KASPERSKY lab

ASSISTONS-NOUS À UNE RÉVOLUTION EN MATIÈRE DE SÉCURITÉ INFORMATIQUE ...OU EST-CE JUSTE UNE UTOPIE ?

Comment évaluer les différentes solutions de sécurité informatique, faire la distinction entre les faits et la surmédiatisation et enfin, choisir le produit dont votre activité a besoin

www.kaspersky.fr

Si vous faites le point sur votre stratégie de sécurité informatique, afin de déterminer si elle vous protège suffisamment bien contre les menaces et les attaques actuelles complexes dont le nombre augmente considérablement chaque jour, vous constaterez que nombreux sont les fournisseurs de solutions de sécurité prêts à se battre pour répondre à vos besoins.

Cependant, comment vous assurez-vous qu'un produit peut vous offrir la meilleure protection possible ? Quelles sont les méthodes qui pourraient porter atteinte à votre productivité ? Quelles sont les fonctionnalités qui pourraient créer des failles dans votre sécurité ? Et enfin, quelle est la stratégie de sécurité la mieux adaptée pour répondre aux besoins spécifiques de votre activité ?

En général, lorsqu'il est question de stratégie informatique, il convient tout d'abord de faire la distinction entre les faits et la surmédiatisation et de déterminer quelles sont les technologies qui tiennent leurs promesses en termes de résultats.

SANS CELA, VOUS RISQUEZ D'ÊTRE PERDANT À PLUSIEURS ÉGARDS

Du fait du développement continu, tant sur le plan du volume que de la sophistication des programmes malveillants, des cyberattaques et de la cybercriminalité, les risques encourus par vos activités se multiplient. Par conséquent, il n'a jamais été aussi essentiel que vous choisissiez la solution de sécurité la plus performante.

Il n'est pas seulement question de savoir quelle part de votre budget informatique vous allez dépenser. Le choix d'une solution de sécurité inadaptée peut entraîner des conséquences onéreuses et durables pour n'importe quelle activité :

- Les attaques de ransomwares consistent à chiffrer les données sensibles ou stratégiques d'une entreprise, provoquant ainsi l'interruption des processus métier quotidiens.
- La fuite d'informations confidentielles concernant des clients peut porter atteinte à la qualité de la relation clientèle, entraîner des pertes sur le plan des ventes et avoir pour conséquence une action en justice intentée par les personnes lésées.
- La perte de données de conception et liées à toute autre forme de propriété intellectuelle peut affaiblir l'avantage concurrentiel durement gagné d'une entreprise.

Une enquête menée auprès de 5 500 entreprises dans 26 pays différents a révélé que :

- **90 % d'entre elles avaient déjà été victimes d'un incident lié à la sécurité**
- **46 % d'entre elles avaient perdu des données sensibles suite à une menace de sécurité**

Source : Enquête sur les risques informatiques mondiaux pour les entreprises, Kaspersky Lab

POURQUOI LES ENTREPRISES RESTENT-ELLES VULNÉRABLES ?

Les solutions de sécurité informatique existent bien évidemment depuis plusieurs années. De ce fait, comment est-il possible que les entreprises soient encore la proie des pirates informatiques ? Les raisons sont multiples.

Les criminels savent depuis bien longtemps qu'ils peuvent tirer beaucoup d'argent de leurs cyberattaques contre les entreprises, c'est pourquoi ils consacrent de plus en plus de temps et d'énergie à mettre au point des techniques toujours plus astucieuses. L'appât du gain est tout simplement bien trop alléchant pour que les cybercriminels interrompent leurs activités. Par conséquent, ils essaieront toujours de jouer au plus fin lorsqu'il s'agit de déjouer les technologies de sécurité existantes.

Ensuite, cela peut s'expliquer par le rôle qu'ont joué de nombreuses entreprises victimes de cyberattaques.

LA FAUTE VIENDRAIT-ELLE DES ENTREPRISES ELLES-MÊMES ?

