Comment lutter contre la multiplication des menaces avec des équipes réduites : passez à l'automatisation

kaspersky

Plus d'informations sur kaspersky.fr
#bringonthefuture

Introduction

La plupart des entreprises, indépendamment de leur taille, localisation ou activité, comprennent désormais qu'en matière de cyberattaque, la question n'est plus de savoir si, mais quand on se fera attaquer. Personne ne doit désormais se considérer à l'abri.

La plupart des experts en cybersécurité sont surchargés. Recruter du personnel IT compétent, sélectionner les solutions de sécurité les plus efficaces du marché, comprendre les nouvelles lois et les problématiques de conformité, connaître les dernières menaces. est très consommateur de temps et n'est que le préalable à la mise en place d'une sécurité efficace.

En général, très peu de professionnels de la sécurité peuvent se permettre de passer leur temps à rechercher des menaces nouvelles ou peu courantes et à y répondre.

C'est là que les éditeurs de cybersécurité, et leurs produits et solutions, entrent en scène. Notre objectif est de vous aider à sécuriser entièrement votre infrastructure et à protéger vos utilisateurs, en engageant le moins de ressources possible (temps et argent).

Les défis

Tout d'abord, examinons certaines des problématiques auxquelles font face les départements informatiques et les responsables de la sécurité informatique.

Multiplication des menaces impliquant une attaque ciblée ou avancée

Les attaques ciblées et les menaces complexes représentent un problème dont l'ampleur augmente constamment. Les outils des cybercriminels deviennent si accessibles et bon marché que presque n'importe quelle personne équipée d'un ordinateur peut désormais lancer une attaque avancée.

Cela dit, les menaces « basiques » restent également problématiques : leur quantité vertigineuse est un réel problème au niveau mondial.

La grande majorité des cybermenaces entrent par un terminal, ou bien sont conçues pour s'y déclencher (ou les deux).

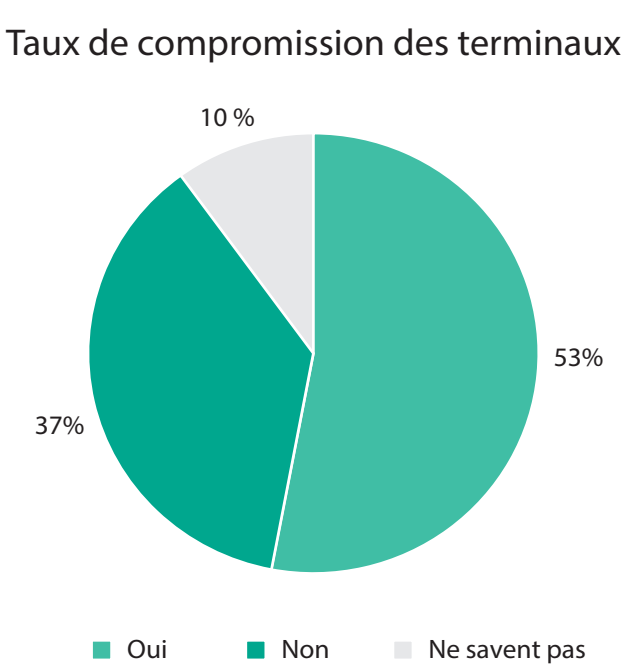
Ainsi, l'un des meilleurs moyens de protéger vos ressources est de protéger vos terminaux.

Selon une étude de l'institut SANS[2], 53 % des organisations ont subi une intrusion, 37 % n'ont pas subi d'intrusion et 10 % ne savent pas si elles en ont subi une.

91 %[1] des organisations ont subi au moins une attaque au cours de l'année passée.

1 organisation sur 10[1] a fait face à une attaque ciblée (à leur connaissance) sur la même période.

- **53 %**[2] des organisations savent que leurs terminaux ont été compromis
- **30 %**[1] des organisations n'ont pas encore entièrement déployé de logiciel contre les programmes malveillants
- **56 %**[3] des violations ne sont pas détectées avant plusieurs mois, voire davantage



2 organisations sur 3[4] pâtissent d'un manque de personnel dédié à la sécurité des informations.

D'après les prévisions, d'ici 2021, **3,5 millions**[5] de postes en cybersécurité seront à pourvoir.

