Gérer la complexité croissante de l'informatique

Rapport 'IT Security economics' 2021 : résumé

kaspersky BRING ON THE FUTURE

Plus d'informations sur kaspersky.fr

Sommaire

Introduction

Dans le rapport IT Security Economics de l'année passée, nous avons établi que 2020 était l'année du changement. Ce changement s'est poursuivi, et s'est même accru cette année, avec la modification permanente qui a touché les modèles de travail et le fonctionnement des entreprises.

En 2021, les entreprises ont adopté un modèle de travail hybride en demandant à leurs salariés de travailler parfois au bureau ou parfois depuis leur domicile. Il a fallu que les entreprises sécurisent leurs réseaux sur les nouveaux ordinateurs portables et tablettes du personnel, qu'elles configurent des réseaux privés virtuels (VPN), qu'elles migrent sur des serveurs dans le cloud et qu'elles approuvent rapidement les nouveaux logiciels de collaboration.

Cette adoption rapide et massive d'outils de télétravail a mis beaucoup de pression sur les équipes de sécurité, qui doivent protéger les réseaux d'entreprise sans compliquer le travail quotidien des salariés.

Notre étude met en évidence une tendance croissante en matière de cybersécurité pour 2021 : les équipes informatiques, à la fois dans les petites et les grandes entreprises, doivent faire face à une infrastructure informatique et à des environnements d'exploitation de plus en plus complexes. Aujourd'hui, elles doivent non seulement continuer à protéger les organisations contre les cybermenaces, mais elles doivent désormais y arriver à travers une infrastructure informatique plus distante, hybride et compliquée.

Dans le contexte actuel de gestion de la crise, les spécialistes de la sécurité informatique se concentrent également sur l'optimisation des budgets de sécurité. Cette année, l'utilisation efficace des ressources figure parmi les sujets les plus importants de leur liste depuis longtemps.

Malgré ces difficultés, nos données révèlent que les entreprises s'en sont plutôt bien sorties l'année passée et qu'elles améliorent leur résilience face aux violations de données. En fait, les petites et moyennes entreprises (PME) signalent une légère augmentation du coût des attaques de données, alors même que ces coûts sont en baisse pour les grandes entreprises.

Ce rapport met en lumière les aspects économiques de la sécurité informatique, en exposant les principales conclusions de l'étude de cette année et en analysant les changements dans les budgets, les violations et les défis de l'entreprise qui affecteront les décideurs de la sécurité informatique en 2021.

Méthodologie

L'Enquête mondiale de Kaspersky sur les risques liés à la sécurité informatique pour les entreprises (de laquelle st issu ce rapport) est une enquête internationale menée auprès de décideurs dans des entreprises informatiques

Au total, 4 303 entretiens avec des entreprises de plus de 50 salariés ont été menés dans 31 pays en mai-juin 2021. Les personnes interrogées ont été invitées à se prononcer sur l'état de la sécurité informatique au sein de leur organisation, sur les types de menaces auxquelles elles sont confrontées et sur les coûts qu'elles doivent supporter pour assurer un redressement après une attaque.

Tout au long du rapport, les entreprises sont appelées soit PME (petites et moyennes entreprises de 50 à 999 salariés), soit grandes entreprises (entreprises de plus de 1 000 salariés). Tous les résultats de l'enquête ne sont pas inclus dans ce rapport.

Principales conclusions

Coût des violations de données

105 000 $ pour les PME

927 000 $ pour les grandes entreprises

Budget de sécurité informatique

267 000 $ pour les PME

11,4 m $ pour les grandes entreprises

- Le coût des violations de données pour les PME a légèrement augmenté (105 000 $ en 2021, contre 101 000 $ en 2020), mais n'atteint toujours pas le point culminant de 2018 (120 000 $). Le coût d'une violation de données pour les grandes entreprises est tombé à 927 000 $, en dessous du précédent plancher de 992 000 $ en 2017.
- Les incidents impliquant le partage de données avec des fournisseurs ont été la violation la plus coûteuse pour les grandes entreprises, avec un impact total de 1,4 million de $ en 2021.
- Les grandes entreprises ont moins signalé les violations de données cette année : 34 % ont évité de le faire, contre 28 % en 2020.
- Les budgets de cybersécurité, prévus au milieu de la pandémie à la fin de 2020, ont diminué de façon spectaculaire pour les grandes entreprises, avec une chute de 19 % à 11,4 millions de $. Ce chiffre est à comparer aux 14 millions de $ de 2020. Pendant ce temps, les budgets de sécurité des PME n'ont que légèrement diminué, passant à 267 000 $ en 2021, contre 275 000 $ l'année dernière (soit une baisse de 3 %).
- La préoccupation numéro un des entreprises en matière de cybersécurité en 2021 est le besoin de budgets plus importants pour sécuriser des environnements de plus en plus complexes (44 %), alors qu'il se trouvait précédemment à la troisième place l'année dernière (41 %) et à la sixième place en 2018.

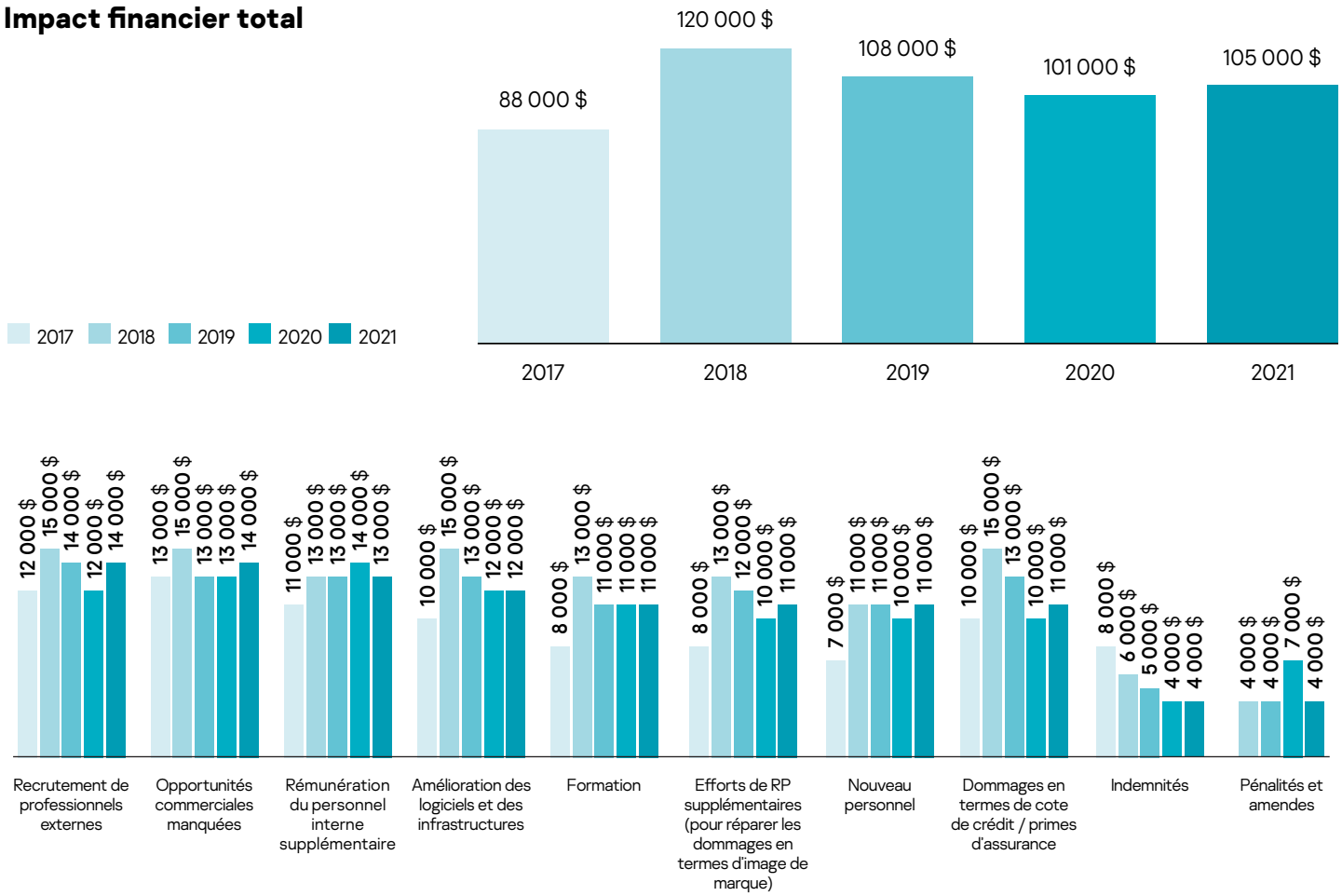
Anciennes menaces, coûts identiques, nouveaux défis

Cette année, les risques liés à la cybersécurité sont restés un grand sujet d'inquiétude pour les petites et les grandes entreprises, à cause des nouvelles menaces qui ont fait leur apparition pendant la pandémie et de la longue période de travail à distance qu'elle a entraînée.