Certaines d'entre elles ont en effet supposé, à tort, qu'elles ne seraient jamais visées par les pirates informatiques. C'est d'ailleurs pour cette raison qu'elles n'ont pas mis en place de mesures de sécurités suffisamment élevées pour assurer la protection de leurs données. Malheureusement, toutes les entreprises sont des cibles potentielles. Même le vol de données sensibles sur les clients ou les employés peut représenter un bénéfice pour les cybercriminels : cela peut entraîner des pertes financières et porter atteinte à la réputation des entreprises qui ont été prises pour cibles.

D'autres entreprises ont probablement décidé d'investir dans des solutions de sécurité afin de protéger des domaines essentiels de leur infrastructure informatique, mais en ont laissé d'autres de côté par mégarde et les ont ainsi rendu vulnérables aux cyberattaques.

Pire encore, certaines entreprises ont placé toute leur confiance dans des technologies prétendument « miraculeuses » et prometteuses mais dont les performances annoncées étaient bien loin de la réalité.

Cette dernière catégorie est particulièrement inquiétante, car elle implique que les entreprises ont été victimes de leur zèle en matière de marketing. Ainsi, après avoir été aveuglées par un faux sentiment de sécurité, du fait de déclarations mensongères à propos d'une nouvelle technologie, peut-être les entreprises ont-elles décidé d'abandonner les systèmes de sécurité éprouvés qui avaient préalablement assuré la protection de leurs données.

Malheureusement, ce scénario est la preuve que certaines entreprises sont prêtes à préférer aux faits des déclarations assorties d'un nombre insuffisant d'arguments pour les rendre valables. Par conséquent, pourquoi les entreprises agissent-elles de la sorte ?

EN FIN DE COMPTE, QUI REMPORTE LA BATAILLE ?

Le combat que se livrent les cybercriminels et les fournisseurs de solutions de sécurité informatique dure depuis de nombreuses années. Tant que cet affrontement continue de faire rage, il constitue une véritable distraction pour les entreprises : ces dernières souhaitant en effet se concentrer exclusivement sur leurs activités principales, développer de nouveaux produits ou services, fidéliser de nouveaux clients et augmenter leur part de marché. La cybercriminalité, et par extension, la sécurité informatique, peuvent alors représenter des distractions inutiles, car elles phagocytent le temps que les entreprises aimeraient consacrer à leurs autres activités.

En conséquence, elles sont fortement tentées de repenser au bon vieux temps, cette période où il n'était même pas question de cyberattaques ou de risques liés à la sécurité informatique. Cependant, le fait de regarder en arrière n'empêchera certainement pas les pirates informatiques de s'adonner à leurs activités criminelles.

LA FRUSTRATION OUVRE LA VOIE À UNE MAUVAISE PROTECTION

Toute nouvelle solution de sécurité promettant d'éradiquer « une fois pour toutes » tous les problèmes liés à la sécurité informatique, sans même proposer de mises à jour ni de surveillance permanente, pourrait constituer la planche de salut de tout dirigeant d'entreprise.

Seulement, ces remèdes miracles n'existent pas et ce n'est pas parce qu'on souhaite décrocher la lune qu'on parviendra à l'attirer jusqu'à soi.

Cependant, lorsqu'il est question de déclarations impressionnantes sur des produits de sécurité, le désir de bâtir un environnement professionnel plus sécurisé peut amener certaines entreprises à prendre des décisions inconsidérées et cela peut s'avérer dangereux. Et d'autant plus périlleux si une entreprise a récemment déploré un incident de sécurité et qu'elle a décidé, en toute hâte, d'adopter une nouvelle stratégie de protection des données, parfois sans même se donner le temps et les moyens nécessaires pour étudier les différentes options proposées par les fournisseurs dans ce domaine.

LES PRODUITS DE SÉCURITÉ DE DERNIÈRE GÉNÉRATION : UNE SOLUTION ENVISAGEABLE ?

Le fait d'ajouter les mots « dernière génération », parfois appelée « Next Gen », au début de n'importe quelle catégorie de produits peut contribuer à générer une image forte de la technologie concernée. Soyons honnêtes, qui voudrait d'un produit dit de la « première génération » alors que les produits de dernière génération sont déjà disponibles et qu'ils promettent monts et merveilles à leurs futurs utilisateurs ?

Malheureusement, les équipes marketing de certains fournisseurs semblent avoir tout saisi de la puissance des mots percutants et savent les utiliser pour charmer les personnes peu méfiantes.

