



LIVEGUARD ADVANCED

**Défense proactive contre
les menaces zero-day et
jamais vues auparavant**

Progress. Protected.

Qu'est-ce qu'une **défense contre les menaces avancées ?**

Une technologie proactive dans le Cloud qui utilise une analyse adaptative avancée, une technologie de machine learning de pointe, de sandboxing 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 LiveGuard Advanced fournit une couche de sécurité supplémentaire pour les produits ESET tels que Mail Security, les produits Endpoints et 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 ?

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 n'ont jamais constitué 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.

Un produit proactif de détection des menaces à partir du Cloud 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, mais cela ne les protège pas de la prochaine attaque qui pourrait utiliser un tout nouveau vecteur.

L'approche d'une sandbox de sécurité 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 potentielle. Cela permet d'être beaucoup plus concluant 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.

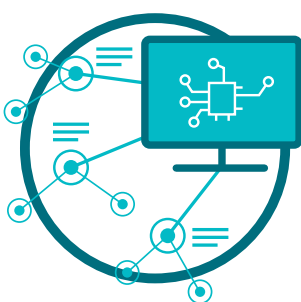
Une sandbox de sécurité dans le Cloud située à l'extérieur du réseau de l'utilisateur peut aller au-delà de la simple analyse de l'apparence et observer le comportement réel de la menace potentielle.

Les 3 piliers de nos produits et technologies



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.



