“opinionway pour CESIN

Baromètre de la cybersécurité des entreprises

Vague 10 – Janvier 2025

Photo de Pixabay sur Pexels

Contact presse :
Véronique LOQUET – ***AL'X COMMUNICATION***
06 68 42 79 68 - vloquet@alx-communication.com

afaq ISO 20252 Étude marketing et d'opinion – AFNOR CERTIFICATION

ESOMAR 25 Corporate

Les objectifs

Contexte et objectifs

- Le **Club des Experts de la Sécurité de l'Information et du Numérique** (CESIN) offre un lieu d'échanges aux **experts de la sécurité et du numérique** au sein des entreprises.

- Le CESIN, avec OpinionWay, a lancé en 2015 sa première grande enquête auprès de ses membres pour connaître :
  - **la perception de la cybersécurité et de ses enjeux** au sein des entreprises membres du CESIN
  - **la réalité** concrète de la sécurité informatique des entreprises.

- L'enquête, renouvelée chaque année, met à jour les résultats sur la perception et la réalité de la cybersécurité, et apporte de nouvelles données sur l'impact de la transformation numérique des entreprises.

La méthodologie

La méthodologie

Echantillon de **401 membres du CESIN,** à partir du fichier des membres du CESIN.

L'échantillon a été interrogé par **questionnaire auto-administré en ligne sur système CAWI** (Computer Assisted Web Interview).

Les interviews ont été réalisées **du 10 décembre 2024 au 7 janvier 2025**.

OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la **norme ISO 20252**

Les résultats de ce sondage doivent être lus en tenant compte des marges d'incertitude : 4,9 points au plus pour un échantillon de 400 répondants.

Toute publication totale ou partielle doit impérativement utiliser la mention complète suivante :

« Sondage OpinionWay pour le CESIN »

et aucune reprise de l'enquête ne pourra être dissociée de cet intitulé.

Le profil des répondants

Un échantillon qui reflète parfaitement la diversité de la population interrogée

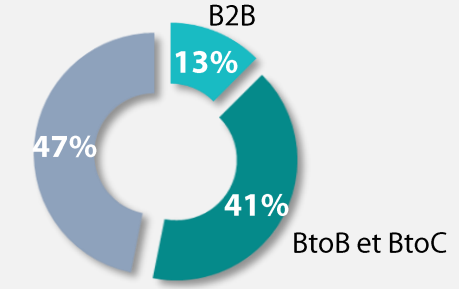
Secteur d'activité de l'entreprise

Information et communication	19%	Services 43%
Activités financières et d'assurance	16%	
Activités spécialisées, scientifiques et techniques	5%	
Arts, spectacles et activités récréatives	1%	
Activités immobilières	1%	
Entreprises et services du numérique	1%	
Industrie manufacturière	16%	Industrie/BTP 22%
Production et distribution d'électricité, gaz, vapeur, air conditionné	2%	
Construction	2%	
Agriculture, sylviculture et pêche	1%	
Production et distribution d'eau, assainissement, gestion des déchets et dépollution	1%	
Industries extractives	<1%	
Administration publique et défense, collectivité	10%	Services publics 16%
Santé humaine et action sociale	5%	
Enseignement	1%	
Commerce	8%	Commerce 16%
Transports et entreposage	5%	
Hébergement et restauration	<1%	
Autre secteur	4%	

Nombre de salariés de l'entreprise

Moins de 250 salariés	14%	TPE / PME
Entre 250 et 999 salariés	14%	ETI 39%
Entre 1 000 et 4 999 salariés	25%	
Entre 5 000 et 9 999 salariés	11%	Grandes entreprises 47%
Entre 10 000 et 49 999 salariés	20%	
50 000 salariés ou plus	16%	

Activité Commerce



L’analyse

01

Un volume de cyberattaques stable en 2024, dont les contours et les conséquences restent globalement identiques à l'année précédente

Définition d'une cyberattaque

« Une cyberattaque, telle que nous l'entendons dans cette enquête, est le fait de subir un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information, entraînant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise et/ou des efforts significatifs de défense pour contenir et traiter l'attaque. Nous ne comptons pas là les tentatives d'attaques qui ont été arrêtées par vos systèmes de prévention. »

La moitié des entreprises ont subi au moins une cyberattaque en 2024, une proportion qui reste stable par rapport à l'année précédente.

401 personnes

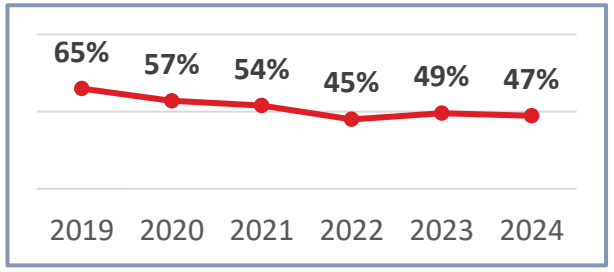
Q4. Au total, combien de cyberattaques significatives ont été subies par votre entreprise au cours des 12 derniers mois ?
Base : ensemble

