FICHE PRODUIT

DYNAMIC THREAT DEFENSE

Déjouez les menaces zero-day grâce à une sandbox de sécurité cloud performante

ENJOY SAFER TECHNOLOGY™

30 ANNÉES D'INNOVATION POUR PROTÉGER VOTRE VIE NUMÉRIQUE

Qu'est-ce qu'une **sandbox de sécurité cloud ?**

Une sandbox de sécurité cloud est un environnement de test isolé dans lequel les programmes suspects sont exécutés et leurs comportements observés, notés et analysés de façon automatisée.

ESET Dynamic Threat Defense offre une couche de sécurité supplémentaire aux autres produits ESET, tels que les solutions Mail Security et Endpoint, pour identifier les menaces inconnues grâce à une sandbox de sécurité cloud. Cette technologie repose sur différents types d'outils de détection qui complètent l'analyse statique du code et l'examen approfondi des échantillons avec le machine learning, l'introspection de la mémoire et la détection comportementale.

Pourquoi utiliser une **sandbox de sécurité cloud ?**

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.

Une sandbox de sécurité cloud fournit un niveau de défense supplémentaire en dehors du réseau de l'entreprise en empêchant les ransomwares de s'exécuter dans un environnement de production.

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.

Bien plus efficace qu'une simple analyse superficielle des menaces potentielles, une sandbox de sécurité cloud creuse sous les apparences et évalue le comportement du code suspect, ce qui lui permet de déterminer avec une certitude accrue s'il s'agit d'une attaque ciblée, d'une menace persistante avancée ou d'un élément inoffensif.

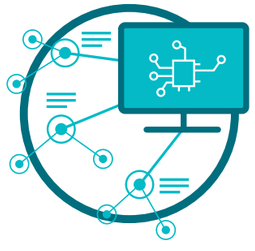
Une sandbox de sécurité cloud fournit un niveau de défense supplémentaire en dehors du réseau de l'entreprise.

Une sandbox de sécurité cloud creuse sous les apparences et évalue le comportement du code suspect.

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 combine la puissance des réseaux neuronaux et d'algorithmes triés sur le volet pour étiqueter correctement les échantillons reçus comme étant 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.

Les avantages ESET

PROTECTION MULTICOUCHE

ESET Dynamic Threat Defense utilise 3 modèles de machine learning différents pour traiter les fichiers reçus. Puis, les échantillons sont exécutés dans une sandbox complète, qui simule le comportement d'un utilisateur pour contrer les techniques d'évasion. Un réseau neuronal de deep learning est ensuite utilisé pour comparer le comportement observé avec les données comportementales existantes. Enfin, la dernière version du moteur d'analyse ESET examine le tout de manière approfondie à la recherche d'anomalies.

VISIBILITÉ COMPLÈTE

Les échantillons analysés sont répertoriés dans la console ESET Security Management Center, avec différentes informations concernant ceux-ci et leur provenance présentées dans un format facile à comprendre. Non seulement les échantillons envoyés à ESET Dynamic Threat Defense sont affichés mais aussi tout ce qui a été envoyé à notre système de protection Cloud, ESET LiveGrid.

MOBILITÉ

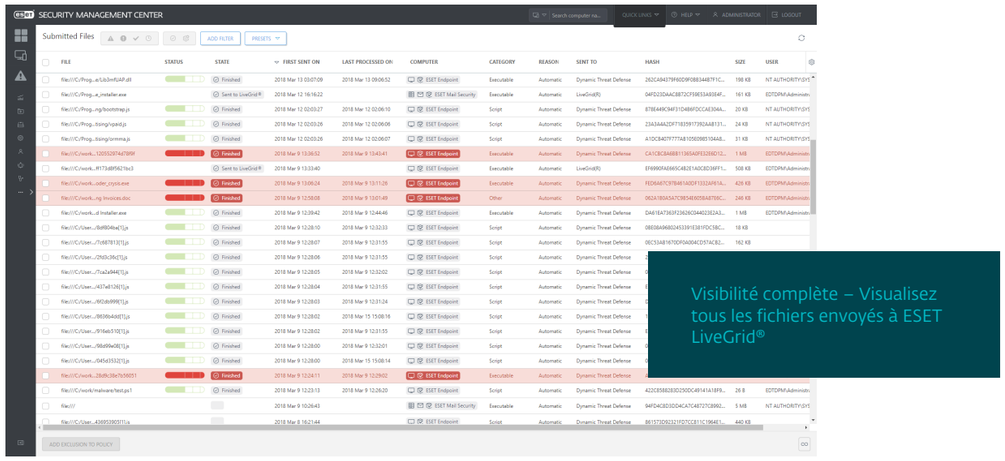
Les utilisateurs d'aujourd'hui sont constamment en déplacement et rarement sur site. C'est pourquoi ESET Dynamic Threat Defense a été conçu pour analyser les fichiers où que vous soyez. En cas de détection d'un élément malveillant, toute l'entreprise est immédiatement protégée.