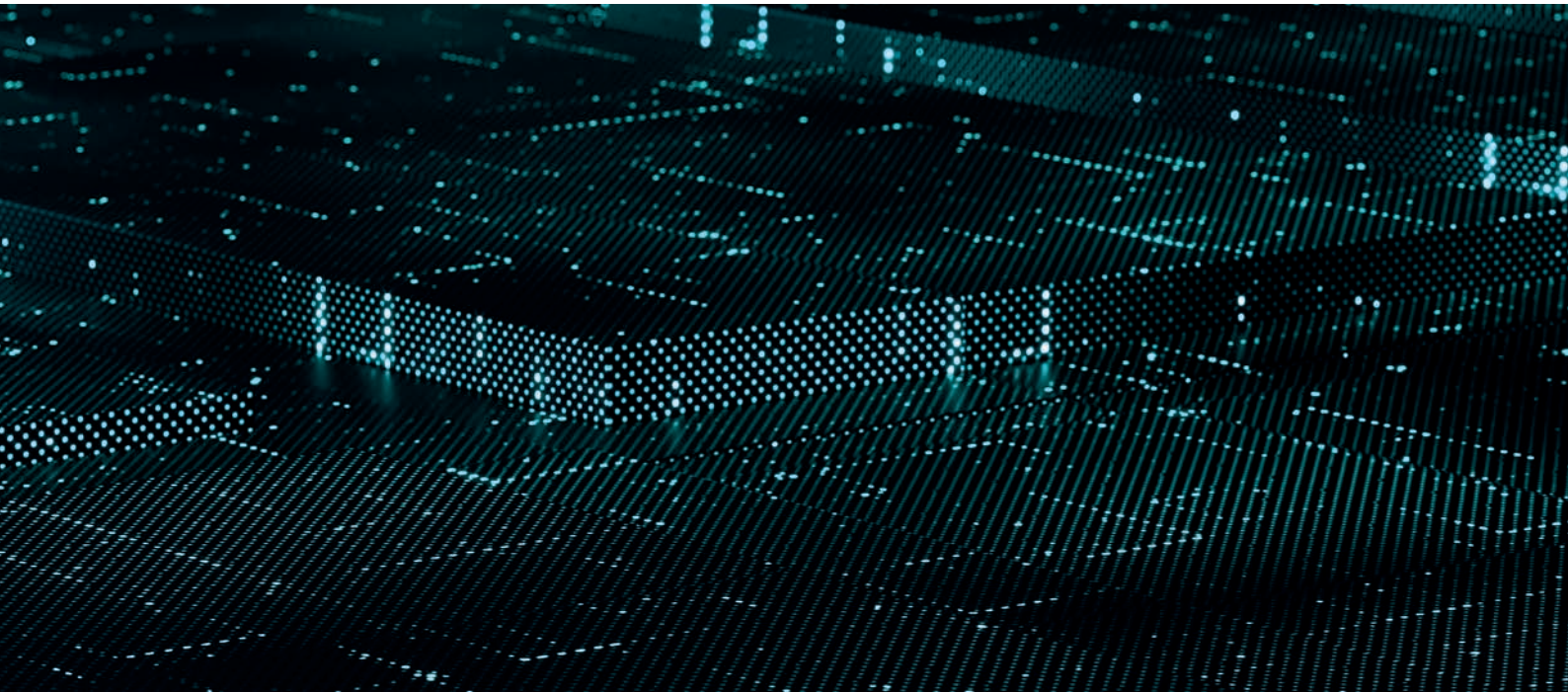
MACHINE LEARNING

La puissance combinée des réseaux neuronaux et des algorithmes développés spécialement classe correctement les échantillons entrants comme sains, potentiellement indésirables ou malveillants.



EXPERTISE HUMAINE

Des chercheurs en sécurité de renommée mondiale partagent leur savoir-faire et leurs informations afin d'assurer la meilleure veille sur les menaces 24 heures sur 24.



La différence ESET

PROTECTION MULTICOUCHE

ESET LiveGuard Advanced est une solution de défense contre les menaces à partir du Cloud, qui envoie tous les échantillons suspects soumis à un environnement de test sécurisé au siège d'ESET, dans lequel leur comportement est évalué à l'aide de flux de renseignements sur les menaces, de multiples outils internes d'ESET pour l'analyse statique et dynamique, et de données de réputation, afin de détecter les menaces zero-day. Quatre couches sont utilisées pour analyser les échantillons, qui peuvent être déployées de manière dynamique en fonction des résultats obtenus. ESET LiveGuard Advanced combine tous les verdicts des couches de détection et évalue l'état de chaque échantillon. Les résultats sont d'abord transmis à la solution de sécurité ESET de l'utilisateur et à l'infrastructure de son entreprise.

VISIBILITÉ TOTALE

Pour chaque échantillon analysé, vous pouvez consulter le résultat final dans la console d'ESET PROTECT. Les clients disposant d'une licence de plus de 100 postes obtiennent également un rapport complet contenant des informations détaillées sur les échantillons et leur comportement observé pendant l'analyse dans la sandbox, le tout sous une forme facile à comprendre. Nous présentons non seulement les échantillons qui ont été envoyés à ESET LiveGuard Advanced, mais également tout ce qui est envoyé à ESET LiveGrid®, le système de protection d'ESET dans le Cloud contre les malwares.

MOBILITÉ

Aujourd'hui, les collaborateurs des organisations travaillent de plus en plus à distance et non sur site. C'est pourquoi ESET LiveGuard Advanced peut analyser des fichiers quelle que soit la localisation des utilisateurs, et 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. Grâce à des paramètres spécifiques, l'utilisateur peut demander à ESET de supprimer les échantillons immédiatement après leur analyse.

VITESSE INÉGALÉE

Chaque minute compte, c'est pourquoi ESET LiveGuard Advanced est capable d'analyser la majorité des échantillons en moins de 5 minutes. Lorsqu'un échantillon a déjà été analysé, il suffit de quelques secondes pour que tous les appareils de votre organisation soient protégés.

ÉPROUVÉ ET FIABLE

ESET est présent dans le secteur de la sécurité depuis plus de 30 ans, et nous continuons de faire évoluer notre technologie pour conserver une longueur d'avance sur les menaces les plus récentes. En conséquence, 1 milliard d'internautes dans le monde sont désormais protégés par ESET. Notre technologie est constamment inspectée et validée par des organismes de tests impartiaux qui montrent l'efficacité de notre approche pour stopper les toutes dernières menaces.

