

Sophos Workspace Protection

Protección asequible y eficaz para empleados remotos e híbridos

Sophos Workspace Protection le permite retomar el control del espacio de trabajo de su empresa. Proteja el acceso a sus apps, datos, empleados e invitados, en cualquier lugar, de forma sencilla y asequible.

La forma de trabajar ha cambiado

Ha desaparecido el perímetro de la red. Los empleados, las apps y los datos pueden estar en cualquier lugar. Las empresas tienen apps privadas propias que alojan o apps SaaS que alquilan, y todos tenemos apps, servicios y sitios en Internet de los que dependemos a diario. La mayoría de las organizaciones también tienen una plantilla híbrida de empleados presenciales y remotos o móviles que pueden estar en la oficina, en casa, de viaje o incluso trabajando en espacios públicos. Todo ello supone un reto enorme para cualquier organización a la hora de supervisar, controlar y proteger todo de forma adecuada.

Las soluciones SASE o SSE tradicionales basadas en la nube resultan caras de operar y, por lo tanto, también de adquirir. Requieren el redireccionamiento del tráfico a puntos de presencia basados en la nube para su inspección, así como el descifrado Man-in-the-Middle, lo que añade una latencia no deseada y crea problemas de usabilidad. Sin duda, tiene que haber un modo mejor. Afortunadamente, lo hay: Sophos Workspace Protection.

Proteja sus apps, datos, empleados e invitados

Sophos Workspace Protection ofrece una solución sencilla y asequible para proteger sus apps, datos, empleados e invitados, estén donde estén. Utiliza una única app, el navegador, para integrar toda la protección que necesita la empresa, sin necesidad de redireccionar el tráfico, procesar datos en la nube ni añadir procesos de descifrado: sencillamente, una experiencia transparente y segura.

Tecnologías incluidas

Sophos Protected Browser

Proporciona una sola app para proteger todas las demás. Integra ZTNA, DNS Protection, controles de apps SaaS, una puerta de enlace web segura y controles de datos locales en un navegador Chromium reforzado totalmente transparente y de uso sencillo.

Sophos ZTNA

Garantiza un acceso seguro solo a las aplicaciones que necesitan los usuarios, haciéndolas invisibles al resto, incluido el mundo exterior, y protegiéndolas de los ataques.

Sophos DNS Protection for Endpoints

Añade una capa adicional de seguridad para proteger contra contenidos web maliciosos y no deseados, tanto en el navegador como en las aplicaciones conectadas a Internet, independientemente de dónde se encuentren los empleados.

Sophos Email Monitoring System

Funciona con su solución de correo electrónico existente para mejorar la seguridad, la visibilidad y la generación de informes sobre amenazas de correo avanzadas que otras soluciones pasan por alto.

VENTAJAS

- Proteja sus apps, datos, empleados e invitados.
- Permita el acceso seguro a sus apps y protéjalas de los ataques.
- Elimine la TI en la sombra y apueste por nuevas tecnologías como la IA generativa de forma segura.
- Proteja a los empleados en Internet y aplique políticas de navegación segura.
- Proteja fácilmente a los invitados, al personal de fusiones y adquisiciones o a cualquiera que necesite acceso temporal.
- Amplíe la Seguridad Sincronizada a los empleados remotos e híbridos.
- Protéjase contra ataques y filtraciones.



Qué ofrece Sophos Workspace Protection



Frene la TI en la sombra:

Supervise y controle el uso no autorizado de aplicaciones web y SaaS.



Posibilite la adopción de la IA generativa:

Fomente y supervise sus soluciones de IA autorizadas, controle el acceso y restrinja el movimiento de datos.



Proteja a los empleados en Internet:

Aplique políticas coherentes para las aplicaciones web y el acceso desde cualquier lugar.



Prevenga costosos errores relacionados con los datos:

Bloquee la función de copiar y pegar o el intercambio de datos confidenciales con sitios web y apps para evitar errores de filtración de datos.



Proteja sus aplicaciones:

Proporcione un acceso seguro a sus propias aplicaciones alojadas, al tiempo que las hace invisibles para el mundo exterior.



Acceso seguro para invitados:

Permita que los invitados, contratistas o personal de adquisiciones accedan fácilmente a sus aplicaciones y sistemas.



Amplíe la Seguridad Sincronizada:

Utilice la Seguridad Sincronizada de Sophos para bloquear temporalmente el acceso de los dispositivos vulnerados a aplicaciones y sistemas importantes.



