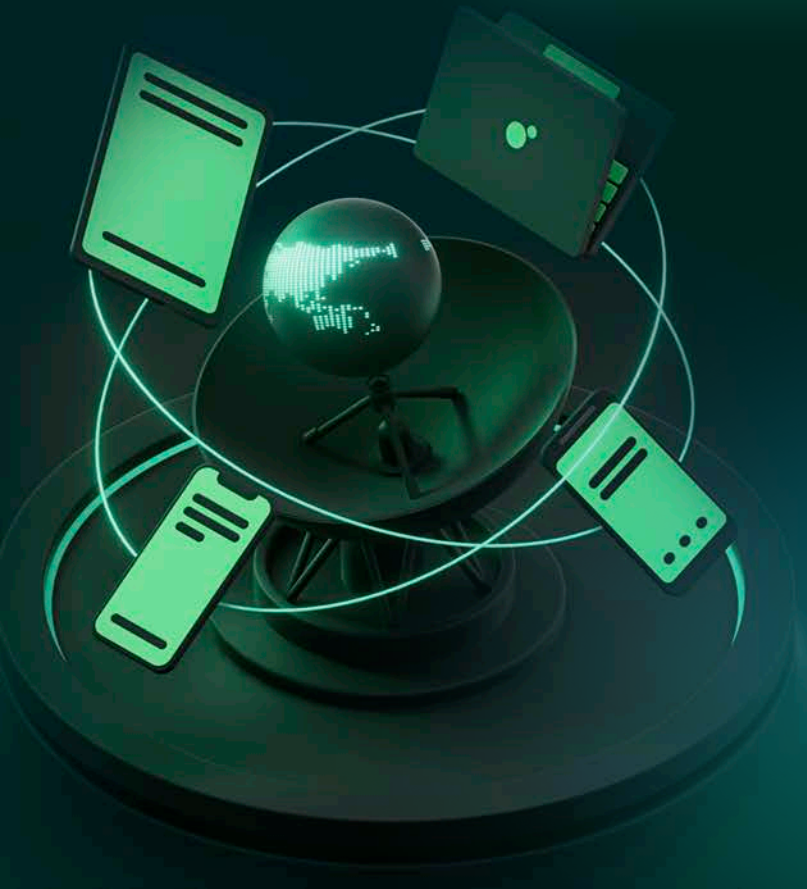
Kaspersky Next EDR Foundations

Liste des fonctionnalités

kaspersky

Sommaire



Qu'est-ce que Kaspersky Next ?

Kaspersky Next est votre nouveau socle de sécurité. La protection en temps réel, la visibilité des menaces et les capacités d'enquête et de réponse EDR et XDR sont assurées par des niveaux progressifs, en fonction de vos besoins et des ressources disponibles. Grâce à cela et aux options de déploiement dans le cloud et sur site, il est facile de choisir votre sécurité et de la développer rapidement et sans problème.