DÉFENSE PROACTIVE

Lorsqu'un échantillon est considéré comme suspect, son fonctionnement est bloqué, dans l'attente d'une analyse par 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.

Cas d'utilisation

Ransomwares

CAS D'UTILISATION

Les ransomwares ont tendance à s'introduire dans les boîtes de messagerie 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 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.

Protection granulaire pour les différents rôles de l'entreprise

CAS D'UTILISATION

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'un bureau 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.



Fichiers inconnus ou douteux

CAS D'UTILISATION

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 étant 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 sur le fait que le fichier était sain ou malveillant.

The screenshot displays the ESET LiveGuard Advanced interface for a file analysis. At the top, the ESET logo and 'LIVEGUARD ADVANCED' are visible. The main analysis results are as follows:

- VERY SUSPICIOUS:** A red banner with a warning icon. The SHA-1 hash is 1872A482C41DC305DF0A95CCD9811B4B2AFD2C and the category is Executable.
- ADVANCED SCANNING ENGINES:**
 - Advanced Unpacking And Scanning:** A red box with a warning icon. The sample undergoes static analysis and state-of-the-art unpacking and is then matched against an enriched threat database. **Sample is malicious.**
 - Advanced Machine Learning Detection:** A green box with a checkmark icon. Static and dynamic analysis is performed by an army of machine learning algorithms, including deep learning. **Sample is clean.**
- BEHAVIORAL ANALYSIS SANDBOX:**
 - Experimental Detection Engine:** A yellow box with an exclamation mark icon. A sample is inserted into "sandboxed scenarios" that closely resemble full-scale user desktops and that are subsequently monitored for any sign of malicious behavior. **Sample is suspicious.**
 - In-Depth Behavioral Analysis:** A red box with a warning icon. The memory dumps produced by previous ETD layers are subject to an in-depth behavioral analysis that identifies known malicious patterns and chains of actions. **Sample is malicious.**
- ANALYZED BEHAVIORS:** A table showing detected behaviors:

Behavior	Status
Anti-Debug Trick	Behaviour not detected
Anti-Debug Trick	Behaviour not detected
Anti-Debug Trick	Behaviour not detected

Fonctions avancées

PROTECTION AUTOMATIQUE

Une fois que tout est configuré, aucune action n'est nécessaire de la part de l'administrateur ou de l'utilisateur. Le produit pour endpoint ou serveur décide automatiquement si un échantillon est sain, mauvais ou inconnu. Si l'échantillon est inconnu, il est envoyé à ESET LiveGuard Advanced pour analyse. Une fois l'analyse terminée, le résultat est communiqué et les produits pour endpoints réagissent en conséquence.

PERSONNALISATION SUR MESURE

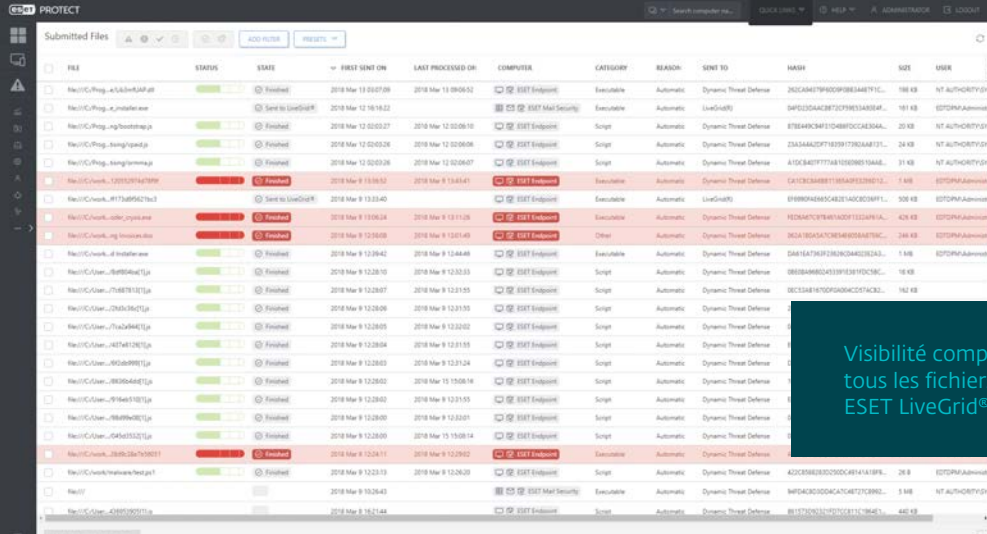
ESET permet une configuration détaillée de la politique de sécurité par ordinateur pour ESET LiveGuard Advanced, afin que l'administrateur puisse contrôler ce qui est envoyé et ce qui doit se passer en fonction du résultat reçu. Les paramètres peuvent être appliqués non seulement par ordinateur, mais également par groupe d'ordinateurs.

