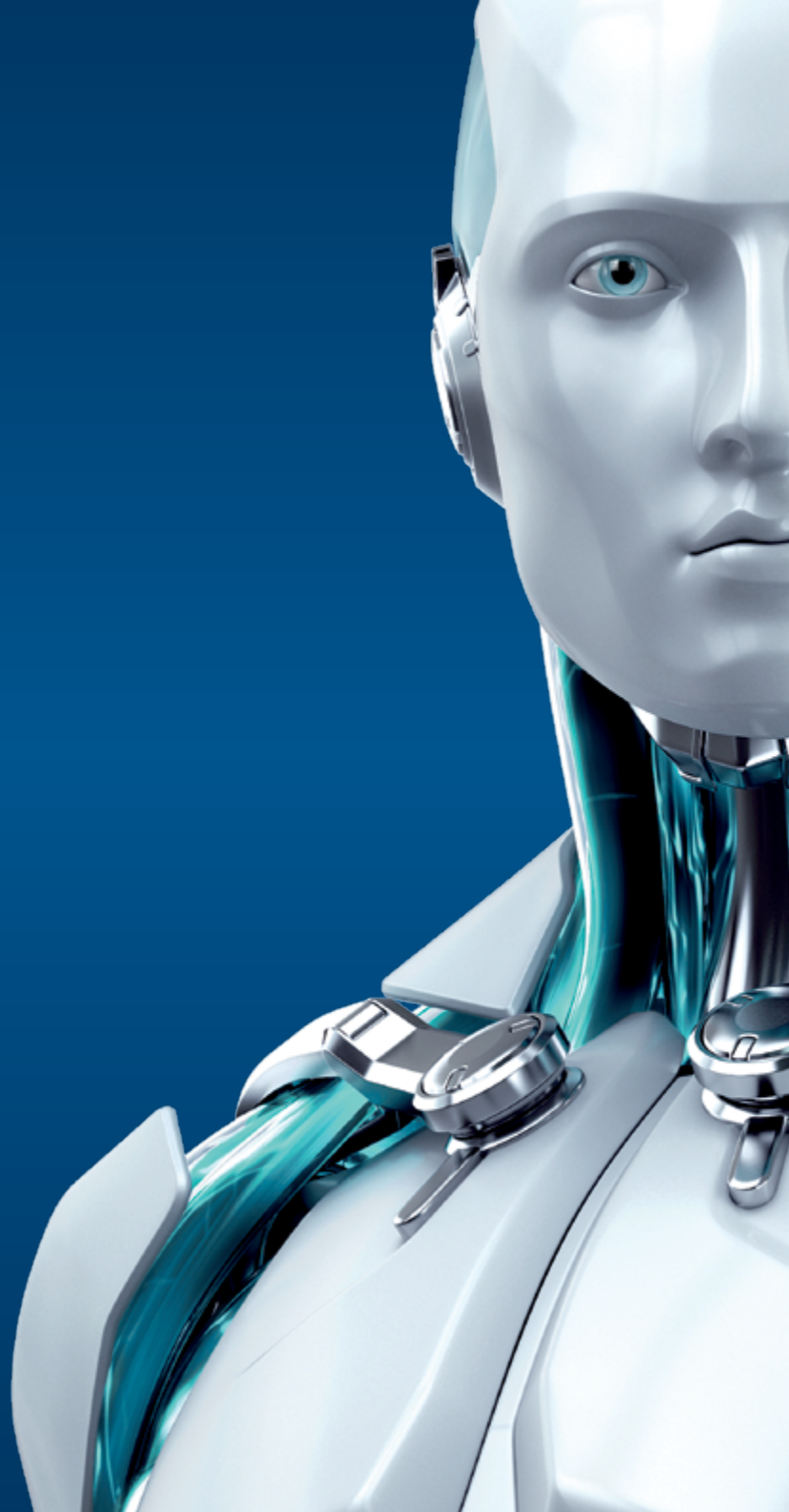
MAIL SECURITY

POUR MICROSOFT EXCHANGE SERVER

ENJOY SAFER TECHNOLOGY™



MAIL SECURITY

POUR MICROSOFT EXCHANGE SERVER

ESET MAIL SECURITY POUR MICROSOFT EXCHANGE ESET

Mail Security pour Microsoft Exchange offre une puissante protection Antivirus et Antispam pour assurer un filtrage efficace des menaces au niveau du serveur.

La solution vous apporte une protection complète du serveur, y compris ses propres fichiers système. Vous avez la possibilité d'appliquer des politiques à des fichiers réels spécifiques, d'assurer une surveillance continue du statut de la sécurité et d'accéder à des paramétrages très fins via la console ESET Remote Administrator.