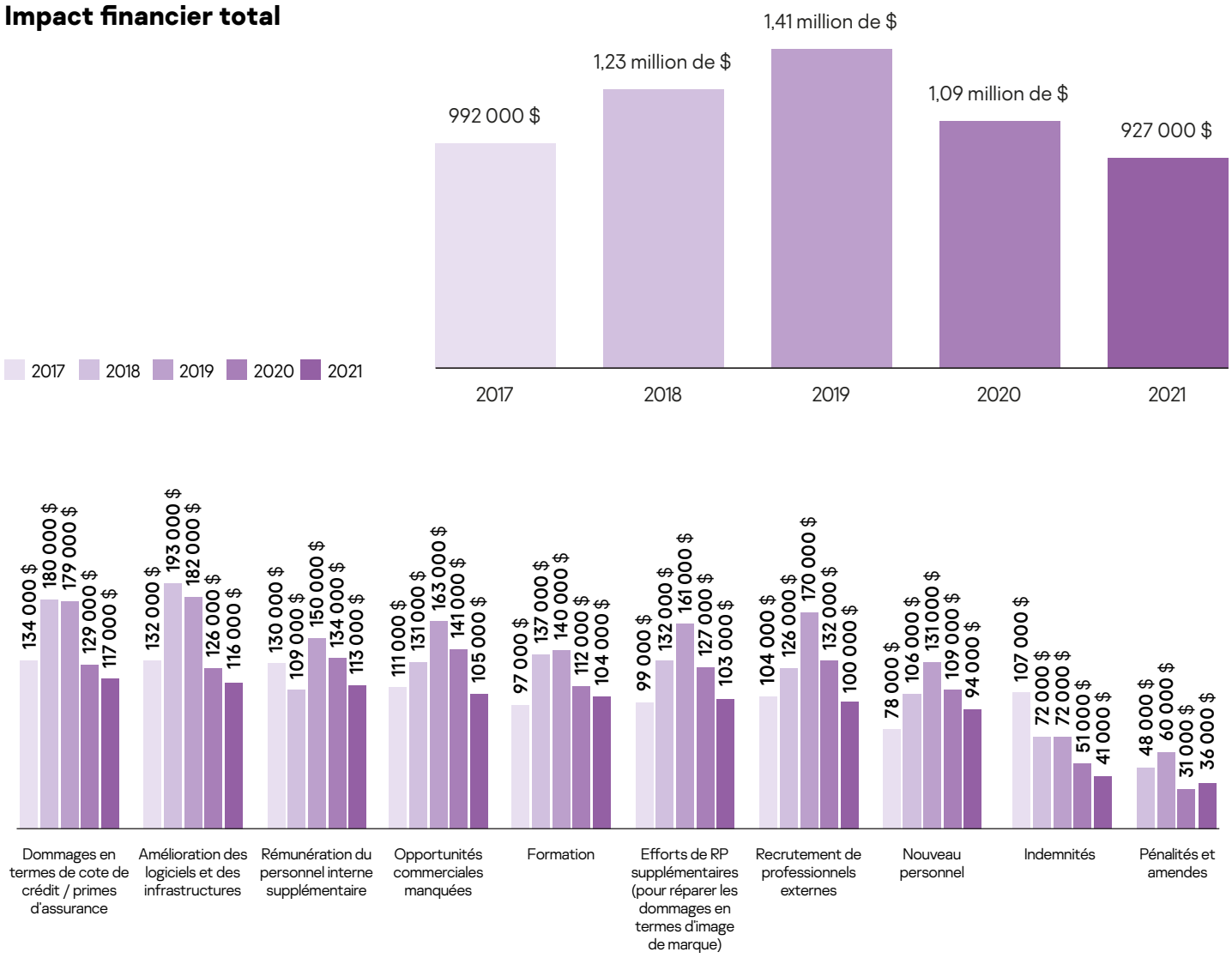
Pourtant, notre étude montre bien que, malgré ces nouvelles menaces, les coûts des violations de données n'ont pas excessivement augmenté en 2021.

En fait, l'impact financier des violations de données n'a connu qu'une légère augmentation de 4 % pour les PME (105 000 $ en 2021, contre 101 000 $ en 2020), et une baisse notable de 15 % pour les grandes entreprises. Pour ces grandes organisations, l'impact est passé de 1,09 million de $ en 2020 à 927 000 $, soit moins que le chiffre le plus bas enregistré en 2017 (992 000 $).

Graphique 1 : Suivi de l'impact financier d'une violation de données pour les PME



Graphique 2 : Impact financier total moyen d'une violation de données pour les entreprises.

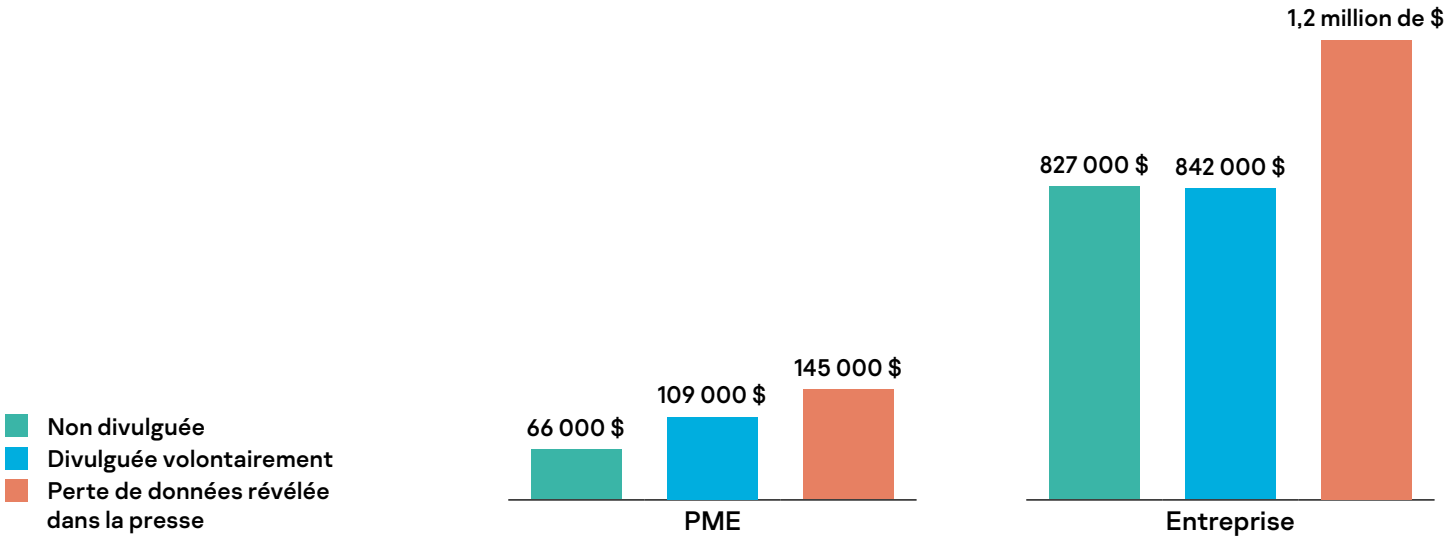


Une des principales raisons à cette baisse de l'impact financier des violations de données dans les entreprises pourrait être due aux améliorations apportées à la détection des attaques, ce qui minimise donc l'impact des violations. Cependant, notre étude a également révélé que les grandes entreprises étaient moins susceptibles de signaler les violations de données cette année, avec 34 % parvenant à éviter de le faire, contre seulement 28 % en 2020.

Cette réduction pourrait s'expliquer par le fait que les entreprises font preuve d'une plus grande proactivité dans l'élimination des conséquences des violations de données. Elles peuvent donc éviter une grande partie de l'impact des fuites et ont alors moins besoin de les signaler. Bien sûr, il est parfois impossible de cacher des attaques, par exemple, si la victime est une autorité publique ou une organisation qui fournit des services à l'État, comme ce fut le cas pour le système de prise de rendez-vous de vaccination contre le Covid-19 en Italie, **attaqué par un ransomware en été 2021**. Dans ces cas-là, lorsque l'attaque est révélée dans la presse, l'impact financier augmente considérablement.

Néanmoins, le nombre élevé d'entreprises ayant évité de divulguer des violations peut aussi signifier que certaines entreprises vulnérables au niveau financier sont réticentes à consacrer du temps et de l'argent à une enquête criminelle ou à risquer leur réputation si une violation est rendue publique.

Graphique 3 : Le coût moyen des violations de données



Changer de tactique face aux violations de données

Les violations de sécurité sont devenues des infractions moins répréhensibles en 2021, avec seulement 21 % de toutes les grandes entreprises ayant licencié des salariés pour cette raison en 2021, contre 24 % en 2020.

Notre étude a révélé que les cadres supérieurs (qu'ils fassent ou non partie de l'équipe informatique) sont moins susceptibles de se faire licencier. Les cadres dirigeants ont 4 % de chances d'être licenciés, contre 8 % pour ceux qui ont un poste fonctionnel en informatique. En parallèle, le nombre de responsables de la sécurité informatique seniors licenciés a diminué de près de la moitié, passant de 14 % en 2018 à 8 % en 2021.

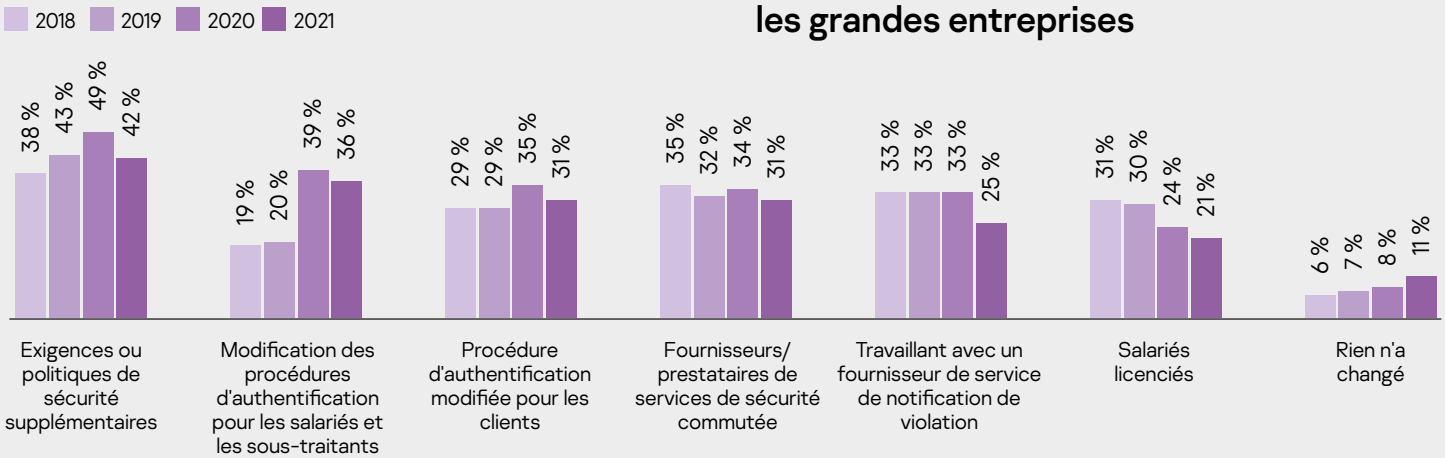
L'une des raisons possibles à ce changement est que, dans un environnement de cybersécurité difficile, les entreprises ont compris qu'elles devaient garder leurs experts en cybersécurité pour renforcer leurs compétences et leurs connaissances, au lieu de leur montrer la porte juste après un incident.