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

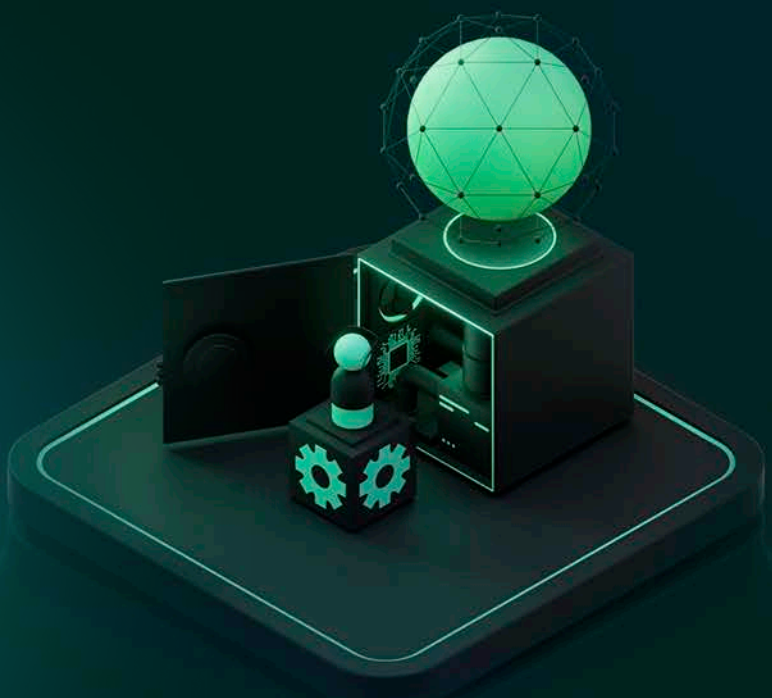
Donnez les moyens à vos experts

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

Qu'est-ce que Kaspersky Next EDR Foundations ?

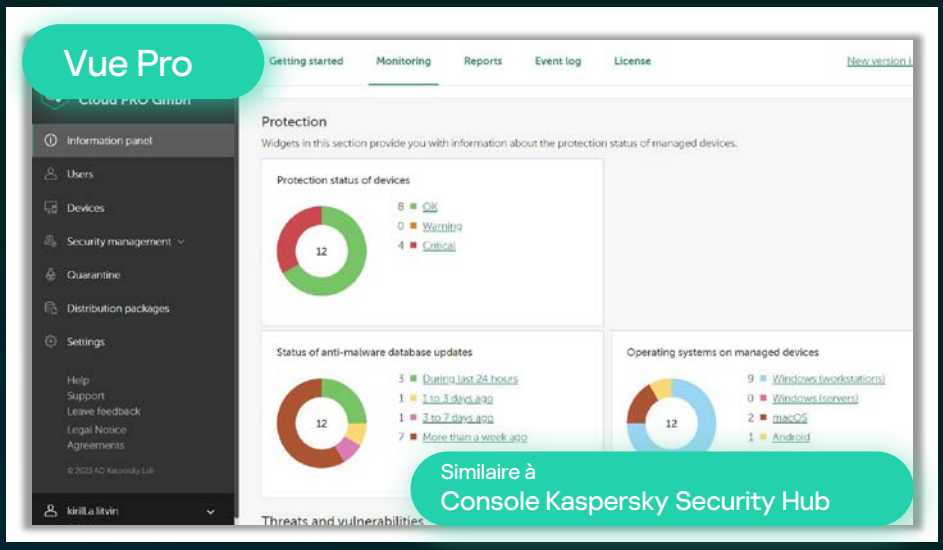
Kaspersky Next EDR Foundations offre une protection simple et abordable pour assurer le bon fonctionnement de votre entreprise. Kaspersky bloque les ransomwares, les programmes malveillants sans fichier, les attaques de type « zero-day » ainsi que les autres menaces émergentes. Grâce à Kaspersky Next EDR Foundations, vous pouvez réaliser une analyse des causes profondes à l'aide d'une chaîne d'exécution visualisée et analyser les détails pour un examen plus approfondi.



Fonctionnalités

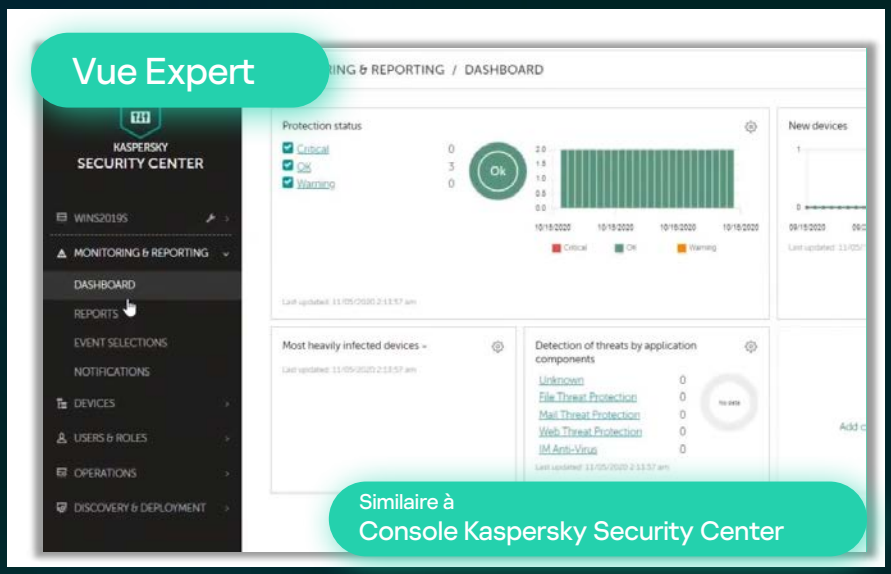
Un mot sur les consoles d'administration

