L’approche préventive d’ESET mise en avant par Gartner

Cybersecurity
Progress. Protected.

L’adoption d’une cybersécurité proactive est un état d’esprit qui porte ses fruits

À mesure que la transformation numérique s’accélère, les organisations sont confrontées à une complexité croissante et une surface d’attaque qui s’étend. Les services cloud, le télétravail et l’innovation reposant sur l’IA réinventent les opérations des entreprises, mais créent également de nouvelles vulnérabilités au niveau des endpoints, de la messagerie, des applications SaaS et des réseaux.

Les acteurs de menaces évoluent rapidement et utilisent des tactiques sophistiquées telles que l’ingénierie sociale et les ransomwares générés par l’IA pour contourner les défenses traditionnelles. De nombreuses organisations manquent de visibilité sur leur surface d’attaque, ce qui les laisse exposées et dans une situation précaire.

C’est pourquoi une stratégie de cybersécurité tournée vers la prévention n’est plus facultative. Elle permet d’atténuer les menaces avancées, de réduire les coûts liés aux atteintes à la sécurité et d’assurer la continuité des opérations.

Ce document décrit comment ESET, qui est distingué par Gartner parmi les plateformes de protection des endpoints, assure la résilience et la protection des organisations dans un monde où le changement est constant.

Pourquoi la cybersécurité proactive est véritablement importante

Soyons clairs : attendre qu’une attaque se produise pour agir n’est plus une stratégie viable depuis longtemps. Le paysage des menaces évolue à un rythme qui exige de la prévoyance, de l’agilité et, surtout, de la prévention. Une posture de cybersécurité proactive n’est pas seulement un choix technique, c’est un impératif stratégique.

Évolution du paysage des menaces : la prévention est une nécessité

Il n’est pas surprenant que les cybermenaces soient de plus en plus sophistiquées, fréquentes et dommageables. Le premier semestre 2025 a vu une montée en puissance des attaques d’ingénierie sociale comme ClickFix, qui ont augmenté de 517 % et représentent désormais 8 % des menaces bloquées sur Windows, Linux et macOS..

Les voleurs d’informations tels que SnakeStealer ont supplanté les anciens malwares, doublant leur nombre de détections et représentant désormais près de 20 % de toutes les activités de vol d’informations.

Mais l'évolution la plus alarmante est sans doute l'émergence de ransomwares générés par l'IA. La découverte par ESET de PromptLock, le premier ransomware alimenté par l'IA générative, marque un tournant.

Ce malware génère des scripts malveillants en temps réel de manière autonome, décidant soit d'exfiltrer soit de chiffrer des données en fonction de requêtes prédéfinies. Les implications sont profondes : les attaquants n'ont plus besoin d'équipes de développeurs ; un modèle d'IA bien configuré suffit pour lancer des attaques complexes et adaptatives.

Rentabilité : la prévention permet d'économiser des millions

Les conséquences financières des cyberincidents sont également considérables. Selon les services de cyber-hygiène de la CISA, l'atténuation précoce des menaces peut réduire les coûts des atteintes à la sécurité jusqu'à 40 % durant les 12 premiers mois, en particulier dans le cas d'incidents à grande échelle.

Cette atténuation précoce des menaces est généralement une mesure préventive qui aide ensuite les organisations à éviter les dépenses en cascade liées à la correction des atteintes à la sécurité, aux frais juridiques, aux amendes réglementaires et aux dommages à la réputation.

Le rapport d'IBM pour 2025 a révélé que le coût moyen d'une atteinte à la sécurité des données atteignait 4,4 millions de dollars. Les coûts étaient les plus bas pour les organisations utilisant des plateformes de DevSecOps, de détection des menaces par l'IA et de SIEM. En revanche, l'IA non sanctionnée, les atteintes à la sécurité de la chaîne d'approvisionnement et les systèmes de sécurité complexes ont fait grimper les coûts, soulignant ainsi la valeur d'une cybersécurité rationalisée, intelligente et proactive.

