Sophos Email

SOPHOS
Cybersecurity delivered.

Présentation du produit et des licences

	Licences	Description des fonctionnalités	Sophos Email Standard	Sophos Email Advanced
	Fournisseurs de service de messagerie compatibles	Compatible avec tous les services de messagerie, dont Google Workspace Gmail et Microsoft 365 : • Microsoft Exchange Online et Microsoft 365 • Microsoft Exchange 2003 ou supérieur • Google Workspace Gmail La prise en charge ne se limite pas à ces plateformes. Une simple configuration MX est nécessaire et Sophos Email est compatible avec n'importe quel service dont vous possédez le domaine et contrôlez les enregistrements DNS associés.	✓	✓
	Intégration des règles de flux de messagerie Microsoft 365	La connexion aux règles Sophos Mailflow crée une connexion directe avec Microsoft 365 depuis la console Sophos Central, sans qu'il soit nécessaire de rediriger les enregistrements MX. Cela accélère le temps de traitement des emails, tout en offrant la même protection avancée. Disponible pour les clients Sophos Email Advanced utilisant Microsoft 365.		✓
	Synchronisation avec Active Directory et Azure Active Directory	Microsoft Active Directory Sync (AD Sync) et Azure AD Sync offrent une manière simple de migrer les environnements sur site Active Directory ou Exchange vers le Cloud. • Synchronisez automatiquement vos utilisateurs avec Sophos Email à l'aide de AD Sync. • Les entreprises ayant intégralement migré dans le Cloud bénéficient de l'entière prise en charge des mises à jour automatiques des données issues de AD.	✓	✓
	Saisissez manuellement les alias	Accès de l'administrateur pour ajouter manuellement des enregistrements d'alias d'adresses électroniques lorsque Active Directory n'est pas disponible.	✓	✓
	Portail libre-service pour les utilisateurs	Sophos Email offre aux utilisateurs un accès aux outils suivants : • Gestion des emails mis en quarantaine (accepter/supprimer les emails) • Modification des règles des listes d'autorisation/blocage • En cas de panne, accès aux emails depuis la boîte de réception d'urgence	✓	✓
	Politiques Domaine/ Groupe/Utilisateur	Créez en quelques minutes des politiques de sécurité uniques pour des individus particuliers, des groupes ou tout un domaine.	✓	✓
	Emplacement du datacenter	Restez conforme aux réglementations sur la protection des données et améliorez l'expérience des utilisateurs, avec un choix de trois datacenters : • Royaume-Uni • États-Unis • Allemagne	✓	✓
CONTINUITÉ DES ACTIVITÉS	Mise en attente, pour ne subir aucune perte d'emails*	En cas de perturbation dans les services de Microsoft ou de Google, les emails du destinataire sont automatiquement mis en attente avec Sophos Email, puis livrés une fois le service restauré (5 jours de réessai inclus).	✓	✓
	Accès 24 h/24 des utilisateurs à une boîte de réception d'urgence*	L'accès en lecture seule aux emails mis en attente est fourni à partir d'une boîte de réception d'urgence disponible 24 h/24 et 7 j/7 sur le portail de l'utilisateur.	✓	✓
	Alertes de l'administrateur*	Si un service tiers de messagerie dans le Cloud tombe en panne, des alertes avertissent que les emails ne peuvent plus être livrés vers un serveur/service.	✓	✓
PROTECTION CONTRE LES MENACES	Mises à jour en temps réel pour bloquer les dernières attaques	Alimenté par les SophosLabs, Sophos Email offre des mises à jour en temps réel qui protègent contre les dernières menaces.	✓	✓
	Détection anti-spam, anti-virus et anti-phishing	Filtrage des emails entrants et sortants pour bloquer les emails indésirables : • Le filtrage par réputation bloque 90 % du spam • Le moteur antispam identifie le pourcentage restant, y compris les attaques de phishing les plus récentes. • Le « Sender Genotype », notre technologie Next-Gen de filtrage par réputation, élimine le spam de botnets au niveau de la connexion IP en surveillant les requêtes de connexion et en rejetant celles montrant des connexions évidentes à des botnets. Sophos Delay Queue assure la protection contre le spam Snowshoe.	✓	✓
	Quarantaine des emails	Les contrôles prédéfinis de Sophos Email, très simples à utiliser, permettent de configurer les politiques de quarantaine et de protéger votre entreprise en quelques secondes. Les utilisateurs reçoivent un résumé des emails mis en quarantaine dans la journée, et peuvent les récupérer eux-mêmes directement depuis leur boîte de réception.	✓	✓

