kaspersky bring on the future

Comment protéger les entreprises contre les cyberattaques complexes

Vous êtes-vous déjà retrouvé éveillé la nuit, inquiet à l'idée qu'une cybermenace avancée puisse se cacher dans votre infrastructure, attendant le moment propice pour dérober votre propriété intellectuelle ou prendre votre entreprise ou votre activité en otage contre rançon ?

Si c'est le cas, c'est tout à fait compréhensible. Comme leur nom l'indique, les menaces persistantes avancées (APT) utilisent des techniques de piratage élaborées pour accéder à vos systèmes. Une fois que les cybercriminels ont franchi vos défenses, ils sont capables de rester invisibles pendant des mois, voire des années, d'obtenir des privilèges d'accès plus élevés, de récolter et d'exfiltrer vos données, ce qui peut avoir des conséquences dévastatrices.

Qui sont les cibles ?

Sans grande surprise, il faut beaucoup de compétences, d'efforts et de ressources pour monter une APT ou une attaque ciblée, ce qui explique que leurs cibles privilégiées soient souvent des gouvernements ou de grandes entreprises détenant des données confidentielles ou exclusives qui justifient l'investissement.

Néanmoins, les APT sont une méthode d'attaque que les entreprises devraient surveiller de près, y compris les PME, qui peuvent elles aussi être ciblées.

Les auteurs d'attaques APT visent, par exemple, de plus en plus les petites entreprises qui se trouvent dans les chaînes d'approvisionnement de leurs cibles ultimes. Comme ces entreprises sont généralement moins bien protégées, elles peuvent servir de tremplin pour accéder aux grandes organisations avec lesquelles elles collaborent.

Par conséquent, que vous soyez à la tête d'une grande entreprise ou d'une PME susceptible d'être exploitée pour cibler une organisation plus importante, il est important de **comprendre la nature des menaces** auxquelles vous pourriez être confronté. Cela inclut les APT et autres attaques ciblées, ainsi que les capacités requises pour s'en défendre.

Tous les secteurs sont ciblés

Au cours des deux dernières années, des attaques ciblées d'origine humaine ont été observées dans tous les secteurs. En 2024, les secteurs informatique et gouvernemental sont arrivés en tête avec 14,7 % et 13,8 % respectivement.

Source : Rapport d'analyse Kaspersky Managed Detection and Response 2024

4.88 millions de dollars

Le coût moyen mondial d'une violation des données en 2024, soit une augmentation de 10 % par rapport à 2023 et le montant total le plus élevé jamais enregistré. Dans la région du Moyen-Orient, cet indicateur est nettement plus élevé, atteignant 8,75 millions de dollars.

Source : Rapport d'IBM sur le coût d'une violation de données 2024

258 jours

Le temps d'identifier et de contenir une violation. Cette période de récupération prolongée ne fait pas qu'aggraver les pertes financières, elle rend également les organisations vulnérables à de nouvelles attaques.

Source : Rapport d'IBM sur le coût d'une violation de données 2024

Comment fonctionnent les APT ?

Tout l'intérêt d'une APT est d'obtenir un accès persistant ou continu aux systèmes informatiques et/ou OT (technologie opérationnelle) de la cible, ce que les pirates informatiques parviennent généralement à faire en suivant un processus en cinq étapes.

Schéma 1 : Les étapes d'une APT en pleine évolution

Phase 1

Obtenir l'accès

Comme un cambrioleur qui force une porte avec un pied-de-biche, les cybercriminels commencent souvent par utiliser un « pied-de-biche numérique », comme un fichier infecté, un email de spam ou de phishing, ou une vulnérabilité d'application, pour insérer des programmes malveillants dans le réseau cible.

Phase 2

S'implanter

Ils implantent ensuite des programmes malveillants qui leur permettent de créer des portes dérobées et des tunnels dont ils se servent pour se déplacer dans les systèmes sans se faire repérer.