VITESSE INÉGALÉE

Chaque minute compte. C'est pourquoi, ESET Dynamic Threat Defense est capable d'analyser la plupart des échantillons en moins de 5 minutes. Si un échantillon a déjà été analysé précédemment, il suffit de quelques secondes pour que tous les appareils de votre entreprise soient protégés.

TECHNOLOGIE ÉPROUVÉE ET FIABLE

Avec plus de 30 ans d'expérience dans le secteur de la sécurité informatique, ESET s'efforce d'innover en permanence afin de garder une longueur d'avance sur les menaces émergentes. Plus de 110 millions d'utilisateurs nous font confiance partout dans le monde. Nos solutions sont systématiquement évaluées et validées par des testeurs tiers, qui vérifient l'efficacité de notre approche contre les menaces les plus récentes.



Visibilité complète – Visualisez tous les fichiers envoyés à ESET LiveGrid®

Cas d’utilisation

Ransomwares

CAS D’UTILISATION

Les ransomwares parviennent souvent par e-mail à des utilisateurs peu méfiants.

SOLUTION

- ✓ ESET Mail Security envoie automatiquement les pièces jointes douteuses à ESET Dynamic Threat Defense.
- ✓ ESET Dynamic Threat Defense analyse l’échantillon et renvoie le résultat à ESET Mail Security généralement dans les 5 minutes.
- ✓ ESET Mail Security détecte et neutralise automatiquement les pièces jointes contenant le malware.
- ✓ La pièce jointe malveillante ne parvient jamais au destinataire.

Protection granulaire pour les différents rôles de l’entreprise

CAS D’UTILISATION

Le niveau de protection requis est différent pour chaque rôle au sein de l'entreprise. Les développeurs et le personnel informatique ont besoin de restrictions de sécurité autres que celles du responsable administratif ou du CEO.

SOLUTION

- ✓ Configurez des politiques spécifiques à chaque poste de travail ou serveur dans ESET Dynamic Threat Defense.
- ✓ Appliquez automatiquement des politiques différentes en fonction du groupe statique ou Active Directory auquel l’utilisateur appartient.
- ✓ Modifiez automatiquement les paramètres de configuration en déplaçant un utilisateur d’un groupe à un autre.

Fichiers inconnus ou suspects

CAS D’UTILISATION

Les employés ou le personnel informatique souhaitent parfois s’assurer qu’un fichier reçu est sûr.

SOLUTION

- ✓ Tous les utilisateurs peuvent envoyer directement un fichier pour analyse depuis les produits ESET .
- ✓ L’échantillon est rapidement analysé par ESET Dynamic Threat Defense.
- ✓ Si un fichier malveillant est détecté, tous les ordinateurs de l’entreprise sont protégés.
- ✓ L’administrateur dispose d’une visibilité complète sur l’identité de l’utilisateur qui a envoyé l’échantillon ainsi que le caractère inoffensif ou malveillant du fichier.

FILE BEHAVIOR REPORT

STATUS	Malicious
SHA-1	FED6A67C97B461A0DF1332AF61A89EA9FB5A540F
SIZE	436736B
CATEGORY	Executable

Detected Behaviors

BEHAVIOR	**Malware detected after execution**
EXPLANATION	Sample has been detected as malicious after execution
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware detected with ESET scanning engine after execution
BEHAVIOR	**New files created in the Windows folder**
EXPLANATION	Sample has created new files in the Windows folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	**Analyzed sample copied**
EXPLANATION	Sample has been copied to a different location
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	**Startup list modified**
EXPLANATION	Sample has added a new entry to the Windows Startup application list
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware wants to run after a system reboot
BEHAVIOR	**Machine Learning detection**
EXPLANATION	Sample behaves very similarly to known malware
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware has been detected by Neural network Machine Learning
BEHAVIOR	**New files in Program Files folder created**
EXPLANATION	Sample has created new files in the Windows Program Files folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Sample may be a Potentially Unwanted Application

DYNAMIC THREAT DEFENSE

Fonctionnalités ESET Dynamic Threat Defense

PROTECTION AUTOMATIQUE

Une fois les solutions mises en œuvre, aucune action n'est requise de la part de l'administrateur ou de l'utilisateur. Le produit de sécurité des terminaux ou du serveur détermine automatiquement si un échantillon est inoffensif, malveillant ou inconnu. Les échantillons inconnus sont envoyés à ESET Dynamic Threat Defense pour analyse. Le résultat est ensuite transmis aux produits de protection des terminaux, qui répondent en conséquence.

