PRÉSENTATION

LIVEGUARD ADVANCED

Prévention proactive dans le cloud contre les menaces avec remédiation autonome

Progress. Protected.

Qu'est-ce que **la défense avancée contre les menaces ?**

Une technologie proactive qui utilise une analyse adaptative avancée, une technologie d'intelligence artificielle de pointe, un sandbox dans le Cloud, et une analyse approfondie des comportements pour prévenir les attaques ciblées ainsi que les nouveaux types de menaces jamais vues auparavant, notamment les ransomwares. ESET propose une prévention avancée des menaces à partir du Cloud avec des fonctionnalités de remédiation autonomes et une recherche de menaces à partir du Cloud. Une visibilité détaillée sur le paysage mondial des malwares permet une protection en temps réel contre les cybermenaces en constante évolution.

ESET LiveGuard Advanced fournit une couche de sécurité supplémentaire pour ESET Mail Security, ESET Endpoint Security et ESET Cloud Office Security. Sa technologie avancée dans le Cloud comporte de nombreux types de capteurs qui effectuent une analyse statique du code, une inspection approfondie des échantillons à l'aide du machine learning, une introspection en mémoire, et une analyse des comportements.

Pourquoi utiliser **une défense proactive dans le Cloud contre les menaces ?**

RANSOMWARES

Les ransomwares sont une préoccupation constante pour les organisations dans le monde entier depuis Cryptolocker en 2013. Bien que les ransomwares existent depuis bien plus longtemps, ils ne constituaient pas précédemment une menace majeure pour les entreprises. Cependant, une seule incidence de ransomware peut aujourd'hui facilement stopper l'activité d'une entreprise en chiffrant des fichiers importants ou nécessaires. Lorsqu'une entreprise est victime d'une attaque de ransomware, elle se rend rapidement compte que les sauvegardes dont elle dispose ne sont pas assez récentes, si bien qu'elle a l'impression qu'elle doit payer la rançon.

La détection proactive des menaces à partir du Cloud avec remédiation autonome fournit une couche de défense supplémentaire à l'extérieur du réseau de l'entreprise pour empêcher les ransomwares de s'exécuter dans un environnement de production.

ATTAQUES CIBLÉES ET FUITES DE DONNÉES

Le paysage actuel de la cybersécurité est en constante évolution, avec de nouvelles méthodes d'attaque et des menaces jamais vues auparavant. Lorsqu'une attaque ou une fuite de données se produit, les entreprises sont généralement surprises que leurs défenses aient été compromises ou ignorent totalement que l'attaque s'est produite. Une fois l'attaque découverte, les entreprises s'empressent alors de mettre en œuvre des mesures d'atténuation réactives pour éviter que l'attaque ne se reproduise. Toutefois, cela ne les protège pas de la prochaine attaque qui pourrait utiliser un tout nouveau vecteur.

L'approche du sandboxing dans le Cloud est beaucoup plus efficace que le simple examen de l'apparence de la menace potentielle, car elle observe plutôt le comportement de la menace. Cela lui permet d'être beaucoup plus concluante lorsqu'il s'agit de déterminer si quelque chose est une attaque ciblée, une menace persistante avancée ou un incident bénin.

L'analyse statique et dynamique est réalisée par un ensemble d'algorithmes de machine learning, utilisant notamment des techniques de deep learning.

Un sandbox de sécurité dans le Cloud situé à l'extérieur du réseau de l'utilisateur peut aller au-delà de la simple analyse de l'apparence de la menace potentielle et observer son comportement.

Les avantages ESET

REMÉDIATION AUTONOME

ESET LiveGuard Advanced est une défense à partir du Cloud contre les menaces, qui évalue tous les échantillons suspects soumis dans un environnement de test sécurisé (sandbox) ESET dans le Cloud. Leur comportement est examiné ici en utilisant les flux de threat intelligence, les multiples outils internes d'ESET pour l'analyse statique et dynamique, et les données de réputation pour détecter les malwares ou les menaces zero-day. Cette défense est prête à l'emploi, et aucune routine d'installation n'a besoin d'être effectuée par l'administrateur ou l'utilisateur. Un échantillon sur l'endpoint qui est identifié comme inconnu est envoyé pour analyse. Une fois l'analyse terminée et une menace identifiée, celle-ci est automatiquement supprimée, évitant ainsi toute perturbation potentielle.

