KASPERSKY lab

KASPERSKY PRIVATE SECURITY NETWORK : SURVEILLANCE DES MENACES EN TEMPS RÉEL : AU CŒUR DE L'INFRASTRUCTURE DES ENTREPRISES

Surveillance globale des menaces utilisée au niveau local

www.kaspersky.fr

UN LABORATOIRE SUR LES MENACES BASÉ DANS LE CLOUD POUR LES CLIENTS DE KASPERSKY LAB

Depuis 2008, la surveillance des menaces basée dans le cloud de Kaspersky Lab (Kaspersky Security Network) a fourni des informations sur les menaces et des données de réputation à des millions de clients dans le monde. À l'aide de données en temps réel rendues anonymes provenant de 80 millions de capteurs placés sur des terminaux partout dans le monde, chaque fichier passant par les systèmes protégés par Kaspersky Lab est analysé en fonction des informations issues de la surveillance des menaces les plus pertinentes.

Les solutions de sécurité standards ont besoin de quatre heures pour recevoir les informations nécessaires pour détecter et bloquer les quelques 360 000 nouveaux programmes malveillants découverts par les chercheurs de Kaspersky Lab chaque jour. Le service de partage des informations sur les menaces via le réseau de sécurité privé de Kaspersky Lab fournit ces données en 30 à 40 secondes.

Bien que les informations traitées par Kaspersky Security Network soient totalement anonymes et dissociées de leur source, Kaspersky Lab sait que certaines entreprises exigent un verrouillage absolu des données, pour des raisons de conformité ou en raison de leur politique. Jusqu'ici, de telles entreprises ne pouvaient généralement pas utiliser les services de sécurité basés dans le cloud.

Cependant, Kaspersky Lab a développé pour ces clients un produit autonome : **Kaspersky Private Security Network,** qui permet aux entreprises de bénéficier de la plupart des avantages liés à la surveillance des menaces basée dans le cloud sans diffuser de données hors de leur périmètre de contrôle. C'est aussi simple que cela : il s'agit d'une version totalement privée, locale et personnelle de Kaspersky Security Network pour les entreprises.

Afin de comprendre comment Kaspersky Private Security Network fonctionne, commençons par examiner Kaspersky Security Network.

Kaspersky Security Network est disponible en tant que composant complémentaire et optionnel des solutions Kaspersky Enterprise Security for Business, Kaspersky Security for Virtualization, Kaspersky Security for Storage, Kaspersky Security for Data Centers, Kaspersky Anti-APT et Kaspersky Fraud Prevention.

SURVEILLANCE DES MENACES EN TEMPS RÉEL RÉALISÉE DANS LE CLOUD

Kaspersky Security Network (KSN) utilise les fonctionnalités haute performance du cloud pour garantir une détection des menaces des plus rapides et des temps de réactions des plus courts. Les informations à la volée sur les dernières menaces sont transférées dans notre cloud sécurisé pour analyse ; chaque fois qu'un système protégé par Kaspersky Lab détecte un fichier, une application ou un site Web suspect, une requête est lancée dans la base de données des menaces basée dans le cloud et le diagnostic sur l'état de sécurité est immédiatement transmis. L'intégration des informations sur les nouvelles menaces dans les bases de données prend généralement des heures avec les techniques conventionnelles, et l'analyse des menaces au niveau local ou sur le système consomme énormément de ressources.

Contribuer à un niveau de sécurité plus élevé

Chaque participant de KSN fournit des informations uniques sur les menaces auxquelles nos utilisateurs sont confrontés qui, regroupées, constituent un organe de surveillance des menaces qui rend Internet plus sûr pour tous. Voici un bon exemple illustrant la puissance des informations : KSN a détecté des modules de l'attaque ciblée extrêmement sophistiquée Equation bien avant qu'elle ne soit qualifiée de groupe de menaces organisées et concertées. Le dropper du cheval de Troie d'Equation, « EquationLaser », et le vers « Funny » ont été détectés et bloqués par KSN en avril 2012 et en juin 2013, respectivement.

Ce qui rend KSN si intéressant dans la détection de l'APT Equation, c'est qu'il illustre à la perfection le rôle que peuvent jouer les participants (particuliers et petites entreprises) en contribuant aux recherches sur les menaces sophistiquées. Plusieurs de ces utilisateurs participent à KSN et nous apprenons beaucoup des informations sur les menaces qu'ils transmettent ; bien que cela puisse paraître surprenant, les utilisateurs constituent une source d'informations sur les menaces extrêmement précieuse pour les entreprises clientes. Ceci est en partie dû au fait qu'ils adoptent des comportements à haut risque en ligne, mais également au fait que les cybercriminels se servent souvent d'eux comme tremplin pour lancer des attaques sur des réseaux d'entreprise plus sécurisés.

