kaspersky

Solutions de sécurité Kaspersky pour les entreprises

Sommaire

À propos du portefeuille de solutions pour les entreprises de Kaspersky

Le portefeuille de solutions pour les entreprises de Kaspersky reflète les exigences de sécurité des entreprises d'aujourd'hui, répondant ainsi aux besoins des organisations à différents niveaux de maturité avec une approche étape par étape. Cette approche associe différents niveaux de protection contre tous les types de cybermenaces pour détecter les attaques les plus complexes, réagir rapidement et de manière appropriée à tout incident, et prévenir les menaces futures.

Rôle de la sécurité des terminaux dans une planification à long terme

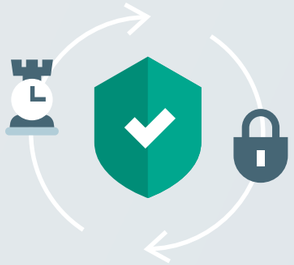
Processus d'évolution de la sécurité traditionnelle

Facteurs décisionnels :

- Tendances du marché
- Solution de sécurité en silo
- Gestion des urgences
- Mise enconformité

L'apport des produits traditionnels :

- Protection des endpoints
- Pare-feu/NGFW (Next Generation Firewall)
- Pare-feu d'application Web
- Prévention des pertes de données
- SIEM

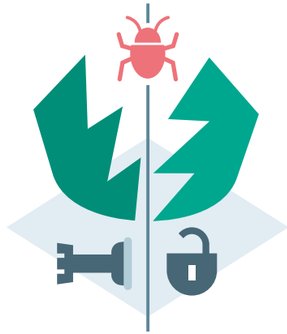


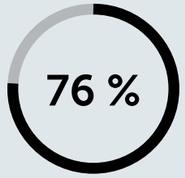
Attributs

- Planification de la sécurité à court terme
- Dépendance aux technologies et fonctionnalités
- Défense périmétrique du réseau

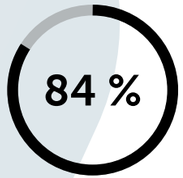
Pourquoi les approches traditionnelles échouent-elles ?

- Complexité croissante des menaces et de l'environnement à risque
- Complexité des technologies de cybersécurité
- Exigences des entreprises pour une stratégie de cybersécurité à long terme





De toutes les alertes sont générées par des terminaux



De toutes les violations de terminaux impliquent plusieurs terminaux

Les terminaux sont les points d'entrée les plus communs dans l'infrastructure d'une organisation, la principale cible des cybercriminels et les principales sources des données nécessaires pour examiner efficacement les incidents complexes.

Solutions de sécurité Kaspersky pour les entreprises

3 étapes vers la planification d'une cybersécurité avancée pour les entreprises

1 Les bases de la sécurité

Environnement à risques étendu

Renforcement des systèmes et blocage automatique d'un maximum de menaces.

Terminaux
- **Kaspersky Endpoint Security for Business**
- **Kaspersky Embedded Systems Security**

Réseau
- **Kaspersky Secure for Mail Server**
- **Kaspersky Security for Internet Gateway**

Cloud
- **Kaspersky Hybrid Cloud Security**

Support
- **Kaspersky Premium Support and Professional Services**

Stockage
- **Kaspersky Security for Storage**

Sensibilisation
- **Kaspersky Security Awareness**

2 Défense avancée

Menaces avancées et attaques ciblées

Détection avancée et réponse rapide face aux menaces complexes non détectées par les solutions préventives.

Terminaux
- **Kaspersky Endpoint Detection and Response**

Services
- **Kaspersky Targeted Attack Discovery Service**

Réseau
- **Kaspersky Anti Targeted Attack**

Veille
- **Kaspersky Threat Intelligence**

Formation
- **Kaspersky Cybersecurity Training**

Confidentialité
- **Kaspersky Private Security Network**

3 Approche de cybersécurité intégrée

Campagnes ciblées et cyberarmes

Préparation aux attaques APT. Niveau élevé d'expertise, fonctionnalités de Threat Intelligence avancées et recherche de menaces en continu.

- **Kaspersky Threat Management & Defense**

4 avantages de cette approche

- Sert de base au développement d'une stratégie de cybersécurité à long terme, en tenant compte des particularités de l'entreprise et de l'évolution des risques liés à l'environnement.
- Investissement optimisé en matière de technologie de sécurité et coût total de possession réduit.
- Réduction des dommages financiers et opérationnels causés par la cybercriminalité.
- Augmentation du retour sur investissement grâce à l'automatisation transparente des flux de travail et à l'absence d'interruption des processus métier.

1 Les bases de la sécurité

Technologies préventives automatisées et sensibilisation à la sécurité

Blocage automatique d'un maximum de menaces

Solution idéale pour les TPE/PME qui ne disposent d'aucune équipe de sécurité dédiée ou d'une expertise très limitée en cybersécurité

- Prévention automatisée multivecteurs d'un grand nombre d'incidents potentiellement causés par des menaces «classiques».
- Étape fondamentale pour les moyennes et grandes entreprises afin de concevoir une stratégie de protection intégrée contre les menaces complexes.