« Le passage vers le travail et les processus à distance a exercé une pression accrue sur le secteur de la sécurité des informations. Étant donné que les postes de cybersécurité sont très demandés et que les professionnels qualifiés sont rares, les entreprises accordent plus de valeur à leurs cadres de sécurité seniors et cherchent à combler les lacunes en matière de compétences », explique Evgeniya Naumova, Executive VP, Corporate Business chez Kaspersky.

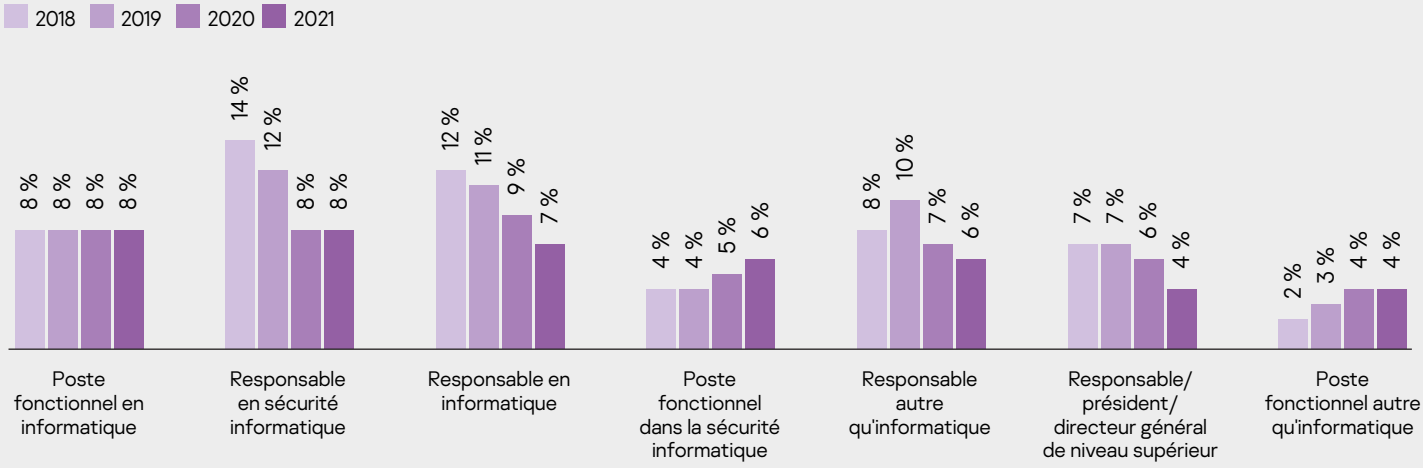
Cette année, l'étude a également révélé que les entreprises étaient moins susceptibles de recruter davantage d'analystes ou de spécialistes de la sécurité informatique en réponse aux incidents, passant de 47 % l'année dernière à 45 % en 2021. On note également une baisse notable du nombre de créations de nouvelles équipes ou services dédiés à la sécurité informatique, passant de 42 % en 2020 à 39 % cette année.

Au lieu de cela, plus d'un tiers des organisations (36 %) ont tendance à recruter des spécialistes qui ne relèvent pas du domaine de la sécurité informatique, mais qui ont des compétences en matière de droit, de conformité et de gestion des risques afin de les aider à faire face aux conséquences des violations ou à préparer un plan de crise si un autre incident se produit. Ce chiffre est corroboré par l'étude Gartner 2020 Board of Directors Survey qui prévoit que d'ici 2025, 40 % des conseils d'administration disposeront d'un comité dédié à la cybersécurité, supervisé par un administrateur qualifié.

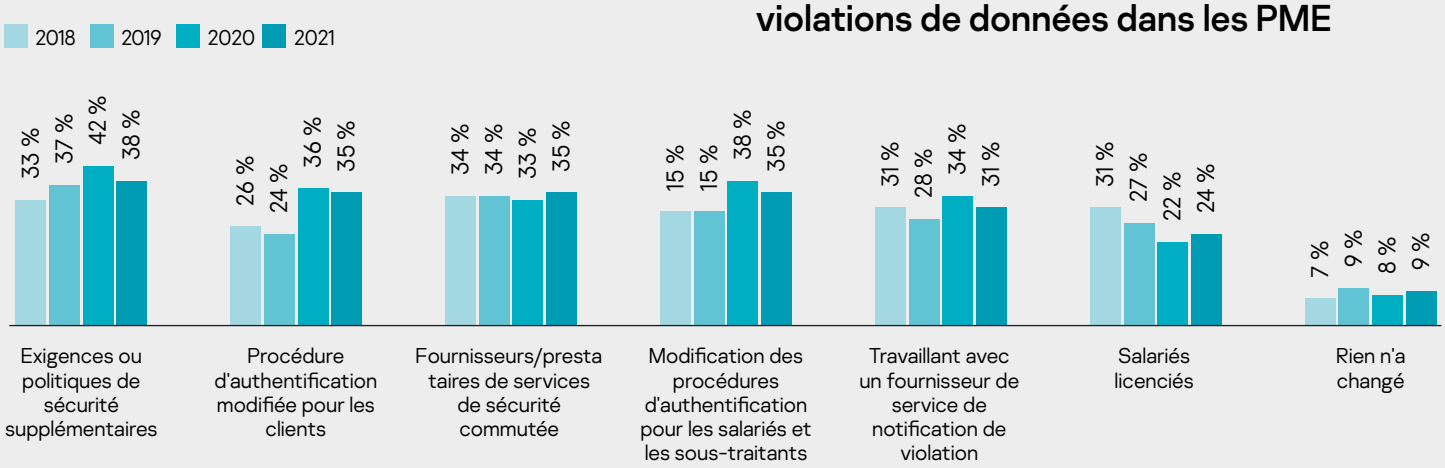
Graphique 4 : Changements apportés après des violations de données dans les grandes entreprises



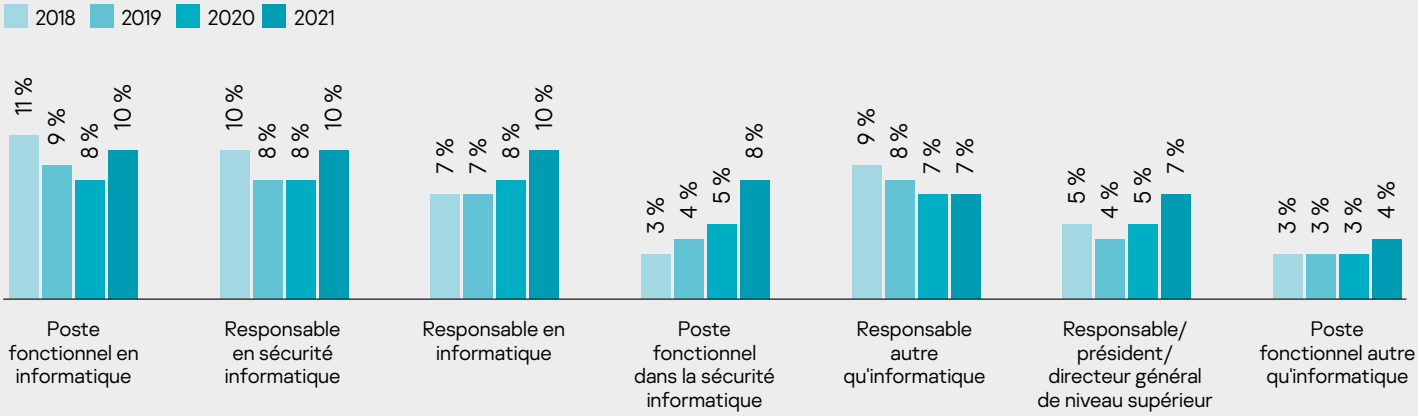
Graphique 5 : Salariés de grandes entreprises licenciés après une violation de sécurité