Examinons comment la protection basée dans le cloud de KSN utilise ces données pour offrir de meilleurs taux de détection, réduire les temps de réaction, minimiser les faux positifs et prendre en charge les listes blanches.

LES TAUX DE DÉTECTION COMPTENT

Les analyses de Kaspersky Lab détectent 360 000 nouveaux fichiers malveillants chaque jour ; 113 500 « wild cards » d' hameçonnage sont ajoutées à notre base de données de lutte contre l' hameçonnage chaque mois.

La cybercriminalité a évolué, pas uniquement en termes de quantité, mais également au niveau du degré de sophistication ; bien que 70 % des menaces auxquelles sont confrontées les entreprises soient connues, 30 % restent des menaces inconnues et avancées que la sécurité traditionnelle basée sur les signatures ne peut plus gérer seule. Les informations issues de la surveillance 24h/24, 7j/7 que les experts collectent sur les types d'attaques que nos utilisateurs subissent et contrecarrent constituent un élément essentiel du système de défense de Kaspersky Lab à plusieurs niveaux. Et Kaspersky Security Network (KSN) joue un rôle primordial en fournissant ces informations.

KSN traite plus de 600 000 requêtes, transportant 14 Go de statistiques globales entrantes par seconde : les informations sont ainsi mises à jour en permanence, ce qui permet aux utilisateurs de KSN de bénéficier d'une augmentation du taux de détection de 2,5 à 3,1 %. L'année dernière, plus de 39 % des utilisateurs de Kaspersky Lab ont été confrontés à des menaces nouvelles et inconnues et les composants antivirus standards n'ont pas été en mesure de les détecter, contrairement à KSN. Au total, 20 % des menaces détectées par les technologies de Kaspersky Lab le sont grâce aux statistiques collectées par KSN.

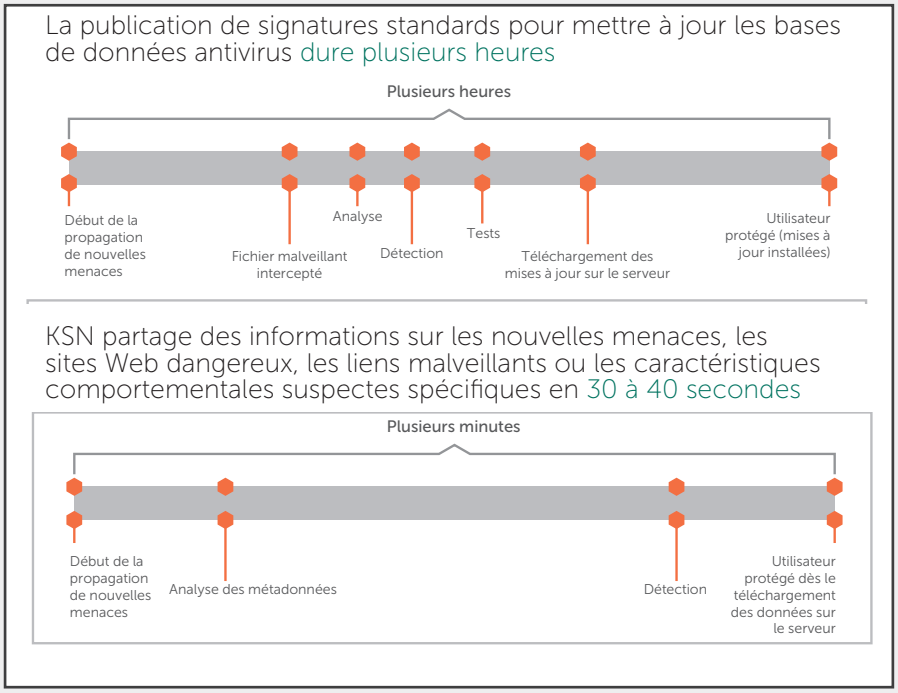
Pensez-y : dans l'environnement actuel des menaces, même une différence de 0,9 % au niveau des taux de détection peut se traduire par des centaines et des centaines de programmes malveillants qui passent à travers les mailles du filet chaque année. Et c'est ce 1 % d'attaques ciblées, qui passent bien souvent inaperçues pendant des mois, voire des années, qui sont généralement les plus nuisibles aux systèmes des entreprises.

Cette expertise et cette protection supplémentaires apportées par KSN pourraient protéger votre entreprise contre les menaces les plus dangereuses, notamment des APT et des programmes malveillants plus sophistiqués. L'analyse de la « structure de l'attaque » montre que les attaquants doivent réussir à passer à travers chaque maillon pour atteindre leur objectif ; une seule atténuation perturbe à la fois la chaîne et l'attaquant.[1]

[1] EM Hutchins, MJ Cloppert et RM Amin : Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (Informer la défense du réseau informatique axée sur les informations en analysant les chaînes de frappe des intrusions et des campagnes nuisibles).