Vous pouvez choisir de gérer votre Kaspersky Next EDR Foundations de différentes manières :



Vue Pro : Une console simplifiée, facile à gérer et hébergée dans le cloud.

Nombre maximum d'hôtes gérés : 2 500



Vue Expert : Une console personnalisable avec des contrôles granulaires, qui offre trois options :

- Basée dans le cloud. Vous ne devez pas installer de serveurs de gestion et votre équipe ne doit pas perdre de temps pour réaliser les mises à jour – tout est hébergé et pris en charge par Kaspersky.
- Nombre minimum d'hôtes gérés : 300
- Sur site, console Internet. Fournit une interface Internet pour la création et la maintenance du système de protection
- Sur site, MMC. Mise en œuvre sous forme de composant logiciel enfichable pour la console d'administration Microsoft (MMC)

Protection des terminaux

Fonctionnalité	Description
Protection multi-niveaux contre les programmes malveillants	Notre dernier moteur de protection contre les programmes malveillants combine une protection basée sur les signatures, une analyse heuristique et comportementale ainsi que des technologies basées sur le Cloud pour protéger vos postes de travail sous Windows contre les menaces connues, inconnues et avancées. Des technologies de détection basées sur la reconnaissance de modèles améliorent les taux de détection et nous aident à réduire la taille des fichiers de mise à jour. Ainsi, vous bénéficiez d'une sécurité fiable qui consomme moins de bande passante.
Détection comportementale	Collecte des informations concernant les actions des applications sur l'ordinateur d'un utilisateur et les fournit à d'autres modules pour assurer une protection plus efficace.
Prévention des exploits	Trace les fichiers exécutables ouverts par les applications vulnérables. En cas de tentative non initiée par l'utilisateur d'exécuter un fichier exécutable à partir d'une application vulnérable, le module bloque l'exécution du fichier.
Moteur d'actions correctives (correction)	Permet d'annuler les actions effectuées par les logiciels malveillants dans le système d'exploitation, offrant ainsi une protection contre les cryptomalwares.
Protection contre les menaces ciblant les fichiers	L'antivirus détecte et élimine les menaces sur un appareil en temps réel en utilisant les bases antivirus de l'application et le service cloud Kaspersky Security Network.
Protection contre les menaces ciblant les emails	Ce module de l'application de sécurité analyse les emails entrants et sortants à la recherche de menaces. Il démarre avec l'application, réside dans la mémoire vive de l'appareil et analyse tous les messages envoyés ou reçus via les protocoles POP3, SMTP, IMAP et NNTP.
Protection contre les cybermenaces	Ce module protège les données entrantes et sortantes envoyées vers et depuis un appareil avec les protocoles HTTP, HTTPS et FTP, et empêche l'exécution de scripts dangereux sur l'appareil.
Pare-feu	Le pare-feu protège chaque terminal contre les menaces réseau lors de la navigation sur Internet ou de l'utilisation d'un réseau local. Il bloque les connexions réseau non autorisées vers l'ordinateur, réduisant ainsi le risque d'infection. Il surveille l'activité réseau des applications sur l'appareil, réduisant le risque de propagation de programmes malveillants sur le réseau. Il restreint également les actions effectuées par les utilisateurs qui ne respectent pas la stratégie de sécurité de l'entreprise (intentionnellement ou non).
Système de prévention des intrusions hébergé sur l'hôte (HIPS)	Le système de prévention des intrusions hébergé sur l'hôte empêche les applications d'effectuer des actions qui peuvent être nuisibles au système d'exploitation et contrôle l'accès aux ressources du système d'exploitation ainsi qu'aux données personnelles.
Protection contre les menaces réseau	Ce module analyse le trafic réseau entrant d'un appareil à la recherche d'activités typiques d'une attaque de réseau, comme l'intrusion d'un appareil distant dans le système d'exploitation. Lorsque la protection contre les menaces réseau détecte une tentative d'attaque réseau sur l'appareil, elle bloque l'activité réseau de l'ordinateur attaquant.
Prévention des attaques BadUSB	Empêche les appareils USB infectés émulant un clavier de se connecter à l'ordinateur. Lorsqu'un appareil USB est connecté à l'ordinateur et identifié comme clavier par le système d'exploitation, l'application invite l'utilisateur à saisir un code numérique généré par l'application. Cette procédure est connue sous le nom d'« autorisation de clavier ».
Protection AMSI	Prend en charge l'interface d'analyse de logiciel anti-programmes malveillants (AMSI) de Microsoft. L'AMSI permet aux applications tierces qui le prennent en charge d'envoyer des objets (comme des scripts PowerShell) à Kaspersky Endpoint Security pour une analyse supplémentaire et d'en recevoir les résultats.
Kaspersky Security Network	Des millions de clients et des milliers d'entreprises consentent à autoriser Kaspersky Security Network (KSN) à recevoir des données anonymes sur les programmes malveillants et les comportements suspects de leurs ordinateurs. Ce flux de données en temps réel nous permet de réagir extrêmement rapidement aux nouveaux programmes malveillants, tout en garantissant un taux inférieur de « faux positifs ».
Défense contre les menaces mobiles	Un ensemble de fonctions de protection des appareils Android et iOS contre les virus et autres programmes malveillants. Voir ci-dessous les détails pour chaque type de système d'exploitation.
Intégration SIEM	Les événements peuvent être exportés vers des systèmes de solutions SIEM tiers qui traitent des questions de sécurité à un niveau organisationnel et technique (c'est-à-dire les SOC). Les protocoles Syslog et CEF/LEEF sont pris en charge. (**Sur site uniquement**)

