



PRÉSENTATION

THREAT INTELLIGENCE

Rapports exclusifs et flux de renseignement sur
les menaces, élaborés par les experts les plus
reconnus du secteur.

Progress. Protected.

Pourquoi ajouter ESET à votre infrastructure de CTI

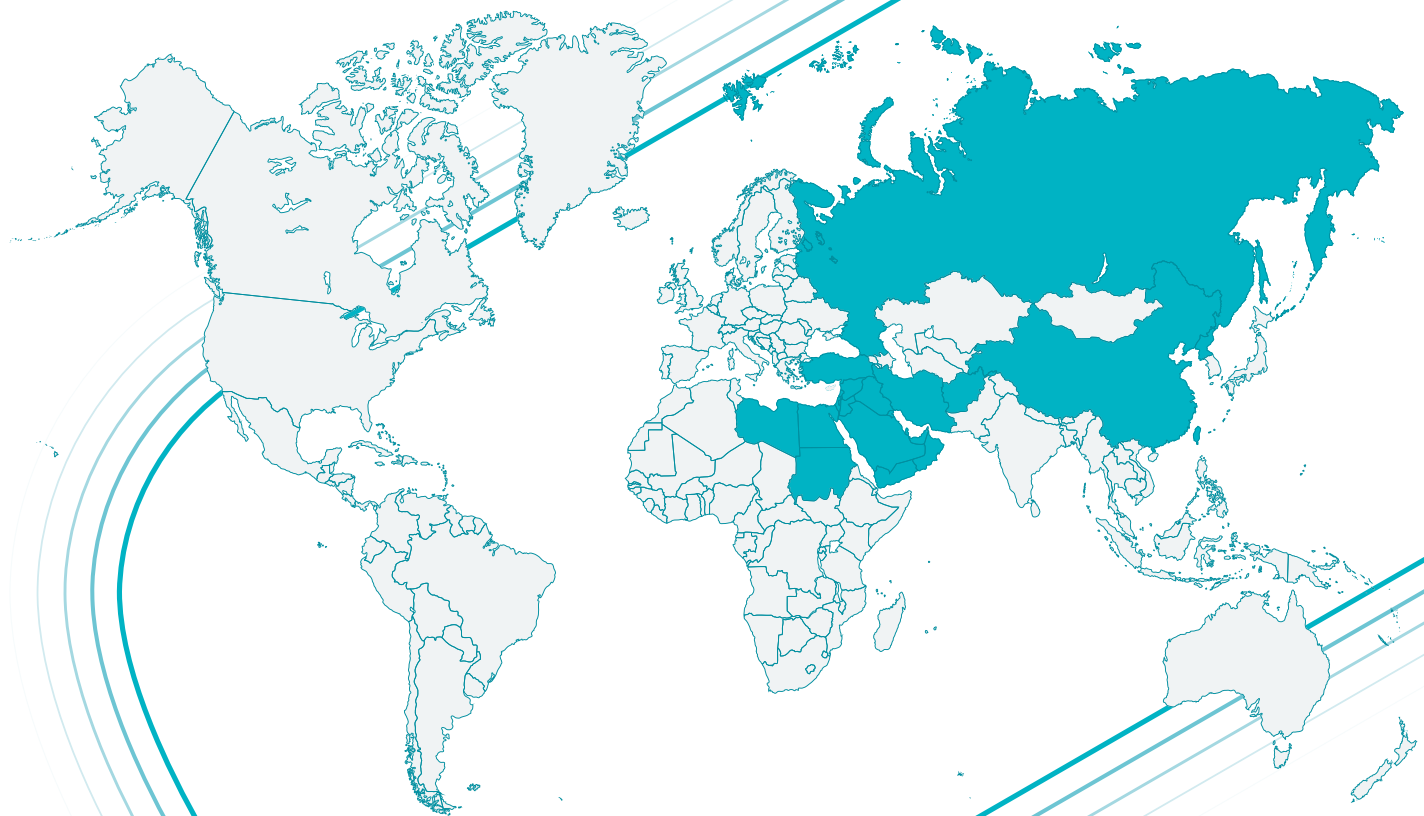
Comprendre le paysage actuel des menaces et les tactiques employées par les cyber-criminels constitue un avantage crucial en termes de connaissances. Ces informations permettent aux organisations de **renforcer efficacement leurs systèmes de défense internes**. Des renseignements de haute qualité sont la pierre angulaire de toute stratégie solide de Cyber Threat Intelligence (CTI).

