kaspersky PRÊTS POUR L'AVENIR

# Kaspersky Sandbox

## Des capacités de détection avancées pour se protéger contre les menaces inconnues et difficilement détectables, sans avoir à embaucher des professionnels de la sécurité informatique

**Les cyberattaques avancées actuelles sont capables de paralyser les entreprises et de faire des ravages au niveau financier et de leur réputation. Le vol d'actifs financiers et de secrets commerciaux, la perte de confiance des clients due à l'indisponibilité des services et de nombreux autres effets négatifs des menaces complexes ont de graves répercussions sur la stabilité et la prospérité des entreprises. Pour prévenir la rapide évolution des cyberattaques, les outils traditionnels conçus pour protéger le périmètre réseau (pare-feu, passerelles de messagerie/Web, serveurs proxy), ainsi que les postes de travail et les serveurs (antivirus et solutions de type plate-forme de protection des terminaux avec des fonctionnalités de base), sont insuffisants. C'est pourquoi les entreprises tournées vers l'avenir doivent sérieusement envisager des outils spécialisés pour détecter, enquêter et répondre aux incidents complexes.**

### La solution Kaspersky Sandbox est adaptée pour :

- Les entreprises sans équipe de sécurité dédiée, dans lesquelles le rôle de la sécurité informatique est assigné au département informatique.
- Les petites entreprises ne souhaitant pas se procurer des ressources supplémentaires en matière de sécurité informatique.
- Les grandes organisations disposant d'une infrastructure géographiquement dispersée et sans spécialiste de la sécurité informatique sur place.
- Les entreprises devant s'assurer que leurs analystes de la sécurité informatique se concentrent entièrement sur les tâches critiques.

Depuis plus de vingt ans, Kaspersky conçoit des outils de protection pour les entreprises de toutes tailles, de tous secteurs et de tous niveaux de maturité en matière de sécurité informatique. Grâce à la recherche, au développement continus et aux progrès que nous avons réalisés pour déceler, enquêter et répondre aux menaces, Kaspersky demeure à l'avant-garde de la lutte contre la cybercriminalité.

Le portefeuille de produits et de services de Kaspersky pour lutter contre les menaces complexes comprend :

- Kaspersky Anti Targeted Attack, une solution performante pour détecter et enquêter sur les menaces complexes et les attaques ciblées au niveau du réseau.
- Kaspersky Endpoint Detection and Response, une solution de détection, d'enquête et de réponse aux cybermenaces complexes visant les postes de travail et les serveurs
- Kaspersky Threat Intelligence Portal, qui permet d'accéder à Cloud Sandbox, avec des rapports analytiques sur les menaces APT et d'autres services

Toutefois, pour utiliser efficacement ces solutions et services, les entreprises ont besoin d'un service de sécurité informatique complet, doté de l'expérience et de l'expertise appropriées. La pénurie mondiale de spécialistes formés pour faire face à des menaces complexes et le coût de leur embauche constituent souvent le principal facteur qui empêche les entreprises d'acquérir ce type de solutions et de services.

Basé sur une technologie brevetée (brevet n° US 10339301B2), Kaspersky Sandbox aide les entreprises à lutter contre le nombre et la complexité croissants des menaces modernes susceptibles de contourner la protection existante des terminaux. En complément des fonctionnalités de Kaspersky Endpoint Security for Business, Kaspersky Sandbox permet aux entreprises de considérablement augmenter le niveau de protection de leurs postes de travail et de leurs serveurs contre les programmes malveillants inconnus, les nouveaux virus et les ransomwares, les exploits « zero-day » et bien autres, sans avoir besoin d'analystes hautement spécialisés dans la sécurité des informations.

Cette solution évite aux petites entreprises d'avoir à recruter et à embaucher ces professionnels très prisés. Elle aide également les grandes entreprises disposant de réseaux distribués à optimiser les coûts pour une protection efficace de leurs bureaux à distance tout en allégeant la charge de travail manuel des analystes de sécurité.

**Options de livraison et de déploiement :**
Kaspersky Sandbox est fourni sous forme d'image ISO, avec CentOS 7 préconfiguré et tous les composants nécessaires à la solution. Il peut être déployé sur un serveur physique ou sur des serveurs virtuels basés sur VMware ESXi.

**Intégration :**
- Les systèmes SIEM peuvent recevoir des informations sur les détections effectuées par Kaspersky Sandbox. Ces informations sont envoyées via Kaspersky Security Center dans le flux général d'événements.
- Une API est implémentée dans Kaspersky Sandbox pour l'intégration avec d'autres solutions, ce qui permet d'envoyer des fichiers à Kaspersky Sandbox pour analyse et de lui demander des réputations de fichiers.

**Évolutivité**
La configuration de base prenant en charge jusqu'à 1 000 terminaux protégés, la solution s'adapte facilement et assure ainsi une protection continue des grandes infrastructures

**Mise en cluster**
Plusieurs serveurs peuvent être mis en cluster pour plus de capacité et une disponibilité élevée.

# Comment ça fonctionne ?

Kaspersky Sandbox exploite nos bonnes pratiques expertes dans la lutte contre les menaces complexes et les attaques APT et est étroitement intégré à Kaspersky Endpoint Security for Business. Il est géré depuis Kaspersky Security Center, notre console d'administration unifiée basée sur des stratégies.

