KASPERSKY lab

Solutions de sécurité Kaspersky Lab pour les entreprises

Kaspersky Lab est le plus grand fournisseur privé de solutions de sécurité informatique dans le monde. La société est classée parmi les 4 premiers fournisseurs de solutions de sécurité informatique pour postes de travail. Depuis sa création en 1997, Kaspersky Lab n'a cessé d'innover et propose aujourd'hui des solutions de sécurité de pointe à destination des grands comptes, PME/TPE et des particuliers. Le groupe Kaspersky Lab est présent dans près de 200 pays et territoires, offrant une protection à plus de 400 millions d'utilisateurs (dont 270 000 entreprises) à travers le monde.

Kaspersky Lab compte 37 bureaux implantés dans 32 pays

KASPERSKY lab LE POUVOIR DE PROTÉGER

SOMMAIRE

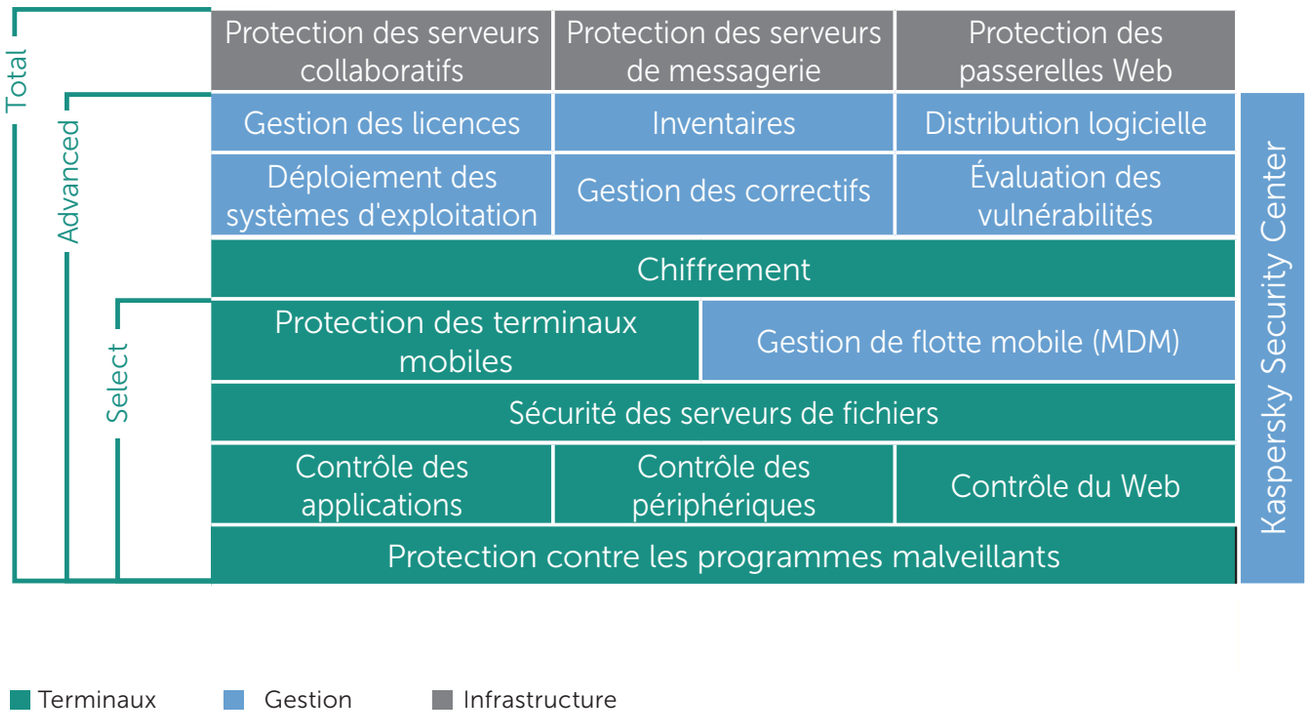
PRODUITS, SOLUTIONS ET SERVICES

Protection de votre système d'information

KASPERSKY SECURITY FOR BUSINESS

Surveillez, gérez et protégez votre environnement informatique avec Kaspersky Endpoint Security for Business.

Notre gamme comprend 3 niveaux de protection ainsi que de nombreuses fonctionnalités qu'il est possible de se procurer 'à la carte'.



Les différentes fonctionnalités sont gérées de façon centralisée, depuis la console d'administration **Kaspersky Security Center.**

Caractéristiques des solutions

Quelle est la solution la mieux adaptée à vos besoins ?

		Select	Advanced	Total	Géré via la console Security Center	Disponible dans une solution à la carte
Outils de contrôle	Protection contre les programmes malveillants	•	•	•	•	
	Pare-feu	•	•	•	•	
	Contrôle des applications	•	•	•	•	
	Contrôle des périphériques	•	•	•	•	
	Contrôle du Web	•	•	•	•	
Sécurité mobile	Sécurité des serveurs de fichiers	•	•	•	•	•
	Protection des terminaux mobiles	•	•	•	•	•
	Gestion de flotte mobile (MDM)	•	•	•	•	•
	Chiffrement		•	•	•	
Gestion des systèmes	Analyse des vulnérabilités		•	•	•	•
	Gestion des correctifs (Patch management)		•	•	•	•
	Inventaires		•	•	•	•
	Gestion des licences		•	•	•	•
	Déploiement d'applications		•	•	•	•
	Déploiement des systèmes d'exploitation		•	•	•	•
	Protection des outils collaboratifs			•		•
	Protection des serveurs de messagerie			•	•	•
	Protection de la passerelle Internet			•		•
	Protection des infrastructures virtuelles				•	•
	Protection des serveurs de stockage				•	•
	Protection de la fraude en ligne et sur mobile					•
	Protection contre les attaques DDoS					•

• Inclus • Inclus en partie (voir pages descriptives du produit)

Solutions à la carte

Protection des serveurs de fichiers

KASPERSKY SECURITY FOR FILE SERVER

POUR WINDOWS, LINUX ET FREEBSD

Kaspersky Security for File Server est une solution efficace, fiable et évolutive destinée à la protection du stockage de fichiers, sans impact perceptible sur les performances du système.

- Protection centralisée, en temps réel
- Gestion hiérarchique du stockage
- Fiabilité et haute tolérance aux pannes
- Solution évolutive et adaptable, même pour les infrastructures les plus complexes

INTÈGRE KASPERSKY SECURITY FOR WINDOWS SERVER

Première solution du marché capable de limiter la propagation des cryptovirus sur les serveurs Windows en cas d'infection.

- Fonction Anti-Cryptor de protection contre le chiffrement des dossiers partagés sur les serveurs de fichiers et les postes de travail infectés par des cryptomalwares
- Protection efficace de vos serveurs Windows, même soumis à fortes charges
- Contrôle du lancement des applications sur les serveurs

Kaspersky Security for File Server est inclus dans KESB - Select, Advanced et Total. Il est également disponible séparément en tant que solution à la carte.

Gestion des systèmes

KASPERSKY SYSTEMS MANAGEMENT

Identifier les vulnérabilités et les corriger dès que possible constitue un élément essentiel dans la défense des entreprises contre les attaques ciblées. Kaspersky Systems Management vous permet d'automatiser les tâches les plus rébarbatives mais néanmoins essentielles :

- Analyse des vulnérabilités : détection et hiérarchisation
- Gestion automatisée des correctifs : patch management
- Inventaires matériels et logiciels automatiques
- Dépannage à distance
- Déploiement d'applications et de systèmes d'exploitation à distance
- Intégration SIEM

Kaspersky Security Management est inclus dans KESB - Advanced et Total. Il est également disponible séparément en tant que solution à la carte.