Depuis plus de 35 ans, ESET est une société privée, sans dettes et en constante croissance. Notre réussite repose sur une approche « Prevention First » s'appuyant sur l'IA doublée d'une expertise humaine. Un **système unique de Threat Intelligence mondiale au cœur de nos opérations s'appuie sur un vaste réseau de R&D** dirigé par des chercheurs reconnus dans le secteur. Nous prenons le temps de bien comprendre les cybermenaces, ce qui nous permet de défendre efficacement contre elles.

Quel que soit le degré d'avancement de vos solutions actuelles de CTI, l'intégration d'**ESET dans votre infrastructure vous apportera une valeur inégalée**. Nos flux complets de Threat Intelligence et nos rapports détaillés sur les auteurs de menaces vous permettent de conserver une longueur d'avance sur les menaces émergentes, et de renforcer vos défenses existantes grâce à des informations utiles et des études de pointe.

Tirez parti de la télémétrie unique d'ESET

La présence mondiale d'ESET, développée au fil des décennies, nous permet de disposer d'une **bibliothèque de renseignements riche et diversifiée** provenant de millions de nœuds. Contrairement à de nombreux concurrents, notre télémétrie est particulièrement forte dans les régions considérées comme « **plus intéressantes** » d'un point de vue **géopolitique** dans le monde de la cyberdéfense. Cette couverture unique se traduit directement par une intelligence de haut niveau. Grâce à la télémétrie d'ESET, **vous avez accès à des informations utiles de haute qualité** qui améliorent vos moyens de détection et de réponse aux menaces.

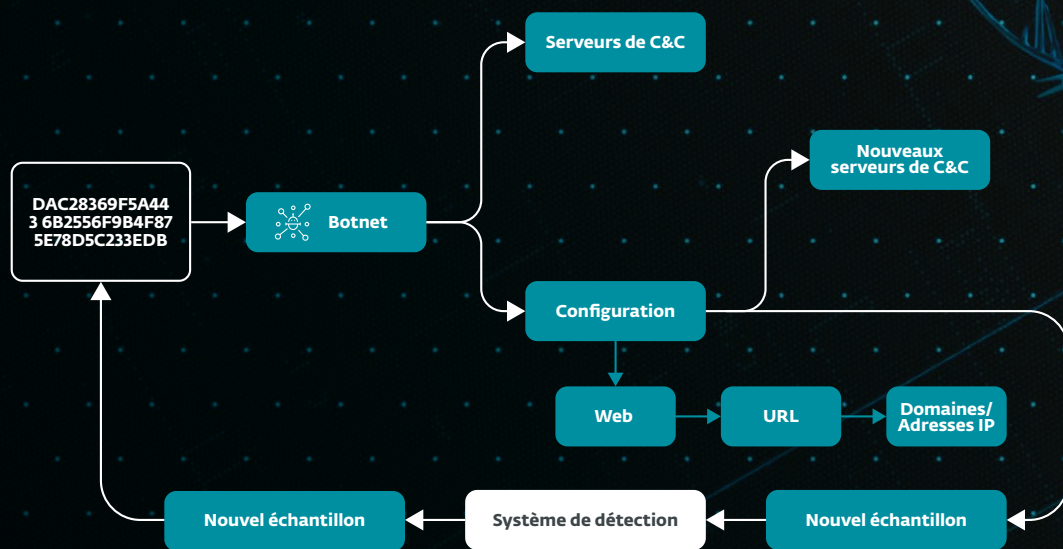


Des informations uniques et enrichies pour des décisions concrètes

La Threat Intelligence ne se limite pas à la collecte d'indicateurs et leur mise en forme ; ESET va bien au-delà. Nous utilisons des technologies de pointe et une expertise approfondie pour traiter et enrichir notre intelligence, afin de veiller à ce qu'elle apporte une valeur réelle à votre entreprise.