PERSONNALISATION SUR-MESURE

Des politiques spécifiques à chaque poste de travail peuvent être configurées pour ESET Dynamic Threat Defense, de façon à permettre à l'administrateur de contrôler les échantillons envoyés ainsi que les actions à mener en fonction des résultats d'analyse.

ENVOI MANUEL

À tout moment, les utilisateurs et les administrateurs peuvent envoyer des échantillons pour analyse via un produit ESET compatible et recevoir le résultat complet. Les administrateurs peuvent consulter les éléments envoyés, l'identité des utilisateurs concernés et les résultats directement dans ESET Security Management Center.

PROTECTION DES E-MAILS AVEC ESET MAIL SECURITY

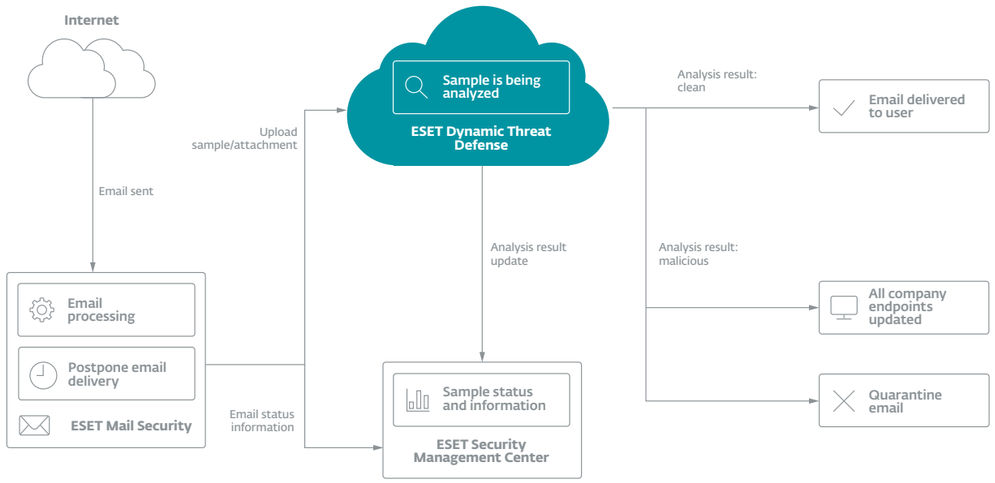
Outre l'analyse de fichiers, ESET Dynamic Threat Defense peut également être associé à ESET Mail Security pour empêcher les e-mails malveillants de parvenir à votre entreprise. Afin de garantir la continuité des activités, seuls les e-mails provenant de l'extérieur de l'entreprise peuvent être envoyés à ESET Dynamic Threat Defense pour analyse.

"La solution ESET se démarque des autres produits du marché par son avantage technique considérable. ESET nous offre une protection complète et fiable, qui nous permet de travailler en toute sérénité, avec la certitude que nos ordinateurs sont sécurisés à 100 %."

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

Fonctionnement
ESET Dynamic Threat Defense

Avec ESET Mail Security



“ Nous sommes si satisfaits de notre expérience avec ESET que nous avons renouvelé nos licences pour trois ans supplémentaires. Nous recommandons vivement les solutions ESET à toutes les entreprises qui souhaitent augmenter leur niveau de sécurité. ”

— 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

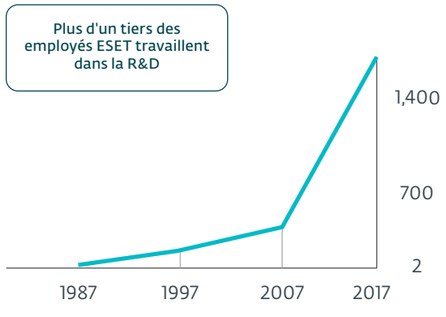
+110 millions
d'utilisateurs partout dans le monde

+ 400 000
Clients Entreprises

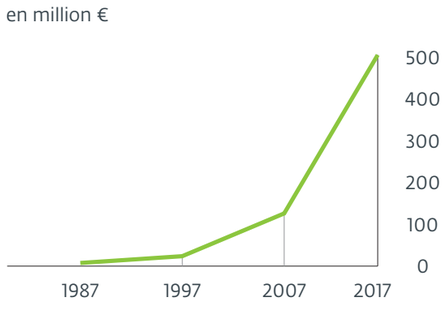
+ 200
pays et territoires couverts

13
centres R&D dans le monde

EMPLOYÉS ESET



CHIFFRE D'AFFAIRES ESET



*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

SE Labs AAA ENTERPRISE ENDPOINT OCT-DEC 2016

THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE WINNER 2017

AV comparatives Approved Business Product 2017

SC MEDIA RECOMMENDED

" 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

ENJOY SAFER TECHNOLOGY™