Sécurité mobile

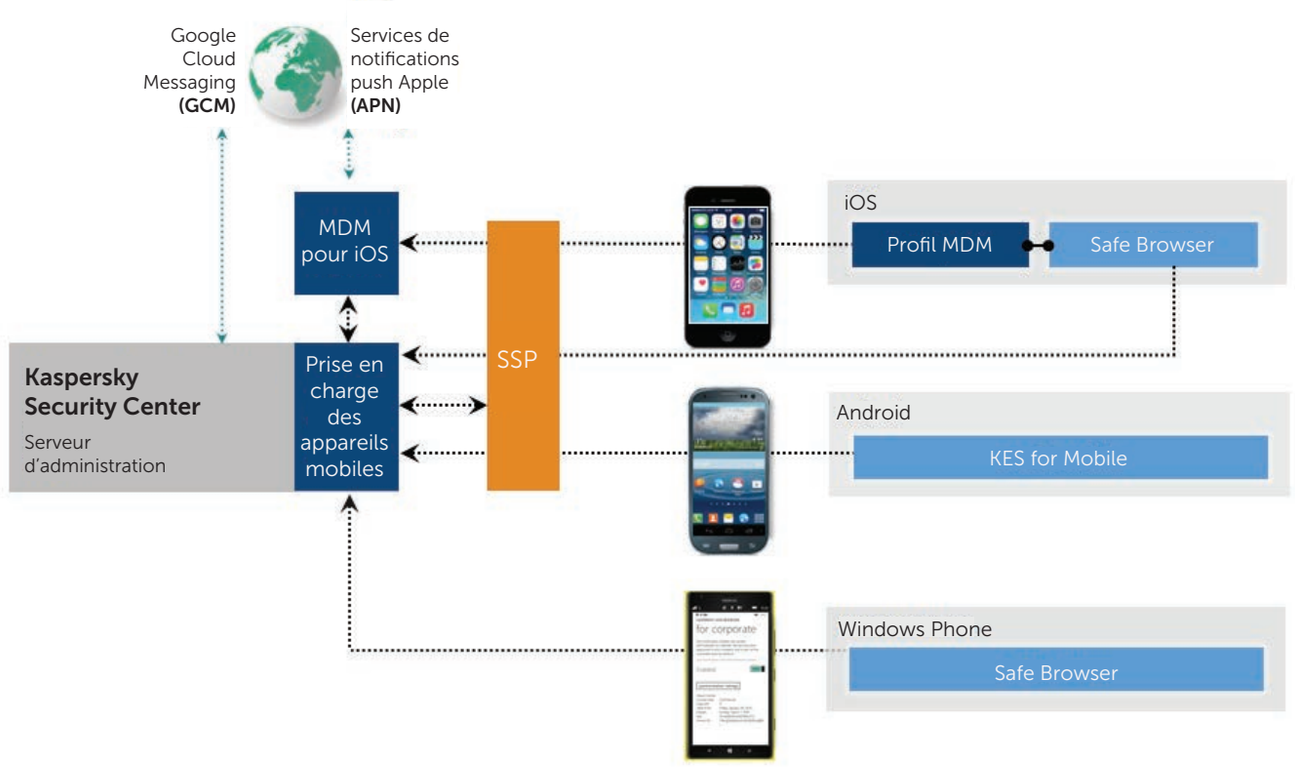
KASPERSKY SECURITY FOR MOBILE

SÉCURITÉ, GESTION ET CONTRÔLE DES SMARTPHONES ET TABLETTES

- **Sécurité mobile** :
  - Puissant anti-malware
  - Anti-phishing, filtrage des SMS et appels entrants
  - Protection Web
  - Détection des terminaux 'jailbreakés'
  - Protection contre le vol

- **Gestion des appareils mobiles** :
  - Intégration aux principales plates-formes : Android, iOS et Windows Phone
  - Contrôle à distance des appareils (OTA, « over-the-air »)

- **Gestion des appareils mobiles** : les outils de contrôle, associés à la mise en conteneurs d'applications permettent de protéger les données et les systèmes de l'entreprise tout en fournissant une politique de sécurité efficace en matière de pratique BYOD.



Architecture de la solution

Kaspersky Security for Mobile est inclus dans KESB - Select, Advanced et Total. Il est également disponible séparément en tant que solution à la carte.

Protection des outils collaboratifs

KASPERSKY SECURITY FOR COLLABORATION

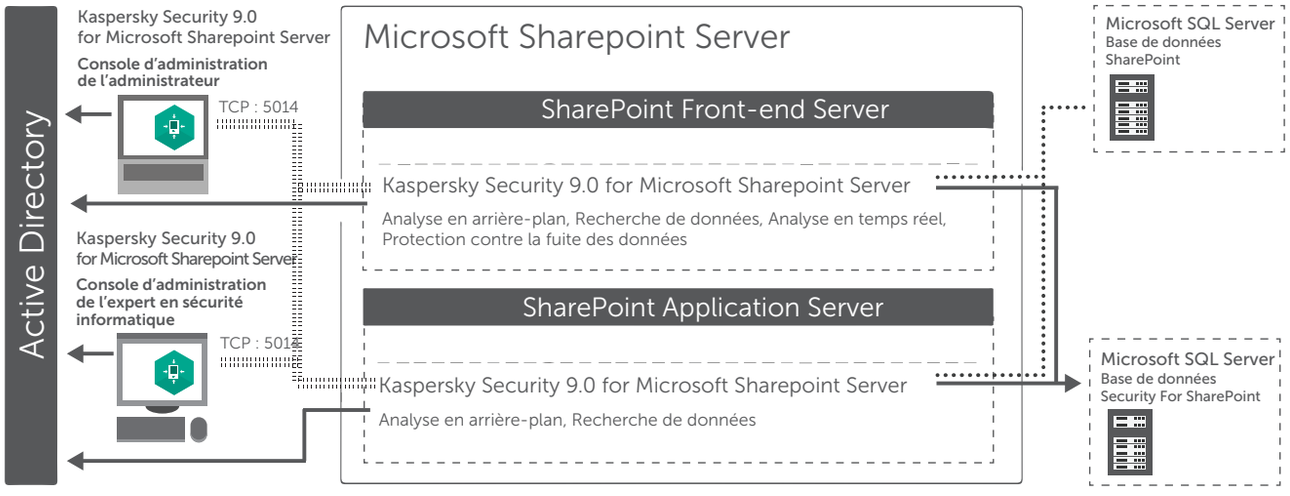
PROTECTION POUR MICROSOFT SHAREPOINT

Kaspersky Security for Collaboration offre à l'ensemble de l'environnement SharePoint et à ses utilisateurs le niveau de sécurité maximal :

- Protège l'ensemble de l'environnement SharePoint
- Prévient la perte de données confidentielles
- Facilite l'application des politiques de l'entreprise grâce au filtrage du contenu
- Intégré à Active Directory

Kaspersky Security for Collaboration analyse le contenu de tous les documents puis enregistre et bloque automatiquement ceux qui contiennent des données confidentielles ou des informations sensibles relatives aux collaborateurs. Il recherche non seulement les mots contenus dans les glossaires préinstallés, ou dans le glossaire personnalisé par l'administrateur, mais analyse également les données structurées.*

Architecture MS SharePoint



**Les fonctionnalités de protection contre les pertes de données sont vendues séparément.*

Kaspersky Security for Collaboration est inclus dans KESB - Total. Il est également disponible séparément en tant que solution à la carte.

