EDR, le guide de l'acheteur

kaspersky BRING ON THE FUTURE

www.kaspersky.fr
#truecybersecurity

Sommaire

Introduction

La garantie d'une disponibilité permanente de données et systèmes fiables à des fins de prise de décision constitue l'un des objectifs majeurs de toute entreprise. L'évolution constante des menaces a concentré l'attention des directeurs d'entreprise sur la cybersécurité. Les équipes en charge des opérations et de la sécurité informatiques doivent adopter une approche complète et cohérente face aux incidents de sécurité et aux violations de données.

La cybersécurité fait désormais partie des trois principales priorités des cadres dirigeants qui considèrent la continuité de l'activité comme un gage de réussite.

Les dirigeants d'entreprise se doivent aujourd'hui de comprendre les menaces spécifiques auxquels leurs sociétés sont confrontées. Dans cette optique, ils doivent se poser les questions suivantes :

- Disposons-nous, au sein de mon entreprise, d'informations suffisantes sur les menaces et risques de sécurité majeurs qui nous affectent et touchent l'ensemble du secteur ?
- Sommes-nous capables de détecter et déjouer rapidement les cyberattaques ?
- Quelle place accordons-nous à la réduction des cyberincidents dans notre stratégie globale de développement commercial ?

Les terminaux en première ligne

Terminaux d'entreprise : vos serveurs, postes de travail, téléphones mobiles et autres équipements sont la source de la synergie entre les données, utilisateurs et systèmes professionnels permettant de générer et de mettre en œuvre les processus métier. Cette multitude d'appareils individuels reste au cœur de tout réseau, tant d'un point de vue commercial que sécuritaire.

Pour protéger ces terminaux, et donc éviter leur utilisation en tant que points d'entrée illégitimes dans votre infrastructure, vos équipes de sécurité de l'information doivent envisager d'adopter des technologies et processus associés à la détection avancée et à la recherche des menaces, au balayage des indicateurs de compromission (IoC), à l'analyse des programmes malveillants, au cyberdiagnostic des incidents, à la mise en œuvre de la Threat Intelligence à l'échelle mondiale et au déploiement d'un processus formel de réponse aux incidents.

Au milieu de tout cela, une question demeure : par où commencer ? Prendre en marche le train du machine learning avancé ? Améliorer vos méthodes de recherche des menaces ? Développer votre surveillance et votre SOC ? Vous pouvez relever tous ces défis, et bien d'autres encore, en adoptant une solution de détection et réponse aux incidents pour les terminaux (EDR, Endpoint Detection and Response) moderne. Que pouvez-vous exactement attendre de ces solutions EDR, et comment les choisir ?

Ce document peut vous aider à choisir la solution EDR la plus adaptée à vos besoins. Notre objectif est de mettre en évidence les principales différences entre les nombreux types de fonctionnalités EDR disponibles sur le marché et de vous aider à identifier les technologies contribuant le plus à la continuité de l'activité et à la sécurité de votre entreprise.

Tout savoir sur le Endpoint Detection and Response

Une nouvelle approche de la sécurité des terminaux

Pour empêcher les attaques, protégez votre périmètre. Il a toujours semblé logique de supposer qu'une fois que le périmètre informatique est suffisamment protégé, il suffit d'étendre la stratégie de sécurité globale aux terminaux.

Cette approche s'avère toutefois insuffisante à l'heure où des technologies telles que les appareils mobiles, les objets connectés (IoT) et le Cloud computing compliquent considérablement la délimitation, et à plus forte raison la défense, d'un périmètre informatique, sans oublier l'évolution des menaces qui a rendu caduque toute approche basée sur un périmètre défensif.

Les attaques ciblées, l'augmentation notable du nombre de techniques de pénétration complexes et de programmes malveillants sans fichier, l'utilisation de logiciels légitimes, les vols d'informations d'identification d'utilisateurs ordinaires, le détournement d'autorisations légitimes, l'exploitation des problèmes inhérents aux stratégies de sécurité et les mauvaises configurations sont autant d'enjeux qui ont poussé les entreprises à reconnaître l'importance des stratégies et solutions de sécurité intégrées. Cette prise de conscience s'est alors traduite par le développement des systèmes de gestion des informations et des événements de sécurité (SIEM, Security Information and Event Management) ainsi que des centres opérationnels de sécurité (SOC, Security Operational Center). Par la force des choses, la cybersécurité d'entreprise est devenue proactive, multifacette et hautement spécialisée.

Le monde évolue, et s'apprête déjà à accueillir un nouveau paradigme de sécurité des terminaux. Les terminaux sont redevenus une priorité. Certains départements informatiques prévoyants estiment déjà depuis longtemps que chaque terminal exige son propre périmètre de sécurité. En outre, en partie à cause des entreprises qui n'ont **pas** su adopter cette approche, et dont la mauvaise visibilité sur les appareils a entraîné un nivellement par le bas de la sécurité globale, les terminaux n'ont jamais cessé d'être une cible privilégiée pour les cybercriminels.