1 Rapport Kaspersky sur les risques informatiques mondiaux, Kaspersky, 2019

2 Risques et protections pour les terminaux de nouvelle génération, Institut SANS, 2017

3 Rapport 2019 d'enquêtes sur la violation des données, Verizon, 2019

4 Étude sur le personnel du domaine de la cybersécurité, (ISC)², 2019,

5 Rapport annuel officiel sur les emplois dans la cybersécurité, Cybersecurity Ventures, 2019

Erreur humaine

Malheureusement, dans toute infrastructure d'entreprise, le maillon le plus vulnérable reste l'utilisateur. Vos utilisateurs accèdent peut-être très régulièrement aux données de l'entreprise à distance et depuis leurs propres appareils. Les matériels tout comme les salariés doivent être protégés.

La détection et la prévention des comportements dangereux dans les environnements informatiques complexes actuels viennent s'ajouter aux tâches des experts en sécurité déjà sous pression.

De plus, les professionnels de l'informatique peuvent également faire des erreurs (après tout, l'erreur est humaine), et ces erreurs peuvent engendrer des attaques par le biais de vulnérabilités présentes sur des appareils personnels ou professionnels mal patchés, par exemple.

La pénurie de ressources

Les experts en informatique ont donc du pain sur la planche.

Même pour les petites entreprises, il existe un volume croissant d'événements de sécurité à traiter, analyser et auxquels répondre quotidiennement ; cela met donc à rude épreuve leur capacité à travailler efficacement et rapidement. Les cybercriminels savent que les entreprises sont en difficulté, et ils en tirent pleinement avantage.

Même les entreprises qui ont la chance de disposer de ressources financières conséquentes subissent cette pénurie mondiale de professionnels formés à la cybersécurité. Ce problème n'est pas nouveau, mais si on s'attache au nombre d'experts formés chaque année, la situation n'est pas prête de s'améliorer.

Pouvoir se préoccuper du bien-être et de l'efficacité de ses experts en sécurité malgré les circonstances, voire tout simplement réussir à les retenir, relève du défi. Le burn-out professionnel est un réel problème, en particulier si votre équipe, aussi compétente et formée soit elle, passe ses journées à réaliser des tâches de routine.

Bien sûr, le problème du budget entre également en jeu. Et il faut encore ajouter tout ce qui coûte pour optimiser votre sécurité sans impacter les vitesses de traitement, la productivité des salariés ou la satisfaction des utilisateurs.

La solution

Alors, quelles sont les solutions ?

Sécurisation des terminaux

En premier lieu, tout repose sur **une protection efficace des terminaux** ; c'est aussi simple que cela. Prévenir les menaces au niveau des terminaux, avant que les alertes ne se déclenchent, réduit le stress, atténue le risque de concrétisation d'une attaque, et permet d'assurer la continuité des activités de manière fluide et sécurisée.

L'approche que nous vous recommandons comprend une combinaison de **défenses multi-niveaux des terminaux** ; une protection de base puissante contre les menaces « basiques », et des défenses multi-niveaux et multifacettes contre les menaces plus complexes.

L'**EDR (Endpoint Detection and Response)** fournit le second niveau de sécurité. L'EPP (Plateforme de protection des terminaux) offre l'identification et la protection initiales, alors que l'EDR offre la visibilité et des options d'analyse plus approfondies, vous permettant de voir comment l'attaque a débuté et à quel stade elle se trouve. Outre la détection, l'EDR fournit également des options de réponse proactive, pour que la menace révélée puisse être contenue de manière rapide et efficace.

L'EDR ne peut être efficace qu'en association avec une protection de base robuste. Plus la solution EPP peut prévenir d'incidents en amont, moins la solution EDR doit en gérer et plus vos ressources peuvent se concentrer sur les incidents les plus critiques.

Gérer le comportement humain

L'un des meilleurs moyens d'éviter l'erreur humaine est de supprimer l'opportunité et la tentation grâce à des **contrôles des applications, du Web et des appareils**. Des contrôles efficaces, loin de représenter une contrainte dans l'entreprise, peuvent réellement stimuler la productivité ; en évitant la perte de temps ainsi que l'accès aux sites Web de divertissement et aux réseaux sociaux potentiellement dangereux, par exemple.

Mais nous sommes convaincus que la solution la plus efficace est est de former les utilisateurs. Une **formation à la cybersécurité** bien conçue peut créer un réel impact sur le comportement des salariés, changer la culture d'entreprise, réduire le risque opérationnel de manière significative et baisser considérablement la charge de travail du département informatique.