Phase 3

Élargir l'accès

Une fois introduits dans le réseau, les pirates informatiques utilisent des techniques comme le piratage de mots de passe pour s'approprier les privilèges des administrateurs, ce qui leur permet de contrôler une plus grande partie du système et d'obtenir des niveaux d'accès supérieurs.

Phase 4

Se déplacer latéralement

Installés plus profondément dans le système et disposant des mêmes privilèges que l'administrateur du réseau, ils peuvent se déplacer à leur guise. Ils peuvent alors accéder à différents serveurs et à d'autres parties sécurisées du réseau.

Phase 5

Observer, apprendre et rester

En s'introduisant plus profondément dans votre système, les cybercriminels peuvent comprendre parfaitement le fonctionnement de l'environnement et ses vulnérabilités, ce qui leur permet de récolter les informations qu'ils souhaitent à leur guise. Ils peuvent également tenter de maintenir ce processus en place, parfois indéfiniment, ou se retirer une fois leurs objectifs atteints.

Quelles sont les conséquences potentielles de subir une attaque APT ?

Il suffit de lire la couverture médiatique de toute organisation confrontée à une attaque ciblée pour se rendre compte que les effets peuvent être à la fois importants et durables. Si les conséquences immédiates comprennent généralement un préjudice financier causé par la perte de données et l'interruption des activités, les effets à plus long terme peuvent se traduire par une atteinte à la réputation de l'organisation et à la confiance des clients ainsi que par d'éventuelles poursuites judiciaires.

À cela s'ajoute bien sûr la question de la réparation des dommages causés à l'infrastructure informatique de l'organisation, qui prend souvent des mois, voire des années. En outre, selon le secteur d'activité dans lequel vous opérez, il peut y avoir des conséquences liées à ce secteur.

Schéma 2: Comprendre l'impact des APT sur la sécurité des entreprises

Finance

- Perturbation des services critiques
- Transactions non autorisées
- Attaques de retrait d'argent
- Conséquences juridiques de l'usurpation d'identité

Gouvernement

- Conséquences potentielles du cyberespionnage
- Dommages aux infrastructures critiques
- Perturbation des services d'administration en ligne
- Exposition des données personnelles des citoyens

Commerce en ligne

- Implications juridiques du détournement de compte par usurpation d'identité
- Transactions frauduleuses
- Impossibilité d'accéder aux services informatiques, pertes de revenus
- Amendes potentielles en vertu du RGPD, de la norme PCI DSS, etc.

Transport

- Perturbations et arrêts d'exploitation
- Retards dans la chaîne d'approvisionnement et augmentation des coûts
- Menace de mort
- Dommages aux infrastructures critiques

Alimentation

- Ruptures de stock et arrêts de production
- Risques de dégradation de la qualité des aliments
- Contamination possible par des produits chimiques, des toxines, etc.
- Besoin de recourir à des procédures manuelles

Soins de santé

- Perturbation des services critiques
- Exposition des données personnelles de patients
- Perte de confiance du public
- Risque vital potentiel

IT et télécommunications

- Perte de clients
- Perte de ventes
- Temps d'arrêt imprévu du réseau
- Interruption des services fixes et mobiles

Industrie

- Catastrophes environnementales
- Perturbation opérationnelle
- Augmentation des temps d'arrêt non planifiés
- Défaillances en cascade ou pannes générales du système

Plus de 2

Des incidents graves se produisent chaque jour.

43 %

de tous les incidents graves détectés par Kaspersky en 2024 sont des attaques ciblées d'origine humaine (APT).

Source : Rapport d'analyse Kaspersky Managed Detection and Response 2024

Quelles sont les conséquences en matière de cybersécurité ?

L'un des principaux dangers des APT et d'autres attaques ciblées est que, même lorsque ces opérations ont été découvertes et que la menace immédiate semble avoir disparu, les pirates peuvent avoir laissé de multiples portes dérobées, leur permettant de refaire surface lorsqu'ils le souhaitent.

Un autre problème est que de nombreuses cyberdéfenses traditionnelles, comme les antivirus et les pare-feu, ne suffisent généralement pas à prévenir de telles attaques.