Protection de la messagerie

KASPERSKY SECURITY FOR MAIL SERVER

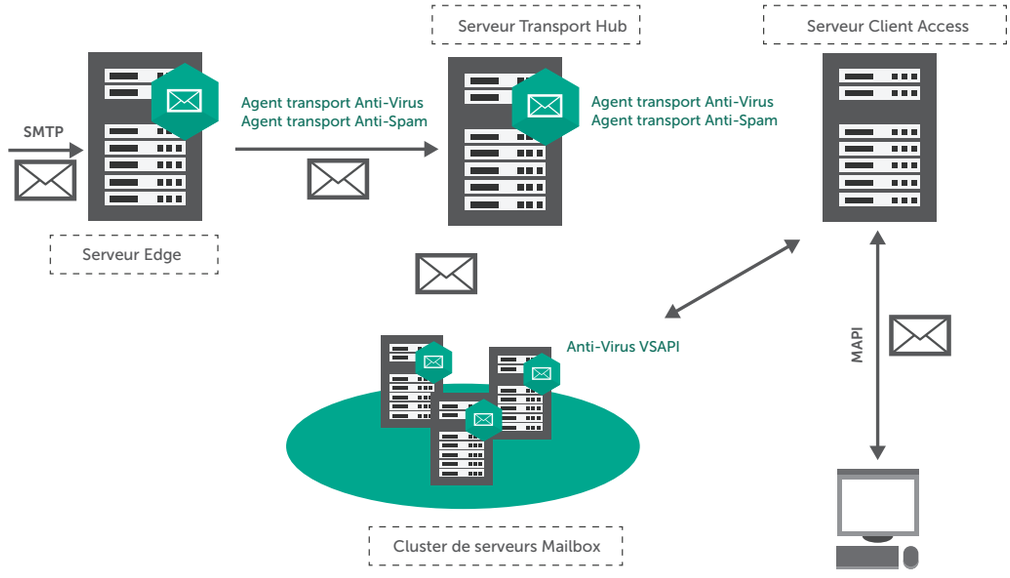
PROTECTION POUR EXCHANGE, LINUX ET DOMINO

Kaspersky Security for Mail Server protège le trafic de messagerie contre les courriers indésirables, les liens de phishing et les programmes malveillants :

- Analyse du courrier entrant, sortant et stocké
- Réduit le trafic grâce à un filtrage intelligent du courrier indésirable
- Prévient la perte de données confidentielles

Il prend en charge les plateformes de messagerie les plus courantes, telles que Microsoft Exchange, Linux Mail Server et IBM Domino. De plus, un module de prévention des pertes de données (DLP) visant à contrôler la propagation d'informations confidentielles peut s'intégrer à la plate-forme de messagerie Microsoft Exchange.

Protection des différents rôles MS Exchange (ex : version 2010)



NOUVEAU !

KASPERSKY SECURITY FOR MAIL GATEWAY

Kaspersky Security for Mail Gateway est une appliance virtuelle qui vous permet de déployer rapidement une passerelle de messagerie virtuelle et de l'intégrer à l'infrastructure de messagerie existante de votre entreprise.

- Protection des courriers entrants et sortants contre les objets malveillants et courriers indésirables (notamment les tentatives de phishing),
- Filtrage du contenu des messages

Kaspersky Security for Mail Server et Kaspersky Security for Mail Gateway sont inclus dans KESB - Total. Ils sont également disponibles séparément en tant que solution à la carte.

Protection des passerelles Internet

KASPERSKY SECURITY FOR INTERNET GATEWAY

ACCÈS INTERNET SÉCURISÉ

L'accès sécurisé à Internet pour l'ensemble des collaborateurs est l'un des piliers centraux de toute stratégie de sécurité d'une entreprise.

Kaspersky Security for Internet Gateway analyse le trafic Web et garantit à l'ensemble de vos effectifs un accès Internet sécurisé en toutes circonstances :

- Analyse en temps réel des protocoles HTTP(s), FTP, SMTP et POP3
- Supporte les plates-formes les plus récentes
- Gère et créé des rapports complets sur l'état de la protection du réseau
- La solution peut être utilisée pour protéger les messageries d'entreprise (pour Microsoft ISA ou TMG).

Kaspersky Security for Internet Gateway est inclus dans KESB - Total. Il est également disponible séparément en tant que solution à la carte.

Protection des infrastructures virtuelles

KASPERSKY SECURITY FOR VIRTUALIZATION

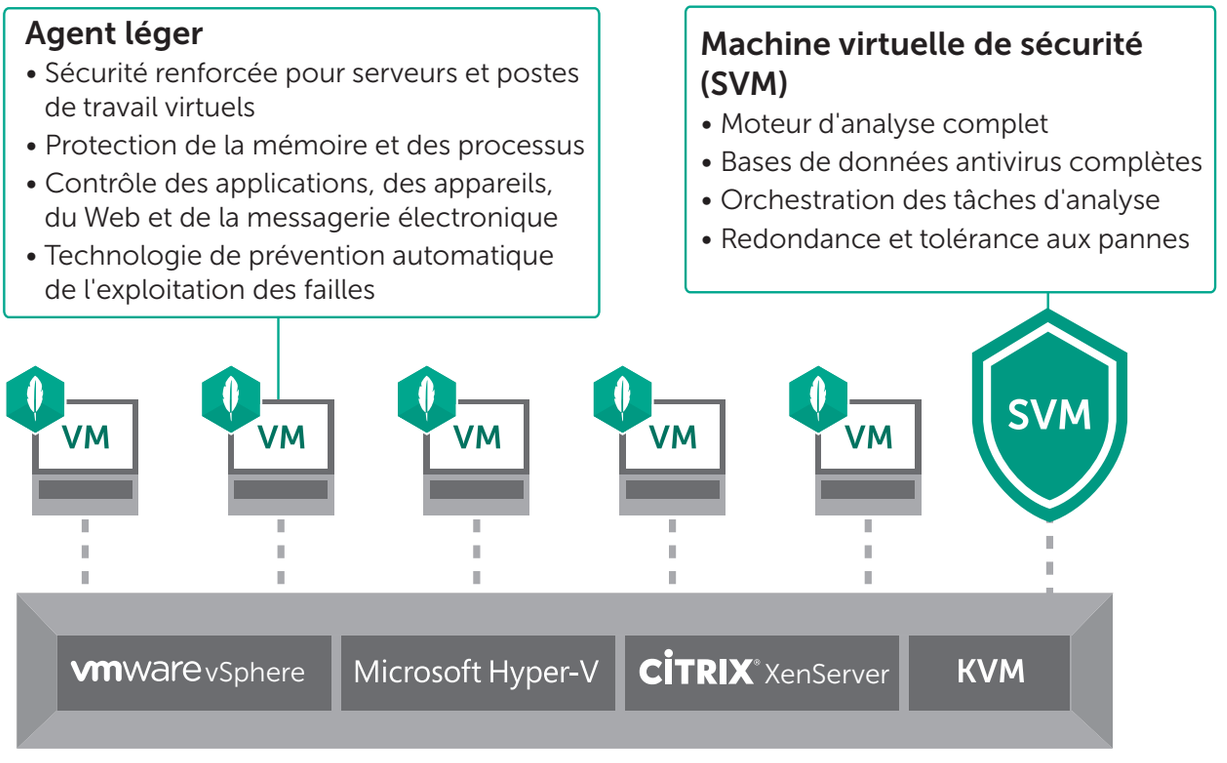
PROTECTION SOUPLE ET EFFICACE POUR LES SERVEURS VIRTUELS ET LES ENVIRONNEMENTS VDI

La solution Kaspersky Security for Virtualization prend en charge les plateformes les plus utilisées, notamment VMware vSphere, Citrix XenServer, Microsoft Hyper-V et KVM. Elle convient ainsi parfaitement aux environnements hétérogènes.

Cette solution s'appuie sur deux approches différentes :

- Sans agent : une appliance virtuelle par hôte exécute des analyses pour détecter les logiciels malveillants sur toutes les machines virtuelles
- Avec agent léger, afin de fournir des niveaux de protection supplémentaires pour chaque machine virtuelle (VM)

La sécurité de vos machines virtuelles est gérée depuis la console Kaspersky Security Center, tout comme vos terminaux, serveurs physiques ou appareils mobiles.



