Kaspersky Next XDR Expert

Vision inégalée. Protection totale.

kaspersky

La complexité de la cybersécurité en entreprise

Face aux cybermenaces, il est extrêmement difficile pour les entreprises de garder le contrôle sur leur cybersécurité tout en se concentrant sur leur cœur de métier. Ajoutez à cela une surface d'attaque qui ne cesse de s'étendre, des exigences réglementaires et une pénurie de compétences à l'échelle mondiale, et vous comprendrez facilement pourquoi les entreprises modernes sont soumises à une telle pression – et pourquoi tant de cyberattaques réussissent.

51 %

des entreprises ont du mal à détecter les menaces avancées et à mener des enquêtes sur celles-ci avec les outils actuels

68 %

des entreprises ont fait l'objet d'une attaque ciblée sur leurs réseaux et ont subi une perte de données comme conséquence directe

6 milliards de dollars

le coût annuel global de la cybercriminalité

400000

nouveaux programmes malveillants détectés chaque jour

Sources : Kaspersky, PurpleSec, CybersecurityVentures

Kaspersky Extended Detection and Response

Visibilité complète. Protection inégalée.

Dans le cadre de la gamme de produits Kaspersky Next, nous avons introduit Kaspersky Next XDR Expert, une solution qui incarne l'approche XDR de Kaspersky et fournit une vue d'ensemble de la sécurité d'une entreprise.

Kaspersky XDR est une solution de cybersécurité robuste qui permet de se défendre contre les cybermenaces complexes. Elle offre une visibilité, une corrélation et une automatisation complètes, en exploitant une gamme variée de sources de données, y compris les données des terminaux, du réseau et du cloud.

Elle a évolué de la plateforme Kaspersky Anti-Targeted Attack en tant que XDR native en 2016 à un XDR ouvert en 2023, offrant une vision globale de la sécurité. Facilement gérée à partir de la plateforme ouverte de gestion unique, Kaspersky XDR offre une sécurité complète sur site, assurant que les données confidentielles des clients demeurent au sein de leur propre infrastructure tout en répondant aux exigences en matière de souveraineté des données.

Open XDR

Les solutions XDR ouvertes sont conçues pour fonctionner avec une large gamme de produits de sécurité, ce qui permet aux organisations d'intégrer divers produits de sécurité provenant de différents fournisseurs, offrant ainsi une plus grande flexibilité et des capacités non liées à un fournisseur particulier.

XDR natif

Les solutions XDR natives fonctionnent généralement de manière transparente avec l'écosystème d'outils de sécurité du fournisseur, offrant ainsi une expérience plus unifiée et cohérente. Ces solutions sont conçues pour fonctionner conjointement et offrent une intégration poussée, une automatisation et des flux de travail simplifiés au sein de la suite de produits de sécurité de l'éditeur.

Principales technologies

Nous proposons Open XDR en tant que plateforme ouverte unique – un outil universel pour créer un écosystème unifié de produits de cybersécurité. Au cœur de Kaspersky XDR se trouvent nos solutions phares – Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Next EDR Foundations et Kaspersky Endpoint Detection and Response Expert. Pour une gestion avancée du réseau, KATA est une option supplémentaire.