Continuité opérationnelle : minimisation des temps d'arrêt

Les cyberattaques ne se contentent pas de compromettre les données : elles perturbent les opérations, entraînant souvent l'arrêt des activités. Et l'impact financier des temps d'arrêt varie considérablement d'un secteur à l'autre.

Comme le souligne Gartner, « Les dirigeants doivent commencer par comprendre les coûts liés aux temps d'arrêt et la perte de revenus. Par exemple, les temps d'arrêt opérationnels coûtent en moyenne 40 000 dollars par heure aux entreprises de produits de consommation emballés, et jusqu'à 3 millions de dollars par heure aux entreprises du secteur automobile ». Nous estimons que ces chiffres soulignent l'urgence de stratégies de cybersécurité proactives qui préservent la continuité de l'activité.

Des solutions telles que la surveillance en continu, la protection des endpoints et la planification de la réponse aux incidents permettent aux organisations de maintenir leurs fonctions essentielles, même sous la contrainte.

La cyber-résilience, qui associe la prévention, la détection et la récupération, n'est plus facultative : c'est un impératif stratégique pour garantir que les opérations ne se contentent pas de survivre à une attaque, mais qu'elles continuent à fonctionner.

Marque, confiance et conformité : renforcement de la confiance

Les clients et les autorités de régulation attendent des organisations qu'elles protègent les données sensibles. La cybersécurité proactive soutient directement la conformité des cadres tels que le NIST Cybersecurity Framework et HIPAA, ainsi que des réglementations telles que SOX et CCPA, qui imposent une robuste gestion des risques, le signalement des incidents et des mesures de protection techniques.

Les violations de la loi HIPAA, par exemple, peuvent coûter aux organisations jusqu'à 50 000 dollars par violation, avec des plafonds annuels atteignant 1,5 million de dollars, tandis que les affaires pénales peuvent donner lieu à des amendes de 250 000 dollars et à des peines d'emprisonnement. En vertu de la réglementation SOX, les dirigeants peuvent se voir infliger des amendes allant jusqu'à 5 millions de dollars et des peines d'emprisonnement de 20 ans pour avoir sciemment effectué de faux signalements.

Par ailleurs, la loi CCPA impose des sanctions pouvant aller jusqu'à 7 500 dollars par violation intentionnelle, un chiffre qui peut grimper rapidement en cas d'atteinte à la sécurité à grande échelle. Cependant, au-delà de l'évitement de ces amendes, la sécurité proactive permet d'instaurer la confiance. Elle indique aux clients que leurs données sont en sécurité, que leur confidentialité est respectée et que leur fidélité est appréciée.

Les coûts cachés d'une approche réactive

La détection tardive des failles de sécurité permet aux attaquants de s'infiltrer plus profondément, ce qui augmente le coût moyen jusqu'à 5,1 millions de dollars en 2025. Le rétablissement devient complexe, exigeant des ressources considérables en matière de réponse aux incidents et d'investigation numérique, souvent prises en charge par des services de DFIR coûteux. Au-delà de la remédiation technique, l'atteinte à la réputation et la perte de clientèle sont des conséquences à long terme. Selon IBM, le coût moyen mondial d'une atteinte à la sécurité des données atteint 4,4 millions de dollars.

Les incidents liés au cyber-risque peuvent avoir des conséquences considérables sur les opérations, les finances, la stratégie et la réputation. Les atteintes à la réputation causées par les failles de sécurité minent la confiance des clients et l'image de marque, ce qui se traduit souvent par une perte de clientèle à long terme et une diminution de la compétitivité sur le marché. Ces coûts cachés font que les stratégies réactives ne sont pas viables.