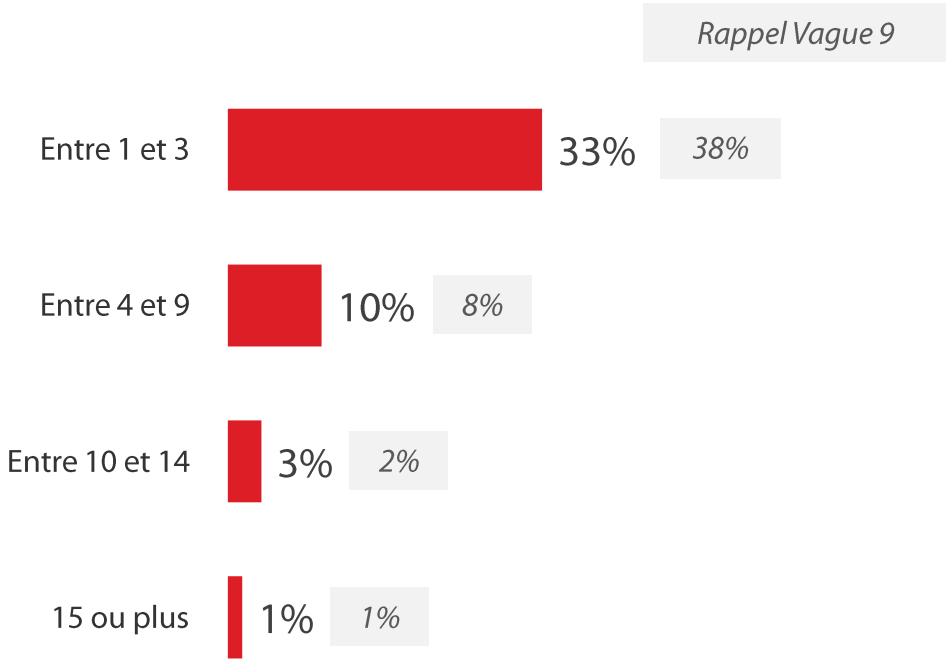
47%

des entreprises ont constaté au moins une cyberattaque

Grande entreprise : 53%

Rappel vagues précédentes





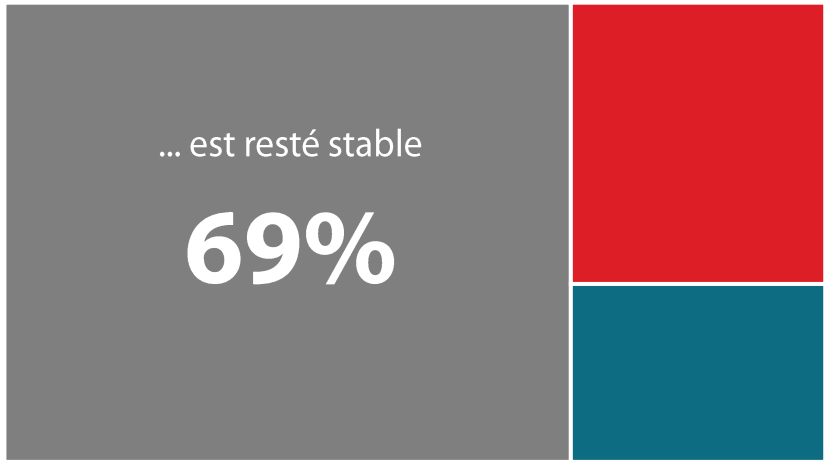
Le nombre d'attaques se stabilise pour la majorité des entreprises, bien qu'1/5 en constate une augmentation.

401 personnes

Q4bis. Et par rapport à l'année dernière, ce nombre d'attaques constatées dans votre entreprise… ?
Base : ensemble

*Parmi les entreprises ayant déclaré avoir subi au moins une attaque en 2024, **37%** indiquent avoir constaté une augmentation de ces dernières.*

En un an, le nombre d'attaques...



... est resté stable
69%

Rappel Vague 9 : 66%

... a augmenté
19%

Rappel Vague 9 : 23%

ETI : 25%

... a diminué
12%

Rappel Vague 9 : 11%

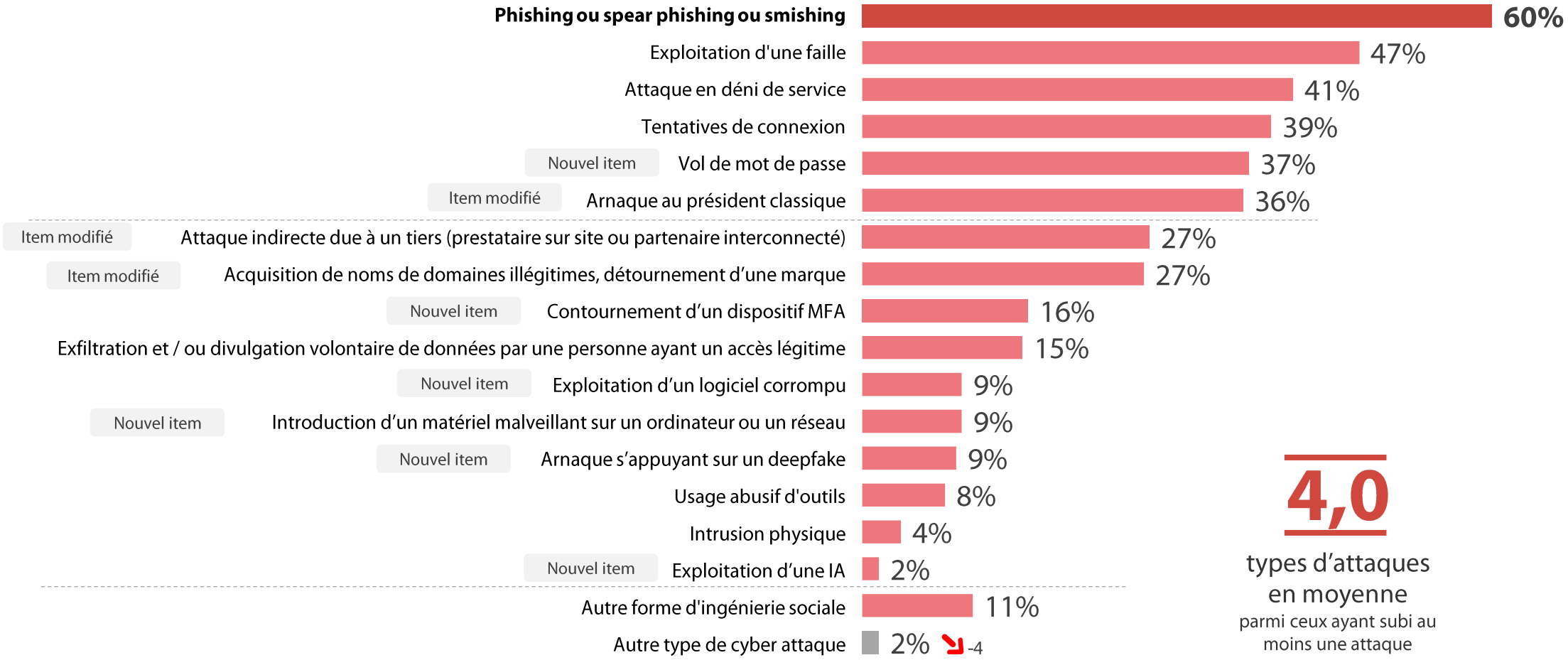
Avec en moyenne 4 vecteurs, le phishing reste en tête des attaques, suivi par l'exploitation d'une faille existante. Les stratégies d'attaque sont similaires à l'année précédente.