Surveillance et analyse

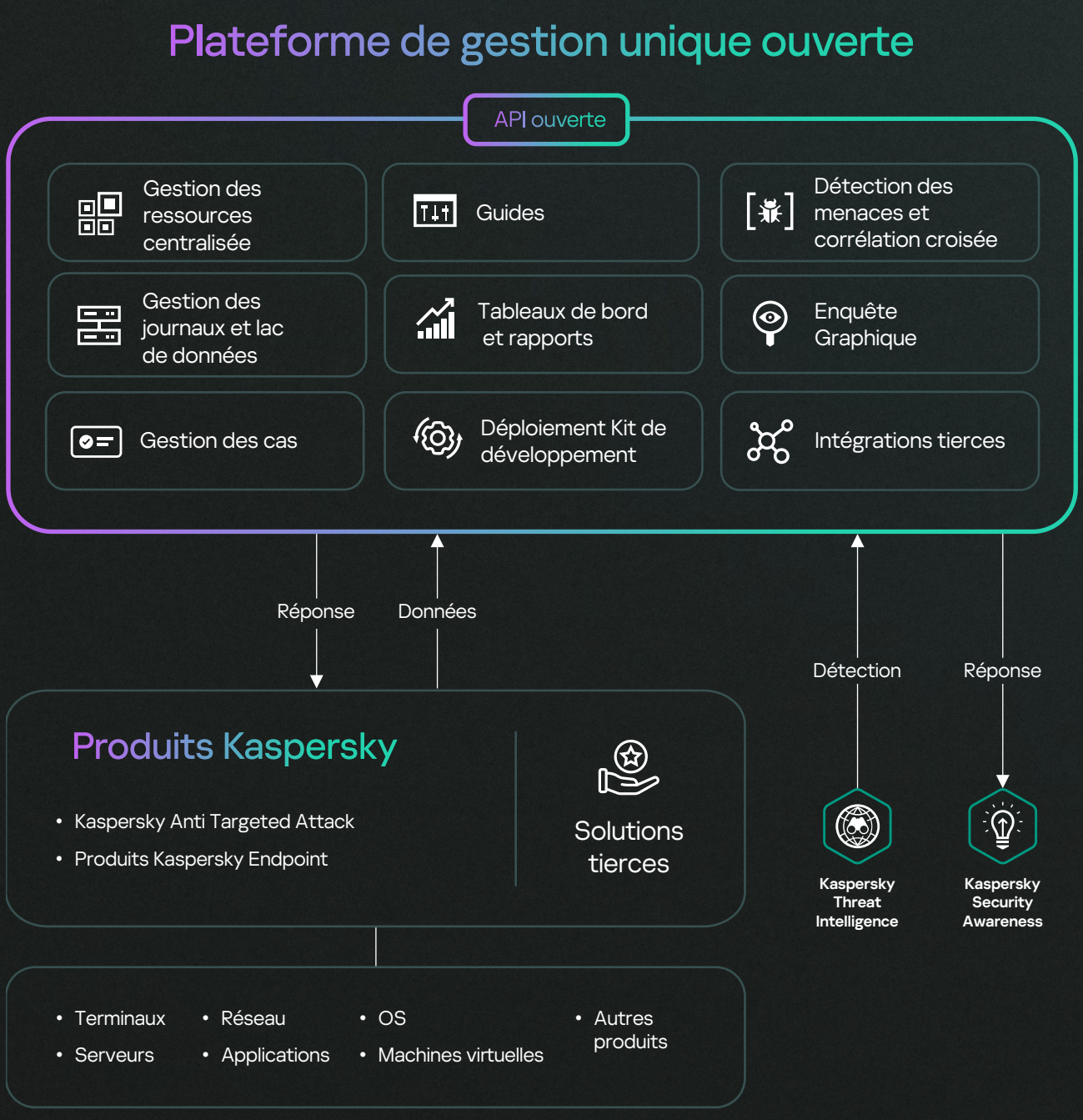
Permet de centraliser la collecte et l'analyse des journaux, de corréler les événements de sécurité en temps réel et de signaler les incidents à temps. Comprend un ensemble de règles de corrélation prêtes à l'emploi et l'accès au riche portefeuille de services de Kaspersky Threat Intelligence pour identifier et hiérarchiser les menaces, les attaques ainsi que les IoC.

Protection des terminaux

Offre une protection robuste des terminaux, assurant une protection contre les ransomwares, les programmes malveillants et les attaques sans fichier. Sur site ou dans le cloud, notre protection des terminaux utilise le Machine Learning et l'analyse comportementale pour protéger tous les types de terminaux fonctionnant sous n'importe quel système d'exploitation majeur.

Endpoint Detection and Response

Offre une visibilité complète et des défenses supérieures sur tous les terminaux d'une entreprise. La détection avancée des menaces reposant sur l'approche unique de Kaspersky en matière de Threat Intelligence, l'automatisation des tâches de routine, les processus d'enquête guidée et les détections personnalisables accélèrent la résolution des incidents.



Des fonctionnalités puissantes, des avantages non négligeables

Fusion de données en temps réel provenant de tiers

La capacité d'intégrer des données provenant de sources tierces s'étend au-delà des seuls terminaux et est renforcée par la corrélation croisée en temps réel.

Réponse et correction automatisées

Mettez en quarantaine les terminaux compromis ou isolez-les, bloquez les activités malveillantes et remédiez aux vulnérabilités, en réduisant les efforts manuels ainsi que le temps de réponse.