Protéjase de las filtraciones:

Proteja la red contra posibles filtraciones que puedan surgir de los sistemas, las aplicaciones y los empleados expuestos a Internet.



Mejore la seguridad del correo electrónico:

Mejora la postura de seguridad del correo electrónico con una capa adicional de protección que complementa las defensas existentes.

Sencillo, asequible y seguro

Sophos Workspace Protection es más asequible y sencillo que las soluciones SASE o SSE basadas en la nube, no requiere redireccionamiento del tráfico ni descifrado Man-in-the-Middle, y es fácil de desplegar y escalar. Se trata de una sencilla app que ya utiliza, el navegador, que protege todas las demás apps, y todo ello gestionado desde una única consola en la nube: Sophos Central. Sophos Protected Browser convierte lo que ha sido un riesgo para la seguridad en un activo de seguridad reforzado.

Unifique y amplíe su protección de firewall y de endpoints

Los firewalls protegen la red, los endpoints protegen los dispositivos y Sophos Workspace Protection protege todo lo demás: sus aplicaciones, datos, empleados e invitados. Unifica y amplía la protección de red y de endpoints para proteger el espacio de trabajo. Además, ofrece un mejor rendimiento junto con Sophos Firewall y Sophos Endpoint, ya que amplía la Seguridad Sincronizada con Security Heartbeat a los empleados remotos e híbridos. Si un dispositivo se ve afectado, las políticas de Heartbeat pueden impedir que se conecte a aplicaciones y datos importantes hasta que se limpie.

Sistema de licencias sencillo para mayor rentabilidad

Comprar Sophos Workspace Protection no podría ser más fácil, gracias a su sencillo sistema de licencias por usuario y sus atractivos precios:

- **Paquete independiente:** compre Sophos Workspace Protection por separado y benefíciase de todos sus componentes, como Sophos Protected Browser, Sophos ZTNA, Sophos DNS Protection for Endpoints y Sophos EMS, que funciona con cualquier firewall o solución para endpoints.
- **Junto con Sophos Endpoint :** con un práctico paquete para facilitar la compra de ambos productos, que mejoran su rendimiento cuando se usan con la Seguridad Sincronizada, ambos gestionados desde Sophos Central.
- **Junto con Sophos Firewall:** amplíe la seguridad de la red a los empleados remotos e híbridos y a los invitados, proteja sus apps con ZTNA y mucho más, todo ello gestionado desde Sophos Central.

Sophos Workspace Protection es el complemento perfecto para cualquier instalación nueva o existente de Sophos.

Especificaciones técnicas

Los productos de Sophos Workspace Protection están diseñados para adaptarse perfectamente a sus entornos existentes, integrándose con los proveedores de identidad y las plataformas más populares.

Proveedores de identidad:

ZTNA y Endpoint DNS Protection:

Microsoft Active Directory (local), Microsoft Entra ID (Azure Active Directory), Okta

Protected Browser:

Microsoft Entra ID (Azure Active Directory), Okta

Sistemas operativos y plataformas:

Puerta de enlace ZTNA:

VMware ESXi 7+, Hyper-V 2016+ y Sophos Firewall

Agente ZTNA:

Windows 10, Windows 11 (procesadores de Intel y ARM); macOS Sonoma, Sequoia, Tahoe (procesadores de Intel y Apple)

Endpoint DNS Protection:

Windows 10, Windows 11 (procesadores de Intel y ARM)

Protected Browser:

Windows 10, Windows 11, Windows Server 2022, Windows Server 2025, (solo procesadores de Intel; en breve, también de ARM); macOS Sonoma, Sequoia, Tahoe (procesadores de Intel y Apple)

Postura del dispositivo:

Agente ZTNA:

Sophos Security Heartbeat (Sophos Endpoint)

Protected Browser:

Sistema operativo, Endpoint Protection (Sophos y otros proveedores) y estado del cifrado de disco

Especificaciones de la puerta de enlace ZTNA

VM recomendada:

Doble núcleo / 4 GB

Clústeres de múltiples nodos:

Las VM pueden agruparse en clústeres con hasta 9 nodos y Sophos Firewall puede desplegarse en HA para aumentar el rendimiento, la capacidad y la continuidad de las actividades de la puerta de enlace

Capacidad y escalado de los nodos:

10 000 conexiones de agente para un solo nodo; hasta 90 000 conexiones de agente en un clúster (9 nodos como máximo)

Obtenga más información e inicie una prueba gratuita en es.sophos.com/workspace-protection.

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

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