Faire preuve d'une plus grande proactivité

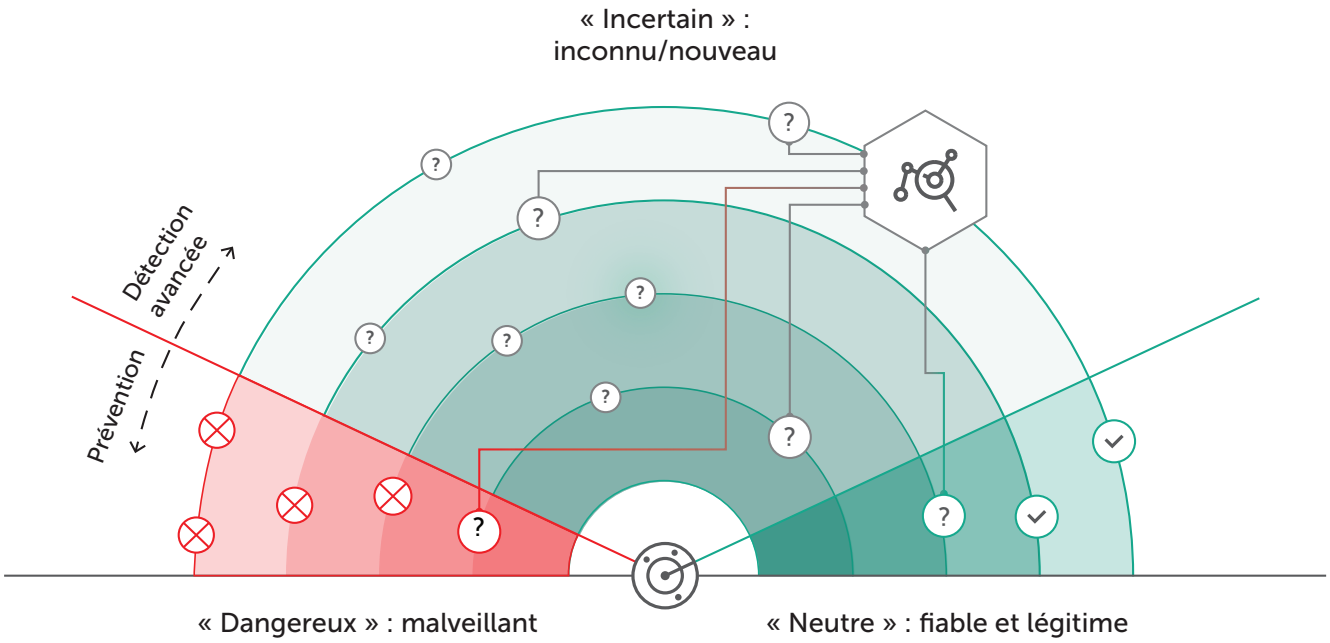
En parallèle, les organismes de réglementation imposent de nouvelles exigences (parmi lesquelles les normes RGPD et PCI DSS), dont certaines exigent une surveillance et un enregistrement continus des incidents sur tous les terminaux d'un réseau. Puisque le nombre d'événements/incidents enregistrés par les solutions actuelles de la plupart des entreprises n'a de cesse d'augmenter, la vérification et l'analyse de chaque événement enregistré deviennent problématiques. La raréfaction des experts de sécurité disposant de compétences d'ingénierie inversée, d'analyse des programmes malveillants, de cyberdiagnostic et de réponse aux incidents nécessaires pour accomplir ces tâches n'arrange pas les choses.

Pour le moment, la plupart des processus de sécurité axés sur les menaces avancées et des approches de surveillance des SOC se fondent sur un système d'émission d'alertes et de réponse à celles-ci. Les agents de sécurité attendent qu'une violation soit avérée pour alerter l'analyste de sécurité, afin que l'équipe de réponse aux incidents puisse enfin intervenir. Dans le meilleur des cas, les responsables de la réponse aux incidents identifient les artefacts d'une attaque au dernier stade de la chaîne de frappe. Dans le pire des cas, ils se contentent de constater les dégâts, parfois plusieurs mois après l'intrusion dans les systèmes. Cette façon de procéder est clairement inadaptée. C'est pourquoi les entreprises réévaluent leurs processus de sécurité, notamment en matière de détection proactive et de résolution des incidents.

Quelles sont les répercussions sur les solutions dédiées aux terminaux ?

La recherche des menaces contribue à déceler les menaces avancées qui se dissimulent au sein de l'entreprise à l'aide de fonctionnalités de recherche proactive appliquées par des professionnels hautement expérimentés et qualifiés.

Les solutions dédiées aux terminaux de dernière génération se focalisent sur la détection efficace des nouvelles menaces ciblant les entreprises, ainsi que sur les patrouilles et les analyses d'événements dans la « zone grise », où des menaces inconnues et indéfinies peuvent se tapir. On parle alors de « recherche proactive des menaces ».



Au-delà de la protection des terminaux

L'efficacité de la recherche des menaces dépend directement des capacités d'un SOC bien en place. La mise à niveau des solutions de sécurité existantes ne suffit pas. Il n'est pas viable de se contenter d'imposer de nouvelles exigences aux solutions de protection des terminaux (EPP, Endpoint Protection) traditionnelles : celles-ci ne s'intégreraient ou ne fonctionneraient pas efficacement.

Examinons certaines problématiques clés résolues efficacement par les solutions EPP traditionnelles, ainsi que les nouveaux défis qui pèsent actuellement sur la sécurité des terminaux :

Problèmes de contrôle et de protection résolus par les solutions EPP traditionnelles :	Nouveaux défis avancés associés à la sécurité des terminaux :
Comment assurer une protection automatique (à la fois prédictive et réactive) contre les menaces existantes, incluant des ransomwares et des cryptovirus	Comment rechercher des preuves d'intrusion, dont des indicateurs de compromission (IoC), en temps réel et sur la totalité du réseau
Comment gérer de manière centralisée et appliquer des contrôles de sécurité pour le Web / les applications / les appareils	Comment détecter et bloquer une intrusion avant qu'elle ne cause d'importants dommages
Comment administrer de manière centralisée l'évaluation des vulnérabilités et les processus de gestion des correctifs	Comment mettre en corrélation les alertes émises par les contrôles de sécurité du réseau afin de visionner en temps réel les activités survenant sur le terminal
Comment protéger les informations et données professionnelles sur les appareils	Comment valider les alertes et incidents potentiels décelés par les solutions de sécurité
Comment déployer des stratégies de protection sur le Web et des e-mails au niveau des terminaux	Comment examiner rapidement et gérer de manière centralisée les incidents sur plusieurs milliers de terminaux
Comment fournir aux utilisateurs de terminaux des ensembles de domaines de sécurité spécifiques adaptés à leurs besoins	Comment réduire les coûts associés aux processus de réponse aux incidents (tâches manuelles, compétences de niveau 3, surcharge d'alertes, etc.) en automatisant les opérations de routine de l'équipe de sécurité

