



PRÉSENTATION

ENDPOINT SECURITY

Puissante protection multicouche
pour les postes de travail et
les ordinateurs portables

Progress. Protected.

Qu'est-ce que la **protection moderne des endpoints** ?

Une solution déployée sur les endpoints pour prévenir les attaques de malwares, détecter les activités malveillantes, et fournir les outils d'enquête et de remédiation nécessaires pour répondre de manière dynamique aux incidents de sécurité et aux alertes.

Les solutions de protection d'ESET pour endpoints s'appuient sur une approche multicouche avec plusieurs technologies travaillant ensemble pour équilibrer constamment les performances, la détection et les faux positifs.

Solutions de protection ESET pour endpoints

✓ ESET Endpoint Security for Windows

✓ ESET Endpoint Security for macOS

✓ ESET Endpoint Antivirus for Windows

✓ ESET Endpoint Antivirus for macOS

✓ ESET Endpoint Antivirus for Linux

Les caractéristiques et les fonctionnalités du produit peuvent varier en fonction du système d'exploitation et du niveau d'abonnement souscrit.

Les avantages ESET

PROTECTION MULTICOUCHE

ESET combine une technologie multicouche, le machine learning et l'expertise humaine pour fournir à nos clients le meilleur niveau de protection possible. Notre technologie s'adapte et évolue en permanence pour offrir le meilleur équilibre entre détection, performances et faux positifs.

PRISE EN CHARGE MULTIPLATEFORME

Les produits de protection d'ESET pour endpoints prennent en charge tous les systèmes d'exploitation : Windows (y compris Windows sur ARM), macOS, Linux et Android. Tous nos produits pour endpoints peuvent être entièrement administrés à partir d'une seule interface. L'administration des appareils mobiles iOS et Android est également entièrement intégrée.

PERFORMANCES INÉGALÉES

L'une des principales préoccupations de nombreuses entreprises est l'impact de leur solution de protection des endpoints sur les performances. Les produits ESET continuent d'exceller dans le domaine de la performance et sortent vainqueurs des tests indépendants qui prouvent la légèreté de nos clients sur les systèmes.

PRÉSENCE MONDIALE

ESET possède des bureaux dans 22 pays, des laboratoires de recherche et de développement dans 11 pays et est disponible dans plus de 176 pays et territoires. Nous disposons ainsi de données qui nous permettent de stopper les malwares avant qu'ils ne se répandent à travers le monde, et d'accorder la priorité aux nouvelles technologies en fonction des menaces les plus récentes ou des nouveaux vecteurs possibles.



Windows 11



vmware®

Toutes les solutions de protection d'ESET pour endpoints sont administrées à partir d'une console ESET PROTECT unique sur site ou dans le Cloud, afin de garantir une vue d'ensemble complète sur votre système d'information..



« CE QUI RESSORT LE PLUS, CE SONT SES AVANTAGES TECHNIQUES ROBUSTES PAR RAPPORT AUX AUTRES PRODUITS DU MARCHÉ. ESET NOUS OFFRE UNE SÉCURITÉ FIABLE, CE QUI SIGNIFIE QUE JE PEUX TRAVAILLER SUR N'IMPORTE QUEL PROJET À TOUT MOMENT EN SACHANT QUE NOS ORDINATEURS SONT PROTÉGÉS À 100 %. »

Fiona Garland, analyste informatique, Mercury Engineering (Irlande), 1 300 postes

Technologie ESET de pointe

Approche multicouche de la cybersécurité conçue pour l'IA

Notre technologie propriétaire ESET LiveSense® comporte plusieurs couches de protection. Elle fonctionne avec ESET LiveGrid®, notre technologie cloud de recherche de menaces, qui collecte et analyse un vaste ensemble d'échantillons suspects. Combinées à l'IA et notre expertise humaine, les solutions de sécurité d'ESET offrent une protection en temps réel contre les cybermenaces en constante évolution.



INTELLIGENCE ARTIFICIELLE

La puissance combinée des réseaux neuronaux et des algorithmes développés spécialement classe correctement les échantillons entrants comme sains, potentiellement indésirables ou malveillants. Pour offrir les meilleurs taux de détection et le plus petit nombre possible de faux positifs, ESET Augur, notre moteur de machine learning, est finement réglé pour coopérer avec d'autres technologies de protection telles que la détection ADN, la sandbox et l'analyse de la mémoire, afin d'extraire des caractéristiques comportementales.