TOUT EST QUESTION DE TIMING

S'il est important de réduire le nombre de menaces qui passent à travers les mailles du filet, le temps nécessaire pour les détecter et les contrecarrer l'est tout autant. La détection et le blocage basés dans le cloud de KSN sont bien plus rapides que ceux offerts par les mises à jour traditionnelles des solutions de lutte contre les programmes malveillants. Les processus de publication et de mise à jour des signatures standards peuvent durer des heures, et les améliorations permettant d'y remédier ne sont pas légion.
À contrario, les mises à jour assistées par le cloud telles que celles de KSN permettent de partager des informations sur les menaces nouvelles et émergentes, les caractéristiques comportementales suspectes, les liens malveillants ou les sites Web dangereux de manière quasi instantanée, en seulement 30 à 40 secondes.



Pensez-y : lorsqu'il s'agit de menaces avancées et sophistiquées, un délai de réaction de quelques heures seulement peut avoir de graves conséquences.

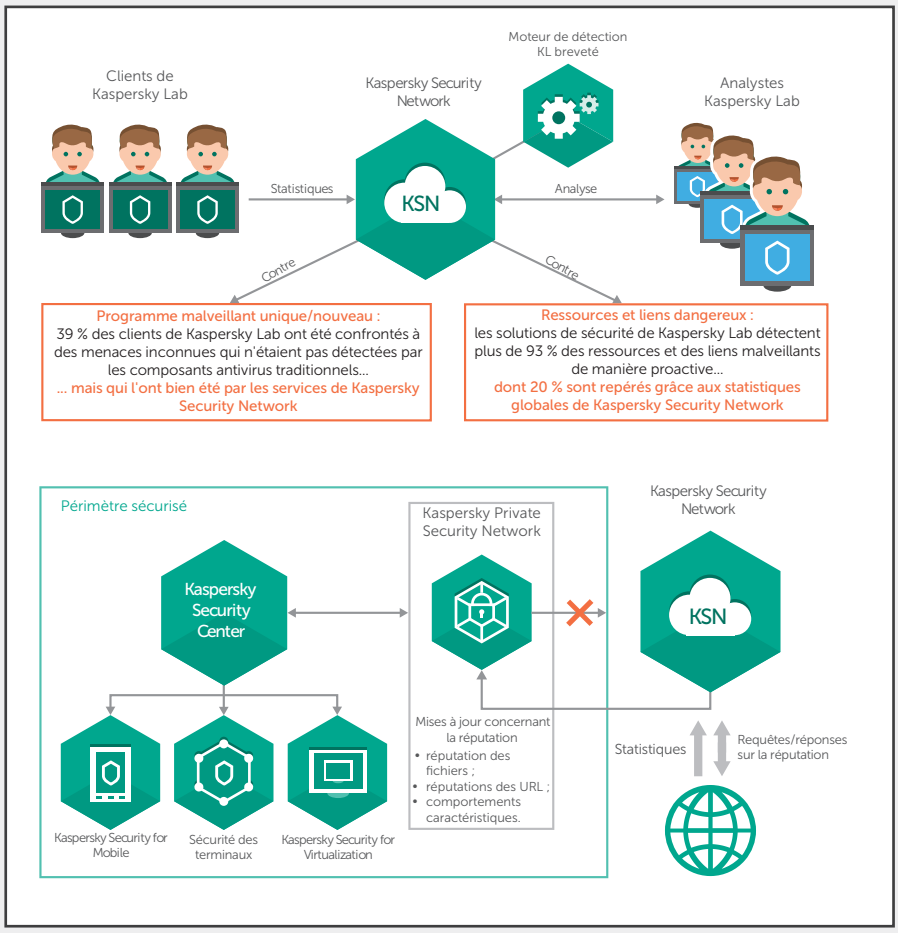
Figure 1 : Réduire les temps de réaction face aux menaces avec Kaspersky Security Network : une vision globale, proactive et en temps réel.

SUPPRIMER LES FAUX POSITIFS

Dans tout système analysant d'importantes quantités de fichiers, les faux positifs peuvent devenir un réel problème et bien souvent chronophage. La flexibilité et la plus grande rapidité de la sécurité assistée par le cloud permet d'accélérer les mises à jour, ce qui augmente la précision et réduit le nombre de faux positifs.