De quoi est-il alors réellement question lorsqu'on parle de « produits de sécurité de dernière génération » ?

Il n'existe pas de norme ANSI ou ISO qui définisse les critères que doit réunir un produit de sécurité pour qu'il puisse porter la dénomination « dernière génération ». Par conséquent, vous devez approfondir votre analyse pour vérifier ce qui se cache derrière les mots « Next Gen » : parfois, cette appellation sera tout simplement l'œuvre d'une équipe marketing et prendra la forme d'une phrase « accrocheuse » laissant entendre que le produit de sécurité en question est doté d'une technologie avancée et qu'il est simple d'utilisation.

LA SÉCURITÉ SE CONSTRUIT AU FIL DU TEMPS MAIS ELLE A BESOIN DE FOURNISSEURS QUI RESPECTENT LEURS ENGAGEMENTS

Il n'existe pas de substitut à une protection basée sur les données de sécurité avancées. Cependant, comme les informations de sécurité ont besoin d'être prises en charge par une importante équipe d'experts en sécurité et en analyse des menaces, répartis à travers le monde, un très faible nombre de fournisseurs de solutions de sécurité peuvent se permettre de consentir à un tel investissement.

Quant aux fournisseurs qui peuvent se permettre d'investir dans des données de sécurité mondiales, les meilleures équipes déploient également des moyens considérables pour anticiper les nouvelles menaces et déterminer quelles sont les améliorations potentielles que les cybercriminels apporteront à leurs techniques, et ce pour que les solutions de sécurité soient opérationnelles et prêtes à repousser les attaques d'un nouveau genre.

Bien qu'il soit possible de donner **l'impression** que les produits Next Gen sont fantastiques, la réalité concernant les solutions de sécurité informatique est parfois tout autre. Les fournisseurs qui proposent des dispositifs de sécurité très stricts admettent que ce n'est pas une mince affaire. Cela prend du temps, de l'énergie, de l'argent et demande une très grande expertise. En somme, personne ne peut résoudre le problème d'un coup de baguette magique.

LES DIFFÉRENTES MENACES EXISTANTES DÉTERMINENT LA STRATÉGIE DE SÉCURITÉ QUE VOUS ALLEZ ADOPTER

Il est primordial que toutes les entreprises se prémunissent contre l'ensemble des cybermenaces existantes :

- Les menaces connues
- Les menaces inconnues
- Les menaces avancées

Cet arsenal de menaces requiert une approche multi-niveaux pour assurer la protection des données de l'entreprise.

Les entreprises sont incapables de prédire exactement les attaques dont leurs systèmes de sécurité seront la cible. Par conséquent, si une entreprise place tous ses espoirs dans une solution Next Gen unique, elle se rend extrêmement vulnérable.

Étant donné que les cybercriminels ne cessent de mettre tout en œuvre pour déjouer les systèmes de sécurité des entreprises, il n'est pas raisonnable de se satisfaire d'un seul niveau de sécurité. En mettant en place plusieurs niveaux de sécurité superposés, si une menace parvient à passer outre l'un de vos boucliers, les autres lignes de défense seront prêtes à vous offrir la protection dont vous avez besoin.

LES RESSOURCES DONT VOUS DISPOSEZ DÉTERMINENT LE SYSTÈME DE GESTION DE LA SÉCURITÉ QUE VOUS ALLEZ METTRE EN PLACE

Aucune activité ne souhaite consacrer trop de temps à la gestion de la sécurité. Par conséquent, il est également important de se procurer une solution de sécurité avec une console unique et intégrée vous permettant de configurer et de contrôler la sécurité de tous les terminaux, notamment les appareils et les serveurs de fichiers.

Ensuite, il est question de faire le choix entre une solution de sécurité avec une infrastructure de gestion sur site ou une autre avec une console basée dans le Cloud et ne nécessitant pas de serveur sur site. Dans la plupart des cas, les solutions de sécurité disposant de consoles sur site vous permettront d'effectuer un contrôle de sécurité d'une grande précision, mais leur mise en place et leur gestion requerront beaucoup de temps et de moyens.