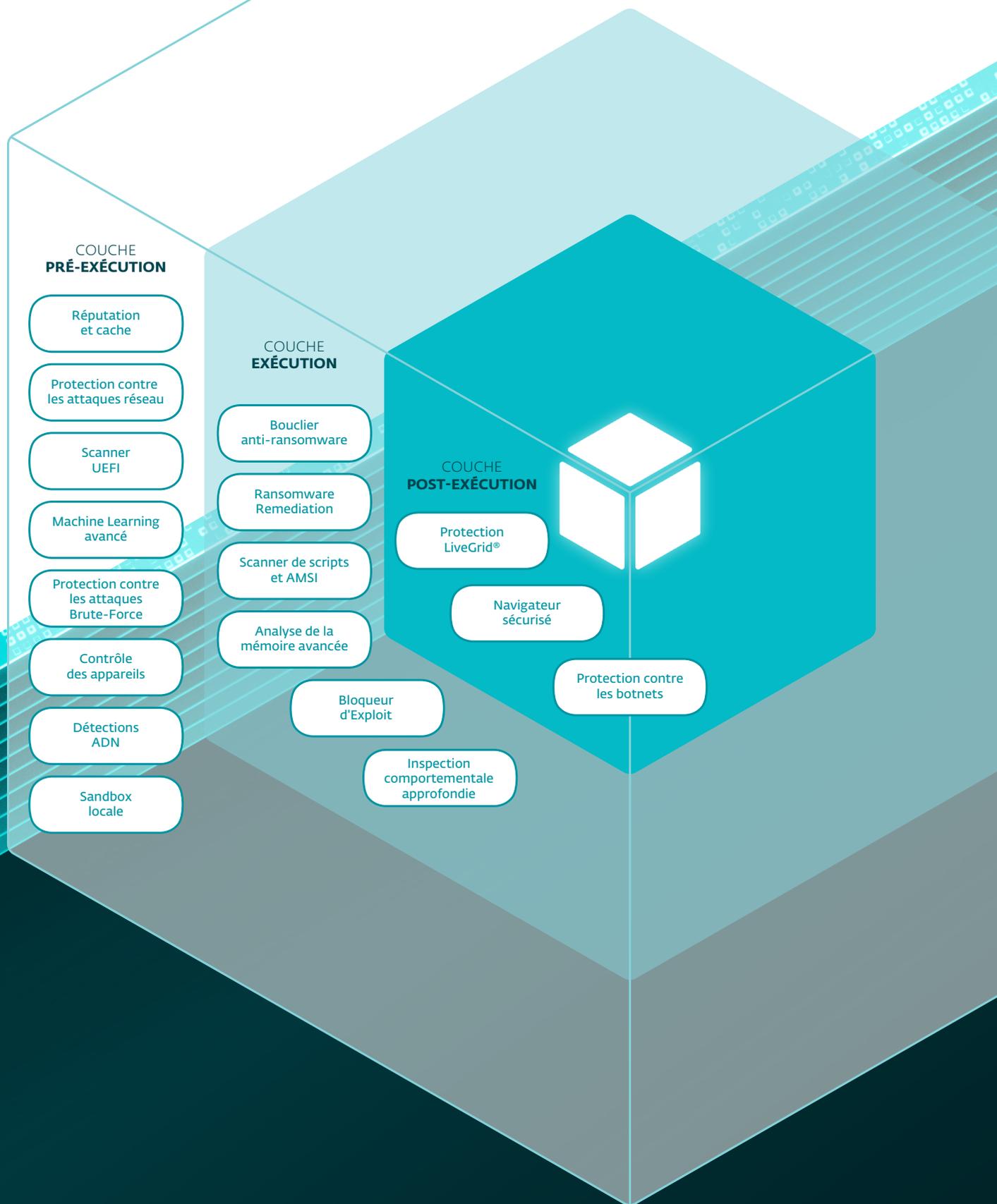
ESET LIVEGRID®

Dès qu'une menace zero-day telle qu'un ransomware est détectée, le fichier est envoyé à notre système de protection contre les malwares dans le Cloud, LiveGrid®, dans lequel la menace est déclenchée et son comportement est surveillé. Les résultats de ce système sont fournis à tous les endpoints du monde entier en quelques minutes, sans nécessiter de mises à jour.