- 1. Télémétrie complète :** Notre intelligence utilise une vaste gamme de télémétrie générée par ESET LiveSense, notre technologie de sécurité multicouche intégrée à la plateforme ESET PROTECT. Cela garantit une collecte étendue et approfondie de données provenant de diverses sources.
- 2. Différentes méthodes de collecte :** Outre LiveSense, nous utilisons différentes méthodes de collecte et de surveillance, notamment des honeypots, des capteurs, des ressources OSINT, l'exploration du web (en clair et en profondeur) et le suivi des menaces. Il en résulte un volume important de données de haute qualité.
- 3. Traitement avancé :** Une fois collectées, toutes les données sont traitées par de robustes systèmes en back-end, qui s'appuient sur l'IA pour classer et analyser les informations automatiquement. Seules les informations les plus pertinentes et les plus utiles sont ainsi mises en avant.
- 4. Analyse d'experts :** Au-delà du traitement automatisé, notre équipe qualifiée d'analystes et de chercheurs spécialisés dans la Threat Intelligence joue un rôle crucial. Ils étudient et analysent en permanence les différents auteurs de menaces, leurs motivations, leurs TTP (tactiques, techniques et procédures) et leurs outils. Cette vérification humaine ajoute une couche supplémentaire de détails et de précision à notre intelligence, allant au-delà de ce que le machine learning et l'auto-matisation peuvent réaliser à eux seuls.





Les échantillons que nous recevons par télémétrie font l'objet d'une analyse comportementale et structurelle approfondie. Ce processus permet d'obtenir d'autres indicateurs utiles, ce qui enrichit encore notre veille sur les menaces. En examinant méticuleusement chaque échantillon, nous extrayons des informations précieuses qui améliorent la qualité et l'efficacité globales de notre intelligence, et vous permettent en retour de mieux comprendre le paysage des menaces.

Sécurité améliorée via des rapports APT détaillés

Rédigés dans un langage concis et utile pour améliorer la posture de sécurité de votre organisation, nos rapports sur les auteurs de menaces (APT) fournissent des informations détaillées sur les campagnes de malwares, leur diffusion et les acteurs impliqués. Accédez à notre serveur MISP et LiveAI, et réservez des sessions en live avec les meilleurs experts d'ESET en Threat Intelligence pour obtenir plus de renseignements.

NOS MEILLEURES ÉTUDES À VOTRE SERVICE

Notre équipe de recherche est bien connue dans le milieu de la cybersécurité grâce à notre blog primé [WeLiveSecurity](#). Les excellentes études de l'équipe et les résumés des activités des auteurs de menaces sont disponibles, avec des informations beaucoup plus détaillées. Les clients d'ESET bénéficient d'un aperçu exclusif sur la totalité du contenu de WeLiveSecurity.

UN CONTENU PERTINENT ET UTILE

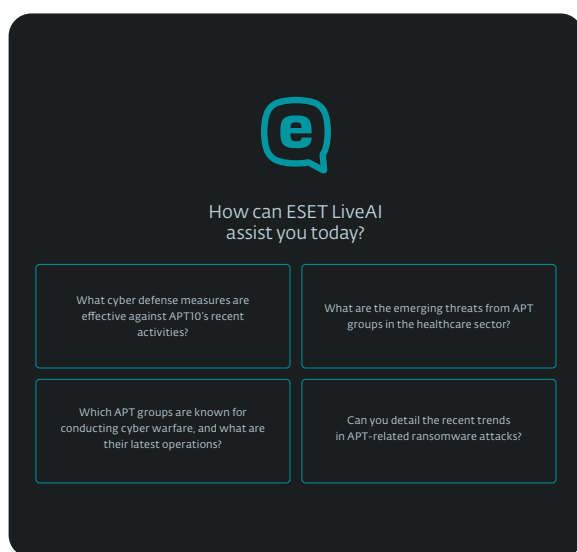
Les rapports fournissent un contexte enrichi sur ce qui se passe et pourquoi. Grâce à cela, les entreprises peuvent se préparer à l'avance à ce qui pourrait arriver. Nos experts veillent à ce que le contenu soit facile à comprendre.

PRENEZ RAPIDEMENT DES DÉCISIONS CRUCIALES

Tout cela aide les entreprises à prendre des décisions cruciales et leur procure un avantage stratégique dans la lutte contre la cybercriminalité. Elles peuvent comprendre ce qui se passe du « côté obscur d'Internet » et s'y préparer rapidement en interne.

ACCÈS À UN ANALYSTE ESET

Chaque client qui commande l'offre APT Reports Premium aura également accès à un analyste ESET pendant quatre heures par mois. C'est l'occasion de discuter de sujets plus en détail et d'essayer de résoudre les questions en suspens.



ESET LiveAI utilise une IA avancée et notre expertise sur les auteurs de menaces pour fournir des informations à la demande et des mesures de protection contre les cyberattaques. Disponible sous la forme d'un chatbot, il répond aux questions de sécurité, propose des résumés sur les auteurs de menaces, compile des IoC (Indicateurs de Compromis) et des TTP, et génère des règles YARA pour une compréhension et une prévention rapides des menaces.