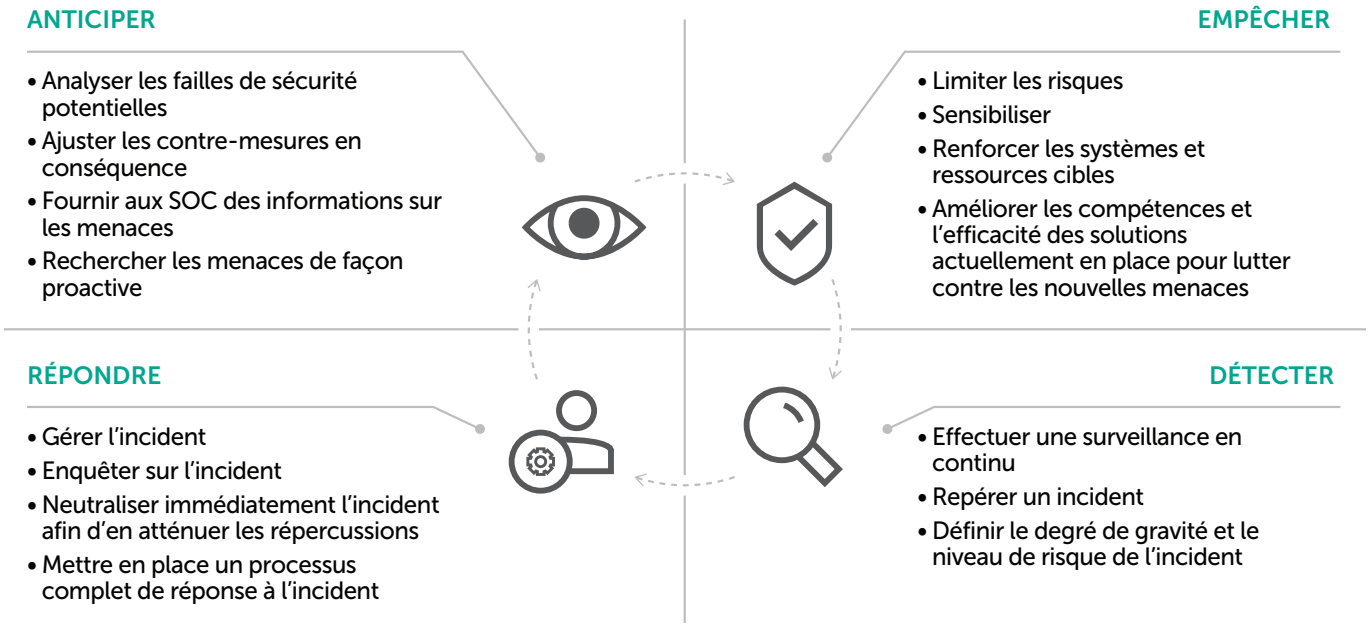
Comment relever ces nouveaux défis ?

Votre stratégie de cybersécurité des terminaux : adaptable, avancée et prédictive

Plus difficiles à détecter et souvent plus compliquées à éliminer, les attaques ciblées et les menaces avancées requièrent une stratégie de sécurité exhaustive et adaptable.

L'un des cadres de sécurité évolutifs les plus efficaces repose sur l'architecture de sécurité viable telle que décrite par Gartner. Cette approche consiste à proposer un cycle d'activités dans quatre domaines principaux : Empêcher, Détecter, Répondre et Prévoir.

- **Empêcher** : bloquer les menaces courantes tout en renforçant les systèmes centraux pour réduire les risques associés aux menaces avancées
- **Détecter** : identifier rapidement les activités qui pourraient signaler une attaque ciblée ou une violation existante
- **Répondre** : confiner précisément la menace, mener des enquêtes et répondre efficacement aux attaques
- **Prévoir** : savoir où et comment les prochaines attaques ciblées sont susceptibles de se produire



Modèle de sécurité adaptable

Concrètement, cette approche suppose que les mesures de prévention traditionnelles, notamment celles dédiées aux terminaux, fonctionnent de pair avec des technologies de détection avancées, des analyses des menaces, des capacités de réponse et des techniques de sécurité prédictives. Il en résulte un système de cybersécurité capable de s'adapter en continu aux défis émergents auxquels sont confrontées les entreprises, et d'y faire face.

Les technologies multiniveaux axées sur la prévention demeurent un atout clé dans cette nouvelle approche proactive de protection contre les attaques ciblées. Cependant, si l'auteur de l'attaque est suffisamment motivé, voire engagé par un tiers pour réussir, une approche uniquement axée sur la prévention ne suffira pas. Vous devez également être en mesure d'identifier rapidement les menaces, de prendre les décisions qui s'imposent et d'anticiper une éventuelle intrusion, tout en simplifiant les opérations manuelles existantes et en automatisant les outils de réponse.

Définition de l'EDR

Caractéristiques clés d'une solution de type EDR

Comme nous l'avons déjà évoqué, Gartner considère que les solutions EDR doivent disposer des principales fonctionnalités suivantes :

- Détecter les incidents de sécurité
- Confiner l'incident dans le terminal, afin de pouvoir assurer le contrôle à distance du trafic réseau ou de l'exécution des processus
- Mener des enquêtes sur les incidents de sécurité
- Rétablir un état antérieur à l'infection sur les terminaux

Détection des incidents de terminaux

Détecter les incidents de sécurité en **surveillant les activités**, objets et violations de stratégies **des terminaux**, ou en validant les indicateurs de compromission (IoC) de sources externes.

Investigation des incidents

Mener des enquêtes sur les incidents de sécurité. La fonction de recherche doit comprendre **une chronologie** de tous les principaux événements survenus sur les terminaux pour déterminer à la fois les modifications techniques apportées et leur impact sur les activités.

(transmission, extension, exfiltration, géolocalisation de C&C et attribution d'adversaires, si possible).

Confinement de l'incident et réponse

Confiner l'incident dans le terminal et **rétablir** sur les terminaux un état antérieur à l'infection.

Retirer les fichiers malveillants, revenir en arrière et annuler d'autres modifications, ou créer des instructions de résolution exploitables par d'autres outils à mettre en œuvre.

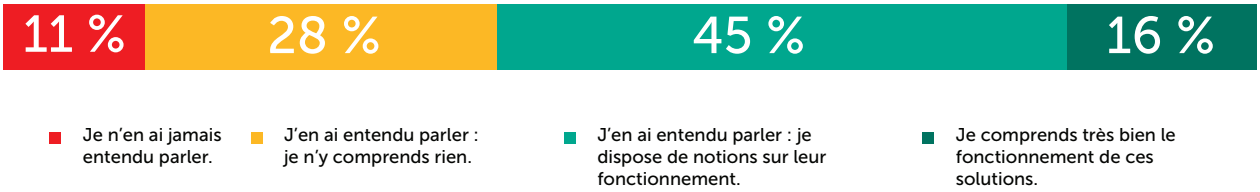
Collecte des données de cyberdiagnostic

Collecter des ensembles de données, décharges RAM, instantanés de disques durs, etc. à des fins d'analyse supplémentaire.