Stratégie axée sur la prévention

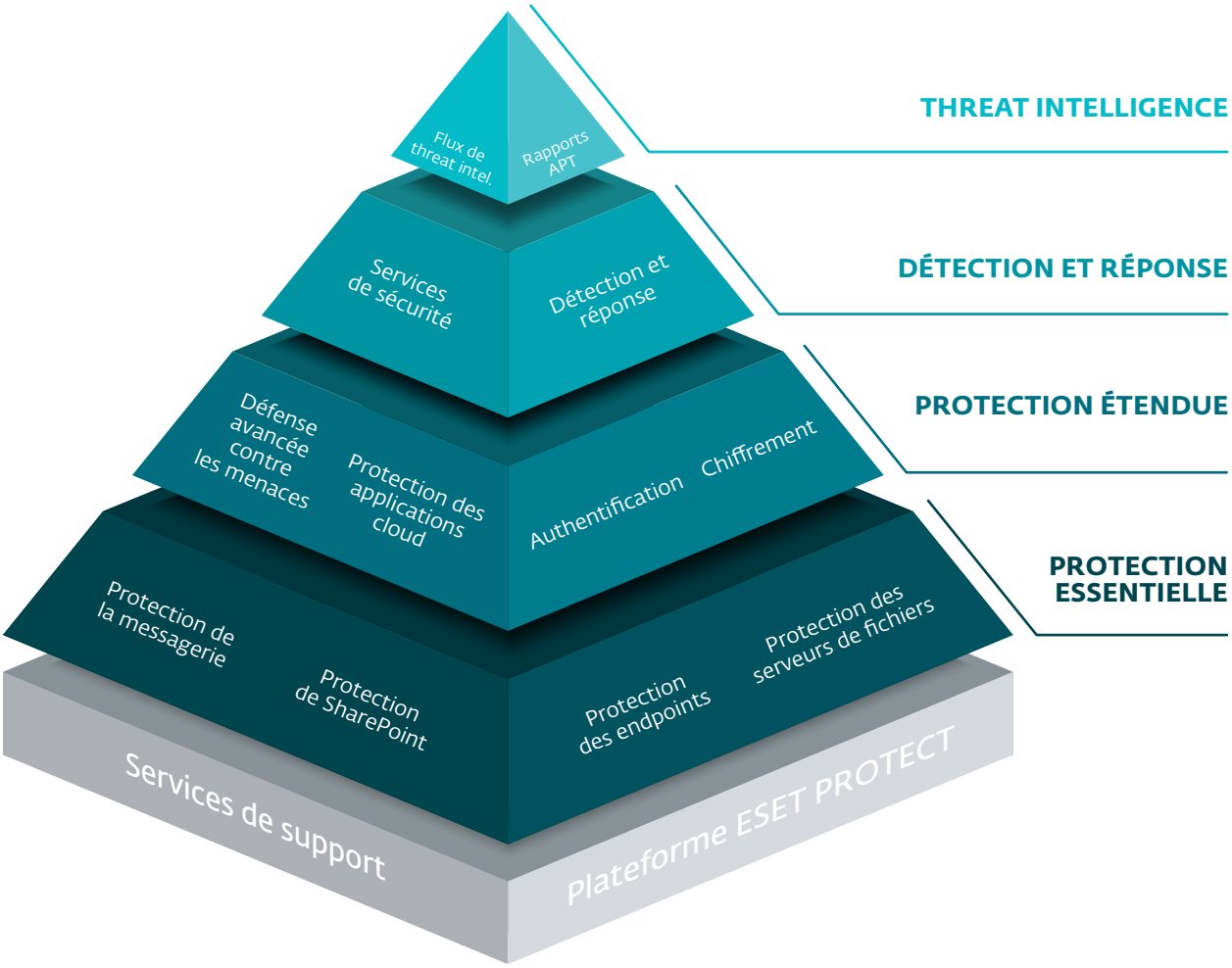
Il est possible de tenir beaucoup de résultats avec une stratégie de prévention qui aborde les problèmes de manière globale. Cependant, une prévention efficace commence par une robuste protection des endpoints. En tant que première couche de défense, elle stoppe les menaces avant qu'elles ne se propagent.

La sécurité multicouche d'ESET pour endpoints associe une heuristique avancée, le machine learning et des systèmes de réputation cloud pour bloquer les ransomwares, les exploitations de vulnérabilités et les malwares générés par l'IA, ce qui en fait la pierre angulaire d'une défense proactive.

La threat intelligence est le second pilier de la prévention, permettant une détection précoce et des décisions stratégiques. ESET Threat Intelligence fournit des flux en temps réel, des rapports APT et une visibilité approfondie sur les menaces émergentes, pour aider les équipes de sécurité à anticiper et neutraliser les attaques avant qu'elles ne prennent de l'ampleur.

