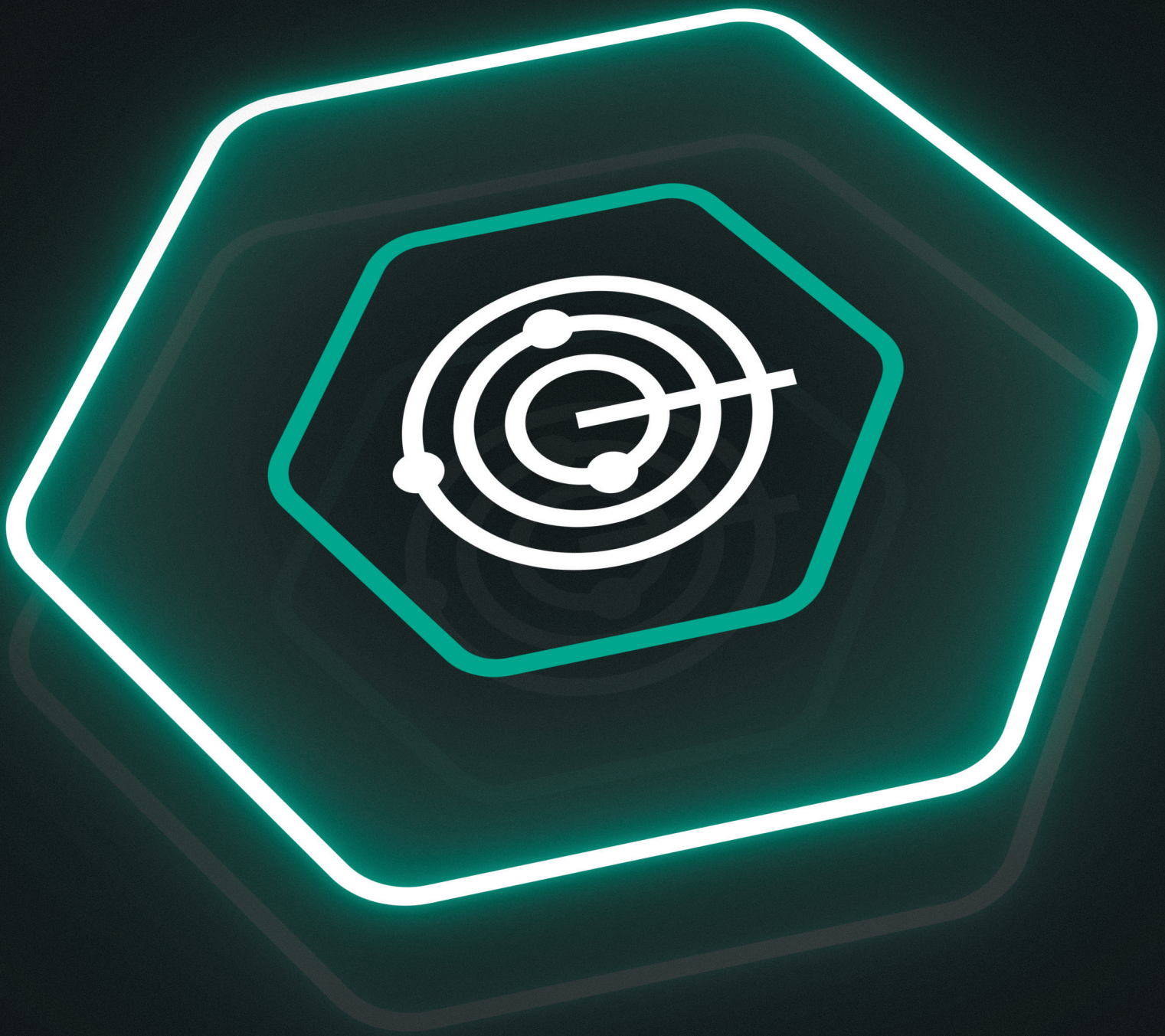


Plateforme Kaspersky Anti Targeted Attack

kaspersky BRING ON THE FUTURE

Les cybercriminels actuels se spécialisent en permanence dans la conception de méthodes uniques et novatrices de pénétration et de compromission de systèmes. Comme les menaces continuent à évoluer et à devenir plus sophistiquées et dévastatrices, il est devenu primordial de les détecter rapidement et d'y répondre de la manière la plus rapide et la plus appropriée.