Graphique 6 : Changements apportés après des violations de données dans les PME



Graphique 7 : Salariés de PME licenciés à la suite d'une violation de sécurité



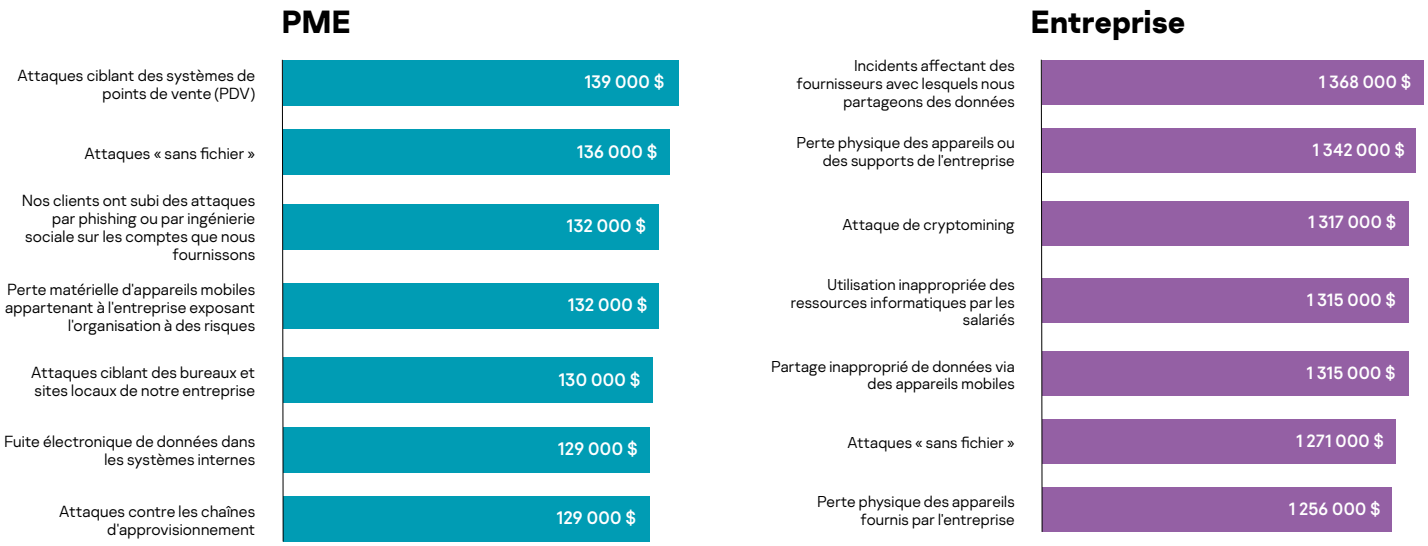
Les violations de données les plus coûteuses commencent par les tiers

Pendant que les entreprises ont mis l'accent cette année sur la protection de leurs réseaux de plus en plus complexes, les éditeurs de logiciels et de données tiers sont devenus un angle mort de la cybersécurité pour de nombreuses organisations. Cette étude met en évidence une augmentation des violations de données impliquant les partenaires et les tiers, chose que les entreprises ont bien du mal à contrôler directement.

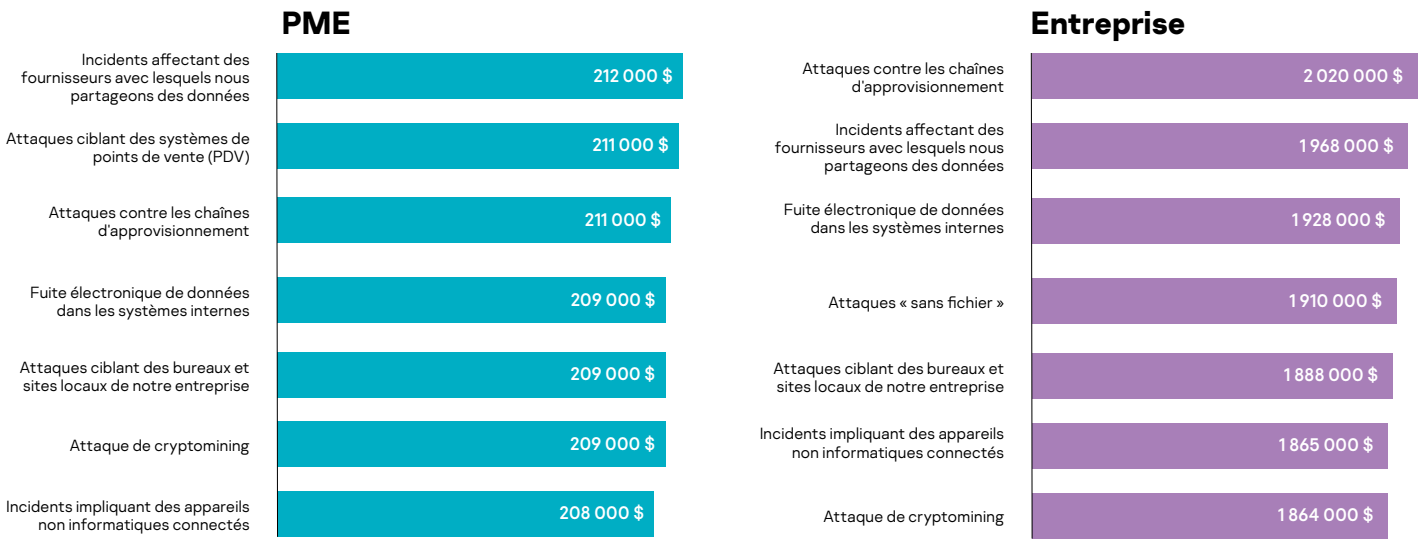
En 2021, les incidents impliquant le partage de données avec des fournisseurs ont été la violation de données la plus coûteuse pour les grandes entreprises (1,4 million de $), une dépense qui n'atteignait même pas le top 5 l'année dernière, ce qui montre à quel point il s'agit d'une préoccupation de premier plan parmi les nombreux autres types d'incidents.

Quant aux PME, les incidents affectant les fournisseurs ont été la forme la plus coûteuse de tous les incidents de cybersécurité (pas seulement les violations de données), ce qui a coûté 212 000 $ aux PME cette année.

Graphique 8 : Impact financier moyen d'une violation de données dans le monde



Graphique 9 : Impact financier moyen des incidents de cybersécurité (pas seulement les violations de données)



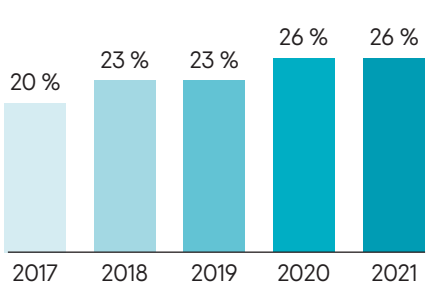
Qu'est-ce qui motive les investissements dans la sécurité informatique ?

Les conditions externes et les événements peuvent influencer les priorités des services informatiques dans les entreprises. La pandémie et la récession économique mondiale le démontrent clairement. Par conséquent, pendant la nouvelle période de planification budgétaire à la fin de l'année 2020, les organisations ont dû adapter leurs plans pour répondre à l'évolution des besoins des entreprises alors que la crise se poursuivait. L'étude a révélé l'impact que cela a eu sur les budgets de sécurité informatique.

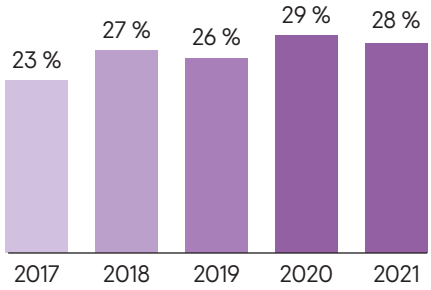
Selon les estimations des organisations elles-mêmes, parmi les PME, leur budget informatique moyen est passé de 1,1 million de dollars en 2020 à 1 million de dollars en 2021. On observe également une baisse de 54,1 millions de $ à 42,9 millions de $ pour les grandes entreprises.

En ce qui concerne les budgets de cybersécurité, dans les grandes entreprises, ceux-ci ont considérablement diminué de 19 %, pour atteindre 11,4 millions de $ en 2021, contre 14 millions en 2020. Les budgets de cybersécurité des PME sont restés à peu près identiques : 267 000 $ en 2021, contre 275 000 $ l'année dernière[1].

Graphique 10 : Pourcentage du budget informatique attribué à la cybersécurité



PME



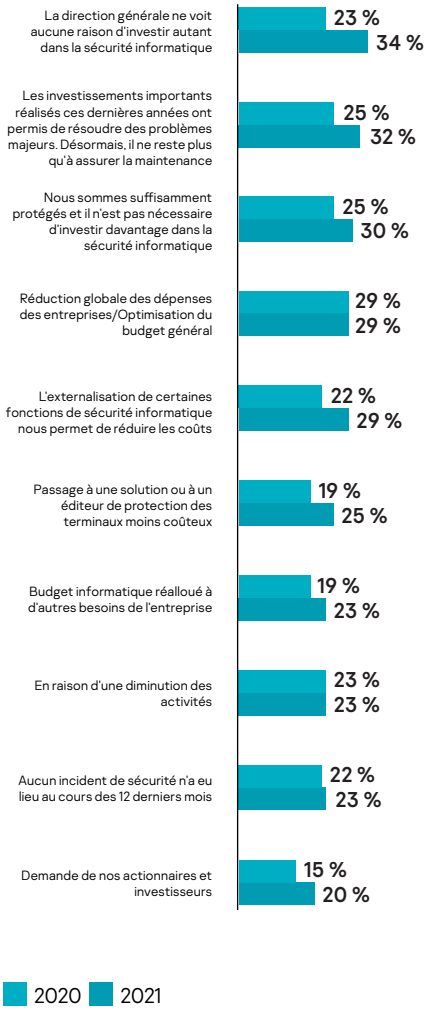
Entreprises

	2018	2019	2020	2021
Faible budget informatique	1 100 000 $	1 200 000$	1 100 000 $	1 000 000 $
Budget de sécurité informatique moyen	256 000 $	267 000 $	275 000 $	267 000 $
Croissance prévue du budget de la sécurité informatique (sur trois ans)	+14 %	+11 %	+12 %	+12 %

	2018	2019	2020	2021
Faible budget informatique	42 100 000 $	74 100 000 $	54 300 000 $	42 900 000 $
Budget de sécurité informatique moyen	10 200 000 $	18 900 000 $	14 000 000 $	11 400 000 $
Croissance prévue du budget de la sécurité informatique (sur trois ans)	+15 %	+11 %	+11 %	+12 %

1 Les chiffres relatifs aux budgets de l'informatique et de la sécurité informatique représentent le budget moyen basé sur les réponses des salariés de services informatique et de la sécurité informatique dans le monde entier, dans des entreprises de tailles et de secteurs différents.