La surveillance en continu et l'évaluation des risques garantissent que les menaces sont non seulement détectées, mais également contextualisées et traitées rapidement, ce qui en fait le troisième pilier d'une stratégie de prévention. ESET MDR (détection et réponse managées) offre une surveillance 24x7, une recherche des menaces et une réponse aux incidents menée par des experts, qui réduit le délai de détection et minimise l'interruption des activités.

Enfin, l'architecture zero trust renforce la couche humaine de la cybersécurité. La formation de sensibilisation à la cybersécurité d'ESET permet aux employés de reconnaître l'hameçonnage, l'ingénierie sociale et les menaces internes, en s'alignant sur les principes de sécurité zero trust qui traitent chaque demande d'accès comme potentiellement risquée, quelle qu'en soit l'origine.



Ensemble, ces piliers forment un cadre résilient et fondé sur l'intelligence, qui fait passer la cybersécurité d'une défense réactive à une prévention proactive.

Implémentation d'une défense proactive

Le pilier central : la protection des endpoints

Dans une stratégie de prévention, la protection des endpoints n'est pas une simple couche, c'est la base. La plupart des menaces trouvent leur origine au niveau de l'endpoint, ce qui en fait la première ligne de défense, et la plus critique. L'approche d'ESET en matière de protection des endpoints repose sur sa technologie propriétaire ESET LiveSense®, un cadre multicouche qui intègre des mécanismes de détection avancés, notamment les DNA Detections, l'analyse comportementale, le machine learning et les systèmes de réputation cloud.

La technologie LiveSense® d'ESET offre une protection en temps réel, intelligente et adaptative à toutes les étapes du cycle de vie des menaces. Combinée à une optimisation par l'IA reposant sur l'intelligence, elle offre d'excellentes performances avec peu de faux positifs, ce qui est idéal dans le cadre d'une main-d'œuvre moderne et distribuée.

Le royaume unificateur : la plateforme ESET PROTECT

La plateforme ESET PROTECT — notée 4,6 / 5 au 30 septembre, à partir des avis de 1 000 utilisateurs de la plateforme d'évaluation Gartner Peer Insights™ pour les fonctionnalités du produit, l'intégration et le support — étend, selon nous, cette philosophie de protection des endpoints en priorité à une console d'administration centralisée conçue pour le cloud.

Elle automatise les principaux workflows de sécurité, s'intègre de manière transparente aux plateformes de SIEM et de XDR, et prend en charge des environnements complexes (sur site, dans le cloud et hybrides). Avec une prise en charge de Windows, macOS, Linux, Android, iOS et des serveurs, elle assure une protection cohérente sur toutes les ressources.

ESET propose des niveaux d'abonnement adaptés à des menaces spécifiques : ransomwares, hameçonnage, menaces internes, attaques contre les identités, etc. Pour les environnements hautement sécurisés, la plateforme ESET PROTECT prend en charge les systèmes isolés et les exigences strictes en matière de résidence des données. Gartner reconnaît ESET comme un Challenger dans son Magic Quadrant™ de 2025 pour les plateformes de protection des endpoints.

Automatisation et outils avancés

L'automatisation est également un élément clé d'une défense proactive. ESET Vulnerability and Patch Management et l'outil Ransomware Remediation récemment lancé permettent un retour en arrière automatisé et une récupération des fichiers à partir de sauvegardes sécurisées, même lorsque les acteurs de menaces tentent de corrompre les points de restauration du système.

Ces outils réduisent les coûts de remédiation et le délai de réponse, renforcent la résilience et empêchent les attaques de dégénérer en véritables crises, ce qui donne aux équipes de sécurité le temps de se concentrer sur la prévention, et pas seulement sur le nettoyage.

