



ENDPOINT SOLUTIONS

Technologie multicouche, machine learning et expertise humaine réunis en synergie dynamique dans des solutions fournies par le leader Européen de la sécurité des terminaux

DES EXPERTS EN CYBERSÉCURITÉ
À VOS CÔTÉS



Qu'est-ce qu'une **Plateforme Endpoint Protection ?**

Une plateforme de protection Endpoint (EPP, Endpoint Protection Platform) est une solution installée sur les terminaux qui empêche les attaques de malware, détecte les activités malveillantes et fournit les capacités d'investigation et de correction nécessaires pour répondre dynamiquement aux incidents et alertes de sécurité

Les solutions de protection des terminaux d'ESET reposent sur une approche multicouche qui allie différentes technologies en synergie dynamique, pour offrir un juste équilibre entre performance, détection et faux positifs.

Pourquoi utiliser des Solutions Endpoint Protection ?

RANSOMWARES

La menace des ransomwares plane sur tous les secteurs d'activité à travers le monde depuis l'apparition de CryptoLocker en 2013. Si les ransomwares existaient déjà bien auparavant, ils ne constituaient pas jusqu'alors une source de préoccupation majeure pour les entreprises. Aujourd'hui, une simple attaque par ransomware peut facilement interrompre l'activité d'une organisation via le chiffrement des fichiers importants. Lors de tels incidents, les sociétés se rendent souvent compte que leurs sauvegardes ne sont pas suffisamment récentes et se sentent obligées de payer la rançon.

Les solutions de protection des terminaux d'ESET offrent plusieurs couches de défense, en bloquant les ransomwares et en les détectant si jamais ils réussissent à s'infiltrer dans les systèmes de l'entreprise. La prévention et la détection des ransomwares sont importantes, car à chaque fois qu'une victime cède au chantage, cela encourage les cybercriminels à poursuivre ce type d'attaque.

ATTAQUES CIBLÉES ET VIOLATIONS DE DONNÉES

Le monde de la cybersécurité actuel évolue au rythme soutenu des nouvelles méthodes d'attaque et des menaces inédites. En cas d'attaque ou de violation des données, les organisations sont généralement surprises par la compromission de leur système de protection ou ignorent totalement qu'un incident a eu lieu. Lorsqu'elles s'en aperçoivent enfin, elles mènent des actions a posteriori pour éviter que l'infection ne se reproduise. Cependant, ces mesures ne les protègent pas d'éventuelles futures attaques utilisant de nouveaux vecteurs.

Les solutions de protection des terminaux d'ESET exploitent les informations de détection transmises par les endpoints du monde entier, afin d'établir des priorités et de bloquer efficacement les menaces les plus récentes avant qu'elles ne se propagent. Par ailleurs, la plupart des plateformes de protection des terminaux proposent une mise à jour via le cloud pour permettre une réponse rapide en cas de non-détection d'une menace, sans devoir attendre la prochaine mise à jour.

ATTAQUES SANS FICHIER

De nouveaux « malwares sans fichier », qui restent confinés dans la mémoire des ordinateurs, déjouent les mécanismes de protection axés sur l'analyse de fichiers. En outre, certaines de ces attaques se servent d'applications existantes intégrées au système d'exploitation pour rendre la détection des contenus malveillants encore plus difficile. Par exemple, PowerShell est très souvent utilisé dans ce type d'attaque.

Les plateformes de protection des terminaux d'ESET sont dotées de capacités de détection des applications vulnérables ou détournées, pour vous protéger des attaques sans fichier. ESET a également développé des outils d'analyse dédiés pour identifier toute anomalie dans la mémoire. Grâce à cette approche multicouche, nous gardons une longueur d'avance sur les malwares les plus récents.

Les solutions de protection des terminaux d'ESET offrent plusieurs couches de défense, en bloquant les malwares et en les détectant si jamais ils réussissent à s'infiltrer dans les systèmes de l'entreprise.

