Solution complète pour la détection et la suppression des programmes malveillants

Kaspersky Scan Engine

kaspersky BRING ON THE FUTURE

Introduction

Kaspersky Scan Engine (KSEn) vous offre la meilleure solution de détection des menaces de sa catégorie, qui peut être intégrée dans presque toutes les applications.

Kaspersky Scan Engine (KSEn) offre une protection complète pour les portails et les applications Web, les serveurs proxy, le stockage en réseau et les passerelles de messagerie.

Cette solution est facile à gérer et à déployer via HTTP et ICAP en tant que service autonome, cluster évolutif ou conteneur Docker. KSEn utilise les dernières méthodes de détection pour détecter et supprimer les logiciels malveillants, notamment les chevaux de Troie, les menaces de phishing, les vers, les rootkits, les logiciels espions et les logiciels publicitaires.

Scénarios d'intégration

- Portails Web et serveurs cloud
- Serveurs de fichiers
- Périphérique de stockage en réseau
- Serveurs de messagerie
- Passerelles Web et proxy
- Boutiques d'applications et places de marché

Fonctionnalités clés

Deux modes principaux

Via un service de type REST, qui reçoit les requêtes HTTP d'applications clientes, analyse les objets transmis à ces requêtes et renvoie les réponses HTTP avec les résultats de l'analyse.

Service ICAP qui analyse le trafic HTTP passant par un serveur proxy / NAS / pare-feu d'applications Web / NGFW / toute autre solution communiquant par le protocole ICAP. Ce modèle d'intégration permet également d'analyser les URL demandées par les utilisateurs. Les pages Web présentant un contenu malveillant, de phishing ou de logiciels publicitaires sont alors filtrées.