Dans quelle mesure les entreprises comprennent-elles le fonctionnement des solutions EDR et leurs avantages pour la continuité de l'activité ? Une enquête de Kaspersky Lab réalisée en 2016 auprès des entreprises a livré des conclusions préoccupantes.

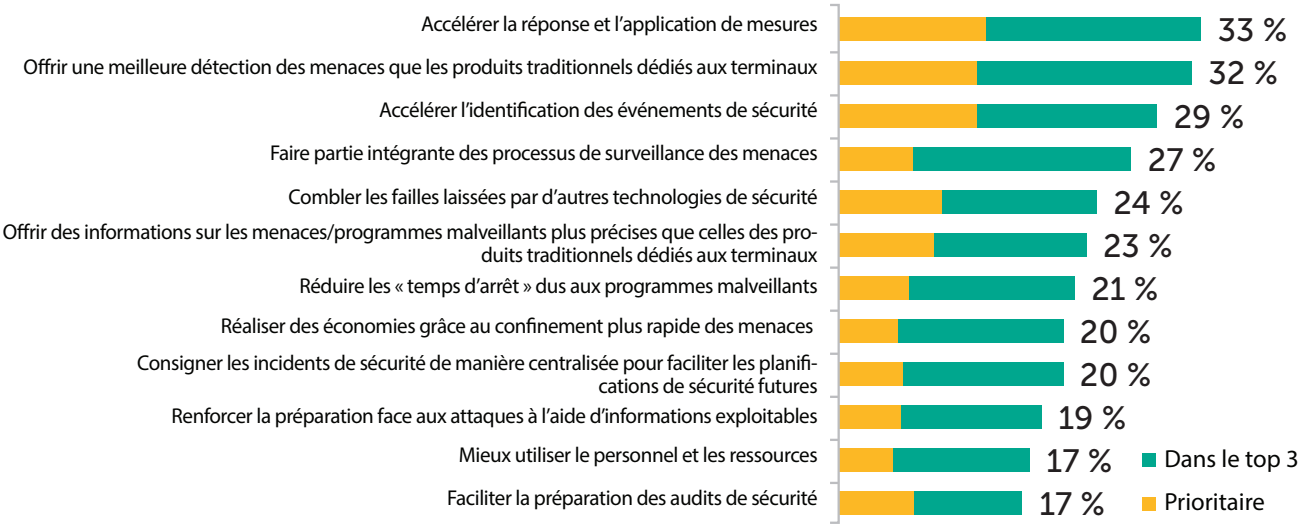
Question posée au panel : « Dans quelle mesure connaissez-vous les solutions de type EDR ? »

Réponse :



Source : Experts informatiques d'entreprises comptant plus de 250 employés

Dans le même temps, les représentants d'entreprises interrogés ont très précisément défini leurs attentes fondamentales ainsi que les avantages qu'ils souhaitent obtenir en adoptant des solutions EDR :



Ce curieux mélange de connaissances limitées et d'attentes clairement définies est problématique. Les fournisseurs de solutions EDR sont évidemment disposés à satisfaire ces attentes, en développant des « fonctionnalités racoleuses », qui promettent monts et merveilles lors de la phase pilote, mais qui s'avèrent nettement moins pratiques et rentables une fois intégrées aux processus de réponse aux incidents, d'enquête ou de recherche des menaces des clients, que de tels processus soient nouveaux ou déjà en place.

Pour cette raison, les solutions EDR font déjà l'objet d'une certaine méfiance.

Que faut-il attendre d'une solution EDR moderne, et comment la choisir ? Examinons 5 enjeux importants à prendre en compte avant de se lancer dans les technologies EDR.

Les 5 principaux défis associés à l'adoption d'une solution EDR

Toute entreprise adoptant de nouvelles technologies ou des processus inhabituels doit forcément composer avec un certain nombre de défis. Puisque les solutions EDR sont plus coûteuses que les solutions EPP, il peut être délicat de justifier l'apport de valeur ajoutée d'un tel investissement par rapport aux coûts d'un système SIEM ou d'outils de cyberdiagnostic, par exemple.

Le principal atout d'une solution EDR d'entreprise réside dans sa **capacité à aider une équipe de sécurité au moyen d'enquêtes reposant sur des questions** (conseils de recherche itératifs et basés sur des questions ou des hypothèses) offrant une certaine visibilité. Une première question ou hypothèse peut porter sur les différents maillons de la chaîne de frappe, et se présenter comme suit : « Une exfiltration de données ou une communication malveillante est-elle en cours ? », ou encore : « Il est probable qu'une possible connexion suspecte vers un domaine externe transite par cette portion du réseau, mais à partir de quels terminal et processus ? ».

Pour proposer de telles capacités, une solution EDR doit intégrer des fonctions **d'aide aux enquêtes**, **de collecte de données** et **de stockage**. Par ailleurs, la **détection des incidents** doit combiner des éléments automatisés et manuels. Enfin, une fois l'incident initial détecté, l'équipe de sécurité et les responsables de la réponse doivent être suffisamment armés pour **confiner facilement** la menace, **corriger** les terminaux et **empêcher** que les activités incriminées ne se reproduisent.

Examinons 5 défis courants que les entreprises doivent prendre en considération dans le choix de solutions EDR avancées ou pour améliorer l'efficacité générale de leur sécurité des terminaux sur les plans de la détection et de la réponse.

Données des terminaux : trop de visibilité

La protection des terminaux sous toutes ses formes commence par la collecte de nouvelles données, puis par leur stockage et leur analyse. En théorie, plus les données collectées sont nombreuses, mieux c'est. Autrefois, cette théorie s'appliquait également aux systèmes SIEM. Il reste que pour interpréter d'importants volumes de données, l'opérateur d'une solution EDR doit également disposer du contexte approprié. Par exemple, la détection rapide d'une connexion malveillante vers un domaine frauduleux n'a que peu d'intérêt si vous ne savez rien du terminal dont elle provient, de la genèse du processus, de sa cause première et des ressources potentiellement affectées.

Les solutions EDR peu sophistiquées du marché collectent des données sans fournir le contexte associé. Ainsi, si elles aident un opérateur à identifier rapidement les machines qui hébergent un fichier présentant une somme de hachage spécifique, elles ne fournissent aucune information sur l'apparition du fichier en question sur ces machines. Parfois, une liste des processus générés est fournie pour l'objet et les activités associées, mais sans la moindre visualisation. De la même manière, des alertes complexes relatives à des comportements atypiques peuvent être émises, sans pour autant s'accompagner d'analyses élémentaires ni de conclusions.