Principales raisons de réduire le budget de sécurité informatique, PME



Malgré cela, l'importance du budget consacré à la cybersécurité continue de croître d'année en année. L'estimation de son importance dans l'écosystème informatique a globalement augmenté, passant de 63 % en 2020 à 65 % en 2021, soit une augmentation de 61 % à 63 % pour les PME, et de 67 % à 68 % pour les grandes entreprises.

« **D'une manière générale, les budgets de cybersécurité ne devraient qu'augmenter, malgré l'existence de certains facteurs qui ont un impact sur cette situation. Pour commencer, avec la migration vers le cloud, l'infrastructure est moins nécessaire, ce qui permet de réduire les budgets d'investissement dans le matériel. Sans oublier les options de sécurité intégrées qui influencent considérablement le marché. En se procurant des options de sécurité intégrées, les entreprises ne voient pas directement combien coûte la cybersécurité. En outre, ces options sont polyvalentes et ne couvrent pas tous les besoins et nuances du client. La plupart du temps, ces options de sécurité nécessitent des couches supplémentaires adaptées aux spécificités de l'activité du client, comme une threat intelligence performante. Cela implique inévitablement un investissement supplémentaire dans la cybersécurité** », explique Evgeniya Naumova.

Lorsqu'il s'agit de définir un budget pour la cybersécurité, Evgeniya souligne également le problème qui se pose lorsque la cybersécurité fait partie du budget informatique global : « **Chaque organisation a sa propre façon de gérer la documentation financière et les processus budgétaires. Le problème n'est pas de respecter la ligne de budget de l'organisation, mais de comprendre que la cybersécurité est importante et donc qu'elle requiert des ressources dédiées et de l'attention.**

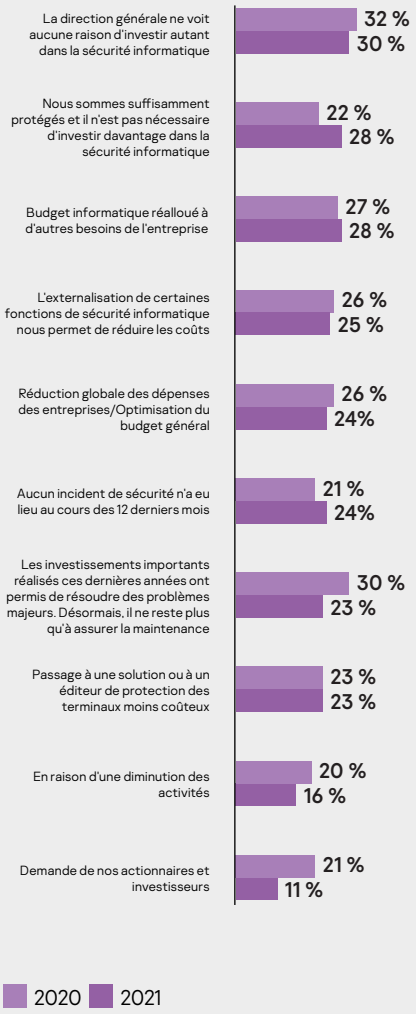
En général, pour qu'un département de sécurité des informations marche correctement, ses projets et ses activités doivent être soutenus au niveau financier, mais aussi au niveau du conseil d'administration. Il est donc très important que les conseils d'administration des entreprises soient conscients des besoins d'un budget de cybersécurité et prennent la responsabilité de les soutenir.

Si le conseil d'administration n'est pas conscient d'un problème au niveau de la sécurité des informations ou qu'il n'accorde pas suffisamment d'attention à ce domaine, celui-ci pourrait devenir un centre de coûts supplémentaires. Inclure un budget de sécurité des informations dans le budget informatique général nécessite un niveau supplémentaire d'approbations et bien souvent, les experts en cybersécurité n'ont pas l'occasion de se justifier et d'expliquer leurs projets devant le conseil d'administration. »

Les entreprises interrogées cette année partagent également leur enthousiasme quant à la poursuite de la croissance des dépenses de cybersécurité, puisque 12 % des PME et des grandes entreprises s'attendent à ce qu'elle se produise au cours des années à venir. Ces prévisions positives ont également été rapportées par **Gartner**, qui prévoit une croissance de 8,4 % des dépenses informatiques générales dans le monde en 2021.

Facteurs dans le budget Elle s'est atténuée

Principales raisons de réduire le budget de sécurité informatique, grandes entreprises



« Si cette diminution dans les budgets informatiques est temporaire, beaucoup d'entreprises ont adopté une attitude d'austérité en 2021. Cela s'explique par plusieurs facteurs.

Les organisations ont tendance à utiliser leurs budgets informatique et de cybersécurité de la manière la plus efficace possible. Cette année, certaines entreprises ont par exemple acheté un service avant la pandémie, mais se sont rendu compte entre temps qu'elles avaient besoin d'autre chose, elles ont donc modifié leurs demandes pour répondre à leurs besoins actuels. Normalement, les entreprises augmenteraient simplement le budget. À la place, elles essaient de comprendre quels services elles ont déjà achetés sans les utiliser, pour les remplacer par un service plus indispensable à leurs activités.

En plus de cela, la croissance des budgets de sécurité des informations a lieu, non parce que les équipes ont besoin de soutien pour les systèmes existants, mais parce qu'elles ont besoin de présenter de nouveaux produits. Face à la pandémie et à la transition vers le travail à domicile, beaucoup d'entreprises ont décidé de suspendre les nouveaux projets informatiques. Par exemple, si les outils de sécurité des informations sont efficaces, elles décident parfois de ne plus les toucher, en arrêtant ou en repoussant les grosses mises à jour ou les nouveaux projets. D'après ce que je sais, plus de la moitié des réductions de budget est due à cela.

L'autre facteur à prendre en compte est l'accélération croissante de l'adoption du cloud. Selon nos observations, il y a deux ans, un grand nombre de clients préférait les solutions sur site dans les clouds privés. Cela impliquait l'achat de beaucoup de matériel. Aujourd'hui, même les organisations les plus fermées ont tendance à utiliser le cloud public.

Cela a entraîné un changement dans le besoin de systèmes de sécurité des informations. Un certain nombre de projets qui ont été créés au fil des ans et qui devaient être utilisés dans une infrastructure sur site peuvent maintenant avoir perdu leur pertinence.

Il faudra un certain temps avant que les clients parviennent à définir un ensemble d'exigences pour le cloud et que les éditeurs mettent au point un ensemble de solutions. Mais la demande est là, et le nouveau package de solutions de cybersécurité à mettre en œuvre va prendre forme.

Le passage des dépenses d'investissement aux frais d'exploitation a également un impact sur le processus budgétaire. Face à l'intensité croissante des attaques et des nouveaux échantillons, les services informatiques ont dû s'efforcer de survivre dans des conditions extrêmes. Dans ces conditions, il ne restait plus qu'à embaucher des fournisseurs de services externes, comme les fournisseurs de services de sécurité gérés (MSSP). Dans le même temps, les budgets qui étaient auparavant consacrés à l'achat de matériel sont désormais utilisés pour se procurer des services. Mais le matériel s'achète pour durer plusieurs années, tandis qu'un service est facturé chaque mois. Par conséquent, si nous comparons d'une année sur l'autre, une partie du budget est passée des dépenses d'investissement aux dépenses d'exploitation. Mais étant donné que les MSSP représentent des frais mensuels, leur part dans les dépenses globales se remarque moins.

Bien que tous ces facteurs aient entraîné une diminution des budgets, ils ont en fait débouché sur une nouvelle ère pour nous. Je suis persuadé que les budgets vont s'en remettre et même s'accroître, mais cela se fera dans un nouveau paysage de systèmes informatiques, avec une utilisation plus active du modèle de service et du cloud », — déclare Veniamin Levtsov, VP, Center of Corporate Business Expertise chez Kaspersky.

La complexité informatique : un défi majeur pour les entreprises

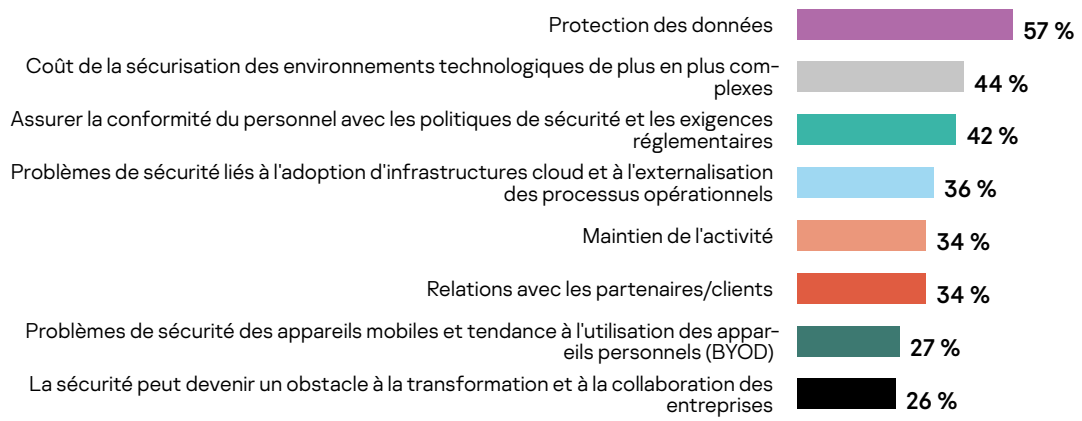
Pour beaucoup d'entreprises, l'infrastructure informatique de plus en plus complexe et la demande d'expertise pertinente pour la soutenir et la protéger est devenue un facteur décisif pour l'investissement.

