

Kaspersky Next EDR Foundations

Une cybersécurité simple, adaptée à votre budget et efficace contre les cybermenaces



kaspersky



Kaspersky Next
EDR Foundations

Une cybersécurité simple, adaptée à votre budget et efficace contre les cybermenaces

La puissante protection des terminaux basée sur le ML (Machine Learning), les contrôles de sécurité flexibles et les outils d'analyse des causes profondes de l'EDR de **Kaspersky Next EDR Foundations** vous offrent tous les outils nécessaires pour construire un noyau solide pour votre cybersécurité. La console conviviale, le déploiement dans le cloud ou sur site et la variété des fonctionnalités destinées à vous faciliter la vie réduisent la complexité et renforcent l'efficacité.



Protégez n'importe quel appareil, n'importe où

Quels que soient l'emplacement de vos bureaux, le lieu de travail de vos collaborateurs dans l'exercice de leurs fonctions ou les appareils qu'ils utilisent, protégez-les tous à partir de la console basée dans le cloud ou sur site.

Kaspersky Next EDR Foundations protège les ordinateurs de bureau et les serveurs de fichiers Windows, les appareils macOS ainsi que les appareils mobiles iOS et Android. Il n'est pas nécessaire d'immobiliser le matériel et les logiciels. En effet, grâce à **Kaspersky Next EDR Foundations**, il est facile de déployer des agents à distance sur les terminaux. Profitez d'une protection instantanée grâce aux stratégies prédéfinies élaborées par nos spécialistes en sécurité



Postes de travail Windows et macOS



Serveurs de fichiers Windows



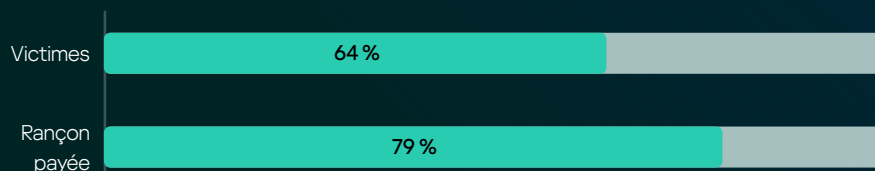
Smartphones et tablettes iOS et Android

64 % des organisations ont déjà été victimes d'attaques de ransomwares. Parmi celles-ci, 79 % ont payé la rançon.

[Comment les chefs d'entreprise perçoivent les menaces liées aux ransomwares](#), Kaspersky, mai 2022

Les ransomwares : plus qu'un simple terme à la mode...

Kaspersky Next EDR Foundations protège vos appareils contre les menaces connues, inconnues et avancées grâce à notre moteur de protection contre les programmes malveillants, le plus testé et le plus récompensé.



Alors que les ransomwares constituent un défi permanent pour les entreprises de toute taille, il est essentiel de disposer de défenses automatisées et de pouvoir prendre des mesures rapidement, même si vos ressources sont limitées. La prévention des ransomwares et l'annulation des activités malveillantes de Kaspersky démontrent une **efficacité totale** contre les attaques par ransomwares et les cryptolockers.

Gain de temps et de ressources

Les petites entreprises peuvent ne pas avoir le budget nécessaire pour se protéger contre les logiciels malveillants en plus de leurs antivirus de bureau. La solution **Kaspersky Next EDR Foundations** vous offre une protection fiable et efficace contre les ransomwares, les programmes malveillants sans fichier et les attaques de type « zero-day », sans pour autant dépasser votre budget ou avoir besoin d'une expertise en cybersécurité.