A contrario, certaines solutions avec des consoles basées dans le Cloud peuvent simplifier grandement la gestion de votre sécurité informatique. Ces solutions sont particulièrement bien adaptées aux entreprises constituées d'équipes de gestion de la sécurité informatique relativement restreintes, voire aux entreprises souhaitant sous-traiter les tâches liées à la gestion de la sécurité informatique à un consultant externe.

Les solutions avec une console basée dans le Cloud peuvent vous apporter des bénéfices considérables :

- Comme la console se trouve dans le Cloud, il est inutile d'acheter, d'installer et de gérer un serveur sur site pour assurer la protection des données.
- La mise en service est particulièrement rapide.
- Les tâches de gestion relatives à la sécurité informatique nécessitent moins de temps et d'effort.
- Les tâches de gestion peuvent être accomplies depuis n'importe quel endroit et appareil disposant d'un accès à Internet.

LES MYTHES DU MARKETING CONCERNANT LES PRODUITS NEXT GEN

Passons en revue certaines des déclarations les plus insolites à propos des produits de sécurité de dernière génération.

Mythe n °1 : les antivirus traditionnels n'ont plus aucune utilité

C'est sans doute le plus grand mythe de tous. Si les antivirus basés sur les signatures ne vous protégeront pas contre les menaces inconnues ou avancées, ils constituent une protection essentielle de toute solution de sécurité informatique dotée de plusieurs lignes de défense. En effet, les antivirus traditionnels demeurent particulièrement efficaces pour bloquer les programmes malveillants connus. De plus, les solutions de sécurité actuelles les plus performantes utilisent la puissance du Cloud pour obtenir de nouvelles signatures plus rapidement pour que les entreprises soient protégées contre les programmes malveillants nouvellement identifiés.

On ne compte plus le nombre d'entreprises ayant appris à leurs dépens que le fait de faire l'impasse sur cet aspect essentiel de la sécurité informatique pouvait entraîner des incidents relativement onéreux et embarrassants. Combien de solutions de sécurité « miraculeuses » ont laissé passer des menaces ou bloqué à tort des entités bénignes, provoquant ainsi l'interruption des activités ?

Mythe n °2 : les mises à jour relatives à la sécurité « ruinent » la performance des services informatiques

Nous sommes tous capables de nous rappeler les tous premiers jours qui ont vu naître la sécurité informatique, une période où les mises à jour des antivirus pouvaient être particulièrement lentes, gênantes et porter atteinte à la performance des ordinateurs. Cependant, la situation a bien changé depuis cette époque.

Heureusement pour nous, il existe aujourd'hui des solutions de sécurité qui ont été conçues pour réduire les impacts pouvant affecter la performance des ordinateurs tout en renforçant leur sécurité grâce à des mises à jour régulières permettant de lutter contre les risques nouvellement identifiés. Elles actualisent également de façon indépendante les différents niveaux de protection existants afin d'assurer en permanence un service de défense élevé.

Mythe n °3 : les solutions de sécurité réduisant au maximum la connectivité permettent d'assurer un niveau de protection adéquat

Afin d'alléger la charge des ressources informatiques, certaines solutions se vantent de générer très peu de mises à jour de sécurité, et parfois de façon plutôt occasionnelle. Malheureusement, cela ne constitue pas la meilleure approche pour libérer de la bande passante sur le réseau de votre entreprise, ni même pour vous apporter un niveau de protection efficace dans vos activités.

Les mises à jour régulières, que ce soit pour les signatures servant à bloquer les programmes malveillants connus ou pour les modèles heuristiques détectant les menaces inconnues, sont essentielles afin de s'assurer que vos défenses sont en mesure de contrer rapidement les nouvelles menaces. De plus, ces mises à jour permettent également de réduire au maximum le taux de faux positifs et ainsi d'éliminer les interruptions inutiles et chronophages pouvant affecter vos activités.

La clé consiste à proposer ces mises à jour de façon à éviter tout impact négatif sur la productivité des utilisateurs.

Mythe n °4 : la révolution est arrivée et elle porte le nom Next Gen !