Parmi les principaux défis auxquels les responsables informatiques déclarent que leurs entreprises sont confrontées, le coût de la sécurisation d'environnements de plus en plus complexes a grimpé en deuxième position (44 %). C'est un bond depuis la troisième place l'année dernière (41 %) et la sixième place en 2018. Il s'agit d'un défi qui n'est devancé que par la protection des données, qui occupe la première place (57 %).

Cette complexité entraîne également la nécessité d'augmenter les budgets. Près de la moitié (47 %) des entreprises ont désigné la complexité accrue de leur infrastructure informatique comme la principale raison d'augmenter le budget de la sécurité informatique (contre 43 % en 2020).

Graphique 11 : Principales préoccupations des PME+

Problèmes de sécurité informatique les plus préoccupants pour les entreprises



Classement des préoccupations

	2018	2019	2020	2021
Protection des données	1ère	1ère	1ère	1ère
Coût de la sécurisation des environnements technologiques de plus en plus complexes	6e	3e	3e ▲	2e
Assurer la conformité du personnel avec les politiques de sécurité et les exigences réglementaires	3e	2e	2e ▼	3e
Problèmes de sécurité liés à l'adoption d'infrastructures cloud et à l'externalisation des processus opérationnels	2e	5e	4e	4e
Maintien de l'activité	5e	4e	5e	5e
Relations avec les partenaires/clients	4e	6e	6e	6e
Problèmes de sécurité des appareils mobiles et tendance à l'utilisation des appareils personnels (BYOD)	7e	7e	7e	7e
La sécurité peut devenir un obstacle à la transformation et à la collaboration des entreprises	N/A	8e	8e	8e

En 2021, les entreprises ont ressenti encore plus le besoin de fournir des fonctionnalités continues tout en assurant la sécurité des actifs numériques de leurs clients, et elles se tournent vers une aide externalisée pour y parvenir.

Notre étude a montré que les entreprises se tournent de plus en plus vers les MSP pour obtenir des compétences particulières afin de se protéger dans un paysage difficile. Tant les PME (52 %) que les grandes entreprises (56 %) ont déclaré que les « besoins en expertise spéciale » étaient la première raison pour laquelle elles ont fait appel à des spécialistes de la sécurité externes. En 2020, les principales raisons d'externaliser la sécurité informatique étaient l'efficacité dans la fourniture de solutions de sécurité pour les grandes entreprises (70 %) et l'efficacité financière pour les PME (42 %).

L'adoption rapide des nouvelles technologies et le changement des modèles de travail, associés à la croissance exponentielle de la complexité informatique, ont encouragé les entreprises à sous-traiter les défis de sécurité auprès de professionnels hautement qualifiés en dehors de leur organisation.

Étant donné que les entreprises d'aujourd'hui doivent sans cesse suivre le rythme de l'économie numérique toujours disponible et connectée, ainsi que celui de la demande constante d'innovation, on peut s'attendre à ce que la tendance à recourir aux experts externes continue d'augmenter.

Conclusion

Au cœur d'une nouvelle année difficile pour les entreprises, les équipes informatiques sont soumises à une pression croissante. Malgré cette pression, notre étude a identifié un certain nombre de tendances récurrentes et laisse entrevoir une perspective positive pour la gestion des violations de données et des incidents de sécurité.

La baisse de l'impact financier des violations de données est une bonne nouvelle pour le secteur. Elle suggère que le travail et le renforcement qui ont été introduits dans les infrastructures informatiques au cours de l'année écoulée pour sécuriser les réseaux portent leurs fruits.

Pourtant, tout n'est pas rose. Avec 47 % des grandes entreprises qui considèrent la complexité accrue de leur infrastructure informatique comme la principale raison d'augmenter le budget de la sécurité informatique, il est clair que les équipes informatiques sont confrontées à des défis accrus par un cadre technologique plus dense et plus complexe.

Tandis que les défis de l'entreprise augmentent suite à l'impact de la pandémie, les équipes informatiques doivent protéger leurs organisations à travers une infrastructure informatique encore plus dispersée. Dans ces conditions, la réduction des budgets de cybersécurité en général est inquiétante, bien que compréhensible, étant donné les mesures d'économie que les entreprises ont dû prendre ces dernières années.

Les décideurs informatiques vont devoir se préparer à la prochaine phase de planification budgétaire. La pandémie n'est pas terminée et les défis liés à la sécurisation des infrastructures à distance complexes ne sont pas près de disparaître. Ils doivent être efficaces et trouver des solutions pour s'adapter aux besoins en sécurité de l'entreprise.

Pour aider les entreprises à relever ces défis constants, et à garantir un alignement des budgets et des mesures avec les priorités actuelles et l'évolution des menaces, Kaspersky propose les mesures suivantes :

- Utilisez une approche fondée sur les risques lorsque vous planifiez votre budget alloué à la cybersécurité. Examinez les **menaces les plus courantes** qui touchent votre secteur d'activité et les entreprises de votre taille, puis, lorsque vous établissez les priorités, tenez compte du coût que cela représente pour votre entreprise et de la probabilité que le risque se concrétise.

- Les solutions de sécurité qui peuvent être gérées à partir du cloud devraient simplifier la protection des succursales et des bureaux distants, et cette question a été une autre préoccupation majeure des spécialistes de la cybersécurité cette année.

- Dans l'environnement professionnel actuel, il est extrêmement important d'investir les budgets de cybersécurité dans des outils qui offrent une efficacité et un retour sur investissement optimaux. Cela signifie des outils qui réduisent le nombre de faux positifs, le temps de détection des attaques, le temps passé sur chaque incident et d'autres indicateurs importants pour les équipes de sécurité informatique, tout en fournissant le niveau de protection le plus fiable et une optimisation des ressources internes.

- Externaliser les tâches de sécurité avancées, par exemple, en demandant un service géré de détection et de réponse auprès de **spécialistes de la sécurité informatique reconnus**[2] peut être une bonne solution pour les organisations qui ne possèdent pas l'expertise interne nécessaire. Le fait de conclure un accord sur les niveaux de service (SLA) garanti avec toute tierce partie et de faire passer les dépenses d'investissement aux dépenses d'exploitation est un moyen de garder sous contrôle les coûts liés à la sécurité.

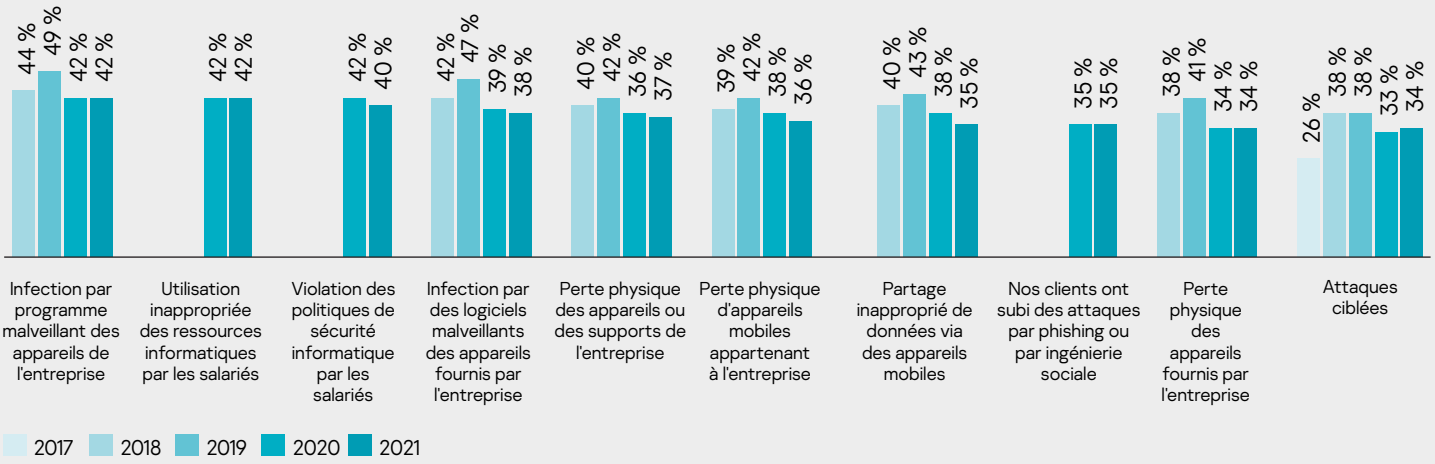
- Offrez à tout votre personnel une **formation de base à la cybersécurité**. Améliorez toujours les compétences de vos spécialistes de la sécurité informatique afin qu'ils puissent faire face à des attaques même très complexes. Par exemple, Kaspersky propose une **formation en ligne portant sur le Threat Hunting et les règles YARA**.

- Utilisez **un ensemble dédié à la protection efficace des terminaux**, des produits de détection et de réponse aux menaces pour détecter et remédier rapidement aux menaces nouvelles et évasives. Kaspersky Optimum Security Framework comprend un ensemble indispensable de protection des terminaux avec EDR et MDR, tandis que Kaspersky Expert Security offre également une technologie anti-APT, une threat intelligence performante et une formation professionnelle pour développer les compétences de votre équipe SOC.

