
SOLUTIONS DE SÉCURITÉ
INFORMATIQUE
KASPERSKY lab
FORTINET
SOPHOS
SISTEK

SOPHOS

Sophos Firewall

Une protection et des performances puissantes

Les appliances de la série XGS dotées de processeurs de flux Xstream dédiés permettent une accélération applicative incomparable, l'inspection haute performance des flux chiffrés TLS, et une protection puissante contre les menaces.

Une protection et des performances puissantes

L'architecture Xstream de Sophos Firewall est conçue pour offrir des niveaux de visibilité, de protection et de performances optimaux permettant de répondre aux défis actuels et futurs.

Inspection des flux chiffrés

Environ 99 % du trafic web est désormais chiffré, le rendant invisible aux yeux de la plupart des pare-feux. De nombreuses entreprises ne parviennent pas à protéger efficacement leurs réseaux contre un nombre croissant de ransomwares, de menaces et d'applications potentiellement indésirables qui exploitent ce manque de visibilité.

Sophos Firewall résout ce problème en permettant aux entreprises de toutes tailles d'utiliser l'inspection des flux chiffrés TLS sans compromettre leurs performances. Nos nouvelles appliances de la série XGS avec processeurs de flux Xstream intégrés placent le trafic TLS sur le FastPath pour une inspection accélérée. De plus, notre moteur d'inspection TLS hautes performances prend en charge le protocole TLS 1.3 sans baisse de performances, ainsi que les dernières suites de chiffrement pour une compatibilité maximale. Il offre également une visibilité accrue sur les flux de trafic chiffré directement dans le tableau de bord. Sophos Firewall met en œuvre une inspection TLS efficace, même pour les réseaux les plus exigeants.

Deep Packet Inspection (DPI)

Vous ne devriez jamais avoir à choisir entre sécurité et performances. Sophos Firewall inclut un moteur d'inspection profonde des paquets (DPI) performant permettant l'analyse en temps réel des flux de communications pour y débusquer les menaces dissimulées. Cette nouvelle architecture combine à la fois performance et sécurité. La pile du pare-feu peut s'appuyer sur le moteur DPI pour réduire considérablement la latence et améliorer l'efficacité globale.

Sophos Firewall bloque les ransomwares et les techniques de piratage les plus récentes avec le moteur DPI haute performance, comprenant un IPS Next-Gen, la protection Web et le contrôle des applications, ainsi que le Deep Learning et la technologie de sandboxing optimisés par SophosLabs Intelix.

Accélération applicative

La plupart des flux réseau sont considérés comme sains et non nocifs (par exemple : trafic réseau à destination de bureaux détachés, télétravailleurs, serveurs applicatifs connus et identifiés, etc.). Ils ne nécessitent pas d'analyse de sécurité profonde, puisqu'ils sont reconnus comme sains et ne transportent pas de charge malicieuse. Une fois classifiés et reconnus sans ambigüité ces flux de données peuvent être traités directement par le FastPath pour permettre de réduire la latence et l'optimisation de la consommation des ressources. Celles-ci peuvent donc être utilisées pour effectuer une analyse approfondie des flux le nécessitant.

Sophos Firewall accélère le trafic SaaS, SD-WAN et Cloud (comme la VoIP, la vidéo et d'autres applications reconnues comme saines) à l'aide de politiques automatiques ou personnalisées en les plaçant sur le FastPath via le processeur de flux Xstream.

SD-WAN

Gérer le routage du trafic applicatif sur plusieurs liaisons WAN et interconnecter un réseau distribué sont des éléments essentiels de toute solution SD-WAN. Souvent, ces tâches sont beaucoup plus difficiles qu'elles ne devraient l'être.

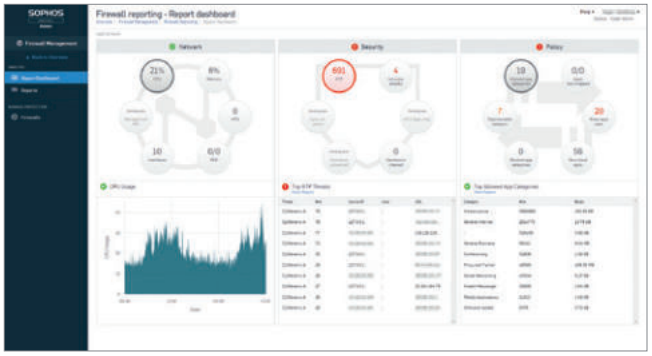
Sophos Firewall avec Xstream SD-WAN offre une solution SD-WAN puissante et intégrée, comprenant la sélection et le routage des liaisons basés sur les performances, l'équilibrage des charges, des transitions sans impact entre les liaisons en cas de perturbation, une orchestration centrale gérée dans le Cloud et l'accélération Xstream FastPath du trafic des tunnels VPN. Sophos Firewall avec Xstream SD-WAN est une solution SD-WAN parmi les meilleures et les plus flexibles disponibles aujourd'hui dans un pare-feu.

Sophos Central

Sophos Central est la plateforme de gestion basée dans le Cloud, qui permet d'administrer vos pare-feux et l'ensemble des solutions de sécurité Sophos.

Gestion dans Sophos Central

Reporting dans Sophos Central



Gestion simple de pare-feux multiples

Sophos Central est la plateforme de gestion Cloud, pour tous vos produits Sophos. Elle facilite l'installation, la surveillance et la gestion quotidienne de Sophos Firewall. Elle offre également des fonctionnalités pratiques comme des alertes, la gestion des sauvegardes, les mises à jour du firmware en un clic et le déploiement rapide de nouveaux pare-feux.

- Administrer tous vos Sophos Firewall et autres produits Sophos depuis une console unique
- Définir des politiques de sécurité pour un seul ou un ensemble de pare-feux.
- Planifier la sauvegarde de la configuration de vos pare-feux et définir leur récurrence
- Programmer les mises à jour de firmware pour l'ensemble de votre réseau en seulement quelques clics

L'option Gestion dans Sophos Central est disponible sans frais supplémentaires.

Création de rapports de pare-feu dans le Cloud

Sophos Central inclut des outils puissants de reporting qui vous permettent de visualiser l'activité et la sécurité de votre réseau, du Web et des applications au cours du temps. Vous bénéficiez d'une variété de rapports intégrés avec des outils puissants pour créer vos propres rapports personnalisés. Vous créez les rapports que vous voulez, comme vous le voulez.

- Augmentez votre visibilité sur l'activité du réseau grâce aux analyses
- Analysez les données pour identifier les failles de sécurité, les comportements suspects des utilisateurs et tout autre événement nécessitant des changements de politique
- Utilisez les modules prédéfinis ou personnalisez chaque rapport pour des scénarios d'utilisation spécifiques

L'option Reporting dans Sophos Central est disponible sans frais supplémentaires pour stocker jusqu'à 7 jours de données de rapport. Les options premium, qui permettent de conserver les données plus longtemps et offrent des fonctionnalités supplémentaires, peuvent être achetées en option, soit individuellement, soit dans le cadre d'autres abonnements ou offres groupées.

Déploiement Zero-touch

Dans Sophos Central, créez une configuration pour un pare-feu Sophos Firewall que vous pourrez ensuite déployer à votre convenance, par exemple sur un site distant. Il n'est pas nécessaire d'avoir du personnel technique sur place, il vous suffit de stocker le fichier de configuration sur une clé USB et de démarrer l'appliance avec la clé USB connectée.

Orchestration SD-WAN

Sophos Central simplifie et facilite l'interconnexion des réseaux superposés SD-WAN entre plusieurs pare-feux Sophos Firewall. En quelques clics, vous pouvez configurer un réseau maillé complet, une topologie en étoile ou un mix des deux, et Sophos Central configurera automatiquement toutes les règles nécessaires d'accès au tunnel VPN et au pare-feu pour activer votre réseau SD-WAN.

Pour en savoir plus sur le système de cybersécurité Sophos Central, visitez sophos.fr/firewall-central.

Sécurité Synchronisée

Security Heartbeat™ : Votre pare-feu et vos systèmes d'extrémité communiquent enfin

Sophos Firewall est la seule solution de sécurité réseau capable d'identifier totalement l'utilisateur et 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 fonction Sophos Security Heartbeat qui partage des données télémétriques et l'état de sécurité entre les systèmes d'extrémité protégés par Sophos Endpoint et le pare-feu, et qui intègre la sécurité des systèmes d'extrémité dans les règles de pare-feu afin de contrôler l'accès et d'isoler les systèmes compromis.

Ce processus est entièrement automatique et permet à de nombreuses entreprises et organisations de gagner du temps et de l'argent dans la protection de leurs environnements.

Contrôle synchronisé des applications

Le Security Heartbeat nous permet de faire plus que de simplement vérifier l'état de sécurité d'un système. C'est également une solution à l'un des plus gros problèmes auxquels font face les administrateurs réseau aujourd'hui : le manque de visibilité sur le trafic réseau.

Le contrôle des applications synchronisées utilise les connexions Heartbeat pour identifier, classer et contrôler automatiquement le trafic applicatif. Toutes les applications chiffrées, personnalisées, évasives et HTTP/HTTPS génériques qui sont actuellement non identifiées seront révélées.

Ce que les pare-feux Next-Gen voient aujourd'hui | **Ce que Sophos Firewall voit**

Vous ne pouvez pas contrôler ce que vous ne voyez pas. Tous les pare-feux d'aujourd'hui dépendent des signatures statiques pour identifier les applications. Mais celles-ci sont inefficaces pour la plupart des applications personnalisées, méconnues, évasives et toutes celles utilisant un protocole HTTP ou HTTPS générique.

Sophos Firewall utilise la Sécurité Synchronisée pour identifier, classer et contrôler automatiquement toutes les applications inconnues. Il bloque facilement les applications non souhaitées tout en priorisant celles qui vous intéressent.

Protection contre les mouvements latéraux

La protection contre les mouvements latéraux isole automatiquement les systèmes compromis en tous points du réseau afin de stopper net les attaques dans leur élan. Les systèmes d'extrémité sains participent en ignorant tout le trafic provenant des systèmes compromis. Cela permet un isolement complet, y compris sur le même segment de réseau, et empêche les menaces et les attaquants de diffuser ou de voler des données.

Synchronisation de l'identifiant utilisateur

L'authentification des utilisateurs est d'une importance capitale dans un pare-feu Next-Gen, mais elle est souvent complexe à implémenter d'une manière simple et transparente. La synchronisation de l'identifiant utilisateur élimine le besoin d'agents d'authentification client ou serveur en partageant l'identité de l'utilisateur entre le système d'extrémité et le pare-feu via le Security Heartbeat. C'est un autre avantage notable offert par l'intégration et le partage d'informations entre votre pare-feu et vos systèmes d'extrémité.

SD-WAN synchronisé : Routage des applications puissant et fiable

Le SD-WAN synchronisé exploite la puissance de la Sécurité Synchronisée pour optimiser la sélection du chemin d'accès au WAN pour vos applications professionnelles importantes.

Avec le contrôle synchronisé des applications, les applications découvertes, qui resteraient autrement inconnues, peuvent être utilisées pour les critères de correspondance du trafic dans les politiques de routage SD-WAN. C'est encore une autre façon dont la Sécurité Synchronisée peut améliorer l'efficacité de votre réseau.

Protection puissante

Identifier. Bloquer. Sécuriser.

Notre pare-feu Next-Gen complet a été conçu pour exposer les risques cachés, bloquer les menaces connues et inconnues, et répondre automatiquement aux incidents.

Expose les risques cachés

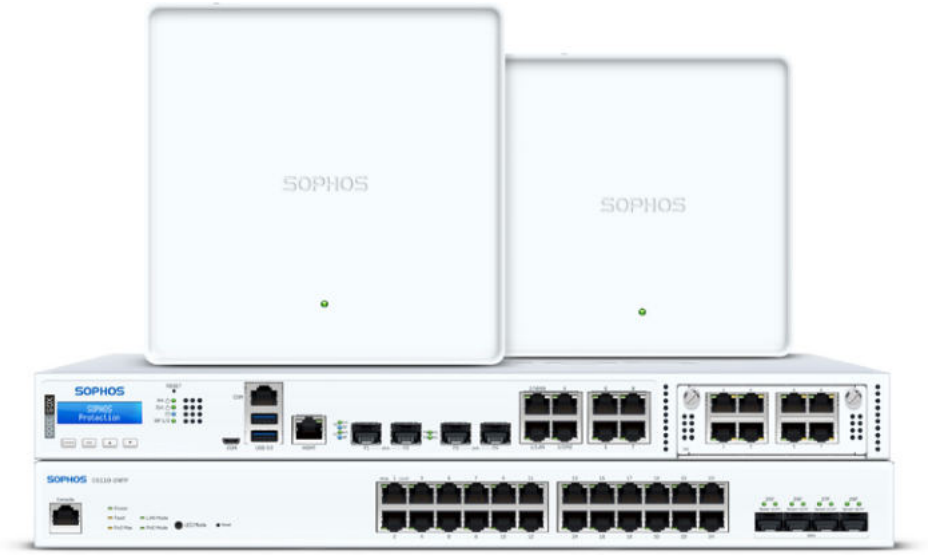
Reprenez le contrôle de votre réseau et obtenez des informations plus approfondies grâce à une visibilité supérieure sur les applications inconnues, les activités à risque, le trafic suspect et les menaces avancées.

Bloque les menaces inconnues

Les technologies puissantes de protection Next-Gen, comme le Deep Learning et la prévention des intrusions, protègent votre entreprise contre les attaques et techniques de piratage les plus récentes.

Répond automatiquement aux incidents

La réponse automatique aux incidents fournie par la Sécurité Synchronisée identifie et isole instantanément les systèmes compromis sur votre réseau pour empêcher les violations et les mouvements latéraux.



Sophos fournit l'ensemble des technologies de réseau gérées depuis une seule console : pare-feu, switchs et points d'accès.

Protection Xstream : Un seul package pour une protection ultime

Le pack de protection Xstream de Sophos Firewall offre toute la protection, les performances et la valeur ajoutée dont vous avez besoin pour optimiser même les réseaux les plus exigeants. Également disponible avec le modèle de la série XGS de votre choix.

Fonctionnalités du module 'Base Firewall'

- **Réseau et SD-WAN :** Sans fil, SD-WAN, routage prenant en compte les applications, régulation du trafic
- **Protection et performances :** Architecture Xstream avec flux de réseau FastPath, inspection TLS 1.3, inspection approfondie des paquets (DPI)
- **SD-WAN et VPN :** Xstream SD-WAN, IPsec/SSL de site à site et VPN d'accès à distance (illimité), SD-RED de site-à-site
- **Reporting :** Journalisation et reporting historiques prêts à l'emploi, reporting dans le Cloud dans Sophos Central (conservation des données de 7 jours)

Module 'Network Protection'

- **Inspection TLS Xstream :** Inspection TLS 1.3 avec des exceptions prédéfinies
- **Moteur DPI Xstream :** inspection approfondie des paquets en continu
- **IPS :** Prévention des intrusions Next-Gen
- **Protection avancée contre les menaces (ATP) :** Protection avancée contre les menaces (ATP)
- **Synchronized Security Heartbeat :** intégration avec Sophos Endpoint pour identifier et isoler les menaces
- **VPN sans client :** HTML5
- **VPN SD-RED :** Gestion des appareils SD-RED
- **Reporting :** Rapports d'activité détaillés du réseau et des menaces

Module 'Web Protection'

- **Inspection TLS Xstream :** Inspection TLS 1.3 avec des exceptions prédéfinies
- **Moteur DPI Xstream :** inspection approfondie des paquets en continu
- **Contrôle du Web :** par utilisateur, groupe, catégorie, URL, mot-clé
- **Protection contre les menaces Web :** malware, PUA, JavaScript malveillant, Pharming
- **Contrôle des applis :** par utilisateur, groupe, catégorie, risque, etc.
- **Contrôle synchronisé des applications :** intégration avec Sophos Endpoint pour identifier les applications inconnues
- **SD-WAN synchronisé :** utilise Le Contrôle synchronisé des applications pour acheminer les applications inconnues
- **Reporting :** Rapports détaillés sur l'activité des sites Web et des applications

Module 'Zero-Day Protection'

- **Inspection TLS Xstream :** Inspection TLS 1.3 avec des exceptions prédéfinies
- **Moteur DPI Xstream :** inspection approfondie des paquets en continu
- **Protection contre les menaces zero-day :** analyse tous les fichiers inconnus à l'aide de l'IA, du Machine Learning et du Sandboxing
- **Optimisé par SophosLabs Intelix :** intelligence et analyses basées dans le Cloud
- **Machine Learning:** utilise plusieurs modèles de Deep Learning
- **Sandboxing dans le Cloud :** analyse runtime dynamique des fichiers inconnus
- **Reporting :** Rapports détaillés de l'analyse de l'intelligence sur les menaces

Gestion dans Sophos Central

- **Gestion des groupes de pare-feux :** Politiques de sécurité synchronisées sur l'ensemble du groupe de pare-feux
- **Sauvegardes et mises à jour du firmware :** stockage et programmation
- **Déploiement zero-touch :** pour les nouveaux pare-feux depuis le Cloud

Orchestration dans Sophos Central

- **Orchestration SD-WAN :** Orchestration VPN de site à site en mode pointer-cliquer
- **Rapport de pare-feu dans le Cloud :** Rapports multi-pare-feux avec sauvegarde, planification et exportation des rapports (données conservées 30 jours)
- **Compatible XDR et MDR :** Prise en charge des services XDR et MDR

Module 'Enhanced Support'

Toutes les options de licence

Nous recommandons le pack de protection Xstream pour une sécurité optimale, mais si vous préférez personnaliser votre protection, tous les abonnements peuvent également être achetés individuellement.

Package de protection Xstream :	
Module 'Base License'	Mise en réseau, sans fil, architecture Xstream, VPN d'accès à distance illimité, VPN site à site, reporting
Module 'Network Protection'	Moteur Xstream TLS et DPI, IPS, ATP, Security Heartbeat, gestion de SD-RED, reporting
Module 'Web Protection'	Moteur Xstream TLS et DPI, sécurité et contrôle du Web, contrôle des applications, reporting
Module 'Zero-Day Protection'	Analyse des fichiers par Machine Learning et sandboxing, reporting
Module 'Central Orchestration'	Orchestration VPN SD-WAN, Central Firewall Reporting Advanced (30 jours), Compatible MDR/XDR
Module 'Enhanced Support'	Support 24/7, mises à jour des fonctionnalités, garantie de remplacement en cas de défaillance matérielle (soumis à contrat)

Protection personnalisée : si vous n'avez besoin que d'une protection de base ou si vous souhaitez personnaliser votre protection, vous pouvez choisir le pack Standard Protection ou acheter l'un des modules de protection séparément.

Pack 'Standard Protection' :	
Module 'Base License'	Mise en réseau, sans fil, architecture Xstream, Xstream SD-WAN, VPN d'accès à distance illimité, VPN de site à site
Module 'Network Protection'	Moteur Xstream TLS et DPI, IPS, ATP, Security Heartbeat, gestion de SD-RED, reporting
Module 'Web Protection'	Moteur Xstream TLS et DPI, sécurité et contrôle du Web, contrôle des applications, reporting
Module 'Enhanced Support'	Support 24/7, mises à jour des fonctionnalités, garantie de remplacement en cas de défaillance matérielle (soumis à contrat)

Modules de protection supplémentaires :	
Module 'Email Protection'	Antispam, AV, DLP et chiffrement intégrés
Module 'Web Server Protection'	Pare-feu d'application Web

Gestion et reporting dans Sophos Central : tous les pare-feux Sophos Firewall incluent la gestion et le reporting dans le Cloud, sans frais supplémentaires.

Gestion et reporting dans Sophos Central (sans coût supplémentaire) :	
Gestion dans Sophos Central	Gestion des groupes de pare-feux, gestion des sauvegardes, planification des mises à jour du firmware
Sophos Central Firewall Reporting	Outils de rapport prédéfinis et personnalisables avec 7 jours de stockage dans le Cloud sans frais supplémentaires (voir les autres options).

Protection supplémentaire : étendez votre protection grâce à ces produits et services supplémentaires.

Services, produits et modules de protection supplémentaires :	
Managed Detection and Response	Threat Hunting, détection et réponse aux menaces 24/7 par une équipe d'experts (en savoir plus)
Sophos Intercept X Endpoint with XDR	Protection Endpoint Next-Gen dotée de fonctions EDR gérées dans Sophos Central (en savoir plus)
ZTNA	Solution Zero Trust Network Access gérée dans Sophos Central (en savoir plus)

Services, produits et modules de protection supplémentaires :	
Central Email Advanced	Antispam, antivirus, DLP, chiffrement gérés dans Sophos Central (en savoir plus)
Sophos Switch	Switchs gérés dans le Cloud (en savoir plus)

Support : le module Enhanced Support est inclus dans tous les packs de protection, mais vous pouvez encore améliorer votre expérience en le mettant à niveau.

Options de support supplémentaires :	
Module 'Enhanced Plus Support Upgrade'	Mettez à niveau votre support avec le support VIP, la garantie matérielle pour les modules complémentaires et l'option TAM (coût supplémentaire)

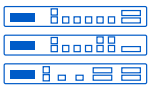
Options de licence pour le Cloud, les environnements virtuels et les appliances logicielles : si vous déployez Sophos Firewall dans le Cloud, dans un environnement virtuel ou en tant que logiciel sur votre propre matériel, le guide des licences ci-dessous peut vous aider à trouver la bonne option.

Modèle	*Instance AWS équivalente*	*VM Azure équivalente*	*Licence logicielle/ virtuelle***
XGS 87(w)	t3.medium	-	2C4
XGS 107(w)	c5.large	Standard_ F2s_v2	-
XGS 116(w)	-	-	4C6
XGS 2100	c5.xlarge	-	-
XGS 2300	m5.xlarge	Standard_ F4s_v2	6C8
XGS 3100	c5.2xlarge	Standard_ F8s_v2	8C16
XGS 4300	c5.4xlarge	Standard_ F16s_v2	16C24
XGS 5500	c5.9xlarge	Standard_ F32s_v2	Illimitée

* Basé sur les cœurs CPU et la RAM

Pour une liste complète des fonctionnalités incluses dans chaque abonnement de protection, veuillez consulter la liste des fonctionnalités de Sophos Firewall.

Options de déploiement

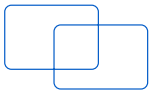


Série XGS

Appliances conçues sur mesure pour une performance incomparable.

AWS/Azure

Protégez l'infrastructure de votre réseau sur les plateformes de service Cloud AWS et Azure.



Virtuel

Installez sur VMware, Citrix, Microsoft Hyper-V et KVM.

Logiciel

Installez l'image Sophos Firewall OS sur votre propre matériel ou serveur Intel.

Cloud

Sophos Firewall offre les meilleures visibilité réseau, protection et réponse pour sécuriser vos environnements Cloud publics, privés et hybrides.

En tant que partenaire APN (AWS Partner Network) d'AWS, Sophos se positionne comme expert en compétences AWS, vendeur AWS Marketplace et partenaire AWS du secteur public.

Sophos Firewall est maintenant disponible dans AWS Marketplace avec la prise en charge de la scalabilité et un modèle de licence PAYG (pay-as-you-go) ou BYOL (bring your own license) pour répondre au mieux à vos besoins.

Sophos Firewall est certifié et optimisé pour Azure et est disponible sur Microsoft Azure Marketplace. Profitez d'un essai gratuit ou des options souples de licence PAYG ou BYOL.

Sophos Firewall est disponible pour Nutanix AHV et Nutanix Flow. Il apporte ainsi à la plateforme d'infrastructure hyperconvergente (HCI) leader du marché le meilleur pare-feu Next-Gen en matière de visibilité, de protection et de réponse. Profitez d'un essai gratuit de 30 jours en utilisant notre image KVM et nos licences flexibles.

Virtuel et logiciel

Sophos Firewall prend en charge une large gamme de plateformes de virtualisation et peut également être déployé en tant qu'appliance logicielle sur votre propre matériel Intel x86 :

Consultez la section Gestion des licences pour obtenir les options de licence disponibles.

Modules de protection

Vous avez un grand choix de modules pour personnaliser la protection offerte par votre pare-feu, selon vos besoins et votre scénario de déploiement.

Module 'Base Firewall'

La licence Base Firewall de Sophos inclut : architecture Xstream, mise en réseau, connexion sans fil, SD-WAN, VPN et reporting.

Architecture Xstream
Permet l'inspection TLS 1.3 haute performance, l'inspection approfondie des paquets et le flux de réseau FastPath pour accélérer le trafic des applications SaaS, SD-WAN et Cloud de confiance. Notez que les modules Network Protection et Web Protection sont nécessaires pour bénéficier de tous les avantages de l'architecture Xstream.

Xstream SD-WAN et mise en réseau
Comprend toutes les capacités SD-WAN, de mise en réseau et de routage, notamment un pare-feu avec état basé sur les zones, NAT, VLAN, les profils SD-WAN, la sélection et la surveillance des liaisons WAN en fonction des performances, l'équilibrage des charges, des transitions sans impact entre les liaisons WAN et l'accélération Xstream FastPath du trafic applicatif, IPSec, VPN et des flux de trafic chiffrés TLS.

Wi-Fi sécurisé
Contrôleur Wi-Fi intégré pour les points d'accès sans fil Sophos APX. La détection des points d'accès en mode plug-and-play facilite la configuration. Prend en charge plusieurs SSID, hotspots, réseaux pour les invités et diverses normes de chiffrement et de sécurité.

VPN
Fournit un VPN de site à site et d'accès à distance basé sur les normes (gratuit jusqu'à la capacité du pare-feu) avec prise en charge de IPsec et SSL. Le client VPN d'accès à distance Sophos Connect pour Windows et Mac offre des options de déploiement et de configuration simples et transparentes. Les tunnels de site à site de couche 2 de SD-RED offrent un VPN alternatif robuste et léger.

Reporting
Des rapports détaillés intégrés fournissent des informations précieuses sur les menaces, les utilisateurs, les applications, l'activité Web, et bien plus encore. Notez que certaines fonctionnalités spécifiques de reporting peuvent dépendre d'autres modules de protection pour en tirer tous les avantages (par exemple, Web Protection ou les rapports sur le Web et les applications).

Le module Base Firewall est inclus avec chaque appliance.

Module 'Network Protection'

Toute la protection dont vous avez besoin pour bloquer les attaques sophistiquées et les menaces avancées, tout en offrant un accès sécurisé au réseau aux utilisateurs de confiance.

Système de prévention des intrusions Next-Gen
Fournit une protection avancée contre tous les types d'attaques modernes. Il va au-delà des ressources serveur et réseau traditionnelles pour aussi protéger les utilisateurs et les applications sur le réseau.

Security Heartbeat
Crée un lien entre vos systèmes d'extrémité protégés par Sophos Central et votre pare-feu, afin d'identifier plus rapidement les menaces, de simplifier les analyses et de minimiser l'impact des attaques. Incorporez facilement le statut Heartbeat dans vos politiques de pare-feu afin d'isoler automatiquement les systèmes compromis.

Protection contre les menaces avancées
Identifie instantanément et répond immédiatement à la majorité des attaques sophistiquées d'aujourd'hui. La protection multicouche identifie les menaces instantanément et Security Heartbeat fournit une réponse d'urgence.

Technologies VPN avancées
Vous obtenez des technologies VPN simples et uniques, notamment notre portail libre-service sans client en HTML5 pour un accès distant incroyablement aisé, ainsi que la gestion de notre technologie VPN SD-RED (Remote Ethernet Device) exclusive, légère et sécurisée.

Le module Network Protection est inclus dans les packs Xstream et Standard Protection et peut également être acheté séparément.

Module 'Web Protection'

Obtenez une visibilité et un contrôle inégalés sur l'ensemble des activités Web et applicatives de vos utilisateurs.

Politique Web puissante par utilisateur et par groupe
Fournit des contrôles de politique de pointe de Secure Web Gateway pour gérer facilement des contrôles Web sophistiqués pour les utilisateurs et les groupes. Appliquez les politiques de sécurité en fonction de mots-clés Web signalant un usage ou un comportement inappropriés.

Contrôle et QoS des applications
Permettent la visibilité et le contrôle de milliers d'applications grâce à des politiques de sécurité granulaires et des options de régulation du trafic (QoS) basées sur la catégorie des applications, les risques et d'autres caractéristiques. Le contrôle synchronisé des applications identifie automatiquement toutes les applications inconnues, évasives et personnalisées présentes sur votre réseau.

Protection avancée contre les menaces Web
Notre moteur de pointe s'appuie sur l'intelligence des SophosLabs et offre la protection ultime contre les menaces polymorphes et furtives du Web. Pour garder votre réseau sécurisé, vous disposez de techniques innovantes telles que l'émulation JavaScript, l'analyse comportementale et la réputation de l'origine.

Analyse puissante du trafic
Optimisée pour des performances optimales, notre inspection SSL Xstream permet une inspection à très faible latence et une analyse HTTPS, tout en maintenant les performances.

L'abonnement Web Protection est inclus dans les packs Xstream et Standard Protection et peut également être acheté séparément.

Module 'Zero-Day Protection'

Les techniques d'analyse dynamique et statique des fichiers sont basées sur l'IA et s'associent pour apporter à votre pare-feu une intelligence sur les menaces sans précédent pour ainsi identifier et bloquer efficacement les ransomwares et toute autre menace connue ou inconnue.

Optimisé par les SophosLabs
Alimenté par les SophosLabs, laboratoire de recherche leader du secteur, l'abonnement 'Zero-Day Protection' inclut une plateforme de recherche et d'analyse des menaces entièrement basée dans le Cloud. Elle fournit l'analyse des fichiers par Deep Learning, des rapports d'analyse détaillés et un indicateur du niveau des menaces qui affiche le niveau de risque des fichiers.

Nous utilisons des couches d'analyse pour identifier les menaces connues et potentielles, réduire les inconnues et obtenir des verdicts et des rapports d'intelligence sur les menaces pour les types de fichiers les plus couramment utilisés.

Analyse statique des fichiers
Identifiez rapidement les menaces sans avoir besoin d'exécuter les fichiers en temps réel en tirant profit de la puissance des modèles de Machine Learning, de la réputation mondiale, de l'analyse approfondie des fichiers et de nombreuses autres fonctionnalités.

Analyse dynamique des fichiers
Exécutez un fichier dans une technologie de sandboxing basée dans le Cloud afin d'observer son comportement et son intention. Des captures d'écran permettent de mieux comprendre les événements clés de l'analyse.

Rapports d'analyse de l'intelligence sur les menaces
Des rapports sur les menaces vous fournissent bien plus qu'un simple verdict « bon », « mauvais » ou « inconnu ». L'utilisation de la data science et des données de recherche des SophosLabs permet d'obtenir un aperçu complet de la nature et des capacités d'une menace.

Le module Zero-Day Protection est inclus dans le pack Xstream et peut également être acheté séparément.

Module 'Central Orchestration'

Orchestration VPN gérée dans le Cloud avec Sophos Central, rapports de pare-feu et intégration MDR/XDR.

Orchestration SD-WAN dans Sophos Central
Facilite l'orchestration VPN. La configuration des tunnels à l'aide d'un assistant permet de créer en un simple clic des réseaux maillés complets, des modèles en étoile ou des configurations complexes de tunnels entre plusieurs pare-feux. Intègre de manière transparente plusieurs fonctionnalités de liaison WAN et SD-WAN et des optimisations de routage pour améliorer la résilience et les performances. S'intègre également à l'authentification des utilisateurs et au Synchronized Security Heartbeat pour contrôler l'accès.

Central Firewall Reporting Advanced (30 jours)
Reporting dans le Cloud avec plusieurs rapports communs pré-packagés pour les menaces, la conformité et l'activité des utilisateurs. Comprend des options avancées pour la création de rapports et d'aperçus personnalisés avec la possibilité d'enregistrer, de planifier ou d'exporter vos rapports personnalisés. Inclut la conservation des données des journaux pendant 30 jours avec la possibilité d'ajouter un stockage supplémentaire pour des besoins de rapports historiques supplémentaires.

Compatible MDR/XDR
Sophos MDR (Managed Threat Response) est un service optionnel de Threat Hunting, de détection et de réponse aux menaces, entièrement managé par une équipe d'experts 24 h/24 et 7 j/7. Sophos XDR offre des fonctionnalités étendues de détection et de réponse, qui sont gérées par votre propre équipe. Que Sophos Firewall soit géré par vous ou par nos équipes, il est déjà configuré pour partager toutes les données sur les menaces requises vers le Cloud.

Le module Central Orchestration est inclus dans le pack Xstream et peut également être acheté séparément.

Module 'Email Protection'

Consolidez la protection de votre messagerie avec un antispam, la protection contre la fuite des données (DLP) et le chiffrement. Nous recommandons Sophos Central Email Advanced pour bénéficier de la meilleure solution de protection de la messagerie basée dans le Cloud. Si vous avez besoin d'une protection de la messagerie essentielle et prête à l'emploi, ce module offre un antispam, la DLP et le chiffrement.

MTA (Message Transfer Agent) intégré
Garantit la continuité de la messagerie de votre entreprise, en permettant au pare-feu de mettre automatiquement les emails en attente lorsque vos serveurs rencontrent un problème.

Live Antispam
Protège contre les campagnes de spam, les tentatives de phishing et les pièces jointes malveillantes les plus récentes.

Quarantaine en libre-service
Donnez à vos utilisateurs un contrôle direct sur leur quarantaine de spams, vous faisant gagner du temps et des ressources.

Chiffrement de la messagerie SPX
Exclusivité de Sophos, SPX permet l'envoi d'emails chiffrés vers n'importe quels destinataires, même ceux ne disposant pas d'une infrastructure de confiance, grâce à notre technologie de chiffrement basée sur un mot de passe (brevet déposé).

Protection contre la perte de données (DLP)
La DLP basée sur les politiques peut enclencher automatiquement le chiffrement ou le blocage/la notification en fonction de la présence de données sensibles dans les emails sortant de l'entreprise.

Le module Email Protection doit être acheté individuellement.

Module 'Web Server Protection'

Renforcez vos serveurs Web et vos applications contre les tentatives de piratage, tout en offrant un accès sécurisé.

Modèles de politiques pour les applications professionnelles
Nos modèles de politique de sécurité vous permettent de rapidement et facilement protéger des applications usuelles telles que Microsoft Exchange Outlook Anywhere ou SharePoint.

Protection contre le piratage et les attaques les plus récentes
Inclut toute une gamme de technologies avancées de protection, dont le durcissement des URL et des formulaires, la prévention contre les liens profonds et les traversées de répertoires, la protection contre les injections SQL et le Cross-Site Scripting (XSS), la signature des cookies, et bien plus.

Reverse Proxy
Garantit une protection et des performances maximales pour vos serveurs accessibles depuis Internet à l'aide d'options d'authentification, de déchargement SSL et de répartition de charge vers les serveurs.

Le module Web Server Protection doit être acheté individuellement.

Appliances Sophos XGS

Tous les pare-feux de la série XGS sont conçus sur une architecture à double processeur, combinant un processeur multicœur à haute performance avec un processeur de flux Xstream dédié pour une accélération ciblée au niveau du matériel. Vous bénéficiez ainsi de toute la flexibilité et de l'adaptabilité d'un pare-feu basé sur x86, ainsi que d'une augmentation significative des performances par rapport aux modèles de pare-feux existants.

Matrice produits

Modèle		*Spécifications techniques*			*Débit*			
	Format	Nb de ports (max.)	Modèle W*	Composants permutables	Pare-feu (Mbit/s)	VPN IPsec (Mbit/s)	Protection contre les menaces (Mbit/s)	Xstream SSL/TLS (Mbit/s)
XGS 87(w)	Desktop	5/- (5)	Wi-Fi 5	-	3 850	3 000	280	375
XGS 107(w)	Desktop	9/- (9)	Wi-Fi 5	2e alimentation en option	7 000	4 000	370	420
XGS 116(w)	Desktop	9/1 (9)	Wi-Fi 5	2e alimentation, 3G/4G, Wi-Fi**	7 700	4 800	720	650
XGS 126(w)	Desktop	14/1 (14)	Wi-Fi 5	2e alimentation, 3G/4G, Wi-Fi**	10 500	5 500	900	800
XGS 136(w)	Desktop	14/1 (14)	Wi-Fi 5	2e alimentation, 3G/4G, Wi-Fi**	11 500	6 350	1 000	950
XGS 2100	1U	10/1 (18)	-	Alimentation externe en option	30 000	17 000	1 250	1 100
XGS 2300	1U	10/1 (18)	-	Alimentation externe en option	39 000	20 500	1 500	1 450
XGS 3100	1U	12/1 (20)	-	Alimentation externe en option	47 000	25 000	2 000	2 470
XGS 3300	1U	12/1 (20)	-	Alimentation externe en option	58 000	31 100	3 000	3 130
XGS 4300	1U	12/2 (28)	-	Alimentation externe en option	75 000	62 500	6 500	8 000
XGS 4500	1U	12/2 (28)	-	Alimentation interne en option	80 000	75 550	8 650	10 600
XGS 5500	2U	16/3 (48)	-	Alim., SSD, Ventilateur	100 000	92 500	14 000	13 500
XGS 6500	2U	20/4 (68)	-	Alim., SSD, Ventilateur	120 000	109 800	17 850	16 000

* 802.11ac

** Second module Wi-Fi en option pour XGS 116w, 126w et 136w uniquement

Méthodologie des tests de performance

Général : Débit maximal mesuré en conditions de test idéales, utilisant l'aide des outils de test standard Keysight-Ixia Breakingpoint. Les performances réelles peuvent varier en fonction des conditions du réseau et des services activés.

- **Pare-feu :** Mesuré en utilisant le trafic HTTP et une taille de réponse de 512 Ko.
- **IMIX du pare-feu :** Débit UDP basé sur un ensemble de tailles de paquets de 66 octets, 570 octets et 1518 octets.
- **IPS :** Mesuré avec IPS avec le trafic HTTP en utilisant des règles IPS par défaut et une taille d'objet de 512 Ko.
- **VPN IPsec :** Débit HTTP en utilisant plusieurs tunnels et une taille de la réponse HTTP de 512 Ko.
- **Inspection TLS :** Les performances sont mesurées avec l'IPS avec des sessions HTTPS et différentes suites de chiffrement.
- **Protection contre les menaces :** Mesurée avec le pare-feu, l'IPS, le contrôle des applications et la prévention des malwares activés en utilisant la taille de réponse HTTP 200 Ko
- **NGFW :** Mesuré avec l'IPS et le Contrôle des applications activés avec le trafic HTTP en utilisant des règles IPS par défaut et une taille d'objet de 512 Ko.

Besoin d'aide pour choisir la bonne solution ?

Pour vous aider à trouver la licence ou l'appliance adaptée à vos besoins, nous vous invitons à contacter votre équipe commerciale ou votre partenaire Sophos local. Sophos offre une assistance gratuite pour le dimensionnement et un outil de dimensionnement des pare-feux pour les partenaires sur le Portail Partenaires Sophos.

Sophos Série XGS - Desktop : PME et succursales

Les clients qui recherchent une solution de sécurité réseau tout-en-un apprécieront les options de connectivité transparentes disponibles pour nos appliances Desktop. Elles offrent le parfait équilibre entre prix et performances, avec la modularité dont les petites entreprises, les points de vente au détail et les succursales ont besoin pour se développer et s'adapter à l'évolution des activités. Tous les modèles Desktop sont disponibles en option avec Wi-Fi intégré.

Tous les modèles sont équipés d'un processeur haut débit et d'un processeur de flux Xstream dédié pour l'accélération matérielle.

Caractéristiques du produit

- Architecture à double processeur pour un excellent rapport prix/performances.
- Chaque modèle est disponible avec le Wi-Fi intégré en option pour une connectivité tout-en-un.
- Une baie d'extension sur tous les modèles XGS 116/126/136 améliore la compatibilité pour la 3G/4G lorsqu'elle est utilisée avec notre module optionnel.
- Un deuxième module radio Wi-Fi en option peut être ajouté aux modèles w dotés d'une baie d'extension.
- Des ports PoE (Power-over-Ethernet) intégrés dans tous les modèles XGS 116, 126 et 136 (2,5 GE sur 136).
- Une deuxième alimentation en option pour tous les modèles XGS 1xx offre une option de redondance rarement disponible dans ce format.
- Le port SFP de tous les modèles peut être utilisé pour le FTTH/FTTP ou avec le modem VDSL en option.

Remarque : Toutes les fonctionnalités de protection sont prises en charge par tous les modèles XGS 1xx et la plupart des modèles XGS 87 et 87w.

Caractéristiques du produit

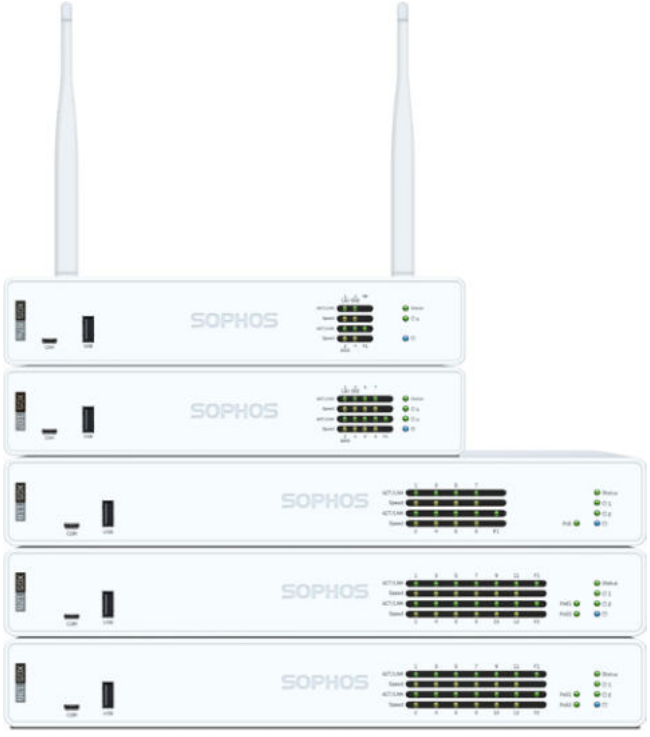
XGS 87 et XGS 87w
Référez-vous aux spécifications techniques.

XGS 107, XGS 107w
Référez-vous aux spécifications techniques.

XGS 116, XGS 116w
Référez-vous aux spécifications techniques.

XGS 126, XGS 126w
Référez-vous aux spécifications techniques.

XGS 136, XGS 136w
Référez-vous aux spécifications techniques.



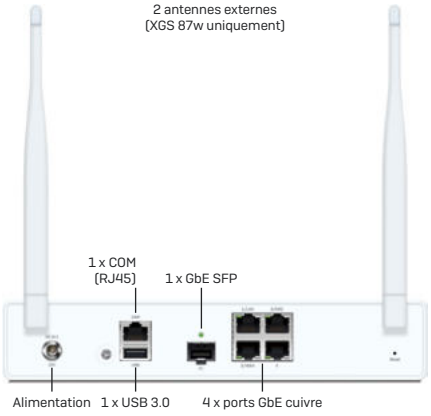
Sophos Série XGS - Desktop : PME et succursales
XGS 87 et XGS 87w

Spécifications techniques

Remarque : Les appliances XGS 87 et 87w ne prennent pas en charge certaines fonctionnalités avancées comme les rapports détaillés intégrés, les doubles moteurs d'analyse antivirus, l'analyse antivirus WAF et l'agent de transfert de messages (MTA). Si vous avez besoin de ces capacités, nous vous recommandons XGS 107(w).

