BROCHURE DE LA SOLUTION

Sophos Workspace Protection

Protection simple et abordable pour les travailleurs distants et hybrides

Sophos Workspace Protection vous permet de reprendre le contrôle sur votre espace de travail professionnel. Sécurisez l'accès à vos applications, vos données, vos employés et vos invités, en tout lieu, aisément et à moindre coût.

La manière dont nous travaillons a évolué

Le périmètre du réseau n'existe plus. Les employés, les applications et les données n'ont plus de frontières. Vous possédez et hébergez des applications privées ou louez des applications SaaS, et tout le monde utilise quotidiennement des applications, des services et des sites Internet. La plupart des organisations disposent également d'une main-d'œuvre hybride composée d'employés sur site, de télétravailleurs ou d'employés itinérants qui peuvent se trouver au bureau, à domicile, en déplacement, voire dans des lieux publics. Tout cela représente un défi incroyable pour toute organisation qui souhaite correctement surveiller, contrôler et sécuriser son infrastructure informatique.

Les solutions SASE ou SSE traditionnelles fournies dans le Cloud coûtent cher à exploiter et sont donc intrinsèquement chères à l'achat. Elles nécessitent le renvoi du trafic vers des points de présence dans le Cloud pour inspection, ainsi qu'un déchiffrement de type «man-in-the-middle», ce qui ajoute une latence indésirable et crée des problèmes d'utilisabilité. Une meilleure solution s'impose. Et elle est désormais disponible avec Sophos Workspace Protection.

Protéger vos applications, vos données, vos employés et vos invités

Sophos Workspace Protection offre une solution simple et abordable pour protéger vos applications, vos données, vos employés et vos invités, où qu'ils se trouvent. La solution utilise une seule application, le navigateur, pour intégrer toute la protection dont vous avez besoin. Il n'y a donc pas de latence du trafic, pas de traitement dans le Cloud, pas de déchiffrement supplémentaire, juste une expérience transparente et sécurisée.

Ce que vous obtenez

Sophos Protected Browser

Fournit une seule application pour protéger toutes vos autres applications. Le composant intègre l'accès réseau Zero Trust, la protection DNS, le contrôle des applications SaaS, une passerelle Web sécurisée et le contrôle des données locales dans un navigateur Chromium renforcé, familier et totalement transparent.

Sophos ZTNA

Fournit un accès sécurisé uniquement aux applications dont les utilisateurs ont besoin, tout en les rendant invisibles pour tous les autres utilisateurs, y compris le monde extérieur, les protégeant ainsi contre les attaques.

Sophos DNS Protection for Endpoints

Ajoute une couche de sécurité supplémentaire pour protéger contre les contenus Web malveillants et indésirables, tant dans le navigateur que dans les applications Web, où que se trouvent les employés.

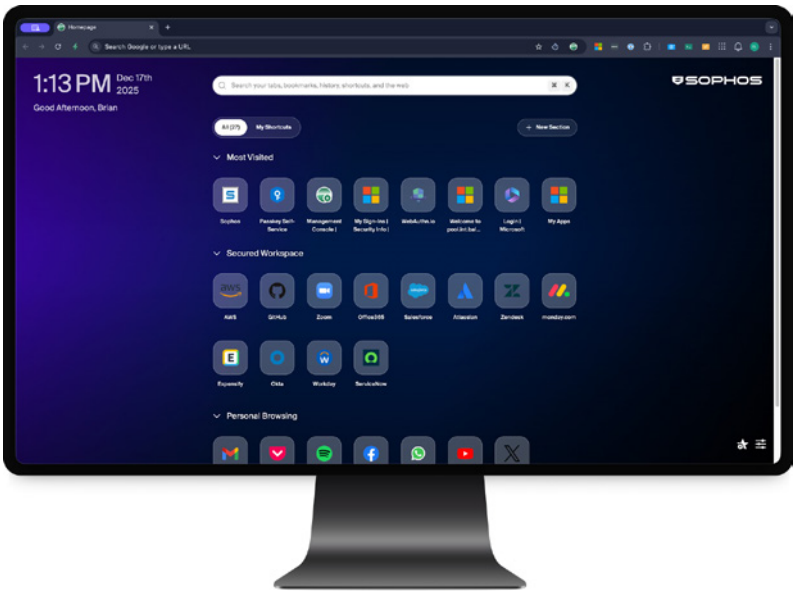
Sophos Email Monitoring System

Fonctionne avec vos solutions de protection de la messagerie en place afin de renforcer la sécurité, la visibilité et le reporting sur les menaces avancées ciblant les emails que d'autres solutions ne détectent pas.

AVANTAGES

- Protégez vos applications, vos données, vos employés et vos invités.
- Permettez un accès sécurisé à vos applications tout en les protégeant contre les attaques.
- Éliminez le Shadow IT et adoptez en toute sécurité les nouvelles technologies telles que l'IA générative.
- Protégez les employés sur Internet et appliquez des politiques de navigation sécurisée.
- Protégez aisément les invités ou toute autre personne ayant besoin d'un accès temporaire.
- Étendez la Sécurité Synchronisée aux employés à distance et hybrides.
- Protégez contre les attaques et les violations.

SOPHOS



Les points forts de Sophos Workspace Protection

Éliminer le Shadow IT :
Surveillez et contrôlez l'utilisation non autorisée des applications Web et SaaS.

Faciliter l'adoption de l'IA générative :
Encouragez l'adoption et surveillez vos solutions d'IA autorisées, contrôlez l'accès et limitez les mouvements de données.

