

# Sophos Email Security



Faites à nouveau confiance à votre boîte de réception grâce à la sécurité des messageries dans le Cloud qui protège vos employés et vos données critiques contre les logiciels malveillants, les tentatives de phishing et les usurpations d'identité.

## Bloquez les emails de phishing et les impostures

De nombreuses cyberattaques commencent par un email de phishing. Le danger ne réside pas dans l'email lui-même, mais plutôt dans ce qu'il incite les gens à faire, comme ceux contenant des liens malveillants ou des malwares que les attaquants essaient de vous inciter à activer.

Pour bloquer les imposteurs, Sophos Email identifie automatiquement les cibles de premier plan dans votre organisation dont l'identité pourrait être usurpée ou risquant de subir une attaque BEC (Business Email Compromise). La solution bloque ensuite l'attaque grâce à l'analyse par Machine Learning du contenu de l'email, à l'authentification de l'expéditeur, à la protection des URL et à la technologie de sandboxing dans le Cloud.

## Empêchez les malwares d'arriver dans les boîtes de réception

La protection multicouche s'appuie sur plus de 35 ans de collecte de renseignements sur les menaces, d'analyse de la réputation et du comportement, et du Machine Learning de pointe pour empêcher les logiciels et URL malveillants d'atteindre les boîtes de réception.

La technologie de sandboxing dans le Cloud de Sophos analyse tous les processus de fichiers, l'activité de ces derniers, l'activité du registre et les connexions réseau pour bloquer les ransomwares, les autres formes de malwares, les exploits et les PUA. L'intelligence artificielle du Deep Learning est utilisée pour stopper net les menaces de type Zero-Day.

## Une plus grande tranquillité d'esprit grâce à la sécurité des données

Sophos Email analyse automatiquement les emails et les pièces jointes pour identifier les données sensibles, en intégrant le chiffrement de manière transparente.

Empêchez la fuite des données à l'aide de politiques DLP à règles multiples pour les groupes et les utilisateurs individuels. Sophos Email assure la protection des informations sensibles contenues dans les emails et les pièces jointes à l'aide de fonctions d'identification des données financières, confidentielles, médicales et personnelles.

Chiffrez les emails et ajoutez une signature numérique pour vérifier l'identité de l'expéditeur avec la norme S/MIME, ou choisissez parmi les options de chiffrement personnalisables, notamment le chiffrement TLS, le chiffrement des pièces jointes (PDF et Office) ou le chiffrement du portail web complet (disponible sous forme de module d'extension).

## Avantages principaux

- Intégration avec les fournisseurs de messagerie professionnelle : Microsoft 365, Google Workspace Gmail, etc.
- Sécurité des messageries basée sur une API pour Microsoft 365 avec protection post-livraison
- Bloquez les spams, malwares, ransomwares et URL malveillantes
- Bloquez les tentatives de phishing et d'usurpation d'identité sans malware
- Protégez les données sensibles grâce au chiffrement des emails et à la protection contre la perte de données (DLP)
- Aussi disponible sur AWS Marketplace

## Sécurité de Microsoft 365

Sophos Email s'intègre à la messagerie Microsoft 365 (M365) en quelques minutes. La sécurité des messageries basée sur une API assure une configuration et un traitement des emails plus rapides.

- La connexion aux règles de flux de messagerie Sophos Mailflow s'effectue en quelques minutes depuis la console Sophos Central, sans qu'il soit nécessaire de rediriger les enregistrements MX.
- La protection post-livraison supprime automatiquement les emails de phishing contenant des URL nouvellement infectées dès que l'état de la menace change.
- L'intégration directe au flux de messages permet un traitement plus rapide de tous les emails, tout en offrant la même protection avancée.

## Centralisez les renseignements sur les menaces pour une réponse plus rapide

Optimisez vos investissements en matière de sécurité et identifiez des indicateurs de compromission jusqu'alors invisibles dans vos environnements grâce aux renseignements sur les menaces provenant des protections Sophos Endpoint et Email partagés dans le Data Lake de Sophos XDR. Étendez la visibilité à la suite Microsoft 365, aux charges de travail des serveurs, aux appareils mobiles, au réseau et bien plus encore.

## Fonctionnalités principales de Sophos Email

Consultez toutes les fonctionnalités sur [sophos.fr/email](https://sophos.fr/email)

| Fonctionnalités de protection                           | Email Advanced | Fonctionnalités de protection    | Email Advanced        |
|---------------------------------------------------------|----------------|----------------------------------|-----------------------|
| Règles de flux de messagerie Microsoft 365              | ✓              | Analyse du nom d'affichage       | ✓                     |
| Protection post-livraison de Microsoft 365              | ✓              | Vérification des domaines sosies | ✓                     |
| Analyse anti-spam et anti-malware                       | ✓              | Politiques DLP multi-règles      | ✓                     |
| Sandboxing dans le Cloud                                | ✓              | Listes de contrôle de contenu    | ✓                     |
| Détection des URL malveillantes                         | ✓              | Application du chiffrement TLS   | ✓                     |
| Protection Time-of-Click contre la réécriture des URL   | ✓              | S/MIME                           | ✓                     |
| SPF, DKIM, DMARC                                        | ✓              | Chiffrement en mode push         | ✓                     |
| Protection contre le phishing par usurpation d'identité | ✓              | Chiffrement en mode pull         | Module complémentaire |

## Reporting complet

Sophos augmente la visibilité grâce à des tableaux de bord clairs, des résumés de la messagerie et des rapports détaillés sur les menaces.

- Historique des messages (affiche les journaux de tous les emails traités par le système)
- Résumé de la messagerie (résumé de tous les emails)
- Résumé des menaces traitées par la technologie de sandboxing (rapports de verdict, y compris les résultats de VirusTotal et les tactiques de la matrice MITRE ATT&CK)
- Résumé d'activité Time of Click (volume d'URLs bloquées, avec avertissement et autorisées)
- Violations de la stratégie DLP (emails loggés par les politiques DLP)
- Résumé de la post-livraison (résumé des emails M365 supprimés après réception dans la boîte mail)
- Résumé sur l'utilisation de la licence

## Augmentez l'efficacité de votre équipe

Gagnez un temps précieux à l'aide de la console de gestion Cloud unique de Sophos. Des millions de personnes font confiance à Sophos pour améliorer leur efficacité en matière de cybersécurité grâce à une configuration, un déploiement et une gestion simplifiés de la protection des messageries, des systèmes endpoint, des charges de travail des serveurs, de la sécurité des appareils mobiles, des pare-feux, du Zero Trust, de la sécurité du Cloud public et bien plus encore — le tout à partir d'une seule interface.

Pour en savoir plus ou contacter un expert : [sophos.fr/email](https://sophos.fr/email)