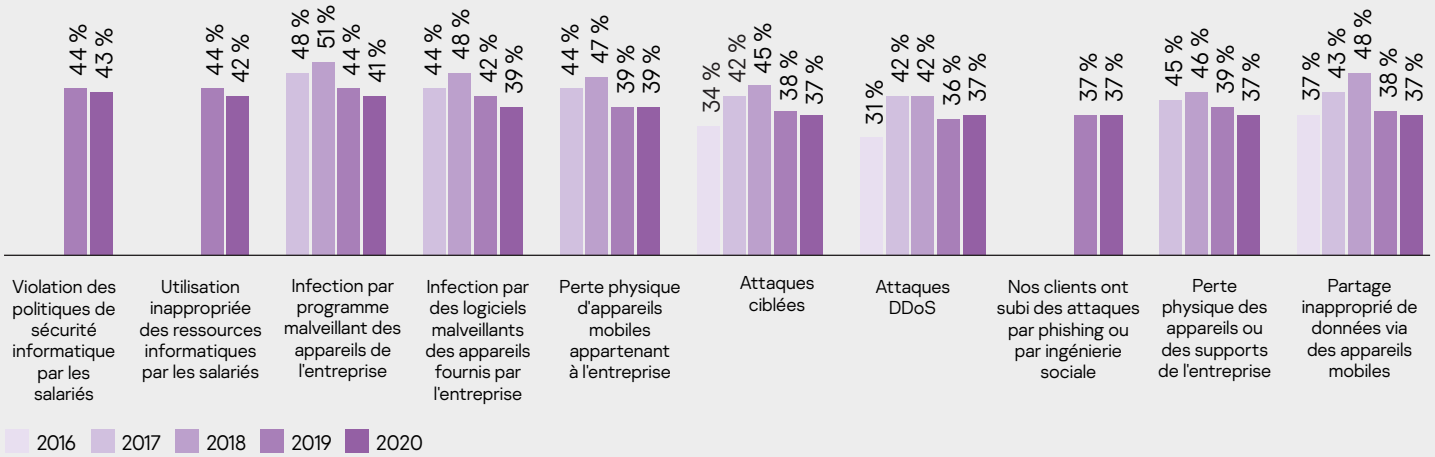
2 L'influente entreprise de recherche et de conseil Forrester a reconnu Kaspersky comme un « leader » pour ses services de Threat Intelligence, dans son rapport « The Forrester New Wave™ : services de Threat Intelligence externes, T1, 2021 ».

Graphiques supplémentaires

Graphique 12 : Top 10 des types d'incidents de sécurité subis par les PME

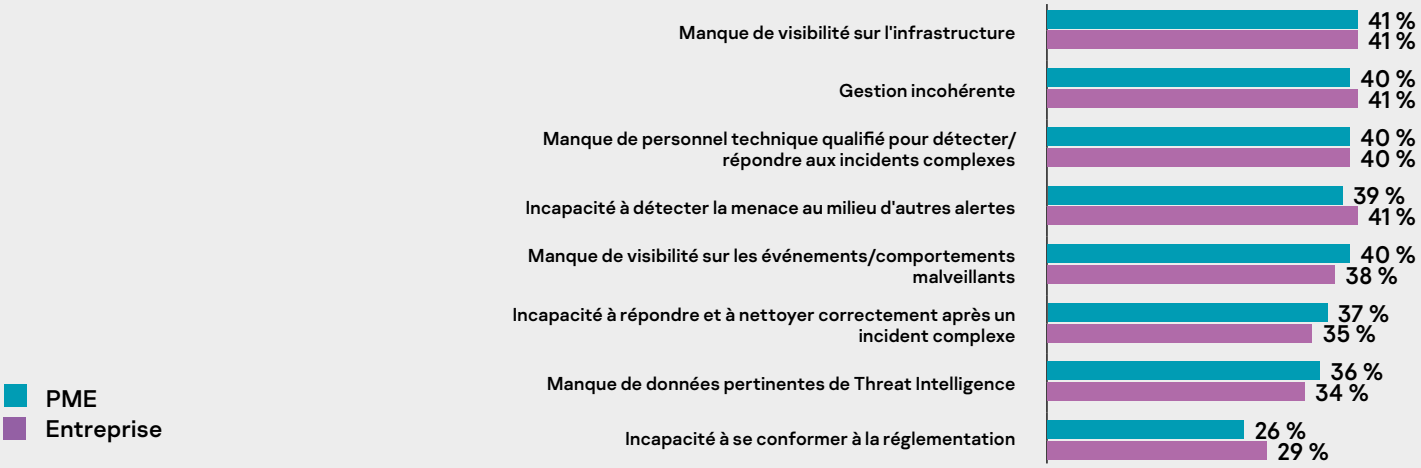


Graphique 13 : Top 10 des incidents de sécurité subis, grandes entreprises

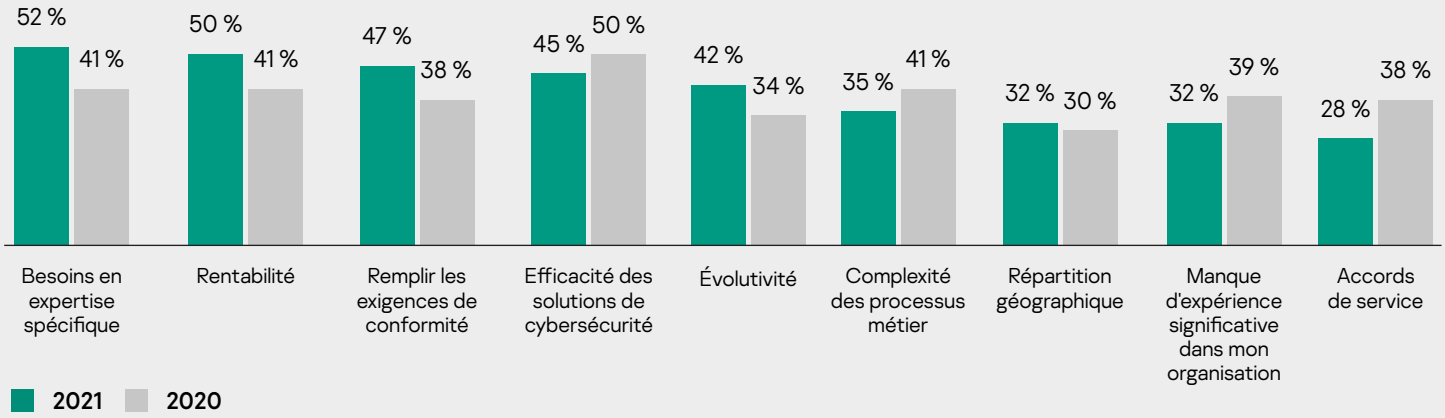


Graphique 14 : Principales préoccupations des PME+

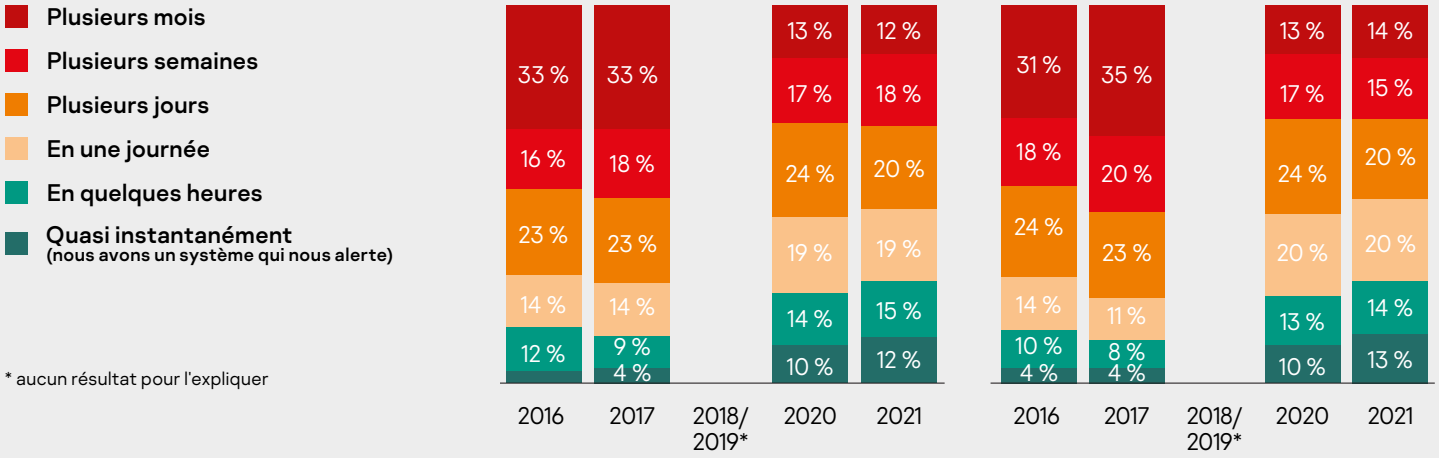
Obstacles majeurs à la protection contre les incidents complexes
(en pourcentage, chaque obstacle faisant partie du top 3 des PME et des grandes entreprises)



