Kaspersky®
Private Security
Network

Kaspersky Security Network : les Big Data au service de la sécurité

Votre protection contre chaque nouvelle génération de menaces

Le nombre de cyberattaques au niveau mondial augmente chaque jour. L'impact sur les entreprises est considérable, avec bien souvent vols de données ou perte d'informations importantes à la clé. Dans tous les types d'entreprises, des start-ups aux leaders du secteur, la continuité des activités est menacée.

Le risque ne tient pas seulement à la quantité des attaques, mais également à leur nature. De nouvelles générations de programmes malveillants apparaissent chaque jour, qui, pour beaucoup, exploitent de nouvelles techniques sophistiquées conçues pour contourner les solutions de sécurité existantes. Dans cet environnement en évolution constante, une protection efficace n'est possible qu'à condition de surveiller étroitement le paysage des menaces et de traduire les données ainsi recueillies en information stratégique et en nouvelles technologies.

Une solution de cybersécurité digne de ce nom doit donc être capable de réagir de façon instantanée et efficace aux nouveaux programmes malveillants tout en anticipant les prochaines manœuvres de l'ennemi. Pour réunir de telles capacités, le Cloud est un élément décisif dans la mesure où il permet d'appliquer de façon distribuée les technologies d'extraction et d'analyse des données pour traiter les informations relatives aux menaces. Les plus performants de ces systèmes, comme Kaspersky Security Network, disposent de points d'acquisition des données répartis à travers le monde et de puissants centres de traitement de ces « Big Data » capables de transformer rapidement toutes ces données brutes en protection réelle. Pour bénéficier d'un taux de détection élevé et assurer à nos clients le meilleur résultat possible, l'expertise humaine reste cependant une pièce maîtresse de ce cycle de traitement des données.

Trois composants clés sont essentiels au bon fonctionnement du mécanisme :

- Acquisition des statistiques mondiales de détection des programmes malveillants, ainsi que des données en temps réel sur les comportements suspects
- Traitement et analyse des Big Data
- Mise à disposition rapide d'informations stratégiques auprès des clients

L'étape la plus difficile dans ce domaine consiste à trier et à analyser les données. Les volumes sont si importants qu'ils exigent de recourir à des technologies d'automatisation basées sur la science des données et capables de digérer les masses de mégadonnées entrantes. L'expertise humaine reste néanmoins un atout important dans ce système. En effet, seules l'intuition et l'expérience humaines peuvent aider les machines à appréhender les créations complexes, et bien souvent très imaginatives, des auteurs de programmes malveillants. Les experts de Kaspersky Lab disposent d'un accès en temps réel à toutes les informations recueillies, ce qui leur permet d'analyser en profondeur les menaces, d'apporter leurs connaissances aux investigations en cours et de développer de nouvelles technologies de détection proactives. Voici les principaux avantages de notre approche pour les clients :

- Détection optimale des programmes malveillants sophistiqués et inconnus.
- Réduction des erreurs de détection (faux positifs).
- Réduction significative du temps de réponse aux nouvelles menaces : les réponses classiques basées sur des signatures peuvent prendre des heures là ou KSN s'en charge en 40 secondes environ.

KSN : les points clés

À l'aide de données en temps réel provenant de millions de capteurs placés sur des terminaux participants aux quatre coins du monde, chaque fichier transitant par les systèmes protégés de Kaspersky Lab est analysé en fonction des informations les plus pertinentes issues de la Threat Intelligence. Ces mêmes données permettent de prendre la mesure la plus appropriée. La participation au réseau KSN est entièrement volontaire et toutes les statistiques recueillies sont anonymisées, sans aucune possibilité de rapprochement avec les données d'utilisateurs particuliers. Le contrat de licence de l'utilisateur final précise les types de données recueillies et les modalités de transfert.