Protection des serveurs de stockage

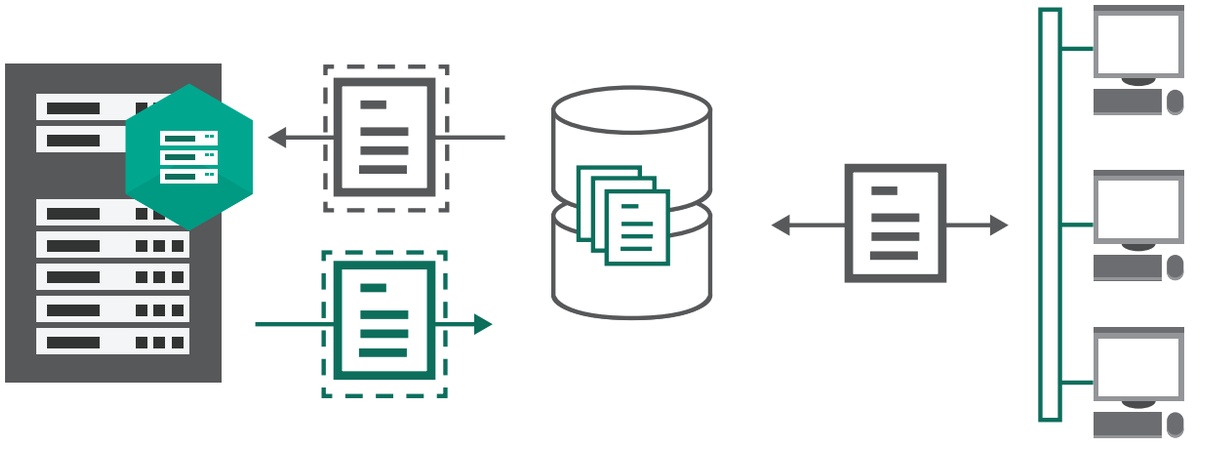
KASPERSKY SECURITY FOR STORAGE

SÉCURITÉ POUR LES DERNIERS SERVEURS NAS

Kaspersky Security for Storage protège efficacement les serveurs NAS (Network Attached Storage) des marques EMC, NetApp, Dell, Hitachi, Oracle et IBM, ainsi que d'autres NAS compatibles ICAP ou RPC :

- Architecture unifiée, tolérant les pannes
- Impact minimal sur les performances NAS
- Sécurité évolutive des environnements de stockage
- Mises à jour automatiques des bases de données de programmes malveillants
- Sauvegarde des objets suspects
- Analyse programmée ou à la demande

Architecture Kaspersky Security for Storage



Serveur Antivirus avec Kaspersky Security for Storage

Stockage EMC VNX et/ou NetAppp

Utilisateurs (Entreprise)

Protection contre la fraude en ligne et sur mobile

KASPERSKY FRAUD PREVENTION

SOLUTION DESTINÉE AUX BANQUES

Kaspersky Fraud Prevention renforce le système de sécurité existant des banques, ce qui permet d'offrir un nouveau niveau de protection contre la fraude. La solution protège les comptes numériques, les ordinateurs et les appareils mobiles des utilisateurs, ainsi que les systèmes de la banque. En protégeant les transactions et les comptes des clients, Kaspersky Fraud Prevention aide les banques à renforcer la fidélité de leur clientèle.

Kaspersky Fraud Prevention prévient activement :

- le piratage de compte
- la falsification de transaction
- le vol d'identité

Kaspersky Fraud Prevention :

- protège 100 % de vos clients, indépendamment de l'appareil ou de la plateforme qu'ils utilisent.
- permet à votre banque de détecter le plus tôt possible l'accès aux comptes par des clients infectés.
- permet de protéger les utilisateurs accédant à leurs comptes bancaires depuis un appareil mobile (Android, iOS et Windows Phone).
- fonctionne sur les PC et Mac de vos clients et leur offre une protection efficace, à la source, contre les programmes malveillants et les attaques sur Internet.
- protège les comptes bancaires numériques contre les tentatives de prise de contrôle de compte.

Protection contre les attaques DDoS

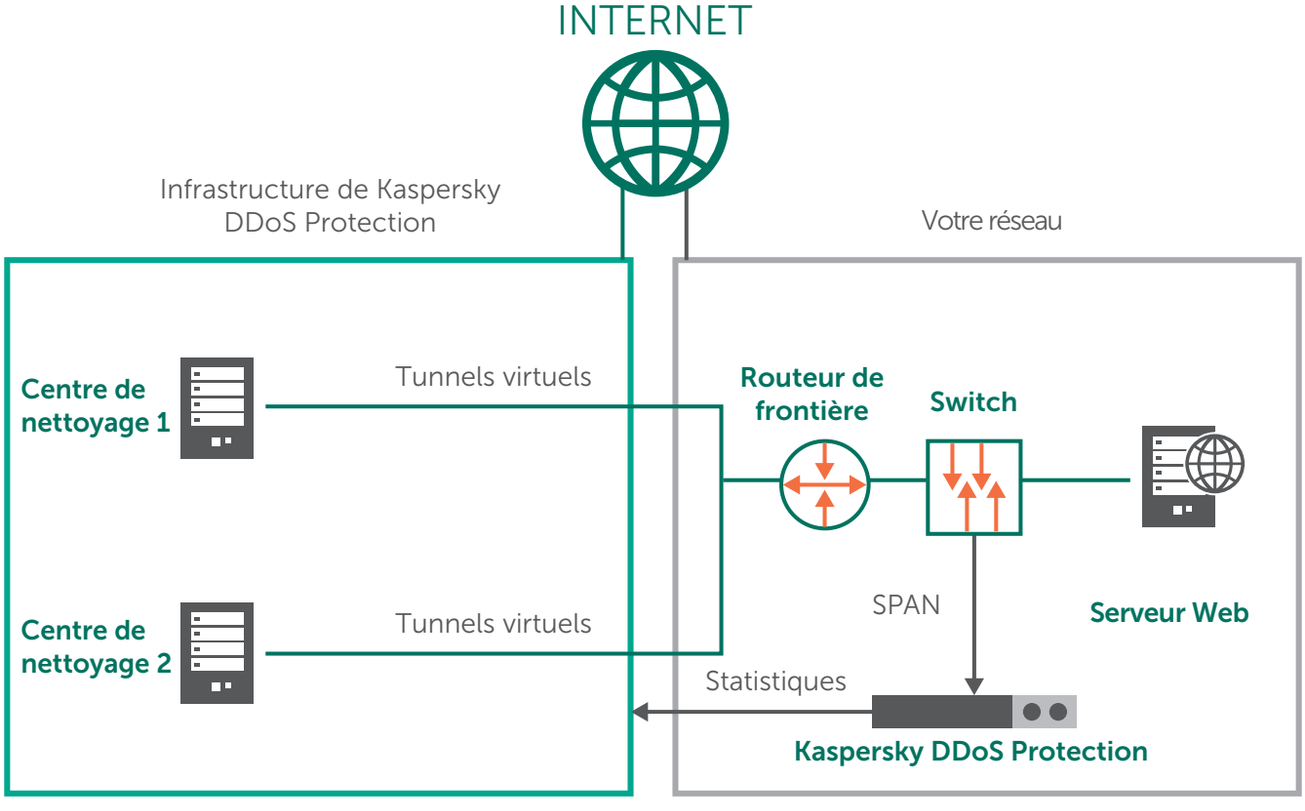
KASPERSKY DDOS PROTECTION

Pour protéger votre entreprise contre les attaques DDoS, vous devez disposer d'une solution qui détecte les attaques le plus rapidement possible. Nos équipes de surveillance des menaces utilisent des méthodes sophistiquées pour étudier le paysage des attaques DDoS et conserver une longueur d'avance sur les pirates.