Lorsqu'il s'agit de protéger vos activités, la surmédiatisation et les slogans accrocheurs ne seront pas suffisants. Ce qui compte le plus, c'est la performance d'une solution qui a déjà fait ses preuves en matière de protection et cela n'a pas de prix lorsque les enjeux sont aussi importants. Pensez donc toujours à vérifier ce qui se cache derrière l'appellation « Next Gen ».

UNE PROTECTION BASÉE SUR DES RÉSULTATS ÉPROUVÉS

Nos clients nous font souvent la réflexion que Kaspersky Lab proposait déjà des solutions de dernière génération bien avant que nos concurrents ne le fassent. Cependant, du fait du flou qui entoure le terme « Next Gen » et des mauvaises interprétations pouvant en découler, nous ne souhaitons pas l'employer pour décrire nos produits.

Certaines personnes peuvent avoir le sentiment que notre apprentissage machine et nos experts en sécurité de renommée mondiale constituent véritablement ce qu'on appelle la « dernière génération ». Mais selon notre point de vue, nous procédons ainsi depuis de nombreuses années et l'un de nos engagements consiste à développer des solutions de sécurité de qualité supérieure, et ce sans avoir recours à des slogans accrocheurs.

Nous préférons nous en tenir aux faits, éviter la surmédiatisation, progresser dans notre mission consistant à nous montrer plus malins que les cybercriminels les plus ingénieux et enfin laisser les résultats que nous avons obtenus au cours de tests indépendants « parler d'eux-mêmes ».

Ces trois dernières années, nos technologies de sécurité ont participé au plus grand nombre de tests et obtenu les récompenses les plus prestigieuses. Lors d'une série complète de tests indépendants, nos produits ont remporté bien plus de prix et figuré bien plus souvent dans le http://www.kaspersky.fr/top3 que ceux de tout autre fournisseur.

PLUSIEURS NIVEAUX DE SÉCURITÉ DANS L'ENSEMBLE DE VOTRE INFRASTRUCTURE INFORMATIQUE

Notre approche en matière de sécurité est multi-niveaux : protection basée sur les signatures, analyses heuristiques et comportementales, fonctionnalité « Protection automatique contre l'exploitation des failles » et bien d'autres technologies avancées. Ces outils sont indispensables pour nous permettre d'être plus performants que nos concurrents.

De plus, grâce à notre réseau Cloud Kaspersky Security Network (KSN) fournissant des informations sur les menaces, nous proposons une réponse plus rapide aux nouvelles attaques.

Tout cela signifie que nous pouvons atteindre :

- Des taux de détection inégalés
- Des taux faibles de faux positifs

Nous proposons un large choix de solutions de sécurité professionnelles intégrées permettant de protéger l'ensemble de vos terminaux, notamment les ordinateurs de bureau, les ordinateurs portables, les serveurs de fichiers, les smartphones et les tablettes. Nous proposons également diverses options de sécurité spécialisées vous permettant de protéger vos systèmes de stockage, vos machines virtuelles, et bien d'autres encore.

Lors de tests indépendants ayant pour objectif d'identifier le nombre de « détections erronées de programmes légitimes en tant que programmes malveillants pendant une analyse du système », les technologies de Kaspersky Lab ont atteint zéro faux positifs.

Les tests ont été réalisés en janvier et février 2016 par l'Institut AV-TEST.

CHOISIR VOTRE SOLUTION DE SÉCURITÉ

Kaspersky Endpoint Security Cloud a été conçue pour répondre aux besoins de sécurité spécifiques des PME, en particulier des entreprises disposant d'équipes restreintes pour gérer la sécurité informatique. Idéale pour les PME, la solution propose :

- Une protection pour les ordinateurs de bureau et les ordinateurs portables Windows, les serveurs de fichiers Windows et les appareils mobiles iOS et Android*

- Une simplicité de gestion, via une console Cloud qui :
  – Permet d'économiser du temps et de l'argent, en supprimant la nécessité d'un serveur dédié
  – Simplifie le déploiement initial, en fournissant des fonctions de sécurité « prêtes à l'emploi »

- Des licences flexibles : licence annuelle ou abonnement mensuel vous permettant d'ajuster votre protection en fonction de vos besoins
  *La fonctionnalité varie pour d'autres appareils et plates-formes.

