Kaspersky EDR Optimum
Kaspersky EDR
Kaspersky MDR

Comparaison fonctionnelle

kaspersky

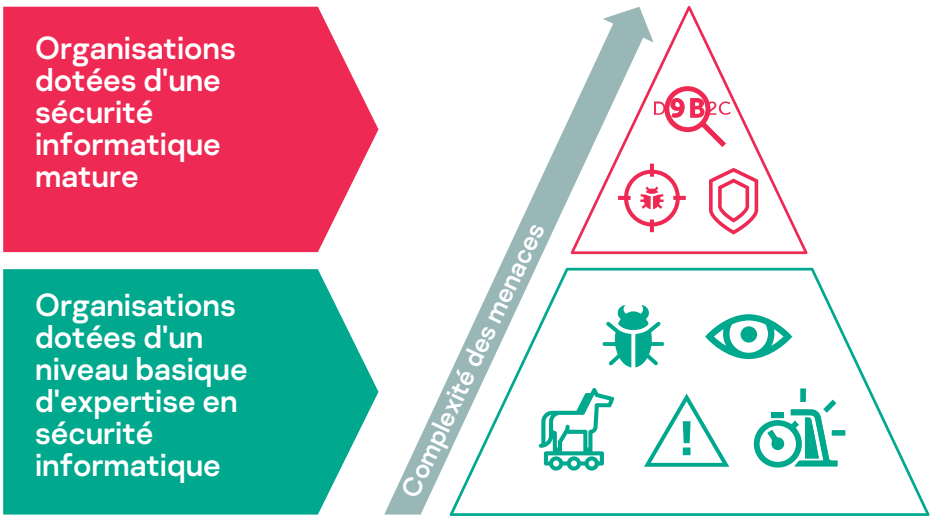
Introduction

Ce document décrit l'approche de Kaspersky en matière de protection contre les menaces complexes et les attaques sophistiquées. Il décrit les capacités de nos produits et services actuels à répondre aux besoins de votre entreprise, en fonction de votre niveau actuel de sécurité informatique et de vos ressources disponibles.

Les cybercriminels attaquent des organisations de toutes tailles et de toutes formes, certaines plus préparées que d'autres à contrer les menaces. Le coût et les efforts requis pour planifier une attaque diminuent constamment, ce qui expose de plus en plus d'organisations aux risques. Les attaques et les menaces, allant des programmes malveillants inconnus, ransomwares et menaces sans fichiers aux attaques de type APT et aux campagnes ciblées utilisent également une multitude d'approches, ce qui témoigne du temps et des efforts que les cybercriminels sont prêts à investir.

Toutes les entreprises doivent être prêtes et capables de parer les menaces d'aujourd'hui, même avec un personnel et une expertise limités. Alors que certaines entreprises disposent de professionnels de la sécurité informatique qualifiés, d'autres peuvent n'en avoir aucun ou tout juste commencer à bâtir leur département de sécurité informatique.

Notre portefeuille comprend une vaste gamme de solutions pour se protéger contre les menaces de différents niveaux, conçues pour répondre aux besoins d'entreprises de tailles et de secteurs variés. Notre approche consiste à aider nos clients potentiels à choisir la combinaison de produits et de services qui leur convient le mieux. Cela implique de tenir compte de leur taille, de leur secteur d'activité et de leur degré actuel de préparation à contrer les menaces, ainsi que des ressources, des connaissances et de l'expertise dont ils disposent.



Kaspersky EDR Optimum

Kaspersky Managed Detection and Response

Kaspersky Endpoint Detection and Response

Kaspersky EDR Optimum

Idéal pour les petites et moyennes entreprises dotées d'une expertise limitée en sécurité informatique ou de ressources limitées

Kaspersky EDR Optimum est conçu pour nos clients ayant une expérience limitée dans la protection contre les menaces, ou dotés d'un département de sécurité informatique restreint et souhaitant comprendre ce qui se passe dans leur infrastructure et répondre aux menaces avant qu'elle ne puissent causer des dégâts. Cette solution complète parfaitement Kaspersky Endpoint Security for Business, notre solution phare de protection de terminaux (EPP). Kaspersky EDR Optimum combine toutes les fonctionnalités de Kaspersky Security for Business Advanced à des capacités EDR de base, gérées conjointement via notre console Kaspersky Security Center.

Cette solution bloque automatiquement des millions de menaces communes, tout en vous aidant à enquêter sur des incidents plus complexes. Ainsi, vous pouvez accroitre votre niveau de protection des terminaux contre une multitude de menaces complexes, sans avoir à multiplier vos ressources de sécurité informatique.

Les capacités EDR fournissent à vos professionnels de la sécurité informatique une carte d'incident contenant des données de détection à utiliser dans les enquêtes détaillées et les analyse des causes profondes. Vous pouvez également créer des indicateurs de compromission (IoC) sur la base des détections reçues, ou importer des IoC à partir de ressources tierces, puis analyser votre infrastructure pour les rechercher. En utilisant les résultats de détection d'IoC, vous pouvez répondre aux menaces automatiquement ou réaliser des activités de réponse « en un clic » comme placer des fichiers en quarantaine, isoler les hôtes, suspendre les processus, supprimer des objets, etc.