VISIBILITÉ TOTALE

La console ESET PROTECT vous permet de visualiser les résultats de chaque échantillon analysé. Les clients disposant de licences pour plus de 100 postes obtiennent également un rapport complet contenant des informations détaillées sur les échantillons et leur comportement observé pendant l'analyse dans le sandbox, le tout sous une forme facile à comprendre. Nous présentons non seulement les échantillons envoyés à ESET LiveGuard Advanced, mais également tous ceux envoyés à ESET LiveGrid®, le système de protection d'ESET dans le Cloud contre les malwares.

PROTECTION OMNIPRÉSENTE

La technologie ESET prend en charge les pratiques de travail de votre organisation. ESET LiveGuard Advanced est en mesure d'analyser les fichiers quelle que soit la localisation des utilisateurs. Les salariés en distanciel ou en mode hybride bénéficient de la même protection que les salariés travaillant dans les bureaux de l'entreprise. Lorsqu'un élément malveillant est détecté, l'ensemble de l'entreprise est immédiatement protégé.

CONFIDENTIALITÉ

ESET prend la confidentialité et la conformité très au sérieux. Les utilisateurs peuvent demander à ESET de supprimer les échantillons immédiatement après leur analyse via des paramètres spécifiques.

VITESSE INÉGALÉE

Le temps est un facteur essentiel pour la cybersécurité, c'est pourquoi ESET LiveGuard Advanced peut analyser la plupart des échantillons en moins de cinq minutes.

DÉFENSE PROACTIVE

Le fonctionnement des échantillons suspects est bloqué en attendant l'analyse d'ESET LiveGuard Advanced. Cela empêche les menaces potentielles de faire des ravages dans le système de l'utilisateur. Lorsque l'analyse est terminée et qu'une menace est détectée sur un endpoint, cette information est relayée en quelques minutes à tous les endpoints du réseau de l'organisation, protégeant immédiatement tout utilisateur qui aurait pu être potentiellement en danger.

DES SOUMISSIONS MANUELLES FACILES ET DES RÉSULTATS CLAIRS

Un utilisateur ou un administrateur peut soumettre à tout moment des échantillons via la console ESET Protect pour analyse, et obtenir des résultats complets. Les administrateurs verront qui a envoyé quoi, et le résultat.

PROTECTION AMÉLIORÉE DE LA MESSAGERIE

ESET LiveGuard Advanced va au-delà de l'analyse des fichiers. Il fonctionne directement avec ESET Mail Security ou ESET Cloud Office Security pour empêcher la réception d'emails malveillants dans votre organisation. Pour prendre en charge la continuité des activités, seuls les emails externes peuvent être envoyés à ESET LiveGuard Advanced pour inspection.

Cas d'utilisation

Ransomwares

PROBLÈME

Les ransomwares ont tendance à s'introduire dans les boîtes mail des utilisateurs peu méfiants via des emails.

SOLUTION

- ✓ ESET Mail Security soumet automatiquement les pièces jointes suspectes à ESET LiveGuard Advanced.
- ✓ ESET LiveGuard Advanced analyse les échantillons, puis renvoie le résultat à ESET Mail Security généralement dans les 5 minutes.
- ✓ ESET Mail Security détecte automatiquement les pièces jointes dont le contenu est malveillant, et y remédie.
- ✓ Les pièces jointes malveillantes n'atteignent jamais les destinataires.

Fichiers inconnus ou douteux

PROBLÈME

Il arrive que les collaborateurs ou le service informatique reçoivent un fichier dont ils souhaitent évaluer le danger.

SOLUTION

- ✓ Tout utilisateur peut soumettre un échantillon pour analyse directement dans tous les produits ESET.
- ✓ L'échantillon est rapidement analysé par ESET LiveGuard Advanced.
- ✓ Lorsqu'un fichier est considéré comme malveillant, tous les ordinateurs de l'organisation sont protégés.
- ✓ L'administrateur informatique dispose d'une visibilité totale sur l'utilisateur qui a soumis l'échantillon, et si le fichier était sain ou malveillant.