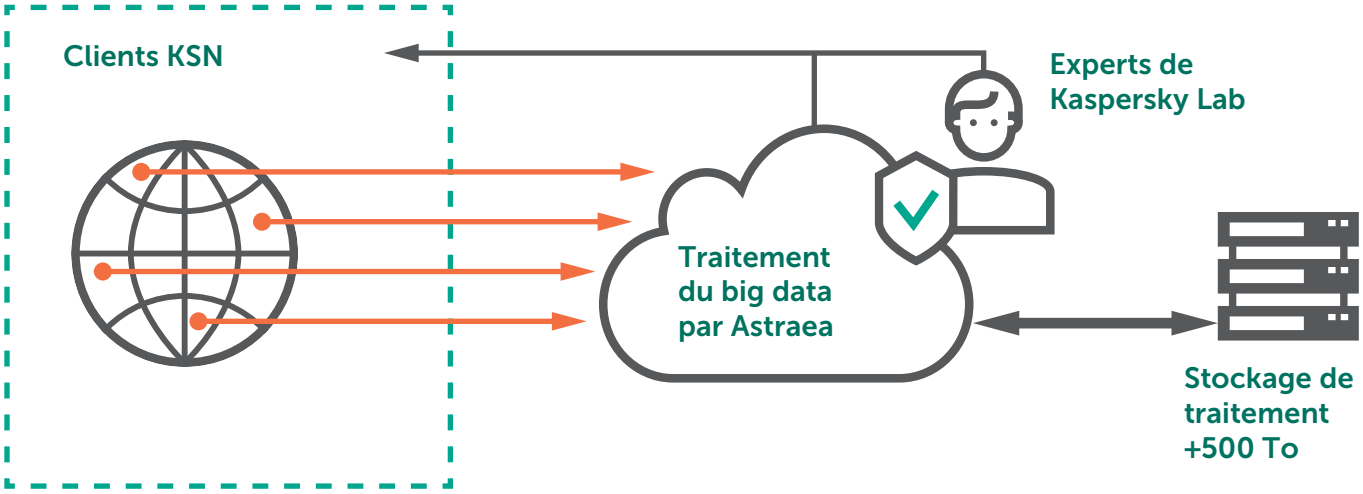

Fig. 1 – Schéma de la transmission des données entre les divers éléments du réseau KSN

KSN utilise une connexion entièrement sécurisée pour envoyer les données. Le système de transmission des données est conçu selon les normes du secteur les plus strictes. Le traitement de toutes les données primaires est effectué automatiquement et l'accès à ce niveau n'a lieu que dans les cas exceptionnels les plus graves.

Astraea, système intelligent d'analyse des Big Data

KSN reçoit quotidiennement des centaines de millions d'enregistrements, dont le volume de données s'élève couramment à des centaines de gigaoctets. Ces données anonymisées sont comprimées et stockées pour utilisation ultérieure ; même après compression, elles occupent toujours plusieurs téraoctets.

L'un des systèmes utilisés par Kaspersky Security Network pour traiter cet énorme flux de données s'appelle Astraea. Chaque jour, il traite, trie et analyse des informations portant sur des millions d'objets. Après avoir trié ces données (qui correspondent aux métadonnées des objets, jamais à leur contenu), Astraea attribue un score à chaque objet.

Tout événement suspect reçu par le système est évalué en termes d'importance et de danger potentiel sur la base de nombreux critères. À la suite de cette analyse, le système calcule la réputation de l'objet et demande des statistiques mondiales à son sujet. Que peut nous dire d'autre l'intelligence collective ? La réputation de l'objet est-elle pire que ce qu'elle semblait être au premier abord ? Ou bien s'agit-il au contraire d'une fausse alerte ? Cette comparaison à d'autres sources permet au système d'affiner ses conclusions et de réduire la probabilité de faux positifs pour les autres utilisateurs.

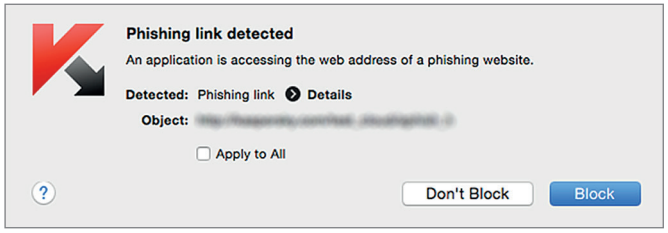

Fig. 2 – Alerte relative à un site dangereux

Une fois le verdict (malveillant, sans danger ou inconnu) confirmé sur la base des statistiques accumulées, cette information est mise à disposition des autres produits Kaspersky Lab compatibles dont les utilisateurs ont activé la fonction Kaspersky Security Network, le tout sans aucune intervention humaine.

