Kaspersky Next
EDR Foundations

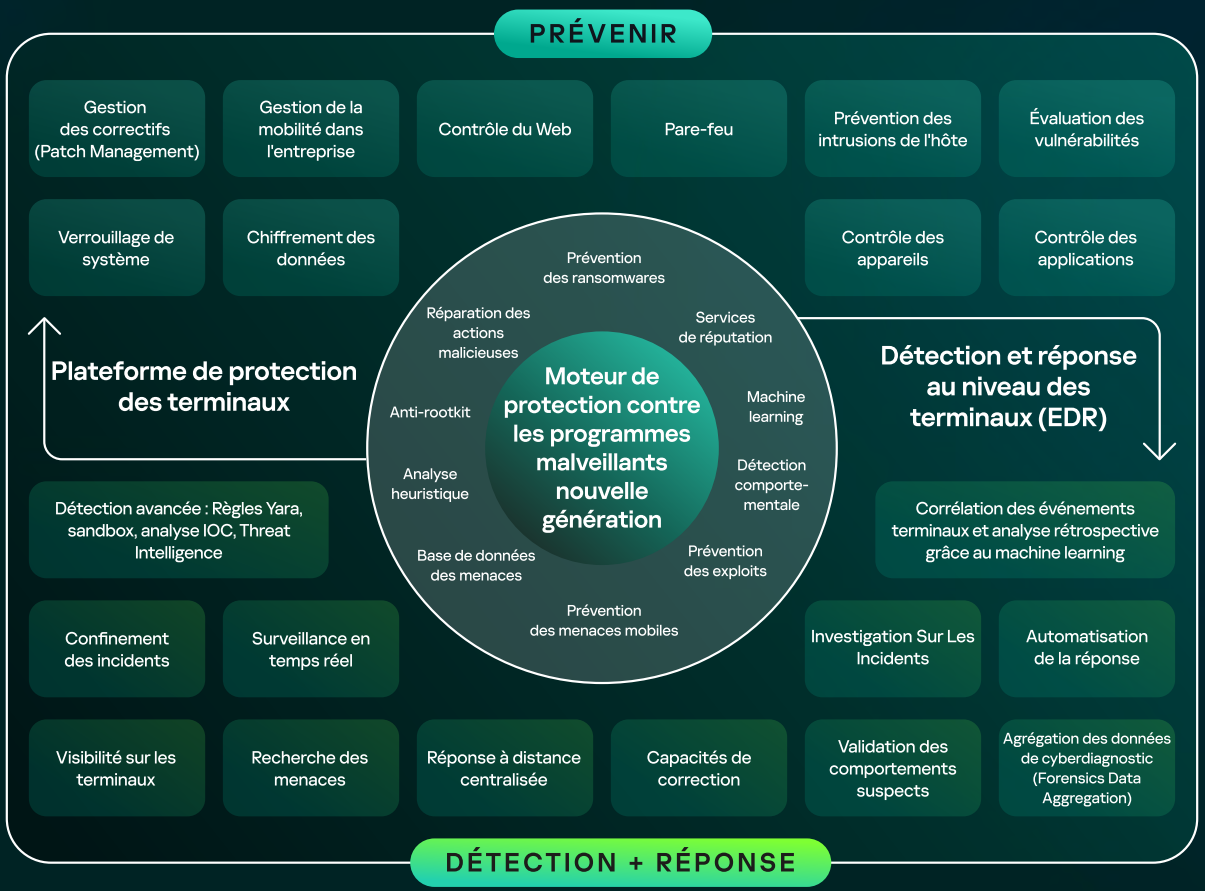
Vous ne le savez peut-être pas encore, mais vous avez déjà besoin de l'EDR

Pourquoi prendre son EPP pour acquis devient un gros problème

Si l'on en croit Mark Twain, « la familiarité engendre le mépris ». Et, si cette citation s'applique généralement à des situations ou à des personnes que vous connaissez particulièrement bien, elle peut tout aussi bien s'appliquer à la cybersécurité. Les plate-formes de protection des terminaux (EPP), par exemple, sont devenues si familières aux équipes informatiques que, pour reprendre une autre expression bien connue, elles font souvent partie des meubles.

Nous ne suggérons en aucun cas que les EPP sont dépassées. En fait, en plus de défendre leur périmètre avec des pare-feu et une protection des emails, la grande majorité des organisations ont concentré leurs efforts sur les terminaux, dont les ordinateurs de bureau, ordinateurs portables, serveurs (physiques et virtuels) et postes de travail, comme défense principale contre les cybermenaces.

Par conséquent, les EPP sont devenus une étape fondamentale dans la lutte contre les attaques complexes. Mais il est tout aussi important de comprendre que la définition d'un EPP évolue elle-même et apporte de nouvelles exigences quant à ce qu'une telle plateforme doit fournir.



Cela s'explique par le nombre croissant de menaces qui contournent les EPP traditionnelles.

Le problème des EPP traditionnels

Regardez à quoi ressemblerait une attaque contre votre entreprise et comment vous réagiriez grâce à notre jeu interactif : kaspersky.com/response-game/fr/

Depuis des années, les petites et moyennes entreprises (PME) et les très petites entreprises peuvent compter sur l'EPP pour se défendre contre une série de menaces courantes. Mais aujourd'hui, les pirates informatiques ciblent des organisations de toutes tailles, de tous secteurs et à tous niveaux de préparation.

Cette évolution du paysage des menaces signifie qu'au fil du temps, des menaces de plus en plus sophistiquées ciblant auparavant uniquement les grandes organisations touchent progressivement les PME et les plus petites entreprises qui ne disposent pas des ressources internes nécessaires pour y répondre efficacement.

