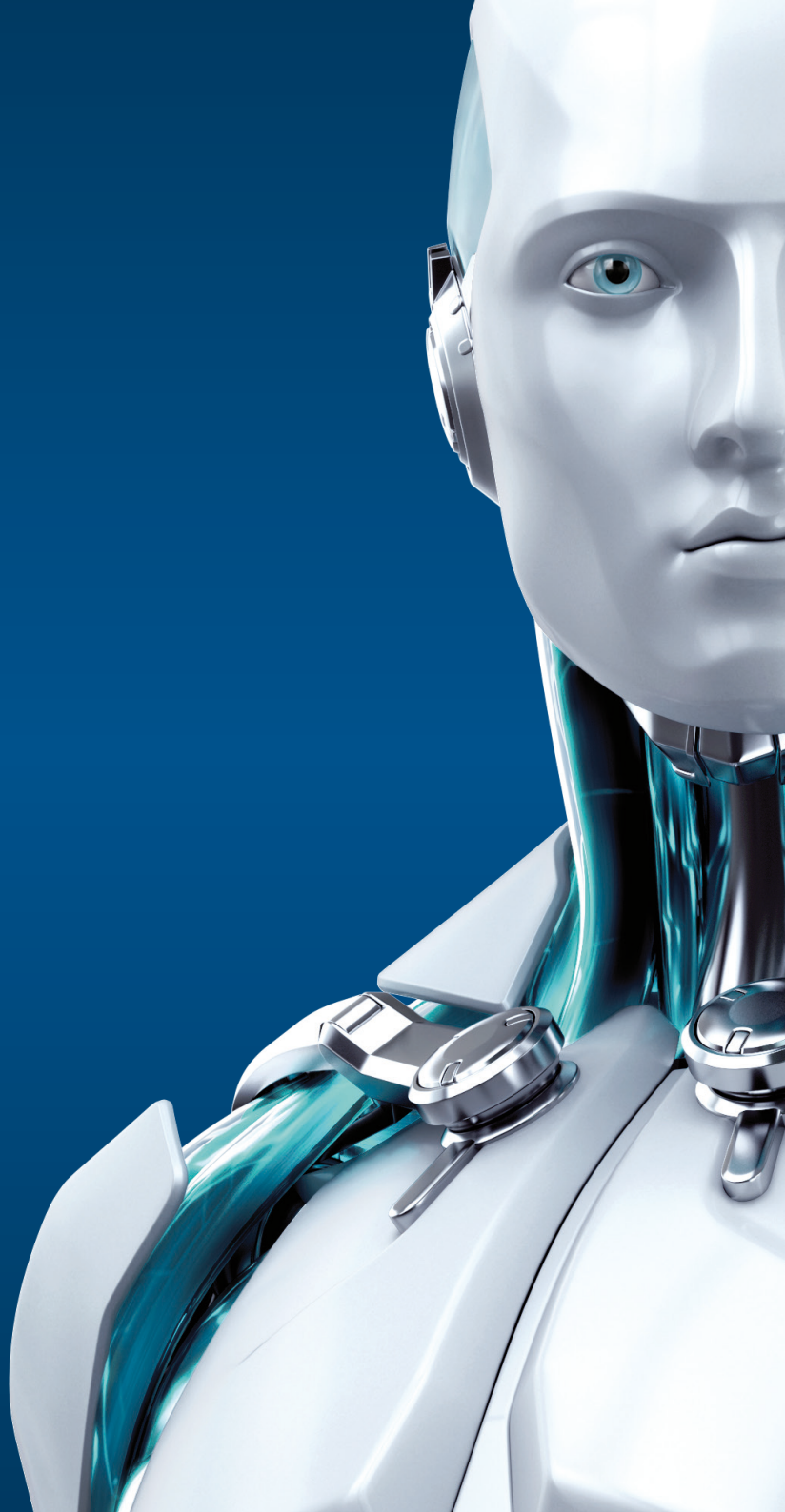
ENDPOINT SECURITY

POUR ANDROID

ENJOY SAFER TECHNOLOGY™



ENDPOINT SECURITY
POUR ANDROID

ESET Endpoint Security pour Android protège votre flotte de terminaux mobiles grâce à la technologie proactive ESET NOD32.

Analysez les applications, fichiers et cartes mémoires, en cas de perte ou de vol, protégez vos périphériques grâce au système antivol : verrouiller, effacer, localiser... Evitez à vos collaborateurs de recevoir des appels ou SMS indésirables. Depuis la console d'administration à distance, appliquez vos politiques de sécurité aux terminaux mobiles de votre entreprise.

Protection des terminaux

Protection en temps réel	Protection en temps réel des fichiers et applications par la technologie proactive ESET NOD32, optimisée pour les smartphones et tablettes. La technologie ESET LiveGrid, système de collecte des échantillons de logiciels malveillants, couplée à l'analyse avancée assurent une protection renforcée de vos terminaux mobiles.
Analyse à la demande	Analyse et nettoyage de la mémoire interne et des supports amovibles en arrière-plan. Option de mise en pause par l'utilisateur et programmation d'analyses régulières.
Analyse sur inactivité	Analyse complète lorsque l'appareil est en charge et l'écran verrouillé.
Anti phishing	Protection contre les tentatives de vol d'informations confidentielles (identifiants, mots de passe, informations bancaires ...) par de faux sites Internet se faisant passer pour dignes de confiance.
Protection contre la désinstallation	Empêche la désinstallation de l'application par l'utilisateur sans le mot de passe administrateur.
Filtrage des appels & SMS	Protège les utilisateurs des appels et SMS* provenant de numéros masqués, certains contacts ou numéros, ou pendant des périodes prédéfinies.
	* La fonctionnalité de blocage des SMS n'est pas disponible à partir des versions 4.4 Kitkat. Ceci est lié aux modifications faites par Google sur le système d'exploitation Android.