SOUSSION MANUELLE

Un utilisateur ou un administrateur peut soumettre à tout moment des échantillons via un produit compatible ESET pour analyse, et obtenir un résultat complet. Les administrateurs verront qui a envoyé quoi, et le résultat, directement dans la console ESET PROTECT.

PROTECTION DE LA MESSAGERIE

Non seulement ESET LiveGuard Advanced travaille sur des fichiers, mais également directement avec ESET Mail Security pour s'assurer que les emails malveillants ne soient pas livrés à votre organisation. Pour assurer la continuité des activités, seuls les emails provenant de l'extérieur de l'organisation peuvent être envoyés à ESET LiveGuard Advanced pour inspection.

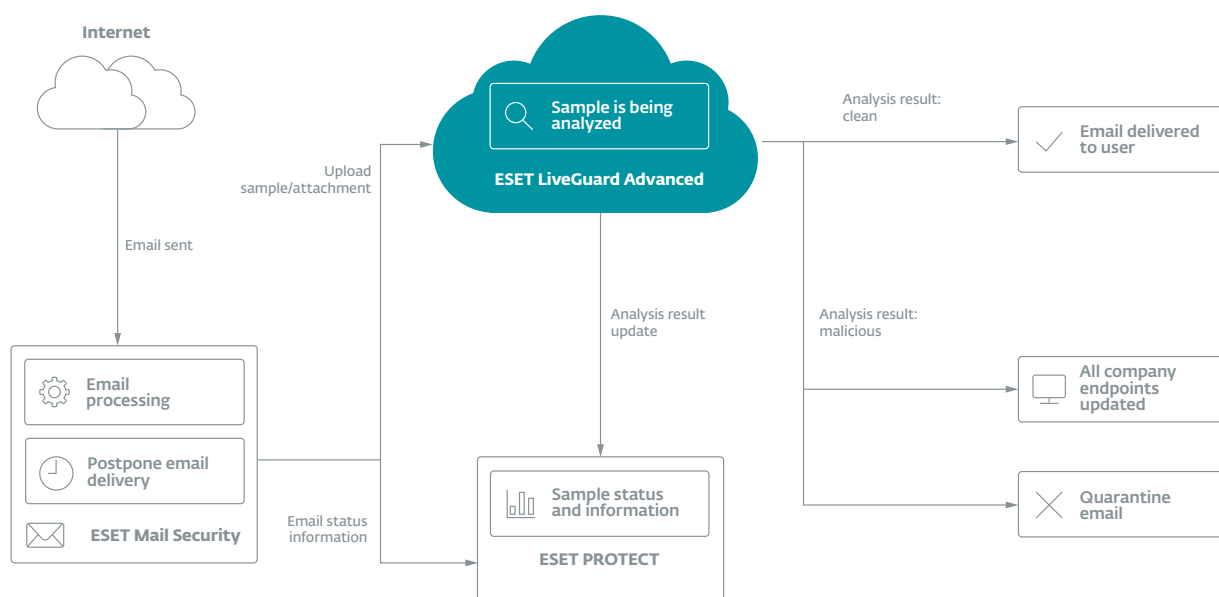


FILE	STATUS	STATE	FIRST SENT ON	LAST PROCESSED ON	COMPUTER	CATEGORY	REASON	SENT TO	HASH	SIZE	USER
Mail\CC_Prog..._a31b0a30d10d.pdf	Finished	Finished	2018 Mar 13 03:07:39	2018 Mar 13 03:08:02	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	36C8A67F9020F3B8A3A87F7C...	188 KB	NT AUTHORITY\SYSTEM
Mail\CC_Prog..._ng...bootmap.exe	Finished	Sent to LiveGrid	2018 Mar 12 16:16:22	2018 Mar 12 16:16:22	ESET Mail Security	Executable	Automatic	LiveGrid	54F5233A238752D9F834858F...	161 KB	ESETDMA\Administrator
Mail\CC_Prog..._ng...bootmap.exe	Finished	Finished	2018 Mar 12 02:03:27	2018 Mar 12 02:06:10	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	878A40C8F81048F0C8A33A...	20 KB	NT AUTHORITY\SYSTEM
Mail\CC_Prog..._dmg...imgapp.js	Finished	Finished	2018 Mar 12 02:03:26	2018 Mar 12 02:06:07	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	23A5A4D2F7E8397730A872...	24 KB	NT AUTHORITY\SYSTEM
Mail\CC_Prog..._dmg...imgapp.js	Finished	Finished	2018 Mar 12 02:03:26	2018 Mar 12 02:06:07	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	A10C84B7F774810388519A...	31 KB	NT AUTHORITY\SYSTEM
Mail\CC_Prog..._120132142738e	Finished	Finished	2018 Mar 9 13:43:52	2018 Mar 9 13:43:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	C413C13A887118A8F1328C...	1 KB	ESETDMA\Administrator
Mail\CC_Prog..._8173d9527ba3	Finished	Sent to LiveGrid	2018 Mar 9 13:33:40	2018 Mar 9 13:33:40	ESET Endpoint	Executable	Automatic	LiveGrid	8F88F8A58482145AC8C8F1...	302 KB	ESETDMA\Administrator
Mail\CC_Prog..._c08e...pygk.exe	Finished	Finished	2018 Mar 9 13:33:24	2018 Mar 9 13:31:28	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	102A67C3761A102D13228A...	429 KB	ESETDMA\Administrator