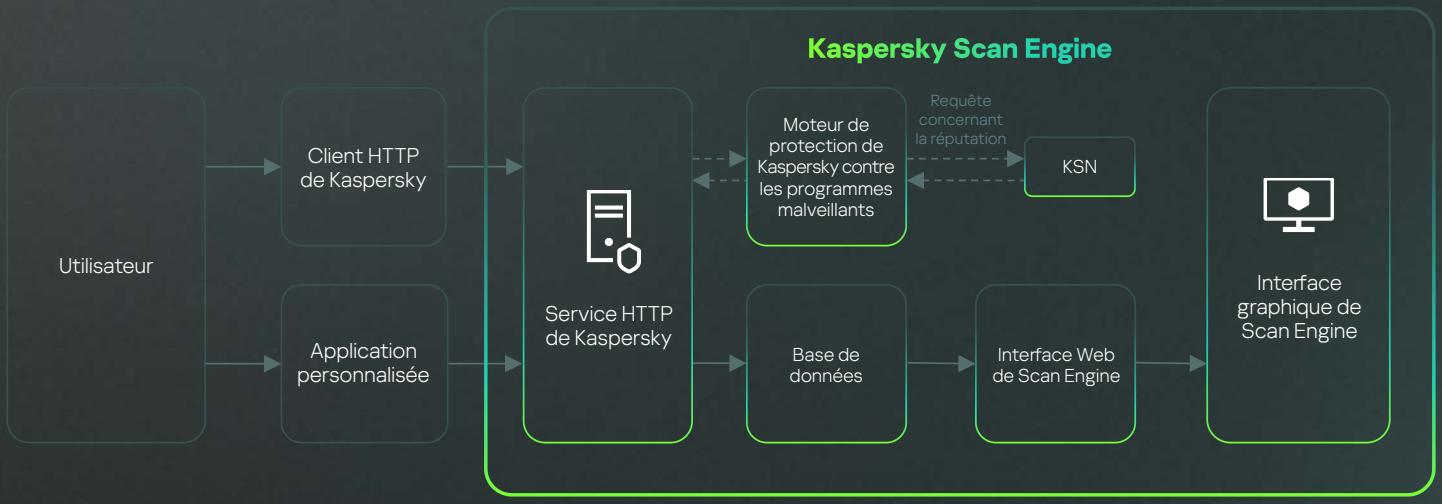
KSEn for Linux

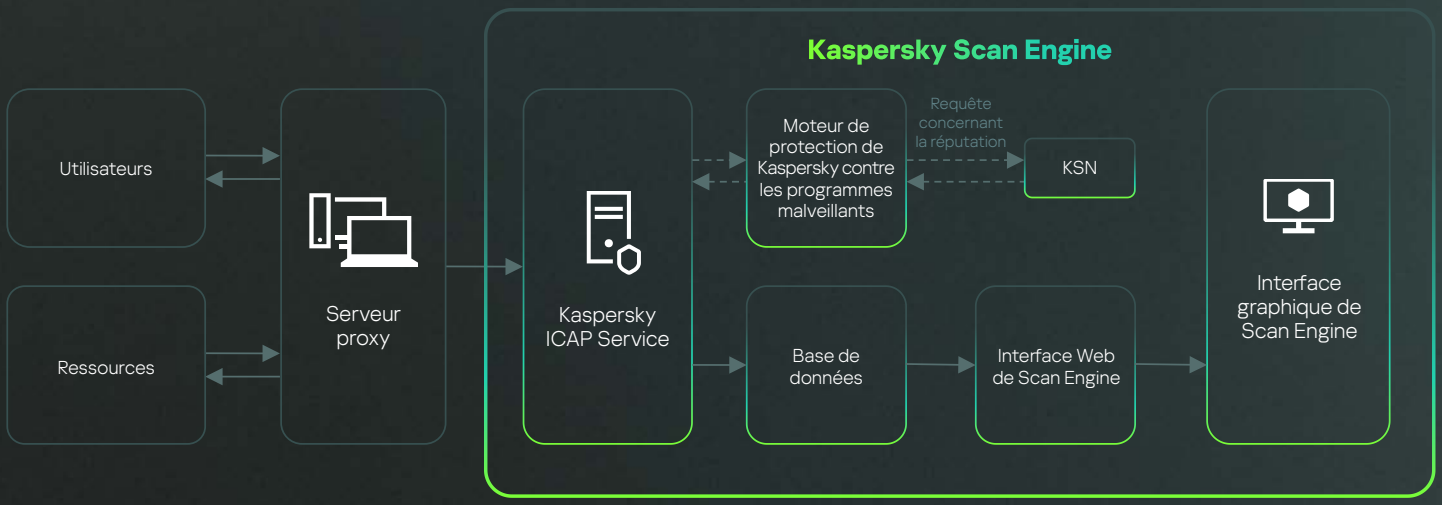
Également disponible en tant que conteneur Docker Linux (en mode HTTP et ICAP). Cette solution peut être déployée en tant que conteneur individuel, vers Docker Swarm, vers Kubernetes, vers AWS EKS et tout autre environnement dans le cloud similaire.

Interface graphique

Kaspersky Scan Engine comprend également une interface utilisateur graphique fondée sur le Web qui vous permet de configurer facilement le comportement du produit, d'examiner ses événements de service et d'analyser les résultats.

Cas d'usage





Intégration avec n'importe quelle solution de réseau

Grâce à une API de type REST riche en fonctionnalités et à un code source ouvert, vous pouvez facilement intégrer Kaspersky Scan Engine à presque toutes les solutions de votre réseau.

Protection des portails Web contre le chargement de programmes malveillants.

Protection du stockage cloud public (compartiment AWS S3, etc.) et privé (Nextcloud, ownCloud et plus à venir) contre le chargement de contenus malveillants.

Protection des boutiques d'applications et des places de marché de logiciels contre le chargement d'applications malveillantes.

Analyse du stockage des fichiers Windows/Linux à la recherche de programmes malveillants.

Plug-in de protection contre les programmes malveillants pour les passerelles Web ou de messagerie de tiers. La liste des intégrations réalisées est disponible sur demande et est constamment mise à jour.

Module de protection contre les programmes malveillants pour le système de gestion des documents de l'entreprise, le pipeline de développement de logiciels et d'autres systèmes qui exigent que les fichiers soient contrôlés pour détecter tout programme malveillant.

Fonctionnalités principales

Protection primée contre les programmes malveillants

La technologie primée de Kaspersky contre les programmes malveillants offre les meilleurs taux de détection du secteur et peut réagir instantanément aux menaces émergentes.

Filtrage des contenus

Kaspersky Security Network filtre les URL malveillantes, de phishing et de logiciels publicitaires.

Détection

Détection d'objets compressés à plusieurs reprises. Le plus grand nombre de formats de compression et d'archive pris en charge.