Vue avant

Vue arrière



Spécifications physiques	
Montage	Kit de montage en rack disponible (commander séparément)
Dimensions **Largeur x hauteur x profondeur**	230 x 44 x 205,5 mm
Poids	1,36 kg/3 lbs (sans emballage) 2,75 kg/6,06 lbs (avec emballage) (légèrement plus pour le modèle W)

Environnement	
Alimentation	AC-DC automatique externe : 100-240VAC, 1,7A@50-60 Hz 12VDC, 5A, 60W
Consommation électrique	23,2W, 79,16 BTU/h (87) (au repos) 27,1W, 92,13 BTU/h (87w) (au repos) 43,4W, 148,09 BTU/h (87) (max.) 46,8W, 159,69 BTU/h (87w) (max.)
Température de fonctionnement	De 0°C à 40°C (fonctionnement) De -20°C à +70°C (à l'arrêt)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, NOM, Anatel (87 uniquement)

Performances	*XGS 87(w)*
Débit du pare-feu	3 850 Mbit/s
IMIX du pare-feu	3 000 Mbit/s
Latence du pare-feu (64 octets, UDP)	6 µs
Débit IPS	1 200 Mbit/s
Débit Protection contre les menaces	280 Mbit/s
NGFW	700 Mbit/s
Connexions simultanées	1 600 000
Nouvelles connexions/sec	35 700
Débit VPN IPsec	3 000 Mbit/s
Tunnel VPN IPSec simultanés	500
Tunnel SSL VPN simultanés	500
Inspection SSL/TLS Xstream	375 Mbit/s
Connexions simultanées SSL/TLS Xstream	8 192

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

Spécification sans fil (XGS 87w uniquement)	
Nb d'antennes	2 externes
Fonctions MIMO	2x2:2
Interface sans fil	802.11a/b/g/n/ac (2,4 GHz/5 GHz)

Interfaces physiques	
Stockage	16 Go eMMC
Interfaces Ethernet (fixes)	4 x GbE cuivre 1 x SFP fibre*
Port de gestion	1 x COM RJ45 1 x Micro-USB (câble incl.)
Autres ports E/S	1 x USB 2.0 (avant) 1 x USB 3.0 (arrière)
Nombre de slots d'extension	0
Connectivité complémentaire en option	Module SFP DSL (VDSK2) Émetteurs-récepteurs SFP

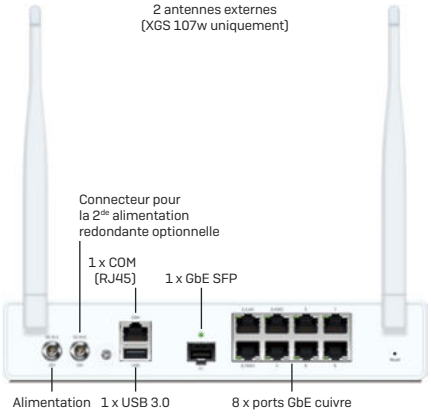
* Émetteurs-récepteurs SFP vendus séparément

Sophos Série XGS - Desktop : PME et succursales
XGS 107, XGS 107w

Spécifications techniques

Vue avant

Vue arrière



Spécifications physiques	
Montage	Kit de montage en rack disponible (commander séparément)
Dimensions **Largeur x hauteur x profondeur**	230 x 44 x 205,5 mm
Poids	1,4 kg/3,09 lbs (sans emballage) 2,8 kg/6,17 lbs (avec emballage) (légèrement plus pour le modèle W)

Environnement	
Alimentation	AC-DC automatique externe : 100-240VAC, 1,7A@50-60 Hz 12VDC, 5A, 60W Seconde alimentation redondante en option
Consommation électrique	107 : 26,1W/89,06 BTU/h (au repos) 107w : 29,8W/101,68 BTU/h (au repos) 107 : 53,9W/183,91 BTU/h (max.) 107w : 57,3W/195,52 BTU/h (max.)
Température de fonctionnement	De 0°C à 40°C (fonctionnement) De -20°C à +70°C (à l'arrêt)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, NOM, Anatel (107 uniquement)

Performances	*XGS 107(w)*
Débit du pare-feu	7 000 Mbit/s
IMIX du pare-feu	3 750 Mbit/s
Latence du pare-feu (64 octets, UDP)	6 µs
Débit IPS	1 500 Mbit/s
Débit Protection contre les menaces	370 Mbit/s
NGFW	1 050 Mbit/s
Connexions simultanées	1 600 000
Nouvelles connexions/sec	44 400
Débit VPN IPsec	4 000 Mbit/s
Tunnel VPN IPSec simultanés	1 000
Tunnel SSL VPN simultanés	1 000
Inspection SSL/TLS Xstream	420 Mbit/s
Connexions simultanées SSL/TLS Xstream	8 192

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

Spécification sans fil (XGS 107w uniquement)	
Nb d'antennes	2 externes
Fonctions MIMO	2x2:2
Interface sans fil	802.11a/b/g/n/ac (2,4 GHz/5 GHz)

Interfaces physiques	
Stockage (quarantaine locale/journaux)	SSD 64 Go intégré
Interfaces Ethernet (fixes)	8 x GbE cuivre 1 x SFP fibre*
Port de gestion	1 x COM RJ45 1 x Micro-USB (câble incl.)
Autres ports E/S	1 x USB 2.0 (avant) 1 x USB 3.0 (arrière)
Nombre de slots d'extension	0
Connectivité complémentaire en option	Module SFP DSL (VDSK2) Émetteurs-récepteurs SFP

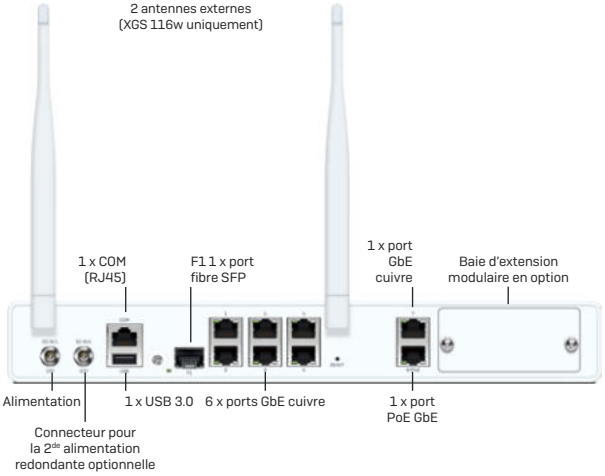
* Émetteurs-récepteurs SFP vendus séparément

Sophos Série XGS - Desktop : PME et succursales
XGS 116, XGS 116w

Spécifications techniques

Vue avant

Vue arrière



Spécifications physiques	
Montage	Kit de montage en rack disponible (commander séparément)
Dimensions **Largeur x hauteur x profondeur**	320 x 44 x 213 mm
Poids	2,2 kg/4,85 lbs (sans emballage) 4,2 kg/9,26 lbs (avec emballage) (légèrement plus pour le modèle W)

Environnement	
Alimentation	AC-DC automatique externe : 100-240VAC, 2,5A@50-60 Hz 12VDC, 12,5A, 150W Seconde alimentation redondante en option
Consommation électrique	116 : 28W/96 BTU/h (au repos) 116w : 30W/102 BTU/h (au repos) 116 : 57W/195 BTU/h (max.) 116w : 60W/205 BTU/h (max.)
Possibilité d'ajouter un PoE	38W/130 BTU/h (max.)
Température de fonctionnement	De 0°C à +40°C (fonctionnement) De -20°C à +70°C (à l'arrêt)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, NOM, Anatel

Performances	*XGS 116(w)*
Débit du pare-feu	7 700 Mbit/s
IMIX du pare-feu	4 500 Mbit/s
Latence du pare-feu (64 octets, UDP)	8 µs
Débit IPS	2 500 Mbit/s
Débit Protection contre les menaces	720 Mbit/s
NGFW	2 000 Mbit/s
Connexions simultanées	1 600 000
Nouvelles connexions/sec	61 500
Débit VPN IPsec	4 800 Mbit/s
Tunnel VPN IPSec simultanés	1 500
Tunnel SSL VPN simultanés	1 250
Inspection SSL/TLS Xstream	650 Mbit/s
Connexions simultanées SSL/TLS Xstream	8 192

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

Spécification sans fil (XGS 116w uniquement)	
Nb d'antennes	2 externes
Fonctions MIMO	2x2:2
Interface sans fil	Wi-Fi 5/802.11a/b/g/n/ac (2,4 GHz/5 GHz)
Second module Wi-Fi en option	Wi-Fi 5/802.11a/b/g/n/ac

Interfaces physiques	
Stockage (quarantaine locale/journaux)	SSD 64 Go intégré
Interfaces Ethernet (fixes)	8 GbE cuivre 1 GbE SFP*
Alimentation par Ethernet - PoE (fixe)	1 x GbE 803.2at (30 W max.)
Ports de gestion	1 x COM RJ45 1 x Micro-USB (câble incl.)
Autres ports E/S	1 x USB 2.0 (avant) 1 x USB 3.0 (arrière)
Nombre de slots d'extension	1
Connectivité complémentaire en option	Module SFP DSL (VDSL2) Module 3G/4G Seconde radio Wi-Fi (XGS 116w uniquement) Émetteurs-récepteurs SFP

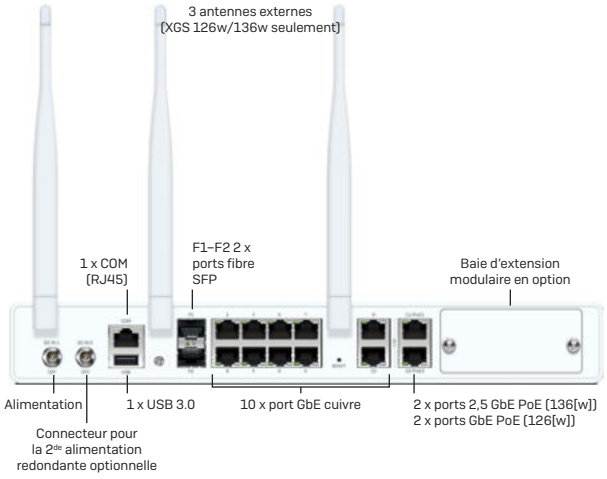
* Émetteurs-récepteurs SFP vendus séparément

Sophos Série XGS - Desktop : PME et succursales
XGS 126, XGS 126w, XGS 136 et XGS 136w

Spécifications techniques

Vue avant

Vue arrière



Spécifications physiques	
Montage	Kit de montage en rack disponible (commander séparément)
Dimensions **Largeur x hauteur x profondeur**	320 x 44 x 213 mm
Poids	2,4 kg/5,29 lbs (sans emballage) 4,4 kg/9,70 lbs (avec emballage) (légèrement plus pour le modèle W)

Environnement	
Alimentation	AC-DC automatique externe : 100-240VAC, 2,5A@50-60 Hz 12VDC, 12,5A, 150W Seconde alimentation redondante en option
Consommation électrique	126/136 : 30 W/102 BTU/h (au repos) 126w/136w : 32W/109 BTU/h (au repos) 126 : 59 W/202 BTU/h (max.) 126w/136 : 62 W/212 BTU/hr (max.) 136w : 65W/222 BTU/h (max.)
Possibilité d'ajouter un PoE	76W/260 BTU/h (max.)
Température de fonctionnement	De 0°C à 40°C (fonctionnement) De -20°C à +70°C (à l'arrêt)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, NOM, Anatel

Performances	*XGS 126(w)*	*XGS 136(w)*
Débit du pare-feu	10 500 Mbit/s	11 500 Mbit/s
IMIX du pare-feu	5 250 Mbit/s	6 500 Mbit/s
Latence du pare-feu (64 octets, UDP)	8 µs	8 µs
Débit IPS	3 250 Mbit/s	4 000 Mbit/s
Débit Protection contre les menaces	900 Mbit/s	1 000 Mbit/s
NGFW	2 500 Mbit/s	3 000 Mbit/s
Connexions simultanées	5 000 000	6 400 000
Nouvelles connexions/sec	69 900	74 500
Débit VPN IPsec	5 500 Mbit/s	6 350 Mbit/s
Tunnel VPN IPSec simultanés	2500	2500
Tunnel SSL VPN simultanés	1 500	1 500
Inspection SSL/TLS Xstream	800 Mbit/s	950 Mbit/s
Connexions simultanées SSL/TLS Xstream	12 288	18 432

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

Spécification sans fil (XGS 126w et XGS 136w uniquement)	
Nb d'antennes	3 externes
Fonctions MIMO	3x3:3
Interface sans fil	Wi-Fi 5/802.11a/b/g/n/ac (2,4 GHz/5 GHz)
Second module Wi-Fi en option	Wi-Fi 5/802.11a/b/g/n/ac

Interfaces physiques		
Stockage (quarantaine locale/journaux)	SSD 64 Go intégré	
Interfaces Ethernet (fixes)	12 x GbE cuivre 2 x SFP fibre*	10 x GbE cuivre 2 x 2,5 GbE cuivre 2 x SFP fibre*
Alimentation par Ethernet - PoE (fixe)	2 x GbE (30W max. par port)	2 x 2,5 GbE (30W max. par port)
Ports de gestion	1 x COM RJ45 1 x Micro-USB (câble incl.)	
Autres ports E/S	1 x USB 2.0 (avant) 1 x USB 3.0 (arrière)	
Nombre de slots d'extension	1	
Connectivité complémentaire en option	Module SFP DSL (VDSL2) Module 3G/4G Seconde radio Wi-Fi (XGS 126w/136w uniquement) Émetteurs-récepteurs SFP	

* Émetteurs-récepteurs SFP vendus séparément

Sophos série XGS - 1U : Périphérie distribuée

Les entreprises de taille moyenne et distribuées qui ont besoin d'une solution polyvalente pour alimenter et protéger leur réseau trouveront leur bonheur avec nos modèles 1U. Ces pare-feux à montage en rack offrent d'excellentes performances, une gamme diversifiée d'interfaces haut débit intégrées et un choix de modules de connectivité supplémentaires. Que votre priorité soit d'assurer une disponibilité maximale de vos liens SD-WAN, de connecter en toute sécurité vos utilisateurs distants ou de protéger le réseau de votre organisation en pleine croissance, vous pouvez les adapter à votre environnement dynamique.

Tous les modèles sont équipés d'un processeur haut débit et d'un processeur de flux Xstream dédié pour l'accélération matérielle.

Caractéristiques du produit

- L'architecture à double processeur prend en charge toutes les fonctions de protection clés sans compromettre les performances.
- Ports cuivre et fibre embarqués.
- Ports bypass LAN sur tous les modèles.
- Baie(s) d'extension avec module Flexi Port sur tous les modèles afin d'adapter la connectivité.
- Seconde alimentation en option pour tous les modèles.
- Module PoE Flexi Port à alimentation centrale en option pour fournir une alimentation redondante aux dispositifs PoE.
- Kit de montage en rack inclus.

Caractéristiques du produit

XGS 2100
Référez-vous aux spécifications techniques.

XGS 2300
Référez-vous aux spécifications techniques.

XGS 3100
Référez-vous aux spécifications techniques.

XGS 3300
Référez-vous aux spécifications techniques.

XGS 4300
Référez-vous aux spécifications techniques.

XGS 4300
Référez-vous aux spécifications techniques.

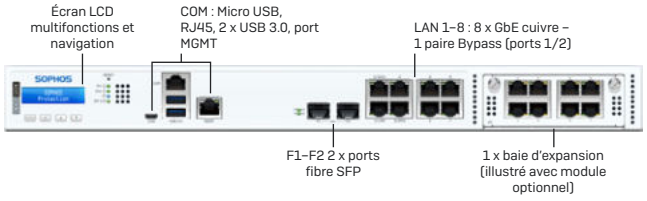
Connectivité de périmètre LAN et WAN

Connectez en toute sécurité vos succursales ou vos sites distants à votre bureau principal avec Sophos SD-RED, des appareils RED (Remote Ethernet Devices), et ajoutez la connectivité au périmètre du LAN avec nos switchs de couche d'accès et nos points d'accès. Vous trouverez plus d'informations à la fin de cette brochure et à la page sophos.fr/switch.

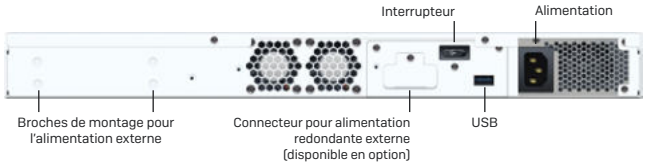
Sophos série XGS - 1U : Périphérie distribuée XGS 2100, XGS 2300

Spécifications techniques

Vue avant



Vue arrière



Spécifications physiques	
Montage	Montage en rack de 1U (2 équerres de montage incluses)
Dimensions **Largeur x hauteur x profondeur**	438 x 44 x 405 mm
Poids	4,7 kg/10,36 lbs (sans emballage) 7 kg/15,43 lbs (avec emballage)

Environnement	
Alimentation	AC-DC automatique interne 100-240VAC, 3-6A@50-60 Hz Option de bloc d'alimentation externe redondant
Consommation électrique	2100 : 43W/146,86 BTU/h (au repos) 2300 : 45W/153,7 BTU/h (au repos) 2100 : 162W/533,5 BTU/h (max.) 2300 : 167W/570,74 BTU/h (max.)
Possibilité d'ajouter un PoE	76W/260 BTU/h (max.)
Température de fonctionnement	De 0°C à 40 °C (fonctionnement) De -20°C à +70 °C (stockage)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, RCM, NOM, Anatel

Performances	*XGS 2100*	*XGS 2300*
Débit du pare-feu	30 000 Mbit/s	39 000 Mbit/s
IMIX du pare-feu	16 500 Mbit/s	20 000 Mbit/s
Latence du pare-feu (64 octets, UDP)	6 µs	4 µs
Débit IPS	6 000 Mbit/s	7 000 Mbit/s
Débit Protection contre les menaces	1 250 Mbit/s	1 500 Mbit/s
NGFW	5 200 Mbit/s	6 300 Mbit/s
Connexions simultanées	6500000	6500000
Nouvelles connexions/sec	134700	148000
Débit VPN IPsec	17 000 Mbit/s	20 500 Mbit/s
Tunnel VPN IPSec simultanés	5000	5 000
Tunnel SSL VPN simultanés	2500	2500
Inspection SSL/TLS Xstream	1 100 Mbit/s	1 450 Mbit/s
Connexions simultanées SSL/TLS Xstream	18432	18432

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

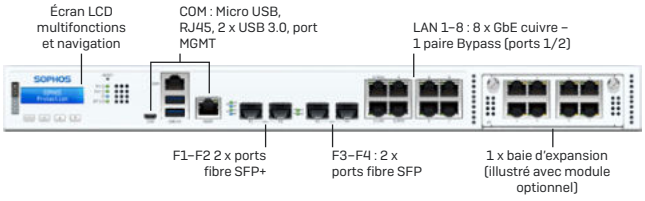
Interfaces physiques	
Stockage (quarantaine locale/journaux)	SSD SATA-III intégré de 120 Go min.
Interfaces Ethernet (fixes)	8 x GbE cuivre 2 x SFP fibre*
Paires de ports de contournement	1
Ports de gestion	1 x RJ45 MGMT 1 x COM RJ45 1 x Micro-USB (câble incl.)
Autres ports E/S	2 x USB 3.0 (avant) 1 x USB 2.0 (arrière)
Nombre de slots Flexi Port	1
Modules Flexi Port (optionnels)	8 ports GbE Cuivre 8 ports GbE fibre SFP 4 ports 10 GE fibre SPF+ 4 ports GbE cuivre bypass (2 paires) 4 ports GbE cuivre PoE + 4 ports GbE cuivre 4 ports 2,5 GbE cuivre PoE 2 ports GbE fibre (LC) Bypass + 4 ports GbE SFP fibre
Densité max. totale de ports (dont l'utilisation de modules)	18
Alimentation par Ethernet (PoE) max. (en utilisant le module Flexi Port)	1 module : 4 ports, 60W max.
Connectivité complémentaire en option	Module SFP DSL (VDSL2) Émetteurs-récepteurs SFP/SFP+
Affichage	Module LCD multifonction

* Émetteurs-receveurs (mini GBIC) vendus séparément

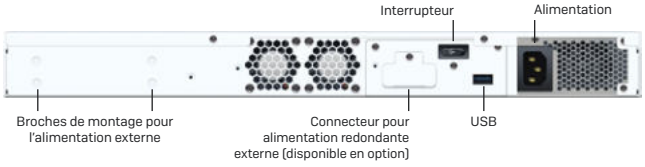
Sophos série XGS - 1U : Périphérie distribuée XGS 3100, XGS 3300

Spécifications techniques

Vue avant



Vue arrière



Spécifications physiques	
Montage	Montage en rack de 1U (2 équerres de montage incluses)
Dimensions **Largeur x hauteur x profondeur**	438 x 44 x 405 mm
Poids	4,7 kg/10,36 lbs (sans emballage) 7 kg/15,43 lbs (avec emballage)

Environnement	
Alimentation	AC-DC automatique interne 100-240VAC, 3-6A@50-60 Hz Option de bloc d'alimentation externe redondant
Consommation électrique	3100 : 50W/170,77 BTU/h (au repos) 3300 : 50W/170,77 BTU/h (au repos) SG 3100 : 182W/621,97 BTU/h (max.) 3300 : 201W/686,68 BTU/h (max.)
Possibilité d'ajouter un PoE	76W/260 BTU/h (max.)
Température de fonctionnement	De 0 à 40°C (fonctionnement) De -20 à +70°C (stockage)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, RCM, NOM, Anatel

Performances	XGS 3100	XGS 3300
Débit du pare-feu	47 000 Mbit/s	58 000 Mbit/s
IMIX du pare-feu	23 500 Mbit/s	27 000 Mbit/s
Latence du pare-feu (64 octets, UDP)	4 µs	4 µs
Débit IPS	10 500 Mbit/s	14 000 Mbit/s
Débit Protection contre les menaces	2 000 Mbit/s	3 000 Mbit/s
NGFW	9 000 Mbit/s	12 500 Mbit/s
Connexions simultanées	12 260 000	13 700 000
Nouvelles connexions/sec	186 500	257 800
Débit VPN IPsec	25 000 Mbit/s	31 100 Mbit/s
Tunnel VPN IPSec simultanés	6500	6500
Tunnel SSL VPN simultanés	5 000	5 000
Inspection SSL/TLS Xstream	2 470 Mbit/s	3 130 Mbit/s
Connexions simultanées SSL/TLS Xstream	55 296	102 400

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

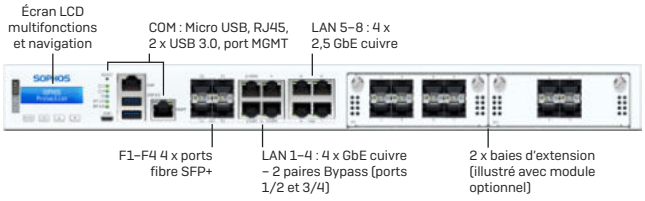
Interfaces physiques	
Stockage (quarantaine locale/journaux)	SSD SATA-III intégré de 240 Go min.
Interfaces Ethernet (fixes)	8 x GE cuivre 2 x SFP fibre* 2 x SFP+ 10 GbE fibre*
Paires de ports de contournement	1
Ports de gestion	1 x RJ45 MGMT 1 x COM RJ45 1 x Micro-USB (câble incl.)
Autres ports E/S	2 x USB 3.0 (avant) 1 x USB 2.0 (arrière)
Nombre de slots Flexi Port	1
Modules Flexi Port (optionnels)	8 ports GbE Cuivre 8 ports GbE fibre SFP 4 ports 10 GbE fibre SFP+ 4 ports GbE cuivre bypass (2 paires) 4 ports GbE cuivre PoE + 4 ports GbE cuivre 4 ports 2,5 GbE cuivre PoE 2 ports GbE fibre (LC) Bypass + 4 ports GbE SFP fibre
Densité max. totale de ports (dont l'utilisation de modules)	20
Alimentation par Ethernet (PoE) max. (en utilisant le module Flexi Port)	1 module : 4 ports, 60W max.
Connectivité complémentaire en option	Module SFP DSL (VDSL2) Émetteurs-récepteurs SFP/SFP+
Affichage	Module LCD multifonction

* Émetteurs-receveurs (mini GBIC) vendus séparément

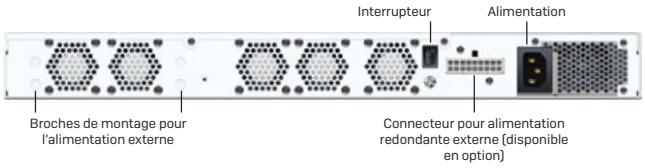
Sophos série XGS - 1U : Périphérie distribuée XGS 4300, XGS 4500

Spécifications techniques

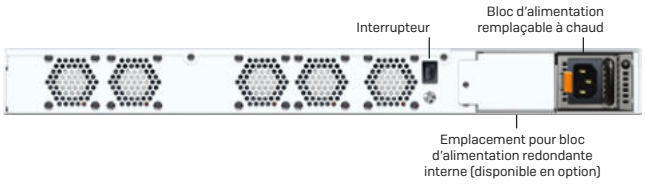
Vue avant



Vue arrière XGS 4300



Vue arrière XGS 4500



Spécifications physiques	
Montage	Montage en rack de 1U (avec les glissières)
Dimensions Largeur x hauteur x profondeur	438 x 44 x 510 mm
Poids	XGS 4300 : 8,7 kg/19,18 lbs (sans emballage) XGS 4500 : 9,7 kg/21,38 lbs (sans emballage) XGS 4300 : 14,9 kg/32,85 lbs (avec emballage) XGS 4500 : 15,9 kg/35,05 lbs (avec emballage)