Votre retour sur investissement

Enfin, toute approche doit pouvoir être justifiée financièrement en termes de retour sur investissement et fonctionner dans des environnements disposant de ressources limitées.

Automatisation et rationalisation

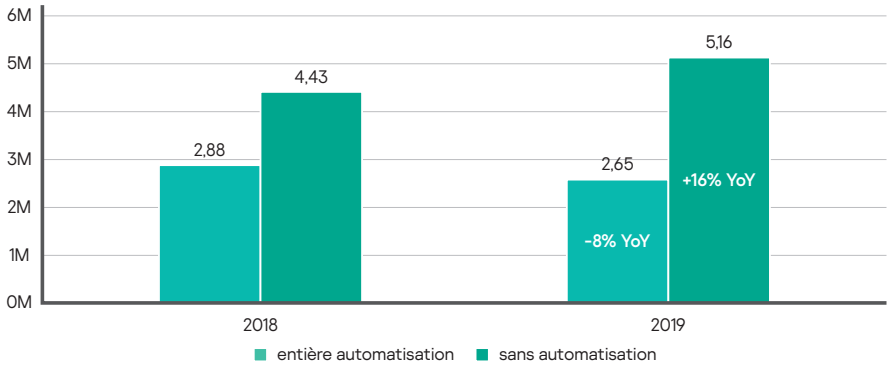
Compte tenu des volumes croissants de menaces et de la pénurie d'experts en sécurité disponibles pour les prendre en charge, **automatiser au maximum les tâches de sécurité** devient essentiel. Cela permet à vos experts en sécurité d'utiliser leur précieux temps et leurs compétences pour gérer les incidents qui requièrent une intervention et une expertise humaines (et contribue à leur bien-être et à leur motivation).

Automatiser les tâches supprime également le risque d'erreur humaine ; prioriser et mettre en œuvre la correction des vulnérabilités de systèmes de manière automatique, par exemple, est bien plus efficace que de compter sur les opérateurs humains qui trouvent le temps d'assumer cette activité essentielle mais ennuyeuse.

Un **déploiement simple** et une **console d'administration** centralisée et rationalisée permettent également d'économiser du temps et des ressources. Passer d'une console à l'autre entre les opérations et se poser sans cesse des questions sur les paramétrages n'est pas simplement chronophage et frustrant, cela ouvre également la voie aux erreurs et omissions.

Les coûts relatifs au confinement pour les organisations ne disposant pas de système d'automatisation de la sécurité ont augmenté de 16 %[6] et ont baissé de 8 % pour celles disposant d'une automatisation[6].

Coûts
relatifs au niveau d'automatisation des tâches de sécurité



6 Rapport 2019 sur le coût d'une violation de données, Ponemon Institute, 2019

Remarque sur la protection multi-niveaux

Nous avons indiqué que toute solution visant à protéger contre toute forme de cybermenace, notamment les attaques avancées et ciblées, doit être multi-niveaux.

Tout d'abord, la solution doit fournir une **protection des terminaux robuste**, notamment des contrôles de terminaux (des fonctionnalités de blocage et de restriction pour le Web, les applications et les appareils) et un moteur de protection contre les programmes malveillants renforcé. Il est également préférable de disposer de fonctionnalités de gestion des correctifs et d'évaluation des vulnérabilités, pour permettre au personnel informatique de gagner du temps et d'épargner ses efforts liés à la réalisation des tâches de routine.

Mais les programmes malveillants avancés apportent d'autres défis nécessitant des niveaux de sécurité supplémentaires. Le programme malveillant peut avoir été spécifiquement conçu pour contourner même les mécanismes de détection de terminaux les plus sophistiqués, en restant caché et inactif jusqu'à ce que l'opportunité de se déclencher se présente. Ici, il faut persuader le programme malveillant de révéler son identité et de s'activer dans un environnement sécurisé et contrôlé. C'est là qu'une **sandbox** entre en jeu. Certaines des sandboxes modernes fournissent également une réponse rapide et automatisée à la menace détectée.

Détecter des comportements complexes sur les terminaux est également un objectif clé de l'**EDR**. À l'instar de l'EPP, l'EDR doit idéalement associer l'automatisation à des outils et à une visibilité pour permettre l'intervention humaine si nécessaire. Les analystes en sécurité doivent pouvoir réaliser une analyse des causes profondes sur les incidents et répondre aux menaces de manière opportune, manuellement ou en utilisant des options de réponse automatisée.