Les meilleures solutions EPP/EDR de leur catégorie

Reconnu comme le leader mondial, Kaspersky est la référence en matière de solutions EPP/EDR dans le monde entier. Kaspersky EDR se distingue à l'échelle mondiale, avec des récompenses à la clé et une participation active à des comités internationaux, comme Interpol ou encore MAPP.

Évolutivité inégalée

Capable de prendre en charge des charges englobant des centaines de milliers de terminaux sur une seule instance, Kaspersky XDR traque les menaces en temps réel tout en assurant une disponibilité maximale.

Souveraineté des données

Kaspersky XDR est l'un des rares fournisseurs à proposer une solution XDR complète sur site, garantissant que les données confidentielles des clients restent au sein de leur propre infrastructure tout en répondant aux exigences en matière de souveraineté des données.

Intégration transparente et étroite dans tous les produits Kaspersky

L'interaction entre les produits atteint un niveau inégalé par les solutions tierces, grâce à un système d'assistance unifié et à une conception parfaitement intégrée.

Multi-location permettant des scénarios MSSP

Proposez le XDR en tant que service avec des clients à part entière – les utilisateurs d'un client ne peuvent pas voir les données des autres clients, tandis que l'administrateur principal (le MSSP) peut mettre en place des processus de détection et de réponse pour tous les clients.

Personnalisation avancée des scénarios de sécurité et analyse des données à l'échelle de l'infrastructure

Permet aux utilisateurs de configurer des scénarios de sécurité complexes avec la possibilité supplémentaire d'analyser les données dans l'ensemble de leur infrastructure.

Capacités d'intégration

Le large éventail d'intégrations qui fonctionnent avec Kaspersky XDR offre une vue unifiée et contextualisée des menaces, donnant à votre équipe de sécurité tous les outils et toutes les informations dont elle a besoin pour protéger votre organisation contre les menaces des cybercriminels.

Les capacités d'intégration du produit incluent la possibilité de recevoir des données (logs) d'autres systèmes et appareils, ainsi que de configurer des réponses automatisées dans d'autres produits. Kaspersky XDR propose un large éventail d'intégrations prêtes à l'emploi, avec Kaspersky et des produits tiers. Il est également possible d'ajouter des intégrations supplémentaires qui peuvent être développées soit par les services professionnels de Kaspersky, soit par des partenaires ou des clients eux-mêmes (y compris en utilisant les fonctionnalités API des produits connectables). L'intégration est possible avec des systèmes provenant de différents domaines et de différents fournisseurs, et de nombreux protocoles et formats de données sont pris en charge.

Par domaine de sécurité

Protection des terminaux

- Solutions EPP et EDR

Protection des réseaux, du Web et des messageries

- Protection des emails
- Network Detection and Response (NDR)
- Pare-feu (FW) et pare-feu de nouvelle génération (NGFW)
- Gestion unifiée des menaces
- Système de détection des intrusions (IDS)

Antivirus dans le Cloud

- Agents de sécurité des accès au cloud (CASB)
- Plateformes de protection des charges de travail dans le cloud (CWPP)

Threat Intelligence

- Veille stratégique contre les cybermenaces (CTI)

Protection de l'identité

- Gestion de l'identité et des accès (IAM)
- Gestion des accès privilégiés (PAM)

Sensibilisation à la sécurité des TO/de l'IdO

Par type de transport

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
  - SQLite
  - MSSQL
  - MySQL
  - PostgreSQL
  - Cockroach
  - Oracle
  - Firebird
- Fichier
- 1c-log et 1c-xml
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- VmWare API

Par type de donnée

- XML
- Syslog
- CSV
- JSON
- SQL
- IPFIX
- CEF
- Netflow 5
- Netflow 9
- KV

Par fournisseur

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper
- Kemptechnologies
- Kerio
- Lieberman
- MariaDB
- Microsoft
- MikroTik
- Minerva
- NetIQ
- NetScout
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto
- Penta Security
- Proofpoint
- Radware
- Recorded
- ReversingLabs
- SailPoint
- SentinelOne
- Sonicwall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMWare
- Vormetric
- WatchGuard - Firebox
- Winchill Fracas
- Zettaset
- Zscaler & etc.

Notre offre

Kaspersky XDR est disponible en deux versions.