Kaspersky Endpoint Security for Business offre une protection très précise pour les organisations ou entreprises plus grandes nécessitant des systèmes de sécurité particulièrement performants. Elle prend en charge de nombreuses plates-formes :

- Ordinateurs de bureau et ordinateurs portables : Windows, Mac et Linux
- Serveurs de fichiers : Windows, Linux et FreeBSD
- Appareils mobiles : Android, iOS et Windows

QUELLE EST LA PROCHAINE ÉTAPE ?

La prochaine fois qu'un fournisseur vous propose une solution de sécurité Next Gen, assurez-vous de lui demander des résultats de tests indépendants pour vérifier la qualité de ses technologies de sécurité dans le monde réel.

En attendant, vous avez pu constater ce que les produits de sécurité Kaspersky Lab ont pu obtenir comme résultats au cours des trois dernières années lors de tests indépendants. Par conséquent, pourquoi ne pas évaluer notre sécurité dès maintenant et essayer nos solutions directement sur vos ordinateurs et appareils mobiles ?

Pour obtenir la version d'essai GRATUITE, valable 30 jours, de Kaspersky Endpoint Security Cloud, accédez à la console Cloud en ligne via le lien suivant : cloud.kaspersky.com

ANNEXE 1

Exemples d'entreprises et leurs solutions de sécurité de prédilection Kaspersky Lab

Nous allons maintenant étudier trois types d'entreprises différents, évaluer leurs besoins en matière de sécurité et enfin déterminer quelle solution Kaspersky Lab correspond le mieux à leurs exigences opérationnelles respectives.

ENTREPRISE A

- PME spécialisée dans le conseil, 60 salariés
- Les salariés travaillent à distance ou occupent des postes de travail partagés
- Ordinateurs portables, téléphones et tablettes sont essentiels pour accomplir les différentes tâches professionnelles
- La polyvalence des fonctions implique une importante utilisation d'Internet
- Les travailleurs temporaires, notamment les stagiaires et les sous-traitants, ont probablement besoin d'avoir accès aux informations confidentielles de l'entreprise pour une durée maximale de 6 mois
- Pas d'équipe informatique en interne : l'entreprise emploie un consultant informatique externe qui dispose d'une expérience limitée en matière de gestion de la sécurité informatique
- Infrastructure informatique relativement limitée
  - Utilisation de serveurs informatiques basés dans le Cloud, pas d'exécution de serveurs internes
  - Les petits systèmes habituels de bureau sont utilisés pour imprimer, stocker, etc.
- Budget informatique limité
  - La plupart des employés utilisent leurs propres ordinateurs portables, smartphones et tablettes

CE QUE L'ENTREPRISE DOIT ATTENDRE DE SA SOLUTION DE SÉCURITÉ

- Une protection rigoureuse contre les cybermenaces
- Une gestion simplifiée de la sécurité, sans même avoir besoin de compétences spécialisées en sécurité, afin de s'assurer qu'une personne externe chargée du support informatique puisse gérer en toute simplicité la sécurité de l'entreprise
- Des licences simples : paiement annuel en ligne
- Pas besoin de réaliser des dépenses supplémentaires en équipement informatique
- La capacité à protéger un large éventail d'appareils : différents modèles d'ordinateurs portables, tablettes et téléphones (appareils iOS pris en charge également)
- L'évolutivité en toute simplicité : déploiement de la sécurité sur les ordinateurs et appareils mobiles des nouveaux arrivants

LA SOLUTION KASPERSKY LAB IDÉALE

Kaspersky Endpoint Security Cloud, licence annuelle

- Protège contre les menaces avancées, inconnues ou connues
- Propose une console basée dans le Cloud facile d'utilisation pour une gestion simplifiée de la sécurité
- Simplifie le processus des licences : les licences annuelles peuvent être installées et renouvelées en ligne
- Permet de réduire les coûts. Comme la console d'administration se trouve dans le Cloud, il est inutile d'acheter, d'installer et de gérer un serveur sur site dédié à la gestion de la sécurité
- Compatible avec les ordinateurs Windows, les iPhones, iPads, téléphones et tablettes Android
- S'adapte aux besoins évolutifs en matière de sécurité. Lorsque de nouveaux employés rejoignent l'entreprise, la console basée dans le Cloud permet de déployer en toute simplicité la solution de sécurité sur les ordinateurs et appareils mobiles supplémentaires