En cas d'attaque ou de violation des données, les organisations sont généralement surprises par la compromission de leur système de protection ou ignorent totalement qu'un incident a eu lieu.

De nouveaux « malwares sans fichier », qui restent confinés dans la mémoire des ordinateurs, déjouent les mécanismes de protection axés sur l'analyse de fichiers.

“ Nous faisons confiance à ESET depuis plusieurs années. Ses solutions de sécurité font leur travail sans que nous devions nous préoccuper de quoi que ce soit. En résumé, ESET est synonyme de fiabilité, de qualité et de service. ”

—Jos Savelkoul, Team Leader ICT-Department,
Hôpital Zuyderland, Pays-Bas ; +10 000 postes



Solutions de protection des terminaux d'ESET

ESET Endpoint Security pour Windows/macOS/Android
ESET Endpoint Antivirus pour Windows/macOS/Linux Desktop
ESET File Security pour Windows Server/Linux/FreeBSD/Azure
ESET Mobile Device Management pour Apple iOS

Les avantages ESET

PROTECTION MULTICOUCHE

ESET allie technologie multicouche, machine learning et expertise humaine afin d'offrir à ses clients un niveau de protection optimal. Nous adaptons nos solutions en permanence pour parvenir à un juste équilibre entre performance, détection et faux positifs.

COMPATIBILITÉ MULTIPLATEFORME

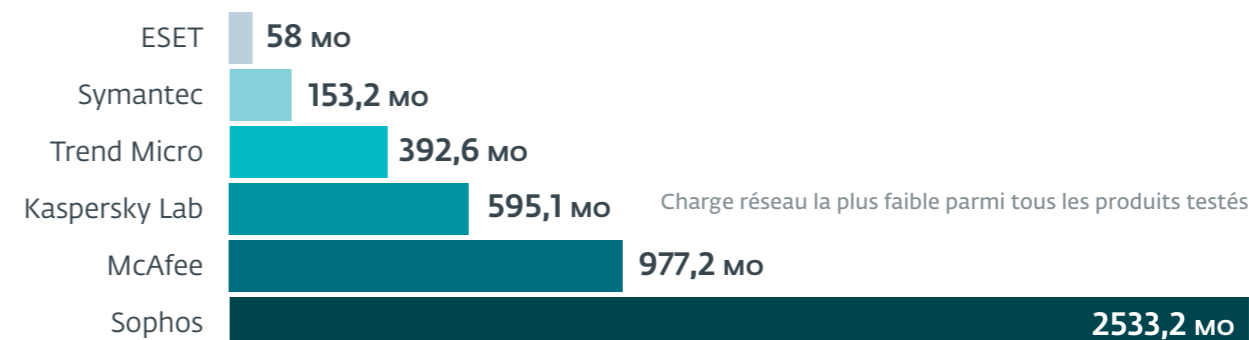
Les solutions de protection des terminaux d'ESET sont compatibles avec tous les systèmes d'exploitation, notamment Windows, Mac, Linux et Android. Tous ces produits peuvent être gérés à partir d'une console unique ; ESET Mobile Device Management pour iOS et Android est également entièrement intégré.

PERFORMANCES INÉGALÉES

L'impact d'une solution de protection des terminaux sur les performances des ordinateurs est une source de préoccupation majeure pour de nombreuses entreprises. Les produits d'ESET excellent dans ce domaine et passent haut la main des tests tiers qui prouvent leur faible impact sur les systèmes.

PRÉSENCE INTERNATIONALE

ESET est implanté dans 22 pays partout dans le monde, avec 13 centres de R&D et une présence dans plus de 200 pays et territoires. Grâce à ce réseau international, nous sommes en mesure de collecter les données nécessaires pour neutraliser les malwares avant qu'ils ne se propagent à l'échelle planétaire et établir un ordre de priorité pour le développement de nos technologies, en fonction des menaces les plus récentes ou des nouveaux vecteurs potentiels.