Kaspersky DDoS protection offre :

- un logiciel de sonde spécifique, fonctionnant au sein de l'infrastructure du client
- des centres de nettoyage du trafic
- des alertes sur les attaques potentielles
- un trafic sécurisé : le centre de nettoyage ne filtre le trafic que pendant une attaque
- une analyse et des rapports détaillés après l'attaque sur le lieu et la manière dont celle-ci s'est déroulée

Architecture de Kaspersky Ddos Protection



Technologie de chiffrement

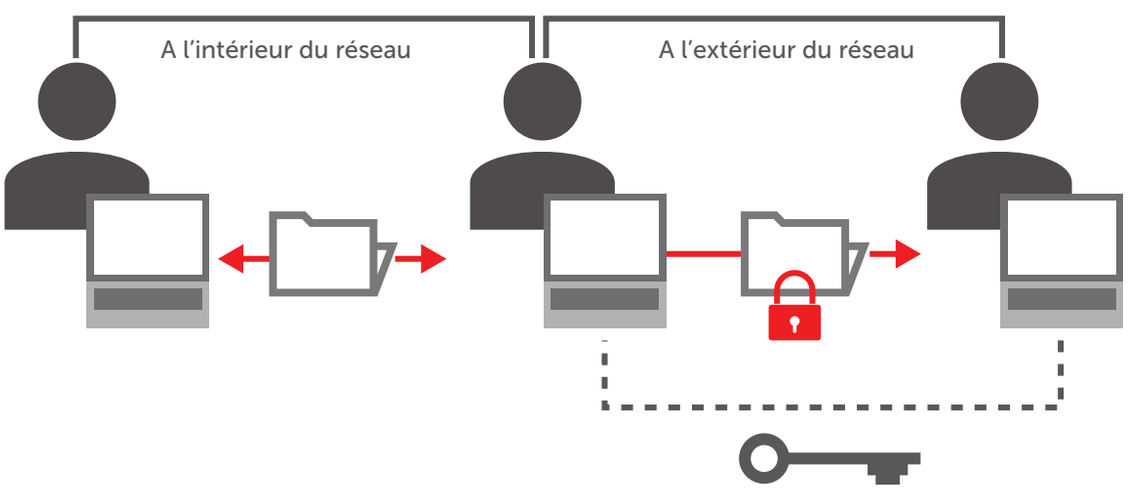
La technologie de chiffrement de Kaspersky Lab empêche l'accès non autorisé à vos données en cas de perte ou de vol d'un appareil ou d'une attaque malveillante ciblant vos données.

Flexibilité totale dans le choix des éléments à chiffrer :

- Chiffrement intégral de disque (FDE)
- Chiffrement au niveau des fichiers/dossiers (FLE)
- Périphériques amovibles (clés USB, disques durs externes)

La technologie de chiffrement de Kaspersky Lab travaille de manière transparente sur l'ensemble des applications, sans compromettre la productivité de l'utilisateur final. L'authentification unique permet un chiffrement en toute transparence, l'utilisateur final n'ayant peut-être même pas conscience que la technologie fait son travail.

Principe de chiffrement



Le chiffrement des données est inclus dans KESB Advanced et Total.

Services de veille stratégiques

SURVEILLANCE DES MENACES

Votre système SIEM dispose-t-il des capacités nécessaires de détection des cybermenaces ? Pouvez-vous avoir l'assurance d'être averti à temps des menaces les plus dangereuses ? Notre portefeuille de services de surveillance des menaces est conçu pour donner aux entreprises les outils nécessaires pour gérer ces risques :

- **Flux d'informations sur les menaces** : optimisez votre solution SIEM et approfondissez vos compétences en matière de criminalité grâce à nos tout derniers flux d'informations sur les cybermenaces. Nos solutions s'intègrent aux principaux SIEM du marché (QRadar, Splunk, ArcSight, etc.)
- **Les rapports de surveillance des menaces APT** permettent d'obtenir un accès exclusif et proactif aux descriptions des campagnes de cyberespionnage les plus sophistiquées, et notamment aux indicateurs de compromission (IOC).
- **Les rapports de veille sur les menaces spécifiques au client** identifient toutes les composantes essentielles de votre réseau disponibles à l'extérieur.

SERVICES D'EXPERTS

Votre expertise interne est-elle suffisante pour résoudre un cyberincident ? Votre infrastructure informatique ou vos applications spécifiques sont-elles entièrement sécurisées face aux cyberattaques potentielles ? Nos services d'experts sont conçus pour atténuer et résoudre ces risques :

- **Tests de pénétration** : apprenez à identifier les points les plus faibles de votre infrastructure et à éviter les dommages provoqués par les cyberattaques. Respectez ainsi les normes du gouvernement, de l'industrie et de l'entreprise (par ex. PCI DSS).
- **Évaluation de la sécurité des applications** : ce service permet d'identifier les vulnérabilités des applications, des solutions reposant sur le Cloud, des systèmes ERP, des services bancaires en ligne et autres applications professionnelles spécialisées aux applications mobiles et embarquées sur différentes plates-formes.
- **Cyberdiagnostic et analyse des programmes malveillants** : ce service retrace de façon détaillée l'historique de tout incident à partir de rapports complets, comprenant notamment les différentes étapes de résolution de l'incident.

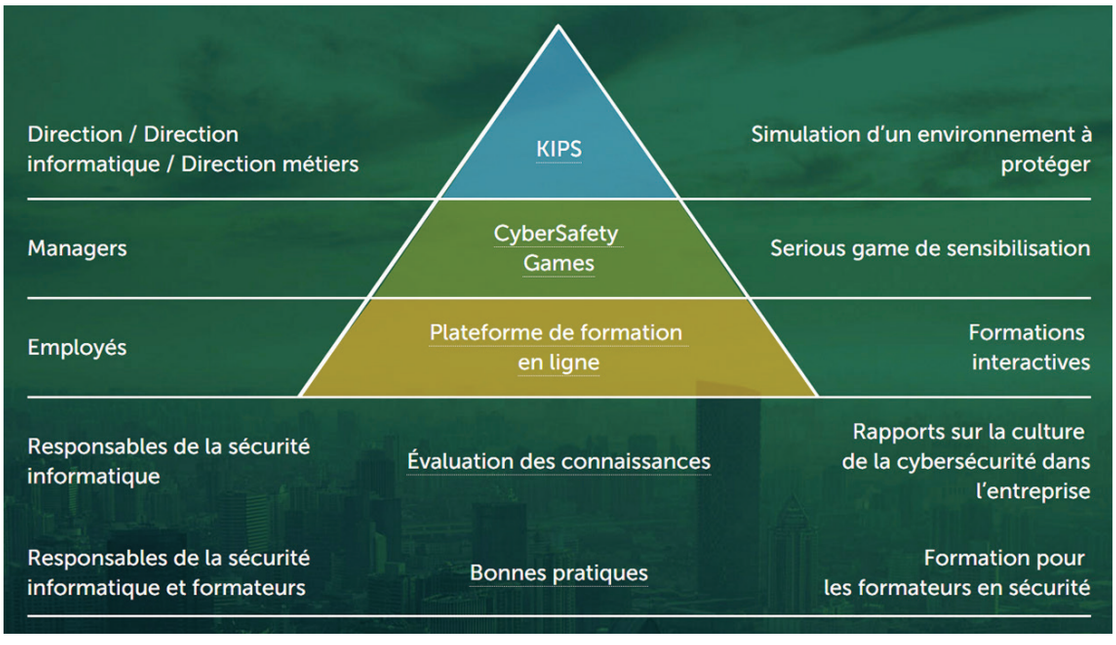
Formations

FORMATIONS À LA CYBERSÉCURITÉ

Nous proposons un portefeuille de formations de sensibilisation à la cybersécurité, ainsi qu'un large choix de programmes de formation, du niveau de base au niveau expert en cybercriminalité et en analyse de programmes malveillants.