Kaspersky Endpoint Security Cloud offre à l'Entreprise A la combinaison adéquate entre sécurité et facilité d'utilisation, sans même avoir besoin d'acheter d'équipement informatique supplémentaire ni même d'investir dans une formation à la sécurité informatique. L'administration simplifiée, rendue possible grâce à une console basée dans le Cloud, permet à l'entreprise de faire appel à un consultant externe en toute simplicité afin qu'il installe et gère la solution de sécurité sur tous les ordinateurs, téléphones et tablettes au sein de l'organisation.

ENTREPRISE B

- Une entreprise de construction qui souhaite se développer et prendre en charge de nouveaux projets dans 10 villes éloignées pour les 3 prochaines années
- Elle emploie actuellement 100 personnes mais ce chiffre augmentera au cours des 12 prochains mois
- Chaque nouveau projet nécessitera d'ajouter du personnel : chefs de chantier, fonctions achat, etc.
- Le nombre de travailleurs temporaires évoluera en fonction de la phase du projet en cours
- La plupart des salariés travaillent à distance la majeure partie du temps
- La polyvalence des fonctions implique une importante utilisation d'Internet
- Un très grand nombre de travailleurs temporaires, notamment des chefs de projet et des sous-traitants spécialisés dans un domaine, ont besoin d'avoir accès aux informations confidentielles de l'entreprise pendant 6 à 12 mois
- Il n'existe pas de budget distinct pour étendre la sécurité nécessaire pour couvrir le nombre des futurs employés. Au lieu de cela, les coûts sont appliqués au sein de chaque projet que la firme obtient
- 1 responsable informatique à temps plein
- Infrastructure informatique relativement limitée :
  - Serveurs informatiques basés dans le Cloud, pas de serveur interne
  - Petits systèmes habituels de bureau utilisés pour imprimer, stocker, etc.
- Budget informatique limité
  - La plupart des employés utilisent leurs propres ordinateurs portables, smartphones et tablettes

Ce que l'entreprise doit attendre de sa solution de sécurité

- Une gestion simplifiée de la sécurité, sans même avoir besoin de compétences spécialisées en sécurité, afin de s'assurer qu'une personne externe chargée du support informatique puisse gérer en toute simplicité la sécurité de l'entreprise
- Pas besoin de réaliser des dépenses supplémentaires en équipement informatique
- Pas d'exigence en matière de planification d'un budget de sécurité informatique annuel. Au lieu de cela, la sécurité devrait être ajustable en fonction des nouveaux projets obtenus
- Évolutivité immédiate, sans avoir besoin de gérer des licences ou des contrats complexes. Au lieu de cela, la solution devrait permettre de payer immédiatement tout ajout de nouveaux utilisateurs
- Capacité à protéger un large éventail d'appareils : différents modèles d'ordinateurs portables, tablettes et téléphones (appareils iOS pris en charge également)
- Capacité à gérer plusieurs modèles d'utilisation différents, permettant ainsi diverses politiques de sécurité d'être appliquées pour des fonctions professionnelles différentes

La solution Kaspersky Lab idéale

Kaspersky Endpoint Security Cloud, licence mensuelle

- Protège contre les menaces avancées, inconnues ou connues
- Propose une console basée dans le Cloud facile d'utilisation pour une gestion simplifiée de la sécurité
- Permet de réduire les coûts. Comme la console d'administration se trouve dans le Cloud, il est inutile d'acheter, d'installer et de gérer un serveur sur site dédié à la gestion de la sécurité
- Il n'est pas utile de fixer un budget annuel ou d'acheter une licence annuelle. Une licence mensuelle est suffisante car elle permet à l'entreprise d'ajuster le nombre d'utilisateurs qu'elle protège. Par conséquent, la firme peut augmenter ou diminuer le nombre d'utilisateurs tous les mois
- Compatible avec les ordinateurs Windows, les iPhones, iPads, téléphones et tablettes Android
- Des politiques individuelles peuvent être configurées à partir de la console basée dans le Cloud
- S'adapte aux besoins évolutifs en matière de sécurité. Lorsque de nouveaux employés rejoignent l'entreprise, la console basée dans le Cloud permet de déployer en toute simplicité la solution de sécurité sur les ordinateurs et appareils mobiles supplémentaires