Gestion de la sécurité

Fonctionnalité	Description
Renforcement de la sécurité des systèmes.	
Évaluation des vulnérabilités	Fournit un aperçu des applications installées sur les appareils de l'entreprise et une liste des correctifs disponibles pour mettre à jour ces applications vers les dernières versions.
Contrôle des applications	Gère le lancement des applications sur les ordinateurs des utilisateurs et réduit le risque d'infection de l'ordinateur en limitant l'accès aux applications. Cette fonctionnalité permet la mise en œuvre de votre stratégie de sécurité d'entreprise pour l'utilisation d'applications.
Contrôle du Web	Permet de contrôler l'accès à Internet en fonction du contenu ou de l'emplacement du site. La liste de refus d'URL empêche les utilisateurs d'accéder à des sites Web indésirables ou potentiellement nuisibles. L'inscription sur la liste n'autorise l'accès qu'à des ressources Internet sûres.
Contrôle des périphériques	Contrôle l'accès aux appareils amovibles et externes connectés à l'ordinateur. Les administrateurs peuvent autoriser ou bloquer l'utilisation de certains appareils par type ou créer une liste d'appareils de confiance.
Gestion des appareils mobiles	Vous pouvez ainsi gérer les appareils mobiles appartenant aux employés de votre organisation afin d'appliquer vos exigences de sécurité de l'entreprise, de contrôler la conformité, de protéger les appareils contre les menaces et d'empêcher la fuite d'informations d'entreprise.