L'apparition de menaces évasives en particulier, avec leur recours aux outils légitimes dans les attaques, dont des scénarios prêts à l'emploi pour contourner l'EPP, leur faible coût et leur facilité d'accès sur le Dark Web, a considérablement augmenté les risques de cybersécurité pour les organisations qui optent pour des solutions EPP traditionnelles.

Ces problèmes sont encore aggravés par le manque de transparence des EPP traditionnels. En effet, ces solutions n'offrent qu'une information feu rouge/feu vert indiquant qu'une attaque est ou n'est pas en cours. Or, ce dont a besoin une équipe informatique ayant des compétences de base en matière de sécurité, c'est d'avoir une visibilité sur l'activité des différents terminaux, afin de pouvoir l'analyser plus en détail et mieux comprendre la menace.

Sans la fonctionnalité EDR, l'EPP classique ne permet pas techniquement une visibilité approfondie des terminaux, une analyse rétrospective et multi-terminaux des attaques et une corrélation des événements, ni la possibilité de choisir parmi plusieurs détections d'événements pertinents pour des attaques complexes afin de déterminer la réponse appropriée. Toutes les solutions EPP disponibles sur le marché ne permettent pas d'accéder aux renseignements sur les menaces nécessaires pour comprendre les principales tactiques, procédures et techniques d'une menace.

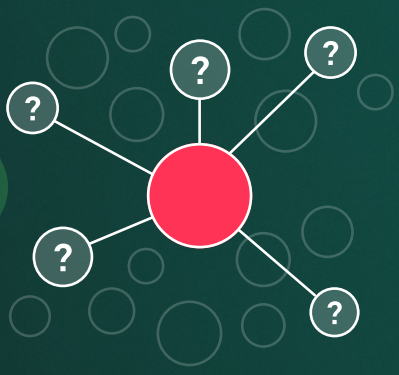
Terminaux multiples et détection d'événements différents

Récolte des données pertinentes pour l'enquête

Machine Learning

- Analyse des attaques multi-terminaux
- Analyse rétrospective
- Mise en corrélation des événements

De la corrélation des événements à la réponse pertinente aux incidents



Visualisation orientée vers l'humain et analyse approfondie

Comment savoir s'il est temps de renforcer vos défenses ?

Obtenez une recommandation personnalisée et choisissez le niveau de Kaspersky Next le plus adapté à vos besoins : go.kaspersky.com/Kaspersky_Next_Tool

Comment savoir si votre EPP ne répond plus à vos besoins ?

Voici les signes avant-coureurs indiquant qu'il est temps de renforcer vos défenses au-delà de la solution EPP traditionnelle :

- Votre EPP ne parvient pas à bloquer un nombre croissant de menaces nouvelles, inconnues et évasives.
- Vous disposez d'une visibilité limitée sur ce qui se passe au niveau de vos terminaux. Cela inclut l'incapacité de réaliser une analyse des causes profondes, une enquête et une réponse en temps réel aux menaces, ou l'obligation de devoir le faire manuellement au moyen d'outils de systèmes d'exploitation (OS) standard au cas par cas. Un processus long, complexe et source d'erreurs.
- Vous ne disposez pas des compétences ou capacités spécialisées en sécurité informatique nécessaires pour gérer des menaces toujours plus sophistiquées.
- Les amendes potentielles ou les atteintes à la réputation de votre entreprise résultant d'un incident de sécurité majeur vous inquiètent.

Si vous rencontrez certains de ces problèmes, une solution EPP moderne peut non seulement vous aider à les résoudre, mais aussi servir de tremplin entre une solution EPP traditionnelle et des solutions de détection et de réponse au niveau des terminaux (EDR) et de détection et réponse étendue (XDR) complètes grâce à de simples fonctionnalités EDR, de quoi dépoussiérer vos meubles.

Comment Kaspersky peut vous aider

Avec seulement trois niveaux de produits, Kaspersky Next sécurise l'ensemble de l'infrastructure d'une entreprise en combinant une protection et des contrôles exceptionnels des terminaux (EPP) avec la transparence et la rapidité de l'EDR, ainsi que la vision complète et la puissance du XDR. Les entreprises peuvent donc choisir les outils utiles dans l'immédiat, puis les mettre à niveau lorsque leurs besoins de protection évoluent.

Notre niveau de base, Kaspersky Next EDR Foundations, offre une protection puissante des terminaux grâce au machine learning, des contrôles de sécurité flexibles et une analyse EDR des causes profondes, ce qui permet aux entreprises de construire leur cybersécurité sur une base solide le plus facilement possible. Une console simple, un déploiement dans le cloud ou sur site, et diverses fonctionnalités favorisant la qualité de vie au travail réduisent la complexité et augmentent l'efficacité.

Et si vous utilisez déjà une solution de sécurité Kaspersky ?

Votre solution Kaspersky	Migration recommandée	Capacités supplémentaires
Kaspersky Endpoint Security Cloud	Kaspersky Next EDR Foundations	• Prévention des attaques BadUSB • Contrôle des applications, du Web et des appareils • Analyse des causes profondes
Kaspersky Endpoint Security Cloud Plus	Kaspersky Next EDR Foundations	• Prévention des attaques BadUSB • Contrôle des applications
Kaspersky Endpoint Security for Business Select	Kaspersky Next EDR Foundations	• Console dans le cloud simple d'utilisation • Analyse des causes profondes • Cloud Discovery

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.com/enterprise

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