Environnement	
Alimentation	XGS 4300 : AC-DC automatique interne 100-240VAC, 3,7-7,4A@50-60 Hz Option de bloc d'alimentation externe redondant XGS 4500 : AC-DC automatique interne remplaçable à chaud 100-240VAC, 3,7-7,4A@50-60 Hz Option de bloc d'alimentation interne redondant
Consommation électrique	4300 : 131W/447,43 BTU/h (au repos) 4500 : 151W/515,74 BTU/h (au repos) 4300 : 268,35W/916,56 BTU/h (max.) 4500 : 268,35W/916,56 BTU/h (max.)
Possibilité d'ajouter un PoE	152W/519 BTU/h
Température de fonctionnement	De 0 à 40°C (fonctionnement) De -20 à +70°C (stockage)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, RCM, NOM, Anatel

Performances	*XGS 4300*	*XGS 4500*
Débit du pare-feu	75 000 Mbit/s	80 000 Mbit/s
IMIX du pare-feu	33 000 Mbit/s	37 000 Mbit/s
Latence du pare-feu (64 octets, UDP)	3 µs	4 µs
Débit IPS	29 500 Mbit/s	36 500 Mbit/s
Débit Protection contre les menaces	6 500 Mbit/s	8 650 Mbit/s
NGFW	23 000 Mbit/s	30 000 Mbit/s
Connexions simultanées	16 600 000	17 200 000
Nouvelles connexions/sec	368 000	450 000
Débit VPN IPsec	62 500 Mbit/s	75 550 Mbit/s
Tunnel VPN IPSec simultanés	8500	8500
Tunnel SSL VPN simultanés	7 500	10 000
Inspection SSL/TLS Xstream	8 000 Mbit/s	10 600 Mbit/s
Connexions simultanées SSL/TLS Xstream	276 480	276 480

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

Interfaces physiques	
Stockage (quarantaine locale/journaux)	XGS 4300 : 1 x SSD SATA-III 240 Go min. XGS 4500 : 2 x SSD SATA-III 240 Go min. (SW RAID-1)
Interfaces Ethernet (fixes)	4 x GbE cuivre 4 x 2,5 GbE cuivre 4 x SFP+ 10 GbE fibre*
Paires de ports de contournement	2
Ports de gestion	1 x RJ45 MGMT 1 x COM RJ45 1 x Micro-USB (câble incl.)
Autres ports E/S	2 x USB 3.0 (avant)
Nombre de slots Flexi Port	2
Modules Flexi Port (optionnels)	8 ports GbE Cuivre 8 ports GbE fibre SFP 4 ports 10 GbE fibre SFP+ 4 ports GbE cuivre bypass (2 paires) 4 ports GbE cuivre PoE + 4 ports GbE cuivre 4 ports 2,5 GbE cuivre PoE 2 ports GbE fibre (LC) Bypass + 4 ports GbE SFP fibre
Densité max. totale de ports (dont l'utilisation de modules)	28
Alimentation par Ethernet (PoE) max. (en utilisant le module Flexi Port)	2 modules : 4 ports, 60W max. chacun
Connectivité complémentaire en option	Module SFP DSL (VDSL2) Émetteurs-récepteurs SFP/SFP+
Affichage	Module LCD multifonction

* Émetteurs-receveurs (mini GBIC) vendus séparément

Sophos série XGS - 2U : Périmètre grande entreprise

Les entreprises distribuées et en pleine croissance qui ont besoin d'un débit maximal, même pour les réseaux les plus complexes, bénéficient d'une protection, de performances et d'une continuité des activités sans compromis grâce à ces pare-feux Next-Gen. Les nouveaux processeurs de flux Xstream fournissent une accélération matérielle dédiée qui permet de gérer facilement la protection complète des applications et du trafic chiffrés et hébergés dans le Cloud. Ces modèles offrent un équilibre parfait entre densité de port et modularité, avec une gamme de ports intégrés à haut débit, ainsi que des modules Flexi Port haute densité supplémentaires disponibles pour étendre davantage la connectivité.

Tous les modèles sont équipés d'un processeur haut débit et d'un processeur de flux Xstream dédié pour l'accélération matérielle.

Caractéristiques du produit

- Architecture à double processeur avec coprocesseur dédié pour l'accélération matérielle.
- Conçu pour exploiter toutes les fonctions clés de protection contre les menaces, telles que l'inspection TLS, le sandboxing et l'analyse des menaces pilotée par l'IA.
- Excellent rapport prix/performances
- Une gamme d'interfaces cuivre standard 1 GE et 8 à 12 interfaces fibre SFP+ 10 GE intégrées.
- Modules Flexi Port standard et haute densité disponibles en option pour étendre et adapter la connectivité.
- Densité maximale de 48 ports (XGS 5500) ou 68 (XGS 6500) avec les modules optionnels.
- Des fonctions de redondance sur tous les modèles pour assurer la continuité des activités.

Caractéristiques du produit

XGS 5500

Référez-vous aux spécifications techniques.

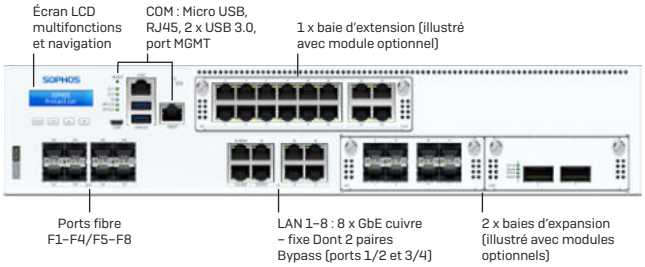
XGS 6500

Référez-vous aux spécifications techniques.

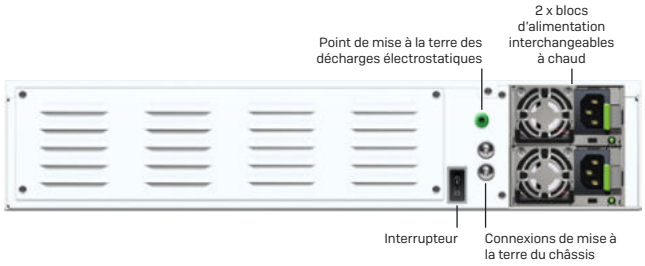
Sophos série XGS - 2U : Périphérie de grande entreprise XGS 5500

Spécifications techniques

Vue avant



Vue arrière



Spécifications physiques	
Montage	Glissières de 2 U (incluses)
Dimensions Largeur x hauteur x profondeur	438 x 88 x 645 mm
Poids	17,8 kg/39,24 lbs (sans emballage) 27 kg/59,53 lbs (avec emballage)

Environnement	
Alimentation	2 x blocs d'alimentation automatique interne 100-240 VAC, PSU 50-60 Hz
Consommation électrique	168,0W/573,81 BTU/h (au repos) 478,01W/1117,43 BTU/h (max.)
Température de fonctionnement	De 0 à 40°C (fonctionnement) De -20 à +70°C (stockage)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, RCM, NOM, Anatel

Performances	XGS 5500
Débit du pare-feu	100 000 Mbit/s
IMIX du pare-feu	52 000 Mbit/s
Latence du pare-feu (64 octets, UDP)	5 µs
Débit IPS	40 000 Mbit/s
Débit Protection contre les menaces	14 000 Mbit/s
NGFW	38 000 Mbit/s
Connexions simultanées	32 400 000
Nouvelles connexions/sec	468 000
Débit VPN IPsec	92 500 Mbit/s
Tunnel VPN IPSec simultanés	10000
Tunnel SSL VPN simultanés	15 000
Inspection SSL/TLS Xstream	13 500 Mbit/s
Connexions simultanées SSL/TLS Xstream	512 000

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

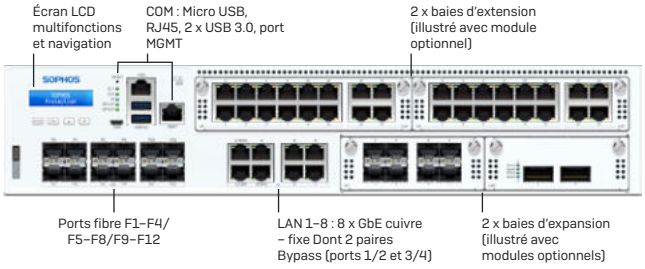
Interfaces physiques	
Stockage (quarantaine locale/journaux)	2 x SSD SATA-III 480 Go min. HW RAID intégré dans le CPU
Interfaces Ethernet (fixes)	8 x GbE cuivre 8 x SFP+ 10 GbE fibre*
Paires de ports de contournement	2
Ports de gestion	1 x RJ45 MGMT 1 x COM RJ45 1 x Micro-USB (câble incl.)
Autres ports E/S	2 x USB 3.0 (avant)
Nombre de slots Flexi Port	2 + 1 pour module haute densité
Modules Flexi Port (optionnels)	8 ports GbE Cuivre 8 ports GbE fibre SFP 4 ports 10 GbE fibre SFP+ 4 ports GbE cuivre bypass (2 paires) 2 ports 40 GbE fibre QSFP+ 8 ports 10 GbE fibre SFP+ 2 ports GbE fibre (LC) Bypass + 4 ports GbE SFP fibre 2 ports 10 GbE fibre (LC) Bypass + 4 ports 10 GbE SFP+ fibre Module haute densité (NIC) : 12 ports GE cuivres + 4 ports 2,5 GE cuivre
Densité max. totale de ports (dont l'utilisation de modules)	48
Connectivité complémentaire en option	Module SFP DSL (VDSL2) Émetteurs-récepteurs SFP/SFP+
Affichage	Module LCD multifonction

* Émetteurs-receveurs (mini GBIC) vendus séparément

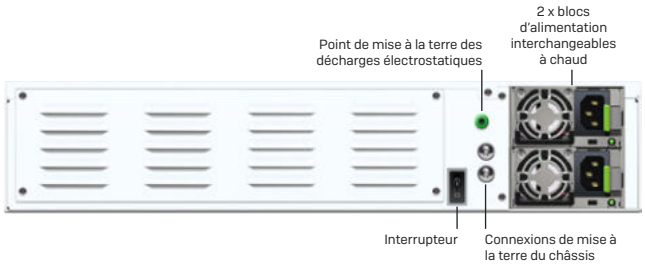
Sophos série XGS - 2U : Périmètre grande entreprise XGS 6500

Spécifications techniques

Vue avant



Vue arrière



Spécifications physiques	
Montage	Glissières de 2 U (incluses)
Dimensions Largeur x hauteur x profondeur	438 x 88 x 645 mm
Poids	17,8 kg/39,24 lbs (sans emballage) 27 kg/59,53 lbs (avec emballage)

Environnement	
Alimentation	2 x blocs d'alimentation automatique interne 100-240 VAC, PSU 50-60 Hz
Consommation électrique	188,00W/642,13 BTU/h (au repos) 497,09W/1697,8 BTU/h (max.)
Température de fonctionnement	De 0°C à 40 °C (fonctionnement) De -20°C à +70 °C (stockage)
Humidité	10 % à 90 %, sans condensation

Certifications produit	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, RCM, NOM, Anatel

Performances	XGS 6500
Débit du pare-feu	120 000 Mbit/s
IMIX du pare-feu	60 000 Mbit/s
Latence du pare-feu (64 octets, UDP)	5 µs
Débit IPS	50 750 Mbit/s
Débit Protection contre les menaces	17 850 Mbit/s
NGFW	46 500 Mbit/s
Connexions simultanées	39 900 000
Nouvelles connexions/sec	496 000
Débit VPN IPsec	109 800 Mbit/s
Tunnel VPN IPSec simultanés	10000
Tunnel SSL VPN simultanés	15 000
Inspection SSL/TLS Xstream	16 000 Mbit/s
Connexions simultanées SSL/TLS Xstream	768 000

Remarque : Pour la méthodologie des tests de performance, veuillez consulter la page 11

Interfaces physiques	
Stockage (quarantaine locale/journaux)	2 x SSD SATA-III 480 Go min. HW RAID intégré dans le CPU
Interfaces Ethernet (fixes)	8 x GbE cuivre 12 x SFP+ 10 GbE fibre*
Paires de ports de contournement	2
Ports de gestion	1 x RJ45 MGMT 1 x COM RJ45 1 x Micro-USB (câble incl.)
Autres ports E/S	2 x USB 3.0 (avant)
Nombre de slots Flexi Port	2 + 2 pour module haute densité
Modules Flexi Port (optionnels)	8 ports GbE Cuivre 8 ports GbE fibre SFP 4 ports 10 GbE fibre SFP+ 4 ports GbE cuivre bypass (2 paires) 2 ports 40 GbE fibre QSFP+ 8 ports 10 GbE fibre SFP+ 2 ports GbE fibre (LC) Bypass + 4 ports GbE SFP fibre 2 ports 10 GbE fibre (LC) Bypass + 4 ports 10 GbE SFP+ fibre Module haute densité (NIC) : 12 ports GE cuivres + 4 ports 2,5 GE cuivre
Densité max. totale de ports (dont l'utilisation de modules)	68
Connectivité complémentaire en option	Module SFP DSL (VDSL2) Émetteurs-récepteurs SFP/SFP+
Affichage	Module LCD multifonction

* Émetteurs-receveurs (mini GBIC) vendus séparément

Adapter la connectivité avec des modules optionnels

Modules de connectivité

Ajoutez des options supplémentaires de connectivité à vos appliances pour renforcer le modèle et les performances de votre réseau.

Série XGS : Modules de connectivité optionnels

Modules Desktop		*Autres modules de connectivité*
 Second module Wi-Fi 5 Pour XGS 116w, 126w et 136w uniquement (non compatible avec la série XG)	 Module 3G/4G Pour les modèles XGS 116(w), 126(w) et 136(w) uniquement (non compatible avec la série XG)	 Modem VDSL2 SFP Pour toutes les séries XGS et SG avec un port SFP Émetteurs-récepteurs optionnels Une gamme d'émetteurs-récepteurs optionnels est disponible, notamment SFP, SFP+.

Série XGS : Matrice des accessoires par modèle Desktop

	Redondance	*Connectivité*				*Montage*
Modèle	*Alimentation*	*Baie d'extension*	*Module 3G/4G*	*Options Wi-Fi*	*Modem VDSL SFP*	*Kit de montage en rack*
XGS 87	-	-	-	-	En option	En option
XGS 87w	-	-	-	Intégré	En option	En option
XGS 107	Seconde alimentation en option	-	-	-	En option	En option
XGS 107w	Seconde alimentation en option	-	-	Intégré	En option	En option
XGS 116	Seconde alimentation en option	1	En option	-	En option	En option
XGS 116w	Seconde alimentation en option	1	En option	Intégré Second module en option	En option	En option
XGS 126	Seconde alimentation en option	1	En option	-	En option	En option
XGS 126w	Seconde alimentation en option	1	En option	Intégré Second module en option	En option	En option
XGS 136	Seconde alimentation en option	1	En option	-	En option	En option
XGS 136w	Seconde alimentation en option	1	En option	Intégré Second module en option	En option	En option

Modules Flexi Port pour 1U et 2U

Adaptez votre infrastructure à votre matériel et changez-le quand vous en avez besoin. Nos modules LAN Flexi Port optionnel vous donnent la liberté de choisir la connectivité dont vous avez besoin : cuivre, fibre, 10 GbE, 40 GbE – c'est vous qui décidez.

Modèles XGS rackables	*Pour XGS 2xxx/3xxx/4xxx uniquement*	*Pour XGS 5500/6500 uniquement*
 8 ports 1G cuivre	 4 ports 1G cuivre PoE + 4 ports 1G cuivre	 2 ports 40G QSFP+
 8 ports 1G SFP	 4 ports 2,5G cuivre PoE	 8 ports 10G SFP+
 4 ports 10G SFP+		 2 ports 10 GbE fibre (LC) Bypass + 4 ports 10 GbE SFP+ fibre
 4 ports 1G cuivre bypass (2 paires)		 Module Port Flexi haute densité (NIC) 12 ports 1G cuivre + 4 ports 2,5 G cuivre
 2 ports GbE fibre (LC) Bypass + 4 ports GbE SFP fibre		

Remarque : Les modules XGS ne sont compatibles avec aucune des anciennes appliances de la série XG.

Série XGS : Matrice des accessoires par modèle 1U

	Redondance		Connectivité modulaire			Montage
Modèle	Alimentation	2d SSD	Modem VDSL SFP	Baies Flexi Port	Modules Flexi Port	Kit de montage en rack
XGS 2100	Externe en option	-	En option	1	• 8 ports 1G cuivre • 8 ports 1G SFP • 4 ports 10G SFP+ • 4 ports 1G Cuivre bypass • 4 ports 1G cuivre PoE + 4 ports 1G cuivre • 4 ports 2,5G cuivre PoE • 2 ports GbE fibre (LC) Bypass + 4 ports GbE SFP fibre	Équerres de montage incluses Glissières en option
XGS 2300	Externe en option	-	En option	1		Équerres de montage incluses Glissières en option
XGS 3100	Externe en option	-	En option	1		Équerres de montage incluses Glissières en option
XGS 3300	Externe en option	-	En option	1		Équerres de montage incluses Glissières en option
XGS 4300	Externe en option	-	En option	2		Glissières incluses
XGS 4500	Interne en option	SSD redondant interne	En option	2		Glissières incluses

Série XGS : Matrice des accessoires par modèle 2U

	Redondance		Connectivité modulaire			Montage
Modèle	Alimentation	SSD	Modem VDSL SFP	Baies Flexi Port	Modules Flexi Port	Kit de montage en rack
XGS 5500	Inclus	Second SSD redondant inclus	En option	2 + 1 pour module haute densité	• 8 ports 1G cuivre • 8 ports 1G SFP • 4 ports 10G SFP+ • 4 ports 1G Cuivre bypass • 2 ports 40G QSFP+ • 8 ports 10G SFP+ • 2 ports GbE fibre (LC) Bypass + 4 ports GbE SFP fibre • 2 ports 10 GbE fibre (LC) Bypass + 4 ports 10 GbE SFP+ fibre • Module Port Flexi haute densité (NIC) 12 ports 1G cuivre + 4 ports 2,5G cuivre	Glissières incluses
XGS 6500	Inclus	Second SSD redondant inclus	En option	2 + 2 pour modules haute densité		Glissières incluses

Sophos Wireless Protection

Simplicité, sécurité, fiabilité

Simplifiez et protégez votre réseau sans fil en utilisant Sophos Firewall comme contrôleur Wi-Fi. Vos points d'accès Sophos sont automatiquement découverts lorsqu'ils sont connectés, vous permettant de configurer rapidement et facilement différents réseaux sans fil : interne, invités, contractuels. Vous obtenez en toute transparence l'intégration du réseau sans fil avec votre pare-feu, des politiques de sécurité cohérentes sur l'ensemble du trafic filaire et sans fil, et une connectivité haut débit fiable.

Appliances matérielles avec Wi-Fi intégré

Toutes nos appliances Desktop de la série XGS sont disponibles avec un point d'accès Wi-Fi intégré. Pour étendre la couverture, il suffit d'ajouter des points d'accès Sophos de la série APX.

Spécifications techniques

Nos points d'accès APX sont conçus à partir de composants sans fil à haut débit, avec des antennes sur mesure, des ressources CPU ultra performantes, plus de mémoire et un chiffrement plus rapide. Avec la technologie 802.11ac Wave 2 (Wi-Fi 5), ils sont spécialement conçus pour un débit accru en charge, de meilleures performances et une meilleure sécurité.

Modèle	*APX 120*	*APX 320*	*APX 530*	*APX 740*
				
Déploiement	Intérieur : montage sur bureaux, murs ou plafonds			
Normes WLAN	802.11 a/b/g/n/ac			
Radios	1 x 2,4 GHz banque unique 1 x 5 GHz banque unique	1 x 2,4 GHz/5 GHz double bande 1 x 5 GHz banque unique 1 x Bluetooth Low Energy (BLE - pour un usage futur)	1 x 2,4 GHz banque unique 1 x 5 GHz banque unique 1 x Bluetooth Low Energy (BLE - pour un usage futur)	
Antennes	2 x antennes double bande interne pour Radio-1 et 2	2 x antennes double bande interne pour Radio-1 2 x antennes internes 5 GHz pour Radio-2 1 x antenne interne 2,4 GHz pour BLE	3 x antennes internes 2,4 GHz pour Radio-1 3 x antennes internes 5 GHz pour Radio-2 1 x antenne interne 2,4 GHz pour BLE	4 x antennes internes 2,4 GHz pour Radio-1 4 x antennes internes 5 GHz pour Radio-2 1 x antenne interne 2,4 GHz pour BLE
Performances	2 x 2:2 MU-MIMO		3 x 3:3 MU-MIMO	4 x 4:4 MU-MIMO
Interfaces	1 x 12V DC-in 1 x RJ45 10/100/1000 Ethernet avec PoE	1 x RJ45 connecteur console port série 1 x RJ45 10/100/1000 Ethernet avec PoE	1 x RJ45 connecteur console port série 1 x RJ45 10/100/1000 port Ethernet 1 x RJ45 10/100/1000 Ethernet avec PoE	
Puissance (MAX.)	11,8W	11,5W	16,7W	22,4W
Alimentation électrique par câble Ethernet (MIN.)	PoE 802.3af		PoE+ 802.3at	
Dimensions Largeur x hauteur x profondeur	144 x 33,5 x 144 mm 5,67 x 1,32 x 5,67 pouces	155 x 38 x 155 mm 6,11 x 1,5 x 6,11 pouces	183 x 39 x 183 mm 7,21 x 1,54 x 7,21 pouces	195 x 43 x 195 mm 7,68 x 1,7 x 7,68 pouces
Poids	0,256 kg	0,474 kg	0,922 kg	1,012 kg

Si vous préférez libérer les ressources de votre pare-feu et que vous recherchez une meilleure évolutivité, vous pouvez gérer vos points d'accès Sophos dans le Cloud en utilisant Sophos Central, sans frais supplémentaires.

Consultez sophos.fr/compare-xgs pour plus d'informations techniques.

SD-RED

Sophos SD-RED : Renforcez votre stratégie SD-WAN

Sophos a longtemps été un pionnier en fournissant un moyen aisé et sécurisé de connecter les succursales et les autres sites distants. Sophos Firewall comprend un certain nombre de fonctionnalités SD-WAN pour vous aider à accélérer les performances des applications et à obtenir une meilleure visibilité sur la santé du réseau afin de garantir que vos sites distants bénéficient des mêmes performances que votre bureau principal.

Nos boîtiers RED sont fabriqués à partir de plateformes réseau à haut débit destinées à un usage professionnel. Ils fonctionnent avec votre Sophos Firewall, que le déploiement soit matériel, logiciel ou dans le Cloud public. Notre gamme complète de points d'accès sans fil Sophos Wireless est également compatible avec Sophos SD-RED. Pour gérer Sophos SD-RED, vous devez avoir un abonnement Network Protection actif.