190 personnes

Q5A. Parmi les vecteurs d'attaques suivants, lesquels ont impacté votre entreprise au cours des 12 derniers mois ?

Base : ont constaté une attaque - plusieurs réponses possibles

47% des entreprises ont subi au moins une cyberattaque en 2023



4,0

types d'attaques en moyenne

parmi ceux ayant subi au moins une attaque

Évolution statistiquement significative par rapport à la vague précédente

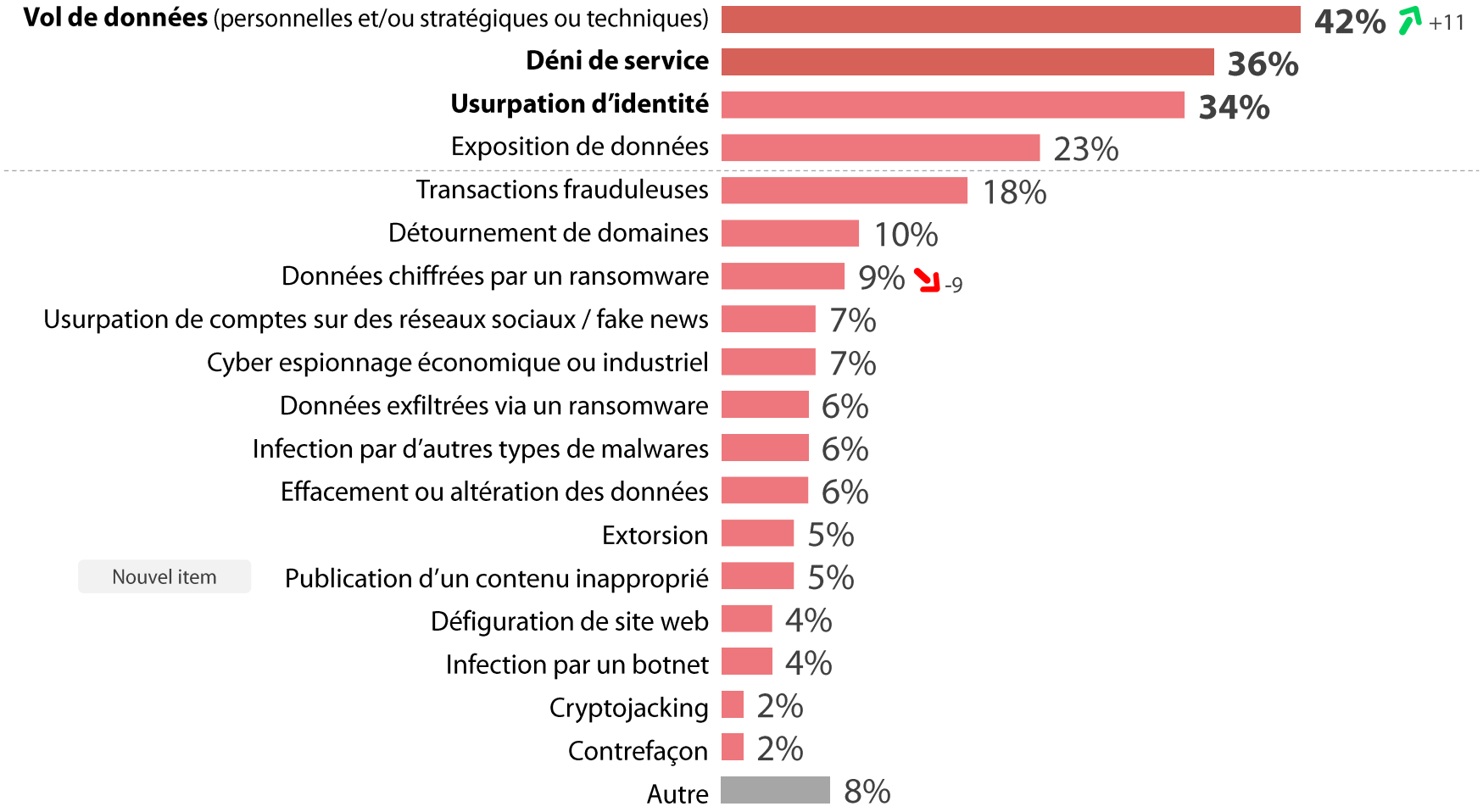
Le vol de données demeure en tête des conséquences de ces attaques et gagne même du terrain. Le déni de service et l'usurpation d'identité sont ensuite constatés par plus d'1/3 des entreprises. A noter, la baisse des données chiffrées par un ransomware.

190 personnes

Q5B. Et quelles ont été les conséquences de cette/ces attaque(s) ?

Base : ont constaté une attaque - plusieurs réponses possibles

47% des entreprises ont subi au moins une cyberattaque en 2023



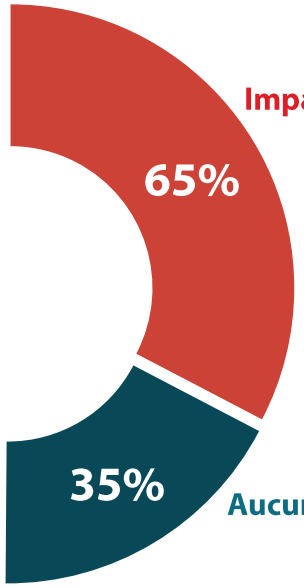
L'impact des cyberattaques sur le business reste stable cette année : 2/3 le subissent. Si la perturbation de la production est toujours la conséquence la plus mentionnée, l'indisponibilité du site web pendant une période significative recule.