Sécurité d'Office dans le cloud

Les clients peuvent également compter sur ESET Cloud Office Security qui protège les applications Microsoft 365 et Google Workspace — Exchange, OneDrive, SharePoint, Gmail et autres — contre le spam, l'hameçonnage et les menaces zero-day. Fonctionnant entièrement dans le cloud, la solution offre une protection évolutive et multitenant avec sandboxing via ESET LiveGuard Advanced, pour assurer la continuité des activités et une collaboration sécurisée.

En tant que couche de prévention, elle bloque les menaces avant qu'elles n'atteignent les boîtes mail des utilisateurs ou le stockage dans le cloud, réduisant ainsi les risques de ransomwares, d'hameçonnage et de pertes de données. Cela est particulièrement utile dans les environnements de travail distants et hybrides, où les applications cloud sont des points d'entrée fréquents pour les attaquants.

Reconnaissance par un cabinet d'analystes du secteur

La plateforme d'ESET Endpoint Protection continue d'être reconnue par Gartner. Dans différents rapports comparatifs et de réflexion, nous pensons qu'ESET a été reconnu comme un fournisseur de cybersécurité compétent et de confiance, en particulier pour les organisations à la recherche d'une protection fiable, flexible et bien prise en charge pour les endpoints.

ESET est reconnu dans le Magic Quadrant 2025 de Gartner

Dans le Magic Quadrant for Endpoint Protection Platforms de Gartner pour 2025, ESET a été nommé Challenger pour son offre ESET PROTECT. À notre avis, cette reconnaissance reflète non seulement la mise en œuvre cohérente d'ESET, mais également sa vision stratégique dans un paysage de menaces qui évolue rapidement.

Nous sommes convaincus que cette reconnaissance dans le Magic Quadrant démontre l'engagement d'ESET à fournir de la valeur grâce à l'innovation, l'excellence opérationnelle et une compréhension approfondie des besoins des clients.

Selon Gartner, les challengers proposent des produits matures de protection des endpoints qui répondent efficacement aux besoins des acheteurs de plateformes de protection pour endpoints. Ils disposent également d'une forte visibilité sur le marché, ce qui leur confère une meilleure capacité d'exécution que les acteurs de niche. Cependant, les challengers sont souvent moins rapides à répondre aux besoins émergents, n'intègrent pas les produits en profondeur et peuvent avoir accumulé une dette technique, ce qui nuit à la facilité d'utilisation. Ils peuvent également ne pas être en phase avec la direction du marché, ce qui a un impact sur l'exhaustivité de leur vision par rapport aux leaders. Les challengers sont des choix pratiques, en particulier pour les clients qui ont établi des relations stratégiques avec eux.

ESET est un fournisseur établi dans la Voix du Client de Gartner pour la catégorie des plateformes de protection des endpoints en 2025

Depuis son lancement en octobre 2015, Gartner Peer Insights a recueilli plus de 300 000 avis vérifiés sur plus de 330 marchés technologiques, offrant aux acheteurs un point de vue unique partagé par des pairs sur les performances des fournisseurs. La Voix du Client est un document qui applique une méthodologie aux analyses agrégées de Gartner Peer Insights sur un marché afin de fournir une perspective globale aux décideurs informatiques.

Cette perspective agrégée des pairs, ainsi que les évaluations détaillées individuelles, peuvent également compléter les études générées par des experts, comme les Magic Quadrants et les Market Guides. Elle peut jouer un rôle clé dans votre processus d'achat, car elle se concentre sur les expériences directes des pairs en matière d'achat, de mise en œuvre et d'exploitation d'une solution.

Dans le rapport Gartner® Peer Insights™ Voix du Client de 2025 pour la catégorie des plateformes de protection des endpoints (EPP), **ESET a été nommé fournisseur établi sur le marché global des EPP**. ESET a une note globale de 4,8 sur 5, basée sur 68 avis au 30 septembre 2025.

Nous estimons que cette reconnaissance souligne les performances exceptionnelles d'ESET et son engagement de longue date à élaborer des solutions qui répondent efficacement aux défis de la cybersécurité dans tous les secteurs. En se concentrant sur les besoins des clients, l'excellence technique et la fiabilité opérationnelle, ESET continue d'apporter de la valeur aux organisations de toutes tailles.