Protection granulaire pour les différents rôles de l'entreprise

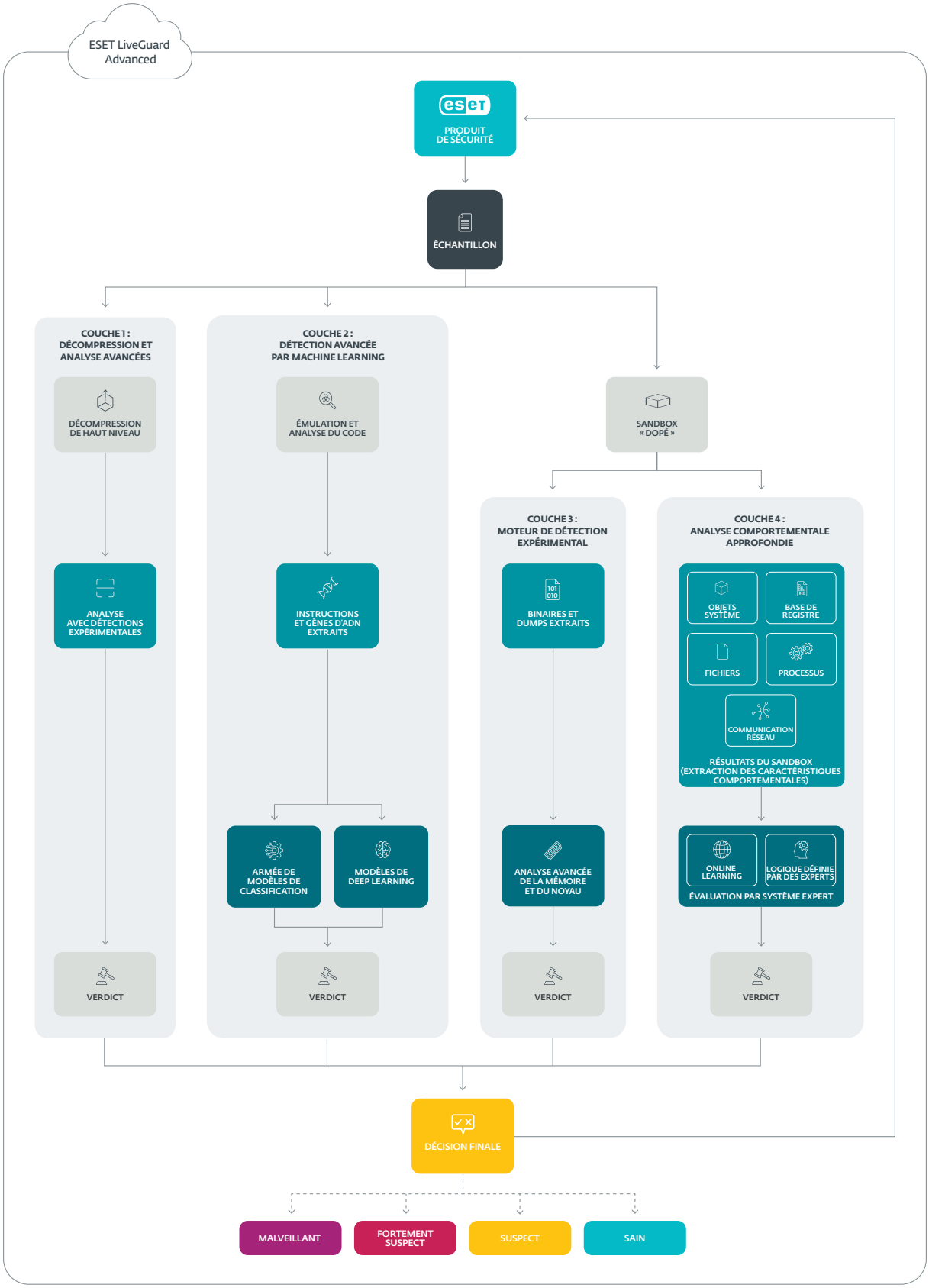
PROBLÈME

Chaque rôle dans l'entreprise nécessite des niveaux de protection différents. Les restrictions de sécurité des développeurs ou des informaticiens sont par exemple différentes de celles du directeur d'une filiale ou du PDG.

SOLUTION

- ✓ Configurez une politique de sécurité unique par ordinateur ou par serveur dans ESET LiveGuard Advanced.
- ✓ Appliquez automatiquement une politique différente basée sur un groupe d'utilisateurs statique ou un groupe Active Directory différent.
- ✓ Modifiez automatiquement les paramètres de configuration simplement en déplaçant un utilisateur d'un groupe à un autre.

Schéma de l'analyse avancée



ESET LiveGuard Advanced utilise 4 couches de détection distinctes pour assurer le plus haut taux de détection. Chaque couche utilise une approche différente et rend un verdict sur l'échantillon. L'évaluation finale comprend les résultats de toutes les informations sur l'échantillon.

COUCHE 1

Décompression et analyse avancées

Les échantillons sont soumis à une analyse statique et une décompression de pointe, puis sont comparés à une base de données de menaces.

COUCHE 2

Machine learning avancé

L'analyse statique et dynamique est réalisée par un ensemble d'algorithmes de machine learning, utilisant notamment des techniques de deep learning.

COUCHE 3

Moteur de détection expérimental

Les échantillons sont insérés dans des « sandbox dopés » qui ressemblent beaucoup aux appareils des utilisateurs grandeur nature. Ils sont ensuite surveillés pour détecter tout signe de comportement malveillant.