Profils de sécurité pratiques basés sur les utilisateurs

- Un seul profil de sécurité est appliqué à tous les appareils sur lesquels l'utilisateur travaille
- Prêt à l'emploi
- Des profils distincts et personnalisés pour les différents appareils et groupes d'employés



Gestion efficace des vulnérabilités

- Obtenez une vue d'ensemble des applications installées sur les appareils de l'entreprise
- Ainsi qu'une liste des correctifs disponibles pour mettre à jour les applications vers les dernières versions



Réponse aux menaces en toute simplicité

- Prévention des menaces entièrement automatisée
- Annulation des activités malveillantes

Réagissez sans attendre aux défis posés par la cybersécurité

Shadow IT

Il est trop facile pour les employés d'utiliser des outils de collaboration non approuvés, ce qui peut créer des problèmes de compatibilité, introduire des risques de sécurité et même compromettre la productivité. Il est essentiel que le service informatique dispose d'une vue d'ensemble de cette situation afin de dresser un plan d'action approprié.

Cloud Discovery vous présente une vue d'ensemble pour que vous puissiez agir

Analyser l'utilisation des services SaaS :

- Tableau de bord – vue statistique
- Rapport PDF pour le PDG ou les RH

Comprendre la situation :

- Les employés ne savent pas toujours quels outils sont légitimes
- Les outils de l'entreprise sont peu pratiques et défectueux
- Les utilisateurs peuvent contourner intentionnellement les stratégies de sécurité

Planifier et réagir :

- Sensibilisez vos employés
- Bloquez certains services/catégories



Réduisez votre surface d'attaque



Contrôle des applications

Gère le démarrage des applications sur les ordinateurs des utilisateurs et réduit le risque d'infection en limitant l'accès à ces applications



Contrôle du web

Contrôle centralisé de l'accès aux ressources Web non liées au travail ou suspectes



Contrôle des appareils

Limite l'accès des utilisateurs à divers appareils afin de protéger les données contre tout stockage, conversion ou transfert illégal.

Analyse des causes profondes et visibilité

Détectez et identifiez les attaques avancées, effectuez une analyse des causes profondes avec une visualisation de la chaîne de frappe et examinez de près les détails pour une vérification supplémentaire.

Où ?

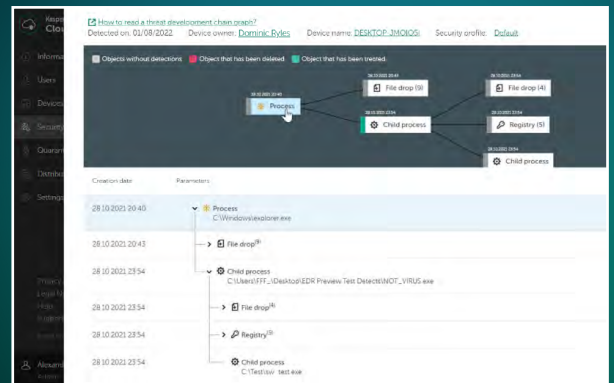
Indique exactement ce qui s'est passé, sur quel hôte et pour quel utilisateur

Comment ?

La visualisation du chemin de propagation des attaques vous permet de constater et d'analyser rapidement la façon dont la menace s'est développée sur l'hôte

Quoi ?

Grâce à des données enrichies et à des outils de visualisation, déterminez la cause profonde de la menace et vérifiez si des mesures de réponse supplémentaires doivent être prises



Reprenez le contrôle des appareils mobiles non gérés

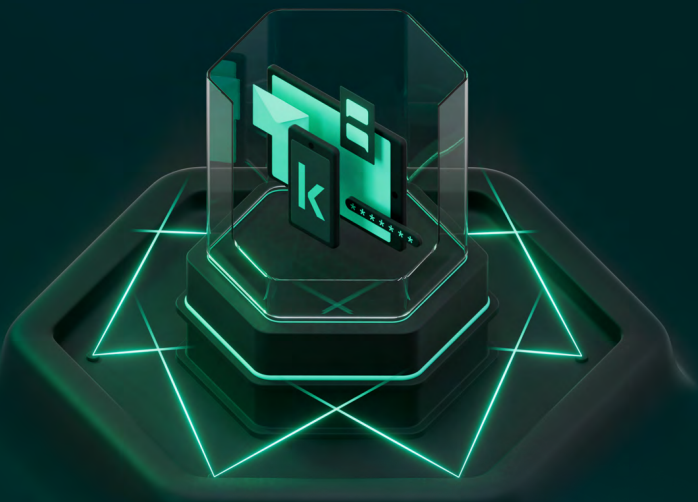
La protection antivirus permet de se défendre contre les menaces, les virus et d'autres applications malveillantes en temps réel.