L'agent Kaspersky Endpoint Security for Business demande des données sur un objet suspect au cache opérationnel partagé des résultats, situé sur le serveur Kaspersky Sandbox. Si l'objet a déjà été analysé, Kaspersky Endpoint Security for Business reçoit le résultat et applique une ou plusieurs options de correction :

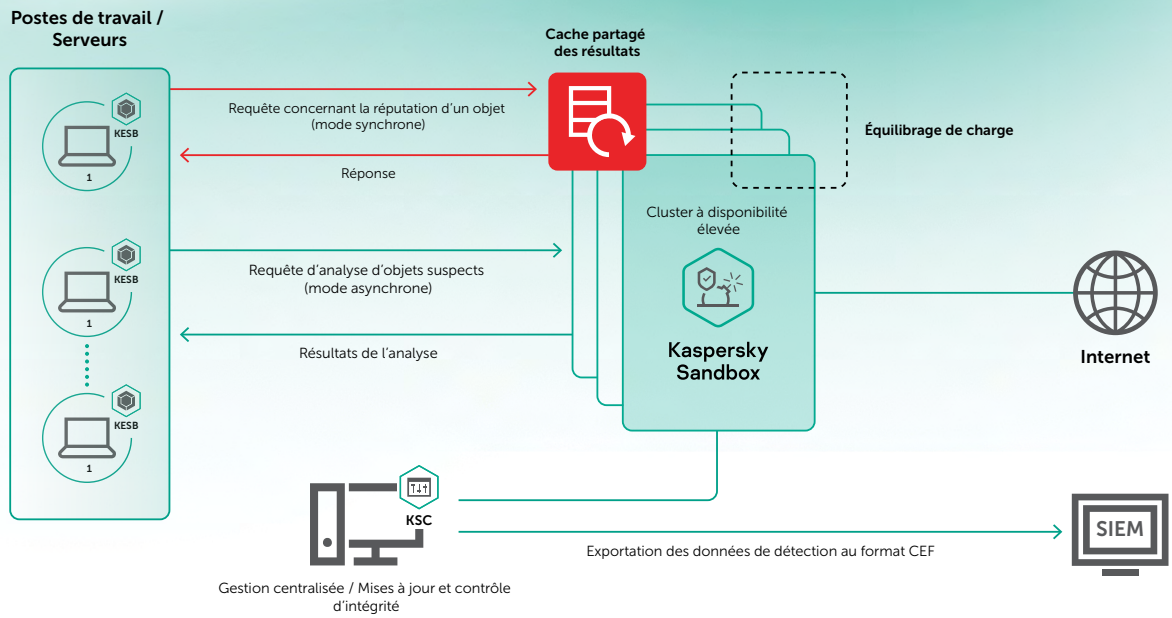
- Supprimer et mettre en quarantaine
- Avertir l'utilisateur
- Lancer une analyse des zones critiques
- Rechercher l'objet détecté sur d'autres ordinateurs du réseau géré.

Si le résultat concernant la réputation d'un objet ne peut pas être obtenu à partir du cache, l'agent Kaspersky Endpoint Security for Business envoie le fichier suspect à la sandbox en attente d'une réponse. La sandbox reçoit une demande d'analyse de l'objet, et l'objet à tester est alors exécuté dans un environnement isolé de l'infrastructure réelle.

L'analyse de fichiers est effectuée dans des machines virtuelles équipées d'outils qui émulent un environnement de travail typique (systèmes d'exploitation/applications installées). Pour détecter l'intention malveillante d'un objet, une analyse comportementale est effectuée, des artefacts sont collectés et analysés, et si l'objet effectue des actions malveillantes, la sandbox le reconnaît comme un programme malveillant. Lors de l'analyse en sandbox, un résultat est attribué à l'objet.

Une fois le processus d'émulation d'objet terminé, le résultat est envoyé en temps réel dans le cache opérationnel partagé des résultats, ce qui permet à d'autres hôtes équipés de Kaspersky Endpoint Security for Business d'obtenir rapidement des données sur la réputation de l'objet analysé sans devoir analyser à nouveau le même fichier. Cette approche assure un traitement rapide des objets suspects, réduit la charge sur les serveurs Kaspersky Sandbox et améliore la rapidité ainsi que l'efficacité de la réponse aux menaces.

**Kaspersky Sandbox** est un ajout essentiel à Kaspersky Endpoint Security for Business. Il bloque automatiquement les menaces avancées, inconnues et complexes sans avoir besoin de ressources supplémentaires et allège la charge de travail des analystes de la sécurité informatique pour leur permettre de se concentrer sur d'autres tâches.




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

**www.kaspersky.fr**

© 2020 AO Kaspersky Lab.
Les marques déposées et les marques de service sont la propriété de leurs détenteurs respectifs.

**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.