Le bref résumé ci-dessus des étapes nécessaires à la mise en place d'une APT ou d'une attaque ciblée indique clairement que la défense contre ces menaces requiert une approche à plusieurs niveaux, intégrant des solutions capables de protéger les terminaux, les réseaux, le cloud, la messagerie électronique, l'accès à Internet et bien plus.

Cela permettra non seulement de prévenir et de réduire le risque d'attaques complexes, mais aussi de minimiser les perturbations et les coûts liés à ce type d'incidents s'ils se produisent.

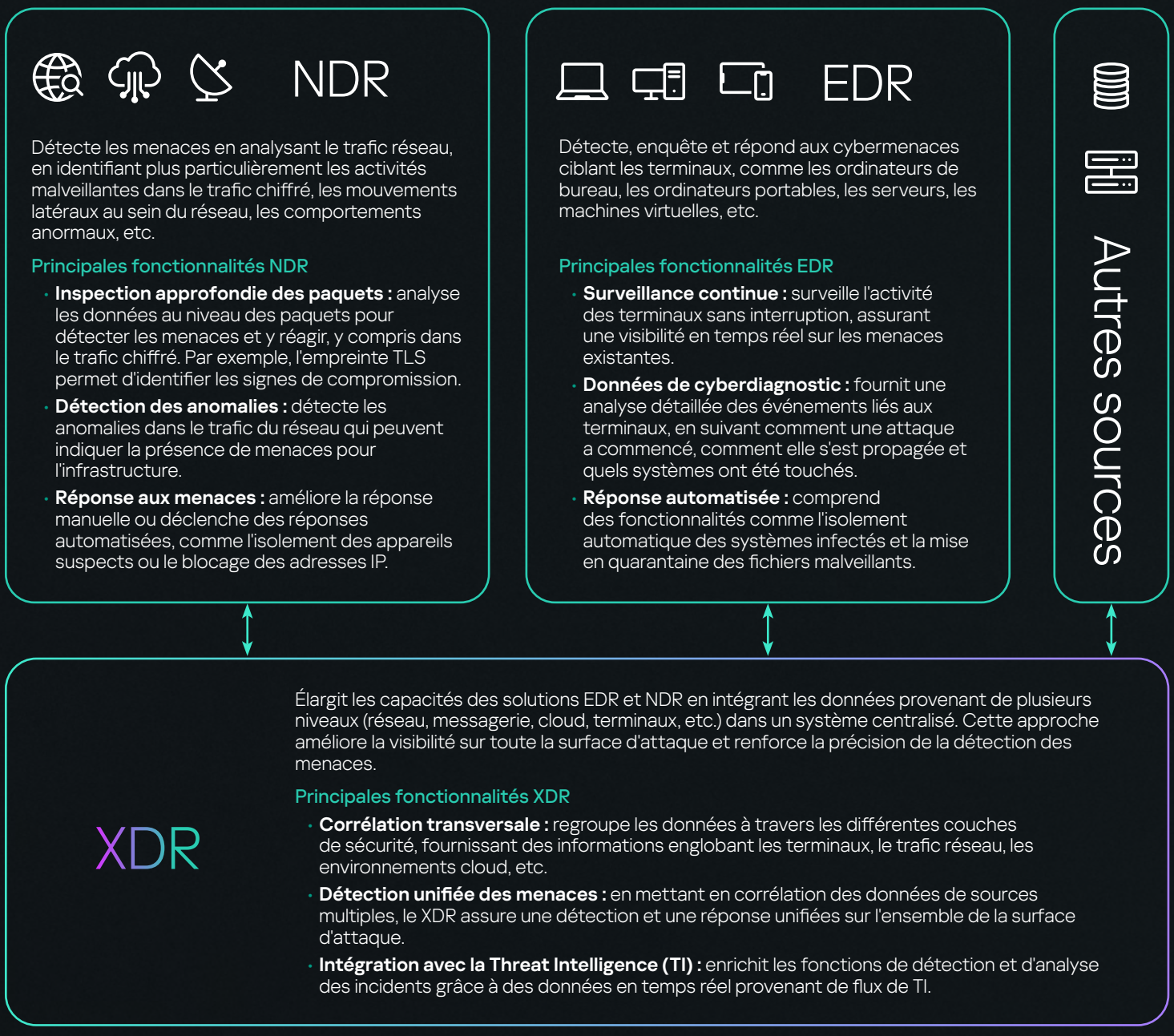
Quels types de solutions cela implique-t-il et comment devriez-vous les déployer ?