Spécifications techniques

Modèle	*SD-RED 20*	*SD-RED 60*
		
Capacité		
Débit maximal	250 Mbit/s	850 Mbit/s
Interfaces physiques (intégrées)		
Interfaces LAN	4 x 10/100/1000 Base-TX (1 GbE cuivre)	4 x 10/100/1000 Base-TX (1 GbE cuivre)
Interfaces WAN	1 x 10/100/1000 Base-TX (partagé avec SFP)	2 x 10/100/1000 Base-TX (port WAN1 partagé avec SFP)
Interfaces SFP	1x SFP fibre (port partagé avec WAN)	1x SFP fibre (port partagé avec WAN1)
Ports PoE (Alim. par Ethernet)	Aucun	2 ports PoE (puissance totale 30 W)
Ports USB	2 x USB 3.0 (avant et arrière)	2 x USB 3.0 (avant et arrière)
Ports COM	1 x Micro-USB	1 x Micro-USB
Connectivité en option		
Baie modulaire	1 (à utiliser avec une carte Wi-Fi OU 4G/LTE optionnelle)	1 (à utiliser avec une carte Wi-Fi OU 4G/LTE optionnelle)
Module Wi-Fi en option	802.11 a/b/g/n/ac Wave 1 (Wi-Fi 5) à double bande 2 x 2 MIMO 2 antennes	802.11 a/b/g/n/ac Wave 1 (Wi-Fi 5) à double bande 2 x 2 MIMO 2 antennes
Module 3G/4G/LTE en option	Carte Sierra Wireless MC7430/MC7455	Carte Sierra Wireless MC7430/MC7455
Modem VDSL en option	Modem VDSL en option (support dans une prochaine version)	Modem VDSL en option (support dans une prochaine version)
Spécifications physiques		
Dimensions Largeur x hauteur x profondeur	225 x 44 x 150 mm 8,86 x 1,73 x 5,91 pouces	225 x 44 x 150 mm 8,86 x 1,73 x 5,91 pouces
Poids	0,9 kg/1,8 kg sans/avec emballage	1,0 kg/2,2 kg sans/avec emballage
Adaptateur d'alimentation	Entrée AC : 110-240VAC @50-60 Hz Sortie DC : 12 V +/- 10 %, 3,7A, 40W	Entrée AC : 110-240VAC @50-60 Hz Sortie DC : 12 V +/- 10 %, 6,95A, 75W
Support pour la redondance de l'alimentation	Oui, seconde alimentation en option	Oui, seconde alimentation en option
Consommation électrique	6,1W, 20,814 BTU (au repos) 22,6W, 77,114 BTU (charge complète)	11,88W, 40,536 BTU/h (au repos) 25,33W, 86,429 BTU/h (charge totale sans PoE) 62,48W, 213,190 BTU/h (charge totale avec PoE)
Température (fonctionnement)	0°C à 40°C (32°F à 104°F)	0°C à 40°C (32°F à 104°F)
Température (stockage)	-20°C à 70°C (-4°F à 158°F)	-20°C à 70°C (-4°F à 158°F)
Humidité	10 % à 90 %, sans condensation	10 % à 90 %, sans condensation
Normes de sécurité		
Certifications (Sécurité, EMC, Radio)	CE/FCC/IC/RCM/VCCI/CB/UL/CCC/KC/ANATEL	CE/FCC/IC/RCM/VCCI/CB/UL/CCC/KC/ANATEL

Consultez sophos.fr/compare-xgs pour plus d'informations techniques.

Ressources supplémentaires

Nous disposons d'un large éventail de ressources pour vous aider à parfaire vos connaissances sur Sophos Firewall et les produits associés.

- Page Web Sophos Firewall - sophos.fr/firewall
- Modèles matériels de la série XGS – sophos.fr/compare-xgs
- Écosystème Sophos Firewall : modules complémentaires et accessoires – sophos.fr/firewall-ecosystem
- Sophos Switch - sophos.fr/switch
- Sophos Zero Trust Network Access - sophos.fr/ztna

Évaluation gratuite – pour les entreprises ou à domicile

Pour tout renseignement supplémentaire, rendez-vous sur Sophos.fr ou contactez l'un de nos agents commerciaux.

30 jours d'essai gratuit sans engagement

Pour évaluer le produit complet, inscrivez-vous à un essai gratuit de 30 jours.

Découvrez-le en action.

Découvrez l'interface utilisateur en accédant à la démo interactive, ou visionnez nos vidéos démontrant comment Sophos simplifie la sécurité du réseau.

Visitez sophos.fr/firewall pour plus d'informations.

Édition familiale gratuite

Sophos Firewall Home Edition est une version logicielle complète conçue uniquement pour l'usage à domicile. Elle protège le réseau, le Web, la messagerie et les applications Web, et possède une fonctionnalité VPN. Elle se limite à 4 cœurs virtuels et 6 Go de RAM.
Rendez-vous sur sophos.fr/freetools

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

22-12-09 BR-FR (DD)

SOPHOS

FORTINET

Product Matrix
June 2024

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG/FWF-40F	FG/FWF-50G	FG/FWF-60F	FG-70F
Firewall Throughput (1518/512/64 byte UDP)	5 / 5 / 5 Gbps	5 / 5 / 4 Gbps	10/10/6 Gbps	10 / 10 / 6 Gbps
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps	4.5 Gbps	6.5 Gbps	6.1 Gbps
IPS Throughput (Enterprise Mix) [2]	1 Gbps	2.25 Gbps	1.4 Gbps	1.4 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	800 Mbps	1.25 Gbps	1 Gbps	1 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	600 Mbps	1.1 Gbps	700 Mbps	800 Mbps
Firewall Latency	2.97 µs	2.42 µs	3.3 µs	2.54 µs
Concurrent Sessions	700 000	720 000	700 000	1.5 Million
New Sessions/Sec	35 000	85 000	35 000	35 000
Firewall Policies	2 000	2 000	2 000	5 000
Max G/W to G/W IPSEC Tunnels	200	200	200	200
Max Client to G/W IPSEC Tunnels	250	250	500	500
SSL VPN Throughput	490 Mbps [10]	—	900 Mbps [10]	405 Mbps [8]
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200 [10]	—	200 [10]	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps	1.3 Gbps	630 Mbps	700 Mbps
Application Control Throughput (HTTP 64K) [2]	990 Mbps	2.8 Gbps	1.8 Gbps	1.8 Gbps
Max FortiAPs (Total / Tunnel)	16 / 8	16 / 8	64 / 32	64 / 32
Max FortiSwitches	8	8	24	24
Max FortiTokens	500	500	500	500
Virtual Domains (Default/Max)	10 / 10	5 / 5	10 / 10	10 / 10
Interfaces	5x GE RJ45	5x GE RJ45	10x GE RJ45	10x GE RJ45
Local Storage	—	64 GB (51G)	128 GB (61F)	128 GB (71F)
Power Supplies	Single AC PS	Single AC PS	Single AC PS	Single AC PS
Form Factor	Desktop	Desktop	Desktop	Desktop
Variants	WiFi, 3G4G	WiFi, DSL, SFP, POE	WiFi, Storage	—

	FG/FWF-80F	FG-90G	FG-100F	FG-120G
Firewall Throughput (1518/512/64 byte UDP)	10 / 10 / 7 Gbps	28 / 28 / 27.9 Gbps	20 / 18 / 10 Gbps	39 / 39 / 28 Gbps
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps	25 Gbps	11.5 Gbps	35 Gbps
IPS Throughput (Enterprise Mix) [2]	1.4 Gbps	4.5 Gbps	2.6 Gbps	5.3 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	1 Gbps	2.5 Gbps	1.6 Gbps	3.1 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	900 Mbps	2.2 Gbps	1 Gbps	2.8 Gbps
Firewall Latency	3.23 µs	3.23µs	4.97µs	3.17 µs
Concurrent Sessions	1.5 Million	3 Million	1.5 Million	3 Million
New Sessions/Sec	45 000	124 000	56 000	140 000
Firewall Policies	5 000	5 000	10 000	10 000
Max G/W to G/W IPSEC Tunnels	200	200	2 000	2 000
Max Client to G/W IPSEC Tunnels	2,500	2 500	16 000	16 000
SSL VPN Throughput	950 Mbps	1.4 Gbps [8]	1 Gbps	1.5 Gbps [8]
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200	200	500	500
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	715 Mbps	2.6 Gbps	1 Gbps	3 Gbps
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps	6.7 Gbps	2.2 Gbps	6.7 Gbps
Max FortiAPs (Total / Tunnel)	96 / 48	96 / 48	128 / 64	128 / 64
Max FortiSwitches	24	24	32	32
Max FortiTokens	500	500	5 000	5 000
Virtual Domains (Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces	8x GE RJ45, 2x Shared Port Pairs	8x GE RJ45, 2× 10GE Shared Port Pairs	2× 10 GE SFP+, 18x GE RJ45, 4x Shared Port Pairs, 8x GE SFP	4× 10 GE SFP+, 18x GE RJ45, 8x GE SFP
Local Storage	128 GB (81F)	120 GB (91G)	480 GB (101F)	480 GB (121G)
Power Supplies	Single AC PS, dual inputs	Single AC PS, dual inputs	Dual AC PS	Dual AC PS
Form Factor	Desktop	Desktop	1 RU	1 RU
Variants	WiFi, 3G4G, DSL, Bypass, Storage	—	—	—

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG-200F	FG-400F	FG-600F	FG-900G	FG-1000F
Firewall Throughput (1518/512/64 byte UDP)	27 / 27 / 11 Gbps	79.5 / 78.5 / 70 Gbps	139 / 137.5 / 70 Gbps	164 / 163 / 153 Gbps	198 / 196 / 134 Gbps
IPsec VPN Throughput (512 byte) [1]	13 Gbps	55 Gbps	55 Gbps	55 Gbps	55 Gbps
IPS Throughput (Enterprise Mix) [2]	5 Gbps	12 Gbps	14 Gbps	26 Gbps	19 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	3.5 Gbps	10 Gbps	11.5 Gbps	22 Gbps	15 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	3 Gbps	9 Gbps	10.5 Gbps	20 Gbps	13 Gbps
Firewall Latency	4.78 µs	4.19 µs / 2.5 µs [7]	4.12 µs / 2.5 µs [7]	3.78 / 2.5 µs [7]	3.45 µs
Concurrent Sessions	3 Million	7.8 Million	8 Million	16 Million	7.5 Million
New Sessions/Sec	280 000	500 000	550 000	720 000	650 000
Firewall Policies	10 000	10 000	30 000	10 000	100 000
Max G/W to G/W IPSEC Tunnels	2 000	2 000	2 000	2 000	20 000
Max Client to G/W IPSEC Tunnels	16 000	50 000	50 000	50 000	100 000
SSL VPN Throughput	2 Gbps	3.6 Gbps [8]	4.3 Gbps [8]	10 Gbps [8]	5.3 Gbps [8]
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	500	5000	10 000	10 000	10 000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	4 Gbps	8 Gbps	9 Gbps	16.7 Gbps	10 Gbps
Application Control Throughput (HTTP 64K) [2]	13 Gbps	28 Gbps	32 Gbps	74.8 Gbps	44 Gbps
Max FortiAPs (Total, Tunnel)	256 / 128	512 / 256	1 024 / 512	2 048 / 1 024	4 096 / 2 048
Max FortiSwitches	64	72	96	96	196
Max FortiTokens	5 000	5 000	5 000	5 000	20 000
Virtual Domains (Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10	10 / 250
Interfaces	4× 10 GE SFP+, 18x GE RJ45, 8x GE SFP	8× 10GE SFP+ , 8x GE SFP, 18 x GE RJ45	4× 25G SFP28, 4× 10GE SFP+ , 8x GE SFP, 18 x GE RJ45	4× 25 GE SFP28, 4× 10 GE SFP+, 1× 2.5GE RJ45, 8 x GE SFP, 17x GE RJ45	2× 100 GE QSFP28, 8x 25 GE SFP28, 16×10 GE SFP+, 8× 10GE RJ45, 1x 2.5GE RJ45, 1 GE RJ45
Local Storage	480 GB (201F)	960 GB (401F)	480 GB (601F)	960 GB (901G)	960 GB (1001F)
Power Supplies	Dual AC PS	Dual AC PS	Dual AC PS	Dual PS	Dual PS
Form Factor	1 RU	1 RU	1 RU	1 RU	2 RU
Variants	—	DC	—	DC	—

	FG-1800F	FG-2600F	FG-3000F	FG-3200F	FG-3300E
Firewall Throughput (1518/512/64 byte UDP)	198 / 197 / 140 Gbps	198 / 196 / 140 Gbps	397 / 389 / 221 Gbps	387 / 385 / 178.5 Gbps	160 / 158 / 100 Gbps
IPsec VPN Throughput (512 byte) [1]	55 Gbps	55 Gbps	105 Gbps	105 Gbps	98 Gbps
IPS Throughput (Enterprise Mix) [2]	22 Gbps	31 Gbps	36 Gbps	63 Gbps	27 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	17 Gbps	27 Gbps	34 Gbps	47 Gbps	23 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	15 Gbps	25 Gbps	33 Gbps	45 Gbps	17 Gbps
Firewall Latency	3.22 µs	3.41 µs	3.92 µs	3.42 µs	3.17 µs
Concurrent Sessions	12 Million / 40 Million [6]	24 Million / 40 Million [6]	70 Million / 230 Million [6]	70 Million	50 Million
New Sessions/Sec	750 000 / 2 Million [6]	1 Million / 2 Million [6]	870 000 / 3 Million [6]	800 000	700 000
Firewall Policies	100 000	100 000	200 000	200 000	200 000
Max G/W to G/W IPSEC Tunnels	20 000	20 000	40 000	40 000	40 000
Max Client to G/W IPSEC Tunnels	100 000	100 000	200 000	200 000	200 000
SSL VPN Throughput	11 Gbps	16 Gbps	11 Gbps [8]	11 Gbps [8]	10 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10 000	30 000	30 000	30 000	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	12 Gbps	20 Gbps	29 Gbps	29 Gbps	21 Gbps
Application Control Throughput (HTTP 64K) [2]	34 Gbps	64 Gbps	115 Gbps	109 Gbps	70 Gbps
Max FortiAPs (Total, Tunnel)	4 096 / 2 048	4 096 / 2 048	4 096 / 2 048	4 096 / 2 048	4 096 / 2 048
Max FortiSwitches	196	196	300	300	300
Max FortiTokens	20 000	20 000	20 000	20 000	20 000
Virtual Domains (Default/Max)	10 / 250	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	4× 100 GE QSFP28, 12x 25 GE SFP28, 2×10 GE SFP+, 8x GE SFP, 18x GE RJ45 [9]	4× 100GE QSFP28/40GE QSFP+, 16× 25GE SFP28, 16× 10GE RJ45, 2× 10GE SFP+, 2x GE RJ45	6× 100GE QSFP28/40GE QSFP+, 16× 25GE SFP28, 18× 10GE RJ45, 2x GE RJ45	4× 400GE QSFP-DD, 12x 50GE SFP56, 4× 25GE SFP28, 2× 10GE RJ45	4× 40GE QSFP+, 16x 25GE SFP28, 4× 10GE RJ45, 14x GE RJ45
Local Storage	2 TB (1801F)	2 TB (2601F)	2 TB (3001F)	2 TB (3201F)	2 TB (3301E)
Power Supplies	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS
Form Factor	2 RU	2 RU	2 RU	2 RU	2 RU
Variants	DC	DC	DC	—	—

* Featured Top selling models, for complete FortiGate offerings please visit www.fortinet.com. FortiGate virtual appliances are also available. All performance values are "up to" and vary depending on system configuration.

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG-3500F	FG-3700F	FG-4200F	FG-4400F	FG-4800F
Firewall Throughput (1518/512/64 byte UDP)	595 / 590 / 420 Gbps	589 / 589 / 420 Gbps	800 / 788 / 400 Gbps	1.15 / 1.14 / 0.50 Tbps	3.1 / 3.1 / 0.93 Tbps
IPsec VPN Throughput (512 byte) [1]	165 Gbps	160 Gbps	210 Gbps	310 Gbps	800 Gbps
IPS Throughput (Enterprise Mix) [2]	72 Gbps	86 Gbps	52 Gbps	94 Gbps	87 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	65 Gbps	80 Gbps	47 Gbps	82 Gbps	77 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	63 Gbps	75 Gbps	45 Gbps	75 Gbps	75 Gbps
Firewall Latency	2.98 µs	3.56 µs / 1.45 µs [7]	3.02 µs	2.98 µs	3.6 µs
Concurrent Sessions	140 Million / 348 Million [6]	140 Million	210 Million / 450 Million [6]	210 Million / 700 Million [6]	280 Million / 1.8 Billion [6]
New Sessions/Sec	1 Million / 5 Million [6]	930 000	1 Million / 7 Million [6]	1 Million / 10 Million [6]	915,000 / 25 Million [6]
Firewall Policies	200 000	200 000	400 000	400 000	400 000
Max G/W to G/W IPSEC Tunnels	40 000	40 000	40 000	40 000	40 000
Max Client to G/W IPSEC Tunnels	200 000	200 000	200 000	200 000	200 000
SSL VPN Throughput	16 Gbps [8]	16 Gbps [8]	16 Gbps	16 Gbps	18 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30 000	30 000	30 000	30 000	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	63 Gbps	55 Gbps	50 Gbps	86 Gbps	63 Gbps
Application Control Throughput (HTTP 64K) [2]	135 Gbps	190 Gbps	135 Gbps	140 Gbps	180 Gbps
Max FortiAPs (Total, Tunnel)	4 096 / 2 048	4 096 / 2 048	8 192 / 4 096	8 192 / 4 096	8 192 / 4 096
Max FortiSwitches	300	300	300	300	300
Max FortiTokens	20,000	20,000	20,000	20,000	20,000
Virtual Domains (Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	6× 100GE QSFP28/40GE QSFP+, 32× 25GE SFP28, 2x GE RJ45	4× 400GE QSFP-DD, 4x ULL 25GE SFP28, 20x 50GE SFP56, 2× 10GE RJ45	8× 100GE QSFP28/40GE QSFP+, 18× 25GE SFP28, 2x GE RJ45	12× 100GE QSFP28/40GE QSFP+, 20× 25GE SFP28, 2x GE RJ45	8× 400GE, 12× 200GE QSFP56, 12× 50GE SFP56, 2× 10GE RJ45
Local Storage	4 TB (3501F)	4 TB (3701F)	4 TB (4201F)	4 TB (4401F)	4 TB (4801F)
Power Supplies	Dual PS	Dual PS	Dual PS	4 PS	4 PS
Form Factor	2 RU	2 RU	3 RU	4 RU	4 RU
Variants	—	—	DC	DC	DC

	FG-6001F	FG-6300F	FG-6500F	FG-7081F	FG-7121F
Firewall Throughput (1518/512/64 byte UDP)	120 - 239 / 120 -238 / 40.5 - 135 Gbps	239 / 238 / 135 Gbps	239 / 238 / 135 Gbps	1.89 / 1.88 / 1.129 Tbps	1.89 / 1.88 / 1.129 Tbps
IPsec VPN Throughput (512 byte) [1]	40 - 160 Gbps	96 Gbps	160 Gbps	378 Gbps	630 Gbps
IPS Throughput (Enterprise Mix) [2]	51 - 170 Gbps	110 Gbps	170 Gbps	405 Gbps	675 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	45 - 150 Gbps	90 Gbps	150 Gbps	330 Gbps	550 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	30 - 100 Gbps	60 Gbps	100 Gbps	312 Gbps	520 Gbps
Firewall Latency	4.8 µs	4.8 µs	4.8 µs	7.5 µs	7.5 µs
Concurrent Sessions	60 - 200 Million	120 Million	200 Million	600 Million	1 Billion
New Sessions/Sec	900 000 - 3 Million	2 Million	3 Million	5.4 Million	9 Million
Firewall Policies	200 000	200 000	200 000	200 000	200 000
Max G/W to G/W IPSEC Tunnels	16 000	16 000	16 000	40 000	40 000
Max Client to G/W IPSEC Tunnels	90 000	90 000	90 000	260 000	260 000
SSL VPN Throughput	9 Gbps	9 Gbps	9 Gbps	13.7 Gbps	13.7 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30 000	30 000	30 000	30 000	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	33 - 110 Gbps	66 Gbps	110 Gbps	324 Gbps	540 Gbps
Application Control Throughput (HTTP 64K) [2]	66 - 220 Gbps	150 Gbps	220 Gbps	900 Gbps	1.5 Tbps
Max FortiAPs (Total, Tunnel)	—	—	—	—	—
Max FortiSwitches	256	256	256	256	300
Max FortiTokens	20 000	20 000	20 000	20 000	20 000
Virtual Domains (Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 3× 10GE SFP+,2x GE RJ45	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 3× 10GE SFP+,2x GE RJ45	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 3× 10GE SFP+,2x GE RJ45	Varied	Varied
Local Storage	2 TB NVMe	2 TB NVMe (6301F)	2 TB NVMe (6501F)	4× 4 TB SSD	4× 4 TB SSD
Power Supplies	3 PS	3 PS	3 PS	6 PS	8 PS
Form Factor	3 RU	3 RU	3 RU	12 RU	16 RU
Variants	—	DC	DC	DC	DC

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS, Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.
4. NGFW performance is measured with Firewall, IPS and Application Control enabled, Enterprise Mix traffic.
5. Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled, Enterprise Mix traffic.
6. Requires Hyperscale license
7. With Ultra-Low Latency ports
8. Uses RSA-2048 certificate
9. FortiOS 7.4+ is required for 100 GE support
10. SSL VPN not supported on FortiOS 7.6.0 and above, for models with 2GB RAM.