COUCHE 4

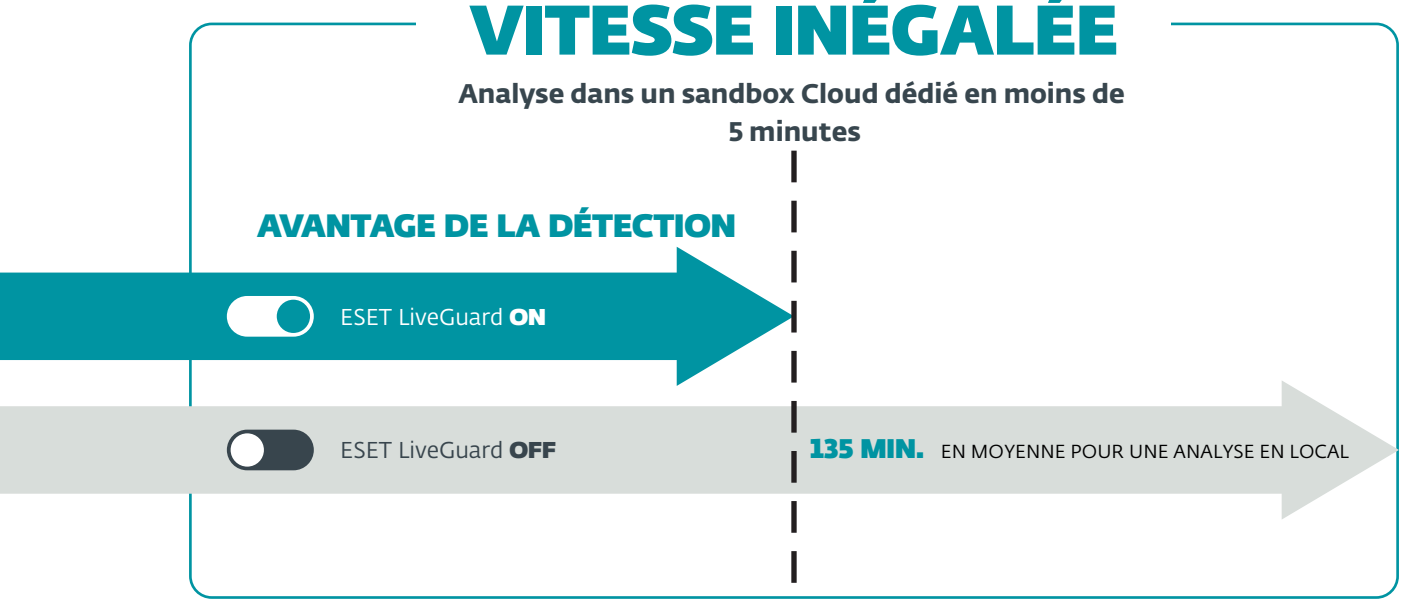
Analyse approfondie des comportements

Tous les résultats du sandbox font l'objet d'une analyse comportementale approfondie qui identifie les chaînes d'actions et les modèles malveillants connus.

LA SOLUTION COMBINE TOUS LES VERDICTS DISPONIBLES DES COUCHES DE DÉTECTION ET ÉVALUE L'ÉTAT DE CHAQUE ÉCHANTILLON. LES RÉSULTATS SONT D'ABORD TRANSMIS À L'APPLICATION DE SÉCURITÉ ESET DE L'UTILISATEUR ET À L'INFRASTRUCTURE DE L'ENTREPRISE, PUIS LES MESURES D'ATTÉNUATION CORRESPONDANTES SONT APPLIQUÉES AUTOMATIQUEMENT.

VITESSE INÉGALÉE

Analyse dans un sandbox Cloud dédié en moins de 5 minutes



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
internautes protégés

+ 400 k
entreprises clientes

200
pays et territoires

13
centres de recherche

QUELQUES-UNS DE NOS CLIENTS

MITSUBISHI MOTORS
Drive your Ambition

Protégés par ESET depuis 2017 : 9 000 endpoints

Allianz Suisse

Protégé par ESET depuis 2016 : +4 000 boîtes mail

Canon
Canon Marketing Japan Group

Protégés par ESET depuis 2016 : 32 000 endpoints

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

RECONNAISSANCES

AV comparatives APPROVED Business Security DEC 2023

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.

G2 Leader WINTER 2024

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**.

kuppingercole ANALYSTS

ESET est **reconnu comme un leader du marché** et un leader en général du MDR, selon le KuppingerCole Leadership Compass 2023.