EXPERTISE HUMAINE

La technologie seule ne fait pas des miracles. ESET investit dans son personnel pour disposer d'une main-d'œuvre formée qui souhaite rester dans l'entreprise. Des chercheurs en sécurité de renommée mondiale partagent leurs connaissances afin d'assurer la meilleure veille sur les menaces 24 h/24.



Le diagramme ci-dessus montre certaines des technologies de base d'ESET et indique approximativement quand et où elles peuvent détecter et/ou bloquer une menace pendant son cycle de vie dans le système. [En savoir plus](#)



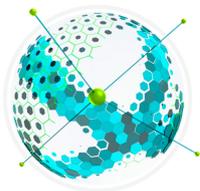
PROTECTION CONTRE LES ATTAQUES BRUTE-FORCE

Une fonctionnalité de sécurité qui protège les appareils contre le piratage des identifiants et l'établissement illégitime d'une connexion à distance. La protection peut être facilement configurée via une politique directement à partir de la console et des exclusions peuvent être créées en cas de blocage qui n'avait pas lieu d'être.



NAVIGATEUR SÉCURISÉ

Conçu pour protéger les ressources d'une entreprise avec une couche de protection spéciale, qui se concentre sur le navigateur en tant que principal outil utilisé pour accéder à des données critiques à l'intérieur du périmètre de l'intranet et dans le Cloud. Le navigateur sécurisé offre une protection renforcée de la mémoire pour le processus de navigation, associée à une protection du clavier. Les administrateurs peuvent également préciser les URL à protéger.



PROTECTION CONTRE LES ATTAQUES RÉSEAU

Cette technologie améliore la détection des vulnérabilités connues au niveau du réseau. Elle constitue une autre couche de protection importante contre la propagation des malwares, les attaques menées via le réseau, et l'exploitation de vulnérabilités pour lesquelles aucun correctif n'a été publié ou déployé.



BOUCLIER ANTI-RANSOMWARE

Une couche de sécurité ESET supplémentaire qui protège les utilisateurs contre les ransomwares. Cette technologie surveille et évalue toutes les applications exécutées en fonction de leur comportement et de leur réputation. Elle est conçue pour détecter et bloquer les processus qui s'apparentent au comportement d'un ransomware.



RANSOMWARE REMEDIATION NOUVEAUTÉ

Fonctionnalité de roll-back complet grâce à une restauration transparente et automatisée des fichiers à partir de sauvegardes sécurisées pour minimiser l'impact des attaques de ransomwares. Cette fonctionnalité propriétaire renforce la protection de Ransomware Shield avec des technologies de détection et de remédiation avancées, surpassant le Volume Shadow Copy Service d'autres fournisseurs.

Remarque : Inclus dans ESET PROTECT Advanced et les niveaux d'abonnement supérieurs.



PROTECTION CONTRE LES BOTNETS

La protection d'ESET contre les botnets détecte les communications malveillantes utilisées par les botnets et identifie en même temps les processus incriminés. Toute communication malveillante détectée est bloquée et signalée à l'utilisateur.



HIPS

La technologie ESET de prévention des intrusions surveille l'activité du système et utilise un ensemble de règles prédéfinies pour reconnaître les comportements suspects du système. Le mécanisme d'autodéfense HIPS empêche le processus incriminé de mener à bien l'activité nuisible.

Cas d'utilisation

Ransomwares

PROBLÈME

Certaines entreprises veulent avoir l'assurance qu'elles seront protégées contre les attaques de ransomwares.

SOLUTION

- ✓ La protection contre les attaques réseau est en mesure d'empêcher les ransomwares d'infecter un système, en bloquant le détournement du réseau.
- ✓ Notre défense multicouche comprend une sandbox intégré au produit, capable de détecter les malwares qui tentent d'échapper à toute détection par l'obscurcissement de leurs actions.
- ✓ Tirez parti du système de protection d'ESET dans le Cloud pour vous protéger automatiquement contre les nouvelles menaces sans avoir à attendre la prochaine mise à jour du moteur de détection.
- ✓ Tous les produits intègrent une protection sous la forme d'un bouclier contre les ransomwares qui veille à ce que les utilisateurs d'ESET soient protégés contre le chiffrement malveillant des fichiers.
- ✓ Restaurer automatiquement tous les fichiers compromis grâce à la fonctionnalité Ransomware Remediation (incluse dans ESET PROTECT Advanced et les niveaux d'abonnement supérieurs).