	Licences	Description des fonctionnalités	Sophos Email Standard	Sophos Email Advanced
PROTECTION CONTRE LES MENACES	Liste d'autorisation/ blocage	La politique d'autorisation ou de blocage des expéditeurs permet aux administrateurs de restreindre les emails à destination ou en provenance d'adresses électroniques, d'adresses IP et de domaines spécifiques, y compris la prise en charge des caractères génériques, ce qui vous permet de bloquer les TLD (domaine de premier niveau) au niveau du pays. Les bannières intelligentes permettent aux utilisateurs de mettre à jour leurs listes personnelles d'expéditeurs autorisés et bloqués à partir de l'email lui-même, tandis que le portail libre-service permet de gérer ces listes.	✓	✓
	Authentification SPF, DKIM et DMARC entrant	• SPF (Sender Policy Framework) pour identifier les adresses IP autorisées à envoyer des emails depuis le domaine • DKIM (Domain Keys Identified Mail) fournit la preuve cryptographique qu'un email a bien été envoyé par un expéditeur spécifique et n'a pas été compromis. • DMARC (Domain Message Authentication Reporting & Conformance) détermine ce qu'il faut faire lorsque des messages échouent les contrôles SPF et DKIM de l'expéditeur.	✓	✓
	Contrôles des anomalies de l'entête	• La détection des anomalies de l'entête identifie si le nom de l'expéditeur affiché correspond au nom d'un utilisateur interne.	✓	✓
	Protection post-livraison de Microsoft 365	La protection post-livraison continue pour Microsoft 365 supprime automatique les emails de phishing contenant des URL nouvellement infectées dès que l'état de la menace change.		✓
	Protection contre l'usurpation d'identité par phishing	• Comparez le nom d'affichage des emails entrants avec le nom d'affichage des fournisseurs de services Cloud les plus souvent utilisés dans ce type d'attaque, et avec les personnes haut placées (ou VIP) de l'entreprise. • Analyse des domaines similaires pour identifier les noms de domaine semblables au domaine de l'entreprise • Les emails suspects peuvent être bloqués, mis en quarantaine, signalés par un avertissement dans la ligne d'objet ou être parés d'une bannière avec un lien direct vers la liste de blocage au niveau de l'utilisateur.		✓
	Protection Time-of-Click des URL	La protection contre la réécriture des URL vérifie la réputation du site web avant la réception de l'email puis au moment où vous cliquez sur le lien, bloquant ainsi les attaques furtives et à retardement.		✓
	Sandboxing de Sophos	Technologie de sandboxing basé dans le Cloud capable de détecter les malwares à la fois connus et inconnus et les applications indésirables avant qu'elles ne s'exécutent.		✓
PROTECTION DES DONNÉES	Chiffrement des emails (TLS, S/MIME, en mode push)	Scanne automatiquement le corps de l'email et les pièces jointes pour identifier les données sensibles, vous permettant de créer aisément des politiques de sécurité pour bloquer ou chiffrer les emails en quelques clics seulement. Vous pouvez aussi donner aux utilisateurs la possibilité de chiffrer eux-mêmes leurs emails grâce à notre module complémentaire dans M365. • Le chiffrement en mode push protège l'email entier ou uniquement les pièces jointes • L'application du chiffrement TLS empêche l'espionnage de l'email en transit • Ajoutez une signature numérique pour vérifier l'identité de l'expéditeur avec S/MIME		✓
	Chiffrement des emails (en mode pull)	Disponible avec Sophos Email Advanced, le chiffrement intégral du portail web en option permet aux utilisateurs de gérer, lire et répondre aux emails chiffrés dans un portail web sécurisé.		**Module complémentaire**
	Protection contre la perte de données (DLP)	La protection contre la perte de données et le contrôle du contenu empêchent les fuites de données grâce au chiffrement des emails basé sur des politiques. Créez des politiques DLP à règles multiples pour les groupes et les utilisateurs individuels afin de garantir la protection des données sensibles contenues dans les emails et les pièces jointes à l'aide de fonctions d'identification des données financières, confidentielles, médicales et personnelles.		✓

*Fonctionnalité non disponible avec l'intégration des règles de flux de messagerie Microsoft 365.

22-02-19 LG-FR (PS)

SOPHOS