Terminaux

- **Kaspersky Endpoint Security for Business**
- **Kaspersky Embedded Systems Security**

Cloud

- **Kaspersky Hybrid Cloud Security**

Réseau

- **Kaspersky Secure Mail Gateway**
- **Kaspersky Security for Internet Gateway**

Formation

- **Kaspersky Security Awareness**

Stockage

- **Kaspersky Security for Storage**

Support

- **Kaspersky Premium Support**
- **Kaspersky Professional Services**

Solutions de sécurité Kaspersky pour les entreprises

Kaspersky Endpoint Security for Business

Les terminaux sont la principale sources des cyberattaques visant les entreprises. En raison de fonctionnalités de prévention et d'automatisation limitées, les experts se retrouvent souvent surchargés par des incidents de sécurité. Chaque terminal peut entraîner une interruption d'activité. Kaspersky Endpoint Security for Business bloque les menaces et renforce les terminaux en alliant sécurité évolutive et outils de contrôle étendus. Les menaces sont bloquées avant qu'elles ne puissent endommager les données ou nuire à la productivité de l'utilisateur, même lorsque le terminal se trouve hors du périmètre de l'entreprise.

Solution idéale pour les entreprises :

ayant des attentes croissantes et diversifiées en informatique

souhaitant réduire le risque et la fréquence des erreurs des utilisateurs entraînant des atteintes à la sécurité

1 Compétences requises

5 Personnalisation et évolutivité

2 Coût

Avantages

Empêche les interruptions d'activité et les erreurs humaines

Accompagne la transformation numérique et protège le personnel nomade

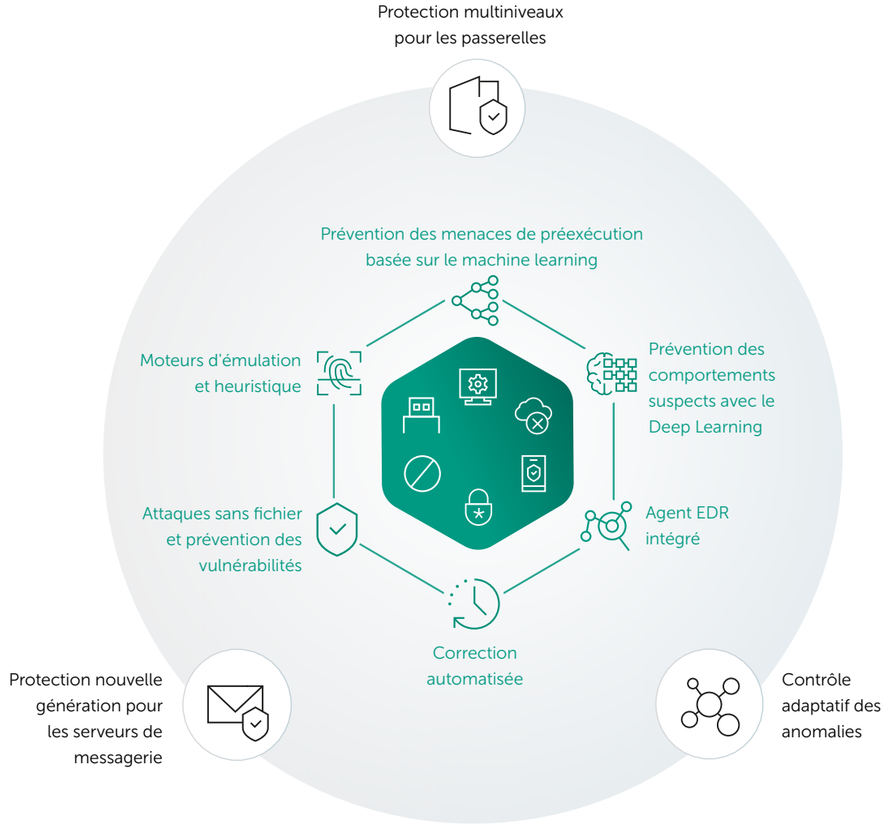
Améliore la préparation aux audits : permet de traquer et corriger les vulnérabilités, les écarts de configuration et les appareils non chiffrés

Optimise le retour sur investissement en réduisant la surface d'attaque et le nombre d'incidents à gérer

Permet de contrôler tous les terminaux grâce à une console intégrée et à un agent unifié

Utilisation

- Réduit l'exposition aux attaques en appliquant un renforcement évolutif et en protégeant les terminaux, les serveurs de fichiers et de messagerie ainsi que les passerelles Internet
- Garantit la conformité des terminaux aux exigences réglementaires
- Automatise la détection, la réponse et les tâches de déploiement de logiciels, faisant ainsi gagner du temps aux experts en sécurité
- Rationalise l'intégration et l'adoption d'autres technologies de sécurité



Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security est une solution qui simplifie et sécurise la transformation numérique lorsque les organisations virtualisent ou déplacent leurs charges de travail dans le cloud. La technologie brevetée Light Agent permet la centralisation et l'optimisation intelligente des fonctionnalités de sécurité, réduisant ainsi considérablement l'utilisation des ressources d'hyperviseur. L'intégration native à une large gamme de plates-formes de virtualisation, de conteneurs et de clouds publics assure une visibilité et un contrôle cohérents dans l'ensemble de l'infrastructure. Un ensemble complet de technologies de sécurité gérées à partir d'une console unique assure une gestion rationalisée des risques dans divers environnements au quotidien.