La protection du Web bloque l'accès aux sites de phishing et aux sites Web malveillants. Elle contrôle aussi l'accès aux sites Web.

La protection par mot de passe sécurise l'accès à l'appareil avec un mot de passe de déverrouillage d'écran qui prend en charge Face ID et Touch ID.

Les contrôles des applications et des fonctionnalités restreignent l'utilisation inappropriée des applications et des fonctionnalités sur les appareils mobiles.

L'antivol permet de localiser à distance l'appareil, de déclencher une alarme en verrouillant l'appareil ou d'effacer des données de l'appareil lorsqu'il est perdu ou volé.



Prochaines étapes

Kaspersky Next EDR Foundations est le premier niveau de la gamme de produits Kaspersky Next. Kaspersky Next comprend trois niveaux, adaptés à la complexité, à la maturité et aux besoins de l'organisation du client. Voici ce que chaque niveau offre et comment il s'articule :

Kaspersky Next EDR Foundations

La manière la plus simple de construire un cadre solide pour votre cybersécurité.

- Protection puissante des terminaux basée sur le ML
- Correction automatique
- Multiples fonctionnalités d'automatisation
- Contrôles de sécurité flexibles
- Outils d'analyse des causes profondes de l'EDR

Kaspersky Next EDR Optimum

Renforcez vos défenses et votre expertise contre les menaces évasives.

- Les fonctionnalités essentielles de l'EDR assurent visibilité, analyse et réponse
- Protection renforcée des terminaux
- Contrôles renforcés, gestion des correctifs et sécurité du cloud
- Formation à la cybersécurité pour les services informatiques

Kaspersky Next XDR Expert

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

- S'intègre parfaitement à votre infrastructure de sécurité existante
- Visibilité en temps réel et connaissance approfondie des menaces
- Détection des menaces avancées
- Corrélations croisées
- Réponse automatisée

Pourquoi Kaspersky ?

Nous sommes une entreprise privée mondiale de cybersécurité qui compte des milliers de clients et de partenaires dans le monde entier. Nous sommes convaincus de l'importance de [la transparence et de l'indépendance](#). Depuis plus de 25 ans, nous concevons des outils et fournissons des services pour assurer la sécurité de nos clients grâce à nos [technologies les plus testées et les plus récompensées](#).

IDC

Rapport IDC MarketScape sur l'évaluation des fournisseurs, catégorie « Worldwide Modern Endpoint Security for Enterprises 2021 »

Acteur principal



AV Test

Protection avancée pour les terminaux : test de protection contre les ransomwares

Protection totale



Radicati Group

Market Quadrant sur les menaces persistantes avancées (APT)

Acteur principal



Étudiez tout cela de plus près

Pour en savoir plus à propos de la façon dont Kaspersky Next EDR Foundations traite les cybermenaces tout en allégeant le travail de votre équipe de sécurité et en préservant vos ressources, veuillez consulter le site :

<https://go.kaspersky.com/next>.

En savoir plus à propos de [Kaspersky Next EDR Foundations](#)



Kaspersky Next
EDR Foundations



Kaspersky Next
EDR Optimum

En savoir plus



Kaspersky Next
XDR Expert

En savoir plus

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/entreprise

kaspersky.fr

© 2024 AO Kaspersky Lab.
Les marques déposées et les marques de service
sont la propriété de leurs détenteurs respectifs.

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

Choisissez le niveau qui vous convient le mieux en
répondant à un bref questionnaire dans notre outil
interactif :

https://go.kaspersky.com/Kaspersky_Next_Tool