		APT Reports	APT Reports Advanced	APT Reports Ultimate
Résumé d'activité bimensuel	Rapports résumant les activités de tous les groupes de pirates étudiés, tel que détaillé ci-dessus (deux rapports par mois)	✓	✓	✓
Rapports d'analyse des menaces	Analyse technique personnalisée ou régulière des menaces les plus courantes (~30 par an)	✓	✓	✓
Aperçu mensuel	Compilation mensuelle des informations avec une vue d'ensemble des menaces	✓	✓	✓
Résumé mensuel	Index et résumé exécutif des rapports et des événements du mois	✓	✓	✓
Accès en avant-première à WeLiveSecurity	Accès en avant-première aux rapports sur les menaces et à une sélection d'articles WeLiveSecurity	✓	✓	✓
Flux des IoC des auteurs de menaces	Accès complet au flux STIX/TAXII contenant les IoC des rapports	✓	✓	✓
Accès au serveur MISP	Accès complet au serveur ESET MISP contenant toutes les informations disponibles dans les rapports	✗	✓	✓
ESET LiveAI	Accès à ESET LiveAI qui fournit des informations et des résumés des rapports disponibles sur les auteurs de menaces	✗	✓	✓
Accès aux analystes	Accès aux analystes via différentes plateformes telles que Teams et la messagerie, limité à quatre heures par mois (non cumulables, y compris le temps de préparation)	✗	✗	✓

Des indicateurs au renseignement : Prendre l'avantage sur la cybercriminalité

Les rapports **ESET Threat Intelligence eCrime** offrent une analyse approfondie des ransomwares et, plus largement, des opérations de cybercriminalité. Bénéficiez d'une visibilité accrue sur les outils des attaquants, leurs infrastructures et leurs stratégies de monétisation, appuyée par la recherche mondiale et la télémétrie d'ESET. Allez au-delà des IoC pour accéder à une intelligence contextualisée qui renforce la défense proactive et la prise de décision stratégique.

Ce qui distingue les rapports ESET eCrime

DÉFENSE PROACTIVE

Accédez à une intelligence qui ne se limite pas aux groupes eCrime, mais qui couvre également les affiliés à l'origine des attaques. Comprenez leurs modes opératoires et anticipez leurs prochaines actions pour garder une longueur d'avance.

EFFICACITÉ OPÉRATIONNELLE

Exploitez des analyses claires et contextualisées issues d'incidents réels pour réduire le bruit. Facilitez la détection des menaces, accélérez les réponses et concentrez les activités de threat hunting là où l'impact est maximal.

VISIBILITÉ EXCLUSIVE

Allez au-delà des flux de menaces publics grâce à une analyse approfondie des tactiques de monétisation, des infrastructures et du comportement réel des affiliés, le tout soutenu par la recherche et la télémétrie mondiale d'ESET.

		eCrime Reports	eCrime Reports Advanced
Résumé d'activité MENSUEL	- Les dernières campagnes de ransomware et d'infostealers, synthétisées en analyses claires et stratégiques - Qui est ciblé, comment les attaques se déroulent et ce qui a échoué - Enseignements clés, IoC et recommandations pour renforcer la résilience	✓	✓
Analyses techniques MENSUEL	- Analyses approfondies de groupes de menace spécifiques (ex. : FIN7) - Chaîne d'attaque complète : de l'accès initial au vol de données - Tactiques, outils et infrastructures des attaquants, cartographie MITRE ATT&CK®, IoC	✓	✓
Résumé des tendances PÉRIODIQUE	- Vue d'ensemble prête pour les décideurs sur l'activité récente des ransomwares et des infostealers - Tendances clés, incidents marquants et menaces émergentes - Aide les directions à évaluer les risques et à définir les priorités, sans complexité technique	✓	✓
eCrime Feed	- IoC récents et qualifiés sur les groupes de ransomware, leurs affiliés et les campagnes d'infostealers - Disponibles au format standard STIX/TAXII	✓	✓
ESET LiveAI	- Exploite les analyses eCrime pour répondre aux questions liées aux menaces - Facilite l'interprétation des incidents et du comportement des attaquants - Rend la Threat Intelligence immédiatement accessible aux équipes et aux décideurs	✗	✓
Accès aux serveurs MISP	- Intégration directe avec une Threat Intelligence qualifiée - Intégration automatique des IoC pour renforcer les défenses - Optimise les workflows, accélère la détection et soutient la réponse à incident	✗	✓

Flux de données clairs et concis

Améliorez votre visibilité sur le paysage des menaces grâce à la télémétrie unique d'ESET. Nous fournissons des flux de données hautement structurés en JSON et STIX 2.1, qui s'intègrent de manière transparente dans les outils SIEM, TIP ou SOAR. Contrairement à de nombreux fournisseurs de Threat Intelligence, nous accordons une attention toute particulière afin que **nos flux soient méticuleusement filtrés et évalués** pour garantir leur pertinence. Cela permet aux systèmes de sécurité existants d'agir automatiquement en cas de besoin, et aux analystes de bénéficier d'une vue d'ensemble sur le paysage mondial des menaces.