Mail\CC_Prog..._ng...troussard.exe	Finished	Finished	2018 Mar 9 12:35:08	2018 Mar 9 12:31:45	ESET Endpoint	Other	Automatic	Dynamic Threat Defense	30CA78A7C76E48803A878C...	248 KB	ESETDMA\Administrator
Mail\CC_Prog..._of...infotext.exe	Finished	Finished	2018 Mar 9 12:35:02	2018 Mar 9 12:34:48	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	D8818A74F8F283063A8232...	1 KB	ESETDMA\Administrator
Mail\CC_Prog..._8595846471a	Finished	Finished	2018 Mar 9 12:33:10	2018 Mar 9 12:33:33	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	08038A8ED43338F39C38...	18 KB	ESETDMA\Administrator
Mail\CC_Prog..._75887813171a	Finished	Finished	2018 Mar 9 12:28:07	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	8E33A81870F0A84C5743C...	162 KB	ESETDMA\Administrator
Mail\CC_Prog..._276d356d71a	Finished	Finished	2018 Mar 9 12:28:08	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._75a2a34471a	Finished	Finished	2018 Mar 9 12:28:05	2018 Mar 9 12:32:02	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._4275d13271a	Finished	Finished	2018 Mar 9 12:28:04	2018 Mar 9 12:31:53	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._8f3d8d9871a	Finished	Finished	2018 Mar 9 12:28:03	2018 Mar 9 12:31:24	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._803d8d9871a	Finished	Finished	2018 Mar 9 12:28:02	2018 Mar 9 12:31:24	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._9f4a518371a	Finished	Finished	2018 Mar 9 12:28:02	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._888d9871a	Finished	Finished	2018 Mar 9 12:28:00	2018 Mar 9 12:32:01	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._454b133271a	Finished	Finished	2018 Mar 9 12:28:00	2018 Mar 9 12:31:54	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._2a652a5200011	Finished	Finished	2018 Mar 9 12:24:11	2018 Mar 9 12:29:02	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense			
Mail\CC_Prog..._8a8d9871a	Finished	Finished	2018 Mar 9 12:23:13	2018 Mar 9 12:26:20	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	A2C8E8832050C48141A18...	28 B	ESETDMA\Administrator
Mail\CC_Prog..._4281700011a	Finished	Finished	2018 Mar 9 12:23:13	2018 Mar 9 12:26:20	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	8F770C1E1033C1C17C...	445 KB	ESETDMA\Administrator