Kaspersky Sandbox

Kaspersky EDR Optimum peut être encore amélioré avec l'outil automatisé Kaspersky Sandbox, qui vous aide à contrecarrer les nouvelles menaces capables de contourner la protection des terminaux. Cette solution mène une analyse dynamique des cybermenaces inconnues et évasives, accroissant significativement le pourcentage de menaces pouvant être bloquées automatiquement.

Kaspersky Endpoint Detection and Response

Idéal pour les moyennes et grandes entreprises dotées d'une expertise en matière de sécurité informatique en développement rapide ou pleinement développée

Kaspersky EDR aide votre équipe de sécurité informatique à délivrer une réponse rapide centralisée aux menaces complexes multi-niveaux, réduisant votre temps de réaction de quelques heures à quelques minutes.

Si votre entreprise est particulièrement attrayante pour les cybercriminels et que vous prévoyez de développer votre propre expertise en matière de sécurité en interne ou même votre propre SOC, Kaspersky Endpoint Detection and Response (EDR) est ce qu'il vous faut. Cet outil fournit des capacités avancées pour contrer les menaces complexes aux organisations dotées d'équipes de sécurité informatique bien développées.

Kaspersky EDR est un outil pour la détection, l'enquête et la réponse aux menaces complexes. Il fonctionne avec n'importe quelle édition de Kaspersky Endpoint Security for Business en utilisant un agent unique, notamment Kaspersky Security for Windows Server ainsi que Kaspersky Security Hybrid Cloud et aux côtés de toute solution tierce de sécurité des terminaux.

Des mécanismes supérieurs de détection des menaces dotés d'indicateurs d'attaque (IoA) uniques, une sandbox intégrée ainsi que d'autres moteurs de détection permettent à vos spécialistes de la sécurité informatique de détecter les menaces complexes et les attaques sophistiquées. Kaspersky EDR recueille en continu des mesures de télémétrie et les envoie à un stockage centralisé, de sorte que lors d'une enquête sur un incident, des données rétrospectives peuvent être rapidement obtenues, ce qui est particulièrement important lorsque les terminaux compromis sont inaccessibles ou que leurs données ont été chiffrées par les cybercriminels.

Cette solution permet à votre équipe de sécurité informatique de mener des enquêtes détaillées sur les incidents, en accédant à Kaspersky Threat Intelligence Portal, et des détections enrichies automatiquement mises en correspondance avec la base de connaissances MITRE ATT&CK. Elle lui permet également de créer des requêtes complexes pour les comportements atypiques et suspects, pour des techniques spécifiques dans MITRE ATT&K, et pour d'autres signes d'activité malveillante, prenant en compte les spécificités de votre infrastructure.

Votre équipe est armée de tout ce qu'il lui faut pour mener une recherche proactive des menaces et prendre les mesures appropriées au bon moment pour repousser avec succès les attaques.

Kaspersky Anti Targeted Attack Platform

Kaspersky EDR peut être déployé dans le cadre de la plateforme Kaspersky Anti Targeted Attack (KATA), combinant des capacités EDR avec une détection avancée des menaces au niveau du réseau pour créer une solution de détection et réponse étendue. Vos spécialistes de la sécurité informatique sont équipés d'une boîte à outils complète pour la détection simultanée des menaces à travers votre réseau, vos e-mails, le web et vos terminaux, dans une solution unique tout-en-un

Kaspersky Managed Detection and Response

Idéal pour les petites et moyennes entreprises ne disposant pas d'une expertise optimale en sécurité informatique ou les entreprises dotées d'une équipe de sécurité informatique mature surchargée par les tâches routinières

Si vous ne disposez pas de vos propres experts en sécurité informatique, le service Kaspersky Managed Detection and Response propose une protection avancée instantanée contre les menaces complexes. Si vous en disposez, cela donne à vos experts davantage de temps pour se concentrer sur les activités qui nécessitent réellement leur attention.

Si vous ne disposez pas d'une équipe de sécurité informatique interne, ou si vos spécialistes de la sécurité informatique sont constamment surchargés par des tâches routinières, vous devriez penser à Kaspersky Managed Detection and Response (MDR). Ce service propose une protection ininterrompue contre les cybermenaces avec une surveillance, détection et hiérarchisation en continu des incidents, assorties de capacités de réponse rapides et précises.

Kaspersky MDR fournit un service intelligent, améliorant instantanément vos niveaux de protection contre les menaces avancées et les attaques ciblées via un déploiement rapide clé en main.

Si vous disposez d'un département de sécurité informatique mature, vous pouvez optimiser les ressources de vos experts en sécurité informatique en confiant les tâches de détection d'incidents à l'équipe Kaspersky. Vos experts peuvent également demander son intervention et disposer de l'expertise unique de Kaspersky en matière de détection des menaces.