Il est essentiel que les entreprises continuent à repenser leur protection en matière de sécurité informatique

afin de garder une longueur d'avance sur le nombre croissant de cybermenaces et de limiter les pertes financières.

Cybersécurité inégalée dans une solution unifiée

De nos jours, les cybercriminels professionnels privilégient une approche multi-vectorielle. La plateforme Kaspersky Anti Targeted Attack combine des fonctionnalités avancées de détection de menaces et d'EDR au niveau du réseau, tout en apportant aux spécialistes de la sécurité informatique l'ensemble des outils dont ils ont besoin pour gérer une détection multidimensionnelle supérieure de menaces, appliquer des technologies de pointe, mener des enquêtes efficaces, rechercher les menaces de manière proactive et réagir rapidement et de manière centralisée, le tout grâce à une solution unique.

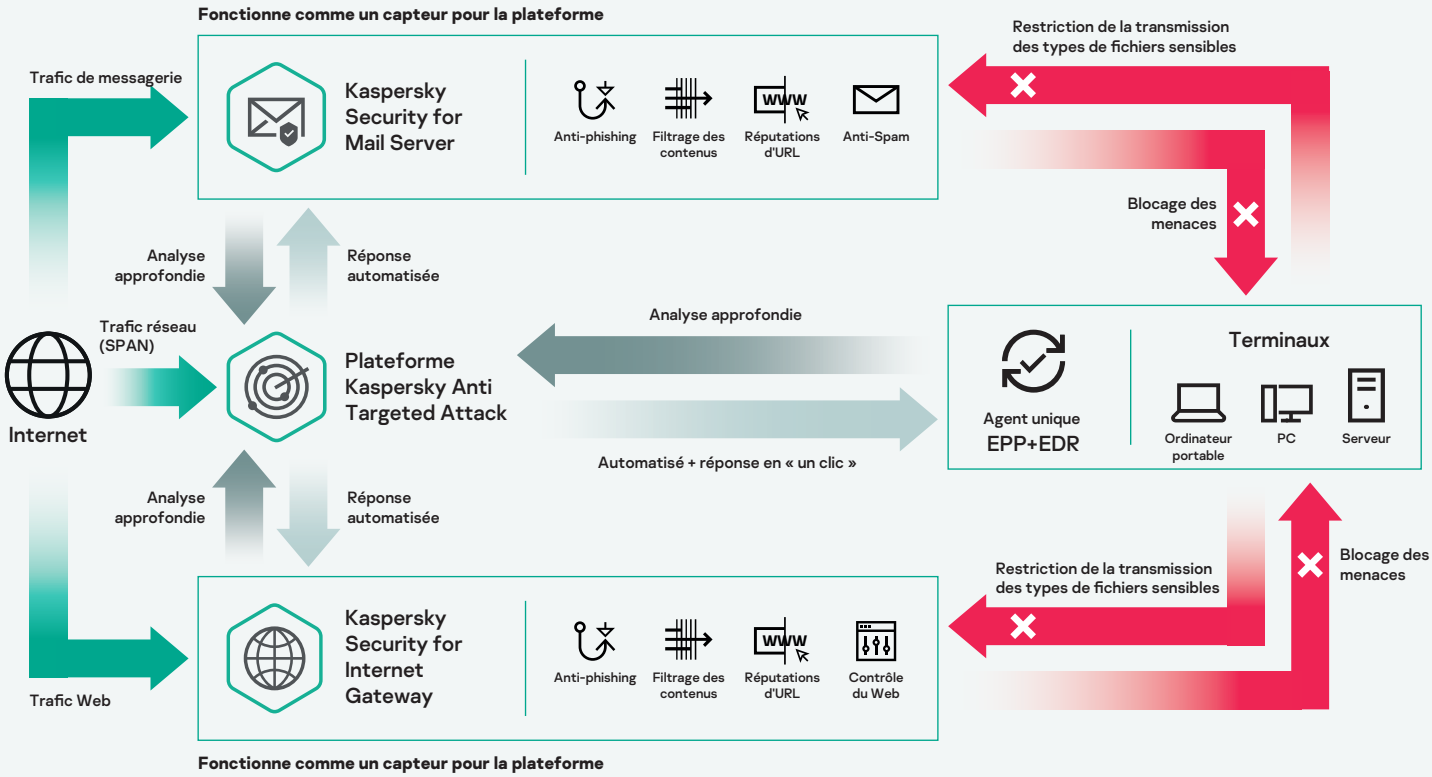
Les attaques les plus sophistiquées portées à votre attention et sous votre contrôle