Source : AV-Comparatives, « Network Performance Test, Business Security Software »

“...La meilleure preuve d'efficacité ? Ce sont les statistiques de notre équipe de support technique : depuis que nous avons opté pour ESET, elle ne reçoit plus d'appels des utilisateurs, car les problèmes liés à l'antivirus ou aux malwares ont disparu !”

— Adam Hoffman, Responsable Infrastructure Informatique,
Mercury Engineering, Irlande ; 1 300 postes

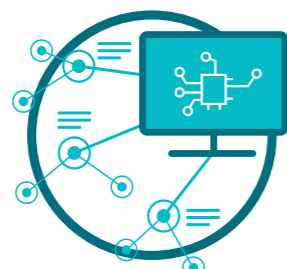
La technologie ESET

Nos produits et technologies reposent sur 3 piliers



ESET LIVEGRID®

Lorsqu'une menace zero-day telle qu'un ransomware est détectée, le fichier est envoyé à notre système cloud de protection anti-malware LiveGrid®, pour l'exécuter et surveiller son comportement. Les résultats sont transmis à tous les endpoints partout dans le monde en quelques minutes, sans nécessiter de mise à jour.



MACHINE LEARNING

Notre moteur de machine learning puissant combine les réseaux neuronaux avec des algorithmes triés sur le volet pour étiqueter correctement les échantillons reçus comme inoffensifs, potentiellement indésirables ou malveillants.



EXPERTISE HUMAINE

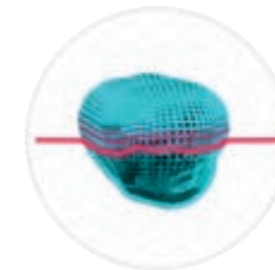
Nos chercheurs en sécurité hors pair partagent leur expertise et leur savoir-faire pour vous apporter les informations sur les menaces dont vous avez besoin 24h/24.

Une seule couche de défense est insuffisante dans un contexte de menaces en constante évolution. Tous les produits de protection des terminaux d'ESET sont capables de détecter les malwares avant, pendant et après leur exécution. En nous concentrant sur l'ensemble du cycle de vie des logiciels malveillants, nous offrons un niveau de protection inégalé.



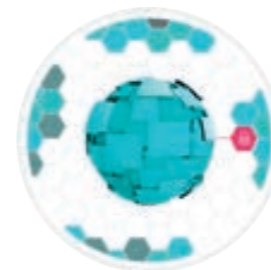
MACHINE LEARNING

Toutes les solutions de protection ESET Endpoint reposent sur le machine learning, outre les autres couches de défense depuis 1997. Aujourd'hui, ESET associe systématiquement le machine learning à ses autres technologies de protection. Plus précisément, notre moteur de machine learning se présente sous forme d'algorithmes générant un résultat consolidé et de réseaux neuronaux.



ANALYSE MÉMOIRE AVANCÉE

La technologie d'analyse avancée de la mémoire d'ESET surveille le comportement des processus malveillants et les analyse lorsqu'ils se montrent sous leur vrai jour dans la mémoire. Les malwares sans fichier ne nécessitent aucun composant persistant dans le système de fichiers pouvant être détecté par une méthode conventionnelle. Seule une analyse de la mémoire permet de détecter et de bloquer ce type d'attaques.



BOUCLIER ANTI-RANSOMWARE

Le bouclier anti-ransomware d'ESET protège les utilisateurs contre les ransomwares. Cette technologie surveille et évalue toutes les applications exécutées, en fonction de leurs comportements et de leur réputation. Elle est conçue pour détecter et bloquer les processus ayant un comportement de ransomware.



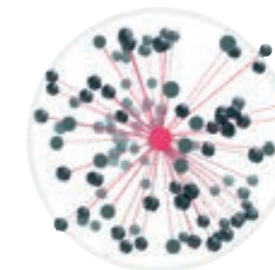
BLOQUEUR D'EXPLOITS

Le bloqueur d'exploits d'ESET surveille les applications vulnérables (navigateurs, lecteurs de documents, clients de messagerie, Flash, Java, etc.). Au lieu de se limiter à des identifiants CVE spécifiques, il cible les techniques d'exploitation de failles. Lorsqu'un processus suspect est enclenché, il est immédiatement bloqué sur l'ordinateur.



