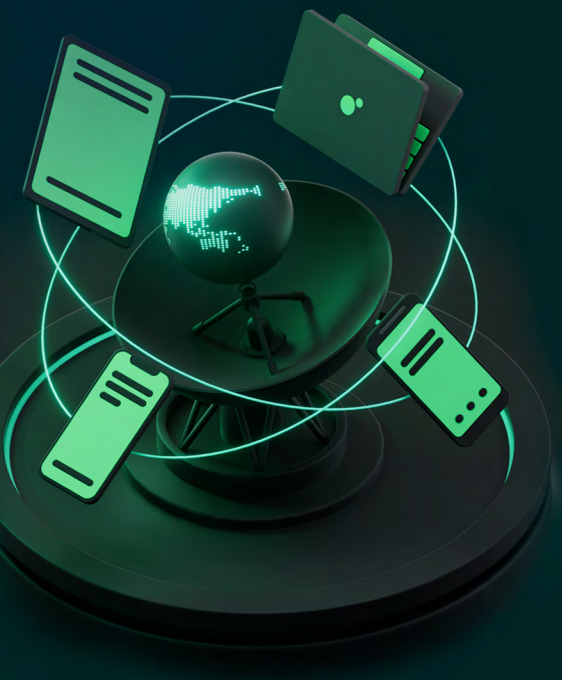
Kaspersky Next
XDR Expert

Présentationde Kaspersky Next XDR Expert

Qu'est-ce que Kaspersky Next XDR Expert ?

Kaspersky Next XDR Expert est le plus avancé des trois niveaux de la gamme de solutions Kaspersky Next. Il s'intègre de manière transparente à l'infrastructure de sécurité existante d'une organisation, offrant une visibilité en temps réel et une connaissance approfondie de l'évolution des cybermenaces, afin de fournir une détection avancée des menaces, une réponse automatisée et une gamme étendue de fonctionnalités XDR essentielles.



Pourquoi Kaspersky Next XDR Expert, et pourquoi maintenant ?

Les cybercriminels affinent sans cesse leurs tactiques et développent des méthodes de plus en plus sophistiquées pour cibler les organisations. Les pirates informatiques d'aujourd'hui adoptent de plus en plus une approche multivectorielle pour organiser leurs attaques, impliquant souvent plusieurs points d'entrée dans l'infrastructure et une variété de tactiques et techniques.

Les menaces persistantes avancées (APT), par exemple, contournent la détection traditionnelle au niveau des terminaux et peuvent rester actives pendant des semaines, voire des mois, en se déplaçant latéralement dans le réseau, en obtenant des autorisations, en exfiltrant des données et en recueillant des informations à partir des différentes couches de l'infrastructure informatique en vue d'une attaque à grande échelle ou d'une violation de données.

Pour assurer une sécurité efficace contre ces menaces, il faut adopter une approche globale et proactive combinant des technologies avancées, des stratégies solides, une surveillance vigilante, une formation continue, etc. Et c'est exactement cette vision à 360° du paysage des menaces que le XDR se propose d'offrir.

En décloisonnant les solutions ponctuelles propres à une couche, le XDR offre aux SOC et aux équipes de sécurité informatique la visibilité et l'intégration de bout en bout nécessaires pour identifier plus vite les menaces, y répondre plus rapidement, les résoudre plus efficacement et minimiser les dommages causés.

Comment le XDR résout ces questions

L'adjectif « étendu » dans « détection et réponse étendues » reflète l'idée que, dans le cadre de la technologie XDR, une solution de détection et de réponse au niveau des terminaux (EDR) est complétée par une série d'outils de sécurité auxquels elle est étroitement intégrée.

Avec le XDR, des solutions de sécurité qui ne sont pas nécessairement conçues pour fonctionner ensemble peuvent interagir de manière transparente sur la prévention, la détection, l'enquête et la réponse aux menaces. Il pourrait s'agir, par exemple, de solutions conçues pour protéger les emails, Internet, le réseau, l'infrastructure dans le cloud, les applications, l'identité, etc., permettant de détecter et d'étudier de nouveaux types de scénarios d'attaque et de renforcer le processus de lutte contre les cybermenaces complexes.

En offrant une vue unique et une visibilité totale entre les outils et les couches de cybersécurité, le XDR permet aux équipes de sécurité surchargées de détecter et de résoudre les menaces plus rapidement et plus efficacement, et de capturer des données plus complètes et contextuelles pour les aider à prendre de meilleures décisions en matière de sécurité et à prévenir de futures attaques.

Pour lutter contre des cybermenaces de plus en plus sophistiquées, les entreprises ne peuvent plus se contenter d'un ensemble unifié d'outils de sécurité provenant du même fournisseur

Découvrez le produit Kaspersky Next qui vous convient le mieux à l'aide de notre outil interactif : https://go.kaspersky.com/Kaspersky_Next_Tool

Quels sont les avantages pour les entreprises ?

Pour lutter contre des cybermenaces de plus en plus sophistiquées, les entreprises ne peuvent plus se contenter d'un ensemble unifié d'outils de sécurité provenant du même fournisseur.