351 personnes

Q7. Quel a été l'impact des cyberattaques sur votre business ?

Base : ont constaté une attaque et / ou une cause d'incidents de sécurité - Plusieurs réponses possibles

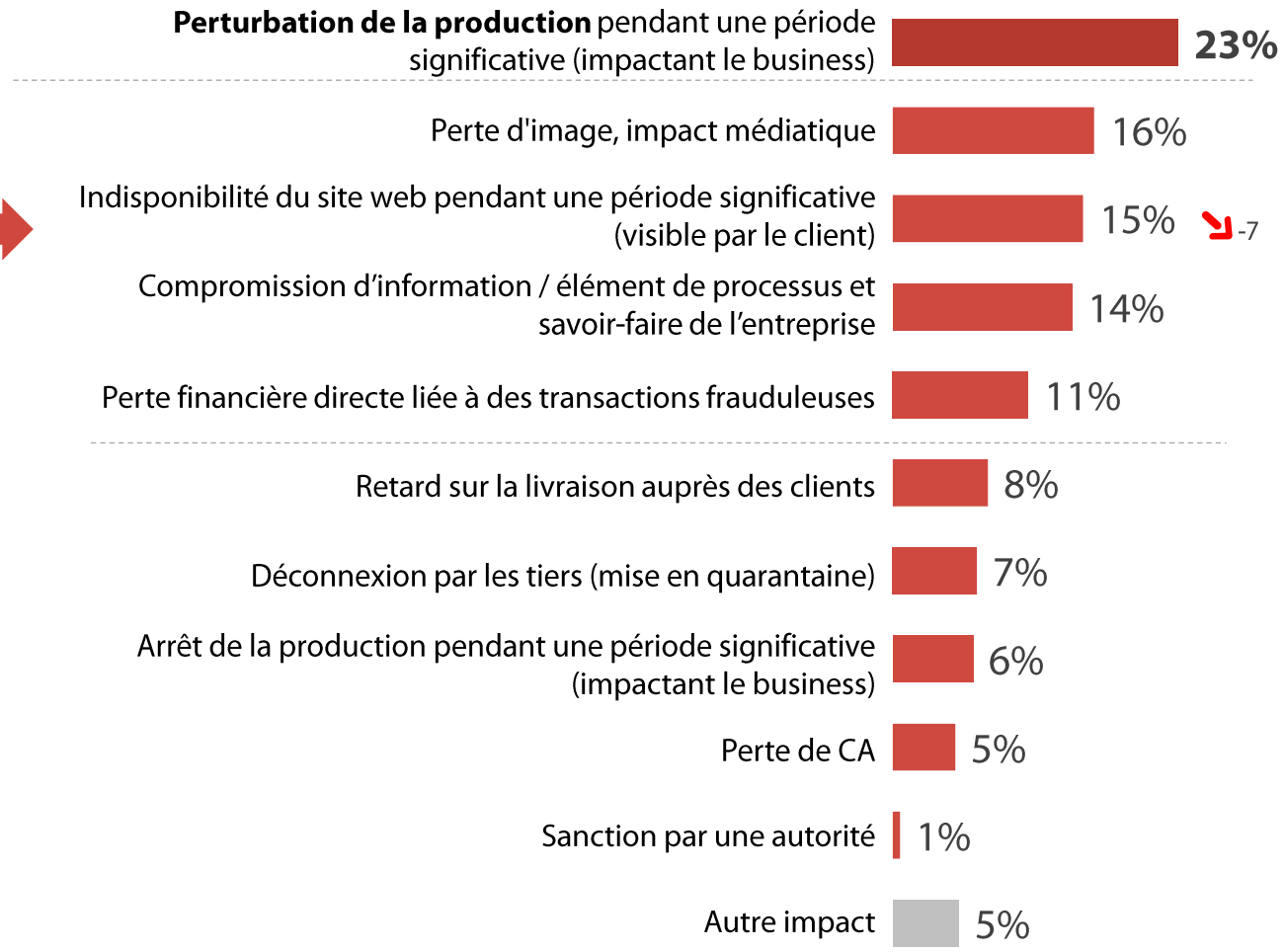
Rappel Vague 9 : 65%



Impacts sur le business

Rappel Vague 9 : 35%

Aucun impact sur le business

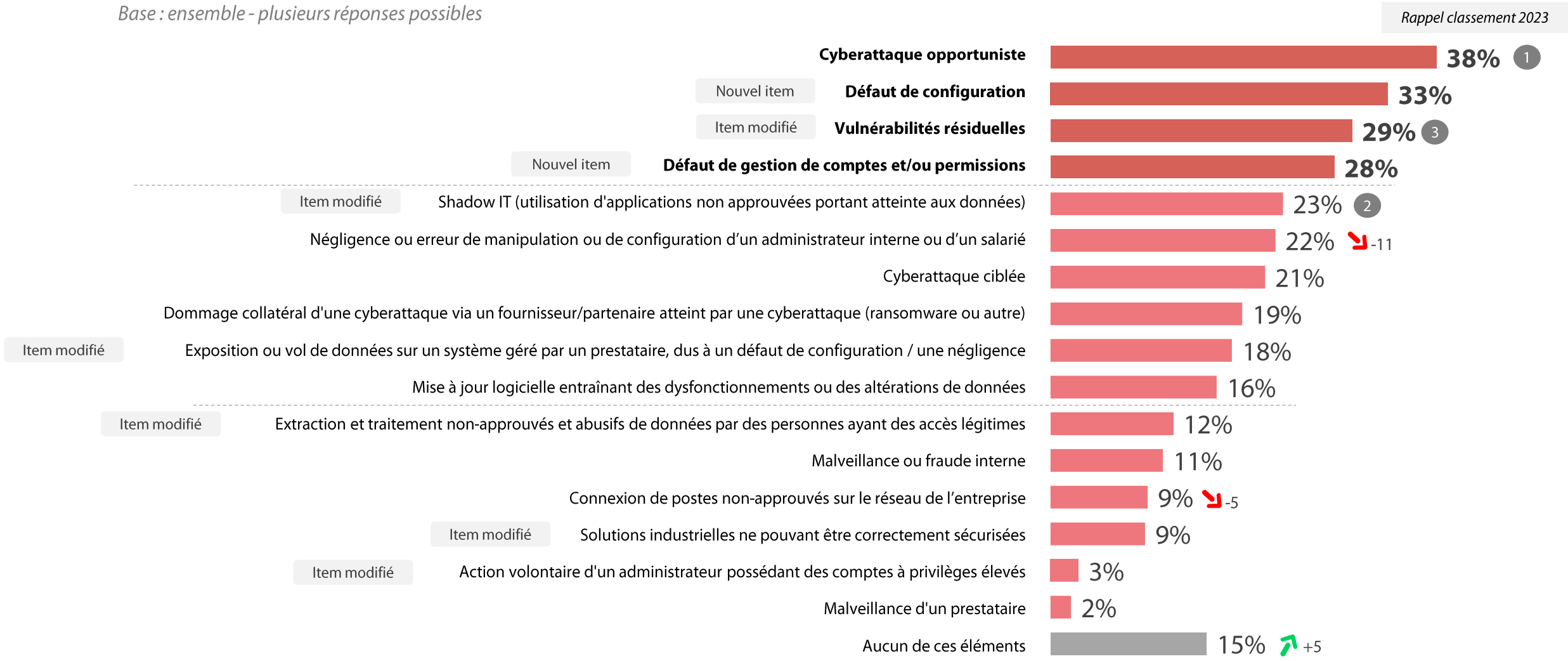


Les incidents de sécurité sont majoritairement causés par des opportunités laissées aux attaques : cyberattaque opportuniste, défaut de configuration, vulnérabilités résiduelles et défauts de gestion de comptes, reléguant alors le Shadow IT à la 5ème place cette année (vs 2ème l'année précédente).

