

SOPHOS

Sophos XG Firewall pour le secteur de l'éducation

Conçu pour l'éducation.

Optimisé pour le secteur de l'éducation, XG Firewall offre une visibilité et des informations incomparables, un contrôle et une sécurité de pointe, et des capacités uniques de réponse aux menaces. Ses capacités puissantes vous aident à contrôler ce qu'il se passe sur votre réseau, à administrer votre pare-feu et à remédier aux menaces.



Conçu pour l'éducation

XG Firewall est doté de fonctionnalités conçues pour aider les institutions éducatives à faire face aux défis quotidiens.

Politique de filtrage Web puissante

XG Firewall utilise un modèle de politique Web puissant mais intuitif, que l'on ne retrouve habituellement que dans des produits professionnels entièrement dédiés au filtrage du Web à des prix bien supérieurs. Il facilite la gestion des politiques de sécurité personnalisées basées sur les utilisateurs et les groupes. De plus, il contient aussi des politiques embarquées pour la protection des mineurs sur Internet et les activités dites « non adaptées aux écoles ». Vous pouvez les utiliser dès la mise en service et les modifier selon vos besoins spécifiques. Vous obtenez également le contrôle total sur SafeSearch, YouTube et les téléchargements de fichiers dans le cadre de chaque politique.

Protection des enfants et conformité

Les cadres juridiques, tels que la loi CIPA (Child Information Protection Act) aux États-Unis, les directives Safeguarding and Prevent Duty of Care au Royaume-Uni et d'autres initiatives similaires dans d'autres juridictions, comme la CNIL en France, sont élaborés pour assurer la sécurité des jeunes utilisateurs en ligne. Bien qu'indispensables, ces cadres représentent un défi de taille pour de nombreuses organisations. XG Firewall offre donc des fonctionnalités intégrées et des paramètres de politique qui aident les organisations à rester en conformité, de manière simple et rapide. XG Firewall inclut des politiques embarquées pour la protection des mineurs et pour des activités prédéfinies, par exemple « non adaptées aux écoles », en plus de fonctionnalités telles que les restrictions Safesearch et YouTube, et le filtrage de mots clés.

Filtrage contextuel par mots clés

XG Firewall vous aide à identifier très tôt des comportements potentiellement problématiques. Il peut enregistrer, surveiller et même appliquer les politiques de sécurité relatives à des listes de mots clés associées au harcèlement, à la radicalisation ou à l'automutilation (par exemple). Vous pouvez programmer des rapports pour identifier les utilisateurs à risque et obtenir des informations détaillées sur leurs activités, notamment la nature et l'endroit où ils postent ainsi que les sites visités.

Aperçu des principaux utilisateurs à risque

Notre Quotient de menace utilisateur (QMU) fournit des informations utiles sur le comportement des utilisateurs. XG Firewall regroupe les données sur les habitudes de navigation de chaque utilisateur en se basant sur l'historique et les éléments considérés comme

malveillants, afin d'identifier les utilisateurs présentant un comportement risqué en ligne. Il vous permet de prendre des mesures immédiates à l'égard des élèves présentant des comportements dangereux pour eux-mêmes ou pour votre réseau. Configurez les rapports pour qu'ils soient envoyés automatiquement aux enseignants ou aux CPE, pour tenir ces derniers informés des élèves à risque.

Protection de pointe contre les menaces

XG Firewall contient toutes les dernières technologies de protection contre les menaces dont vous avez besoin pour stopper net dans leur élan les piratages et les attaques. La technologie de Sandboxing de Sandstorm analyse dans un environnement sécurisé tous les fichiers qui arrivent par le Web ou par email à la recherche de comportements malveillants. Elle utilise pour cela la technologie du Deep Learning d'Intercept X, notre produit Endpoint Next-Gen. Notre Système de prévention des intrusions (IPS) de premier plan détecte tous les piratages ou les attaques tentant d'exploiter une faille sur le réseau. Et notre solution de protection Web effectue une émulation de JavaScript pour détecter les menaces qui se cachent dans des sites Web compromis, comme le cryptojacking.

Prise en charge de Chromebook

XG Firewall prend en charge davantage de méthodes d'authentification que tout autre pare-feu (y compris les services d'annuaire, basés sur les clients, sans client, et bien sûr les Chromebook) avec un agent facile à déployer qui permet à tous les utilisateurs de se doter de politiques et de rapports basés sur les besoins de leurs clients.

Sécurité synchronisée

XG Firewall s'intègre avec Sophos Intercept X pour offrir une protection ultime au niveau du réseau et des systèmes Endpoint, tout en permettant d'activer les fonctionnalités de la sécurité synchronisée. La fonction Security Heartbeat™ partage des informations en temps réel entre les systèmes Endpoint protégés par Sophos et le pare-feu. XG Firewall peut ainsi isoler automatiquement tout système compromis ou infecté jusqu'à ce que ce dernier soit nettoyé, empêchant ainsi la propagation des menaces. Vous obtenez également une idée précise des applications non identifiées sur votre réseau, car chiffrées ou évanescentes. Ces avantages supplémentaires en matière de visibilité, de protection et de réponse ne sont possibles qu'avec la sécurité synchronisée de Sophos.

Puissant. Simple. Abordable.

Sophos XG Firewall fournit dans un package extrêmement abordable toute la visibilité, la sécurité et le contrôle dont les établissements scolaires ont besoin, tout en facilitant la gestion quotidienne et la création de rapports.

