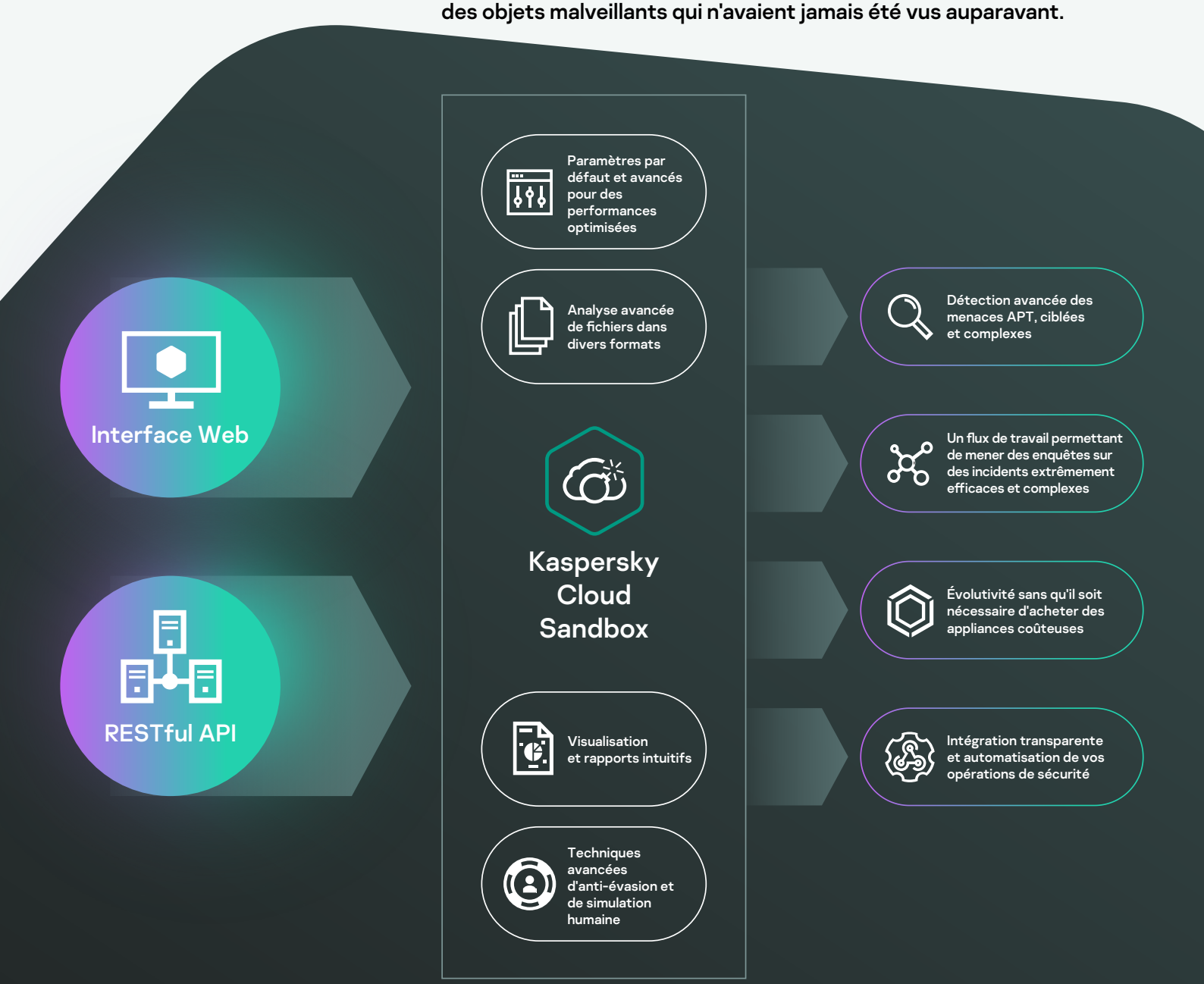
Kaspersky Cloud Sandbox

kaspersky BRING ON THE FUTURE

Kaspersky Cloud Sandbox

Il est impossible d'éviter les attaques ciblées d'aujourd'hui uniquement avec les outils antivirus traditionnels. Les moteurs antivirus sont uniquement capables d'arrêter les menaces connues et leurs variations, tandis que d'ingénieux cybercriminels utilisent tous les moyens à leur disposition pour se soustraire à la détection automatique. Les pertes provenant d'incidents relatifs à la sécurité des informations continuent de croître de manière exponentielle, soulignant l'importance croissante des capacités de détection immédiate pour assurer une réponse rapide et contrer la menace avant que des dommages importants ne soient causés.