- Des données riches en métadonnées, détaillées et préparées avec très peu de faux positifs.
- Nous veillons à ce que les données soient peu volumineuses, très pertinentes et dédoublées, avec un score de confiance.
- Le résultat du filtrage avancé, avec les observations des chercheurs d'ESET.
- Leader du marché, en particulier pour les données relatives aux botnets.
- Faibles exigences en matière d'utilisation grâce à un contenu bien structuré.
- Flux en temps réel ; uniquement des IoC récents et prévalents.

FLUX DE DONNÉES MALVEILLANTES

Des informations en temps réel sur les échantillons de malwares récemment découverts, leurs caractéristiques et les IoC. Inclut les horodatages des empreintes de fichiers et les types de menaces afin de bloquer les fichiers malveillants avant qu'ils ne causent des dommages.

FLUX RANSOMWARE

Des informations en temps réel sur les familles de ransomwares actives et les échantillons les plus répandus. Permet un blocage proactif afin de prévenir les compromissions et les interruptions coûteuses.

FLUX BOTNET

Alimenté par le tracker de botnets d'ESET, ce flux comprend trois sous-flux : botnets, C&C et cibles. Il fournit des détails de détection, des empreintes de fichiers, les horodatages des dernières communications, les fichiers téléchargés, les adresses IP, les protocoles et les informations sur les cibles.

FLUX IOC APT

Des analyses sur les menaces persistantes avancées (APT), basées sur la recherche ESET. Exportées depuis le serveur central ESET MSP et alignées avec les rapports APT. Disponibles au sein des rapports ou en tant que flux autonome.

FLUX ADWARE PUA

Fort de plus de vingt ans d'expertise dans la classification des PUA (Potentially Unwanted Applications), ESET fournit une intelligence d'une profondeur et d'une précision inégalées. Ce flux délivre des informations en temps réel sur les adwares actifs et les menaces similaires, permettant un blocage proactif avant impact.

FLUX APPLICATIONS À DOUBLE USAGE

Assure le suivi des outils légitimes (ex. : RMM) détournés par les attaquants, contribuant à rester informé de l'état de l'abus tout en réduisant le bruit grâce à des données ciblées à faible redondance.

FLUX DOMAINES

Fournit des données sur les domaines malveillants, incluant le nom de domaine, l'adresse IP et la date associée. Les domaines sont classés par niveau de sévérité, ce qui permet de prioriser les actions, comme le blocage des domaines à haut risque.

FLUX URL

Un flux qualifié d'URL spécifiques, avec des informations détaillées sur chaque adresse et son domaine d'hébergement. Il inclut uniquement des détections à forte confiance, accompagnées d'explications claires et compréhensibles pour chaque URL signalée.

FLUX IP

Fournit des données exploitables sur les adresses IP malveillantes. Sa structure est alignée avec les flux domaines et URL. Il permet d'identifier les menaces courantes, de bloquer les IP à forte sévérité, de surveiller celles à risque plus faible et d'approfondir l'analyse grâce à des données complémentaires afin d'évaluer l'impact potentiel.

FLUX MENACES ANDROID

Fournit des informations en temps réel sur les menaces Android les plus répandues et leurs IoC, permettant un blocage proactif. Issu de la télémétrie ESET, ce flux est mis à jour quasi en temps réel avec une déduplication quotidienne.

FLUX INFOSTEALERS ANDROID

Flux spécialisé au sein des menaces Android, fournissant des détails sur les échantillons d'infostealers actifs et les données associées. Il offre une visibilité sur les familles en activité et permet de les bloquer de manière proactive avant qu'elles ne causent des dommages.

FLUX URL FRAUDULEUSES

Anticipez les arnaques grâce à des données en temps réel sur les URL frauduleuses. Ce flux couvre les boutiques en ligne frauduleuses, les arnaques à l'investissement, les arnaques sentimentales et les escroqueries liées aux cryptomonnaies. Agrégé à partir de l'ensemble des sources URL d'ESET, il est mis à jour quasi en temps réel, avec une déduplication toutes les 24 heures.