Certaines solutions collectent toutes les données des terminaux pour les présenter directement sur l'interface, à la manière d'une fenêtre directe sur la base de données. À moins que l'opérateur ne soit un scientifique des données ou un spécialiste du big data doublé d'un expert de la sécurité, il lui sera difficile de prendre une décision en fonction de ces données non décryptées.

De tels systèmes génèrent souvent des milliers de messages et des millions d'alertes, qu'il faut valider. La gestion simultanée de plus de 50 ou 60 incidents d'une gravité modérée à critique semble impossible, même pour les équipes de surveillance et d'intervention des plus grandes entreprises. Nous nous retrouvons ainsi avec une solution en mesure de tout détecter, mais qui fournit à la fois trop ou pas suffisamment d'informations, celles-ci pouvant être difficilement exploitées (voire pas du tout).

La répartition des alertes entre votre équipe de sécurité et un fournisseur de services de sécurité gérés (MSSP, Managed Security Service Provider) externe pourrait constituer un compromis viable, mais il vous faudrait trouver un fournisseur disposant de suffisamment d'expérience et d'expertise. Sans hiérarchisation appropriée des incidents, vous risqueriez d'allouer une énorme quantité d'argent et de ressources au traitement d'alertes non critiques. Comme avec tout MSSP, les questions de la confiance, de la confidentialité des données et des limites de conformité viennent également compliquer les choses.

Recommandations :

- Recherchez des solutions qui ne se contentent pas de signaler les risques par le biais d'alertes automatisées, mais qui offrent également une personnalisation poussée, incluant la configuration de rôles utilisateur distincts, l'affectation de groupes VIP et la création rapide de listes blanches. Vous pourrez ainsi vous concentrer sur l'essentiel, réduire les tâches superflues et vous assurer que le MSSP externe accède uniquement aux informations stratégiques.
- Interrogez-vous sur l'ampleur de l'analyse de données que vous comptez mettre en place dans votre entreprise, ainsi que sur la quantité de données à stocker et traiter. Gardez à l'esprit que les capacités nécessaires à la gestion de plusieurs téraoctets de données peuvent augmenter sensiblement les coûts matériels.

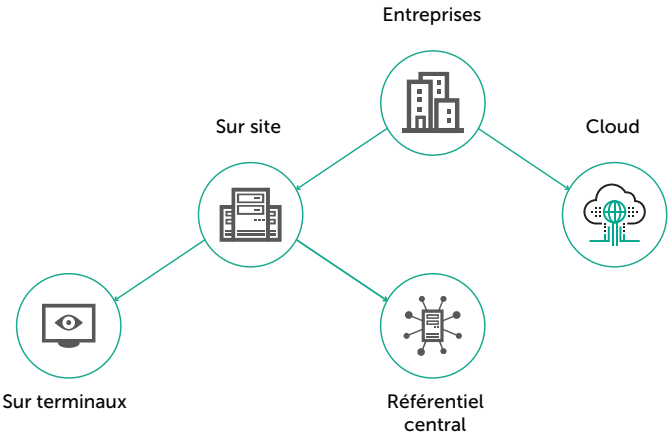
2

Responsabilités associées aux données agrégées et stockées

Les modalités de collecte et de stockage des données ont également leur importance. Vous devez poser les questions suivantes à un fournisseur de solutions EDR :

- En quelle quantité et dans quel but les données sont-elles stockées ?
- Quelles sont les données stockées ?
- Où les données sont-elles stockées ?

Il existe plusieurs approches de stockage :



Examinons-les de plus près.

Cloud

Bon nombre de fournisseurs proposent des solutions Cloud pour stocker les données, voire gérer les agents EDR (référentiels de métadonnées, ou « MDR », pour Metadata Repository). Celles-ci sont pratiques, mais le volume de données qu'elles peuvent télécharger simultanément est limité. Ce type de solution exige également l'ouverture d'un conduit pour transmettre les données à l'extérieur de l'entreprise, ce qui peut s'avérer problématique dans certains environnements. Si vous envisagez cette option, vous devez vous poser les questions suivantes :

- Sommes-nous disposés à envoyer des données de sécurité dans un Cloud public ? De quels niveaux de contrôle disposerons-nous ?
- L'éditeur ou le fournisseur de solutions Cloud (parfois un tiers) qui stockera mes données est-il digne de confiance ? Quelle est la fiabilité des mesures de cybersécurité de celui-ci ?
- L'utilisation d'un tel service constitue-t-elle une infraction à des normes de sécurité internes et/ou exigences réglementaires ?
- Si seuls de petits volumes de données non stratégiques sont envoyés dans le Cloud, quelle peut être l'efficacité de la solution ?

Intégration aux agents

La présence d'un cache local sur chaque appareil fournit un compromis entre un stockage encombrant et le Cloud. Cette approche est moins invasive pour le réseau et offre une prise en charge instantanée d'un grand nombre d'agents. Les informations importantes sont enregistrées directement dans le cache du terminal, et toutes les analyses sont réalisées en temps réel par le biais de requêtes. Par contre, un stockage décentralisé n'est pas toujours le mode d'analyse et d'exploitation des informations le plus rapide et le plus efficace. Par exemple, en cas d'indisponibilité d'un sous-segment du réseau, il devient impossible d'intégrer dans l'analyse globale les données provenant des machines affectées.

Référentiel sur site centralisé

Toutes les informations essentielles sont rassemblées et analysées par un serveur dédié, doté d'un référentiel. Une base de données locale et des outils d'analyse (par exemple, une sandbox) font tout le travail. Cette approche locale présente plusieurs avantages : les données ne sont pas stockées sur des appareils potentiellement compromis, comme cela peut être le cas avec le stockage reposant sur des agents. Aucune charge n'est imposée aux ressources de l'ordinateur, et vous pouvez exécuter les requêtes des terminaux et réaliser une « recherche rapide » dans la base de données proprement dite, le tout en temps réel. Les solutions sur site de ce type s'avèrent particulièrement utiles lorsque des réglementations ou normes de sécurité interdisent le transfert de données à l'extérieur de l'entreprise.