Regrouper des technologies EPP, Sandbox et EDR permet de gérer les programmes malveillants « basiques » de manière rapide et efficace, de limiter les opportunités d'erreur humaine, de réduire le risque d'une attaque ciblée ou avancée réussie en détectant et en répondant même aux menaces « zero-day », inconnues et nouvelles.

De plus, disposer d'une solution intégrée pour l'ensemble de l'infrastructure signifie qu'aucune faille exploitable par les pirates et attaquants n'existe entre les différents outils.

La solution Kaspersky

Avec Kaspersky Endpoint Security, nous avons créé une solution intégrée hautement automatisée comprenant une protection et des contrôles des terminaux, une sandbox automatisée et un EDR, associés à une plateforme de formation à la cybersécurité (disponible en option).

Protection des terminaux robuste

La solution Kaspersky Endpoint Security for Business est connue pour fournir un EPP incroyablement robuste (notamment une protection contre les ransomwares et les attaques sans fichier) et utiliser le moteur de protection contre les programmes malveillants le plus testé et le plus primé du marché.

Les niveaux de protection des terminaux fournis par Kaspersky Endpoint Security for Business comprennent :

- Notre moteur de protection contre les programmes malveillants primé
- La protection et la détection des ransomwares
- La détection comportementale avec Rollback automatique qui identifie et bloque les menaces avancées, y compris les programmes malveillants sans fichier et la prise de contrôle de comptes administrateur, et annule toutes les modifications déjà apportées.
- Des défenses contre les menaces mobiles et une intégration EMM
- Les fonctionnalités IPS/HIPS
- Une gestion des pare-feux (dont ceux des systèmes d'exploitation)
- La Threat Intelligence Kaspersky Security Network
- Chiffrement, y compris la gestion du chiffrement intégrée au système d'exploitation
- Security Advisor - surveille les modifications apportées pour optimiser les paramètres de sécurité
- Une gestion des correctifs et des vulnérabilités automatisée
- Une installation des systèmes d'exploitation et des logiciels tiers
- Une intégration des systèmes SIEM

Contrôles granulaires

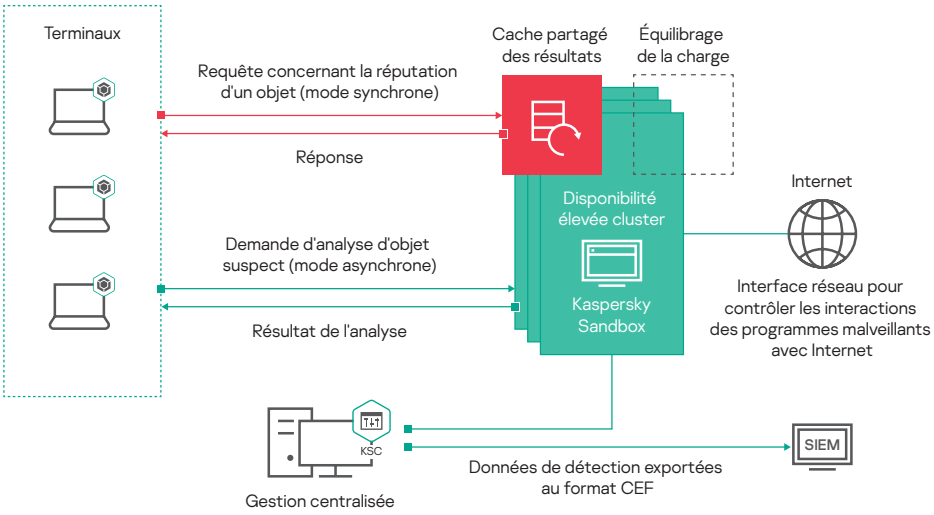
Le renforcement des systèmes et l'atténuation des erreurs humaines sont fournis via des contrôles, comprenant notamment :

- Le contrôle des applications avec la mise sur liste blanche basée sur les catégories
- Le contrôle adaptatif des anomalies qui applique automatiquement le plus haut niveau de sécurité approprié à chaque utilisateur de l'entreprise
- Le contrôle des appareils qui contrôle et bloque l'installation des appareils externes
- Le contrôle du Web qui bloque ou restreint l'accès aux sites potentiellement dangereux, chronophages ou inappropriés

Pour en savoir plus sur Kaspersky Endpoint Security for Business, rendez-vous sur https://www.kaspersky.fr/small-to-medium-business-security/endpoint-advanced

Sandbox automatisée

Kaspersky Sandbox détecte et répond automatiquement aux menaces conçues pour contourner la protection des terminaux ; sans aucune intervention humaine requise.