Étant donné que l'évolutivité économique et rapide représente un facteur essentiel de l'entreprise B, le modèle d'abonnement mensuel pour Kaspersky Endpoint Security Cloud constitue le choix idéal. Il n'est pas nécessaire de payer à l'avance une licence annuelle. Au lieu de cela, il suffit que l'entreprise ajoute de nouveaux utilisateurs ou en réduise le nombre en fonction de ses besoins. En procédant ainsi, l'entreprise peut disposer d'une solution de sécurité flexible qui lui permet également de contrôler ses coûts.

ENTREPRISE C

- Entreprise spécialisée dans le développement de logiciels en B2B, 500 employés
- Prévoit une augmentation de son personnel de 30 % au cours des 12 prochains mois
- Planifie efficacement ses programmes de recrutement : développeurs, testeurs, experts en technologie, personnel de vente et d'avant-vente, et bien d'autres encore
- La plupart des employés travaillent en interne sur le réseau local de l'entreprise
- Les cadres supérieurs traitent des données clients confidentielles qui doivent être stockées de façon sécurisée
- Infrastructure informatique interne très développée : serveurs, stockage, sous-systèmes, réseau local, etc.
- Utilise une grande variété de plates-formes informatiques : Windows Server pour la production, Linux pour la gestion du réseau et des ordinateurs Mac pour la conception
- Des ordinateurs portables standardisés sont remis aux employés par l'entreprise et leur gestion est assurée par l'équipe informatique interne
- Un budget informatique dédié est réalisé tous les ans
- Besoin permanent d'adopter de nouvelles technologies afin d'augmenter le potentiel commercial de l'entreprise
- Une équipe informatique interne très spécialisée gère l'infrastructure informatique de l'entreprise
- Du fait de la grande diversité de fonctions au sein de l'entreprise, notamment des développeurs, managers, personnel en contact direct avec la clientèle, employés administratifs, personnel du back-office etc., l'entreprise a besoin de pouvoir mettre en place et gérer de nombreuses politiques de sécurité différentes

Ce que l'entreprise doit attendre de sa solution de sécurité

- Fonctionnalités de sécurité avancées pouvant être gérées par les experts de la sécurité informatique internes de l'entreprise
- Peut être déployée intégralement au sein du réseau local de l'entreprise
- Compatible avec une grande variété de plates-formes : Windows, Linux et Mac
- Assistance pour la gestion des appareils mobiles
- Prise en charge d'un très grand nombre de politiques de sécurité différentes : outils de contrôle du Web, restrictions de démarrage des applications, etc.
- Chiffrement avancé afin de protéger les données sensibles

La solution Kaspersky Lab idéale

Kaspersky Endpoint Security for Business ADVANCED

- Protège contre les menaces avancées, inconnues ou connues
- Offre des fonctionnalités de sécurité plus avancées, notamment des outils de contrôle flexibles
- Toutes les fonctions d'administration de la sécurité et de protection des terminaux s'exécutent localement
- La console de gestion unique et unifiée pour tous les appareils pris en charge s'exécute via un serveur sur site
- Protège Windows, Linux et Mac
- Comprend la gestion des appareils mobiles (MDM)
- Propose des contrôles des politiques performants qui permettent de traiter des ensembles complexes de politiques de sécurité
- Comprend une fonctionnalité flexible de chiffrement des données

L'entreprise C dispose d'une infrastructure informatique plus complexe, avec une grande variété de plates-formes devant être protégées, notamment sur des ordinateurs Windows, Mac et Linux. De plus, l'entreprise a besoin de fonctionnalités supplémentaires de sécurité, telles que le chiffrement des données et des outils de contrôle flexibles, c'est pourquoi Kaspersky Endpoint Security for Business ADVANCED constitue la solution parfaite. Cette option offre également à l'entreprise un contrôle encore plus approfondi de la sécurité informatique. Ainsi, l'équipe informatique interne de l'entreprise peut mettre en place des politiques de sécurité individuelles correspondant à la grande variété de fonctions de la société.