Protection contre les menaces mobiles

Fonctionnalité	Description	Vue Pro	Vue Expert
Android			
Protection antivirus	Détecte et neutralise les menaces sur votre appareil en utilisant les bases antivirus et le service cloud Kaspersky Security Network. Protège l'appareil contre les menaces, les virus et autres applications malveillantes en temps réel, analyse les nouvelles applications et les paquets de distribution dans le dossier Téléchargements. Analyse tous les fichiers ouverts, modifiés, déplacés, copiés, exécutés et enregistrés sur l'appareil par l'utilisateur. Bloque les applications et les programmes publicitaires qui peuvent être utilisés par des malfaiteurs pour endommager l'appareil et les données de l'utilisateur.	✓	✓
Protection des mots de passe	Protège l'accès à l'appareil grâce à un mot de passe de déverrouillage de l'écran.	✓	✓
Prévention des vols	Protège les informations stockées sur l'appareil contre tout accès non autorisé en cas de perte ou de vol de l'appareil. Verrouillez et localisez l'appareil, déclenchez une alarme ou effacez les données à distance.	✓	✓
Contrôle des applications	Gérez les applications sur les appareils des utilisateurs à l'aide d'un ensemble de règles. Vous pouvez configurer deux types de règles dans le Contrôle des applications : Règles par application et règles par catégorie.	✓	✓
Contrôle de la conformité	Vérifie la conformité des paramètres de l'appareil de l'utilisateur avec les exigences de sécurité de l'entreprise. Par exemple, si l'appareil est rooté et que ses bases antivirus sont obsolètes, des mesures de protection peuvent être configurées.	✓	✓
Contrôle du Web	Bloque l'accès aux sites Web dangereux et malveillants. Contrôle l'accès aux sites Internet en fonction de leur contenu et de leur emplacement.	✓	✓
Contrôle des fonctionnalités	Permet d'interdire l'utilisation des modules caméra, Bluetooth et Wi-Fi sur un appareil afin de minimiser le risque de fuite de données sensibles, et de configurer la connexion automatique à un réseau Wi-Fi d'entreprise sur Android.	✓	✓
Contrôle du Wi-Fi	Définit les paramètres du réseau Wi-Fi lorsque l'appareil se connecte à Internet.	✓	✓
Synchronisation et mise à jour des bases de données en itinérance	Permet de synchroniser les appareils avec le Serveur d'administration et de mettre à jour la base de données antivirus lorsque l'on se trouve dans la zone d'itinérance. L'utilisateur peut également les exécuter manuellement à tout moment.	✓	✓