Prendre une décision intelligente basée sur le comportement d'un fichier tout en analysant simultanément la mémoire du processus, l'activité réseau etc. est l'approche optimale pour comprendre les menaces sophistiquées, ciblées et personnalisées les plus récentes. Alors que les données statistiques peuvent manquer d'informations sur les programmes malveillants récemment modifiés, les technologies de sandboxing sont des outils puissants qui permettent d'enquêter sur l'origine d'un échantillon de fichier, de collecter des indicateurs de compromission basés sur l'analyse comportementale et de détecter des objets malveillants qui n'avaient jamais été vus auparavant.



Génération de rapports complets

- Chargement et exécution des DLL
- Connectivités externes avec noms de domaine et adresses IP
- Création, modification et suppression de fichiers
- Informations détaillées de Threat Intelligence avec contexte exploitable pour chaque indicateur de compromission révélé (IoC)
- Décharges de mémoire de processus et de trafic réseau (PCAP)
- Requêtes et réponses HTTP et DNS
- Création d'extensions mutuelles (mutex)
- API compatible REST
- Modification et création des clés du registre
- Processus créés par le fichier exécuté
- Captures d'écran
- **etc.**

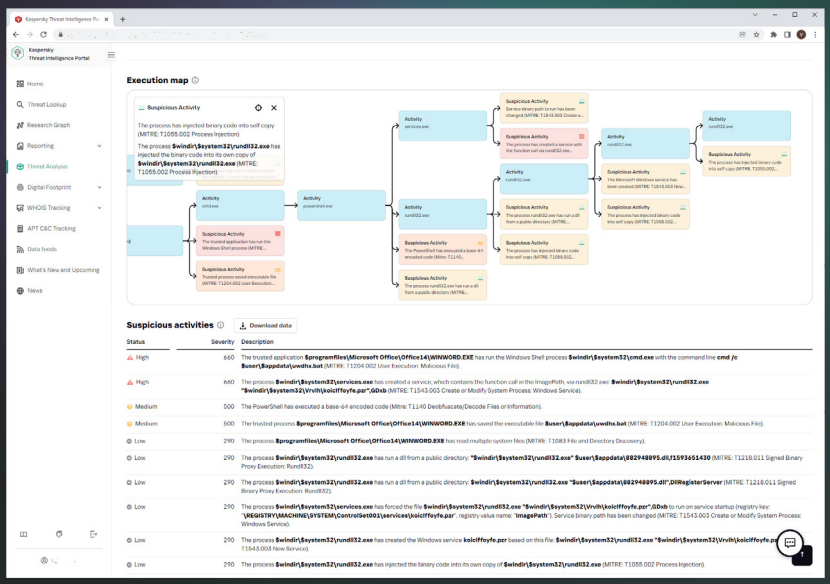
Détection et atténuation proactives des menaces

Les logiciels malveillants utilisent un large panel de méthodes pour attaquer sans être détectés. Si le système ne respecte pas les paramètres requis, le programme malveillant s'autodétruira certainement, ne laissant aucune trace. Pour que le code malveillant s'exécute, l'environnement de sandboxing doit être capable d'imiter avec précision le comportement normal de l'utilisateur final.

La Kaspersky Cloud Sandbox offre une approche hybride combinant la Threat Intelligence glanée à partir de pétaoctets de données statistiques (grâce à Kaspersky Security Network et à d'autres systèmes propriétaires), l'analyse comportementale et l'anti-évasion, avec des technologies de simulation humaine telles que le sélecteur automatique, le défilement des documents et des processus factices.

Ce produit a été développé dans notre laboratoire sandbox interne, pendant plus d'une décennie. La technologie intègre toute notre connaissance des comportements malveillants gagnée pendant 20 ans de recherche continue sur les menaces. Cela nous permet de détecter plus de 360 000 nouveaux objets malveillants chaque jour et d'offrir à nos clients des solutions novatrices en termes de sécurité.

Dans le cadre de notre Threat intelligence Portal, Cloud Sandbox est le composant important dans votre flux de travail pour la Threat intelligence. Tandis que le portail récupère les dernières informations détaillées de Threat Intelligence sur les URL, les domaines, les adresses IP, les hachages de fichiers, les noms des menaces, les données statistiques/comportementales, les données WHOIS/DNS, etc., la Cloud Sandbox permet de relier ces connaissances aux indicateurs de compromission générés par l'échantillon analysé.



Vous pouvez désormais mener des enquêtes très efficaces et complexes sur les incidents pour acquérir une compréhension immédiate de la nature de la menace, puis tirer des conclusions à mesure que vos recherches révèlent les indicateurs de menace interconnectés.

L'inspection peut être très gourmande en ressources, surtout lorsqu'il s'agit d'attaques à plusieurs niveaux. Kaspersky Cloud Research Sandbox stimule la réponse aux incidents et les activités de cyberdiagnostic, en vous offrant l'évolutivité nécessaire pour traiter automatiquement les fichiers sans avoir à acheter des appliances coûteuses ou à vous soucier des ressources système.

www.kaspersky.fr