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

Fonctionnement d'ESET LiveGuard Advanced

Avec ESET Mail Security



ESET LiveGuard Advanced est compatible avec les produits de sécurité ESET Endpoint, Server et Cloud (Microsoft 365), et est entièrement intégré aux consoles d'administration ESET.

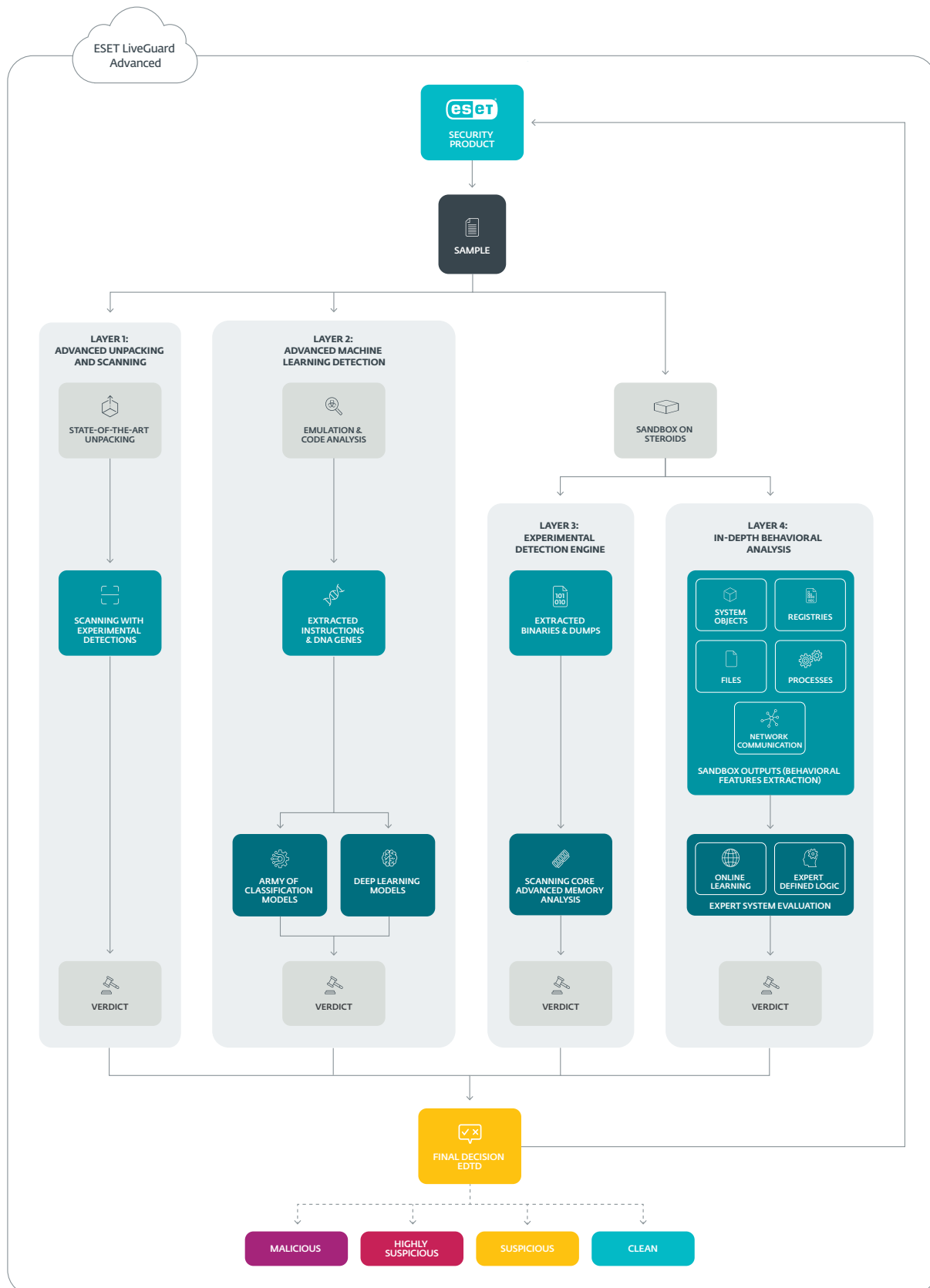
« Un produit incroyable ! »