- **Sensibilisation des utilisateurs finaux à la cybersécurité** : elle aide les entreprises à renforcer les connaissances de leurs employés en matière de sécurité.
- **Formation pour les professionnels de la sécurité informatique** : couvrant tous les niveaux, elle améliore les compétences des experts en sécurité de votre entreprise et réduit les risques d'incidents.

Nos programmes de formation et de sensibilisation s'adressent à tous les niveaux de l'entreprise.



Protection des Data Centers

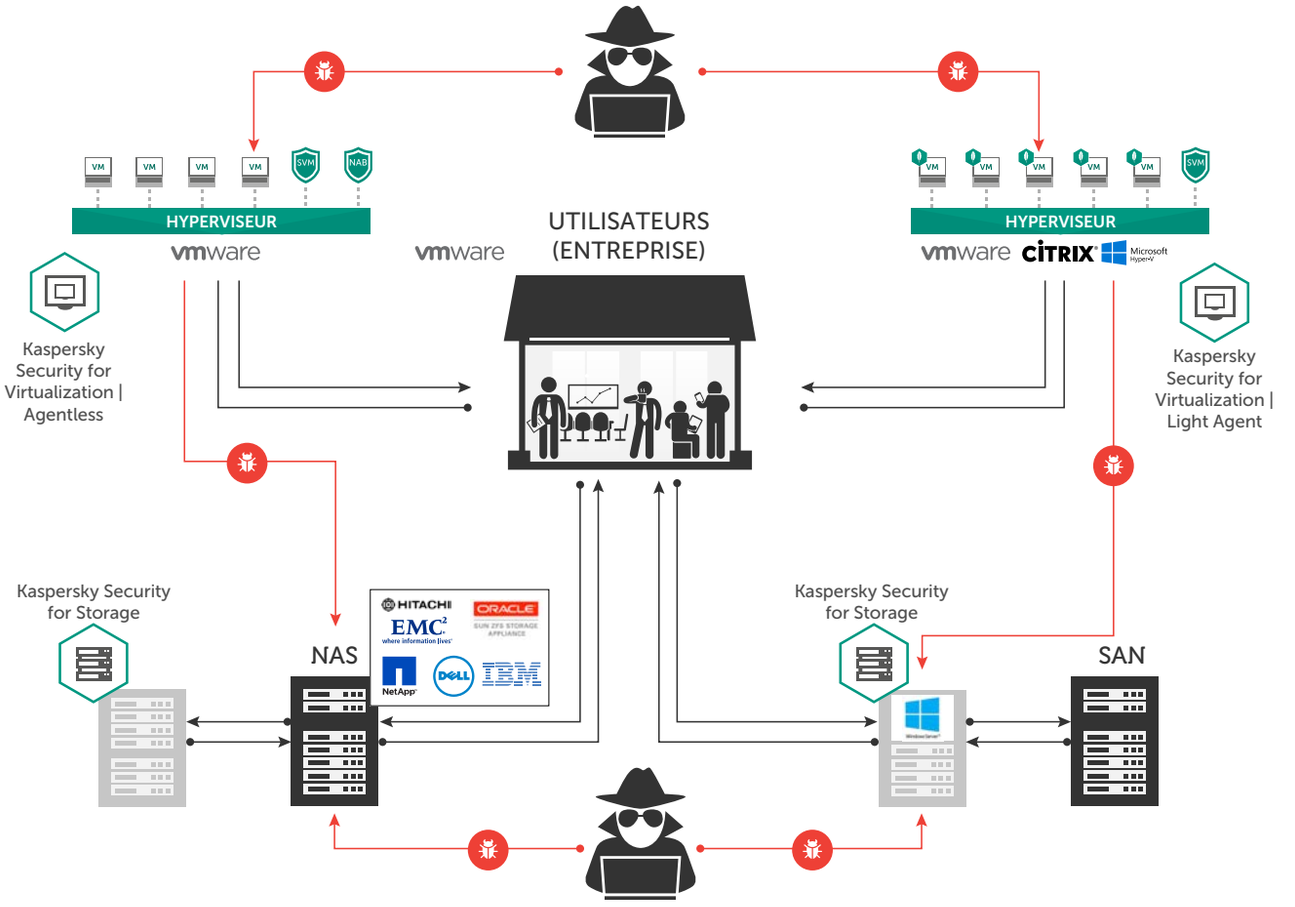
Protection des Data Centers en combinant 2 solutions Kaspersky Lab :

- SECURITY FOR VIRTUALIZATION

- SECURITY FOR STORAGE

Nous proposons des solutions centrées sur la protection de deux secteurs essentiels de votre data center : l'infrastructure virtuelle et les systèmes de stockage de données. Convenant idéalement aux environnements à plusieurs hyperviseurs et systèmes de stockage, ces solutions Kaspersky Lab comprennent :

- des mesures de sécurité conçues spécifiquement pour les plates-formes principales de virtualisation, dont VMware, Citrix, Microsoft et KVM.
- des mesures de sécurité destinées aux systèmes de stockage en réseau (NAS), notamment EMC, NetApp, DELL, IBM, Hitachi et Oracle.

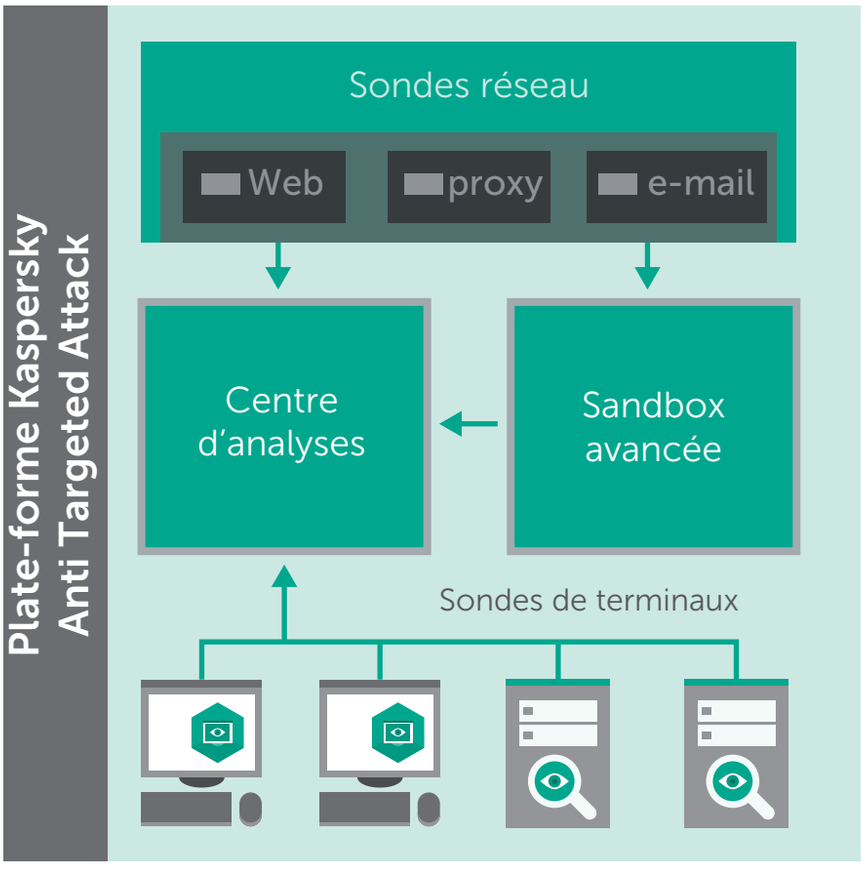


Protection contre les attaques ciblées – APT

KASPERSKY ANTI TARGETED ATTACK

Kaspersky Anti Targeted Attack est une plate-forme utilisant à la fois les données recueillies par notre service de veille stratégique mondiale, et de puissantes technologies de détection et d'analyse :