Solution idéale pour les entreprises :

qui virtualisent les charges de travail des postes de travail et serveurs

qui migrent ou conservent leurs infrastructures dans des clouds publics

exploitant des clouds publics et des conteneurs pour les opérations DevOps

Avantages

Assure une visibilité et un contrôle cohérents à l'échelle des déploiements de data center et dans le cloud

Réduit la surface d'attaque et les temps d'arrêt ce qui complique tout mouvement latéral

Libère jusqu'à 30 % des ressources d'hyperviseur et réduit la durée de connexion de quelques minutes à quelques secondes

Accompagne la mise en conformité

Assure une collaboration efficace entre le service informatique et les équipes de développement et de sécurité des informations, ce qui permet de réduire les risques et les lacunes en matière de sécurité

Utilisation

- Protection des ressources pour les infrastructures de serveurs virtualisés
- Sécurité pour VMWare et Citrix VDI
- Assure la conformité en respectant les exigences de sécurité de base
- Protection des charges de travail dans le cloud pour les instances AWS et Azure avec un déploiement automatisé et une visibilité cohérente via l'intégration d'API natives
- Sécurité pour les opérations DevOps grâce à la protection de conteneur et à l'API de gestion

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server protège contre les menaces par email, les empêchant d'atteindre le terminal, source de la plupart des piratages informatiques et programmes malveillants. Tous les types de programmes malveillants (ransomwares et cryptomineurs inclus) sont bloqués, ainsi que les tentatives de phishing, avec une attention particulière à la prévention des attaques BEC (Business Email Compromise). La solution bloque également l'envoi de mass mails indésirables et empêche ainsi les transmissions de données indésirables.

Solution idéale pour les entreprises :

disposant d'un service informatique bien développé et ayant des préoccupations concernant la sécurité des données et leur confidentialité

comptant fortement sur les communications par email et exigeant une gestion granulaire

souhaitant enrichir leurs données de détection APT avec le contexte des emails, mais aussi bloquer les composants APT véhiculés par email

Avantages

Augmente la productivité en bloquant les mass mails indésirables (spam inclus) et en offrant des catégories de courriers pour une gestion plus pratique des communications

Permet d'éviter les interruptions d'activité en bloquant les menaces par email

Améliore la sécurité des données en empêchant le transfert indésirable de certaines données

Permet de réduire les frais de service en limitant les incidents au niveau de l'utilisateur

Améliore l'efficacité de la sécurité de la passerelle de messagerie existante en ajoutant des fonctionnalités de détection de meilleure qualité, sans faux positif supplémentaire

Utilisation

- Fonctionne avec un large éventail d'agents Mail Transfer externes ou comme appliance virtuelle complète
- Assure via des API la sécurité des serveurs Microsoft Exchange au niveau de la passerelle et de la boîte de réception
- Bloque le transfert indésirable de certains fichiers
- S'intègre à Kaspersky Anti Targeted Attack pour bloquer les composants APT véhiculés par email

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway offre une protection contre les menaces Web au niveau du périmètre de défense de l'entreprise, les empêchant d'atteindre la principale cible de toutes les formes d'attaques : le terminal. La solution permet d'empêcher le piratage informatique et bloque tous les types de logiciels malveillants (ransomwares et cryptomineurs inclus) ainsi que les tentatives de phishing. Associez-la à votre proxy pour des performances améliorées, ou déployez-la comme une appliance virtuelle complète, prête à l'emploi.

Solution idéale pour :

Toute entreprise disposant d'un service informatique développé et ayant des préoccupations concernant la sécurité des données et leur confidentialité

Les MSP et xSPs (opérateurs de télécommunications inclus)

2 Compétences requises

5 Personnalisation et évolutivité

1 Coût

Avantages

Empêche les interruptions d'activité en bloquant les menaces Web avant que quelqu'un ne clique dessus et ne les laisse entrer

Améliore l'efficacité de la sécurité de la passerelle Web existante en ajoutant des fonctionnalités de détection de meilleure qualité, sans faux positif supplémentaire

Permet de réduire les frais de service en réduisant le nombre d'incidents au niveau de l'utilisateur

Améliore la productivité et réduit les risques en régissant l'utilisation d'Internet et la transmission de certains types de fichiers

Offre des environnements multiclients pour faciliter le travail des MSP

Utilisation

- Bloque les ressources Web malveillantes et le phishing, ainsi que les logiciels malveillants téléchargés
- Empêche l'utilisation de ressources Web indésirables
- Permet de gérer des espaces de travail distincts avec leurs propres ensembles de règles
- Filtre les types de fichiers indésirables entrants et sortants, selon plusieurs critères
- S'intègre à Kaspersky Anti Targeted Attack en tant que sonde Web et bloque les composants d'attaques ciblées selon les résultats de la détection avancée

Kaspersky Security for Storage

Un système de stockage connecté facilement peut aisément devenir une source d'infection dans l'ensemble de l'infrastructure, mais aussi une cible pour les menaces comme les ransomwares. Kaspersky Security for Storage protège les données de l'entreprise et empêche l'infection du réseau grâce à un solide ensemble de technologies de protection qui s'appuient sur une Threat Intelligence mondiale. La solution comprend des fonctionnalités uniques (anti-chiffrement à distance, par exemple) activées par l'intégration aux API des systèmes de stockage.

Solution idéale pour les entreprises :

disposant d'un service informatique développé et ayant des préoccupations concernant la sécurité des données et leur confidentialité

utilisant de gros volumes de données privées/ sensibles (par exemple, banques, commerce en ligne et assurance)

2 Compétences requises

5 Personnalisation et évolutivité

4 Coût

Avantages

Protège les données lors de toute connexion aux systèmes de stockage sans intrusion dans le logiciel de stockage

Réduit les tâches administratives et renforce la sécurité grâce à une console d'administration centralisée

Préserve la continuité des activités en protégeant les données stockées contre les ransomwares et cryptowipers exécutés à distance

Accompagne la mise en conformité en offrant une sécurité pour une vaste gamme de modèles qui peuvent ensuite être utilisés comme systèmes de stockage réglementés

Utilisation

- Protège les systèmes de stockage connectés au réseau et le serveur sur lequel ils s'exécutent
- Chaque fois qu'un nouveau fichier apparaît dans le système de stockage sécurisé, ou qu'un fichier existant est modifié, une recherche de programmes malveillants est effectuée. Des analyses sur demande sont également possibles
- Lorsque les fichiers commencent à être chiffrés à distance, la solution détecte et bloque la source sur le réseau, empêchant tout autre dommage*

* Uniquement avec l'intégration d'API disponible pour certains systèmes de stockage

Kaspersky Embedded Systems Security

Doté d'une puissante Threat Intelligence, d'une détection des programmes malveillants en temps réel, de contrôles complets des appareils et des applications ainsi que d'une gestion flexible, Kaspersky Embedded Systems Security assure une sécurité tout-en-un spécialement conçue pour les systèmes embarqués.

Solution idéale pour

Services financiers

Vente au détail et transport

Fournisseurs de services DAB et PDV

Avantages

Atténue les risques liés aux menaces ciblant des infrastructures financières particulières

Répond aux exigences de conformité des réglementations telles que PCI/DSS, SWIFT, etc.

Optimise les coûts administratifs via une console d'administration unique

Cas d'utilisation

- Sécurise les systèmes embarqués rarement mis à jour et dispersés géographiquement qui présentent des préoccupations spécifiques et uniques en matière de sécurité
- Protection pour les systèmes Windows XP plus supportés, mais encore largement utilisés sur du matériel bas de gamme
- Une conception efficace offre une sécurité performante sans risque de surcharge des systèmes

2 Compétences requises

5 Personnalisation et évolutivité

3 Coût

Kaspersky Premium Support (MSA) service

Lorsqu'un incident de sécurité se produit, le temps nécessaire à l'identification de sa cause et à son élimination est crucial. La détection et la résolution rapides d'un problème peuvent permettre aux entreprises de réaliser des économies considérables. Nos forfaits MSA (Maintenance Service Agreement) sont spécifiquement conçus pour atteindre cet objectif. Accès 24 h/24 à nos experts, hiérarchisation appropriée et éclairée des problèmes avec des délais de réponse garantis et des correctifs privés : tout ce qui est nécessaire pour assurer la résolution de votre problème le plus vite possible.

Solution idéale pour toute organisation utilisant les produits Kaspersky

Avantages

Assure la continuité des activités grâce à des experts dédiés, chargés de traiter vos problèmes et de les résoudre aussi rapidement que possible

Réduction des coûts d'un incident de sécurité en accédant à une ligne de support prioritaire, mais aussi en assurant des délais de réponse garantis et des correctifs privés

Un responsable commercial technique dédié agit comme votre représentant Kaspersky avec le pouvoir de mobiliser toute l'expertise nécessaire pour résoudre rapidement vos problèmes

Utilisation

- Faites remonter vos problèmes critiques de manière accélérée aux spécialistes qui travaillent en coulisses au siège de Kaspersky. Ces experts sont les mieux placés pour délivrer rapidement la solution la plus adaptée à votre problème
- Des mesures proactives propres à votre système, dont des correctifs prioritaires et personnalisés, vous assurent une protection complète
- Réduisez le temps passé à la maintenance et au dépannage de vos précieuses ressources internes

1 Compétences requises

5 Personnalisation et évolutivité

3 Coût

Solutions de sécurité Kaspersky pour les entreprises

Kaspersky Professional Services service

La cybersécurité représente un investissement important. Tirez le meilleur parti de votre solution en faisant appel à des experts qui comprennent exactement la façon dont vous pouvez optimiser votre sécurité pour répondre aux besoins uniques de votre organisation. Nos experts en sécurité sont à votre disposition pour vous aider à déployer, configurer et mettre à niveau les solutions Kaspersky sur toute l'infrastructure informatique de votre entreprise, dans le respect de notre méthodologie et de nos bonnes pratiques.

Les services professionnels de Kaspersky comprennent :

- Déploiement et mises à jour
- Configuration
- Formation sur les produits

Solution idéale pour toute organisation utilisant les produits Kaspersky

1 Compétences requises
5 Personnalisation et évolutivité
3 Coût

Avantages

Optimise votre retour sur investissement sur vos solutions de sécurité en garantissant qu'elles fonctionnent à 100 % de leur capacité

Réduit les coûts pour le personnel informatique interne

Minimise les risques de temps d'arrêt grâce à des audits réguliers des configurations du produit, assurant ainsi des mécanismes de défense le plus à jour possible

Réduit la période d'adoption du produit, permettant ainsi de profiter plus rapidement de tous les bénéfices du produit dès sa mise en oeuvre

Utilisation

- Réduit les risques de mise en œuvre qui peuvent diminuer la protection, avoir un impact négatif sur la productivité et même entraîner un temps d'arrêt
- Minimise l'impact de la mise en œuvre de votre nouvelle solution de sécurité sur les opérations métier quotidiennes et réduit les coûts globaux de mise en œuvre
- Prépare votre personnel à gérer la maintenance continue du produit grâce à nos programmes de formation correspondants, permettant ainsi d'éviter les erreurs, de démontrer les comptabilités du produit et d'expliquer les principes opérationnels

Kaspersky Security Awareness

Nos programmes de formation ont pour objectif de modifier les habitudes des utilisateurs et de déclencher de nouveaux comportements. Le portefeuille de solutions de sensibilisation à la sécurité Kaspersky comprend :
- Automated Security Awareness Platform (ASAP) : solution de sensibilisation pour tous les salariés qui aspirent à renforcer leurs compétences en cyberhygiène
- Cybersecurity for IT Online (CITO) : formation destinée aux experts en informatique générale et qui souhaitent développer des compétences pratiques pour reconnaître un éventuel scénario d'attaque et recueillir des données sur les incidents ;
- Kaspersky Interactive Protection Simulation (KIPS) : expérience de jeu interactif sur le thème de la cybersécurité destiné aux décideurs.

Solution idéale pour les entreprises

ayant des attentes croissantes et diversifiées en informatique

souhaitant réduire le risque et la fréquence des erreurs des utilisateurs entraînant des atteintes à la sécurité

1 Compétences requises
4 Personnalisation et évolutivité
4 Coût

Avantages

Protège les entreprises de l'intérieur

Assure un « cyberenvironnement sûr » dans le cadre de la culture de l'entreprise

Réduit les erreurs humaines de 80 % maximum

Utilisation

- Renforce la vigilance par le biais de scénarios et situations types, simulations de cyberattaques, différentes tâches et explications
- Permet d'acquérir une meilleure compréhension des menaces potentielles et les compétences nécessaires pour y faire face
- Développe les compétences pratiques indispensables pour reconnaître une éventuelle attaque au cours d'un incident PC semblant inoffensif. Apprend également à recueillir des données sur les incidents pour les transmettre à la sécurité informatique
- Permet aux dirigeants et aux décisionnaires de mieux comprendre la sécurité

2 Défense avancée

Technologie de détection avancée et réponse centralisée

Solutions de sécurité Kaspersky pour les entreprises

Détection avancée et réponse rapide face aux menaces complexes non détectées par les solutions préventives

- Environnements informatiques de plus en plus complexes avec une surface d'attaque accrue
- Gestion d'une petite équipe de sécurité dotée d'une expertise limitée
- Capacités basiques de réponse à incident

Solution idéale pour les moyennes entreprises :

Protection
Kaspersky Endpoint Detection and Response

Formation
Kaspersky Cybersecurity Training

Services
Kaspersky Targeted Attack Discovery

Réseau
Kaspersky Anti Targeted Attack

Confidentialité
Kaspersky Private Security Network

Veille
Kaspersky Threat Intelligence

Kaspersky Endpoint Detection and Response

Pour vous défendre le plus tôt possible contre les menaces avancées, il est indispensable de compléter les technologies préventives avec des capacités avancées de détection et de réponse. Kaspersky EDR est une solution spécialisée qui traite les menaces avancées sur vos terminaux, en partageant un seul agent avec notre solution de protection Kaspersky Endpoint Security. Kaspersky EDR offre une visibilité complète sur tous les terminaux du réseau de l'entreprise, ce qui permet l'automatisation des tâches de routine afin de détecter, hiérarchiser, enquêter et neutraliser les menaces les plus complexes.

Solution idéale pour

les grandes entreprises

les organisations utilisant déjà Kaspersky Endpoint Security

les SOC (Security Operation Centers) et les équipes d'intervention en cas d'incident

4 Compétences requises

3 Personnalisation et évolutivité

2 Coût

Avantages

Réduit les risques liés aux menaces avancées et aux attaques ciblées

Optimise les coûts administratifs grâce à l'automatisation des tâches et à une interface métier simplifiée unique

Augmente la vitesse et l'efficacité du traitement des incidents

Augmente la productivité, faisant ainsi gagner du temps à vos équipes informatiques et de sécurité pour d'autres tâches

Accompagne la mise en conformité grâce à des politiques de sécurité internes et des exigences réglementaires

Utilisation

- Gère le cycle complet de protection des terminaux, du blocage automatique des menaces à la réponse aux incidents complexes en cas de menaces avancées, en utilisant un seul agent
- Fournit un accès rapide aux données du terminal, même lorsque des postes de travail compromis ne sont pas disponibles ou que les données sont chiffrées
- Vient compléter les enquêtes sur les incidents avec une recherche des menaces, une analyse IoA et un mappage MITRE ATT&CK
- Assure une réponse efficace dans des infrastructures distribuées, dans le cadre de vastes actions automatisées

Kaspersky Anti Targeted Attack

Le nombre et la qualité des attaques ciblées augmentent constamment. Pour contrer ces nouvelles menaces, il est nécessaire d'adapter en permanence vos systèmes de sécurité. Kaspersky Anti Targeted Attack se concentre sur la détection des menaces avancées au niveau du réseau, avec collecte de données, analyse et corrélation entièrement automatisées, et permet aussi de comprendre en détail l'étendue de la menace. Le résultat assure une protection efficace de l'infrastructure de votre entreprise contre les menaces complexes et les attaques ciblées, sans qu'aucune ressource supplémentaire ne soit nécessaire.

Solution idéale pour

les grandes entreprises

les équipes SOC

les MSSP

toute organisation respectant la conformité

4 Compétences requises

3 Personnalisation et évolutivité

5 Coût

Avantages

Réduit les risques liés aux menaces avancées et aux attaques ciblées

Réduit les dommages financiers et opérationnels en introduisant un seul système fiable pour assurer la protection contre les attaques complexes

Optimise les coûts administratifs grâce à l'automatisation des tâches et à une interface métier simplifiée unique

Rationalise les tâches grâce à l'automatisation transparente des flux de travail et à l'absence d'interruption des processus métier

Contribue à garantir la conformité aux exigences réglementaires

Utilisation

- Détection rapide des actions de cybercriminels qui contournent les technologies préventives, via la surveillance et le contrôle centralisés des points d'entrée potentiels dans l'infrastructure
- Détection de signes de menace et corrélation d'événements multivecteurs d'une attaque, pour assurer une enquête plus efficace
- En cas d'incident, mise à disposition de l'équipe d'intervention de toutes les informations nécessaires sur les menaces détectées

Solutions de sécurité Kaspersky pour les entreprises

Kaspersky Private Security Network

Kaspersky Private Security Network 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. Il s'agit d'une version totalement privée, locale et personnelle de Kaspersky Security Network pour les entreprises.

Solution idéale pour

les entreprises aux exigences strictes en matière de contrôle des données

les infrastructures critiques dotées de réseaux physiquement isolés

les opérateurs de télécommunications, MSP et autres

Avantages

Assure une meilleure détection des menaces ciblant votre entreprise

Garantit des temps de réponse plus rapides grâce à un accès en temps réel aux statistiques concernant les menaces et la réputation

Augmente l'efficacité opérationnelle en réduisant les faux positifs

Respecte les normes réglementaires pour la sécurité des environnements et systèmes isolés

Utilisation

- Tous les avantages de la sécurité hébergée dans le cloud, sans la nécessité de partager des informations en dehors de votre infrastructure contrôlée
- Permet d'établir une protection personnalisée en ajoutant vos propres « verdicts »
- Solution adaptée aux réseaux critiques isolés

4 Compétences requises

4 Personnalisation et évolutivité

5 Coût

Kaspersky Targeted Attack Discovery

service

Kaspersky Targeted Attack Discovery est un service d'évaluation complet qui détermine si vous êtes actuellement la cible d'une attaque, ce qui se passe et qui est le cybercriminel. Nos experts détectent, identifient et analysent les incidents en cours ainsi que ceux qui ont eu lieu auparavant, et dressent une liste des systèmes affectés par ces attaques. Nous vous aidons à repérer les éventuelles activités frauduleuses, à identifier quelles peuvent être les sources d'un incident et à planifier les mesures correctives les plus efficaces.

Solution idéale pour

les entreprises ne comptant aucune équipe de sécurité ou peu matures sur le sujet des attaques avancées

les institutions gouvernementales

les infrastructures critiques

Avantages

Prévient et limite les dommages résultant d'un système compromis, réduisant ainsi considérablement le coût des incidents

Permet de maintenir la relation de confiance avec vos clients, partenaires et investisseurs, afin de favoriser les opportunités commerciales

Permet d'éviter les pénalités et amendes

Renforce votre protection contre de futurs incidents grâce à des recommandations de remédiation

Utilisation

- Permet de comprendre l'empreinte numérique de votre organisation et les risques connexes
- Permet d'évaluer le risque en effectuant des inspections approfondies de votre infrastructure et de vos données informatiques (fichiers journaux, par exemple) et en analysant vos connexions réseau sortantes
- Permet d'identifier les signes d'intrusions actuelles ou passées dans vos réseaux
- Permet de reconnaître en quoi cette attaque affecte vos systèmes et quelles sont les possibilités qui s'offrent à vous

1 Compétences requises

5 Personnalisation et évolutivité

3 Coût

Kaspersky Threat Intelligence

La lutte contre les cybermenaces d'aujourd'hui nécessite une vue à 360 degrés des tactiques et outils utilisés par les cybercriminels. Récupérer ces renseignements et identifier les contre-mesures les plus efficaces exige une vigilance constante et des niveaux élevés d'expertise. Avec plusieurs pétaoctets de données sur les menaces des technologies avancées de machine learning et une équipe unique d'experts partout dans le monde, Kaspersky vous aide en vous proposant les informations sur les dernières menaces, et vous permet de préserver votre immunité, même en cas de cyberattaques qui ne sont pas encore détectables.

Solution idéale pour

les grandes entreprises

les institutions gouvernementales

les SOC (Security Operation Center) et les équipes d'intervention en cas d'incident

les MSSP

Avantages

Détecte instantanément les menaces pour empêcher l'interruption d'activité

Réduit les risques de pertes financières dues à des incidents

Garantit des investissements rentables dans certaines technologies et le personnel approprié en fonction des informations sur les menaces ciblant votre entreprise

Empêche les concurrents d'avoir un avantage concurrentiel injuste par le biais de l'exfiltration de la propriété intellectuelle

Permet de bâtir une **défense proactive et évolutive**

Utilisation

- Renforcer les solutions de sécurité réseau grâce à des **flux de données sur les menaces** constamment à jour
- Hiérarchiser efficacement les énormes quantités d'alertes de sécurité, et identifier instantanément celles qui devraient être transmises aux équipes d'intervention en cas d'incident avec **Threat Data Feeds** et **CyberTrace**
- Assurer une « connaissance situationnelle » en temps réel et exploiter les flux de Threat Intelligence plus efficacement avec **CyberTrace**
- Identifier l'empreinte numérique de votre organisation et réduire les risques connexes avec des **rapports de Threat Intelligence personnalisés**

Kaspersky Cybersecurity Training: Incident Response

service

La formation à la cybersécurité est un impératif pour les entreprises confrontées au volume croissant et à l'évolution des menaces. Le personnel chargé de la sécurité informatique doit bien maîtriser les techniques avancées, élément clé d'une stratégie efficace de gestion et d'atténuation des menaces. Kaspersky Cybersecurity Training permet d'offrir à votre équipe de sécurité interne toutes les connaissances nécessaires pour faire face à un paysage des menaces en constante évolution.

Solution idéale pour

les grandes entreprises

les institutions gouvernementales

les SOC (Security Operation Centers) et les équipes d'intervention en cas d'incident

les MSSP

Avantages

Réduit rapidement et efficacement les éventuels dommages dus à des incidents de sécurité, afin de diminuer considérablement les coûts de l'incident

Permet d'éviter les pénalités et amendes

Permet de maintenir la relation de confiance avec vos clients, partenaires et investisseurs, afin de favoriser les opportunités commerciales

Renforce vos défenses contre les incidents futurs grâce aux enseignements tirés

Cas d'utilisation

- Distinguer les menaces persistantes avancées (APT) des autres types de menaces
- Comprendre les diverses techniques des cybercriminels et l'anatomie des attaques ciblées
- Appliquer des méthodes de surveillance et de détection spécifiques
- Élaborer des règles de détection efficaces
- Reconstruire la logique et la chronologie de l'incident et suivre le flux de travail de réponse de l'incident

3 Approche de cybersécurité intégrée

Threat Management and Defense

Être prêt en cas d'attaques APT

Solution idéale pour les entreprises avec un niveau d'expertise élevé, ayant l'habitude d'utiliser la Threat Intelligence et le Threat Hunting.

- Environnements complexes et distribués
- Équipe de sécurité interne ou SOC
- Coûts élevés des incidents et violations de données
- Soumis à des impératifs de conformité

Services

- **Kaspersky Managed Protection**
- **Kaspersky Incident Response**

Formation

- **Kaspersky Cybersecurity Training**

Veille

- **Kaspersky Threat Intelligence**

Kaspersky Threat Management and Defense

Kaspersky Threat Management and Defense est une solution spécialisée qui offre un cadre complet pour une détection rapide des menaces, une enquête sur les incidents, ainsi que des fonctionnalités de réponse et de correction. Elle se compose des éléments suivants : threat intelligence de niveau mondiale, technologies avancées de détection des menaces et de réponse, éventail de formations sur la cybersécurité, recherche continue de menaces et réponse aux menaces qui contournent les barrières de sécurité existantes. La solution peut être intégrée à votre stratégie organisationnelle actuelle pour contrer les menaces complexes, en complétant ainsi les technologies de protection existantes et en vous faisant bénéficier d'une expertise performante, le cas échéant.

Solution idéale pour

les grandes entreprises

les institutions gouvernementales

les SOC et les équipes d'intervention en cas d'incident

les MSSP

5 Compétences requises

5 Personnalisation et évolutivité

5 Coût

Avantages

Réduit les dommages financiers et opérationnels causés par la cybercriminalité et permet de maintenir la stabilité des entreprises

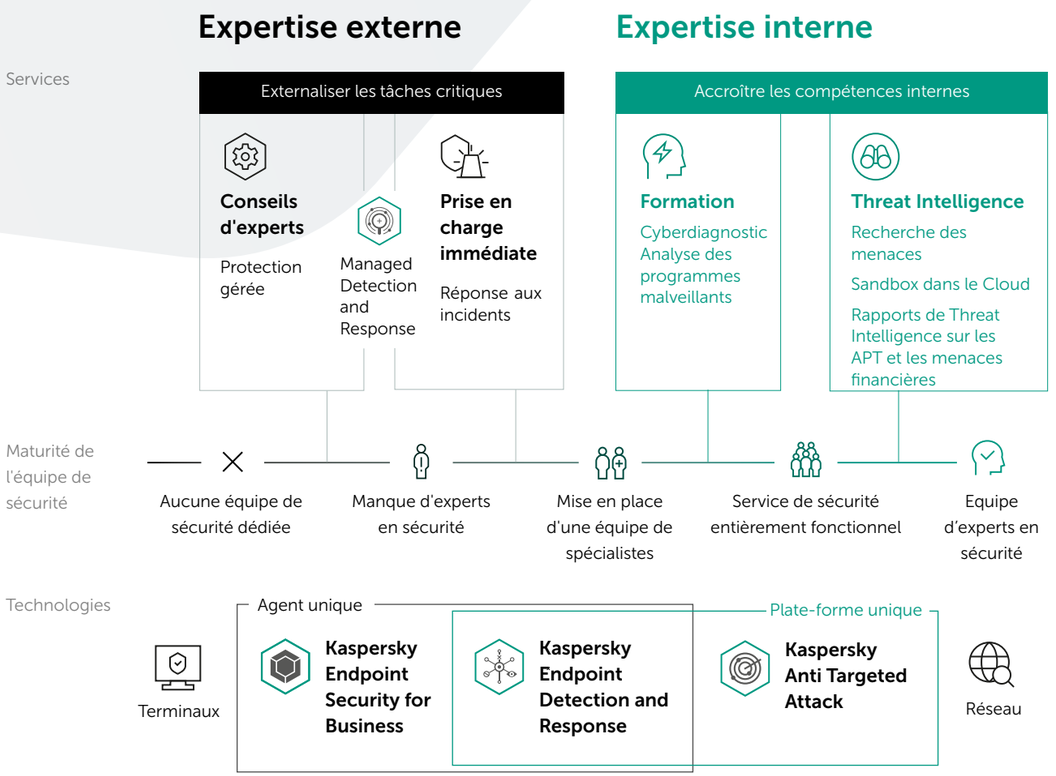
Augmente le retour sur investissement grâce à l'automatisation et à l'absence d'interruption des processus métier

Réduit les taux de roulement du personnel et augmente l'efficacité opérationnelle en développant l'expertise en interne

Déploie des stratégies de sécurité des informations avisées et rentables en fonction de modèles de menaces personnalisés

Utilisation

- La plate-forme technologique tout-en-un automatise la tâche fastidieuse de collecte de preuves et les tâches manuelles courantes
- La Threat Intelligence proactive fournit le contexte nécessaire pour détecter, hiérarchiser, enquêter et répondre rapidement aux menaces
- Stratégie de gestion des menaces via des compétences avancées
- La recherche des menaces permet de détecter des menaces inconnues et avancées conçues pour contourner les technologies préventives
- L'accès à une expertise tierce assure une enquête efficace et une réponse aux incidents complexes



Eléments à ne pas oublier lors de la création d'une stratégie de cybersécurité à long terme

Une approche de cybersécurité en silo met les entreprises en danger

L'augmentation des coûts de violations de données et réseaux imposent de sérieuses pressions financières sur les entreprises voulant opérer une transformation, d'où l'importance de la cybersécurité. Pour réussir dans cet environnement, les entreprises doivent faire de la cybersécurité une partie intégrante de leur stratégie globale, notamment en lui attribuant un rôle clé dans la gestion des risques et la planification à long terme.

La cybersécurité n'est pas qu'un simple objectif, mais une quête perpétuelle

Le plan de sécurité d'une entreprise doit être régulièrement examiné et ajusté en fonction des nouvelles connaissances et des nouveaux outils disponibles. Chaque incident de sécurité doit faire l'objet d'une analyse approfondie et entraîner la création de nouvelles procédures et mesures de gestion des attaques pour empêcher que des incidents similaires ne se reproduisent à l'avenir. Les défenses existantes doivent être continuellement améliorées.

La sensibilisation, la communication et la coopération sont essentielles au succès dans un monde où les cybermenaces évoluent rapidement

Plus de 80 % des incidents informatiques sont dus à l'erreur humaine. La formation du personnel à tous les niveaux est essentielle pour accroître la sensibilisation à la sécurité à l'échelle de l'organisation et motiver tous les salariés à prêter attention aux cybermenaces et à leurs contre-mesures, même s'ils ne pensent pas que cela fait partie de leurs responsabilités.

Adopter une mentalité proactive « de détection et de réponse » est le meilleur moyen de contrer des menaces en constante évolution

Les systèmes de prévention traditionnels fonctionnent de pair avec les technologies de détection avancées, les analyses de menaces, les capacités de réponse et les techniques de sécurité prédictives. Il est ainsi possible de créer un système de cybersécurité qui s'adapte en continu aux défis émergents auxquels les entreprises sont confrontées.

Caractéristiques des solutions

Quelle est la solution la mieux adaptée à vos besoins ?

	Kaspersky Endpoint Security	Cloud/Cloud+	Select	Advanced	Total	à la carte
Outils de contrôle	Protection contre les programmes malveillants	•	•	•	•	
	Pare-feu	•	•	•	•	
	Contrôle des applications		•	•	•	
	Contrôle des périphériques	•	•	•	•	
	Contrôle du Web	•	•	•	•	
	Sécurité des serveurs de fichiers	•	•	•	•	
Sécurité mobile	Protection des terminaux mobiles	•	•	•	•	
	Gestion de flotte mobile (MDM)	•	•	•	•	
	Chiffrement	(•)		•	•	•
	Inventaires			•	•	
	Déploiement d'applications			•	•	
	Vulnérabilités et gestion des correctifs	(•)		•	•	•
	Protection des serveurs de messagerie				•	•
	Protection de la passerelle Internet				•	•
	Protection des infrastructures cloud hybrides					•
	Protection des serveurs de stockage					•
	Protection de la fraude en ligne et sur mobile					•
	Protection contre les attaques DDoS					•
	Protection contre les attaques ciblées					•
	Protection des systèmes embarqués et IoT					•
	Protection des environnements industriels critiques					•

• Inclus (•) Cloud+ uniquement

Pourquoi choisir Kaspersky ?

La plus testée. La plus récompensée

Kaspersky a obtenu plus de premières places que tous les autres éditeurs de sécurité lors de tests indépendants. Et c'est une performance que nous répétons année après année.

www.kaspersky.fr/top3

L'une des solutions les plus fortement recommandées

Avec un taux de satisfaction client de 4,6 sur 5, Kaspersky a une fois de plus été récompensé aux Gartner Peer Insights Customer's Choice pour ses plates-formes de protection des terminaux, le 28 mai 2019.*

Transparence totale

Avec l'ouverture de notre centre de transparence, le traitement des données statistiques est désormais basé en Suisse, ce qui nous permet de garantir la souveraineté de vos données mieux que n'importe quel autre éditeur.

*Gartner Peer Insights Customers' Choice est le reflet d'avis subjectifs provenant d'évaluations, de classements et de données d'utilisateurs finaux individuels, appliqués à une méthodologie documentée. Il ne reflète pas le point de vue de Gartner ou ses sociétés affiliées ni ne constitue une approbation de leur part. Lire sur le site Web

kaspersky BRING ON THE FUTURE*

Nous contacter

Rechercher un partenaire près de chez vous :
https://www.kaspersky.fr/partners
Solutions de cybersécurité pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Actualités dédiées à la sécurité informatique :
https://www.kaspersky.fr/blog/

#bringonthefuture

www.kaspersky.fr