- Dans un contexte de pénurie mondiale d'experts en sécurité informatique, le XDR assure la protection globale d'une infrastructure informatique en expansion et en mutation face à un paysage de cybermenaces en évolution rapide.
- En automatisant les tâches de routine, le XDR réduit les efforts manuels et les temps de réponse, simplifie le travail de ressources précieuses et rares comme les spécialistes en sécurité informatique, et les libère pour traiter les incidents complexes.
- En permettant une analyse comportementale et télémétrique en temps réel à travers plusieurs couches de sécurité, les analystes de sécurité peuvent mieux visualiser les cybermenaces, les cibler et les éliminer en fonction de la gravité de leur impact sur l'infrastructure informatique de l'organisation.
- Le XDR permet de réduire le temps moyen de détection (MTTD) et le temps moyen de réponse (MTTR), essentiels dans la lutte contre les menaces complexes et les attaques ciblées.

De plus, même si votre organisation dispose de ressources limitées en experts, le XDR peut vous protéger d'attaques complexes grâce à des fonctionnalités comme :

- L'automatisation accrue des processus.
- L'utilisation d'une console unique et unifiée.
- Des guides et une automatisation permettant une interaction étroite entre les outils de sécurité informatique dans le cadre du XDR et de scénarios communs.
- Un seul environnement de lac de données (data lake).
- Un enrichissement intégré avec des données fiables et pertinentes sur les menaces.
- Réduction des faux positifs et de l'impact des menaces réelles.

Comment Kaspersky Next XDR Expert peut vous aider

Avantages de la solution

La plateforme Open XDR complète s'intègre de manière transparente à l'infrastructure, aux outils et aux applications de sécurité existants

Elle fournit une visibilité en temps réel et des informations approfondies sur l'évolution des cybermenaces afin d'assurer une détection avancée des menaces et une réponse automatisée

Comment ça fonctionne ?

Détection des menaces complexes grâce à la corrélation croisée de plusieurs sources de données

Inclut une puissante fonctionnalité EDR avec des capacités de détection et de réponse avancées

Permet une recherche proactive des menaces afin de découvrir des attaques complexes bien cachées

Valeur commerciale

L'approche par écosystème, couplée à une conception ouverte, optimise l'efficacité des outils de cybersécurité mis en œuvre, économise des ressources et réduit le risque

Simplifie le travail des spécialistes de la sécurité informatique et leur procure le contexte supplémentaire nécessaire pour enquêter sur les attaques perpétrées avec plusieurs vecteurs

Minimise les temps moyens de détection et de réponse (MTTD et MTTR), ce qui est essentiel pour combattre les menaces complexes et les attaques ciblées

Fournit une protection globale contre le paysage des menaces en évolution

À qui la solution s'adresse

Organisations disposant d'importantes ressources en matière de sécurité et recherchant une plateforme unique avec ce qui suit :

- Une image cohérente de ce qui se passe dans l'infrastructure protégée
- Recherche des menaces et Threat Intelligence intégrées
- Hiérarchisation des incidents supérieure et moins d'alertes de faux positifs

Qu'obtenez-vous ?

Protection des terminaux

Antivirus pour fichiers, Internet et emails, protection réseau, détection des comportements, correction, prévention des exploits, HIPS, AMSI, anti-chiffreur, protection BadUSB

Gestion de la sécurité

Pare-feu, Internet, appareil, contrôle des applications, contrôle adaptatif des anomalies, Cloud Discovery, blocage du cloud, contrôle de l'intégrité des fichiers, inspection des journaux, contrôle de l'intégrité du système

Protection et gestion des appareils mobiles

Protection, contrôles et gestion, MDM iOS

Scénarios informatiques

Évaluation des vulnérabilités, gestion des correctifs, nettoyage des données, inventaire des logiciels et des équipements, installation d'applications tierces et de systèmes d'exploitation, connexion à distance

Chiffrement

Chiffrement et gestion du chiffrement

Fonctionnalités EDR

Analyse des causes profondes, analyse IOC, réponse automatisée en un seul clic, recommendations de réponse

Fonctionnalités EDR avancées

Collecte de données télémétriques, fonctionnalités de recherche des menaces, détection des indicateurs d'attaque (IoA), cartographie MITRE ATT&CK

Capacités XDR

Agrégation d'alertes, sandbox, intégration d'AD, threat intelligence / enrichissement Kaspersky Security Network, gestion des cas, guides manuels et automatisés, graphique d'enquête, connecteurs tiers, gestion des journaux et lac de données (data lake), réponse entièrement automatisée, détection des menaces et corrélation croisée

Et si vous utilisez déjà une solution de sécurité Kaspersky ?

Votre solution Kaspersky	Migration recommandée	Capacités supplémentaires
Kaspersky Endpoint Detection and Response Standard / Advanced / Expert*	Kaspersky Next XDR Expert	• Scénarios croisés • Agrégation des alertes • Flux de travail en cas d'incident • Graphique d'enquête

* N'oubliez pas que vous pouvez toujours acheter ou utiliser Kaspersky EDR Expert en tant que solution autonome, ou la mettre à niveau et l'utiliser dans le cadre de Kaspersky Next XDR Expert

En savoir plus à propos de Kaspersky Next XDR Expert

Kaspersky Next XDR Expert

Kaspersky Next EDR Foundations — En savoir plus

Kaspersky Next EDR Optimum — En savoir plus

Pour en savoir plus à propos de Kaspersky Next, consultez le site : https://go.kaspersky.com/next

Actualités des cybermenaces : securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les PME : kaspersky.fr/business
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise

kaspersky.fr