Informations générales

	Kaspersky EDR Optimum	Kaspersky EDR	Kaspersky MDR
Description	Endpoint Protection, Detection and Response	Endpoint Detection and Response	Managed Detection and Response
Conçu pour les	PME dotées de connaissances en sécurité informatique ou de ressources limitées	Moyennes et grandes entreprises dotées d'une expertise en matière de sécurité informatique en développement rapide ou pleinement développée	PME ne disposant pas d'une expertise optimale en sécurité informatique ou entreprises dotées d'une équipe de sécurité informatique mature surchargée par les tâches routinières
Réponse aux menaces	Des menaces les plus communes aux plus complexes, comme les ransomwares et les menaces sans fichier, etc.	Menaces complexes, sophistiquées et attaques ciblées, de style APT	Des menaces communes aux plus complexes et sophistiquées, y compris APTs
Systèmes d'exploitation pris en charge	Windows	Windows Linux (S1 2021) MacOS (2021)	Windows Linux (S3 2020) MacOS (S1 2021)
Format d'utilisation	Sur site Cloud	Sur site Cloud (2021)	Cloud
Configuration matérielle	Faible	Haute (installation de serveur requise)	Faible
Fonctionnalités EPP	● En tant que composant de Kaspersky Endpoint Security for Business Advanced	● Kaspersky Endpoint Security for Business et Kaspersky Hybrid Cloud Security, et aux côtés d'autres EPP tiers	● Fonctionne conjointement avec Kaspersky Endpoint Security for Business, Kaspersky Hybrid Cloud Security
Ou avec d'autres éditeurs d'EPP	○	●	●

Détection des menaces

	Kaspersky EDR Optimum	Kaspersky EDR	Kaspersky MDR
Détection	◒	●	●
Communes, ainsi que certaines menaces complexes	● Ils utilisent des composants de détection de la solution Kaspersky Endpoint Security for Business	● Peut utiliser les composants de détection de Kaspersky Endpoint Security for Business ou tout autre produit tiers EPP	● Ils utilisent des composants de détection de la solution Kaspersky Endpoint Security for Business
Les attaques sophistiquées et les attaques ciblées	○	●	● Détection par les analystes Kaspersky
Possibilité de rajouter une logique de détection personnalisée sur la base de TTP	○	● Détection basée sur des indicateurs d'attaques personnalisés (IoA rules)	● Mis à jour par les analystes Kaspersky sur la base des spécifications du client
Analyse approfondie de fichiers suspects	● via l'intégration avec Kaspersky Sandbox	● Composant Sandbox intégré avec mappage MITRE ATT&CK	● Analystes Kaspersky pendant l'enquête ou à la demande du client
Threat Hunting	○	●	● Réalisé par les analystes Kaspersky

Investigation sur les incidents

	Kaspersky EDR Optimum	Kaspersky EDR	Kaspersky MDR
Enquête	◒	●	● Réalisé par les analystes de Kaspersky
Informations de détection détaillées	●	●	●
Analyse basée sur l'IoC	●	●	●
Option de création d'IoC	◒ A partir des détections de Kaspersky Endpoint Security for Business	●	● Par des analystes de Kaspersky et à partir des détections de Kaspersky Endpoint Security for Business
Niveau de contexte de l'événement pour l'analyse des causes profondes	◒ Enrichissement à partir des détections de Kaspersky Endpoint Security for Business	●	●
Accès au Threat Intelligence Portal	◒ Open TIP	● Kaspersky TIP	● Kaspersky TIP
Mappage MITRE ATT&CK	○	●	●
Soumission de fichiers manuelle à la sandbox pour l'analyse	○	●	● Par les analystes de Kaspersky ou à la demande du client
Informations détaillées sur les fichiers suspects	○	●	●
Accès aux données « brutes » pour analyse	◒ A partir des détections de Kaspersky Endpoint Security for Business	●	● Réalisé par les analystes Kaspersky dans le cadre de l'enquête
Analyse rétrospective	○	●	● Par les analystes Kaspersky
Cyberdiagnostic de base	○	●	● Par les analystes Kaspersky

Réponse

	Kaspersky EDR Optimum	Kaspersky EDR	Kaspersky MDR
Outils de réponse aux menaces complexes	●	●	● Lancement automatique et reposant sur les recommandations de réponse
Réponse automatique	Repose sur les résultats de la détection de Kaspersky Endpoint Security for Business et la détection des IoC créés	Auto-prévention sur la base des résultats de détection de la sandbox	Règles de réponse élaborées par les analystes Kaspersky
Réponse semi-automatisée	●	●	●
Interruption du lancement d'un fichier exécutable	●	●	●
Isolation de l'hôte	●	●	●
Activités de réponse additionnelles (lancement de fichier/ script, arrêt du processus, quarantaine de fichier, suppression de fichier)	●	●	●
investigation sur les incidents et réponse adaptée	○	●	● Fourni par les analystes de Kaspersky

www.kaspersky.fr