Recommandations :

- Pour le stockage Cloud, jugez votre fournisseur de solutions EDR en fonction du contrôle et de la confidentialité des données qu'il propose.
- Pour les environnements sensibles, et lorsque des règles de conformité réglementaire imposent des restrictions au transfert de données externes, votre évaluation peut porter sur les options de mise en œuvre sur site entièrement isolée et de distribution privée des informations sur les menaces.
- Pour le stockage de données reposant sur des agents, demandez-vous ce qui se passerait en cas d'indisponibilité d'un terminal, ou de compromission de celui-ci par un pirate (autrement dit, les mesures de protection des données, de l'ordinateur et de l'agent proprement dit).
- Pour les solutions sur site, examinez la capacité de stockage des données en interne et le volume de données envoyé par chaque appareil.

Les exigences matérielles dépendent du nombre d'agents. Par exemple, si une solution EDR a seulement besoin d'un petit serveur pour prendre en charge des centaines de milliers d'agents, il y a un problème quelque part. En moyenne, un terminal génère tous les jours environ 10 mégaoctets de données télémétriques précieuses. Ainsi, si vous disposez de 10 000 nœuds, vous devez viser une base de données rétrospective de 100 gigaoctets de données par jour, soit 3 To par mois.

Détection : recherche manuelle ou moteurs automatisés

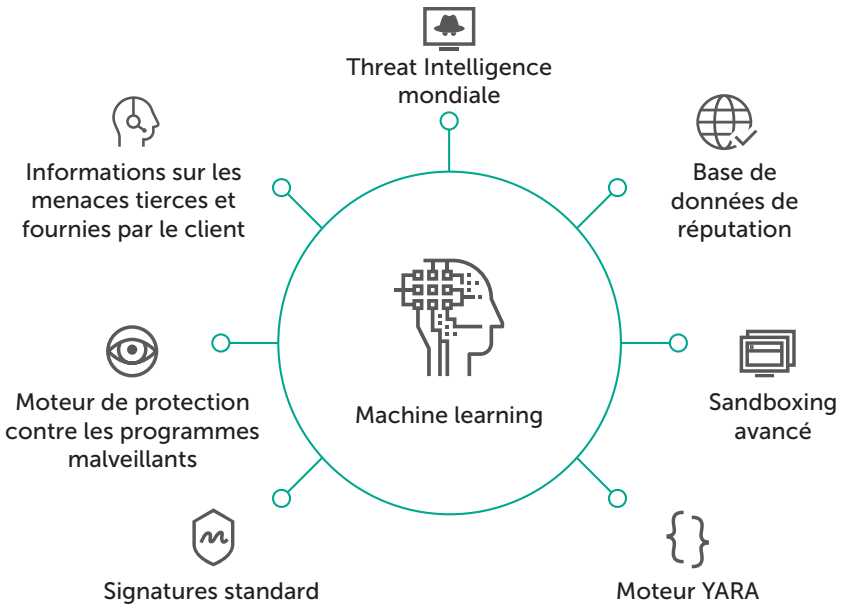
Maintenant que vous en savez davantage sur les données et le stockage, nous allons passer à l'analyse des données, en abordant la recherche et la surveillance des menaces (Threat Intelligence), qu'elles soient réalisées manuellement à l'aide des ressources, bases de données et kits d'outils de votre fournisseur, ou automatiquement par le biais du système EDR. Plus une attaque est détectée tôt, moins elle risque d'entraîner des répercussions financières et des interruptions. La vitesse et l'efficacité de la détection sont donc d'une importance capitale, et les techniques de détection manuelles seules ne constituent généralement pas l'approche la plus rapide ni la plus efficace. Bon nombre de fournisseurs proposent des techniques de détection prétendument avancées, incluant le balayage en temps réel des indicateurs de compromission (IoC) ou la recherche rapide dans des bases de données de données de cyberdiagnostic stockées de manière centralisée, en ajoutant une composante d'automatisation aux fonctionnalités de détection des incidents.

Pour tirer le meilleur parti de vos données agrégées, vous avez besoin de techniques d'analyse automatisées, aidant vos analystes à mettre en évidence les risques et menaces pesant sur le réseau. Les analyses sur plusieurs dimensions et niveaux doivent faire remotner en continu non seulement de nouveaux incidents de sécurité, mais aussi des informations exploitables, afin d'aider votre équipe de sécurité à prendre les bonnes décisions et à évacuer rapidement les événements non critiques.

De telles technologies de détection et de recherche des menaces doivent d'une part mettre en lumière les activités malveillantes, et d'autre part aller « au-delà des programmes malveillants » pour détecter les violations plus sophistiquées. Il est ici question à la fois des couches de filtrage des technologies de prévention, qui sont au cœur de la plupart des solutions EPP, et des systèmes d'analyse avancés.

Les solutions de sécurité qui utilisent plusieurs technologies de détection peuvent augmenter sensiblement vos chances de repérer les attaques et intrusions plus rapidement, avant que celles-ci ne causent d'importants dégâts à votre entreprise. Les solutions EDR doivent désormais intégrer plusieurs moteurs de détection pour garantir une détection des menaces avancées combinant des analyses statiques, comportementales et dynamiques à une Threat Intelligence mondiale et à des technologies de machine learning.

L'objectif principal est d'exploiter autant de moteurs de détection que possible pour disposer en interne des fonctionnalités d'un laboratoire d'analyse de virus, celles-ci permettant de valider les prédictions et de mener de nouvelles enquêtes ou de faciliter celles en cours.



Selon les fournisseurs, les techniques de détection et les moteurs utilisés comprennent généralement une combinaison d'outils manuels et de systèmes automatisés :

Mécanismes de détection manuels

- Chargement des indicateurs de compromission (IoC) et recherche automatisée/manuelle
- Recherche rapide dans les données rétrospectives
- Sandboxing (possibilité d'envoyer un objet spécifique dans une sandbox dédiée ou dans le Cloud)
- Accès aux sources de Threat Intelligence du fournisseur

Détection automatisée

- Protection contre les programmes malveillants
- Règles YARA (personnalisables par le fournisseur et/ou votre équipe de sécurité)
- Informations sur les menaces (transmises automatiquement par le fournisseur)
- Services de réputation (fichiers et/ou domaines)
- Analyse automatisée des objets suspects dans des sandboxes
- Machine learning, ou apprentissage automatique
  - Deep learning, ou apprentissage profond (aucune signature, réseau de neurones artificiels)
  - Intelligence artificielle (établissement de données de référence, analyse comportementale)

Recommandations :

- Interrogez votre fournisseur de solutions EDR sur ses technologies de détection disponibles et opérationnelles.
- Demandez-lui s'il utilise des moteurs de détection internes, OEM ou open source.
- Assurez-vous de la qualité et de l'actualisation des informations sur les menaces qui alimentent ces moteurs.
- Si plusieurs technologies de détection sont employées, quels sont leurs modes d'intégration et de mise en corrélation ? (L'objectif étant d'éviter la consignation d'incidents distincts dans différents moteurs pour un même événement.)