Protéger les employés sur le web :
Appliquez des politiques de sécurité cohérentes pour les applications Web et l'accès, en tout lieu.

Éviter les erreurs coûteuses liées aux données :
Bloquez le copier-coller ou l'échange de données sensibles avec des sites Web et des applications afin de prévenir les fuites de données.

Protéger vos applications :
Offrez un accès sécurisé à vos propres applications hébergées tout en les rendant invisibles au monde extérieur.

Sécuriser l'accès des invités :
Accordez aisément l'accès à vos applications et systèmes aux invités, sous-traitants ou personnel chargé des acquisitions.

Étendre la Sécurité Synchronisée :
Utilisez la Sécurité Synchronisée de Sophos pour empêcher temporairement les appareils compromis d'accéder aux applications et aux systèmes importants.

Protéger contre les violations :
Protégez votre réseau contre les violations potentielles pouvant résulter de l'exposition à Internet des systèmes, des applications ou des employés.

Renforcer la sécurité de vos messageries :
Renforcez la sécurité de vos messageries grâce à une couche de sécurité supplémentaire qui complète vos défenses existantes.

Facile, abordable, sécurisé

Sophos Workspace Protection est plus simple et plus abordable que les solutions SASE ou SSE fournies dans le Cloud. Elle ne nécessite pas de latence ni de déchiffrement intermédiaire, et est facile à déployer et à dimensionner. Vous obtenez une application simple que vous utilisez déjà : un navigateur, qui protège toutes vos autres applications, le tout géré à partir d'une seule console Cloud : Sophos Central. Sophos Protected Browser transforme ce qui était auparavant une faille de sécurité en un puissant atout en matière de sécurité.

Unifier et étendre la protection de votre pare-feu et de votre protection Endpoint

Les pare-feux protègent votre réseau, les solutions Endpoint protègent vos appareils, et Sophos Workspace Protection protège tout le reste : vos applications, vos données, vos employés et vos invités. La solution unifie et étend la protection de votre réseau et de vos terminaux afin de sécuriser l'espace de travail. Elle fonctionne de façon optimale avec Sophos Firewall et Sophos Endpoint en étendant la fonction du Security Heartbeat synchronisé à vos employés distants et hybrides. Si un appareil est compromis, les stratégies Heartbeat peuvent l'empêcher de se connecter à des applications et données importantes jusqu'à ce qu'il soit nettoyé.

Licences simples — excellent rapport qualité-prix

L'achat de Sophos Workspace Protection est on ne peut plus simple grâce à un système de licence par utilisateur et à des tarifs attractifs :

- **Standalone :** Achetez Sophos Workspace Protection en version standalone et bénéficiez de toutes les composantes dont Sophos Protected Browser, Sophos ZTNA, Sophos DNS Protection for Endpoints et Sophos EMS, qui fonctionnent avec n'importe quel pare-feu ou solution Endpoint.
- **Achetez avec Sophos Endpoint : un bundle pratique pour simplifier l'achat des deux produits qui fonctionnent en parfaite synergie grâce à la Sécurité Synchronisée, tous deux gérés depuis Sophos Central.**
- Achetez avec Sophos Firewall : **étendez la sécurité de votre réseau aux travailleurs distants et hybrides ainsi qu'aux invités, protégez vos applications avec une solution ZTNA, et bien plus encore, le tout géré depuis Sophos Central.**

Sophos Workspace Protection est le complément idéal à toute installation Sophos existante ou nouvelle.

Spécifications techniques

Les produits Sophos Workspace Protection sont conçus pour s'intégrer parfaitement à vos environnements existants, en s'adaptant aux fournisseurs de solutions de gestion des identités et aux plateformes les plus courants.

Fournisseurs d'identité :

ZTNA et Endpoint DNS Protection :
Microsoft Active Directory (sur site), Microsoft Entra ID (Azure Active Directory), Okta

Navigateur protégé :
Microsoft Entra ID (Azure Active Directory), Okta

Systèmes d'exploitation et plateformes :

Passerelle ZTNA :
VMware ESXi 7+, Hyper-V 2016+ et Sophos Firewall

Agent ZTNA :
Windows 10, Windows 11 (processeurs Intel et ARM) ; macOS Sonoma, Sequoia, Tahoe (processeurs Intel et Apple)

Endpoint DNS Protection :
Windows 10, Windows 11 (processeurs Intel et ARM)

Navigateur protégé :
Windows 10, Windows 11, Windows Server 2022, Windows Server 2025 (processeurs Intel uniquement — ARM bientôt disponible) ; macOS Sonoma, Sequoia, Tahoe (processeurs Intel et Apple)

Posture de l'appareil :

Agent ZTNA :
Sophos Security Heartbeat (Sophos Endpoint)

Navigateur protégé :
Système d'exploitation, protection Endpoint (Sophos et autres fournisseurs) et état du chiffrement des disques

Spécifications de la passerelle ZTNA

VM recommandée :
2 cœurs / 4 Go

Clustering multinœuds :
Les machines virtuelles peuvent être regroupées en clusters comprenant jusqu'à 9 nœuds et Sophos Firewall peut bénéficier d'un déploiement en HA pour améliorer les performances, la capacité et la continuité opérationnelle de la passerelle.

Capacité et scalabilité des nœuds :
10 000 connexions d'agents pour un seul nœud, jusqu'à 90 000 connexions d'agents dans un cluster (9 nœuds max.)

Pour en savoir plus et commencer votre essai gratuit : sophos.fr/workspace-protection

Sophos France
Tél. : +33 1 34 34 80 00
Email : info@sophos.fr

2026-01-07 BR-FR (DD)