Flux de travail Kaspersky Sandbox

Les objets analysés sont exécutés par les serveurs sandbox en cluster dans une machine virtuelle isolée qui simule un poste de travail.

La sandbox analyse les données à la recherche d'une activité suspecte ou malveillante, et transmet le diagnostic à l'agent du terminal ayant demandé l'analyse, ainsi qu'au cache opérationnel, permettant aux autres hôtes de récupérer rapidement les informations concernant l'objet analysé sans avoir à l'analyser de nouveau.

Une fois le fichier détecté comme étant malveillant, son indicateur de compromission (IoC) peut être utilisé pour lancer une tâche de correction automatique afin de supprimer le fichier de toutes les autres machines présentes sur le réseau.

Les techniques utilisées par Kaspersky Sandbox comprennent :

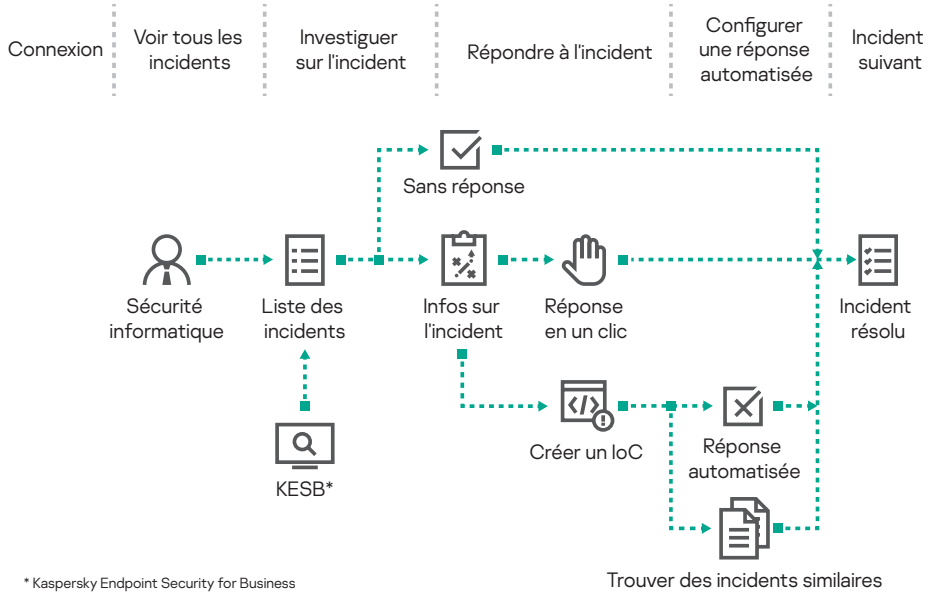
- Surveillance de l'interaction avec les ressources Internet
- Chargement du module
- Modes d'analyse synchrone et asynchrone
- Techniques de contre-évasion
- Application de différents modes d'émulation
- Modélisation des actions utilisateur
- Génération automatique d'IoC et analyse de l'infrastructure
- Prévention automatique

Pour en savoir plus sur Kaspersky Sandbox, rendez-vous sur https://www.kaspersky.fr/enterprise-security/malware-sandbox

EDR Optimum

Kaspersky EDR Optimum fournit à la fois une analyse et des réponses automatisées et manuelles aux menaces avancées faisant surface au niveau d'un terminal.

Un comportement utilisateur anormal peut être identifié, et les menaces difficilement détectables, en particulier celles sans fichier, sont automatiquement détectées et corrigées alors qu'elles tentent d'imiter un comportement normal. Les informations visuelles et la capacité à réaliser une analyse des causes profondes permettent d'assurer une réaction et une neutralisation rapides.