Malwares sans fichier

PROBLÈME

Les malwares sans fichiers constituent une menace relativement nouvelle. Comme ils ne s'exécutent qu'au sein de la mémoire, une approche différente de celle des malwares traditionnels basés sur des fichiers est nécessaire.

SOLUTION

- ✓ Le scanner de la mémoire avancé est une technologie ESET unique qui protège contre ce type de menace en surveillant le comportement des processus malveillants et en les analysant une fois qu'ils se démasquent dans la mémoire.
- ✓ La technologie multicouche, le machine learning et l'expertise humaine offrent à nos clients le meilleur niveau de protection possible.

Piratage des mots de passe

PROBLÈME

Le protocoles RDP (accès à distance) et SMB (bloc de messages serveur) sont des vecteurs d'attaque attrayants qui peuvent permettre à un pirate d'obtenir le contrôle complet d'un système à distance.

SOLUTION

- ✓ La protection contre les attaques par force brute offre une défense efficace contre les attaques frontales à distance sur des endpoints protégés par mot de passe.
- ✓ Les appareils sont protégés contre l'usurpation d'identité et l'établissement illégitime de connexions à distance.
- ✓ Des exclusions peuvent être créées en cas de blocage qui n'avait pas lieu d'être.
- ✓ Les utilisateurs peuvent également ajouter leurs propres règles ou modifier celles qui existent déjà.

Identifiants volés

PROBLÈME

Les attaques d'hameçonnage et les faux sites web imitant des entreprises légitimes pour voler des identifiants de connexion et des données financières sont en augmentation.

SOLUTION

- ✓ Les produits ESET pour endpoints sont conçus pour protéger les ressources d'une entreprise à l'aide d'une couche de protection unique, qui se concentre sur le navigateur en tant que principal outil utilisé pour accéder à des données critiques à l'intérieur du périmètre de l'intranet et dans le Cloud.
- ✓ La fonction de navigateur sécurisé protège les données sensibles lors de la navigation en ligne.
- ✓ D'un simple clic, les administrateurs peuvent choisir d'inclure tous les portails bancaires et de paiement, et décider de protéger le navigateur pour des sites web spécifiques.

Voici ESET

Défense proactive. Minimisez les risques par la prévention.

Conservez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre approche axée sur l'IA et la prévention. Nous combinons la puissance de l'IA et l'expertise humaine pour améliorer l'efficacité et la facilité d'utilisation de la protection.

Bénéficiez d'une protection de haut niveau grâce à notre Threat Intelligence interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des chercheurs reconnus.

ESET PROTECT, notre plateforme de cybersécurité XDR, combine des fonctionnalités de nouvelle génération de prévention, de détection et de recherche proactive de menaces, avec une gamme étendue de services de sécurité, notamment de détection et de réponse managés.

Nos solutions hautement personnalisables comprennent une assistance locale et ont un impact minimal sur les performances. Elles identifient et neutralisent les menaces connues et émergentes avant qu'elles ne puissent se déclencher. Elles favorisent la continuité des activités, et réduisent les coûts de mise en œuvre et d'administration.

ESET protège votre entreprise afin que vous puissiez maximiser le potentiel de la technologie.

ESET EN QUELQUES CHIFFRES

+ 1 Mrd

internauts
protégés

+ 500 k

entreprises
clientes

176

pays et
territoires

11

centres de
recherche

QUELQUES-UNS DE NOS CLIENTS



Protégé par ESET depuis
2017 : 9 000 endpoints



Protégé par ESET depuis
2016 : +4 000 boîtes mail



Protégé par ESET depuis
2016 : 32 000 endpoints



Partenaire de sécurité FAI
depuis 2008 : 2 millions
d'utilisateurs

RECONNAISSANCES



ESET est constamment **parmi les éditeurs les plus performants des tests indépendants** d'AV-Comparatives, et atteint les meilleurs taux de détection avec peu voire aucuns faux positifs.



ESET obtient régulièrement les meilleures notes sur la plateforme mondiale d'évaluation des utilisateurs G2, et ses solutions sont **appréciées par les clients du monde entier**.



ESET a été reconnu comme un leader dans le domaine de la sécurité des endpoints dans l'évaluation des fournisseurs IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024.