401 personnes

Q6. Parmi les causes des incidents de sécurité rencontrées par l'entreprise, cyberattaques incluses, quelles sont celles auxquelles votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?

Base : ensemble - plusieurs réponses possibles



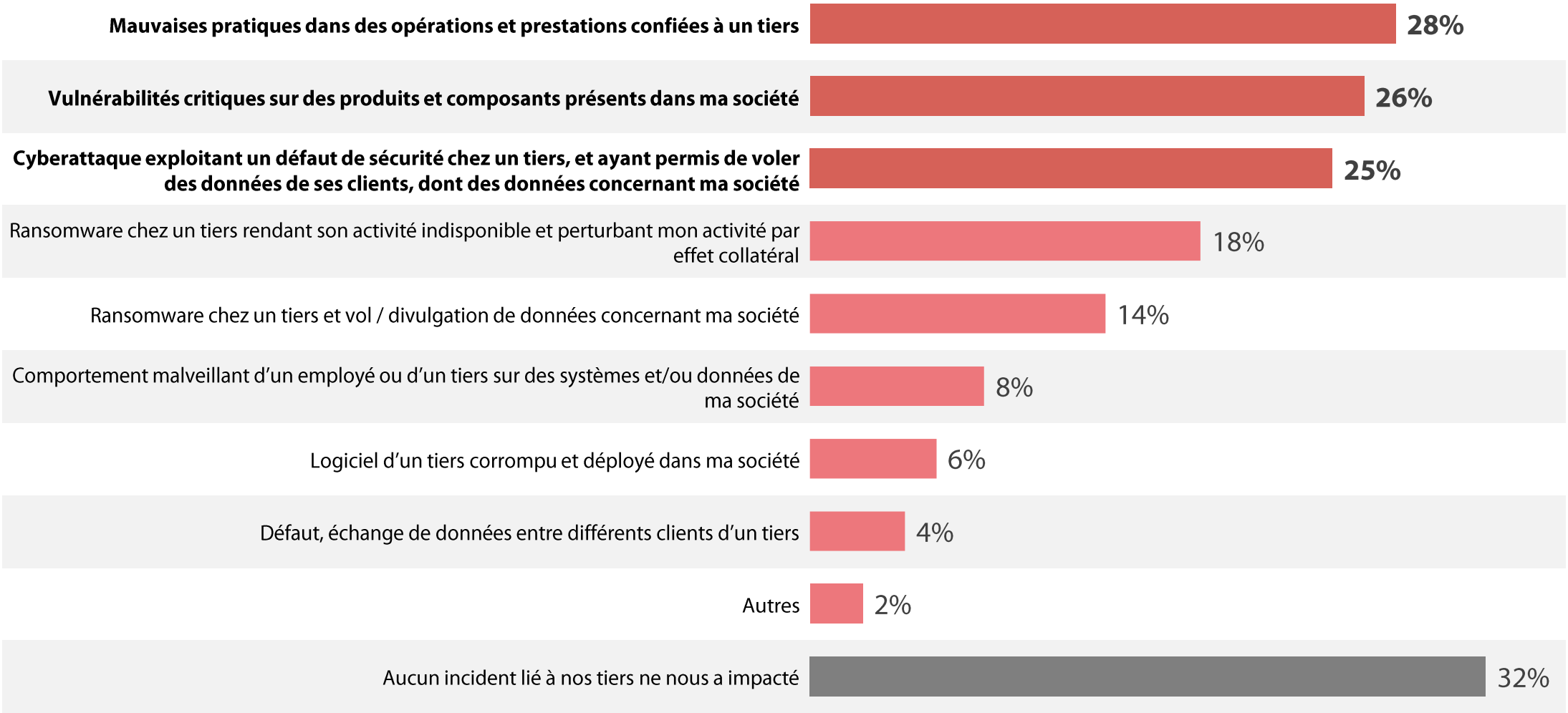
Concernant les incidents liés aux tiers, ¼ des entreprises ont constaté des mauvaises pratiques dans les opérations confiées aux tiers, des vulnérabilités critiques sur des produits ou une cyberattaque liée à un défaut de sécurité d'un tiers.