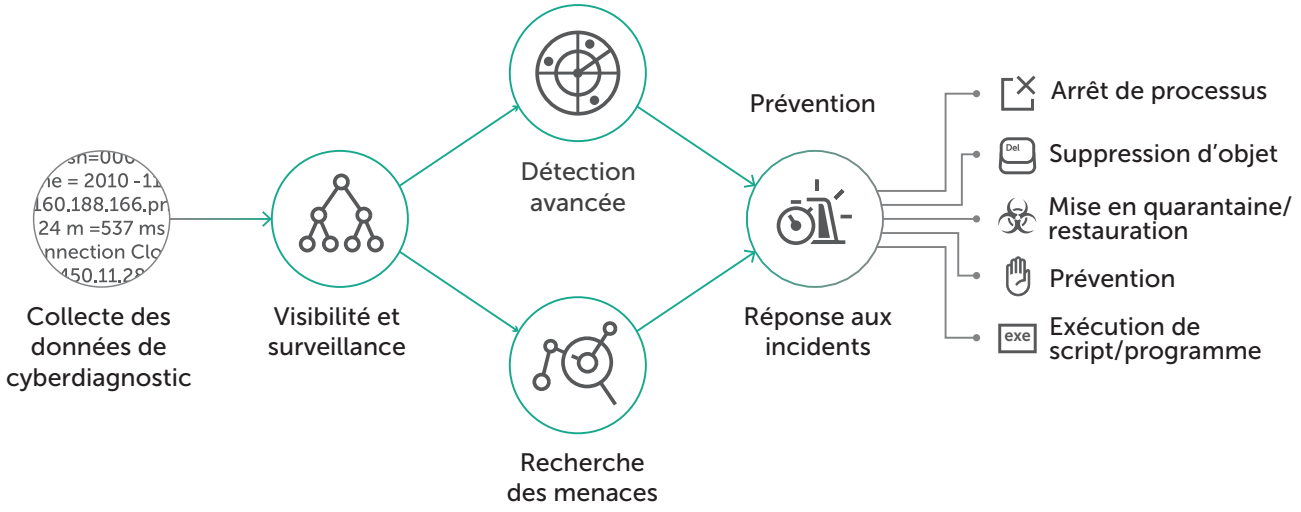
4

Ne vous contentez pas de réagir : intervenez

S'il est aisé de réagir à un incident, seule une intervention efficace permet de le résoudre. Le processus de réponse se déclenche une fois qu'un incident de sécurité a été confirmé suite à un tri et à une enquête préliminaire. Une fois qu'il a été établi qu'il ne s'agit pas d'un « faux positif », une réponse rapide et précise est requise.

Le processus de gestion des réponses aux incidents dépend de la gravité de l'incident. La plupart des incidents n'ont que peu d'impact sur les activités (lorsqu'ils sont détectés immédiatement). Certains peuvent toutefois donner lieu à des situations dangereuses, incluant des violations de données majeures, des crimes financiers, de l'espionnage industriel, ou même pire. C'est dans ces situations critiques qu'un processus d'enquête et de réponse d'urgence s'impose.

Une fois que vous avez manuellement détecté une menace potentielle ou reçu une alerte de sécurité, que ce soit par le biais de votre produit EDR ou d'une solution de sécurité tierce, que se passe-t-il ? Avez-vous recensé les processus de tri, d'enquête et de réponse de votre entreprise ? Sans de tels processus, votre équipe de sécurité risque de crouler rapidement sous les flux de travail inhérents à une solution EDR.



La détection d'une menace active est la première étape stratégique pour repousser une attaque. Une fois la menace identifiée, vous devez intervenir rapidement, parfois sur plusieurs milliers de terminaux. Pour être efficace, une solution EDR doit offrir une gestion centralisée des incidents sur tous les terminaux d'un réseau d'entreprise, avec des flux de travail parfaitement intégrés. En outre, un large éventail de réponses automatisées évite d'avoir à utiliser des processus de résolution traditionnels, comme l'effacement et la création de nouvelles images, qui peuvent entraîner des interruptions coûteuses et une perte de productivité.

Les fonctionnalités de réponse principales, qui dépendent de l'approche du fournisseur, doivent se focaliser sur les opérations courantes suivantes :

- Empêcher l'exécution de fichiers exécutables portables (PE, Portable Executable), de documents de bureau et de scripts
- Supprimer à distance le fichier sur le poste de travail
- Mettre le fichier en quarantaine et le restaurer si nécessaire
- Récupérer le fichier et le soumettre à une analyse pendant l'enquête (par exemple, exécution de sandbox forcée)
- Forcer l'arrêt du processus
- Exécuter le programme/script sur le poste de travail

Pour améliorer la précision des réponses, certains fournisseurs peuvent proposer des scénarios supplémentaires, notamment d'isolation de réseaux et de processus, de désactivation d'utilisateurs, d'annulation et de résolution.

Recommandations :

Concentrez votre attention sur :

- Les fournisseurs capables de gérer des bases de données d'informations sur les menaces performantes et exhaustives, et de proposer une assistance et des conseils d'expert selon les besoins.
- Les solutions EDR appuyées par des formations efficaces, apprenant à votre équipe de sécurité à mettre en place des processus performants pour tirer le meilleur parti de votre investissement.
- Des flux de travail parfaitement intégrés entre les processus de détection, de recherche manuelle des menaces, de gestion des indicateurs de compromission (IoC) tiers et de réponse aux incidents, évitant d'alterner entre plusieurs consoles ou solutions.
- Des agents imperceptibles pour les utilisateurs finaux, y compris pendant les enquêtes, sans incidence sur le comportement des utilisateurs et n'occasionnant pas d'interruptions.

5

Prévention : solutions EDR ou EPP ?