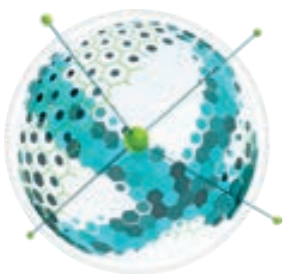
SANDBOX INTÉGRÉE

Les malwares d'aujourd'hui sont souvent obscurcis pour tenter d'échapper à la détection. Afin d'identifier le comportement réel qui se cache sous les apparences, nous utilisons une sandbox intégrée. Grâce à cette technologie, les solutions ESET émulent différents composants matériels et logiciels pour exécuter les programmes suspects dans un environnement virtualisé isolé.



PROTECTION ANTI-BOTNET

La protection anti-botnet d'ESET détecte les communications malveillantes des botnets, tout en identifiant les processus en cause. Toute communication malveillante détectée est bloquée et signalée à l'utilisateur.



PROTECTION CONTRE LES ATTAQUES RÉSEAU

Cette technologie améliore la détection des failles connues à l'échelle du réseau. Elle offre une couche de protection supplémentaire importante contre la propagation des malwares, les attaques réseau et l'exploitation de failles pour lesquelles aucun correctif n'a encore été publié ou installé.



DÉTECTION ADN

Il existe divers types de détection, allant du hachage spécifique à la détection ADN d'ESET, qui repose sur des définitions complexes de comportements malveillants et de caractéristiques des malwares. Si le code malveillant peut être facilement modifié ou obscurci par les attaquants, le comportement des objets est en revanche plus difficile à changer. La détection ADN d'ESET est justement conçue pour tirer profit de ce principe.