401 personnes

Nouvelle question en 2024

Q40 : Quels incidents liés à vos tiers vous ont impactés ?

Base : ensemble - plusieurs réponses possibles



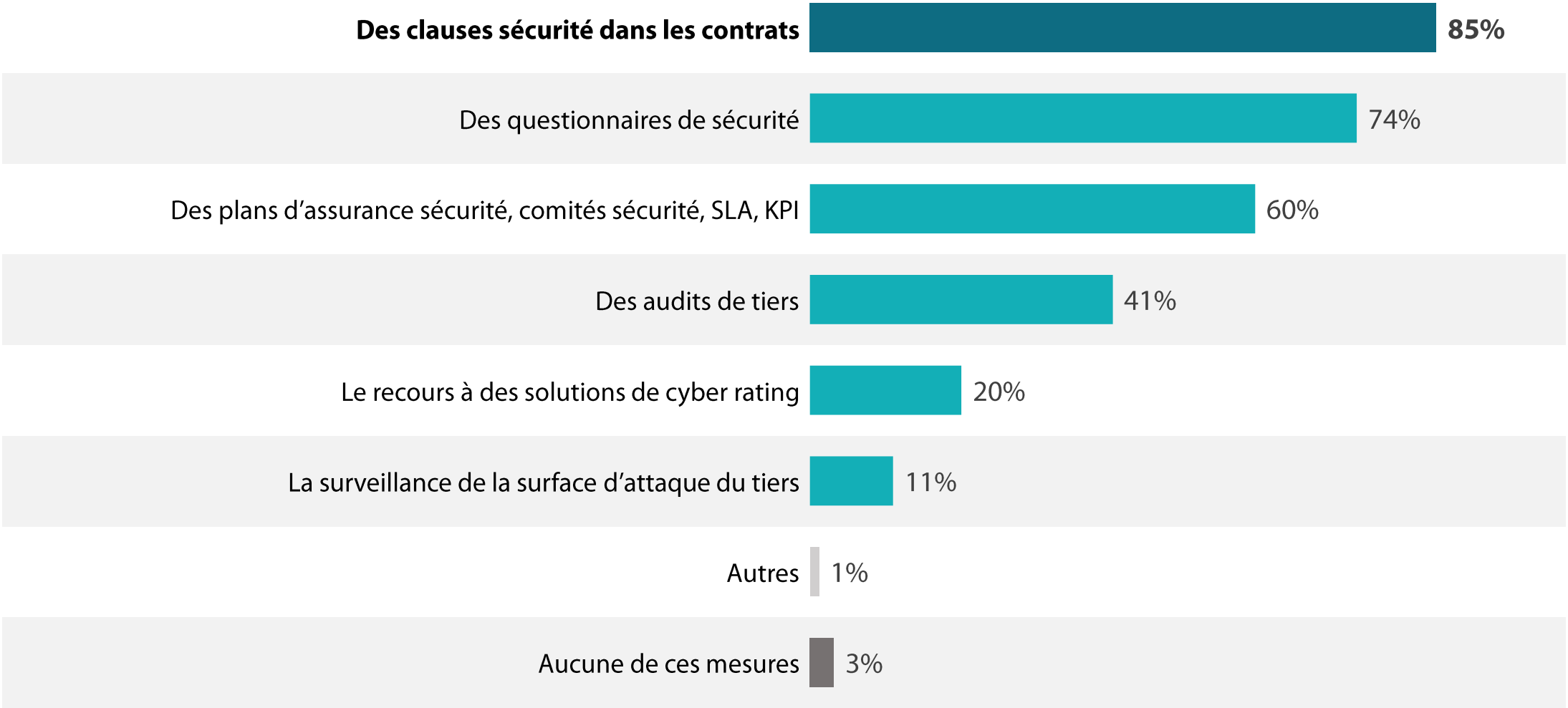
Pour adresser ce risque lié aux tiers, les entreprises misent en premier lieu sur les clauses sécurité dans les contrats, puis dans les questionnaires de sécurité et enfin dans des plans d'assurance sécurité.

401 personnes

Nouvelle question en 2024

Q43 : Quelles mesures avez-vous entreprises pour adresser le risque lié aux tiers ?

Base : ensemble - plusieurs réponses possibles



Le risque de cyberespionnage est un risque jugé élevé par près de 4 entreprises sur 10, ce qui constitue un élément important compte tenu du fait que certaines entreprises ne sont pas, du fait de leur activité, très concernées par ce type de risque.

401 personnes

Q9. Aujourd'hui, comment évaluez-vous le niveau des menaces relatives au cyberespionnage pour votre entreprise ?

Base : ensemble

Item modifié
Très élevé : figure dans le top 3 des risques cyber identifiés — 10%

Item modifié
Assez élevé : figure dans le top 10 des risques cyber identifiés — 27%