Protections Anti-malware et Antispam

Antivirus et Antispyware	Elimine tous types de menaces : virus, rootkits, vers et spyware Analyse optionnelle dans le Cloud : Utilise une base de données Cloud, intégrant une liste blanche de fichiers fiables. Permet une détection renforcée et des analyses plus rapides. Seules les informations relatives à des exécutables et fichiers archives sont envoyées vers le Cloud. Ces données sont anonymes.
Antispam et Anti-phishing	Blocage des spams et tentatives de phishing grâce à un taux élevé d'interception même sans la configuration manuelle d'un seuil SCL (Spam Confidence Level). Après l'installation, le module antispam est fonctionnel même sans paramétrage manuel ou seuil.
Gestion locale de la quarantaine	Chaque propriétaire de boîte aux lettres peut gérer directement, via son navigateur, ses spams ou messages considérés comme suspects dont la livraison a été bloquée. Selon les droits définis par l'administrateur, l'utilisateur pourra libérer, rechercher des messages et effectuer des actions sur ces derniers. Les actions proposées varient en fonction de la raison pour laquelle il a été placé en quarantaine. Un rapport régulier des messages en quarantaine et liens pour actions pourra être envoyé à l'utilisateur.
Analyse à la demande de la base de données	L'administrateur peut choisir quelles bases de données, et en particulier, quelles boîte aux lettres sont analysées. Ces analyses peuvent également être limitées en utilisant la modification de l'horodatage de chaque message pour choisir celui qui doit être analysé. Ainsi, vous réduisez au minimum les ressources du serveur consacrées à cette tâche.
Règles de traitement des messages	Cette fonctionnalité vous offre un large éventail de combinaisons pour chaque message. Les paramètres évalués comprennent les champs standards comme le sujet, expéditeur, corps du texte, en-tête mais permettent également un traitement ultérieur conditionnel en fonction des résultats précédents des filtres antispam et de l'analyse antivirus. Les archives corrompues ou protégées par mot de passe sont détectées et les pièces jointes sont examinées en interne pour déterminer le véritable type de fichier et non la supposée extension. Les règles peuvent être modifiées selon les actions souhaitées.
Bloqueur d'Exploit	Renforce la sécurité des navigateurs Internet, lecteurs PDF, clients de messageries ou MS Office. Surveille les comportements et activités suspects, typiques d'exploitations de failles. Protection renforcée contre les attaques ciblées et exploits inconnus – Attaques zero-day.
Analyse mémoire avancée	Protection efficace contre les logiciels malveillants utilisant des leurres pour masquer leur activité. Surveille les processus et la mémoire vive.
Bouclier système (HIPS)	Définit les règles d'accès à la base de registre, processus, applications et fichiers. Assure une protection contre la falsification et détecte les menaces en fonction du comportement du système.
Contrôle des périphériques	Blocage des périphériques non autorisés à se connecter au serveur. Création de règles pour les groupes d'utilisateurs en accord avec les politiques de sécurité de votre entreprise. La fonction « blocage souple », informe l'utilisateur que son périphérique est bloqué tout en lui laissant l'accès, mais en enregistrant ses activités.

Protection des infrastructures complexes

Indépendance des instantanés	Les mises à jour et les modules de programme peuvent être stockés en dehors de l'emplacement par défaut – ainsi ils ne seront pas affectés en cas de retour à un instantané précédent de la machine virtuelle. Les mises à jour et modules n'ont pas besoin d'être téléchargés à chaque retour à un instantané précédent de la machine virtuelle qui peut alors bénéficier de toutes les performances pour une restauration rapide.
Compatibilité native Cluster	Permet de dupliquer automatiquement les paramètres de la solution lorsqu'elle est installée dans un environnement de type cluster. Grâce à un assistant intuitif, reliez plusieurs instances d'ESET Mail Security au sein d'un cluster afin de les gérer comme une seule installation : plus besoin de dupliquer les modifications faites manuellement vers les autres instances.
ESET Shared Local Cache	ESET Shared Local Cache compare les métadonnées des fichiers avec celles qui ont déjà été stockées et place automatique sur liste blanche les fichiers sains. Chaque fois qu'un fichier précédemment non analysé est trouvé, il est automatiquement ajouté au cache. Cela signifie que les fichiers déjà analysés sur une machine virtuelle ne seront pas analysés à plusieurs reprises sur les autres machines présentes dans le même environnement – optimisation des performances. Comme ces communications se font sur la même machine physique, il y a très peu de retard dans l'analyse, ce qui entraîne des économies de ressources considérables.
Compatibilité Windows Management Instrumentation (VMI)	Possibilité de contrôler les fonctionnalités clés d'ESET Mail Security via Windows Management Instrumentation. ESET Mail Security peut également être intégré dans d'autres solutions de SIEM (Software Information and Event Management) comme Microsoft System Center Operations Manager, Nagios et autres.

SUPPORT TECHNIQUE INCLUS

Allez plus loin grâce à l'aide apportée par nos spécialistes. Bénéficiez du support technique en français dès que vous en avez besoin.

Simplicité d'utilisation

Exclusions de processus	Définition par l'administrateur de processus ignorés par le module de protection en temps réel – toutes les opérations sur les fichiers pouvant être attribuées à ces processus sont considérées comme sûres. Cette fonctionnalité est très utile pour les processus qui interférent souvent avec la protection en temps réel, comme la sauvegarde ou la migration en direct d'une machine virtuelle. Les processus exclus peuvent accéder aux fichiers ou objets dangereux sans déclencher d'alerte.
Micro-définitions incrémentales	Des mises à jour et actualisations régulières sont téléchargées et appliquées de manière incrémentale par petits paquets. Ce concept permet d'économiser les ressources système et la bande passante sans aucun impact sur la vitesse de l'ensemble du réseau, des serveurs ou sur les besoins des postes en mémoire ou CPU.
Installation basée sur les composants	Choix des composants à installer : - Protection en temps réel du système de fichiers - Protection Internet et email - Contrôle des périphériques - Interface utilisateur (GUI) - ESET Log Collector - Autres
Administration à distance	ESET Mail Security est entièrement administrable via ESET Remote Administrator. Déploiement, exécution de tâches, collecte des logs, notifications et vue globale sur la sécurité de votre réseau à partir d'une console d'administration web unique.
ESET Log Collector	Regroupement de tous les logs pertinents à une demande d'assistance auprès d'ESET dans une archive. Cette archive peut ensuite être envoyée simplement par email ou uploadée.
ESET License Administrator	Gestion via un navigateur web de toutes les licences depuis un seul et même endroit. Rassemblement, délégation et gestion de vos licences sans nécessité d'utiliser la console ESET Remote Administrator.