FortiManager™ Centralized Management Platform

	FMG-200G	FMG-410G	FMG-1000G	FMG-3000G	FMG-3100G	FMG-3700G	FMG-VM-BASE to FMG-VM-UL-UG
Devices/VDOMs (Maximum)	30	150	1,000	4,000+	4,000+	10,000+	10 to Unlimited
Sustained Log Rates	50	50	50	150	150	150	Hardware dependent
GB/Day	2	2	2	10	10	10	1-50
Total Interfaces	4x GE RJ45	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2x 25GE SFP28	2x GE RJ45, 2x 25GE SFP28	2x GE RJ45, 2x 25GE SFP28	2× 10GE RJ45, 2× 25GE SFP28	1 / 4 (vNIC Min / Max)
Storage Capacity	2× 4 TB	8× 4 TB	8× 4 TB	16× 4 TB	16× 4 TB	60× 4TB HDD + 6× 3.2TB NVMe SSD	80 GB / 16 TB (Min / Max)

FortiAnalyzer™ Centralized Logging and Reporting Solution

	FAZ-150G	FAZ-300G	FAZ-810G	FAZ-1000G	FAZ-3100G	FAZ-3510G	FAZ-3700G	FAZ-VM-BASE to FAZ-VM-GB2000
GB Logs/Day	25	100	200	660	3,000	5,000	8,300	1 to +2,000
Analytic Sustained Rate (logs/sec)	500	2,000	4,000	20,000	42,000	60,000	100,000	—
Collector Sustained Rate (logs/sec)	750	3,000	6,000	30,000	60,000	90,000	150,000	—
Total Interfaces	2x GE RJ45	4x GE RJ45	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2× 25GE SFP28	2x GE RJ45, 2× 25GE SFP28	2× 10GE RJ45, 2× 25GE SFP28	2× 10GE RJ45, 2× 25GE SFP28	1 / 4 (vNIC Min / Max)
Storage Capacity	2× 2 TB	2× 4 TB	4× 4 TB	8× 4 TB	16× 4TB HDD + 2× 1.92TB SSD	24× 4TB HDD + 2× 3.84TB NVMe SSD	60× 4TB HDD + 6× 3.2TB NVMe SSD	500 GB to +100 TB

FortiSIEM™ Unified Event Correlation and Risk Management Solution

	FSM-500G "COLLECTOR"	FSM-2000G "SUPERVISOR"	FSM-2200G "SUPERVISOR"	FSM-3500G "SUPERVISOR"	FSM-3600G "SUPERVISOR"
Performance Benchmark	8K EPS. 500 SNMP, 200 WMI for Performance/100 WMI for Logs	20K EPS with Collectors	20K EPS with Collectors	40K EPS with Collectors	50K EPS with Collectors
Recommended Max. UEBA users	N/A	10 000	10 000	10 000	10 000

FortiAuthenticator™ User Identity Management Server

	FAC-300F	FAC-800F	FAC-3000F	FAC-VM BASE to FAC-VM-10000-UG
Max Local + Remote Users/ User Group	1,500 / 150	8,000 / 800	40,000 / 240,000	100 / 10 to +10,000 / 1,000
Max NAS Devices	500	2,666	80,000	33 to +33,333
Max FortiTokens	3,000	16,000	480,000	200 to +20,000
Interfaces	4x GE RJ45	4x GE RJ45, 2x SFP	4x GE RJ45, 2x SFP	1 - 4 vNICs
Storage Capacity	2	2× 2 TB	2× 2 TB	60 GB to 16 TB

FortiAP™ Wireless Access Point

	FortiAP Series	FortiAP U-Series
Management	FortiGate-Managed, Cloud-Managed	FortiGate-Managed, Cloud-Managed, Controller-Managed
Security	Via FortiGate	Via FortiGate

* Frequency selection and power may be restricted to abide by regional regulatory compliance laws.
For Complete selection of FortiAPs, including remote and outdoor devices, please refer to Fortinet Wireless Solution Matrix

FortiSwitch™ Secured Access Switch

	100 Series	200 Series	400 Series	500 Series	600 Series	1000 Series	2048F	3032E
Main Port Speed	1 Gbps	1 Gbps	1 Gbps	1 Gbps	2.5/5 Gbps	10 Gbps	25 Gbps	40/100 Gbps
Main Port Count Options	8, 24, 48	24, 48	24, 48	24, 48	24, 48	24, 48	48	32
Uplink Port Speed	1 or 10 Gbps	1 Gbps	10 Gbps	10 Gbps	25 Gbps	40 or 100 Gbps	100 Gbps	n/a
Redundant Power Supplies	—	Some Models	Some Models	Optional RSU	•	•	•	•
PoE Options	•	•	•	•	•	—	—	—

For Complete selection of FortiSwitches, please refer to http://www.fortinet.com/products/fortiswitch

FortiNAC™ Network Access Control Solution

	FNC-CA-500F	FNC-CA-600F	FNC-CA-700C	FNC-M-550F
Type	Mid-range Control and Application Server	High Performance Control and Application Server	Ultra High Performance Control and Application Server	Centralized Management Appliance
Target Environment	Small Environments	Medium Environments	Large Environments with few Persistent Agents	Multi-site environments with multiple appliances
Capacity	Manages up to 5,000 ports in the network*	Manages up to 15,00 ports in the network*	Manages up to 25,000 ports in the network*	manage up to 50 CA servers

Ports in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices. Virtual appliances are also available, please refer to www.fortinet.com for more information

FortiSandbox™ Advanced Threat Prevention System

	PAAS FORTISANDBOX CLOUD	FSA-VM	FSA-500G	FSA-1500G	FSA-3000F
Effective Sandboxing Throughput [1] (Files/Hour)	20 - 4,000	100 - 1,000	10,000	32,000	68,000
Number of Users [2]	8 – 1,600	40 – 1,600	1,400	4,000	6,400
Number of Local VMs	—	up to 8	2 + 12 Optional	2 + 26 Optional	8 + 64 Optional

1. Tested based on files with 80% documents and 20% executables. Includes both static and dynamic analysis with pre-filtering enabled; measured based on v4.2.22
2. Based on a ratio of one user per 25 emails

FortiClient™ Advanced Endpoint Security

	Windows	MAC OS X	Linux	Android	iOS	Chromebook
Zero Trust Security (ZTNA) Options	✓	✓	✓	—	—	Partial
Next Generation Endpoint Security (EPP / APT) Options	✓	✓	✓	—	—	—
Cloud Based Endpoint Security (SASE) Options	✓	✓	✓	—	—	—
Security Fabric Components	✓	✓	Partial	Partial	Partial	Partial
VPN Client	✓	✓	SSL VPN only	✓	SSL VPN only	—

FortiMail™ Messaging Security Server

	FML-200F	FML-400F	FML-900F	FML-2000F	FML-3000F	FML-3200E
Email Routing* (Msg/Hr)	50,000	250,000	800,000	1.6 Mil	3.5 Mil	3.4 Mil
Performance Enterprise ATP* (Msg/Hr)	30,000	150,000	400,000	800,000	2.1 Mil	2.0 Mil
Email Domains	20	100	800	1,000	2,000	2,000
Server Mode Mailboxes	150	400	1,500	2,000	3,000	3,000
Storage Capacity	1× 1 TB	2× 1 TB	2× 2 TB (8 TB Max)	2× 2 TB (12 TB Max)	2× 2 TB (20 TB Max)	2× 2 TB (20 TB Max)

* Measured based on 100KB message size, no queuing.
Virtual appliances are also available, please refer to www.fortinet.com for more information

FortiWeb™ Web Application Firewall

	FWB-100F	FWB-400F	FWB-600F	FWB-1000F	FWB-2000F	FWB-3000F	FWB-4000F
Throughput (HTTP)	100 Mbps	500 Mbps	1 Gbps	2.5 Gbps	5 Gbps	10 Gbps	70 Gbps
Total Interfaces	4x GE RJ45	4x GE RJ45, 4x GE SFP	2 (+2 bypass) x GE RJ45, 4x GE SFP	2× 10GE SFP+, 4x GE RJ45 Bypass, 4x GE SFP	4× 10GE SFP+, 4x GE RJ45 Bypass, 4x GE SFP	10× 10GE SFP+ (incl. 2 Bypass) , 8x GE RJ45 Bypass	2× 40GE QSFP Bypass, 10× 10GE SFP+ (incl. 2 Bypass) , 8x GE RJ45 Bypass

Virtual appliances are also available, please refer to www.fortinet.com for more information

Virtual Appliance Support Matrix

	VMWare vSphere	Citrix Xen Server	Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Amazon AWS	Microsoft Azure	Oracle OPC/OCI	Google GCP	Alibaba Aliyun
FortiGate-VM *	•	•	•	•	•	•	• / #	• / #	• /#	• /#	• / #
FortiManager-VM	•	•	•	•	•	•	• / #	•	•	•	•
FortiAnalyzer-VM	•	•	•	•	•	•	• / #	•	•	•	•
FortiWeb-VM	•	•	•	•	•	•	• / #	• / #	•	•	•
FortiWeb Manager-VM	•						•				
FortiMail-VM	•	•		•	•	•	• / #	• / #		•	
FortiAuthenticator-VM	•		•	•	•		•	•	•		
FortiADC-VM	•	•	•	•	•	•	• / #	• / #	• / #	• / #	
FortiVoice-VM	•	•		•	•		•	•			
FortiRecorder-VM	•	•		•	•		#				
FortiSandbox-VM	•			•	•	•	• / #	#			
FortiSIEM-VM	•			•	•	•	•	•			•
FortiProxy-VM	•			•							

*Available as FortiGate-VMX solution for VMware NSX environment, AzureStack and RackSpace (PAYG)
on-demand

List of Other Products

FortiADC Application Delivery Controller
FortiCASB Cloud Access Security Broker
FortiCarrier CGN Gateway
FortiCNP Cloud-native Protection Solution
FortiDDoS DDoS Mitigator
FortiDeceptor Deception-based Solution
FortiDevSec Application Security Testing
FortiEDR EDR Solution
FortiExtender 3G/4G WAN Extender
FortiIsolator Browser Isolation Platform
FortiMonitor NPMD, DEM and IM Systems
FortiNDR Virtual Security Analyst™
FortiPAM Privileged Access Management
FortiProxy Secure Web Gateway
FortiRecorder Network Video Security
FortiRecon Digital Risk Protection Service
FortiSASE Cloud Secure Web Gateway
FortiSIEM SIEM with UEBA Solution
FortiSOAR SOAR Solution
FortiTester Network Tester
FortiToken 2 Factor Authentication Token
FortiVoice Secure VoIP Solution
FortiWLM Wireless Manager
FortiXDR Extended Detection and Response

FORTINET

www.fortinet.com

PROMTX-2024-R151-AUG (Web)

KASPERSKY lab

Solutions de sécurité Kaspersky Lab pour les entreprises

Kaspersky Lab est le plus grand fournisseur privé de solutions de sécurité informatique dans le monde. La société est classée parmi les 4 premiers fournisseurs de solutions de sécurité informatique pour postes de travail. Depuis sa création en 1997, Kaspersky Lab n'a cessé d'innover et propose aujourd'hui des solutions de sécurité de pointe à destination des grands comptes, PME/TPE et des particuliers. Le groupe Kaspersky Lab est présent dans près de 200 pays et territoires, offrant une protection à plus de 400 millions d'utilisateurs (dont 270 000 entreprises) à travers le monde.

Kaspersky Lab compte 37 bureaux implantés dans 32 pays

KASPERSKY lab LE POUVOIR DE PROTÉGER

SOMMAIRE

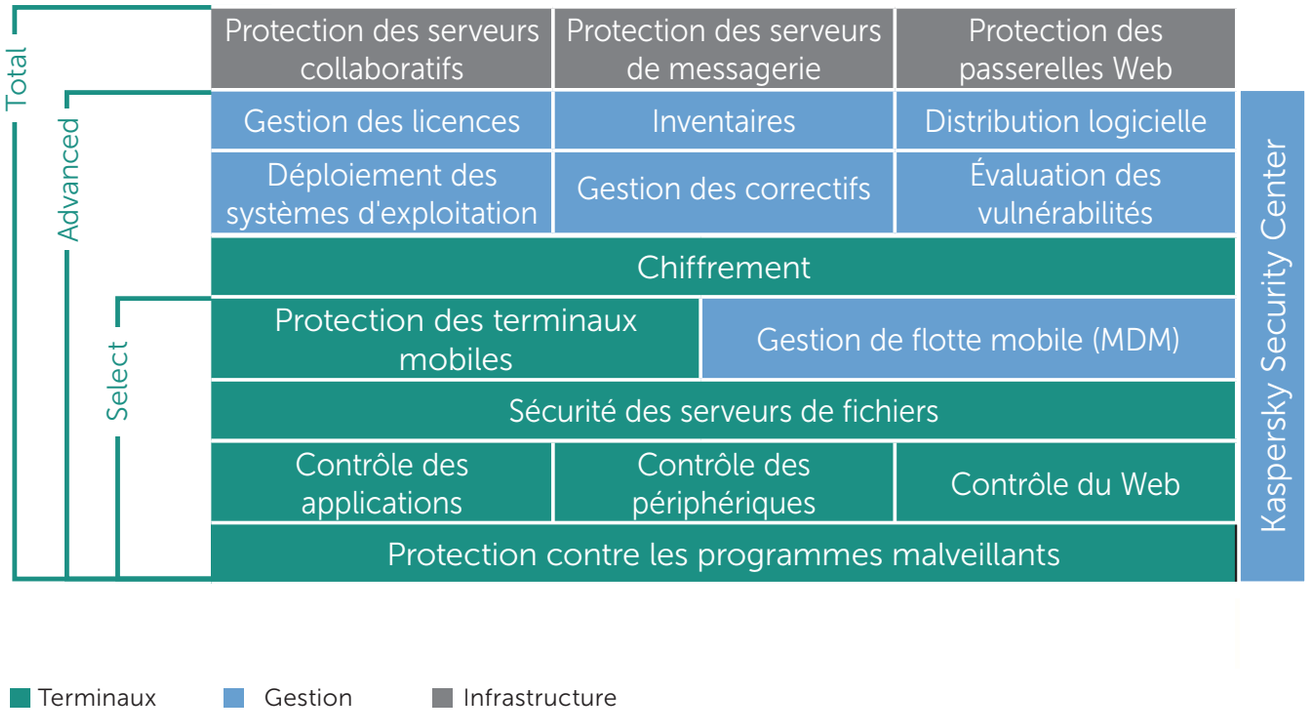
PRODUITS, SOLUTIONS ET SERVICES

Protection de votre système d'information

KASPERSKY SECURITY FOR BUSINESS

Surveillez, gérez et protégez votre environnement informatique avec Kaspersky Endpoint Security for Business.

Notre gamme comprend 3 niveaux de protection ainsi que de nombreuses fonctionnalités qu'il est possible de se procurer 'à la carte'.



Les différentes fonctionnalités sont gérées de façon centralisée, depuis la console d'administration **Kaspersky Security Center.**

Caractéristiques des solutions

Quelle est la solution la mieux adaptée à vos besoins ?

		Select	Advanced	Total	Géré via la console Security Center	Disponible dans une solution à la carte
Outils de contrôle	Protection contre les programmes malveillants	•	•	•	•	
	Pare-feu	•	•	•	•	
	Contrôle des applications	•	•	•	•	
	Contrôle des périphériques	•	•	•	•	
	Contrôle du Web	•	•	•	•	
Sécurité mobile	Sécurité des serveurs de fichiers	•	•	•	•	•
	Protection des terminaux mobiles	•	•	•	•	•
	Gestion de flotte mobile (MDM)	•	•	•	•	•
	Chiffrement		•	•	•	
Gestion des systèmes	Analyse des vulnérabilités		•	•	•	•
	Gestion des correctifs (Patch management)		•	•	•	•
	Inventaires		•	•	•	•
	Gestion des licences		•	•	•	•
	Déploiement d'applications		•	•	•	•
	Déploiement des systèmes d'exploitation		•	•	•	•
	Protection des outils collaboratifs			•		•
	Protection des serveurs de messagerie			•	•	•
	Protection de la passerelle Internet			•		•
	Protection des infrastructures virtuelles				•	•
	Protection des serveurs de stockage				•	•
	Protection de la fraude en ligne et sur mobile					•
	Protection contre les attaques DDoS					•

• Inclus • Inclus en partie (voir pages descriptives du produit)

Solutions à la carte

Protection des serveurs de fichiers

KASPERSKY SECURITY FOR FILE SERVER

POUR WINDOWS, LINUX ET FREEBSD

Kaspersky Security for File Server est une solution efficace, fiable et évolutive destinée à la protection du stockage de fichiers, sans impact perceptible sur les performances du système.

- Protection centralisée, en temps réel
- Gestion hiérarchique du stockage
- Fiabilité et haute tolérance aux pannes
- Solution évolutive et adaptable, même pour les infrastructures les plus complexes

INTÈGRE KASPERSKY SECURITY FOR WINDOWS SERVER

Première solution du marché capable de limiter la propagation des cryptovirus sur les serveurs Windows en cas d'infection.

- Fonction Anti-Cryptor de protection contre le chiffrement des dossiers partagés sur les serveurs de fichiers et les postes de travail infectés par des cryptomalwares
- Protection efficace de vos serveurs Windows, même soumis à fortes charges
- Contrôle du lancement des applications sur les serveurs

Kaspersky Security for File Server est inclus dans KESB - Select, Advanced et Total. Il est également disponible séparément en tant que solution à la carte.

Gestion des systèmes

KASPERSKY SYSTEMS MANAGEMENT

Identifier les vulnérabilités et les corriger dès que possible constitue un élément essentiel dans la défense des entreprises contre les attaques ciblées. Kaspersky Systems Management vous permet d'automatiser les tâches les plus rébarbatives mais néanmoins essentielles :

- Analyse des vulnérabilités : détection et hiérarchisation
- Gestion automatisée des correctifs : patch management
- Inventaires matériels et logiciels automatiques
- Dépannage à distance
- Déploiement d'applications et de systèmes d'exploitation à distance
- Intégration SIEM

Kaspersky Security Management est inclus dans KESB - Advanced et Total. Il est également disponible séparément en tant que solution à la carte.

Sécurité mobile

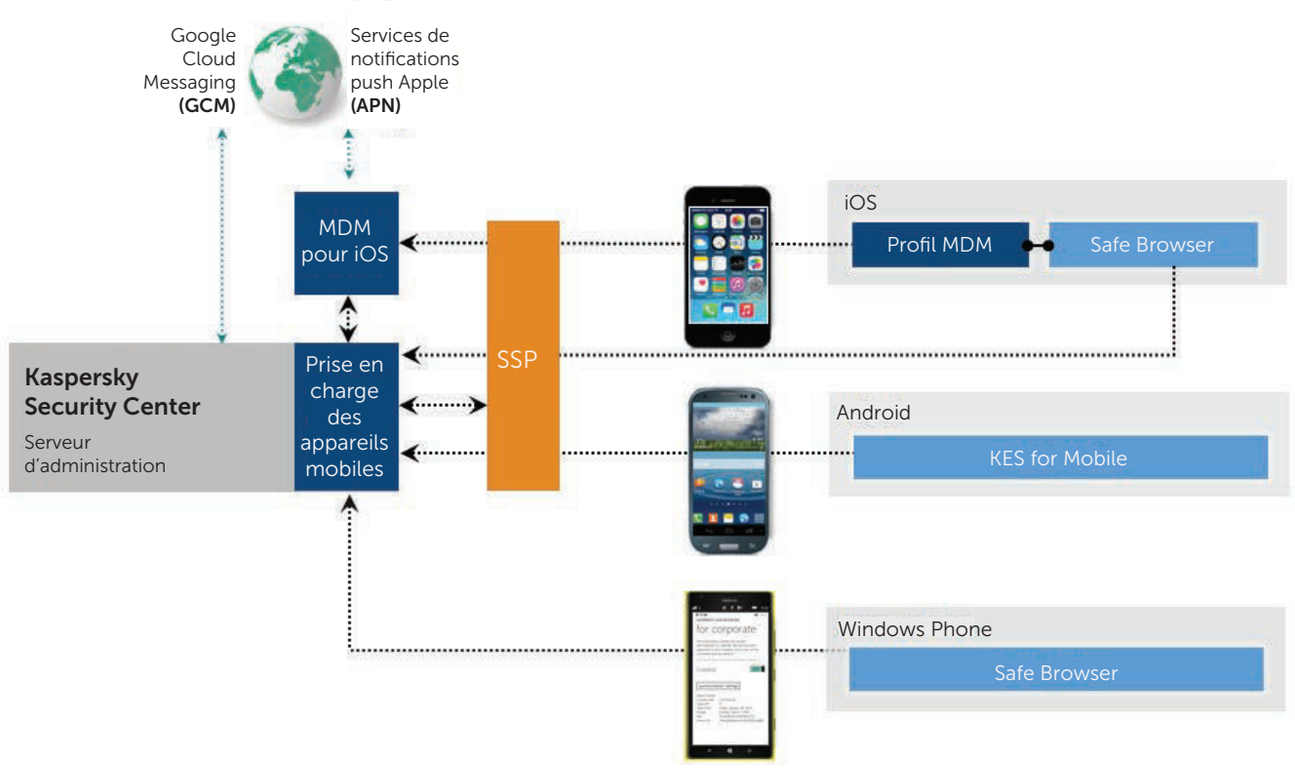
KASPERSKY SECURITY FOR MOBILE

SÉCURITÉ, GESTION ET CONTRÔLE DES SMARTPHONES ET TABLETTES

- **Sécurité mobile** :
  - Puissant anti-malware
  - Anti-phishing, filtrage des SMS et appels entrants
  - Protection Web
  - Détection des terminaux 'jailbreakés'
  - Protection contre le vol

- **Gestion des appareils mobiles** :
  - Intégration aux principales plates-formes : Android, iOS et Windows Phone
  - Contrôle à distance des appareils (OTA, « over-the-air »)

- **Gestion des appareils mobiles** : les outils de contrôle, associés à la mise en conteneurs d'applications permettent de protéger les données et les systèmes de l'entreprise tout en fournissant une politique de sécurité efficace en matière de pratique BYOD.



Architecture de la solution

Kaspersky Security for Mobile est inclus dans KESB - Select, Advanced et Total. Il est également disponible séparément en tant que solution à la carte.

Protection des outils collaboratifs

KASPERSKY SECURITY FOR COLLABORATION

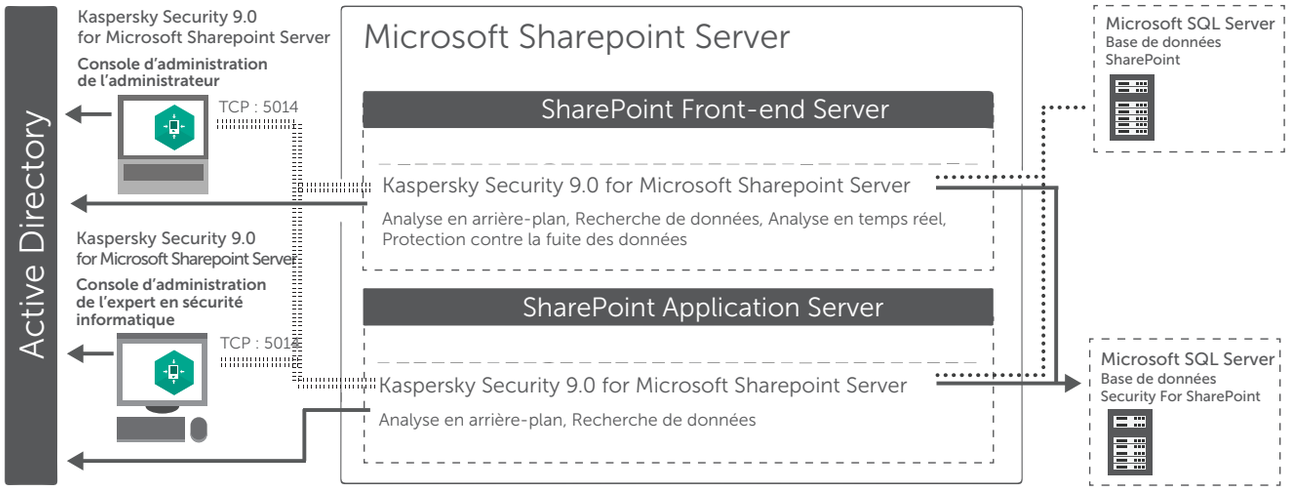
PROTECTION POUR MICROSOFT SHAREPOINT

Kaspersky Security for Collaboration offre à l'ensemble de l'environnement SharePoint et à ses utilisateurs le niveau de sécurité maximal :

- Protège l'ensemble de l'environnement SharePoint
- Prévient la perte de données confidentielles
- Facilite l'application des politiques de l'entreprise grâce au filtrage du contenu
- Intégré à Active Directory

Kaspersky Security for Collaboration analyse le contenu de tous les documents puis enregistre et bloque automatiquement ceux qui contiennent des données confidentielles ou des informations sensibles relatives aux collaborateurs. Il recherche non seulement les mots contenus dans les glossaires préinstallés, ou dans le glossaire personnalisé par l'administrateur, mais analyse également les données structurées.*

Architecture MS SharePoint



**Les fonctionnalités de protection contre les pertes de données sont vendues séparément.*

Kaspersky Security for Collaboration est inclus dans KESB - Total. Il est également disponible séparément en tant que solution à la carte.