Item modifié
Assez faible : présent dans la cartographie des risques cyber — 40%

Item modifié
Très faible : absente de la cartographie des risques cyber — 23%

37% **Estiment un niveau élevé des menaces relatives au cyberespionnage**

Industrie/BTP : 46%

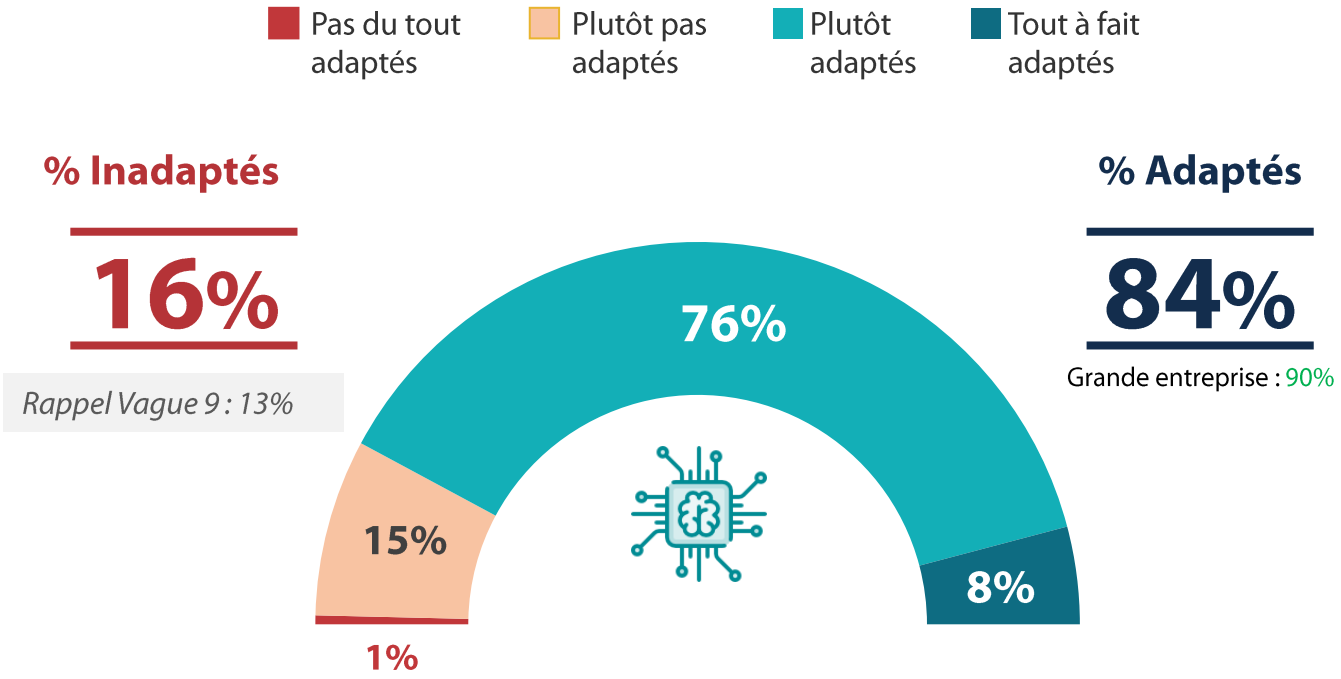
02

Des moyens de défense performant qui prouvent leur efficacité au fil des ans (notamment les pares-feux, l'EDR et le MFA)

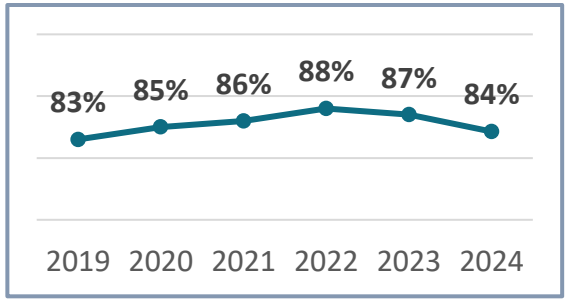
Dans les mêmes proportions que l'année dernière, l'adéquation des solutions et services de sécurité disponibles sur le marché est toujours satisfaisante pour les entreprises.

401 personnes

Q25. Pensez-vous que les solutions et services de sécurité disponibles sur le marché sont tout à fait, plutôt, plutôt pas ou pas du tout adaptés à votre entreprise ?
Base : ensemble