Aucune entreprise ne souhaite passer du temps à compiler, réviser et éditer encore et encore les listes d'applications acceptables et « sûres ». Et qu'en est-il des pilotes des imprimantes, des logiciels de mise en réseau et des mises à jour essentielles ? Comment veillez-vous à ce que les mises à jour essentielles ne soient pas qualifiées de dangereuses par erreur ?
Kaspersky Lab's Dynamic Whitelist s'en charge pour vous. Conçue par un laboratoire dédié aux listes blanches qui travaille avec des centaines de partenaires à l'international, cette solution consiste principalement en une énorme base de données de logiciels « sains », continuellement mise à jour avec des informations sur les types de fichiers, les mises à jour, les fichiers d'installation et, plus important, les logiciels eux-mêmes. La base de données de Kaspersky Lab, à laquelle Kaspersky Security Network a accès en permanence, contient près de 1,5 milliards de fichiers.
Un programme qualifié de « sain » un jour peut contenir un code malveillant le lendemain : seules une surveillance et une analyse constantes peuvent garantir la fiabilité des informations sur la réputation. Une analyse indépendante menée par West Coast Labs a révélé que la base de données basée dans le cloud de Kaspersky Lab contenait des données sur 94 % des logiciels sains publiés dans le monde.
Aucun cloud de sécurité n'est parfait ; les URL et fichiers malveillants peuvent parfois être qualifiés de fiables/non fiables par erreur. En outre, les performances sont analysées en permanence afin d'en améliorer la qualité.

ADOPTER KASPERSKY PRIVATE SECURITY NETWORK POUR RÉPONDRE AUX EXIGENCES EN MATIÈRE DE CONFIDENTIALITÉ, DE POLITIQUE DE SÉCURITÉ ET DE CONFORMITÉ



La première image illustre le fonctionnement de Kaspersky Security Network. La seconde montre comment Kaspersky Private Security Network fonctionne en s'intégrant totalement à l'infrastructure de l'entreprise.

Maintenant que vous avez connaissance des avantages et fonctionnalités de KSN, voyons comment Kaspersky Private Security Network répond aux besoins des entreprises appliquant des contrôles rigoureux des données.

Premièrement, bien que les données de KSN soient toujours rendues totalement anonymes, Kaspersky Private Security Network pousse la sécurité encore plus loin en apportant le cloud dans les locaux. Les entreprises profitent ainsi d'un contrôle total sur les données tout en bénéficiant des informations sur les menaces recueillies par KSN.

KASPERSKY PRIVATE SECURITY NETWORK : UNE SOLUTION LOCALE POUR DES AVANTAGES AU NIVEAU MONDIAL

Kaspersky Private Security Network est installé au sein même du data center de l'entreprise. Les spécialistes informatiques et de la sécurité de l'entreprise gardent ainsi le contrôle total de cette solution. En parallèle, l'entreprise bénéficie de tous ses avantages en matière de sécurité : analyse des menaces en temps réel, analyse de la réputation, détection proactive des menaces et liste blanche dynamique.

KPSN convient particulièrement aux entreprises assujetties à des normes gouvernementales, industrielles ou de conformité réglementaire strictes. Une option de déploiement « air-gap » (isolement du réseau) est même disponible pour les segments du réseau pour lesquels une connexion Internet n'est pas souhaitable.

Si de nombreux éditeurs de sécurité assistée par le cloud proposent des « proxies de mise en cache » qui réduisent le nombre de requêtes de données de réputation adressées par le système au cloud, Kaspersky Lab est unique dans sa capacité à déployer le cloud totalement au niveau local, dans le propre data center de l'entreprise et sans transaction sortante avec des serveurs tiers. Ceci est essentiel pour garantir certains paramètres gouvernementaux et industriels.

Afin de gagner en sécurité, les mises en œuvre de KPSN conservent les bases de données de signatures locales. En effet, certaines solutions transfèrent totalement cette fonctionnalité au cloud, et le client se retrouve exposé aux attaques au cours du transfert. Avec KPSN, c'est impossible : au cours du déploiement, les bases de données locales de Kaspersky Lab (qui peuvent être mises à jour manuellement) continuent d'assurer une protection optimale, supprimant ainsi toute faille de sécurité.

Une fois installé et lancé, KPSN peut devenir une source unique d'informations sur les menaces exploitable pour d'autres solutions utilisées : centre des opérations de sécurité, SIEM, gestion des risques relatifs aux virus de redirection Google, analyses criminalistiques et processus d'élimination...qui peuvent toutes être intégrées aux sources de données, offrant ainsi une vision unique de la sécurité et de la capacité de réponse aux menaces de votre entreprise.


Twitter.com/
KasperskyFrance


Facebook.com/
KasperskyLabFrance


Youtube.com/
KasperskyFrance

Kaspersky Lab, Moscou, Russie
www.kaspersky.fr

Tout savoir sur la sécurité sur Internet :
www.securelist.fr

Rechercher un partenaire près de chez vous :
www.kaspersky.fr/partners/
buyoffline/liste-des-partenaires

KASPERSKY lab