La plateforme agit comme une solution de détection et d'intervention étendue offrant une protection tout-en-un contre les APT, alimentée par notre service de surveillance des menaces et connectée à l'infrastructure MITRE ATT&CK. Tous les points d'entrée des menaces (réseau, Web, messagerie, PC, ordinateurs portables, serveurs et machines virtuelles) sont sous votre contrôle.

La plateforme Kaspersky Anti Targeted Attack est entièrement intégrée à **Kaspersky Endpoint Security for Business** et partage un agent unique avec Kaspersky EDR. Elle est également intégrée à **Kaspersky Security for Mail Server** et à **Kaspersky Security for Internet Gateway**, qui servent de capteurs à la plateforme, fournissant une réponse automatisée aux menaces plus complexes transmises par email et par le Web.

Plateforme Kaspersky Anti Targeted Attack :

- **RÉDUCTION** du temps nécessaire à l'identification et au blocage des menaces
- **SIMPLIFICATION** de l'analyse des menaces et de la réponse aux incidents
- **ÉLIMINATION** des failles de sécurité et réduction des temps d'arrêt dus aux attaques
- **AUTOMATISATION** des tâches manuelles pendant la détection des menaces et l'intervention
- **ALLÈGEMENT** de la charge de travail du personnel des services informatiques, lui permettant de se consacrer à d'autres tâches essentielles
- **MISE EN CONFORMITÉ** totale avec la réglementation



Une solution de sécurité fiable et totalement confidentielle

Toutes les analyses d'objets sont effectuées sur site, sans flux de données sortantes, et Kaspersky Private Security Network fournit des mises à jour de réputation entrantes en temps réel tout en préservant l'isolation complète des données de l'entreprise.

Une plateforme unifiée pour accélérer l'innovation dans la transformation numérique grâce à ce qui suit :

- **Continuité intégrale des activités.** Nous intégrons la sécurité et la conformité dans les nouveaux processus dès le début
- **Visibilité totale** de votre infrastructure informatique d'entreprise
- **Flexibilité maximale** permettant un déploiement dans les environnements physiques et virtuels, là où la visibilité et le contrôle sont nécessaires
- **Automatisation des tâches de détection des menaces et d'intervention**, et optimisation de la rentabilité de votre sécurité, de votre réponse aux incidents et de vos équipes SOC
- **Intégration étroite et simple** avec les produits de sécurité existants, ce qui améliore les niveaux de sécurité globaux et protège l'investissement dans les anciens produits de sécurité

Principales fonctionnalités :

Architecture de capteurs multi-niveaux : une visibilité à 360 degrés grâce à une combinaison de capteurs réseau, Web et email, et d'agents de terminaux.

Moteurs avancés de détection des menaces : utilisation de données provenant de capteurs réseau (analyse du trafic réseau) et d'agents de terminaux (fonctionnalités EDR) pour des résultats rapides et moins de faux positifs.

Sandbox avancée : fournit un environnement sûr pour l'analyse approfondie de l'activité des menaces, prenant en charge la randomisation des composants du système d'exploitation, l'accélération du temps dans les machines virtuelles, les techniques anti-évasion, la simulation de l'activité des utilisateurs et la mise en correspondance des résultats avec la base de connaissances MITRE ATT&CK, le tout en contribuant à une détection hautement efficace reposant sur le comportement.