Comment protéger les entreprises contre les cyberattaques complexes

Bien qu'une plateforme de protection des terminaux (EPP) ne permette pas à elle seule de se protéger contre des attaques ciblées, elle apportera une source indispensable de données à utiliser dans l'analyse d'attaques nouvelles, en cours ou passées. Par conséquent, ce type de plateforme doit être utilisé dans le cadre d'un ensemble d'autres solutions :

- Endpoint detection and response (EDR) : assure la protection et la visibilité des terminaux au niveau des appareils, détecte les menaces pesant sur les postes de travail, les serveurs, etc., et y répond.
- Network detection and response (NDR) : surveille et analyse le trafic du réseau, détecte les anomalies et répond aux menaces existantes sur le réseau.
- Extended detection and response (XDR) : intègre l'EDR, le NDR et d'autres couches de sécurité pour améliorer la visibilité et automatiser la réponse aux menaces.

Schéma 3 : EDR, NDR, XDR : comment ça marche ?



En 2024, le délai moyen d'enquête et de signalement des incidents de haute gravité a augmenté de 48 %, ce qui indique une hausse de la complexité moyenne des attaques par rapport à 2023. Ce constat est corroboré par le fait que la grande majorité des règles de détection et des entrées-sorties déclenchées l'ont été par des outils XDR spécialisés, et non par les journaux du système d'exploitation comme les années précédentes.

Source : Rapport d'analyse Kaspersky Managed Detection and Response 2024

Quelle(s) solution(s) choisir ?

Le choix de la ou des bonnes solutions dépend des besoins particuliers de votre organisation, de son infrastructure et du paysage des menaces :

- Choisissez l'EDR si les outils traditionnels de protection des terminaux ne suffisent plus et si vous avez besoin d'une protection plus avancée contre les cybermenaces (comme les programmes malveillants, les ransomwares, le phishing et autres) ciblant les terminaux.
- Choisissez le NDR si les menaces basées sur le réseau sont votre principale préoccupation et si vous avez besoin de capacités avancées pour analyser les anomalies du trafic réseau et y répondre.
- Choisissez le XDR si vous recherchez une protection complète sur plusieurs vecteurs et la possibilité de corréler les menaces sur l'ensemble de votre infrastructure informatique.
- Mieux encore, combinez l'EDR, le NDR et le XDR en un seul écosystème de sécurité pour assurer une défense complète contre un large éventail de cybermenaces évasives et avancées.

Schéma 4 : EDR, NDR, XDR : pour qui ?

Solution de cybersécurité	Quelle est l'organisation la mieux adaptée ?
EDR	• Les organisations qui accordent la priorité à la protection des terminaux et qui ont besoin d'informations en temps réel sur l'activité des terminaux. • Les organisations disposant de nombreux terminaux distribués, comme les institutions financières ou les prestataires de soins de santé, qui tireront un grand profit de la capacité de l'EDR à détecter les menaces basées sur les terminaux et à y répondre en temps réel.
NDR	• Les organisations qui dépendent fortement du trafic réseau et qui ont besoin de capacités avancées pour détecter les menaces basées sur le réseau. • Les entreprises disposant d'une équipe dédiée à la sécurité informatique ou les entreprises fortement réglementées, comme les centres de données, les fournisseurs de services ou les agences gouvernementales, peuvent tirer profit de la capacité du NDR à détecter les menaces basées sur le réseau et à y répondre.
XDR	• Les organisations qui ont besoin d'une plateforme de sécurité unifiée dotée de capacités complètes de détection et de réponse aux menaces dans l'ensemble de leur infrastructure informatique. • Les grandes organisations dotées d'environnements informatiques complexes qui ont besoin d'une approche globale de la sécurité. Par exemple, une entreprise multinationale disposant de centres de données sur site et d'environnements cloud gagnerait à utiliser le système XDR pour assurer une détection unifiée des menaces sur plusieurs plateformes, tout en réduisant la complexité opérationnelle par la centralisation de la réponse aux incidents.