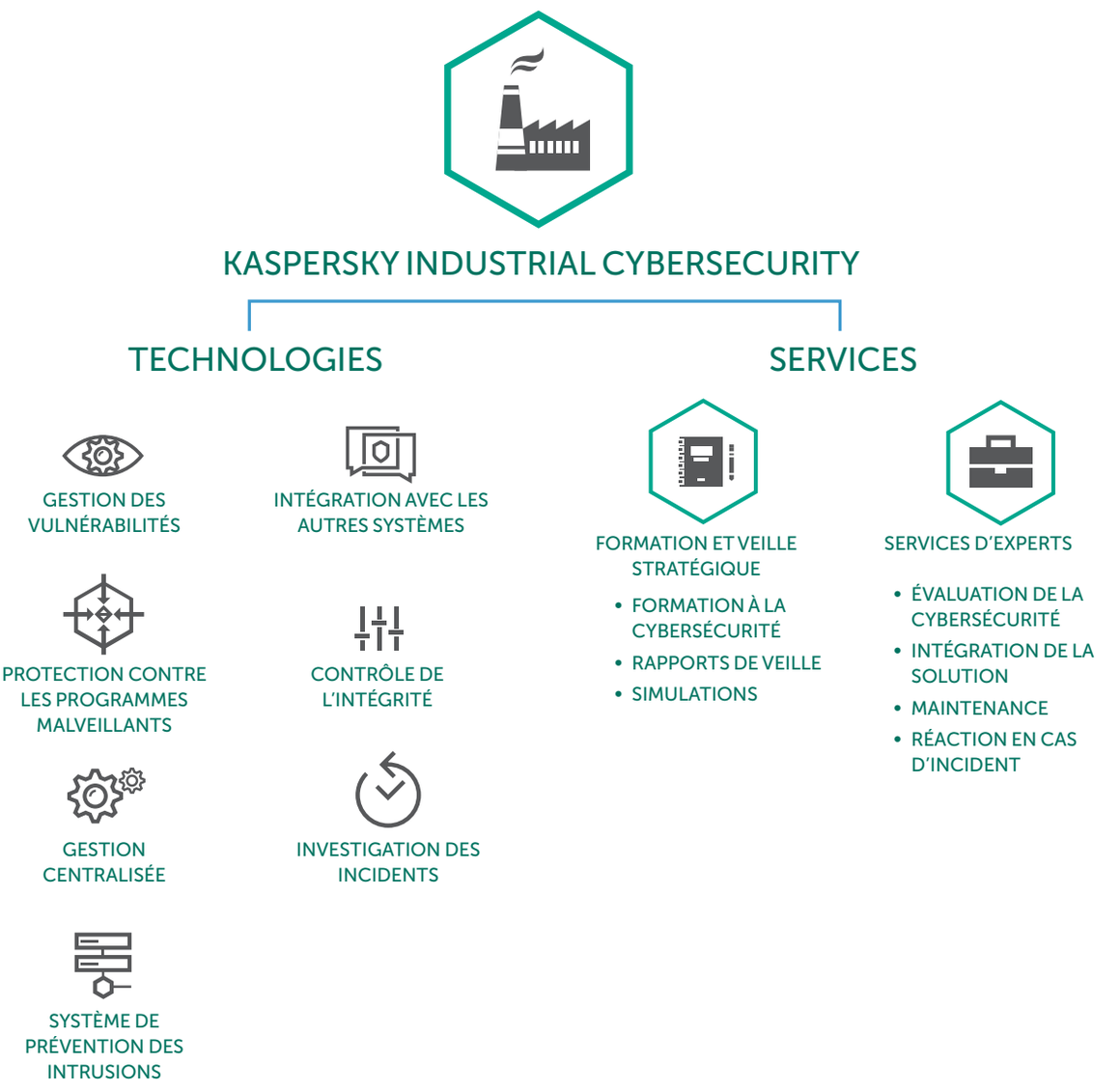
- **une architecture de sondes multi-niveaux**, pour une visibilité à 360 degrés : une combinaison de sondes réseau, Web et de messagerie électronique, ainsi que de sondes de terminaux.
- **une sandbox avancée**, pour évaluer les nouvelles menaces. Elle propose un environnement isolé et virtualisé où les objets suspects peuvent être exécutés en toute sécurité, afin d'en observer le comportement.
- **des moteurs d'analyse puissants**, pour des diagnostics rapides et moins de faux positifs. Notre analyseur d'attaques ciblées évalue les données du réseau et des terminaux saisies par les sondes, puis génère rapidement des diagnostics de détection des menaces destinés à votre équipe de sécurité.



Protection des environnements industriels critiques

KASPERSKY INDUSTRIAL CYBERSECURITY

Kaspersky Industrial CyberSecurity est spécialement conçu pour tenir compte des besoins uniques de l'industrie et se focalise notamment sur la préservation de la continuité des processus technologiques. Les paramètres polyvalents et flexibles de la solution permettent de configurer cette dernière pour répondre aux exigences et besoins uniques de chaque installation industrielle.



Protection des DAB et des terminaux de points de vente

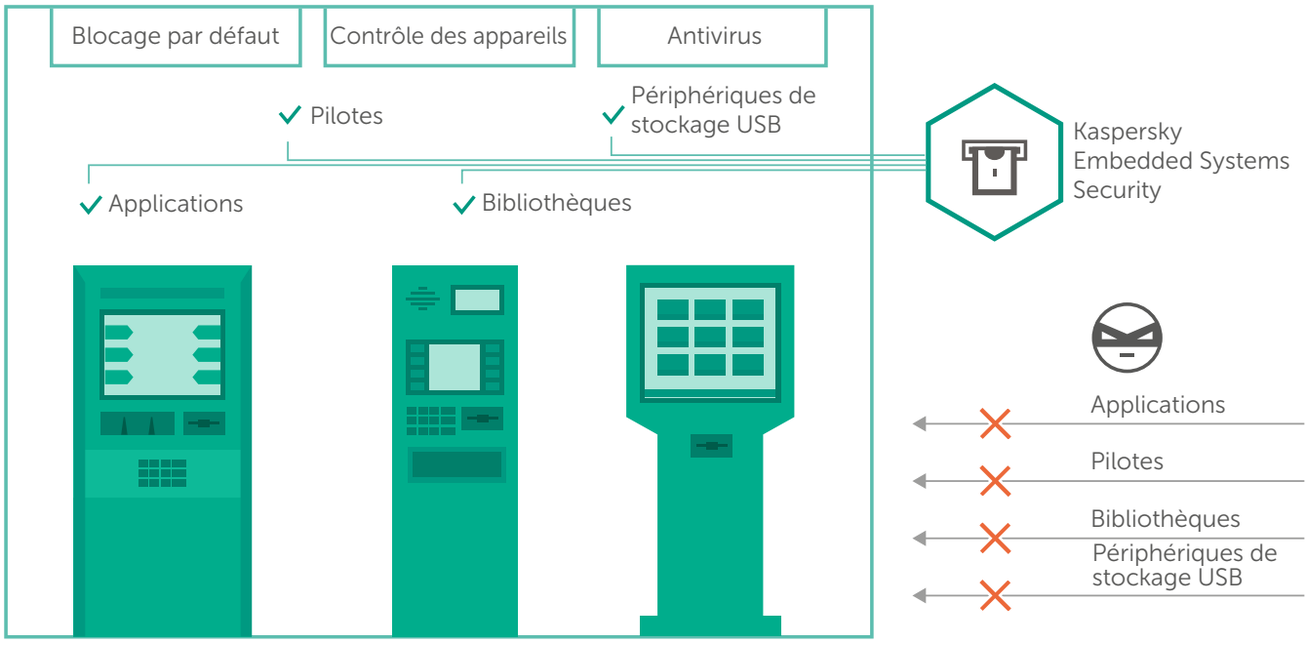
KASPERSKY EMBEDDED SYSTEMS SECURITY

Kaspersky Lab a conçu une solution de sécurité spécifiquement destinée aux entreprises gérant des distributeurs automatiques de billets et des terminaux de points de vente.