Protection de la messagerie

KASPERSKY SECURITY FOR MAIL SERVER

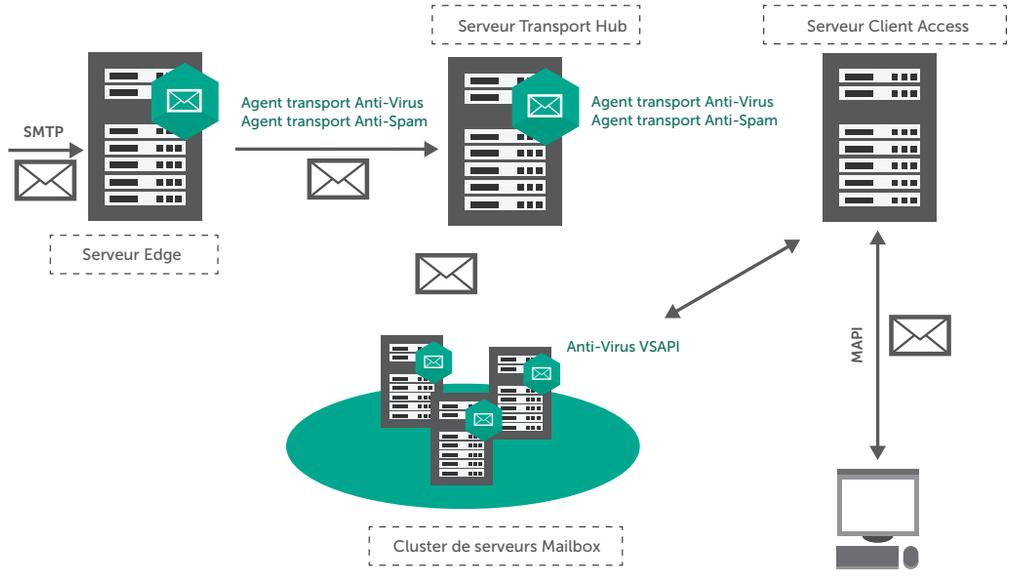
PROTECTION POUR EXCHANGE, LINUX ET DOMINO

Kaspersky Security for Mail Server protège le trafic de messagerie contre les courriers indésirables, les liens de phishing et les programmes malveillants :

- Analyse du courrier entrant, sortant et stocké
- Réduit le trafic grâce à un filtrage intelligent du courrier indésirable
- Prévient la perte de données confidentielles

Il prend en charge les plateformes de messagerie les plus courantes, telles que Microsoft Exchange, Linux Mail Server et IBM Domino. De plus, un module de prévention des pertes de données (DLP) visant à contrôler la propagation d'informations confidentielles peut s'intégrer à la plate-forme de messagerie Microsoft Exchange.

Protection des différents rôles MS Exchange (ex : version 2010)



NOUVEAU !

KASPERSKY SECURITY FOR MAIL GATEWAY

Kaspersky Security for Mail Gateway est une appliance virtuelle qui vous permet de déployer rapidement une passerelle de messagerie virtuelle et de l'intégrer à l'infrastructure de messagerie existante de votre entreprise.

- Protection des courriers entrants et sortants contre les objets malveillants et courriers indésirables (notamment les tentatives de phishing),
- Filtrage du contenu des messages

Kaspersky Security for Mail Server et Kaspersky Security for Mail Gateway sont inclus dans KESB - Total. Ils sont également disponibles séparément en tant que solution à la carte.

Protection des passerelles Internet

KASPERSKY SECURITY FOR INTERNET GATEWAY

ACCÈS INTERNET SÉCURISÉ

L'accès sécurisé à Internet pour l'ensemble des collaborateurs est l'un des piliers centraux de toute stratégie de sécurité d'une entreprise.

Kaspersky Security for Internet Gateway analyse le trafic Web et garantit à l'ensemble de vos effectifs un accès Internet sécurisé en toutes circonstances :

- Analyse en temps réel des protocoles HTTP(s), FTP, SMTP et POP3
- Supporte les plates-formes les plus récentes
- Gère et créé des rapports complets sur l'état de la protection du réseau
- La solution peut être utilisée pour protéger les messageries d'entreprise (pour Microsoft ISA ou TMG).

Kaspersky Security for Internet Gateway est inclus dans KESB - Total. Il est également disponible séparément en tant que solution à la carte.

Protection des infrastructures virtuelles

KASPERSKY SECURITY FOR VIRTUALIZATION

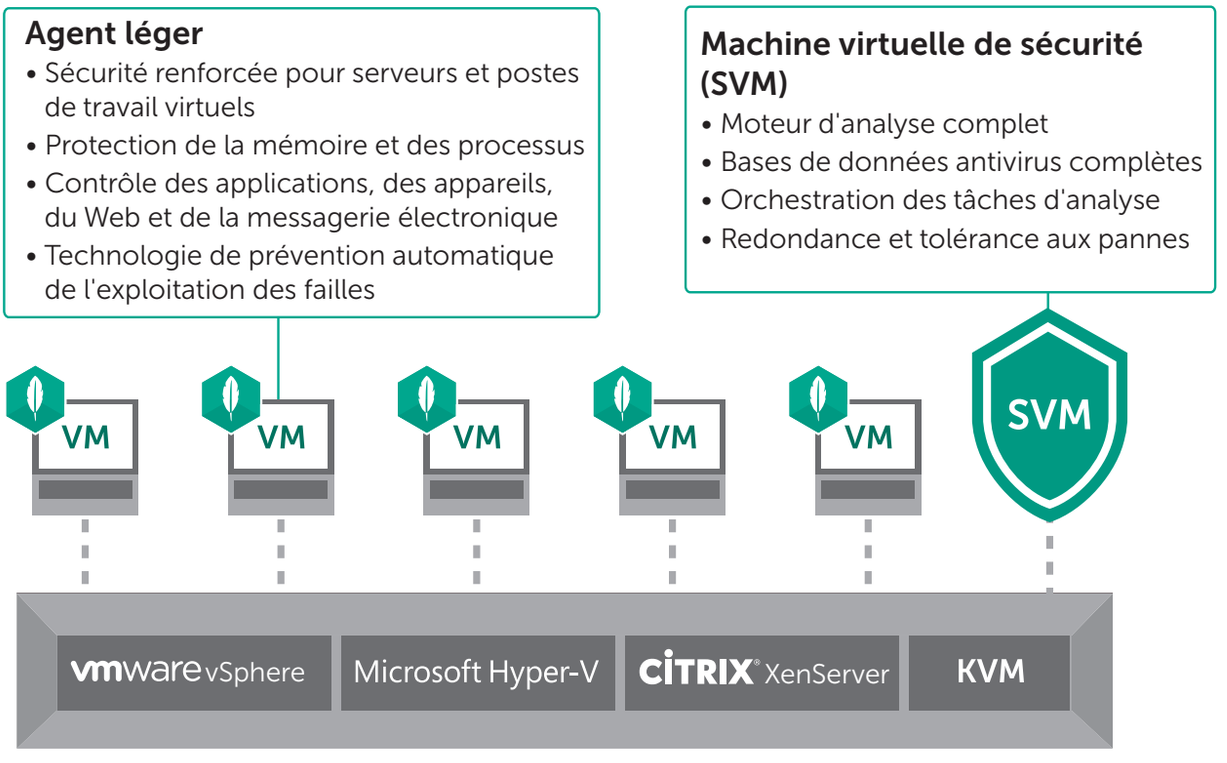
PROTECTION SOUPLE ET EFFICACE POUR LES SERVEURS VIRTUELS ET LES ENVIRONNEMENTS VDI

La solution Kaspersky Security for Virtualization prend en charge les plateformes les plus utilisées, notamment VMware vSphere, Citrix XenServer, Microsoft Hyper-V et KVM. Elle convient ainsi parfaitement aux environnements hétérogènes.

Cette solution s'appuie sur deux approches différentes :

- Sans agent : une appliance virtuelle par hôte exécute des analyses pour détecter les logiciels malveillants sur toutes les machines virtuelles
- Avec agent léger, afin de fournir des niveaux de protection supplémentaires pour chaque machine virtuelle (VM)

La sécurité de vos machines virtuelles est gérée depuis la console Kaspersky Security Center, tout comme vos terminaux, serveurs physiques ou appareils mobiles.



Protection des serveurs de stockage

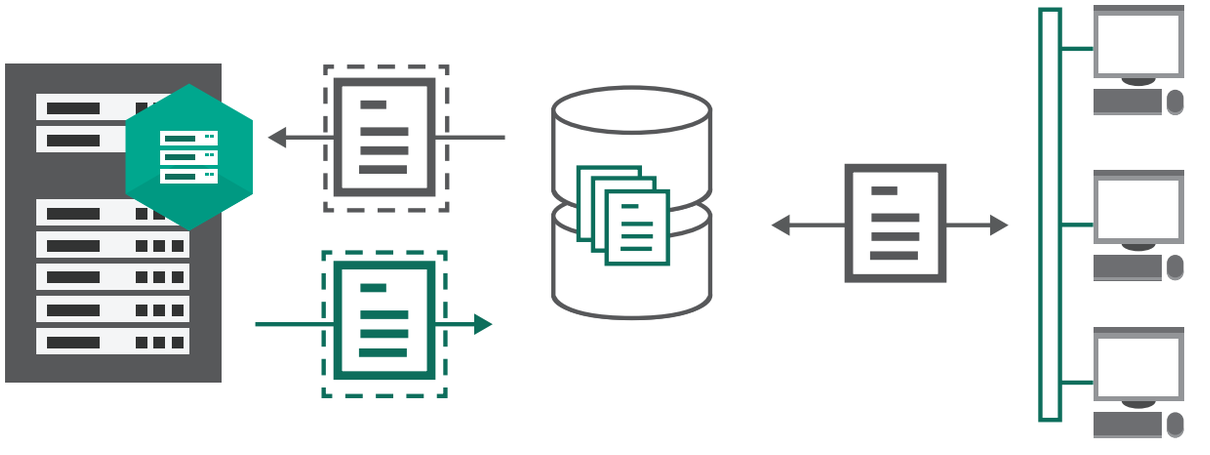
KASPERSKY SECURITY FOR STORAGE

SÉCURITÉ POUR LES DERNIERS SERVEURS NAS

Kaspersky Security for Storage protège efficacement les serveurs NAS (Network Attached Storage) des marques EMC, NetApp, Dell, Hitachi, Oracle et IBM, ainsi que d'autres NAS compatibles ICAP ou RPC :

- Architecture unifiée, tolérant les pannes
- Impact minimal sur les performances NAS
- Sécurité évolutive des environnements de stockage
- Mises à jour automatiques des bases de données de programmes malveillants
- Sauvegarde des objets suspects
- Analyse programmée ou à la demande

Architecture Kaspersky Security for Storage



Serveur Antivirus avec Kaspersky Security for Storage

Stockage EMC VNX et/ou NetAppp

Utilisateurs (Entreprise)

Protection contre la fraude en ligne et sur mobile

KASPERSKY FRAUD PREVENTION

SOLUTION DESTINÉE AUX BANQUES

Kaspersky Fraud Prevention renforce le système de sécurité existant des banques, ce qui permet d'offrir un nouveau niveau de protection contre la fraude. La solution protège les comptes numériques, les ordinateurs et les appareils mobiles des utilisateurs, ainsi que les systèmes de la banque. En protégeant les transactions et les comptes des clients, Kaspersky Fraud Prevention aide les banques à renforcer la fidélité de leur clientèle.

Kaspersky Fraud Prevention prévient activement :

- le piratage de compte
- la falsification de transaction
- le vol d'identité

Kaspersky Fraud Prevention :

- protège 100 % de vos clients, indépendamment de l'appareil ou de la plateforme qu'ils utilisent.
- permet à votre banque de détecter le plus tôt possible l'accès aux comptes par des clients infectés.
- permet de protéger les utilisateurs accédant à leurs comptes bancaires depuis un appareil mobile (Android, iOS et Windows Phone).
- fonctionne sur les PC et Mac de vos clients et leur offre une protection efficace, à la source, contre les programmes malveillants et les attaques sur Internet.
- protège les comptes bancaires numériques contre les tentatives de prise de contrôle de compte.

Protection contre les attaques DDoS

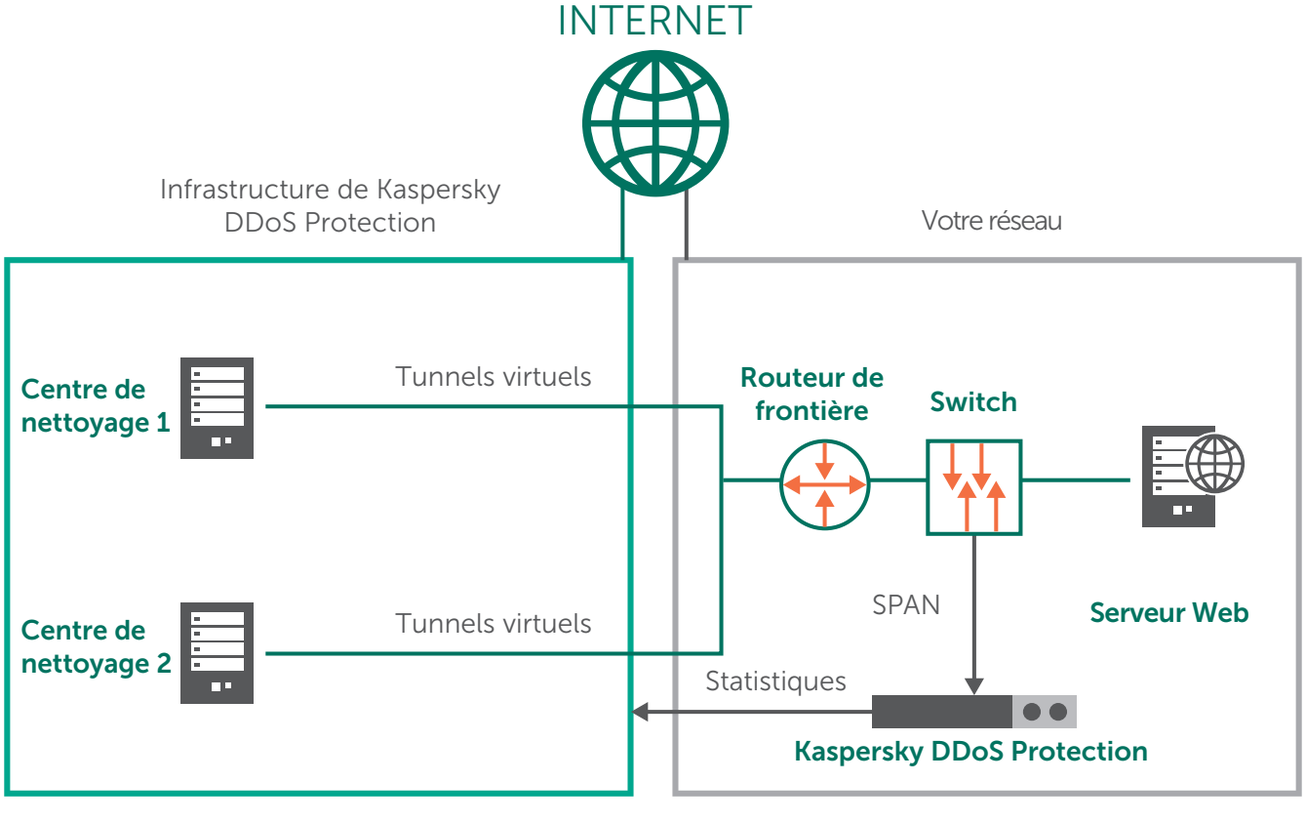
KASPERSKY DDOS PROTECTION

Pour protéger votre entreprise contre les attaques DDoS, vous devez disposer d'une solution qui détecte les attaques le plus rapidement possible. Nos équipes de surveillance des menaces utilisent des méthodes sophistiquées pour étudier le paysage des attaques DDoS et conserver une longueur d'avance sur les pirates.

Kaspersky DDoS protection offre :

- un logiciel de sonde spécifique, fonctionnant au sein de l'infrastructure du client
- des centres de nettoyage du trafic
- des alertes sur les attaques potentielles
- un trafic sécurisé : le centre de nettoyage ne filtre le trafic que pendant une attaque
- une analyse et des rapports détaillés après l'attaque sur le lieu et la manière dont celle-ci s'est déroulée

Architecture de Kaspersky Ddos Protection



Technologie de chiffrement

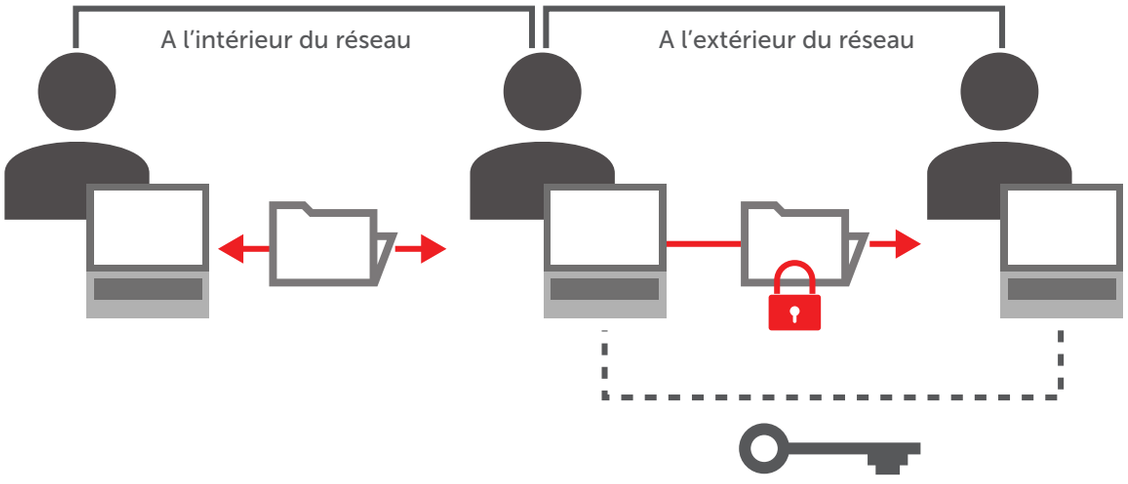
La technologie de chiffrement de Kaspersky Lab empêche l'accès non autorisé à vos données en cas de perte ou de vol d'un appareil ou d'une attaque malveillante ciblant vos données.

Flexibilité totale dans le choix des éléments à chiffrer :

- Chiffrement intégral de disque (FDE)
- Chiffrement au niveau des fichiers/dossiers (FLE)
- Périphériques amovibles (clés USB, disques durs externes)

La technologie de chiffrement de Kaspersky Lab travaille de manière transparente sur l'ensemble des applications, sans compromettre la productivité de l'utilisateur final. L'authentification unique permet un chiffrement en toute transparence, l'utilisateur final n'ayant peut-être même pas conscience que la technologie fait son travail.

Principe de chiffrement



Le chiffrement des données est inclus dans KESB Advanced et Total.

Services de veille stratégiques

SURVEILLANCE DES MENACES

Votre système SIEM dispose-t-il des capacités nécessaires de détection des cybermenaces ? Pouvez-vous avoir l'assurance d'être averti à temps des menaces les plus dangereuses ? Notre portefeuille de services de surveillance des menaces est conçu pour donner aux entreprises les outils nécessaires pour gérer ces risques :

- **Flux d'informations sur les menaces** : optimisez votre solution SIEM et approfondissez vos compétences en matière de criminalité grâce à nos tout derniers flux d'informations sur les cybermenaces. Nos solutions s'intègrent aux principaux SIEM du marché (QRadar, Splunk, ArcSight, etc.)
- **Les rapports de surveillance des menaces APT** permettent d'obtenir un accès exclusif et proactif aux descriptions des campagnes de cyberespionnage les plus sophistiquées, et notamment aux indicateurs de compromission (IOC).
- **Les rapports de veille sur les menaces spécifiques au client** identifient toutes les composantes essentielles de votre réseau disponibles à l'extérieur.

SERVICES D'EXPERTS

Votre expertise interne est-elle suffisante pour résoudre un cyberincident ? Votre infrastructure informatique ou vos applications spécifiques sont-elles entièrement sécurisées face aux cyberattaques potentielles ? Nos services d'experts sont conçus pour atténuer et résoudre ces risques :

- **Tests de pénétration** : apprenez à identifier les points les plus faibles de votre infrastructure et à éviter les dommages provoqués par les cyberattaques. Respectez ainsi les normes du gouvernement, de l'industrie et de l'entreprise (par ex. PCI DSS).
- **Évaluation de la sécurité des applications** : ce service permet d'identifier les vulnérabilités des applications, des solutions reposant sur le Cloud, des systèmes ERP, des services bancaires en ligne et autres applications professionnelles spécialisées aux applications mobiles et embarquées sur différentes plates-formes.
- **Cyberdiagnostic et analyse des programmes malveillants** : ce service retrace de façon détaillée l'historique de tout incident à partir de rapports complets, comprenant notamment les différentes étapes de résolution de l'incident.

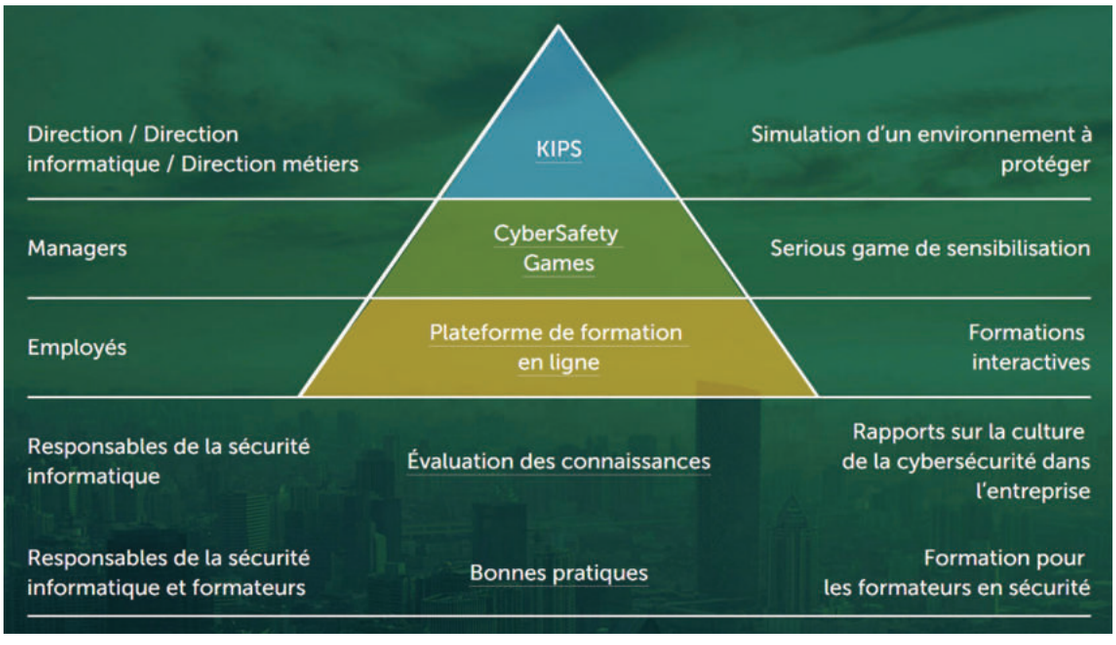
Formations

FORMATIONS À LA CYBERSÉCURITÉ

Nous proposons un portefeuille de formations de sensibilisation à la cybersécurité, ainsi qu'un large choix de programmes de formation, du niveau de base au niveau expert en cybercriminalité et en analyse de programmes malveillants.