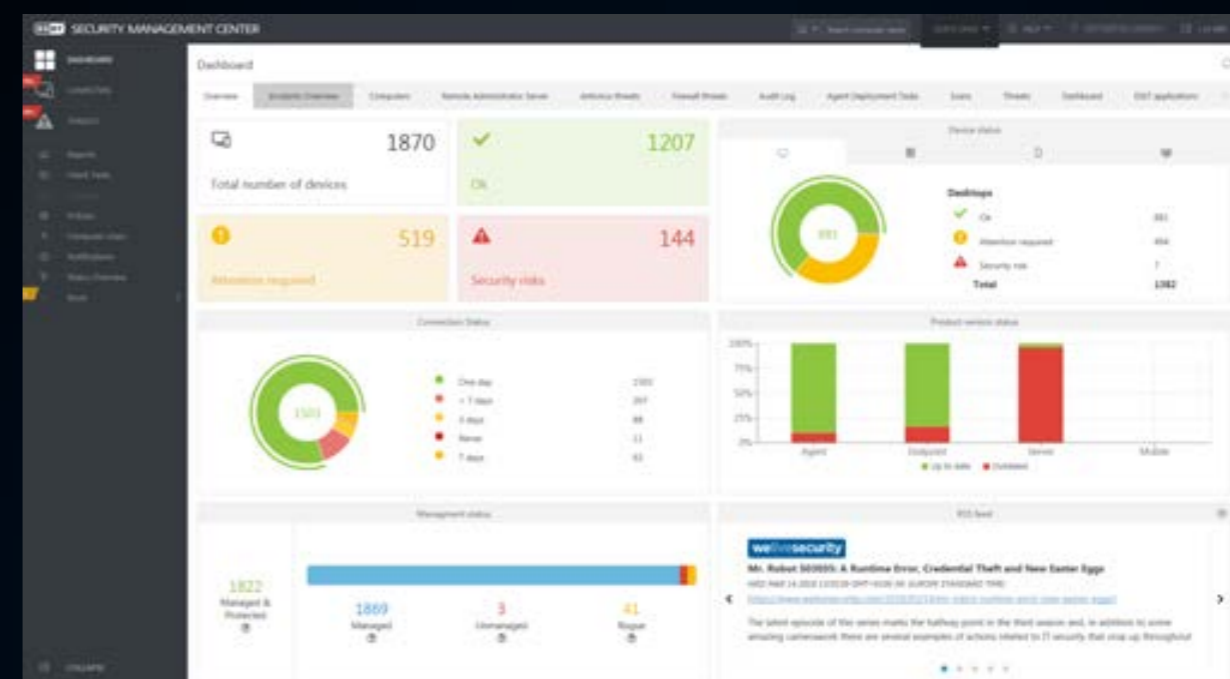
HIPS

Le système de prévention des intrusions sur l'ordinateur hôte (HIPS, Host-based Intrusion Prevention System) d'ESET surveille les activités du système et reconnaît les comportements suspects en fonction de règles prédéfinies. Le mécanisme d'autodéfense du système HIPS empêche le processus mis en cause de mener des activités nuisibles.



UEFI SCANNER

ESET est le premier éditeur de sécurité des terminaux à intégrer dans sa solution une technologie dédiée à la protection de l'UEFI (Unified Extensible Firmware Interface). Le scanner UEFI d'ESET est conçu pour vérifier et assurer la sécurité de l'environnement pré-démarrage, tout en surveillant l'intégrité du firmware. L'utilisateur est informé de toute modification détectée.



ESET Security Management Center

Toutes les solutions ESET Endpoint sont gérées depuis une console unique – ESET Security Management Center – pouvant être installée sous Windows ou Linux. Outre l'installation, ESET propose également une appliance virtuelle que vous pouvez importer pour une mise en service simple et rapide.

“ La solution d'ESET se démarque des autres produits du marché par un avantage technique considérable. Grâce à la protection complète et fiable qu'elle nous offre, nous pouvons travailler en toute sérénité, avec la certitude que nos ordinateurs sont sécurisés à 100 % . ”

— Fiona Garland, Business Analyst Group IT ,
Mercury Engineering, Irlande ; 1 300 postes

Cas d'utilisation

Ransomwares

Certaines entreprises ont besoin de protection supplémentaire contre les attaques par ransomwares.

SOLUTION

- ✓ La protection contre les attaques réseau empêche les ransomwares d'infecter un système en bloquant les failles à l'échelle du réseau.
- ✓ Notre approche de défense multicouche inclut une sandbox intégrée capable de déceler les malwares qui tentent d'échapper à la détection à l'aide de techniques d'obscurcissement.
- ✓ Utilisez le système cloud de protection anti-malware d'ESET pour vous protéger automatiquement contre les nouvelles menaces, sans devoir attendre la mise à jour suivante du moteur de détection.
- ✓ Tous nos produits contiennent un bouclier anti-ransomware qui assure la protection des entreprises contre le chiffrement malveillant des fichiers.

Malwares sans fichier

Les malwares sans fichier sont une menace relativement récente. Résidant uniquement dans la mémoire, ils nécessitent une approche de détection autre que celle utilisée pour les fichiers malveillants traditionnels.

SOLUTION

- ✓ La technologie unique d'ESET, l'analyse avancée de la mémoire déjoue ce type de menace en surveillant le comportement des processus malveillants et en les analysant lorsqu'ils se montrent sous leur vrai jour dans la mémoire.

- ✓ Accélérez le recueil de données et l'investigation en envoyant la menace à ESET Threat Intelligence pour obtenir des informations sur son fonctionnement.

- ✓ En alliant technologie multicouche, machine learning et expertise humaine, ESET offre à ses clients un niveau de protection optimal.

Menaces zero-day

Les menaces zero-day constituent un problème majeur pour les entreprises, car elles ne savent pas se protéger contre ces attaques inconnues.