Qu'est-ce que vous préférez ?

« J'apprécie la facilité du déploiement sur tous mes postes de travail et la rapidité avec laquelle il a sécurisé mon réseau. J'ai trouvé des logiciels indésirables et je vois passer tous les jours des emails de sa part signalant le blocage de bugs réseau avant qu'ils ne deviennent un problème. Je dors mieux en sachant que mon réseau est protégé par ESET. »

— Michael P. / Responsable réseau / ETM (51 à 1 000 employés)

Fonctionnement 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 des menaces.

COUCHE 2

Détection avancée par machine learning

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 dopées » 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 de la 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 LA SOLUTION DE SÉCURITÉ ESET DE L'UTILISATEUR ET À L'INFRASTRUCTURE DE SON ENTREPRISE.

VITESSE INCOMPARABLE



Analyse dans une sandbox dédiée dans le Cloud en moins de 5 minutes

AVANTAGE DE LA DÉTECTION



ESET LiveGuard activé



ESET LiveGuard désactivé

+ 135 min

en moyenne

À propos d'ESET

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour offrir une protection complète et multicouche contre les menaces de cybersécurité aux entreprises et aux particuliers du monde entier. ESET est depuis

longtemps un pionnier des technologies de machine learning et dans le Cloud qui préviennent, détectent et traitent les malwares. ESET est une société privée qui encourage la recherche et le développement scientifiques dans le monde entier.

ESET EN QUELQUES CHIFFRES

+ 1 milliard
d'internautes
protégés

+ 400 000
entreprises
clientes

+ 200
pays et
territoires

13
centres de
recherche

QUELQUES-UNS DE NOS CLIENTS



Protégé par ESET
depuis 2017 :
9 000 endpoints



Protégé par ESET
depuis 2016 :
+4 000 boîtes mails

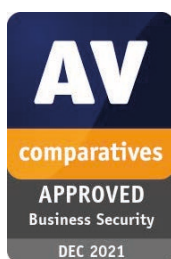


Protégé par ESET
depuis 2016 :
32 000 endpoints



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

RESPECT DES NORMES LES PLUS ÉLEVÉES



ESET a reçu le prix Business Security APPROVED de AV - Comparatives dans le cadre du test de sécurité des entreprises de décembre 2021.



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.



Les solutions ESET sont régulièrement reconnues par les principaux cabinets d'analyse, notamment dans « The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021 » en tant qu'éditeur cité en exemple.



49 rue de la vanne - 92120 Montrouge - France
commercial@eptimum-pro.com
Tél : +33. (1).77.70.05.90.