Flux de travail Kaspersky EDR Optimum

Fonctionnant au sein de la solution Kaspersky Endpoint Security, Kaspersky EDR Optimum est capable d'utiliser différentes techniques pour détecter les attaques et les visualiser dans la chaîne de frappe des attaques. Il peut notamment repérer les traces suivantes :

- Injection de processus
- Dépôts de fichiers
- Modifications de la clé de registre
- Connexions
- Anomalies dans le comportement de l'utilisateur

Après la détection d'une menace, les options de réponse incluent :

- Isolement de l'hôte
- Exécution d'une analyse de l'hôte
- Suppression de fichiers (en quarantaine)
- Arrêt de processus
- Empêchement de l'exécution du processus

Kaspersky EDR Optimum combine de hauts niveaux d'automatisation, en incluant des processus tels que l'importation et la génération d'IoC, en réalisant d'autres analyses et en répondant aux incidents, grâce à des options de réponse manuelle aux incidents en un seul clic.

Pour en savoir plus sur Kaspersky EDR Optimum, rendez-vous sur http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Gestion et administration

Tous les composants de notre solution sont conçus en interne d'après un code unique, administrés via la même console unique et utilisant le même agent de terminal polyvalent. La gestion quotidienne est donc centralisée, simple et efficace.

Selon Forrester[7], l'une des principales exigences pour la plupart des organisations est que leur solution de sécurité soit déployée sans provoquer (ou peu) d'interruptions pour les utilisateurs. Ce principe est au cœur même de Kaspersky Endpoint Security

7 Étude Total Economic Impact™ des solutions de sécurité Kaspersky, Forrester, 2020

- **52 %** des entreprises considèrent les salariés comme la principale menace pour la cybersécurité en entreprise[7]
- **60 %** des salariés ont des données confidentielles sur leur appareil professionnel (données financières, base de données de messagerie, etc.)
- **30 %** des salariés reconnaissent qu'ils partagent l'identifiant et le mot de passe de leur PC professionnel avec des collègues[8]

Sensibilisation à la sécurité

Nous proposons également des produits de formation en ligne qui combinent une expertise en matière de cybersécurité aux meilleures technologies et pratiques d'apprentissage. Cette approche permet de changer le comportement des utilisateurs et de créer un environnement de cybersécurité sûr dans toute l'entreprise.

Notre plateforme de formation propose un programme automatique qui peut être paramétré en 10 minutes seulement. Les salariés sélectionnés par groupes, reçoivent ensuite des emails à intervalle régulier les invitant à se rendre sur la plateforme pour suivre les différents modules :

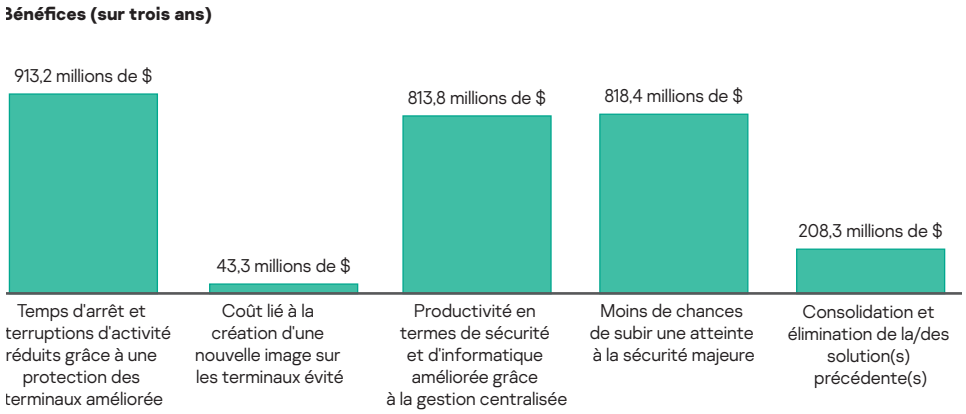
- modules d'apprentissage
- renforcement des compétences email
- tests
- simulations d'attaques par phishing

Vous pouvez suivre la progression de vos utilisateurs via un tableau de bord convivial, comprenant l'état d'avancement des formations ainsi que des conseils sur la manière de motiver les participants et d'optimiser vos résultats.