Kaspersky Embedded Systems Security propose notamment un mode « blocage par défaut uniquement », où la configuration requise débute à 256 Mo de RAM et 50 Mo d'espace disque disponible, avec le système d'exploitation Windows XP et du matériel de faible puissance.

Cette solution unique répond à trois objectifs clés :

- une sécurité efficace pour les systèmes « difficiles à gérer »
- la conformité avec les exigences PCI DSS 5.1, 5.1.1, 5.2, 5.3 et 6.2
- un étalement chronologique en douceur pour le remplacement des systèmes et des équipements obsolètes



La protection Cloud Kaspersky Lab

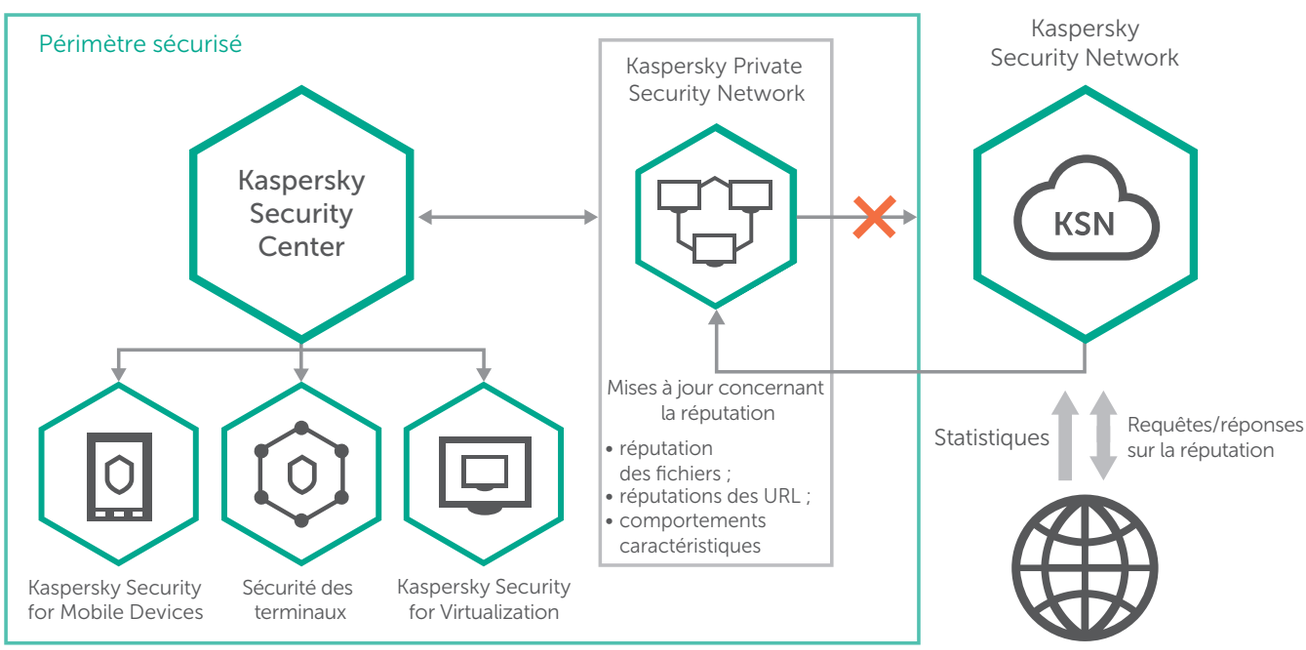
KASPERSKY SECURITY NETWORK

Les solutions de sécurité standard ont besoin de 4 heures pour recevoir les informations nécessaires à la détection et à l'interception des quelque 310 000 nouveaux programmes malveillants découverts chaque jour par les chercheurs de Kaspersky Lab. Le service de partage des informations sur les menaces via le réseau Kaspersky Security Network fournit ces données en 30 à 40 secondes.

KASPERSKY PRIVATE SECURITY NETWORK

Kaspersky Private Security Network apporte une réponse aux principaux problèmes de cybersécurité des entreprises sans qu'une seule donnée ne quitte le réseau local.

- identifie les sources des programmes malveillants et évite leur propagation
- identifie et différencie les attaques ciblées des menaces d'ordre plus général
- limite les dommages causés par les incidents de cybersécurité
- évalue la recherche d'incidents et les besoins en matière de mesures correctives
- réduit les faux positifs
- respecte les normes strictes en matière de confidentialité, de sécurité et de réglementation



Contrats de maintenance et support

MAINTENANCE SERVICE AGREEMENT (MSA)

Une assistance de qualité en cas d'incident, de problèmes de configuration, d'incompatibilité et autre est essentielle pour les entreprises qui recherchent la tranquillité d'esprit et une disponibilité optimale.

En cas de besoin, les spécialistes Kaspersky Lab seront disponibles via des lignes téléphoniques prioritaires dédiées, en français, dans des délais d'intervention adaptés aux besoins de votre entreprise. Le schéma ci-dessous décrit les options d'assistance disponibles.

	Assistance standard		Assistance supérieure	
	MSA Starter	**MSA Plus**	**MSA Business**	**MSA Enterprise**
Ligne téléphonique prioritaire	Oui	Oui	Oui	Oui
Responsable technique du compte	Non	Non	Oui	Oui, dédié
Assistance en langue locale	8 x 5	8 x 5	8 x 5	24 x 7 x 365
Assistance, niveau de gravité 1	8 x 5	8 x 5	24 x 7 x 365	24 x 7 x 365
Délai d'intervention, niveau de gravité 1	8 heures de travail	6 heures de travail	4 heures	30 minutes
Assistance, niveau de gravité 2	8 x 5	8 x 5	8 x 5	24 x 7 x 365
Services professionnels Consultation	Non	Non	Coût additionnel	Bilan technique et rapports personnalisés
Nombre d'incidents	6	12	36	Illimité

SERVICES PROFESSIONNELS

- **Service découverte** : vous garantit une utilisation optimale de nos produits en fonction des besoins spécifiques de votre entreprise.
- **Service de mise à niveau** : assistance technique supplémentaire au cours d'un projet de mise à niveau d'un produit Kaspersky Lab.
- **Service de configuration** : recommandations en termes de paramètres de configuration et de politiques.
- **Service de bilan technique** : audit de l'environnement du réseau et des paramètres des produits du client (sur place ou à distance) et réalisation, par nos experts, d'un rapport complet contenant des recommandations pour optimiser la sécurité de l'entreprise.
- **Service de conseil** : service personnalisé (incluant bonnes pratiques, conseils, formations et apprentissages ciblés) veille à l'efficacité de votre réaction face au changement sans interrompre les activités de votre entreprise. Un service complet de dépannage est inclus.


Twitter.com/
kasperskyfrance


Facebook.com/
kasperskylabfrance


Youtube.com/
/user/KasperskyFrance

Kaspersky Lab France,
Rueil Malmaison
www.kaspersky.fr

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

Trouver un partenaire près
de chez vous :
www.kaspersky.fr/partners

KASPERSKY lab