De la même manière, lorsque des ressources Web ont été détectées comme étant malveillantes, les utilisateurs qui tentent d'y accéder sont automatiquement avertis du danger.

Quels que soient les avantages de l'automatisation, la protection est impossible sans intelligence humaine, qui seule permet au système de juguler les astuces et les techniques d'évitement de cybercriminels en chair et en os. C'est pourquoi KSN, tout comme d'autres systèmes de Kaspersky Lab, applique le principe « HuMachine » : la fusion de la puissance des machines et de l'expérience des experts humains. Comment ça marche ?

Lorsque le niveau de menace associé à un objet ne peut être déterminé, les données sont envoyées à des experts qui procèdent à une analyse approfondie supplémentaire avant d'ajouter les données à KSN pour détection instantanée via le Cloud. Parallèlement, des modèles de détection heuristiques peuvent être adaptés pour repérer, sur la base d'indicateurs similaires, des spécimens de programmes malveillants très variés.

Astraea est un système hautement intelligent, qui apprend en permanence à gérer efficacement le paysage en constante évolution des menaces. À mesure que les anciens critères d'apprentissage perdent de leur pertinence, il devient néanmoins vital d'identifier et d'appliquer les nouveaux critères qui permettront de contrer efficacement les « inventions » des attaquants. C'est également pour cette tâche que la machine a besoin d'experts.

La transmission des informations stratégiques par KSN est rapide et se mesure en secondes. Une telle rapidité permet de garantir un niveau de protection élevé face aux cybermenaces en temps réel. En cas d'attaque massive, même si les informations concernant les programmes malveillants en question sont déjà parvenues aux serveurs KSN mais qu'elles n'ont pas encore été communiquées aux utilisateurs finaux sous forme de fichiers de détection, le système peut les fournir immédiatement dès qu'un utilisateur en fait la demande.

Naturellement, tout cela consomme de la bande passante et le trafic Internet est susceptible d'être limité. Pour éviter ce problème et réduire la charge sur la connexion Internet, KSN peut utiliser des serveurs de cache installés sur le réseau local.

Si l'utilisateur a désactivé KSN, il ne recevra d'informations exactes au sujet des nouveaux programmes malveillants qu'après avoir effectué la mise à jour ; avant cela, il reste protégé par d'autres mécanismes proactifs.

KPSN

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 Threat Intelligence basée dans le Cloud sans diffuser de données hors de leur périmètre de contrôle. Il s'agit d'une version de Kaspersky Security Network totalement privée, locale et propre à l'entreprise.
KPSN peut être installé sur un serveur local spécial pour assurer une protection adaptable à tous les appareils connectés. KPSN n'exige pas d'accès Internet : dans les environnements d'utilisation particulièrement stricte, les mises à jour peuvent être effectuées manuellement à l'aide d'un support portable sécurisé. Dans tous les cas, la mise à disposition d'un flux de données entrant accélère considérablement la réaction aux menaces en perpétuelle évolution.

Conclusion

Inutile d'être directement impliqué dans la sécurité informatique pour comprendre le besoin de protection immédiate contre de nouvelles menaces. Même lorsque Kaspersky Security Network n'est pas activé, les multiples couches de technologies de protection au sein de nos solutions assurent une protection efficace à l'ensemble des utilisateurs.

Ce qu'apportent en plus KSN et sa protection instantanée basée dans le Cloud, c'est la possibilité d'utiliser des mécanismes de sécurité supplémentaires importants, à même de réduire le nombre de faux positifs tout en augmentant la qualité de détection grâce à des données supplémentaires en temps réel sur les menaces, les applications autorisées et les autres informations pertinentes.