Architecture Xstream

XG Firewall renouvelle la manière dont nous identifions les risques cachés, protégeons contre les menaces et répondons aux incidents sans nuire aux performances. Notre architecture Xstream pour XG Firewall utilise une architecture unique de traitement des paquets qui offre des niveaux extrêmes de visibilité, de protection et de performance.

La sécurité et un contrôle de pointe

XG Firewall offre toutes les technologies avancées dont vous avez besoin pour protéger votre réseau des ransomwares et des menaces avancées les plus récentes. Vous obtenez également la meilleure protection et la meilleure application des politiques de filtrage Web disponibles, dans une console facile à configurer et à administrer.

Une réponse incomparable aux menaces

Sophos XG Firewall est la seule solution de sécurité des réseaux capable d'identifier totalement la source d'une infection sur votre réseau et, en réponse, de limiter automatiquement l'accès aux autres ressources du réseau. Cela est possible grâce à notre Security Heartbeat™ qui partage des données télémétriques et l'état de sécurité entre les systèmes Endpoint protégés par Sophos et XG Firewall.

Connectez-vous et économisez avec le SD-WAN

Connecter les écoles dans votre collectivité peut se révéler très coûteux. C'est pourquoi nous avons intégré le SD-WAN, ou Software-Defined Wide Area Networking, dans nos pare-feu XG. Avec le SD-WAN, connectez chaque école à votre collectivité pour un coût bien inférieur au prix du MPLS (Multi-Protocol Label Switching). Transmettez en toute sécurité des informations sensibles sur les élèves et le personnel entre différents sites. Suivez le rythme d'évolution des technologies et des applications éducatives sur le réseau. Et obtenez des performances et une disponibilité constantes pour les applications Cloud, telles que Dropbox Education, G Suite, ClassDojo et autres, dans les salles de classe et les bureaux administratifs, où qu'ils se trouvent.

Une valeur exceptionnelle, un prix extrêmement abordable

XG Firewall a été conçu pour offrir d'excellentes performances et une efficacité en matière de sécurité garantissant un retour sur investissement optimal. XG Firewall se retrouve constamment parmi les mieux notés du marché dans les tests indépendants, et aucun autre pare-feu que XG Firewall n'offre autant dans une seule appliance.

Gestion et édition de rapports en toute simplicité

XG Firewall facilite la gestion et l'extraction d'informations sur votre réseau. Avec Sophos Central Firewall Manager vous pouvez administrer un ou plusieurs pare-feu XG depuis n'importe quel endroit. Tout commence par un tableau de bord propre et informatif et des indicateurs tricolores qui vous signalent immédiatement ce qui requiert votre attention dès que vous vous connectez. Sophos Central Firewall Reporting fournit les outils et la flexibilité nécessaires pour créer des rapports personnalisés qui offrent un aperçu instantané des applications, des risques, des tendances, etc. qui ont un impact sur votre réseau. Le service est disponible dans le Cloud sans frais supplémentaire. De plus, notre politique de filtrage Web est sans pareil avec son ensemble d'outils puissants mais intuitifs pour gérer la conformité sur votre réseau. Le personnel éducatif peut aussi aider à la gestion quotidienne des exceptions de politique Web pour leurs programmes d'étude en classe.



Comment acheter

Choisissez la protection dont vous avez besoin :



Protection réseau

Prévention des intrusions de premier ordre, Deep Learning et technologie avancée de protection contre les menaces pour stopper net les menaces les plus récentes dans leur élan.



Protection Sandstorm

Technologie Next-Gen de sandboxing dans le Cloud qui intègre le Deep Learning, la détection des exploits et CryptoGuard pour détecter les dernières menaces basées sur des fichiers.



Protection Web

Filtrage et protection puissants du Web à l'aide du filtrage du contenu par mots clés, du contrôle de SafeSearch et YouTube, et de l'identification et du contrôle des applications.



Security Heartbeat™

Relie vos systèmes d'extrémité protégés par Sophos à XG Firewall pour fournir une visibilité maximale sur la santé du réseau, une défense coordonnée contre les attaques et un isolement automatique des terminaux.



Protection de la messagerie

Obtenez une sécurité totale des protocoles de messagerie SMTP, POP et IMAP contre le spam, le phishing et la perte de données grâce à notre protection tout-en-un qui allie le chiffrement des emails basé sur les politiques, le DLP et l'antispam.



Protection des serveurs Web

Renforcez vos serveurs de fichiers et serveurs Web contre les tentatives de piratage tout en offrant un accès sécurisé aux utilisateurs externes grâce à l'authentification reverse proxy.

Bundles avantageux Sophos XG Firewall

Pour une solution ultime en matière de protection, de valeur, de tranquillité d'esprit, choisissez l'un de nos avantageux bundles :

EnterpriseProtect Plus est notre bundle pare-feu Next-Gen optimisé. Il inclut une appliance matérielle de la série XG, le support avancé, et tout ce dont vous avez besoin pour la protection réseau, la protection Web, le contrôle des applications et le sandboxing.

TotalProtect Plus est votre bundle de protection totale. Il inclut une appliance matérielle de la série XG, le support avancé, et notre gamme complète de protections, y compris la protection des réseaux, du Web, du sandboxing, de la messagerie et des serveurs Web.

Essai gratuit de 30 jours sans engagement

Pour évaluer toutes les fonctionnalités de XG Firewall, inscrivez-vous à un essai gratuit de 30 jours.

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

© Copyright 2020. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

20-01-16 FR (NP)

SOPHOS