Pour en savoir plus sur Kaspersky Security Awareness, rendez-vous sur : https://www.kaspersky.fr/enterprise-security/security-awareness

Votre retour sur investissement

Comme pour toute solution, vous devez évaluer les coûts par rapport aux bénéfices que nous offrons. Vous trouverez ci-dessous un exemple de retour sur investissement type des solutions Kaspersky, s'appuyant sur une étude Forrester[7] portant sur Kaspersky Endpoint Security for Business :

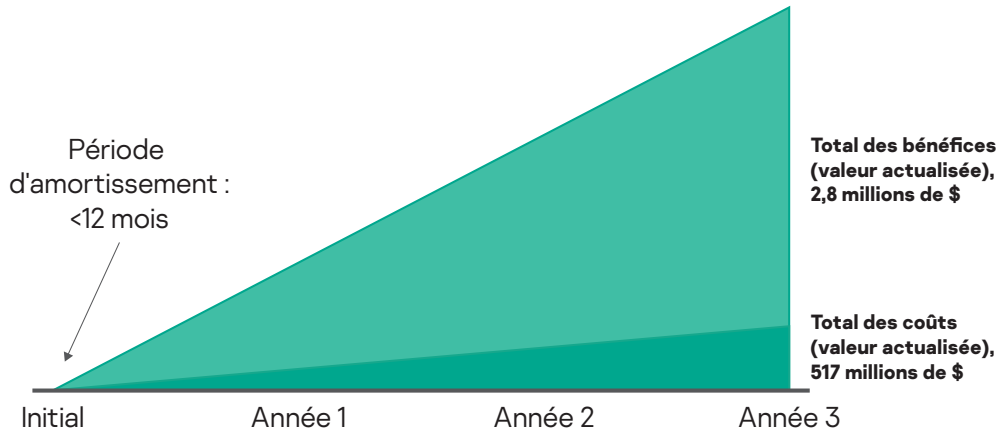


Les entretiens de Forrester avec les clients existants et l'analyse financière ultérieure ont révélé qu'une entreprise générait des bénéfices s'élevant à 2,8 millions de dollars sur trois ans pour un coût de 500 000 dollars et à un retour sur investissement de 441 %.

La valeur actualisée ajustée en fonction du risque (PV) a chiffré les bénéfices réalisés par les entreprises interrogées pour l'étude Forrester :

- **Près d'1 million de dollars :** l'impact financier engendré par l'amélioration de la disponibilité au niveau du terminal grâce à un nombre réduit d'interruptions.
- **Plus de 40 000 dollars :** le nombre réduit d'incidents liés à la sécurité a permis une hausse de la productivité informatique en diminuant le besoin de créer une nouvelle image sur les terminaux.
- **Plus de 800 000 dollars :** une gestion simplifiée de multiples solutions de sécurité grâce à une console d'administration centralisée, permettant des gains de productivité.
- **Plus de 800 000 dollars :** une amélioration significative de l'ensemble du système de sécurité a réduit les chances d'être victime d'une atteinte à la sécurité « majeure ».
- **Plus de 200 000 dollars :** les économies associées à la mise en œuvre d'une solution Kaspersky.

Résumé financier



7 Étude Total Economic Impact™ des solutions de sécurité Kaspersky, Forrester, 2020

8 Mettre de l'ordre dans le fouillis numérique, Kaspersky, 2019

En résumé

La protection des terminaux est essentielle pour protéger votre entreprise. Et le meilleur moyen de protéger vos terminaux est de disposer d'une solution multi-niveaux, utilisant différentes techniques pour détecter et répondre aux menaces d'une manière hautement automatisée, tout en permettant une intervention humaine pour les tâches plus complexes et les décisions importantes.

La solution intégrée Kaspersky Endpoint Security a été spécifiquement conçue pour gérer le besoin des organisations en termes de protection contre les menaces basiques, les attaques avancées et ciblées et les erreurs humaines grâce à :

- la mise en place d'une **stratégie de protection, de détection et de réponse intégrée et multi-niveaux**
- l'**automatisation** de vos défenses, en réduisant le temps et les efforts requis pour répondre, même aux attaques ciblées et avancées
- l'obtention des **plus hauts niveaux de détection**
- le développement **d'une culture de la cybersécurité via des contrôles et une sensibilisation à la sécurité**
- l'assurance d'un **retour sur investissement notable**

Tout cela signifie que vous pouvez profiter des plus hauts niveaux de sécurité, même contre les cybermenaces les plus complexes, sans monopoliser de ressources précieuses.

Pour en savoir plus sur la manière dont Kaspersky Endpoint Security peut aider à sécuriser votre organisation contre les attaques complexes sans mettre vos ressources sous pression, rendez-vous sur https://www.kaspersky.fr/enterprise-security/endpoint

www.kaspersky.fr