Analyse rétrospective : proposée même dans les situations où les terminaux compromis sont inaccessibles ou lorsque les données ont été chiffrées, grâce à la collecte automatisée des données, des objets et des résultats, et au stockage centralisé.

Deux modes d'interaction de la surveillance des menaces : comparaison automatisée avec les données de réputation mondiale du réseau Kaspersky Security Network, et requêtes manuelles de recherche des menaces et d'enquête via le portail Kaspersky Threat Intelligence.

Recherche des menaces automatique en temps réel : les événements sont corrélés à un ensemble unique d'indicateurs d'attaque (IoA) générés par les chercheurs de menaces Kaspersky et mis en correspondance avec la matrice MITRE ATT&CK, fournissant des descriptions d'événements, des exemples et des recommandations de réponse clairs.

Recherche proactive des menaces grâce à notre outil puissant et flexible de création de requêtes : les analystes peuvent élaborer des requêtes complexes pour rechercher des comportements atypiques et des activités suspectes ainsi que des menaces propres à votre infrastructure.

Pour résumer

Protection fiable des données, sécurité de l'infrastructure informatique, stabilité des processus commerciaux et conformité sont aujourd'hui des conditions préalables au développement durable des entreprises.

La plateforme Kaspersky Anti Targeted Attack aide les entreprises matures en matière de sécurité informatique à mettre en place des systèmes de défense fiables qui protègent leur infrastructure contre les menaces de style APT et les attaques ciblées. En outre, ces systèmes répondent aux exigences de conformité réglementaire, sans exiger de ressources supplémentaires en matière de sécurité informatique. Les incidents complexes sont rapidement identifiés, étudiés et traités, ce qui augmente l'efficacité de votre équipe de sécurité informatique en la déchargeant des tâches manuelles, grâce à une solution unifiée qui maximise l'utilisation de l'automatisation et la qualité des résultats.

La solution éprouvée la plus efficace de l'industrie

SE Labs a testé la plateforme Kaspersky Anti Targeted Attack contre une série d'attaques de piratage **et nous a attribué une classification triple A**.

Dans le test indépendant « ICSA Labs : Test de défense contre les menaces avancées (T3 2019) », la plateforme Kaspersky Anti Targeted Attack **a enregistré un taux de détection de 100 % sans aucun faux positif**.

Radicati Group place Kaspersky parmi **les leaders dans son Market Quadrant 2020 pour la protection contre les menaces APT**.

Le Gartner Peer Insights Customers' Choice pour les solutions EDR 2020 désigne Kaspersky comme le meilleur fournisseur

Kaspersky est l'un des six seuls fournisseurs au monde à être reconnu par le Gartner Peer Insights Customers' Choice pour les solutions EDR en 2020 – le témoignage ultime de la reconnaissance des clients de Kaspersky EDR – la plateforme Kaspersky Anti Targeted Attack comprenant Kaspersky EDR en son cœur.

Décharge de responsabilité de Gartner

Gartner Peer Insights Customers' Choice est le reflet d'avis subjectifs provenant d'évaluations, de classements et de données d'utilisateurs finaux individuels, appliqués à une méthodologie documentée. Il ne reflète pas le point de vue de Gartner ou ses sociétés affiliées, ni ne constitue une approbation de leur part.

Qualité de la détection confirmée par l'évaluation MITRE ATT&CK

Kaspersky EDR, l'élément central de la plateforme Kaspersky Anti Targeted Attack, a participé à la phase 2 de l'évaluation MITRE (APT29) et a démontré des performances élevées dans la détection des principales techniques ATT&CK appliquées à des étapes cruciales d'attaques ciblées modernes.

Pour en savoir plus, rendez-vous sur kaspersky.fr/MITRE

Pour en savoir plus sur la plateforme Kaspersky Anti Targeted Attack, consultez le site suivant :

kaspersky.com/enterprise-security/anti-targeted-attack-platform

Actualités sur les cybermenaces : securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security

www.kaspersky.fr

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûr où la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur kaspersky.fr/transparency

Proven. Transparent. Independent.