos

Si bien no existe un único proveedor que pueda trasladar su empresa a un modelo de confianza cero, Sophos cuenta con una enorme variedad de tecnologías para ayudarle a conseguirlo.



La administración de la confianza cero

Sophos Central, nuestra plataforma de ciberseguridad nativa en la nube, le permite gestionar un entorno de confianza cero. Organiza todas nuestras tecnologías en una única consola para proporcionarle una visión global de todas las tecnologías en un único lugar, así como interfaces API para conectar cualquier otra tecnología de terceros que esté utilizando.

También tiene la opción de incorporar un sistema SIEM para agrupar los registros de sus productos de Sophos y otros proveedores para poder tener una visión integral de todo lo que sucede. Con nuestras API es muy fácil extraer información de nuestra plataforma Sophos Central para verterla en cualquier solución SIEM que utilice.

La **Seguridad Sincronizada de Sophos** (controlada mediante Sophos Central) también tiene un papel importante aquí. Con la Seguridad Sincronizada habilitada, las soluciones de Sophos comparten información entre ellas y responden automáticamente a los incidentes. En el contexto de la confianza cero, las soluciones pueden adaptarse a los escenarios a través de políticas dinámicas y automatizar tareas complejas como el aislamiento de equipos, entre otras.

La seguridad y el control de los recursos y activos

Muchos de nuestros productos le ayudan a proteger múltiples recursos y activos al mismo tiempo, pero esto no significa en modo alguno que pueda emplear una única tecnología y despreocuparse. Proteger a las personas, por ejemplo, requiere un gran número de tecnologías diferentes como parte de una red robusta diseñada con base en la confianza cero.

Cloud Optix proporciona el análisis y la visibilidad continuos que necesitan las empresas para detectar, responder y evitar brechas de seguridad y cumplimiento que las dejan expuestas. En un entorno de confianza cero, Cloud Optix puede ayudar a proteger, dentro de la nube pública, datos, dispositivos, cargas de trabajo y redes.

Intercept X ofrece una protección para endpoints inigualable y es capaz de detener la más amplia variedad de ataques con una combinación única de detección de malware con Deep Learning, prevención de exploits, detección de comportamientos y funciones antiransomware. En un entorno de confianza cero, Intercept X puede ayudar a proteger todos sus recursos y activos.

Intercept X for Server está diseñado para proteger entornos de servidores híbridos, locales y en la nube. En un entorno de confianza cero, Intercept X for Server puede ayudar a proteger tanto sus dispositivos como sus cargas de trabajo.

Managed Threat Response (MTR) es nuestra solución de respuesta a amenazas a cargo de expertos. Fusiona la tecnología de Machine Learning con la inteligencia humana y ofrece funciones de búsqueda, detección y respuesta a amenazas las 24 horas. En un entorno de confianza cero, MTR puede ayudar a proteger todos sus recursos y activos.

Phish Threat es nuestra solución especializada contra el phishing. Ofrece a sus empleados formación de concienciación sobre seguridad, además de informes complementarios diseñados para que pueda evaluar el nivel de preparación de su empresa frente a la amenaza del phishing. En un entorno de confianza cero, Phish Threat puede ayudarle a proteger a su personal.

SafeGuard Encryption cifra el contenido tan pronto como se crea. Protege sus datos de forma proactiva validando continuamente al usuario, la aplicación y la integridad de la seguridad de un dispositivo antes de permitir que accedan a datos cifrados y, por consiguiente, en un entorno de confianza cero, puede ayudarle a proteger sus datos.

Secure Web Gateway permite una protección web avanzada y ofrece unos niveles de seguridad, control y visibilidad web sin precedentes. En un entorno de confianza cero, Secure Web Gateway puede ayudar a proteger tanto redes como cargas de trabajo.

Sophos Email se sirve de la inteligencia artificial para proporcionar una seguridad predictiva más inteligente para el correo electrónico. En un entorno de confianza cero, Sophos Email puede ayudar a proteger sus redes y cargas de trabajo.

Sophos Home está diseñado para proteger los ordenadores de su hogar y se basa en la misma tecnología que incluyen muchos de nuestros productos empresariales. En un entorno de confianza cero, Sophos Home puede ayudarle a proteger a su personal.

Sophos Mobile es nuestra solución segura de gestión unificada de endpoints (UEM) que ayuda a las empresas a dedicar menos tiempo y esfuerzo a la gestión y la protección de endpoints tradicionales y móviles. En un entorno de confianza cero, Sophos Mobile puede ayudar a proteger sus dispositivos, datos y personal.

Sophos Wireless ofrece una forma fácil y efectiva de gestionar y proteger sus redes inalámbricas. En un entorno de confianza cero, Sophos Wireless puede ayudarle a proteger sus redes.

Sophos XG Firewall proporciona una completa protección de firewall next-gen que expone los riesgos ocultos, bloquea las amenazas desconocidas y responde automáticamente a los incidentes. En un entorno de confianza cero, XG Firewall puede ayudar a proteger todos sus recursos y activos.

Emplear estas tecnologías le resultará muy útil en su transición a un modelo de confianza cero. Sin embargo, como se ha mencionado anteriormente, no existe un único proveedor o tecnología, ni siquiera Sophos, que pueda trasladarle a un entorno de confianza cero. Para dar la opción a sus usuarios de utilizar servicios en la nube estén donde estén, también necesitará implementar una potente solución de gestión de acceso e identidad (IAM) con inicio de sesión único (SSO) para utilizar su fuente de identidad única y fidedigna en todos sus sistemas y servicios: esto es un aspecto clave de la confianza cero.

Encontrará más información sobre nuestros productos y servicios y podrá iniciar demostraciones instantáneas de los mismos en es.sophos.com.

Nuestra visión de la ciberseguridad

La confianza cero y nuestra visión de la ciberseguridad, la Seguridad Sincronizada, comparten muchos de los mismos objetivos y se complementan mutuamente.

La Seguridad Sincronizada es la ciberseguridad como sistema. Analiza, adapta y automatiza continuamente las tareas más complejas en TI al tiempo que supervisa dinámicamente toda la actividad del sistema, el comportamiento de los usuarios, el tráfico de red y las posturas de cumplimiento en tiempo real. Todas las tecnologías comparten información entre ellas y se proporcionan datos y visibilidad entre sí en una situación en que solas no verían nada.

La tecnología debe hablar. Solamente a través de esta comunicación podemos lograr las políticas adaptativas y dinámicas que necesitamos, basadas en múltiples fuentes de datos, para conseguir una red de confianza cero.

Conclusión

Actualmente, la confianza cero no es más que una filosofía en cuanto a la ciberseguridad que muy pocos están en condiciones de adoptar. Sin embargo, a medida que sigan debilitándose los perímetros de seguridad, la necesidad de implementarla será cada vez más frecuente. Los ciberdelincuentes no dejan de innovar, y las defensas tienen dificultades para seguirles el ritmo. El modelo de confianza cero representa una forma de minimizar realmente las amenazas al tiempo que se establecen nuevos estándares en los protocolos de ciberseguridad.

Es momento de pensar distinto. Es hora de evolucionar.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

10-03-20 WP-ES (DD)

SOPHOS