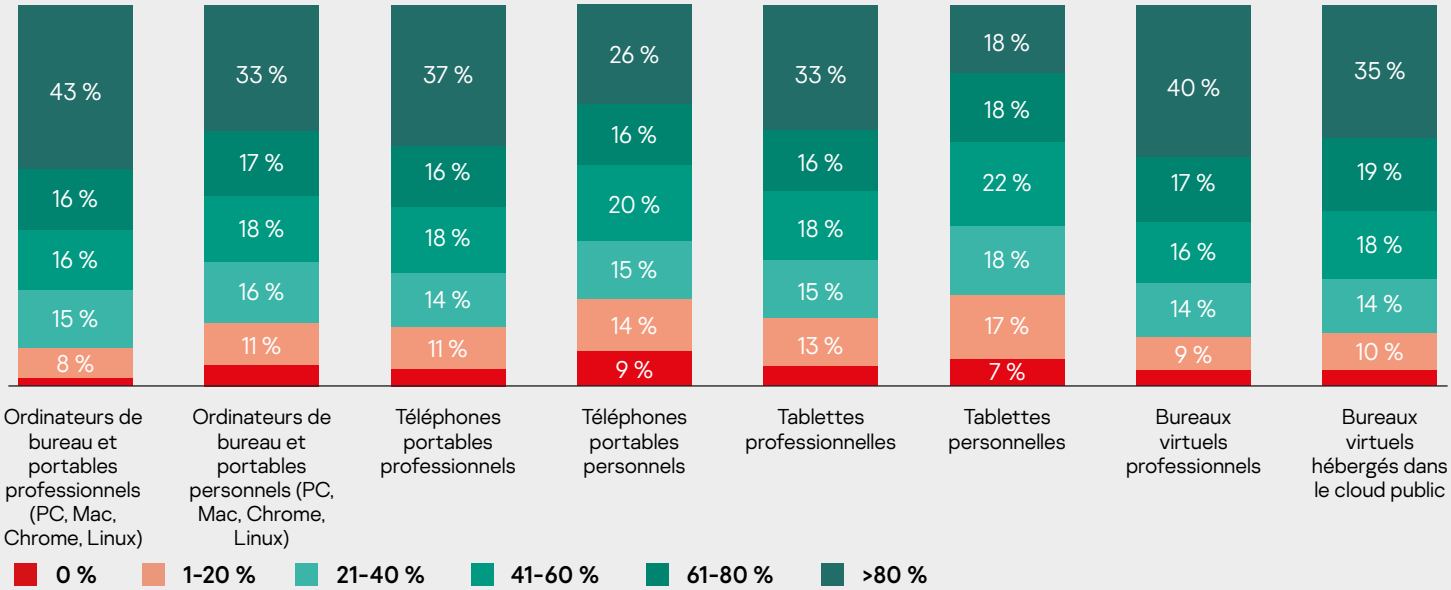
Graphique 14 : Raisons d'externaliser les fonctions auprès de MSP/MSSP



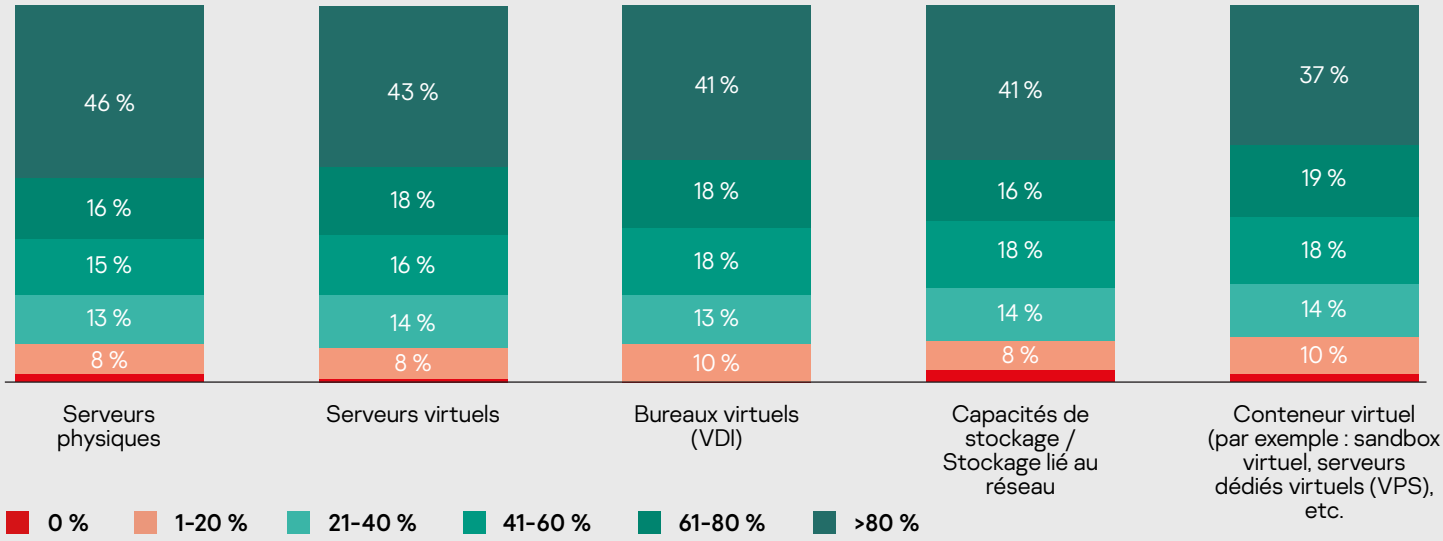
Graphique 15 : Temps nécessaire pour détecter une violation des données



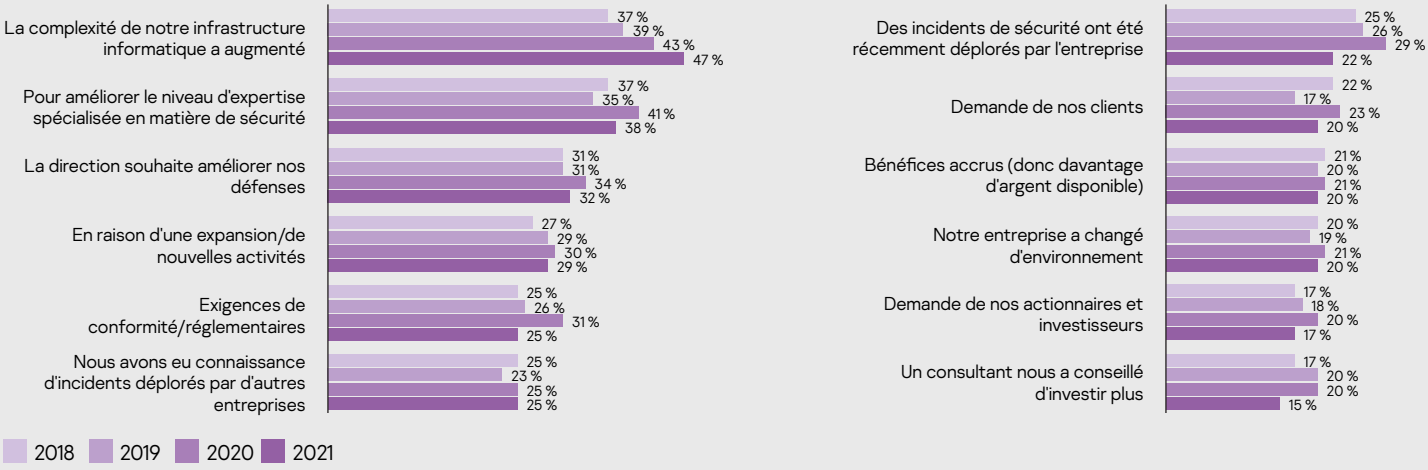
Graphique 16 : Répartition des appareils de différents types possédant un logiciel de sécurité des terminaux



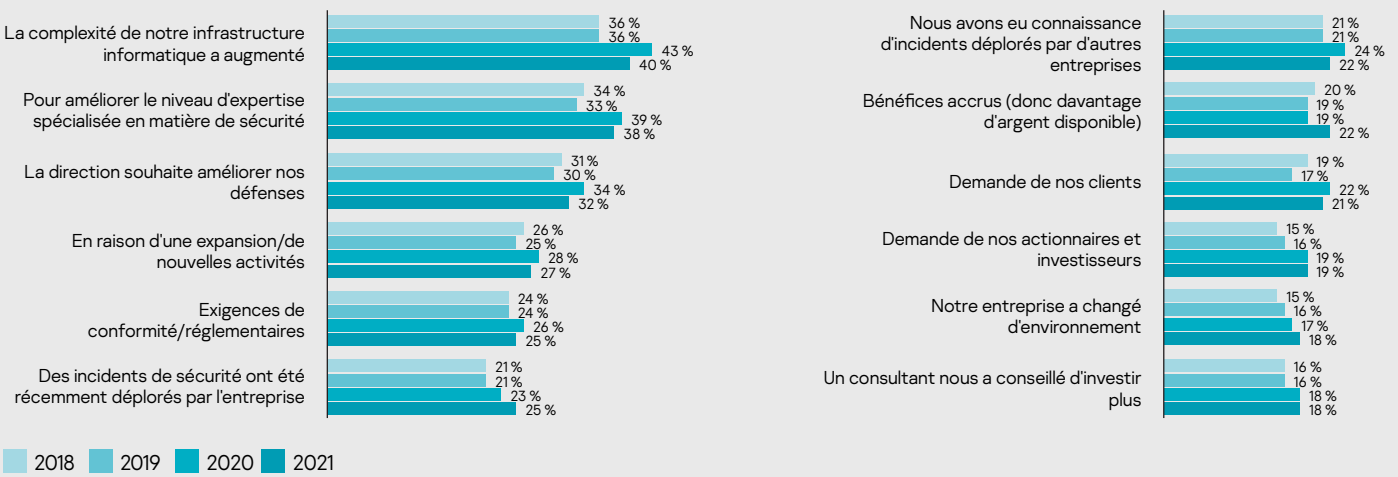
Graphique 17 : Appareils possédant un logiciel de sécurité des terminaux, par type



Graphique 18 : Principales raisons d'augmenter les budgets de sécurité informatique dans les grandes entreprises



Graphique 19 : Principales raisons d'augmenter les budgets de sécurité informatique dans les PME



Actualitéssur les cybermenaces : securelist.com
Actualités sur la sécurité informatique : business.kaspersky.fr

kaspersky.fr

kaspersky

GBD-8445 Q3/21 V1