- **Sensibilisation des utilisateurs finaux à la cybersécurité** : elle aide les entreprises à renforcer les connaissances de leurs employés en matière de sécurité.
- **Formation pour les professionnels de la sécurité informatique** : couvrant tous les niveaux, elle améliore les compétences des experts en sécurité de votre entreprise et réduit les risques d'incidents.

Nos programmes de formation et de sensibilisation s'adressent à tous les niveaux de l'entreprise.



Protection des Data Centers

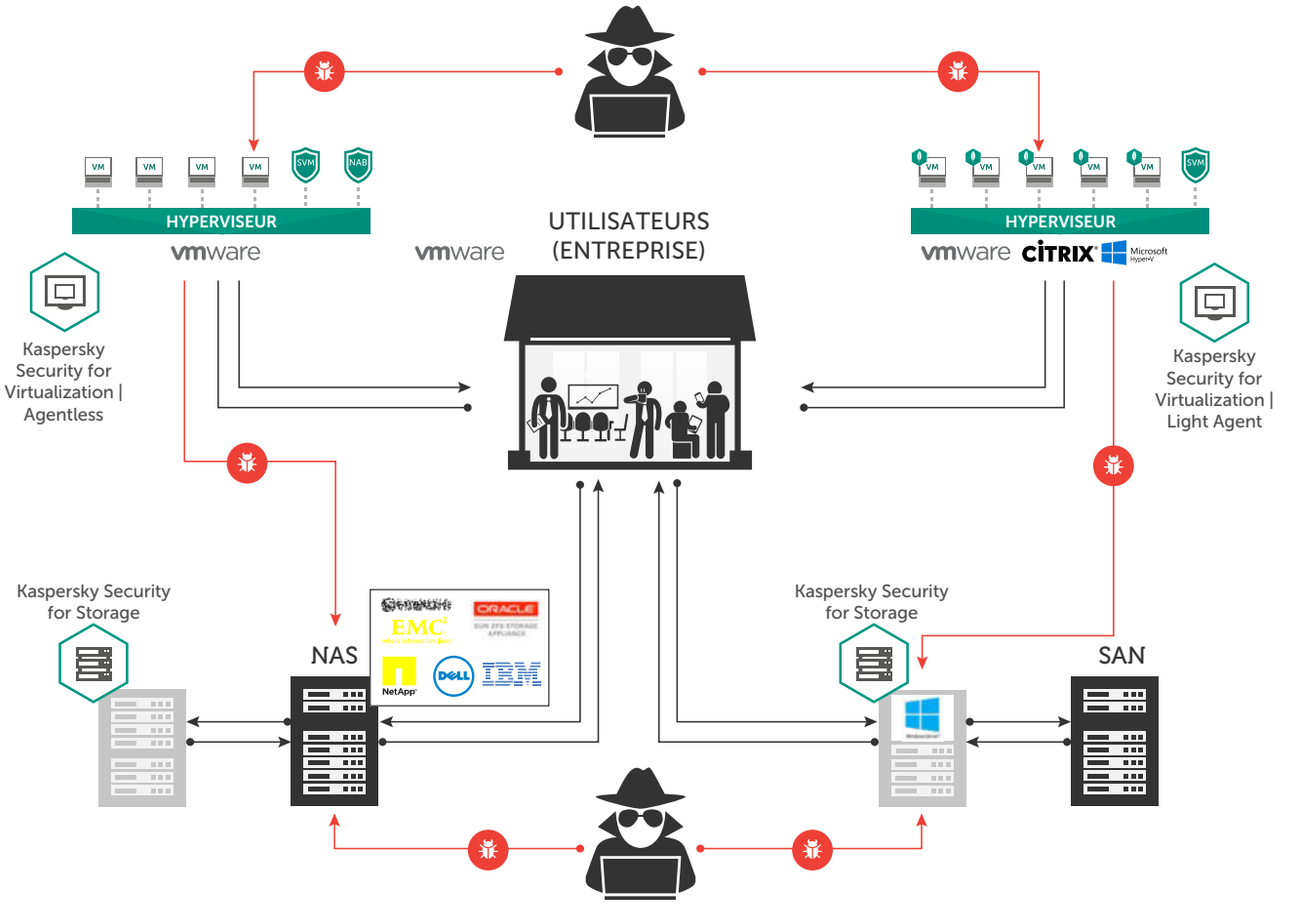
Protection des Data Centers en combinant 2 solutions Kaspersky Lab :

- SECURITY FOR VIRTUALIZATION

- SECURITY FOR STORAGE

Nous proposons des solutions centrées sur la protection de deux secteurs essentiels de votre data center : l'infrastructure virtuelle et les systèmes de stockage de données. Convenant idéalement aux environnements à plusieurs hyperviseurs et systèmes de stockage, ces solutions Kaspersky Lab comprennent :

- des mesures de sécurité conçues spécifiquement pour les plates-formes principales de virtualisation, dont VMware, Citrix, Microsoft et KVM.
- des mesures de sécurité destinées aux systèmes de stockage en réseau (NAS), notamment EMC, NetApp, DELL, IBM, Hitachi et Oracle.

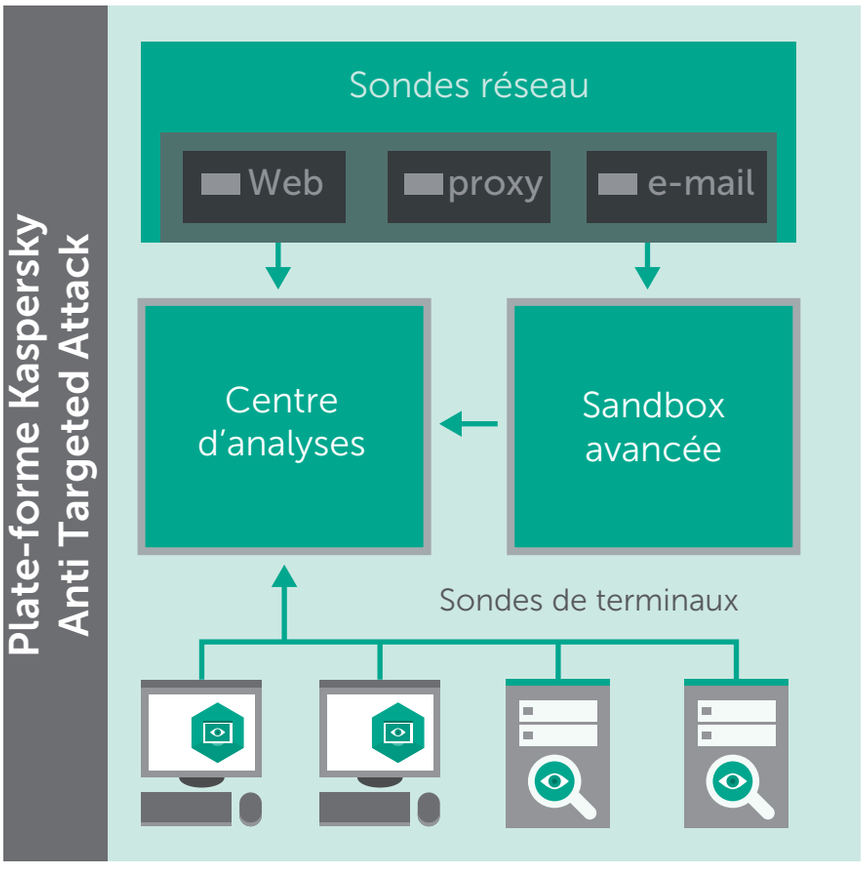


Protection contre les attaques ciblées – APT

KASPERSKY ANTI TARGETED ATTACK

Kaspersky Anti Targeted Attack est une plate-forme utilisant à la fois les données recueillies par notre service de veille stratégique mondiale, et de puissantes technologies de détection et d'analyse :

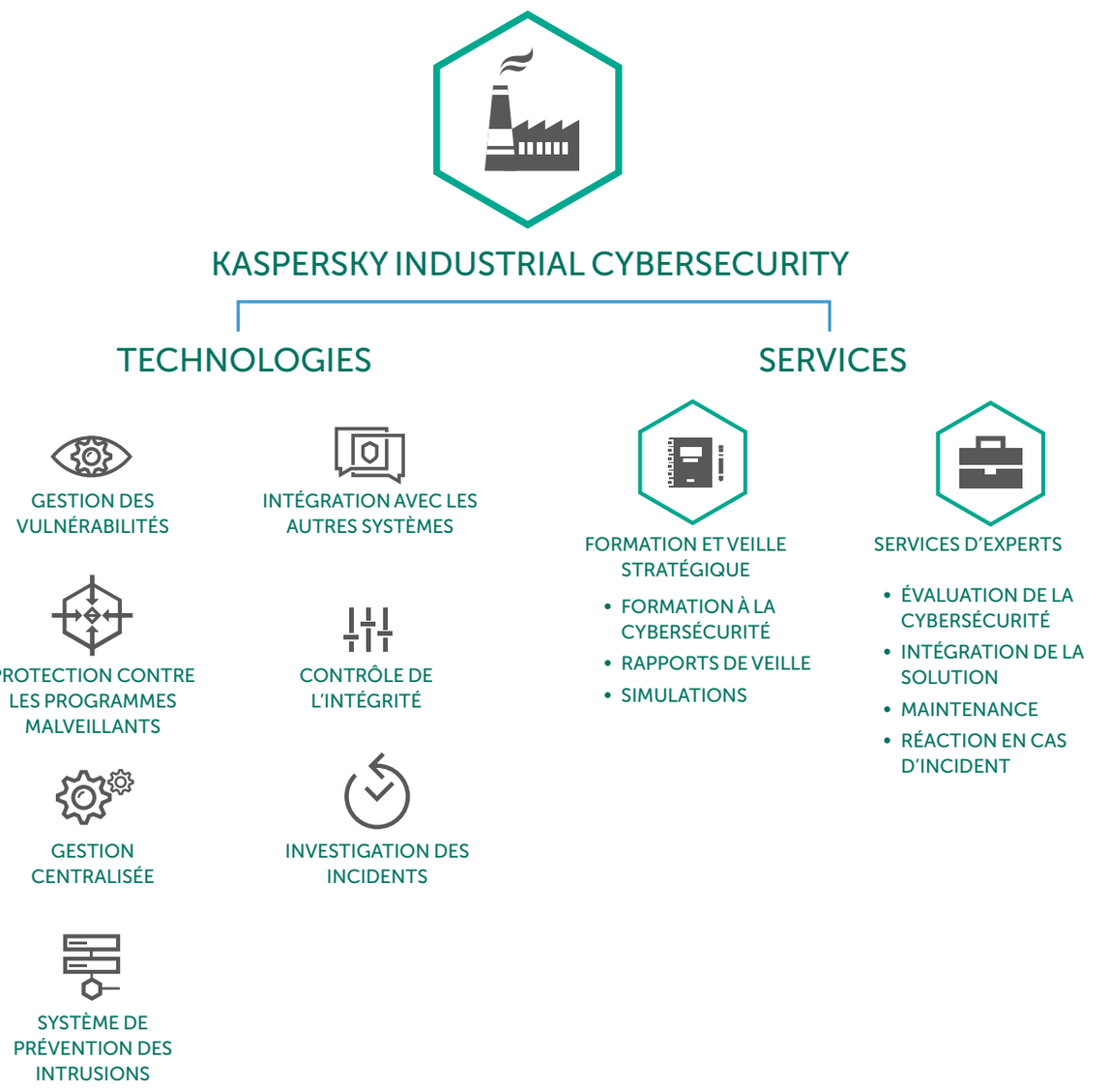
- **une architecture de sondes multi-niveaux**, pour une visibilité à 360 degrés : une combinaison de sondes réseau, Web et de messagerie électronique, ainsi que de sondes de terminaux.
- **une sandbox avancée**, pour évaluer les nouvelles menaces. Elle propose un environnement isolé et virtualisé où les objets suspects peuvent être exécutés en toute sécurité, afin d'en observer le comportement.
- **des moteurs d'analyse puissants**, pour des diagnostics rapides et moins de faux positifs. Notre analyseur d'attaques ciblées évalue les données du réseau et des terminaux saisies par les sondes, puis génère rapidement des diagnostics de détection des menaces destinés à votre équipe de sécurité.



Protection des environnements industriels critiques

KASPERSKY INDUSTRIAL CYBERSECURITY

Kaspersky Industrial CyberSecurity est spécialement conçu pour tenir compte des besoins uniques de l'industrie et se focalise notamment sur la préservation de la continuité des processus technologiques. Les paramètres polyvalents et flexibles de la solution permettent de configurer cette dernière pour répondre aux exigences et besoins uniques de chaque installation industrielle.



Protection des DAB et des terminaux de points de vente

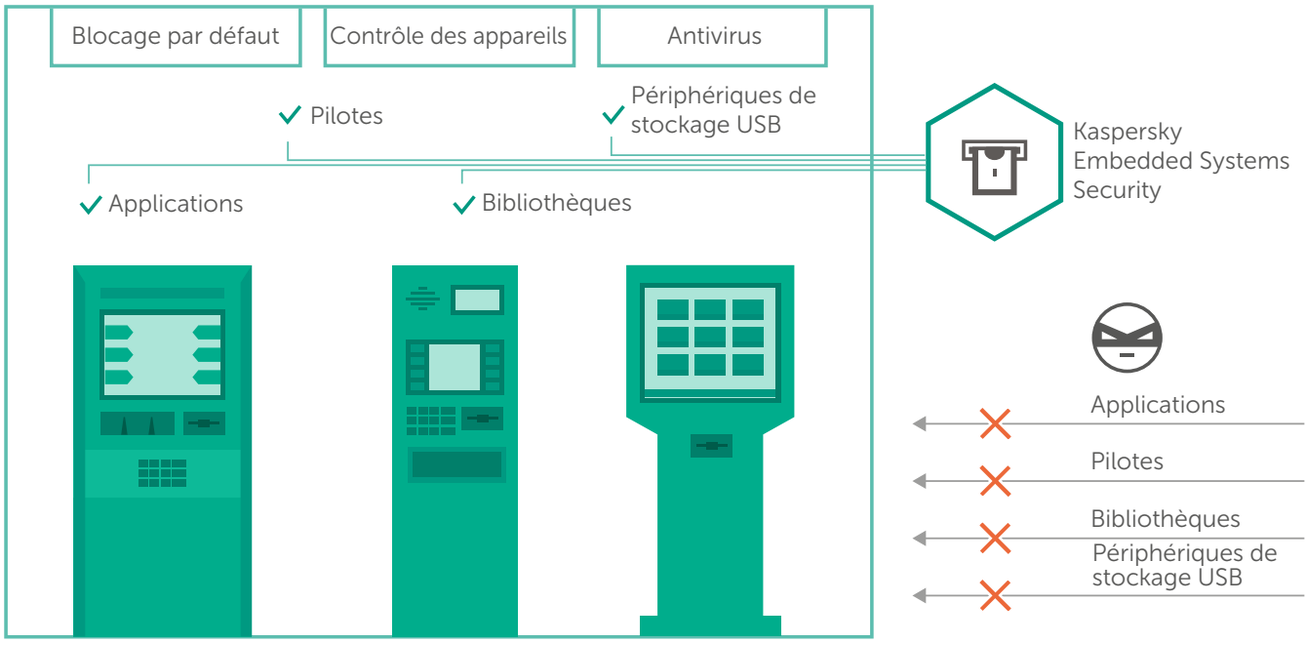
KASPERSKY EMBEDDED SYSTEMS SECURITY

Kaspersky Lab a conçu une solution de sécurité spécifiquement destinée aux entreprises gérant des distributeurs automatiques de billets et des terminaux de points de vente.

Kaspersky Embedded Systems Security propose notamment un mode « blocage par défaut uniquement », où la configuration requise débute à 256 Mo de RAM et 50 Mo d'espace disque disponible, avec le système d'exploitation Windows XP et du matériel de faible puissance.

Cette solution unique répond à trois objectifs clés :

- une sécurité efficace pour les systèmes « difficiles à gérer »
- la conformité avec les exigences PCI DSS 5.1, 5.1.1, 5.2, 5.3 et 6.2
- un étalement chronologique en douceur pour le remplacement des systèmes et des équipements obsolètes



La protection Cloud Kaspersky Lab

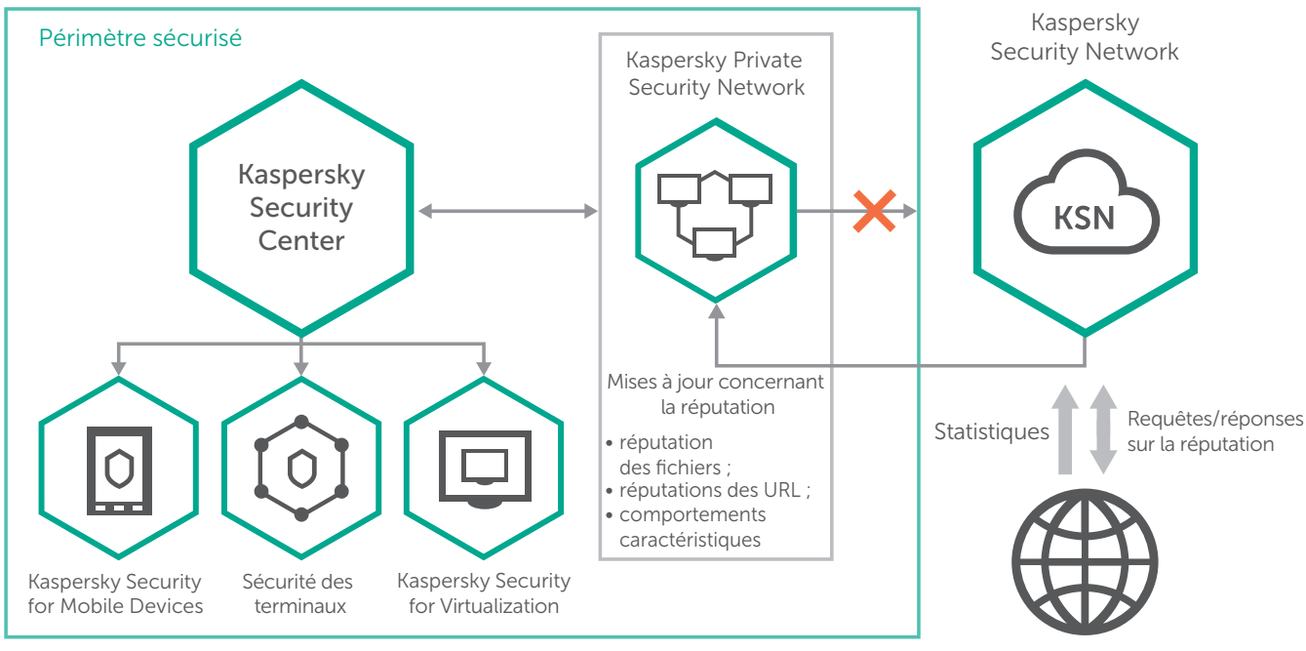
KASPERSKY SECURITY NETWORK

Les solutions de sécurité standard ont besoin de 4 heures pour recevoir les informations nécessaires à la détection et à l'interception des quelque 310 000 nouveaux programmes malveillants découverts chaque jour par les chercheurs de Kaspersky Lab. Le service de partage des informations sur les menaces via le réseau Kaspersky Security Network fournit ces données en 30 à 40 secondes.

KASPERSKY PRIVATE SECURITY NETWORK

Kaspersky Private Security Network apporte une réponse aux principaux problèmes de cybersécurité des entreprises sans qu'une seule donnée ne quitte le réseau local.

- identifie les sources des programmes malveillants et évite leur propagation
- identifie et différencie les attaques ciblées des menaces d'ordre plus général
- limite les dommages causés par les incidents de cybersécurité
- évalue la recherche d'incidents et les besoins en matière de mesures correctives
- réduit les faux positifs
- respecte les normes strictes en matière de confidentialité, de sécurité et de réglementation



Contrats de maintenance et support

MAINTENANCE SERVICE AGREEMENT (MSA)

Une assistance de qualité en cas d'incident, de problèmes de configuration, d'incompatibilité et autre est essentielle pour les entreprises qui recherchent la tranquillité d'esprit et une disponibilité optimale.

En cas de besoin, les spécialistes Kaspersky Lab seront disponibles via des lignes téléphoniques prioritaires dédiées, en français, dans des délais d'intervention adaptés aux besoins de votre entreprise. Le schéma ci-dessous décrit les options d'assistance disponibles.

	Assistance standard		Assistance supérieure	
	MSA Starter	**MSA Plus**	**MSA Business**	**MSA Enterprise**
Ligne téléphonique prioritaire	Oui	Oui	Oui	Oui
Responsable technique du compte	Non	Non	Oui	Oui, dédié
Assistance en langue locale	8 x 5	8 x 5	8 x 5	24 x 7 x 365
Assistance, niveau de gravité 1	8 x 5	8 x 5	24 x 7 x 365	24 x 7 x 365
Délai d'intervention, niveau de gravité 1	8 heures de travail	6 heures de travail	4 heures	30 minutes
Assistance, niveau de gravité 2	8 x 5	8 x 5	8 x 5	24 x 7 x 365
Services professionnels Consultation	Non	Non	Coût additionnel	Bilan technique et rapports personnalisés
Nombre d'incidents	6	12	36	Illimité

SERVICES PROFESSIONNELS

- **Service découverte** : vous garantit une utilisation optimale de nos produits en fonction des besoins spécifiques de votre entreprise.
- **Service de mise à niveau** : assistance technique supplémentaire au cours d'un projet de mise à niveau d'un produit Kaspersky Lab.
- **Service de configuration** : recommandations en termes de paramètres de configuration et de politiques.
- **Service de bilan technique** : audit de l'environnement du réseau et des paramètres des produits du client (sur place ou à distance) et réalisation, par nos experts, d'un rapport complet contenant des recommandations pour optimiser la sécurité de l'entreprise.
- **Service de conseil** : service personnalisé (incluant bonnes pratiques, conseils, formations et apprentissages ciblés) veille à l'efficacité de votre réaction face au changement sans interrompre les activités de votre entreprise. Un service complet de dépannage est inclus.


Twitter.com/
kasperskyfrance


Facebook.com/
kasperskylabfrance


Youtube.com/
/user/KasperskyFrance

Kaspersky Lab France,
Rueil Malmaison
www.kaspersky.fr

Tout savoir sur la
sécurité sur Internet :
www.securelist.com

Trouver un partenaire près
de chez vous :
www.kaspersky.fr/partners

KASPERSKY lab

commercial@sistek.pro