Connecteurs de plateforme

Plusieurs plateformes tierces prises en charge, nativement ou via des connecteurs, comme Amazon S3, Nextcloud, ownCloud, Kubernetes, etc.

Désinfection des fichiers

Désinfection des fichiers, archives et objets codés infectés. Toute menace détectée peut être totalement supprimée ou, si cela est possible, seule la charge utile malveillante peut être supprimée, en laissant le reste du fichier intact.

Agent

Moteur antivirus pouvant être mis à jour : les technologies de détection et la logique de traitement peuvent être mises à niveau ou modifiées via des mises à jour régulières de la base de données antivirus.

Fonctionnalités avancées

Analyseur heuristique sophistiqué et technologies de détection avancées reposant sur le Machine Learning.

Big Data

Optimisé par le Big Data : Kaspersky Security Network fournit des informations sur la réputation des fichiers et des ressources Web, ce qui permet d'assurer une détection plus rapide et plus précise.

Évolutivité

Kaspersky Scan Engine offre des performances de premier ordre et s'adapte très facilement.

Reconnaissance de format

Une couche de filtrage supplémentaire est possible grâce au composant Reconnaissance de format. Vous pouvez utiliser ce composant pour reconnaître et ignorer des fichiers dans certains formats pendant le processus d'analyse. Des dizaines de formats sont pris en charge, notamment les fichiers exécutables, les fichiers MS Office, les fichiers multimédias et les archives.

Prise en charge du protocole TLS

La communication via le protocole TLS est prise en charge en cas d'exécution en mode service de type REST.

Mode cluster

Kaspersky Scan Engine peut fonctionner en mode cluster : plusieurs instances de Kaspersky Scan Engine peuvent être déployées dans le même réseau et administrées via l'interface Web.

Nouvelles fonctionnalités de Kaspersky Scan Engine 2.1

Depuis juin 2022

Sécurité et conformité

- Mode multi-utilisateurs et contrôle d'accès basé sur les rôles.
- Audit des opérations.
- Prise en charge de l'authentification des clients HTTP via des jetons.
- API Protection contre le piratage des mots de passe par force brute dans l'interface utilisateur Web.

Modifications architecturales

Scan Engine est divisé en deux modules qui peuvent être publiés séparément : (1) le moteur AV (la trousse SDK KAV) et (2) la fonctionnalité principale du produit (Scan Engine en tant qu'enveloppe sur la trousse SDK KAV).

Amélioration de la documentation

Manuels d'intégration avec les SIEM (MicroFocus ArcSight, Splunk) Manuels d'intégration avec Oracle Solaris VScan, F5 Application Security Manager, GoAnywhere MFT, Dell Isilon OneFS.

Amélioration du fonctionnement

Systemd est entièrement pris en charge pour travailler avec les services (démarrage/arrêt/état/redémarrage).

Amélioration du mode cluster

Les nœuds inactifs sont automatiquement retirés du cluster et prennent en charge les clusters hétérogènes (HTTP et ICAP).

Modifications dans syslog

Plusieurs destinations.
Filtre d'événements à envoyer.

Récompensée

Récentes récompenses décernées aux produits Kaspersky par des laboratoires d'essai indépendants

SE Labs INTELLIGENCE-LED TESTING BEST Small Business Endpoint WINNER 2021

AV comparatives Lowest False Positives 2022 BRONZE

AV comparatives Top Rated 2022

AV comparatives ATP 2022 BRONZE

AV comparatives Top Rated 2020

SE Labs AAA July 2022 Enterprise Advanced Security EDR Detection

SE Labs AAA Oct-Dec 2022 Enterprise Endpoint Security EPS Protection

AV comparatives Certified EPR 2022 Strategic Leader

AV-TEST av-test.org 2022 AWARD BEST USABILITY Kaspersky Endpoint Security

AV-TEST av-test.org 2021 AWARD BEST PROTECTION Kaspersky Endpoint Security

AV-TEST av-test.org 2021 AWARD BEST PERFORMANCE Kaspersky Endpoint Security

AV-TEST av-test.org 2022 AWARD BEST PERFORMANCE Kaspersky Endpoint Security

En savoir plus

Kaspersky Scan Engine

Une version d'essai offerte de 30 jours est disponible !
Veuillez cliquer sur le lien ci-dessous et faire une demande d'essai de KSEn.

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture