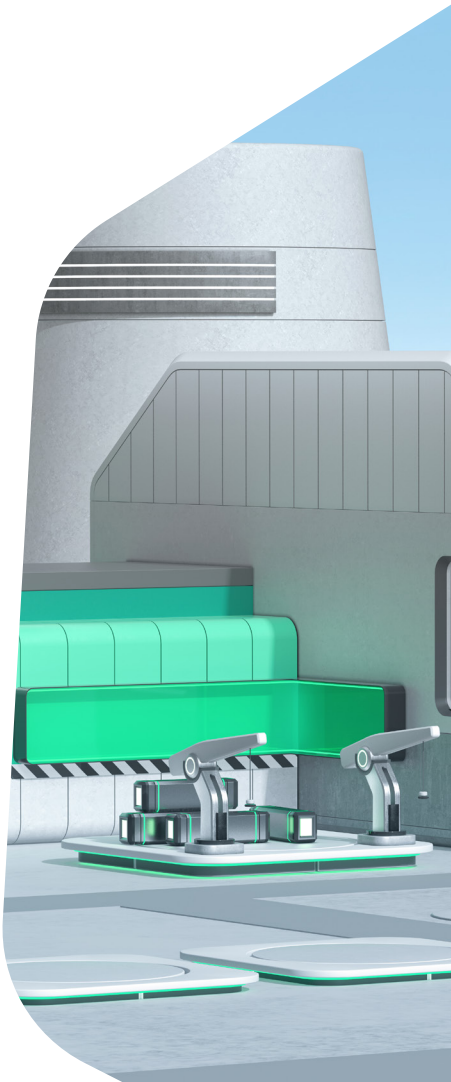
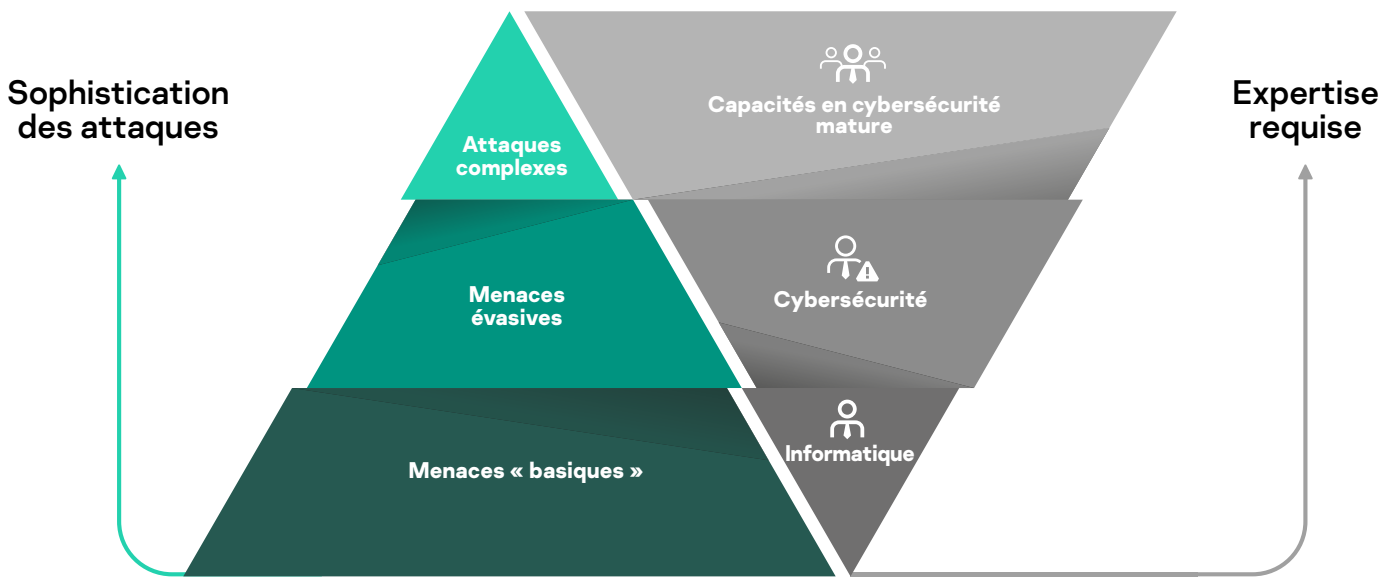
Solutions de sécurité Kaspersky pour les entreprises

À propos du portefeuille de solutions pour les entreprises de Kaspersky

La première étape consiste à établir les bases de la sécurité de votre organisation en choisissant le produit ou service adapté. Toutefois, le développement d'une stratégie de cybersécurité d'entreprise est la clé de tout succès à long terme. Le portefeuille de solutions pour les entreprises de Kaspersky reflète les exigences de sécurité des entreprises d'aujourd'hui, répondant ainsi aux besoins des entreprises 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.



Types de menaces et expertise requise pour les contrecarrer



Planification de la sécurité à court et à long terme

Processus d'évolution de la sécurité traditionnelle

Prise de décision :

- Tendances du marché
- Solution de sécurité en silo
- Approche de gestion des urgences
- Approche axée sur la conformité

Exploitation de produits traditionnels :

- Plateformes de protection des terminaux (EPP)
- Pare-feu / Pare-feu nouvelle génération (NGFW)
- Pare-feu d'application Web (WAF)
- Prévention des pertes de données
- Systèmes de gestion des événements et des informations de sécurité (SIEM)
- Autres

Attributs

- Planification de sécurité à court terme
- Dépendance aux technologies et fonctionnalités
- Défense du réseau basée sur un périmètre

Raisons de l'échec des approches traditionnelles :

- Complexité croissante des menaces et de l'environnement à risques
- Complexité des technologies de cybersécurité
- Pour réussir sa transformation numérique, une entreprise a besoin d'une stratégie de cybersécurité à long terme

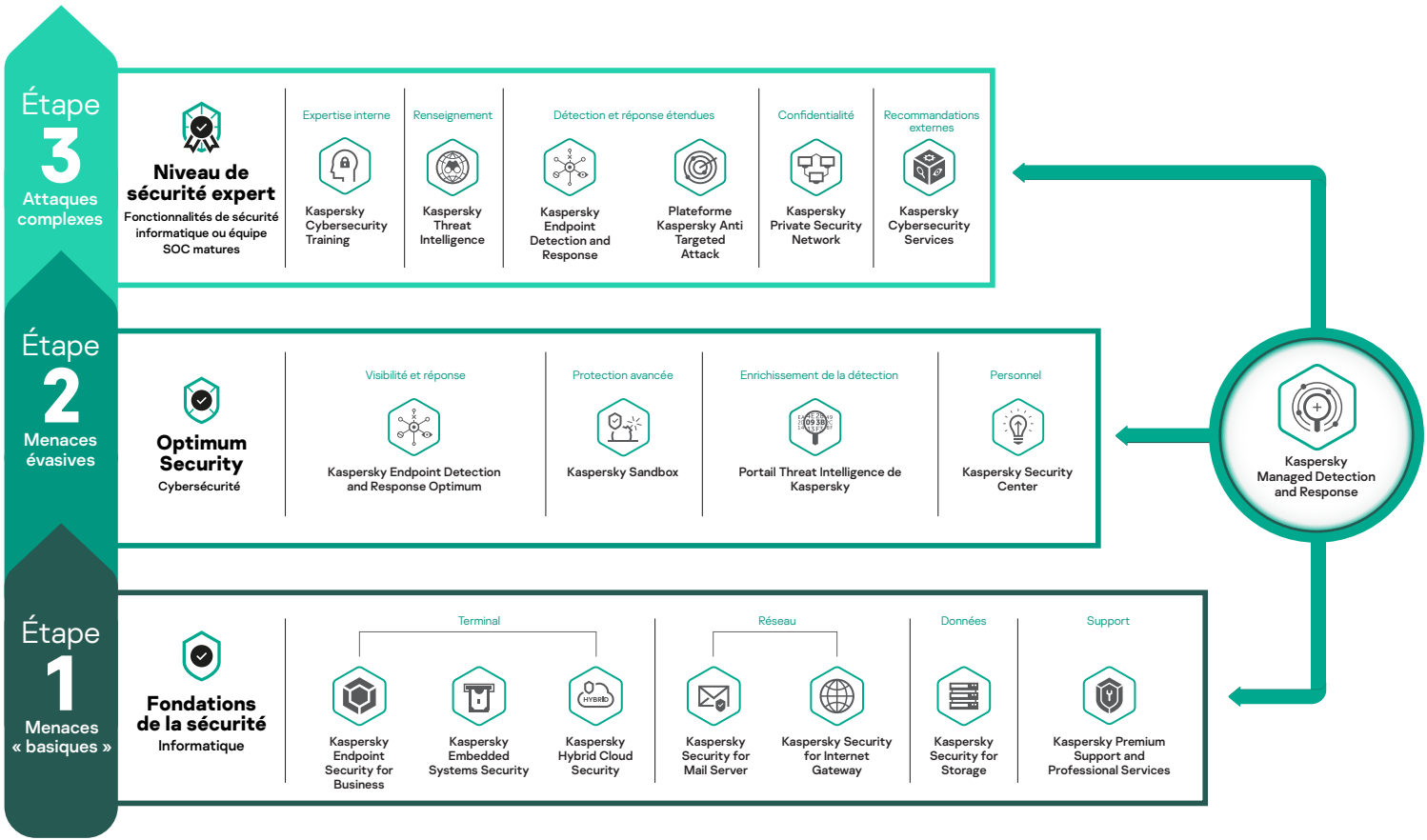
Les terminaux sont les points d'entrée les plus communs dans l'infrastructure d'une organisation, la principale cible des cybercriminels et les principales sources des données nécessaires pour examiner efficacement les incidents complexes.

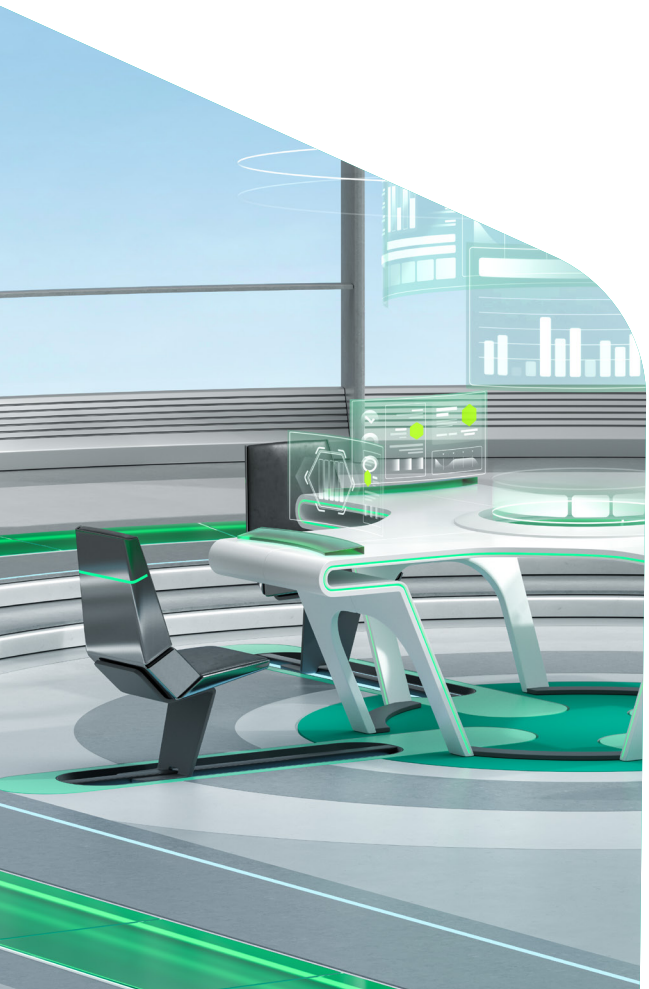
des entreprises détectent les attaques presque instantanément

le coût supplémentaire d'une violation de données si elle est détectée après sept jours

Source : rapport économique sur la sécurité informatique en 2020 par Kaspersky

L'approche par étape de Kaspersky en matière de cybersécurité





Phase 1
Fondations de la sécurité

Blocage du plus grand nombre possible de menaces

- L'étape de base pour les organisations de toutes tailles et complexité dans l'élaboration d'une stratégie de défense intégrée contre les menaces complexes
- Généralement suffisant pour les petites entreprises dotées seulement d'une équipe informatique et ne disposant pas de spécialistes en sécurité informatique

Kaspersky Endpoint Security for Business

La réputation de votre entreprise doit être défendue à tout prix. C'est pourquoi nous ne nous contentons pas de protéger et de contrôler tous vos terminaux. Kaspersky Endpoint Security for Business protège votre entreprise contre toute une série de menaces, des menaces liées au BIOS aux menaces sans fichier, tandis que le durcissement des serveurs améliore leurs défenses grâce à des contrôles particuliers qui empêchent la perte d'informations personnelles et financières. De plus, elle est fournie à partir du cloud ou sur site pour assurer une sécurité flexible et une gestion facile.

Le choix idéal si vous souhaitez :

- Empêcher les salariés d'exposer votre entreprise ou eux-mêmes à une attaque
- Réduire le nombre d'incidents relatifs aux terminaux qui doivent être traités manuellement
- Sécuriser divers environnements grâce à une défense flexible qui a fait ses preuves

2 Compétences requises

5 Personnalisation et évolutivité

2 Niveau d'investissement

Avantages commerciaux

- Réduisez le coût total de possessions en automatisant votre défense contre différentes menaces dans un produit tout-en-un
- Garantissez la continuité des activités en protégeant tous les appareils, où qu'ils soient
- Répondez aux exigences en matière de conformité tout en offrant la souplesse nécessaire pour externaliser la gestion de la sécurité informatique

Application pratique

- Réduit le risque de subir une attaque grâce aux technologies de protection des terminaux qui ont reçu le plus de récompenses
- Assure que votre infrastructure informatique est mise à jour et gérée à partir du cloud ou de la console sur site
- Permet de migrer rapidement et facilement à partir de solutions tierces
- Permet d'ajouter organiquement de nouvelles technologies, y compris l'EDR et d'autres fonctionnalités, sans avoir à les réinstaller sur les terminaux
- Permet de protéger les données tout en atteignant les objectifs de conformité grâce à la gestion du chiffrement intégrée, dont la suppression des données à distance et le contrôle des appareils sous différents systèmes d'exploitation

Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security simplifie et sécurise votre transformation numérique lorsque votre organisation virtualise ou déplace ses charges de travail dans le cloud. La technologie brevetée d'agent léger réduit 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 de la même console assure une gestion rationalisée des risques au quotidien, dans divers environnements.

Le choix idéal si vous souhaitez :

- Virtualiser les charges de travail pesant sur vos postes de travail et vos serveurs
- Déplacer ou gérer des infrastructures dans des clouds publics (IaaS)
- Intégrer les étapes de sécurité dans vos pipelines DevOps
- Exploiter la mise en conteneurs de manière sécurisée

2 Compétences requises

5 Personnalisation et évolutivité

2 Niveau d'investissement

Avantages commerciaux

- Limite les dommages financiers et d'atteinte à la réputation en réduisant votre surface d'attaque et les temps d'arrêt dus aux attaques
- Optimise les coûts informatiques en libérant jusqu'à 30 % des ressources d'hyperviseur
- Assure la conformité en respectant les exigences de sécurité de base
- 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

Application pratique

- Assure une visibilité et un contrôle cohérents à l'échelle des déploiements de data center et dans le Cloud
- Sécurité pour VMWare et Citrix VDI
- Protection des charges de travail dans le cloud pour les instances AWS, Azure et Google Cloud avec un déploiement automatisé et une visibilité cohérente via l'intégration d'API natives
- Sécurité pour DevOps avec protection des conteneurs, interfaces d'intégration des pipelines et API de gestion

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security est une solution multi-niveaux spécialisée, conçue pour protéger vos appareils embarqués Windows ainsi que les anciens terminaux dont le système d'exploitation n'est pas pris en charge et que vous ne pouvez pas mettre à niveau. Le contrôle des applications est associé à une fonctionnalité de protection contre les programmes malveillants dont la prévention des vulnérabilités ainsi que la protection contre les menaces réseau, la surveillance de l'intégrité et d'autres couches de sécurité pour une protection optimale adaptée à vos processus et aux fonctionnalités des appareils.

Le choix idéal si vous souhaitez :

- Protéger des distributeurs de billets, des systèmes de point de vente, du matériel médical ou tout autre système embarqué qui n'est pas industriel
- Optimiser la sécurité des systèmes dont le matériel et le système d'exploitation sont obsolètes, comme d'anciens terminaux
- Intégrer la sécurité de votre infrastructure embarquée dans votre écosystème de sécurité Kaspersky

2 Compétences requises

5 Personnalisation et évolutivité

2 Niveau d'investissement

Avantages commerciaux

- Garantit des processus métier continus et sans interruption dans des domaines où une attaque pourrait avoir un impact dévastateur d'un point de vue financier, juridique et d'atteinte à la réputation
- Permet d'éviter d'être obligé de procéder à une mise à niveau et de continuer à utiliser en toute sécurité et aussi longtemps que vous le voulez d'anciens terminaux qui répondent à des besoins spécifiques et qui ne peuvent pas être remplacés pour le moment
- Assure une conformité totale via des mécanismes de protection fiables, y compris ceux que les régulateurs recommandent spécifiquement

Application pratique

- Configurez le scénario de sécurité le plus efficace pour votre système, en fonction de l'utilisation et du niveau de puissance, parmi différents scénarios et différentes couches de sécurité
- Garantissez une protection simple et durable lorsque des opérations de maintenance fréquentes ne sont pas possibles
- Déjouez les attaques internes, qui constituent un risque majeur pour les appareils embarqués qui ne peuvent pas être attaqués par email ou via le Web
- Protégez les appareils qui ont une mauvaise connexion Internet

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server empêche que les menaces par email, telles que les programmes crimeware et ransomware, le phishing et le spam, n'atteignent vos terminaux (car utilisés dans la plupart des piratages informatiques et programmes malveillants). La mise en œuvre de l'intelligence artificielle dans le cloud et les modèles basés sur le Machine Learning sur site garantissent des taux de détection élevés avec un nombre exceptionnellement faible de faux positifs et permet de lutter contre les menaces par email sophistiquées, y compris la compromission d'emails professionnels (BEC). Le spam est bloqué efficacement, avant qu'il ne fasse perdre du temps.

Le choix idéal si vous souhaitez :

- Renforcer votre capacité à lutter à la fois contre les attaques massives et les attaques extrêmement ciblées qui se diffusent par email
- Couvrir un grand nombre de scénarios de protection de la messagerie sur différentes plateformes et avec différents schémas de déploiement

3 Compétences requises

4 Personnalisation et évolutivité

2 Niveau d'investissement

Avantages commerciaux

- Limite les effets perturbateurs des attaques par emails et par programmes malveillants véhiculées par les emails
- Améliore la productivité des salariés en éliminant les distractions liées au spam
- Réduit les charges de travail en matière d'informatique et de sécurité informatique et optimise vos coûts opérationnels
- Limite les risques juridiques et d'atteinte à la réputation en contrôlant le transfert de contenu envoyé par email

Application pratique

- Renforcez de manière critique la défense de votre infrastructure au niveau du serveur de messagerie en bloquant les menaces avant qu'elles n'atteignent leur cible, à savoir les utilisateurs et vos terminaux
- Améliorez la sécurité de la passerelle sans ajouter de faux positifs
- Renforcez vos fonctionnalités avancées de détection des menaces Kaspersky et intégrez des capacités de réponse automatisée au niveau de la passerelle

Kaspersky Security for Internet Gateway

Avec son application de base Kaspersky Web Traffic Security, Kaspersky Security for Internet Gateway offre une protection solide au niveau de la passerelle contre les cybermenaces sur Internet, telles que les programmes malveillants, les ransomwares, le minage, le phishing en ligne et les ressources Web malveillantes. Cet outil vous permet également de contrôler l'utilisation du Web en limitant l'accès à des ressources Web spécifiques conformément aux politiques de l'entreprise et en limitant le transfert de certains types de fichier.

Le choix idéal si vous souhaitez :

- Empêcher les menaces Web d'affecter vos terminaux
- Limiter les risques d'infection et améliorer la productivité globale en appliquant des contrôles sur l'utilisation d'Internet
- Réduire la charge de travail de vos équipes chargées de l'informatique et de la sécurité informatique en bloquant automatiquement les menaces Web au point d'entrée

2 Compétences requises

5 Personnalisation et évolutivité

2 Niveau d'investissement

Avantages commerciaux

- Réduit les interruptions d'activité et les conséquences des perturbations de sécurité au sein du réseau
- Améliore l'efficacité en matière d'informatique et de sécurité informatique et optimise vos coûts opérationnels
- Protège votre organisation les menaces basées sur le piratage informatique en ligne
- Permet d'améliorer la productivité des salariés en contrôlant l'accès en ligne à des ressources Web spécifiques

Application pratique

- Renforcez votre défense basée sur les terminaux au niveau de la passerelle
- Complétez et renforcez la sécurité de la passerelle Web sans ajouter de faux positifs
- Protégez les appareils qui ne pourraient pas être protégés autrement au niveau du terminal, pour des motifs professionnels ou d'utilisation
- Développez vos fonctionnalités avancées de détection des menaces Kaspersky en ajoutant du contexte et en permettant une réponse automatisée au niveau de la passerelle

Kaspersky Security for Storage

Un système de stockage connecté facilement accessible peut facilement 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 notre Threat Intelligence mondiale. Inclut des fonctionnalités uniques (anti-chiffrement distant, par exemple) activées par l'intégration aux API des systèmes de stockage.

Le choix idéal si vous souhaitez :

- Protéger des systèmes de stockage connectés contre des attaques externes et la propagation de l'infection
- Protéger des données précieuses se trouvant sur des systèmes de stockage connectés contre les attaques de ransomware
- Gérer la sécurité de votre système de stockage de données en même temps que les terminaux et les serveurs protégés par les solutions Kaspersky

3 Compétences requises

4 Personnalisation et évolutivité

3 Niveau d'investissement

Avantages commerciaux

- Assure la continuité des activités en empêchant les attaques massives par programme malveillant qui utilisent les systèmes de stockage pour se propager
- Aide au respect de la conformité en offrant un moyen de protection fiable pour votre système de stockage des données réglementé
- Réduit les problèmes de fonctionnement grâce à une gestion unifiée avec les autres solutions Kaspersky de protection des terminaux et des serveurs

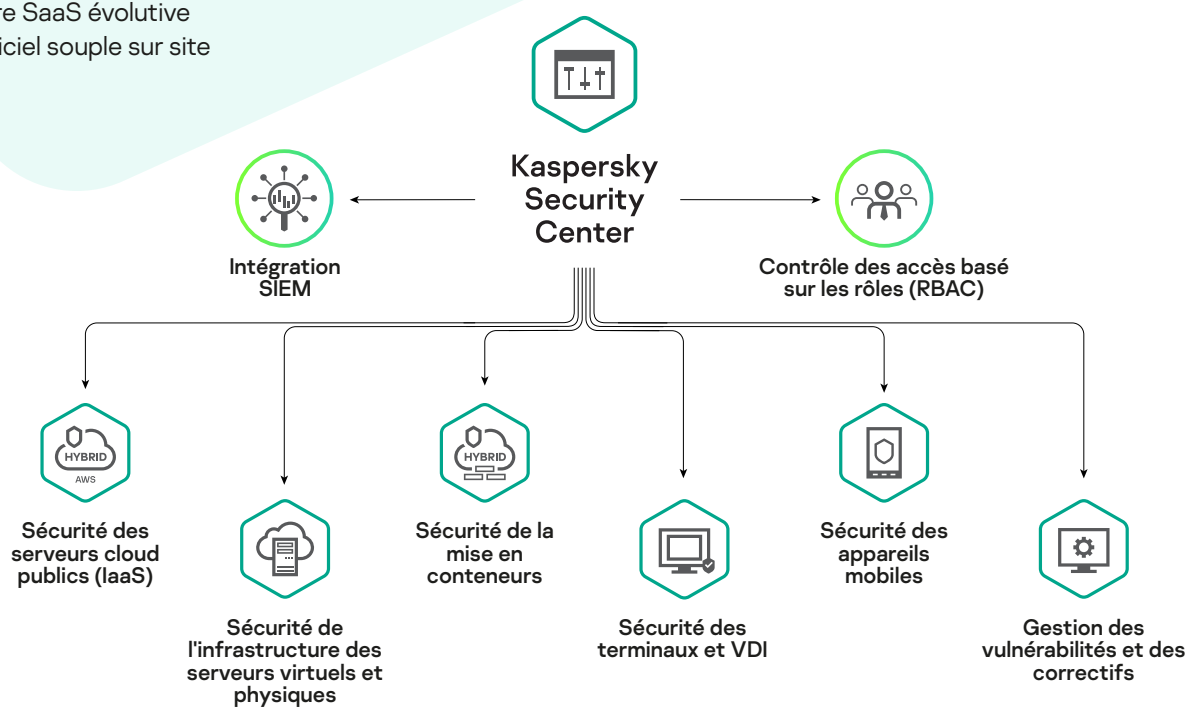
Application pratique

- Protection des systèmes NAS, DAS et/ou SAN utilisés dans votre infrastructure
- Protection à la fois des systèmes de stockage et du serveur utilisé pour héberger la solution de sécurité (produit tout-en-un)
- Protection contre la perte de données due aux cryptovirus exécutés à distance

Gestion unifiée

Kaspersky Security Center pour la gestion de plusieurs charges de travail et le contrôle basé sur une politique, est proposé comme :

- Offre SaaS évolutive
- Logiciel souple sur site



Kaspersky Premium Support (MSA)

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.

Le choix idéal si vous souhaitez :

- Etre sûr que vos systèmes informatiques sont protégés, non seulement par des technologies de sécurité reconnues, mais aussi par les compétences de nos experts

1 Compétences requises

5 Personnalisation et évolutivité

3 Niveau d'investissement

Avantages commerciaux

- Assure la continuité des activités grâce à des experts dédiés à votre service, chargés de traiter votre problème et de le résoudre aussi rapidement que possible
- Réduction des coûts d'un incident de sécurité en accédant à une ligne d'assistance 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 le problème

Application pratique

- Faites remonter vos problèmes critiques de manière accélérée à des spécialistes qui sont les mieux placés pour délivrer rapidement la solution la plus adaptée à votre problème
- Bénéficiez d'une protection complète avec des mesures proactives propres à votre système
- Réduisez le temps que vos précieuses ressources internes consacrent à la maintenance et au dépannage

Kaspersky Professional Services

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.

Le choix idéal si vous souhaitez :

- Accélérer, optimiser et personnaliser votre solution Kaspersky afin de respecter les bonnes pratiques en matière de cybersécurité

Avantages commerciaux

- Optimise votre retour sur investissement sur vos solutions de sécurité en garantissant qu'elles s'exécutent à 100 % de leur capacité
- Réduit les coûts pour le personnel informatique interne
- Minimise l'impact de la mise en œuvre d'une nouvelle solution de sécurité sur les opérations commerciales quotidiennes et diminue les coûts globaux de mise en œuvre
- Permet de s'assurer que tout nouveau problème critique est traité rapidement et efficacement

Application pratique

- 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 les risques de temps d'arrêt grâce à des audits réguliers des configurations du produit, assurant ainsi la mise en place de mécanismes de défense à jour
- Réduit la période d'adoption du produit, permettant ainsi de profiter immédiatement de tous les avantages

1 Compétences requises

5 Personnalisation et évolutivité

3 Niveau d'investissement

Phase 2
Optimum Security

Technologie de détection avancée et réponse centralisée

Permet aux petites équipes de cybersécurité de s'attaquer même aux menaces qui contournent la prévention automatique, grâce à une solution qui tient compte des ressources disponibles et qui est élaborée de façon organique dès les solutions de sécurité de base

Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response (EDR) Optimum fournit aux organisations l'expertise en matière de cybersécurité suffisante pour lutter contre de nombreuses menaces évasives. Ce produit dispose des fonctionnalités de protection de Kaspersky Endpoint Security for Business Advanced et est géré à partir de Kaspersky Security Center. Il propose un ensemble d'outils faciles à utiliser et est basé sur l'analyse simplifiée des causes profondes, la recherche d'indicateurs de compromission (IoC) et les options de réponse automatisée ou « en un seul clic ».

Le choix idéal si vous souhaitez :

- Augmenter la visibilité sur les menaces pour tous vos terminaux
- Réduire votre temps moyen de réponse
- Optimiser vos ressources de sécurité informatique et améliorer leur efficacité

3 Compétences requises

4 Personnalisation et évolutivité

3 Niveau d'investissement

Avantages commerciaux

- Réduit les risques, notamment financiers et d'atteinte à la réputation, liés aux menaces qui échappent à la protection préventive
- Permet d'optimiser les charges de travail des salariés et l'utilisation des ressources grâce à un flux de travail rationalisé et une série de fonctionnalités d'automatisation
- Améliore l'efficacité grâce à un outil économe et accessible qui ne nécessite pas une expertise approfondie et qui se maîtrise rapidement

Application pratique

- Bénéficiez d'une visibilité granulaire sur les alertes de sécurité des terminaux
- Analysez davantage la menace détectée sur l'hôte afin de connaître son ampleur et la cause profonde
- Découvrez si vous faites l'objet d'une attaque en recherchant des indicateurs de compromission importés à partir de sources tierces
- Permet de répondre automatiquement aux menaces dès la détection ou durant votre enquête en quelques clics seulement

Kaspersky Managed Detection and Response Optimum

Kaspersky Managed Detection and Response Optimum vous offre des fonctionnalités de sécurité informatique instantanément matures via un déploiement clé en main, rapide et évolutif sans qu'il soit nécessaire d'investir dans du personnel ou des compétences supplémentaires. Grâce aux modèles de Machine Learning brevetés, à une Threat Intelligence continue et unique et à la recherche de menaces automatisée avec indicateurs d'attaque propriétaires, votre organisation est protégée en permanence contre les menaces complexes qui utilisent des tactiques, des techniques et des procédures connues.

Le choix idéal si vous souhaitez :

- Établir et améliorer une solution rapide et efficace de détection des menaces et de réponse par le biais d'une surveillance en continu
- Diminuer rapidement la probabilité que votre entreprise fasse l'objet de menaces avancées sans que votre équipe de sécurité informatique ne passe trop de temps à approfondir ses compétences et maîtriser de nouvelles solutions

2 Compétences requises

5 Personnalisation et évolutivité

4 Niveau d'investissement

Avantages commerciaux

- La certitude rassurante d'être protégé en permanence, même contre les menaces les plus innovantes
- Une réduction du coût total relatif à la sécurité, en supprimant le besoin d'employer et de former un large éventail de spécialistes dédiés en interne afin de couvrir toutes les éventualités

Application pratique

- Permet une approche systémique de la protection grâce à la prévention, la détection, la recherche et la réponse automatiques vis-à-vis des menaces qui ciblent vos réseaux
- Garantit une réaction rapide en cas d'incident tout en gardant le contrôle total de toutes les actions
- Offre une visibilité complète en temps réel sur toutes les détections, les ressources couvertes et l'état de protection actuel

Kaspersky Sandbox

Kaspersky Sandbox vous protège automatiquement contre les menaces nouvelles et inconnues conçues pour contourner la protection des terminaux. Ce complément de Kaspersky Endpoint Security for Business aide les entreprises à améliorer considérablement leur niveau de protection des terminaux et des serveurs contre les menaces telles que les programmes malveillants inconnus, les nouveaux virus et les ransomwares, les exploits « zero-day » et bien d'autres, sans avoir à recruter du personnel de sécurité.

Le choix idéal si vous souhaitez :

- Renforcer votre défense contre les menaces évasives
- Une détection automatisée avancée
- Optimiser la charge de travail de vos salariés et les exigences en matière d'expertise

1 Compétences requises

3 Personnalisation et évolutivité

2 Niveau d'investissement

Avantages commerciaux

- Réduit les risques de sécurité informatique et garantit la continuité des activités
- Offre une protection contre les menaces avancées sans affecter les performances des terminaux, ni la productivité des utilisateurs
- Limite les frais de main-d'œuvre grâce à une réduction des opérations manuelles
- Optimise les coûts pour une protection avancée des bureaux à distance contre les menaces

Application pratique

- Permet d'effectuer une analyse dynamique approfondie et de détecter les menaces inconnues et évasives
- Fournit une réponse automatisée sur tous les terminaux protégés
- Permet de ne pas perdre en productivité et renforce la sécurité des terminaux surchargés en délégant à la sandbox l'analyse des comportements, tâche très exigeante au niveau des ressources
- S'intègre aux solutions tierces via une API
- Permet d'économiser des heures de travail grâce à l'installation simple et au fonctionnement entièrement automatique de votre sandbox, sans besoin de compétences avancées en informatique ou en cybersécurité

Portail Threat Intelligence de Kaspersky

Le portail Threat Intelligence de Kaspersky réunit dans un seul et même service Web toutes les connaissances que nous avons acquises sur les cybermenaces. Il vous permet de vérifier les indicateurs de menace suspects, qu'il s'agisse d'un fichier, d'un hachage de fichier, d'une adresse IP ou d'une URL. Le portail analyse les objets avec un ensemble de technologies de détection avancées comme la détection basée sur la réputation via Kaspersky Security Network, des modèles de Machine Learning structurels et la détection dynamique avancée grâce à Kaspersky Cloud Sandbox, indiquant si un objet se trouve dans la catégorie « Positif », « Négatif » ou « Neutre ». Les données contextuelles fournies vous aident à hiérarchiser les menaces et à y répondre plus efficacement.

Le choix idéal si vous souhaitez :

- Pouvoir accéder gratuitement à une source fiable de Threat Intelligence
- Hiérarchiser les incidents de manière plus efficace
- Accélérer les enquêtes et la découverte des menaces

3 Compétences requises

4 Personnalisation et évolutivité

0 Niveau d'investissement

Avantages commerciaux

- Permet de contourner l'un des principaux obstacles à l'adoption commerciale de la Threat Intelligence, à savoir son coût élevé
- Permet de conserver une protection efficace de vos réseaux en vous offrant un accès à des données intégralement vérifiées

Application pratique

- Valider/hiérarchiser en urgence les alertes ou les incidents représentant de réelles menaces à partir des niveaux d'impact et de risque ;
- Identifier immédiatement les alertes qui doivent être transmises à votre équipe de réponse aux incidents ;
- Isoler les menaces réelles et déterminer où concentrer les ressources limitées de réponse en cas d'incident ;
- Éliminer la nécessité d'exécuter des recherches complexes dans différentes bases de données pour trouver des précisions sur un élément particulier ou une attaque ;
- Découvrir des menaces jamais détectées auparavant

Kaspersky Security Awareness

Kaspersky Security Awareness regroupe plusieurs produits de formation ludiques sur ordinateur qui façonnent les compétences en cyberhygiène de vos salariés et les motive à respecter les pratiques de sécurité, et ce à tous les niveaux de la structure de l'entreprise. Ce produit se compose des éléments suivants :

— Kaspersky Interactive Protection Simulation & CyberSafety Management Games : pour l'implication et la motivation
— Gamified Assessment Tool : pour définir leur niveau
— Online Learning Platform & Cybersecurity for IT Online : pour acquérir des compétences pratiques
— [Dis]connected : un jeu éducatif informel qui renforce les compétences récemment acquises

Le choix idéal si vous souhaitez :

- Diminuer le nombre d'incidents dus à l'ignorance ou à la négligence des salariés
- Développer une compréhension plus juste des mesures de cybersécurité auprès du personnel à tous les niveaux
- Inculquer une forte culture de la cybersécurité dans votre organisation grâce à des solutions prêtes à l'emploi

2 Compétences requises

4 Personnalisation et évolutivité

3 Niveau d'investissement

Avantages commerciaux

- Permet de réduire le nombre d'incidents de sécurité dus à l'homme, garantissant ainsi la continuité des activités et réduisant l'impact des incidents
- Incite et motive à l'apprentissage et convertit les membres de la direction en partisans de mesures et d'initiatives sur la cybersécurité
- Améliore la culture de la cybersécurité dans votre organisation

Application pratique

- Inculquez à vos salariés les connaissances et les compétences nécessaires pour adopter et conserver un comportement sûr
- Favorisez une attitude saine dans l'entreprise en ce qui concerne les problèmes de cybersécurité
- Permettez aux salariés d'améliorer leurs résultats au quotidien sans exposer votre entreprise aux risques cybernétiques

Phase 3
Niveau de sécurité expert

Assurez une protection contre les attaques complexes et de type APT. Cette solution est adaptée aux profils suivants :

Accordez la priorité à une protection étendue reposant sur la Threat Intelligence, des conseils d'experts et le transfert de connaissances, afin de permettre aux équipes de sécurité informatique expérimentées de faire face à des menaces complexes et à des attaques ciblées.

Kaspersky Endpoint Detection and Response

Un outil EDR performant et doté de nombreuses fonctionnalités pour les experts en sécurité informatique, offrant une visibilité totale, une détection des menaces performante et une analyse efficace, avec un accès rapide aux données recueillies. Votre processus d'enquête bénéficie de l'analyse rétrospective, d'indicateurs d'attaque propriétaires et du mappage MITRE ATT&CK, ainsi que de la recherche proactive des menaces et de l'accès à Kaspersky Threat Intelligence. Découvrez la séquence de l'intrusion dans son intégralité, comprenez les attaques complexes à plusieurs niveaux qui ciblent les terminaux et réagissez rapidement et de manière appropriée !

Le choix idéal si vous souhaitez :

- Renforcer la protection de vos terminaux
- Améliorer davantage les fonctionnalités de réponse aux incidents en interne en réduisant constamment votre temps moyen de détection et de réponse
- Perfectionner vos opérations proactives de recherche des menaces

4 Compétences requises

3 Personnalisation et évolutivité

4 Niveau d'investissement

Avantages commerciaux

- Vous aide à surveiller vos ressources les plus précieuses
- Atténue les risques de cybersécurité et réduit les dommages financiers et opérationnels dus à des incidents au niveau des terminaux
- Diminue vos coûts opérationnels pour la sécurité informatique en simplifiant l'analyse des incidents liés aux terminaux ainsi que leur réponse
- Contribue à garantir la conformité aux exigences réglementaires

Application pratique

- Détectez efficacement (avec des fonctionnalités éprouvées via l'évaluation MITRE) les attaques avancées au niveau des terminaux et réagissez rapidement
- Effectuez une analyse rétrospective et des enquêtes efficaces sur des données agrégées de manière centralisée
- Centralisez la gestion des incidents avec une enquête et une réponse guidées
- Traquez les menaces cachées grâce à des fonctionnalités automatisées et proactives de recherche des menaces
- Kaspersky EDR fait partie de Kaspersky Anti Targeted Attack Platform, constituant ensemble une solution de détection et de réponse étendue

Plateforme Kaspersky Anti Targeted Attack

La plateforme Kaspersky Anti Targeted Attack Platform (KATA) combine des fonctionnalités avancées de détection des menaces et d'EDR au niveau du réseau via la solution Kaspersky EDR, et agit comme une solution de détection et de réponse étendues, en offrant une protection APT tout-en-un optimisée par notre infrastructure Threat Intelligence et MITRE ATT&CK via une console Web unique. Vos experts en sécurité informatique disposent de tous les outils nécessaires pour gérer la découverte de menaces multidimensionnelles supérieures, mener des enquêtes efficaces, rechercher les menaces de manière proactive et réagir de manière rapide et centralisée, le tout grâce à une solution unique.

Le choix idéal si vous souhaitez :

- Mettre en œuvre une défense efficace et élargie contre les attaques les plus sophistiquées avec un système unique et puissant
- Bénéficier d'une visibilité totale sur l'ensemble de l'entreprise
- Réduire votre temps moyen de détection et de réponse
- Optimiser votre centre d'opérations de sécurité
- Améliorer votre système de sécurité tout en veillant à la confidentialité

5 Compétences requises

3 Personnalisation et évolutivité

5 Niveau d'investissement

Avantages commerciaux

- Atténue les risques de cybersécurité et réduit les dommages financiers, opérationnels et d'atteinte à la réputation dus à des attaques ciblées complexes
- Diminue les coûts opérationnels pour la sécurité informatique en rationalisant et en automatisant les processus de gestion des incidents
- Contribue à garantir la conformité aux exigences réglementaires

Application pratique

- Protégez plusieurs points d'entrée contre des menaces potentielles au niveau du réseau et des terminaux
- Détectez rapidement des menaces avancées qui contournent vos technologies préventives actuelles
- Traquez les menaces cachées grâce à des fonctionnalités automatisées et proactives de recherche des menaces
- Fournissez à votre équipe de sécurité informatique des informations opportunes sur les menaces détectées pour une enquête plus approfondie
- Permettez une réponse centralisée aux incidents complexes via une large gamme de scénarios automatisés

Managed Detection and Response

Laissez à Kaspersky le soin de se charger des processus de triage et d'enquête des incidents qui sont coûteux en temps et en ressources. Toutes les fonctionnalités de Kaspersky Managed Detection and Response Optimum combinées avec la recherche gérée des menaces qui utilisent des tactiques, des techniques et des procédures inconnues, l'accès direct par téléphone aux analystes du SOC Kaspersky, la conservation des données brutes pendant une durée allant jusqu'à 3 mois, un accès privilégié à Kaspersky Threat Intelligence et une API permettant l'intégration avec des systèmes de tickets tiers, ce qui réduit considérablement le temps que vous consacrez à la gestion des flux de travail.

Le choix idéal si vous souhaitez :

- Permettre à votre équipe de sécurité informatique interne expérimentée de passer davantage de temps sur des incidents critiques qui nécessitent toute leur attention
- Améliorer davantage l'efficacité de votre équipe de sécurité en augmentant vos bonnes pratiques en interne grâce à l'expertise de Kaspersky

2 Compétences requises

5 Personnalisation et évolutivité

5 Niveau d'investissement

Avantages commerciaux

- Profitez de tous les avantages d'un centre d'opérations de sécurité (SOC) sans avoir à créer le vôtre
- Maximisez la valeur de vos solutions de sécurité Kaspersky
- Réduisez le coût total lié à la sécurité et le besoin en futurs investissements supplémentaires dans ce domaine en augmentant instantanément les capacités de sécurité informatique sans avoir à employer et former un large éventail de spécialistes de la sécurité en interne

Application pratique

- Profitez de fonctionnalités personnalisées de détection, de hiérarchisation, d'enquête et de réponse en continu
- Consultez nos experts et bénéficiez d'éléments de contexte complémentaires sur les menaces observées sur vos réseaux
- Utilisez la recherche rétrospective des menaces grâce aux informations de Threat Intelligence nouvellement acquises
- Optimisez les enquêtes sur les incidents en recherchant les menaces et leurs relations dans la base de connaissances complète de Kaspersky

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence offre des éléments contextuels détaillés et significatifs par le biais du cycle de gestion des incidents. Nos informations uniques et immédiatement exploitables peuvent être fournies sous diverses formes et dans différents formats, ce qui permet une intégration fluide dans vos flux de travail de sécurité. Ce portefeuille comprend des flux de Threat Intelligence, des rapports interprétables par les humains spécifiques aux secteurs et aux menaces ainsi qu'un référentiel consultable contenant des pétaoctets de données sur les menaces, les objets légitimes et leurs diverses relations.

Le choix idéal si vous souhaitez :

- Optimiser vos capacités de prévention et de détection
- Remplacer un système de sécurité réactif par un système proactif
- Perfectionner votre programme de Threat Intelligence
- Pouvoir prendre des décisions stratégiques plus éclairées en matière de sécurité

4 Compétences requises

5 Personnalisation et évolutivité

5 Niveau d'investissement

Avantages commerciaux

- Permet de réduire le roulement du personnel de sécurité informatique en évitant aux analystes de subir un burn-out
- Améliore l'efficacité des opérations de sécurité en minimisant les interruptions d'activité et l'impact des incidents
- Permet d'optimiser le retour de votre investissement dans la sécurité informatique en l'adaptant à votre propre environnement à risques

Application pratique

- Renforcez les solutions de sécurité avec des données de mises à jour en permanence et interprétables par une machine
- Améliorez la hiérarchisation des alertes en déterminant les alertes critiques qui doivent être transmises aux équipes de réponse aux incidents
- Accélérez les enquêtes conduites par des humains en révélant les relations entre les menaces détectées
- Justifiez votre budget de sécurité informatique en présentant des scénarios de risques clairs et pertinents

Kaspersky Cybersecurity Training

Le développement des compétences est un impératif pour les entreprises confrontées à un volume croissant de menaces qui évoluent en permanence. 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, comme le reverse engineering, la création de règles YARA et l'exploitation des preuves numériques. Kaspersky Cybersecurity Training permet d'offrir à votre équipe de sécurité interne toutes les connaissances nécessaires pour gérer un environnement de menaces en constante évolution.

Le choix idéal si vous souhaitez :

- Améliorer l'expertise interne en matière de sécurité informatique
- Renforcer les pratiques de votre centre des opérations de sécurité
- Développer les capacités de recherche des menaces en interne

4 Compétences requises

3 Personnalisation et évolutivité

4 Niveau d'investissement

Avantages commerciaux

- Inculque à votre équipe SOC les compétences nécessaires pour atténuer plus vite et plus efficacement les risques potentiels des incidents de sécurité
- Vous évite de perdre du temps et de l'argent à essayer de recruter du personnel qualifié difficile à trouver et à attendre ensuite qu'il assimile les caractéristiques spécifiques de votre entreprise
- Vous permet de conserver et de motiver vos salariés via un programme de développement de carrière basé sur les compétences

Application pratique

- Améliorez votre réponse aux incidents par l'analyse des programmes malveillants, vous permettant de comprendre la menace et de développer le plan de réponse le plus efficace
- Conservez un ensemble de preuves sur les systèmes hôte ou réseau afin de révéler la cause première d'un incident, empêcher que des incidents similaires ne se reproduisent et éviter les actions en justice
- Mettez en place des processus de réponse aux incidents évolutifs, rapides et efficaces afin de garantir une parfaite restauration malgrè un large éventail de menaces dans les réseaux d'entreprise

Kaspersky Cybersecurity Services

Kaspersky Cybersecurity Services permet de profiter de toute l'expertise de Kaspersky pour répondre à des incidents touchant la sécurité des informations, révéler des tentatives de compromission passées et présentes et mener des évaluations de la sécurité spécifiques au secteur et dans l'ensemble de l'entreprise afin de colmater les failles de sécurité avant leur exploitation et d'empêcher les futures attaques. En collaborant avec les experts de Kaspersky, vos équipes de sécurité informatique internes peuvent lutter plus efficacement contre les menaces toujours plus sophistiquées.

Le choix idéal si vous souhaitez :

- Pouvoir compter sur un partenaire qui sera toujours à vos côtés en cas d'incident
- Déterminer si vos systèmes de détection et de prévention sont suffisants
- Vous assurer que votre approche de la sécurité est proactive

Avantages commerciaux

- Garantit que les dommages consécutifs à des incidents, quelle qu'en soit la complexité, sont minimisés grâce à un accès permanent à une expertise éprouvée en sécurité informatique
- Réduit considérablement les pertes possibles en cas de temps d'arrêt et évite la mauvaise publicité
- Permet une conformité totale aux réglementations, évitant ainsi les pénalités et les amendes

Application pratique

- Rétablissez plus rapidement vos systèmes et vos opérations commerciales
- Détectez les tentatives de compromission et atténuez les effets des incidents avant qu'ils ne se fassent ressentir
- Améliorez la sécurité des infrastructures d'industries spécifiques
- Évaluez vos capacités de défense et identifiez les points faibles à corriger

Kaspersky Private Security Network

Kaspersky Private Security Network 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 totalement privée, locale et personnelle de Kaspersky Security Network pour les entreprises.

Le choix idéal si vous souhaitez :

- Protéger une organisation pour laquelle le respect de la confidentialité est une exigence majeure par des politiques strictes qui empêchent toute donnée de sortir de son infrastructure informatique
- Respecter les réglementations les plus strictes en matière de protection des données
- Faciliter la circulation des données de Threat Intelligence au sein de votre organisation afin de renforcer la protection et de réduire les temps de réponse

Avantages commerciaux

- Assure la continuité des activités grâce à une détection et une réponse efficaces et au partage des informations en interne
- Augmente l'efficacité opérationnelle en limitant le plus possible le nombre de faux positifs
- Respecte les normes réglementaires pour la sécurité des environnements et systèmes isolés

Application pratique

- Protégez votre infrastructure isolée, voire air-gaped, sans compromettre l'efficacité de la détection des menaces
- Organisez des installations nationales d'échange de données sur les menaces
- Intégrez vos solutions avancées de détection des menaces de Kaspersky à d'autres solutions BtoB de Kaspersky via votre propre réseau interne de Threat Intelligence

5 Compétences requises

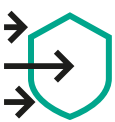
5 Personnalisation et évolutivité

5 Niveau d'investissement

Choses 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 commerciale 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. 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 les menaces actuelles 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.

Pourquoi choisir Kaspersky ?

La plus testée. La plus récompensée

Kaspersky a obtenu plus de premières places que tous les autres fournisseurs de sécurité lors de tests indépendants. Et c'est une performance que nous répétons année après année. www.kaspersky.com/top3

Qualité de la détection confirmée par l'évaluation MITRE ATT&CK

MITRE | ATT&CK®

Le logo GARTNER PEER INSIGHTS CUSTOMERS' CHOICE est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses sociétés affiliées et son utilisation ici fait l'objet d'une autorisation. Tous droits réservés. 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.

Kaspersky a une fois de plus été nommé par le Gartner Peer Insights Customers' Choice pour les plateformes de protection des terminaux.

Kaspersky est un « Customers' Choice » dans le 'Gartner Peer Insights 'Voice of the Customer' d'avril 2020 : Rapport de solutions EDR.

En 2020, Kaspersky a été nommé par le Gartner Peer Insights Customers' Choice pour les passerelles Web sécurisées

Proven.
Transparent.
Independent.

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 fournisseur.

kaspersky