FLUX ARNAQUES CRYPTO

Gardez une longueur d'avance sur les arnaques liées aux cryptomonnaies grâce à des mises à jour en temps réel sur les domaines frauduleux, les URL et les données associées. Issu de la télémétrie étendue d'ESET, ce flux fournit des informations ciblées et précoces pour bloquer les menaces de manière proactive et protéger vos actifs.

FLUX PIÈCES MALVEILLANTES JOINTES

L'e-mail constitue une cible privilégiée des attaques. Ce flux fournit des données en temps réel sur les pièces jointes malveillantes, issues de la vaste télémétrie d'analyse e-mail d'ESET.

FLUX URL DE PHISHING

Fournit une intelligence en temps réel sur les URL de phishing actives, issues de la base de données dédiée d'ESET. Mis à jour en continu avec une déduplication quotidienne, ce flux permet de détecter et de bloquer les sites frauduleux avant qu'ils ne compromettent des données sensibles.

FLUX SMISHING

Apporte des informations récentes sur le phishing par SMS (smishing), incluant les domaines, les URL et les indicateurs associés. Issu de la télémétrie étendue d'ESET, ce flux est mis à jour quasi en temps réel avec une déduplication quotidienne.

FLUX ARNAQUES SMS

Protégez-vous contre les arnaques par SMS grâce à un flux en temps réel sur les

Découvrez la puissance d'ESET Threat Intelligence

Planifiez une démonstration dès aujourd'hui et découvrez la valeur unique qu'ESET Threat Intelligence peut apporter à votre organisation. Avec un taux de renouvellement de 100 %, nos clients satisfaits témoignent de l'efficacité de nos solutions. Laissez-nous vous montrer comment renforcer vos défenses en cybersécurité.

Pas encore prêt pour une démonstration en live ?

Commencez par créer un [compte de démonstration](#) sur le portail ESET Threat Intelligence afin d'explorer les différents feeds et les rapports APT.

Voici ESET

Défense proactive. Minimisez les risques par la prévention.

Gardez une longueur d'avance sur les menaces cyber connues et émergentes, attaques ciblées, menaces zero-day, ransomwares, phishing et bien plus encore grâce à notre approche prévention-first, native de l'IA.

ESET combine la puissance de l'intelligence artificielle et l'expertise humaine pour offrir une protection simple, efficace et durable.

Bénéficiez d'une sécurité de pointe, fondée sur la science, soutenue par plus de 30 ans de recherche interne et de Threat Intelligence mondiale. Notre vaste réseau de R&D ESET, piloté par des chercheurs reconnus par l'industrie, alimente notre plateforme de cybersécurité cloud primée.

Les solutions ESET sont hautement personnalisables, intègrent un support local et ont un impact minimal sur les performances.

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

ESET EN QUELQUES CHIFFRES

+ 1 Mrd

internautes
protégés

500k+

entreprises
clientes

178

pays et
territoires

11

centres
de recherche

QUELQUES-UNS DE NOS CLIENTS



Protégé par ESET
depuis 2017 :
9 500 endpoints



Protégé par ESET
depuis 2016 :
+4 000 boîtes mail



Protégé par ESET
depuis 2016 :
23 000 endpoints



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

RECONNAISSANCES



Lauréat des prix **Best Enterprise Endpoint**
et **Best Small Business Endpoint** aux SE
LABS Awards 2025



Désigné **Customers' Choice** par Gartner®
Peer Insights™ dans le rapport "**Voice of
the Customer – Endpoint Protection
Platforms 2026**"



Reconnu comme **Leader** dans le Frost
Radar™ : Endpoint Security 2025, illustrant
l'excellence en matière de croissance et
d'innovation

Gartner and Peer Insights™ sont des marques déposées de Gartner, Inc. et/ou de ses filiales. Tous droits réservés. Le contenu de Gartner Peer Insights™ reflète les opinions d'utilisateurs finaux individuels basées sur leurs propres expériences et ne doit pas être interprété comme des faits établis, ni comme représentant les points de vue de Gartner ou de ses filiales. Gartner ne recommande aucun fournisseur, produit ou service présenté dans ce contenu et ne fournit aucune garantie, expresse ou implicite, concernant ce contenu, y compris quant à son exactitude ou son exhaustivité, ni aucune garantie de qualité marchande ou d'adéquation à un usage particulier.