Les solutions EDR intègrent de plus en plus d'outils de prévention dans le but de proposer une polyvalence complète. Compte tenu du gain de maturité des fonctions de prévention, il est probable que les fonctionnalités de prévention, de visibilité, de détection et de réponse sur les terminaux finissent par converger vers un même produit.

Mais nous n'en sommes pas encore là. S'il peut être tentant de rechercher une solution associant la prévention aux tâches de détection et de réponse, nous vous déconseillons d'accorder trop d'importance à cet aspect pour le moment. Sélectionnez votre produit en fonction de la visibilité et des capacités de détection et de réponse qu'il propose. Si une telle solution fournit également des éléments de prévention, c'est un plus. Méfiez-vous toutefois des solutions EDR prétendument de nouvelle génération, intégrant des fonctions de prévention immatures. Si vous tentez de remplacer votre solution EPP traditionnelle par une solution EDR, il est peu probable que vous disposiez d'un même niveau de prévention.

Ceci dit, de nombreux fournisseurs de solutions EPP achètent ou développent désormais leurs propres solutions EDR. Si vous êtes satisfait de votre solution EPP et que le fournisseur de celle-ci vous propose une solution EDR, il est utile de vous interroger sur les interactions entre ces solutions et sur ce que leur association peut vous apporter, a fortiori si cela peut vous éviter d'installer un deuxième agent pour les fonctionnalités EDR.

Recommandations :

- Consultez la feuille de route du produit EDR, notamment les fonctionnalités de prévention supplémentaires qu'il est susceptible d'intégrer au fil du temps.
- Si l'idée d'une solution intégrée combinant protection des terminaux, détection et réponse aux incidents vous plaît, consultez le catalogue de produits EDR de votre fournisseur de solutions EPP, tout en vous renseignant sur les fonctionnalités EPP que proposent les autres fournisseurs de solutions EDR.
- Examinez l'architecture de toute solution EDR, en accordant une attention particulière à la possibilité d'utiliser un seul agent pour les fonctionnalités EPP et EDR.

L’avenir de la sécurité des terminaux pour les entreprises

Les chefs de file du marché tenteront d’adopter de nouvelles technologies et de mettre à profit les développements internes pour renforcer leurs fonctionnalités EDR.

Les experts en sécurité affirment que le marché de la sécurité des terminaux actuel croule sous le nombre de fournisseurs. Il devient évident qu’une telle situation ne peut durer. Les principaux fournisseurs finiront par absorber les petites entreprises, en utilisant les produits de celles-ci pour compléter leurs catalogues et améliorer leurs marques respectives. Les chefs de file du marché tenteront d’adopter de nouvelles technologies et de mettre à profit les développements internes pour renforcer leurs fonctionnalités EDR.

La véritable sécurité des terminaux « Next Gen », qui associera les méthodes de contrôle et de protection traditionnelles à des technologies avancées, évoluera au fil des innovations apportées par les principaux acteurs du marché EPP. La génération actuelle d’agents de protection des terminaux avancés, par exemple de type EDR, propose uniquement certains aspects d’une fonction EPP authentique. Pour le moment, ces agents ne prétendent pas constituer des suites de protection des terminaux tout-en-un.

La sécurité des terminaux redevient une priorité pour les entreprises, et est en passe de prendre encore plus d’ampleur. À terme, les clients adapteront et feront évoluer leurs stratégies de sécurité, en les articulant autour des technologies avancées de protection des terminaux et de la surveillance des activités sur ces derniers.

D’un point de vue technologique, ces solutions avancées se réuniront au sein d’une approche adaptative de la protection, tout en proposant un renforcement des systèmes, une prévention des activités malveillantes et une détection avancée. La surveillance des menaces dans le Cloud et le machine learning sur site, la recherche des menaces incluant des réponses actives et des enquêtes rapides, et enfin l’analyse des comportements et des informations sur les menaces apporteront également leur pierre à l’édifice.

Recommandations

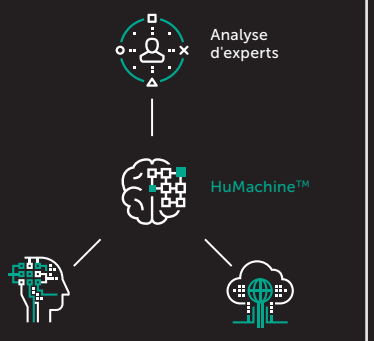
Une fois qu'ils ont pris conscience de la nécessité de disposer d'une protection et d'une analyse plus poussée des terminaux, les professionnels de sécurité se retrouvent inévitablement avec une longue liste de besoins et très peu de budgets pour y répondre. Même sans budget, il est pertinent d'évaluer les technologies actuelles et développements futurs envisageables à la lumière de vos objectifs commerciaux et de vos capacités internes. En étudiant de près les différentes options disponibles, vous pouvez aider les décisionnaires de votre entreprise à se focaliser sur les avantages dont recèlent les nouvelles technologies et augmenter la précision des prochaines allocations de budgets pour la sécurité. Ainsi, lorsque viendra le moment d'investir, vous pourrez le faire en toute connaissance de cause.

Mesures à prendre immédiatement

1. Évaluez vos fonctionnalités de sécurité globales. Quels sont la rapidité et le niveau d'unification de votre processus de réponse aux incidents actuel ? Fonctionnalités EDR mises à part, vos solutions existantes répondent-elles à vos besoins ? Où vous situez-vous à cet égard par rapport à vos concurrents et à votre secteur ?
2. Dressez l'inventaire de vos fonctionnalités actuelles de détection sur terminaux. Effectuez des analyses et envisagez de nouvelles sources d'informations, en intégrant par exemple des flux d'informations sur les menaces à votre système SIEM.
3. Demandez-vous comment développer votre expertise de réponse aux incidents en interne. Évaluez les compétences de votre équipe et étudiez les modalités de formation appropriées.
4. Commencez à recenser vos exigences réelles/besoins à venir et établissez une présélection de solutions EDR adaptées.

Quelques liens utiles

1. Incident Response Guidelines (directives en matière de réponse aux incidents, en anglais) : https://cdn.securelist.com/files/2017/08/Incident_Response_Guide_eng.pdf
2. Estimez votre budget de sécurité informatique à prévoir pour 2018 à l'aide d'un outil simple, qui vous donnera une réponse en quelques clics : https://calculator.kaspersky.com/fr/



Solutions de cybersécurité Kaspersky Lab
pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.fr