Fonctionnalité	Description	Vue Pro	Vue Expert
Détection d'accès racine	Les fichiers système ne sont pas protégés sur un appareil piraté et peuvent être modifiés. En outre, des applications tierces de sources inconnues peuvent être installées sur les appareils piratés. Lors de la détection d'une tentative de rootage, nous vous recommandons de restaurer immédiatement l'appareil dans son état normal.	✓	✓
Configuration de la messagerie	Permet de configurer la messagerie Exchange pour qu'elle fonctionne avec l'adresse email, les contacts et le calendrier de l'entreprise sur l'appareil mobile.		✓
Prise en charge de KNOX/Exchange ActiveSync (EAS)	L'application Kaspersky Endpoint Security for Android peut être déployée par la console Samsung KNOX Mobile Enrollment. Le protocole Exchange ActiveSync peut être utilisé pour configurer les restrictions des fonctionnalités de l'appareil afin d'assurer la sécurité d'un appareil EAS.		✓
Prise en charge d'Android Work Profile	Permet de configurer un conteneur séparé (en utilisant Android Work Profile) pour vos applications et données d'entreprise		✓
Intégration de l'ICP	Permet d'établir la connexion avec votre autorité de certification Microsoft et de transférer les certificats pour les emails, le VPN et l'authentification Wi-Fi vers les appareils mobiles connectés		✓
iOS			
Contrôle du Web	Contrôle l'accès aux sites Internet en fonction de leur contenu et de leur emplacement. Les paramètres ne sont appliqués qu'aux appareils supervisés.	✓	✓
Protection contre le phishing et les programmes malveillants en ligne	Sécurise l'appareil iOS contre les ressources de phishing et les programmes malveillants auxquels les employés peuvent être confrontés.		✓
Protection des mots de passe	Protège l'accès à l'appareil grâce à un mot de passe de déverrouillage de l'écran.	✓	✓
Paramètres du proxy	Protège le trafic lors de la connexion de l'appareil à Internet grâce à un proxy HTTP global. Les paramètres ne sont appliqués qu'aux appareils supervisés.	✓	✓
Outils de protection antivol	Les fonctionnalités de verrouillage et d'effacement à distance peuvent être appliquées à un appareil volé afin de le protéger contre la perte de données.	✓	✓
Contrôle des fonctionnalités	Restreint l'accès de l'utilisateur aux fonctionnalités natives de l'appareil iOS, notamment le contrôle de l'appareil photo, l'installation d'applications, les captures d'écran, AirDrop, iCloud, etc. Au total, jusqu'à 40 fonctionnalités différentes sont prises en charge. Veuillez noter que certaines fonctionnalités ne peuvent être gérées que pour les appareils supervisés.	✓	✓
Configuration du nom du point d'accès	Configure le nom du point d'accès (APN) lors de la connexion aux services de données d'un réseau mobile.	✓	✓
Configuration AirPrint	Configure AirPrint pour l'impression de documents à partir de l'appareil.	✓	✓
Contrôle du Wi-Fi	Définit les paramètres du réseau Wi-Fi lorsque l'appareil se connecte à Internet.	✓	✓
Configuration de la messagerie	Configure les comptes de messagerie appartenant à l'utilisateur de l'appareil.	✓	✓
Configuration CalDAV	Configure les comptes CalDAV appartenant à l'utilisateur de l'appareil pour gérer le calendrier.	✓	✓
Abonnements au calendrier	Configure l'abonnement à des calendriers tiers pour l'ajout d'événements sur l'appareil.	✓	✓
Détection des déverrouillages	Les fichiers système ne sont pas protégés sur un appareil piraté et peuvent être modifiés. Lors de la détection d'un jailbreak, nous vous recommandons de restaurer immédiatement l'appareil dans son état normal.		✓

Antivirus dans le cloud

Fonctionnalité	Description
Cloud Discovery	Permet de découvrir et de restreindre l'utilisation inappropriée ou non autorisée des ressources cloud, ainsi que le temps perdu sur les réseaux sociaux et les messageries. Surveillez plus de 2 700 services cloud. Chaque service cloud détecté dispose désormais d'une note indiquant le degré de dangerosité lié à son utilisation. L'administrateur informatique peut donc facilement évaluer les risques et décider d'autoriser ou de bloquer un service en particulier.

Fonctionnalités EDR essentielles

Fonctionnalité	Description
Analyse des causes profondes	Un graphique de propagation de la menace présente les processus clés, les connexions réseau, les bibliothèques DLL, les ruches de registre affectés ou impliqués dans l'alerte. Toutes les détections sont mises en évidence sur le graphique, fournissant à l'analyste le contexte complet de l'incident et facilitant le processus de découverte des modules affectés. Le graphique permet d'obtenir des informations complémentaires sur les processus, etc. Disponible sur les appareils Windows, Mac et Linux.

Location multiple

La location multiple est le mode de fonctionnement lorsque la solution est utilisée pour protéger l'infrastructure de plusieurs organisations en même temps. Kaspersky Next EDR Foundations à location multiple aide les fournisseurs de services à offrir une protection gérée des terminaux. La console à location multiple est facile à utiliser et permet de gérer plusieurs clients à l'aide d'un seul compte. Un maximum de 300 utilisateurs peut être réparti dans des espaces de travail indépendants et isolés, avec leurs propres profils de sécurité.

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 : kaspersky.fr/blog/category/business
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security

kaspersky.fr

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 grâce à un bref questionnaire dans notre outil interactif : https://go.kaspersky.com/Kaspersky_Next_Tool