Avis de non-responsabilité Peer Insights : Les contenus Gartner Peer Insights sont des opinions d'utilisateurs finaux individuels qui s'appuient sur leur propre expérience des fournisseurs listés sur la plateforme, et ne devraient pas être considérés comme étant des déclarations de faits ni des opinions de Gartner ou de ses affiliés. Gartner n'endosse aucun fournisseur, produit ou service décrit dans ce contenu et n'offre aucune garantie, explicite ou implicite, concernant ce contenu, son exactitude ou son exhaustivité, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier.

Une confiance qui s'étend à toutes les secteurs et les régions

ESET jouit de la confiance d'utilisateurs issus d'un large éventail de secteurs d'activité et de zones géographiques. Selon le rapport Gartner Peer Insights Voix du Client de 2025 :

- 37 % des avis proviennent du secteur public, de l'administration et de l'éducation
- 21 % proviennent des services et 10 % de la santé
- Les 32 % restants représentent d'autres secteurs

ESET se distingue parmi l'Éventail des fournisseurs de Gartner pour les plateformes de protection des endpoints en 2025

Un document Éventail des fournisseurs synthétise les analyses de Gartner Peer Insights en informations utiles pour les acheteurs d'informatique d'entreprise. Il leur offre une visibilité sur le paysage des fournisseurs d'un marché étudié par Gartner, sur la base des fournisseurs que les pairs évaluateurs ont pris en compte et sélectionnés dans leur processus d'achat.

Les fournisseurs sélectionnés ou considérés comme les plus fréquents sur un marché sont inclus dans le graphique de l'Éventail des Fournisseurs. Cette perspective agrégée des pairs peut être utilisée en conjonction avec d'autres études publiées par Gartner pour faciliter le processus de présélection et d'achat de technologies. Les fournisseurs mentionnés dans le rapport sont classés en trois catégories :

- Sélection ciblée
- Équilibré
- Considération générale

ESET est reconnu comme un fournisseur équilibré

Dans l'édition 2024 de l'Éventail des Fournisseurs de Gartner pour les plateformes de protection des endpoints, ESET a été reconnu comme un fournisseur équilibré ; une désignation donnée aux fournisseurs qui, à notre avis, sont fréquemment considérés et sélectionnés par rapport à d'autres sur le marché.

Nous pensons que cette reconnaissance confirme qu'ESET est régulièrement sélectionné et choisi par les acheteurs qui évaluent les plateformes de protection des endpoints, ce qui reflète à la fois sa force technique et la confiance du marché.

Ce retour d'information renforce le fait que la défense proactive n'est pas seulement une question de technologie, mais aussi de valeur. L'approche d'ESET allie rentabilité, fiabilité opérationnelle et proximité avec le client, ce qui, selon nous, en fait un choix privilégié pour les organisations qui recherchent à la fois protection et partenariat.

Rapport de Gartner sur les Moyens Critiques pour les plateformes de protection des endpoints en 2025

Un document sur les Moyens Critiques est une analyse comparative qui évalue les produits ou les services concurrents par rapport à un ensemble de différentiateurs critiques identifiés par Gartner. Il vous montre quels produits ou services sont les mieux adaptés à différents cas d'utilisation et vous donne des conseils pratiques sur les produits/services à ajouter à votre liste de fournisseurs en vue d'une évaluation plus approfondie.

Ce rapport complète le Magic Quadrant de Gartner en approfondissant les fonctionnalités des produits, leur souplesse de déploiement et leurs atouts opérationnels, ce qui permet aux acheteurs de se faire une idée plus précise de la manière dont les solutions répondent à leurs besoins spécifiques.

ESET PROTECT : taillé pour toutes les tailles d'entreprises

La solution d'ESET est conçue pour offrir une protection fiable sans complexité inutile, ce qui la rend idéale pour les organisations qui accordent la priorité à l'efficacité, la conformité et la continuité.

Options de déploiement flexibles

ESET PROTECT propose un ensemble de modèles de déploiement pour répondre aux différents besoins en infrastructure :

- Administration hybride : options sur site et dans le cloud
- Disponibilité mondiale : Amérique du Nord, Europe et Asie
- Toutes connectivités prises en charge : fonctionne efficacement dans des environnements où l'accès à Internet est limité ou intermittent.