Dans la mesure où les menaces plus complexes et plus ciblées ont tendance à infliger des dommages nettement plus importants que les attaques de masse, on ne saurait surestimer la valeur d'une information stratégique telle que celle fournie par Kaspersky Security Network. Le degré élevé de précision des informations est assuré par un mécanisme bien huilé d'interaction entre robots et experts : l'approche Kaspersky HuMachine. Toute entreprise se doit de garantir à ses clients le meilleur résultat possible, dans toutes les situations. C'est cet objectif que Kaspersky Security Network, tout comme sa version « privée », permet d'atteindre.

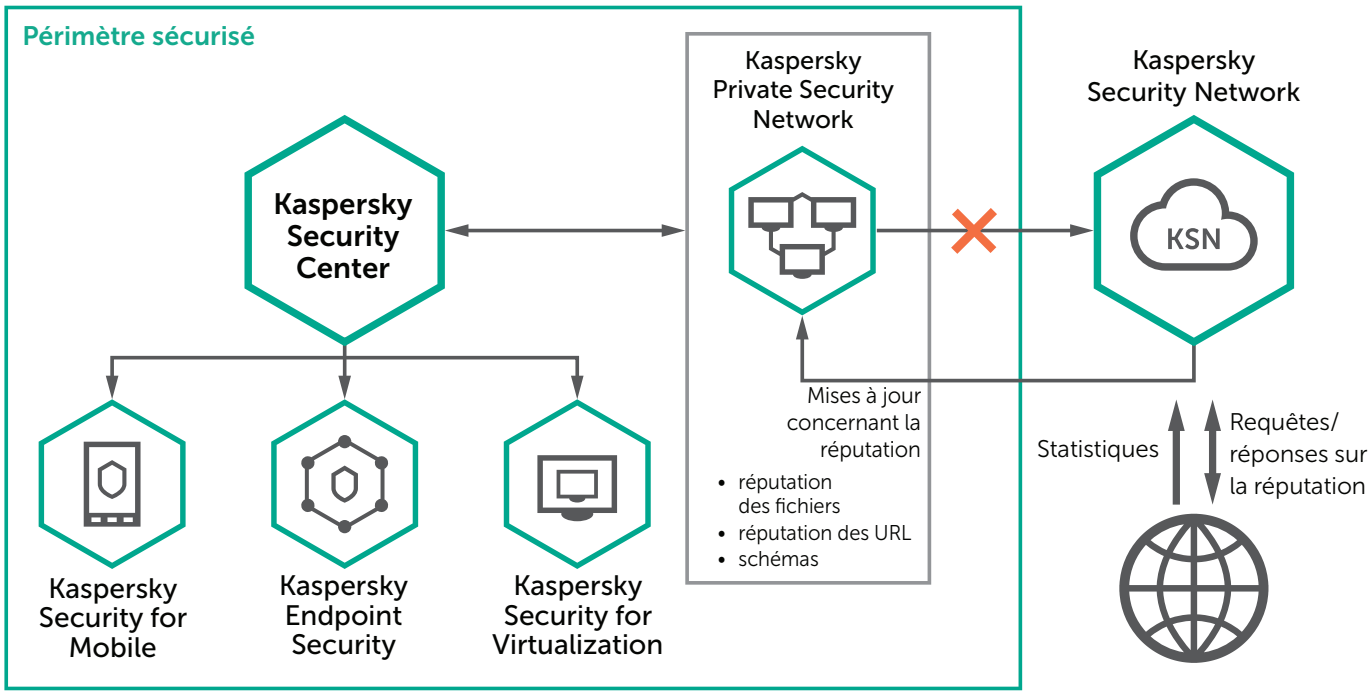

Fig. 3 – Schéma de l'infrastructure KPSN dans un périmètre sécurisé

Tout savoir sur la sécurité sur Internet : **www.viruslist.fr**
Rechercher un partenaire près de chez vous : **http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires**

www.kaspersky.fr
#truecybersecurity

© 2017 AO Kaspersky Lab. Tous droits réservés. Les marques déposées et marques de service sont la propriété de leurs détenteurs respectifs.