Kaspersky XDR Core

Kaspersky XDR Core s'adresse aux clients qui disposent déjà de solutions pour terminaux et EDR et qui ne souhaitent pas les remplacer, préférant étoffer leurs fonctionnalités avec un moteur de corrélation, des réponses automatisées et des connecteurs tiers.

Kaspersky Next XDR Expert

Kaspersky Next XDR Expert combine une protection des terminaux de pointe avec les capacités de détection avancées de Kaspersky EDR Expert, un moteur de corrélation ainsi que des réponses automatisées. Il est possible d'ajouter des connecteurs tiers pour rassembler toutes les données.

Valeur ajoutée grâce à des capteurs supplémentaires

Kaspersky XDR permet d'intégrer de manière transparente des capteurs supplémentaires conçus pour protéger des ressources particulières, de s'intégrer de manière transparente au XDR pour apporter une valeur ajoutée et de transformer le XDR en une plateforme cohésive qui offre aux analystes un espace de travail centralisé englobant toutes les solutions intégrées.

Kaspersky XDR renforce non seulement votre protection grâce à l'EDR, mais offre également des possibilités d'intégration flexibles, permettant aux clients d'ajouter des produits à l'écosystème à tout moment.

		Kaspersky XDR Core	Kaspersky Next XDR Expert
Plateforme ouverte de gestion unique et ses modules	Moteur de corrélation croisée • Connecteurs tiers • Gestion des journaux et lac de données • Détection des menaces et corrélation croisée • Gestion des ressources • Tableaux de bord et rapports	●	●
	Modules XDR • Gestion des cas • Automatisation et orchestration des réponses (guides) • Enquête • Boîte à outils de déploiement • API ouverte	●	●
Fonctionnalités de Kaspersky Endpoint*	Détection automatisée, semi-automatisée et manuelle		●
	Surveillance des terminaux protégés		●
	Confinement des menaces		●
	Options de récupération		●
	Protection et gestion des appareils mobiles		●
	Identification et blocage dans le cloud		●
	Sécurité pour MS O365, Data Discovery		●
	Formation à la cybersécurité pour les administrateurs informatiques		●

* La disponibilité des fonctionnalités varie en fonction de la méthode de mise en œuvre

Kaspersky XDR Core

Kaspersky Unified Monitoring and Analysis Platform

Modules XDR

Kaspersky Next XDR Expert

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Next EDR Foundations

Kaspersky Endpoint Detection and Response Expert

Modules XDR

Présentation de Kaspersky Next

Kaspersky Next EDR Foundations

Une sécurité robuste pour tous

Protégez tous vos terminaux

Si vos besoins sont

- Protection renforcée des terminaux
- Contrôles de sécurité de base
- Automatisation maximum

Kaspersky Next EDR Optimum

Renforcez vos défenses

Renforcez votre sécurité grâce à des enquêtes et des réponses essentielles

Si vos besoins sont

- Amélioration de la visibilité et des capacités de réaction
- Sécurité étendue du cloud
- Contrôles de niveau professionnel

Kaspersky Next XDR Expert

Donnez les moyens à vos experts

Protégez votre entreprise contre les menaces les plus complexes et les plus avancées

Si vos besoins sont

- Détection des menaces avancées
- Intégration harmonieuse
- Outils puissants de recherche des menaces

Pourquoi Kaspersky XDR ?

La plus testée. La plus récompensée. La protection Kaspersky.

Kaspersky est une entreprise mondiale de cybersécurité bien établie, qui a fait ses preuves en matière d'expertise en sécurité. Nous protégeons des organisations dans le monde entier depuis plus de 25 ans et avons reçu d'innombrables prix et distinctions pour nos produits et services. Entre 2013 et 2022, les produits Kaspersky :

827
ont participé à 827 études et avis indépendants

587
ont réussi à obtenir 587 premières places

685
ont réussi à se classer parmi les trois premiers

En 2023, Kaspersky a été désigné leader du marché des solutions XDR par le cabinet mondial de recherche et de conseil en technologies ISG. L'ISG définit les « leaders » comme des entreprises proposant une offre complète de produits et de services et faisant preuve d'innovation et de stabilité concurrentielle.

En savoir plus

Kaspersky Extended Detection and Response

Demander une démonstration

www.kaspersky.fr

#kaspersky
#bringonthefuture