Points forts et cas d'utilisation idéaux

ESET PROTECT se distingue par l'efficacité de sa protection, offrant constamment d'excellentes capacités de prévention et de détection dans différents environnements. Sa console d'administration dans le cloud est à la fois intuitive et puissante, pour permettre aux équipes de sécurité de gérer efficacement les endpoints sans complexité inutile.

Son architecture d'administration hybride mature est ce qui distingue véritablement ESET. Que la solution soit déployée dans le cloud, sur site ou en configuration hybride, ESET assure la continuité et la conformité, même dans les environnements à faible connectivité ou isolés. Cette flexibilité en fait un choix fiable pour les organisations soumises à des exigences réglementaires strictes ou des contraintes opérationnelles.

En ce qui concerne les cas d'utilisation, ESET PROTECT est particulièrement bien adapté aux organisations qui ont besoin d'une protection fiable et légère des endpoints sans sacrifier les performances ou la facilité d'administration. Elle convient parfaitement aux environnements où la gouvernance des données et la conformité réglementaire ne sont pas négociables, tels que l'administration, la santé et la finance.

Pour les entreprises qui n'ont pas besoin d'une prise en charge étendue des systèmes d'exploitation, mais qui exigent stabilité, simplicité et sécurité, ESET offre une solution convaincante. Sa capacité à fonctionner efficacement dans des environnements à l'architecture ou à la bande passante limitées en fait un outil idéal pour les équipes distribuées, les bureaux distants et les secteurs où les politiques d'infrastructure sont strictes.

Conclusion

Dans le paysage dynamique des menaces d'aujourd'hui, la cybersécurité n'est plus seulement un défi technique, c'est un impératif stratégique pour l'entreprise. Les organisations doivent aller au-delà de la défense réactive et adopter un état d'esprit proactif, axé sur la prévention, afin de protéger leurs opérations, leurs données et leur réputation.

Nous pensons qu'ESET, reconnue par Gartner dans de nombreux rapports, offre une combinaison convaincante d'excellence technique, de fiabilité opérationnelle et d'innovation centrée sur le client. Protection multicouche des endpoints, threat intelligence, plateforme d'administration conçue pour le cloud, outils d'automatisation avancés : ESET propose une solution unifiée adaptée aux besoins modernes.

Que vous soyez une entreprise de taille moyenne à la recherche d'une protection économique ou une organisation internationale évoluant dans des environnements réglementaires complexes, ESET vous offre la flexibilité, la confiance et la performance nécessaires pour devancer les menaces en constante évolution.

Comme le montre la reconnaissance de Gartner, ESET n'est pas seulement un fournisseur, c'est un partenaire de cybersécurité qui aide les organisations à renforcer leur résilience, réduire les risques et prospérer dans un monde où le changement est la seule constante.

Attribution :

Gartner, Inc. Magic Quadrant pour les plateformes de protection des endpoints. Evgeny Mirolyubov, Deepak Mishra, Franz Hinner. 14 juillet 2025

Gartner, Inc. Voix du Client pour les plateformes de protection des endpoints. Contributeurs de la communauté des pairs. 23 mai 2025

Clause de non-responsabilité concernant les marques :

GARTNER est une marque commerciale déposée et une marque de service de Gartner, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays, et est utilisée ici avec autorisation. Tous droits réservés. MAGIC QUADRANT et PEER INSIGHTS sont des marques déposées de Gartner, Inc. et/ou de ses filiales, et sont utilisées ici avec autorisation. Tous droits réservés.

Clause de non-responsabilité en matière d'objectivité :

Gartner ne cautionne aucun fournisseur, produit ou service décrit dans ses publications d'études, et ne conseille pas aux utilisateurs de technologie de choisir uniquement les fournisseurs les mieux notés ou désignés. 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.

À propos d'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 protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie. Progress. Protected.

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat intelligence de renommée mondiale

Support local et personnalisé

eset
Cybersecurity
Progress. Protected.