Kaspersky Anti Targeted Attack

Comment Kaspersky peut vous aider

Kaspersky Anti Targeted Attack (KATA) offre une protection anti-APT complète contre les cybermenaces complexes. La solution aide les organisations à :

- Détecter et analyser rapidement les attaques ciblées, et y répondre efficacement.
- Assurer une protection des messageries sur tous les principaux points d'entrée des attaques, y compris les réseaux, les emails, le Web et les terminaux.
- Protéger les ressources critiques.
- Assurer la conformité avec les réglementations des différents secteurs d'activités.

Tout cela est possible grâce aux puissantes technologies NDR et EDR disponibles dans les trois versions de Kaspersky Anti Targeted Attack.

Les trois niveaux de KATA offrent une protection contre les menaces persistantes avancées (APT) allant du NDR essentiel et avancé au XDR natif.

- KATA : solution NDR essentielle qui offre des fonctions de base pour détecter les cybermenaces et y répondre.
- KATA NDR Enhanced : s'appuie sur les fonctionnalités fondamentales du module KATA et offre des capacités NDR avancées.
- KATA Ultra : associe les capacités NDR et EDR pour offrir une fonctionnalité XDR native. Ce service sécurise plusieurs points d'entrée des menaces, notamment les réseaux, le Web, la messagerie électronique, les terminaux, les serveurs et les machines virtuelles.

Schéma 5 : Kaspersky Anti Targeted Attack. Un choix flexible.

Critères de comparaison	KATA	KATA NDR Enhanced	KATA Ultra
Description	Essential NDR	NDR avancé	NDR+EDR (XDR natif)
Fonctionnalité NDR essentielle	•	•	•
Sandboxing avancé	•	•	•
Kaspersky Threat Intelligence et enrichissement MITRE ATT&CK	•	•	•
Fonctionnalité NDR		•	•
Fonctionnalités EDR Expert			•
Fonctionnalités XDR native			•

Choisissez une fonctionnalité NDR essentielle ou avancée, ou optez pour la solution combinée NDR et EDR pour les scénarios XDR natifs, afin de vous protéger contre les cybermenaces les plus complexes, le tout sur une plateforme unique. Avec le niveau KATA Ultra, vous profitez d'une protection APT complète, tout-en-un, et d'une visibilité sur l'ensemble de votre infrastructure informatique.

Pourquoi choisir Kaspersky Anti Targeted Attack

Visibilité totale de votre infrastructure informatique

Fournit un ensemble complet de technologies uniques pour éliminer les zones d'ombre et contrôler tous les points d'entrée des menaces possibles, y compris le réseau, le Web, les terminaux et la messagerie, le tout au sein d'une seule plateforme unifiée.

Une protection renforcée par une Threat Intelligence mondiale

Enrichit l'analyse des menaces et la réponse grâce à un accès direct à la base de données de réputation mondiale de Kaspersky Private Security Network, à Kaspersky Threat Intelligence et au mappage avec le cadre MITRE ATT&CK.

Technologies testées et éprouvées de manière indépendante

Utilise des technologies innovantes pour la détection avancée des menaces par ML, les enquêtes approfondies et la réponse rapide aux incidents, ce qui est reconnu par les principales agences d'analyse et apprécié par des clients importants à l'échelle mondiale.

Kaspersky Anti Targeted Attack

En savoir plus

Présentation vidéo de Kaspersky Anti Targeted Attack

Visionner maintenant

Les prévisions en matière de menaces avancées

Lire maintenant

www.kaspersky.fr