Sécurité des terminaux

Permet l'application des politiques de sécurité par l'administrateur sur la flotte de terminaux mobiles. ESET mobile Security notifie automatiquement l'utilisateur et l'administrateur en cas de non-conformité des paramètres de l'appareil avec la politique de l'entreprise et propose des modifications.

Paramètres de sécurité	Définition des conditions de complexité des mots de passe. Paramétrage du nombre de tentatives maximum de déverrouillage avant la réinitialisation de l'appareil. Définition de la date de validité du code de déverrouillage. Paramétrage du temps avant le verrouillage de l'écran. Demande aux utilisateurs de chiffrer leurs terminaux mobiles. Blocage de l'utilisation de la caméra intégrée.

Politique(s) de sécurité des terminaux – permet à l'administrateur de contrôler le paramétrage prédéfini des appareils pour déterminer s'il est conforme ou non aux politiques de sécurité de l'entreprise. L'administrateur peut gérer l'utilisation de la mémoire, la connexion Wi-Fi, l'utilisation des data et les appels à l'étranger, les sources inconnues – autre que la boutique Google Play, le débogage USB, NFC, le chiffrement des données et leur état.

Antivol

Commandes antivol	Toutes ces commandes peuvent être actionnées par l'administrateur via la console ESET Remote Administrator, via un SMS avec un code de vérification à deux facteurs, ou directement depuis l'interface produit de l'administrateur – fonctionnalité très utile si vous n'utilisez pas la gestion à distance ou lorsque l'administrateur est hors du bureau.
Verrouillage à distance	En cas de perte ou de vol, verrouillage à distance de l'appareil. Après le blocage du terminal, les personnes non autorisées ne pourront accéder aux données stockées. Une fois l'appareil retrouvé, une commande de déverrouillage à distance permet à nouveau l'utilisation de l'appareil.
Localisation à distance	Localisation de l'appareil et suivi de sa position GPS à distance.
Effacement à distance	Suppression en toute sécurité des contacts, messages et données stockés dans la mémoire interne de l'appareil, ainsi que sur la carte mémoire. Les procédures de nettoyage avancées garantissent que les données supprimées ne pourront être restaurées. La solution ESET Endpoint Security quant à elle reste installée ce qui permet, même après effacement, de continuer à utiliser les commandes antivol.
Sirène	Activation distante d'un son, même si l'appareil est en mode silencieux. Une fois la sirène déclenchée, l'appareil est automatiquement verrouillé.
Réinitialisation	Suppression de toutes les données accessibles depuis l'appareil et réinitialisation des paramètres d'origine.
Message personnalisé	Envoi par l'administrateur d'un message personnalisé vers un ou plusieurs appareils. Le message s'affiche comme un pop-up afin que l'utilisateur ne puisse le manquer.
Information verrouillage d'écran	L'administrateur peut définir des informations personnalisées (raison sociale, adresse email, message ...) qui seront affichées sur l'écran du terminal, même quand celui-ci est verrouillé.
Correspondance SIM	Lorsqu'une carte SIM non autorisée est insérée, l'appareil est verrouillé automatiquement. Toutes les informations de cette carte SIM sont envoyées à l'administrateur.
Contacts administrateur	Liste blanche de coordonnées protégée par un mot de passe, autorisées à déclencher les commandes SMS utilisées pour contrôler le terminal. Ces coordonnées seront utilisées pour les notifications relatives aux fonctionnalités antivol.

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.

Contrôle des applications

Gérez efficacement les applications installées, bloquez des accès et empêchez les utilisateurs de les désinstaller.

Paramétrage du contrôle des applications	Paramétrage manuel des applications que vous souhaitez bloquer. Blocage basé sur des catégories : jeux, réseaux sociaux ... Blocage basé sur les permissions : applications utilisant la localisation, l'accès aux listes de contacts ... Blocage par source : applications provenant de sources autres que les stores par défaut. Créer des exceptions : liste blanche d'applications. Paramétrer une liste d'applications obligatoires
Audit des applications	Suivez les applications et leurs accès aux données de l'entreprise. Gérez et contrôlez efficacement les accès des applications.

Simplicité d'utilisation et de gestion

Import/Export paramétrage	Si vos terminaux mobiles ne sont pas gérés via ESET Remote Administrator, l'administrateur peut facilement appliquer des paramétrages d'un terminal aux autres. Pour cela, il lui suffit d'exporter ces réglages dans un fichier et d'importer ce même fichier dans les autres terminaux utilisant la solution ESET Endpoint Security pour Android.
Centre de notifications	Consultation de toutes les notifications et des solutions associées à partir d'une même interface.
Administration en local	Possibilité d'administrer le terminal en local si celui-ci n'est pas géré par ESET Remote Administrator. Tous les paramètres sont protégés par un mot de passe admin.
Identification renforcée	Seuls les terminaux présents sur la liste blanche peuvent se connecter à ESET Remote Administrator. Simplification de l'identification des terminaux par nom, description et IMEI.
Assistant de configuration	Des assistants de configuration sont disponibles pour chaque fonctionnalité afin de faciliter le paramétrage local des terminaux.
Administration à distance	Gestion complète des solutions ESET Endpoint par la console d'administration 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 Licence Administrator	Gestion via un navigateur web de toutes vos licences en un point central. Permet la fusion, délégation et gestion de vos licences sans nécessité d'utiliser la console ESET Remote Administrator.