SOLUTION

- ✓ Les produits de protection des terminaux d'ESET font appel à l'heuristique et au machine learning, dans le cadre d'une approche multicouche, pour prévenir et bloquer les malwares inédits.
- ✓ Nos 13 centres de R&D répartis dans le monde entier contribuent à la mise en place d'une réponse rapide aux malwares dès leur première occurrence, quel que soit leur lieu d'apparition.
- ✓ Le système cloud de protection anti-malware d'ESET vous protège automatiquement contre les nouvelles menaces, sans que vous ayez besoin d'attendre la mise à jour suivante du moteur de détection.

“ESET réunit tout ce dont nous avons besoin : une technologie fiable, une détection robuste, une présence locale et un excellent support technique.”

— Ernesto Bonhoure, responsable infrastructure informatique, Hôpital Alemán, Argentine ; > 1 500 postes

À propos d'ESET

ESET, acteur mondial de la sécurité informatique, est désigné comme unique Challenger dans le Gartner Magic Quadrant 2018, « Endpoint Protection »

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe, qui protègent en temps réel les entreprises et les

particuliers du monde entier contre des menaces de cybersécurité en constante évolution.

En tant qu'entreprise privée non endettée, nous sommes libres de mener toutes les actions nécessaires pour offrir à nos clients une protection optimale et complète.

ESET EN QUELQUES CHIFFRES

+110 millions
d'utilisateurs
partout dans le
monde

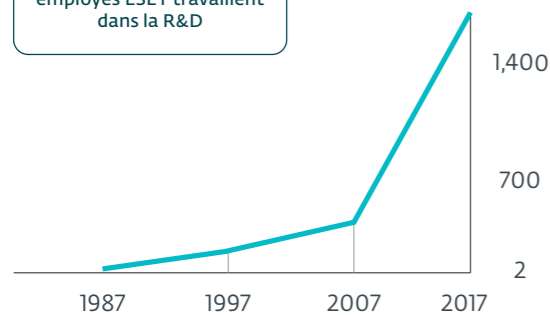
+ 400 000
Clients
Entreprises

+ 200
pays et
territoires
couverts

13
centres
R&D dans
le monde

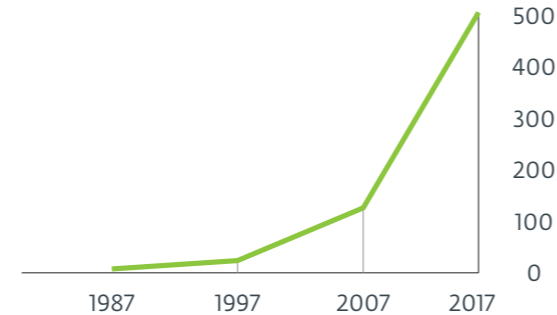
EMPLOYÉS ESET

Plus d'un tiers des
employés ESET travaillent
dans la R&D



CHIFFRE D'AFFAIRES ESET

en million €



*Gartner ne recommande aucun fournisseur, produit ou service mentionnés dans ses rapports d'études. Les opinions exprimées par Gartner dans ses publications ne doivent pas être interprétées comme des faits établis. Gartner décline toute responsabilité, expresse ou tacite, relative à cette étude, notamment toute garantie de valeur commerciale ou d'adéquation à un usage particulier.

QUELQUES-UNS DE NOS CLIENTS

HONDA

Protégé par ESET depuis 2011
Licence prolongée 3 fois, étendue 2 fois

GREENPEACE

Protégé par ESET depuis 2008
Licence prolongée/étendue 10 fois

Canon

Protégé par ESET depuis 2016
Plus de 14 000 endpoints

T ..

Partenaire de sécurité FAI depuis 2008
2 millions d'utilisateurs

NOS RÉCOMPENSES LES PLUS PRESTIGIEUSES



" Avec ses excellentes fonctionnalités anti-malware, sa simplicité de gestion et sa présence internationale, ESET fait partie des meilleurs candidats du marché pour les appels d'offres de solutions de sécurité. "

KuppingerCole Leadership Compass
Enterprise Endpoint Security: Anti-Malware Solutions, 2018



Contactez-nous :
Email : contact@lgandco.fr
Tel : 01 77 70 05 95
www.lgandco.fr