Rappel vagues précédentes

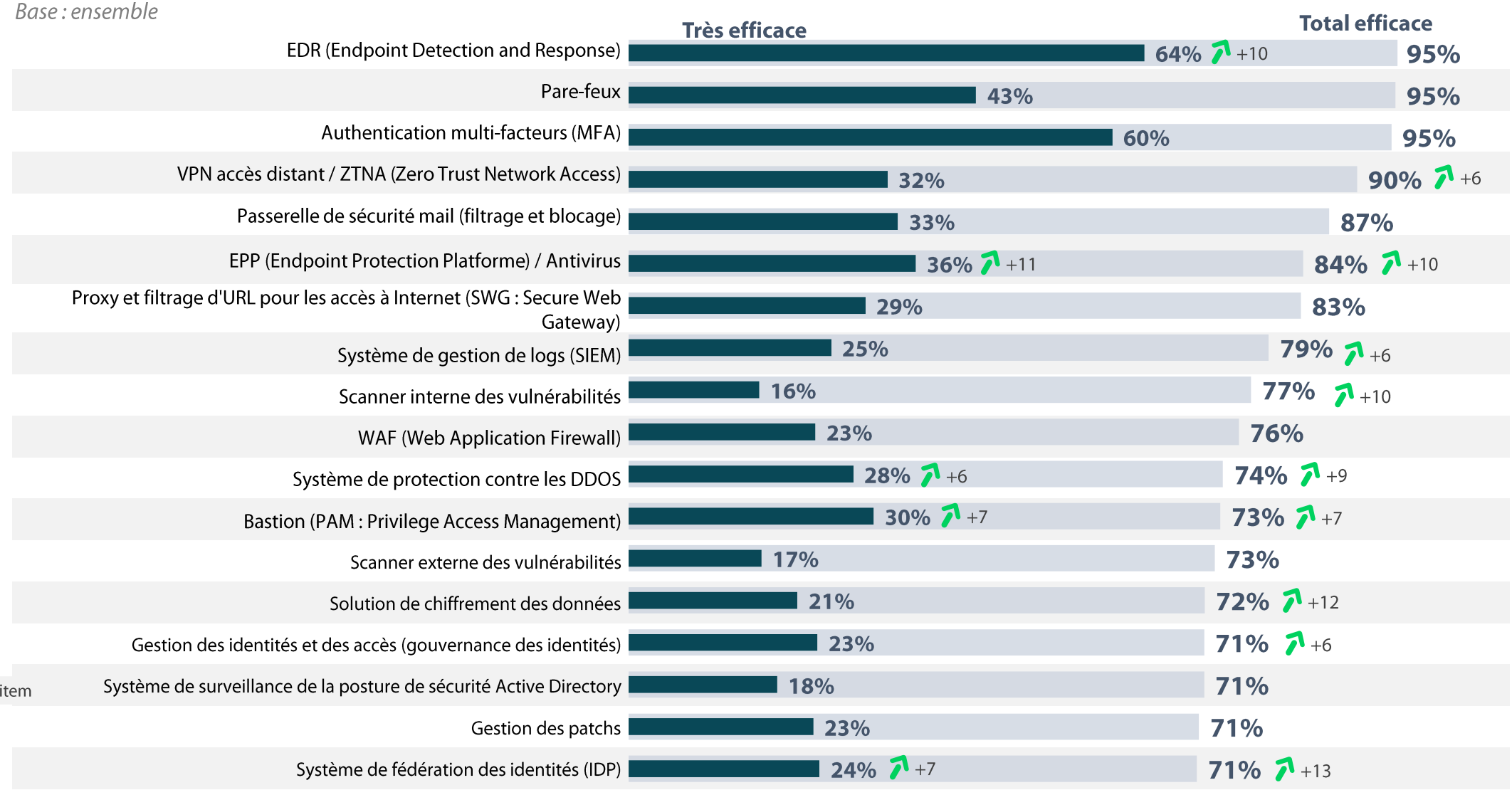


Dans le détail, l'EDR, les pares-feux et le MFA sont considérés comme les solutions les plus efficaces, l'EDR gagnant même des points sur la modalité « très efficace ».

401 personnes

Q13. Pour chacune des solutions suivantes, estimez-vous qu'elle est très efficace, plutôt efficace, plutôt pas efficace ou pas du tout efficace ?

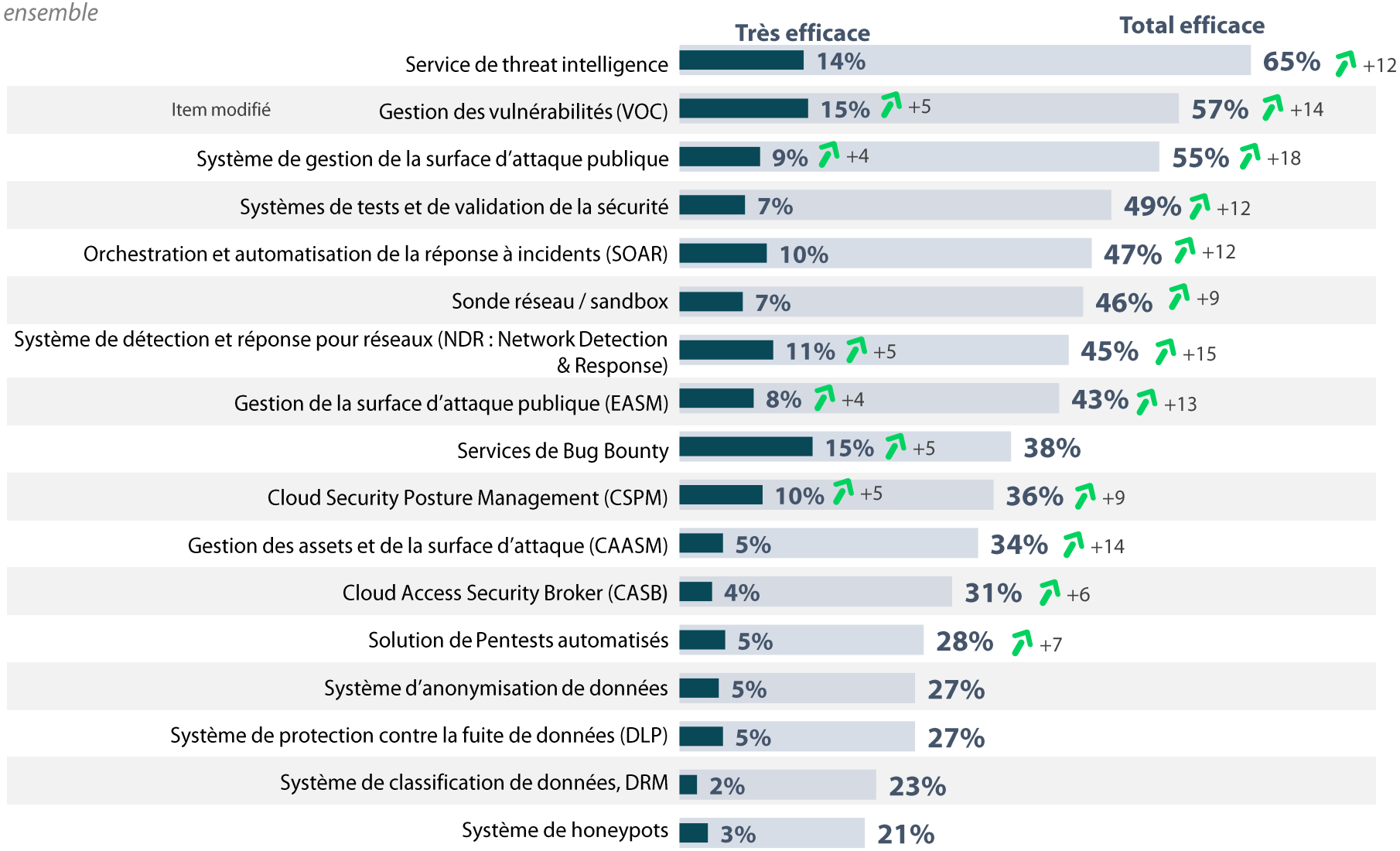
Base : ensemble



L'efficacité de la majorité des autres solutions progresse également cette année.

401 personnes

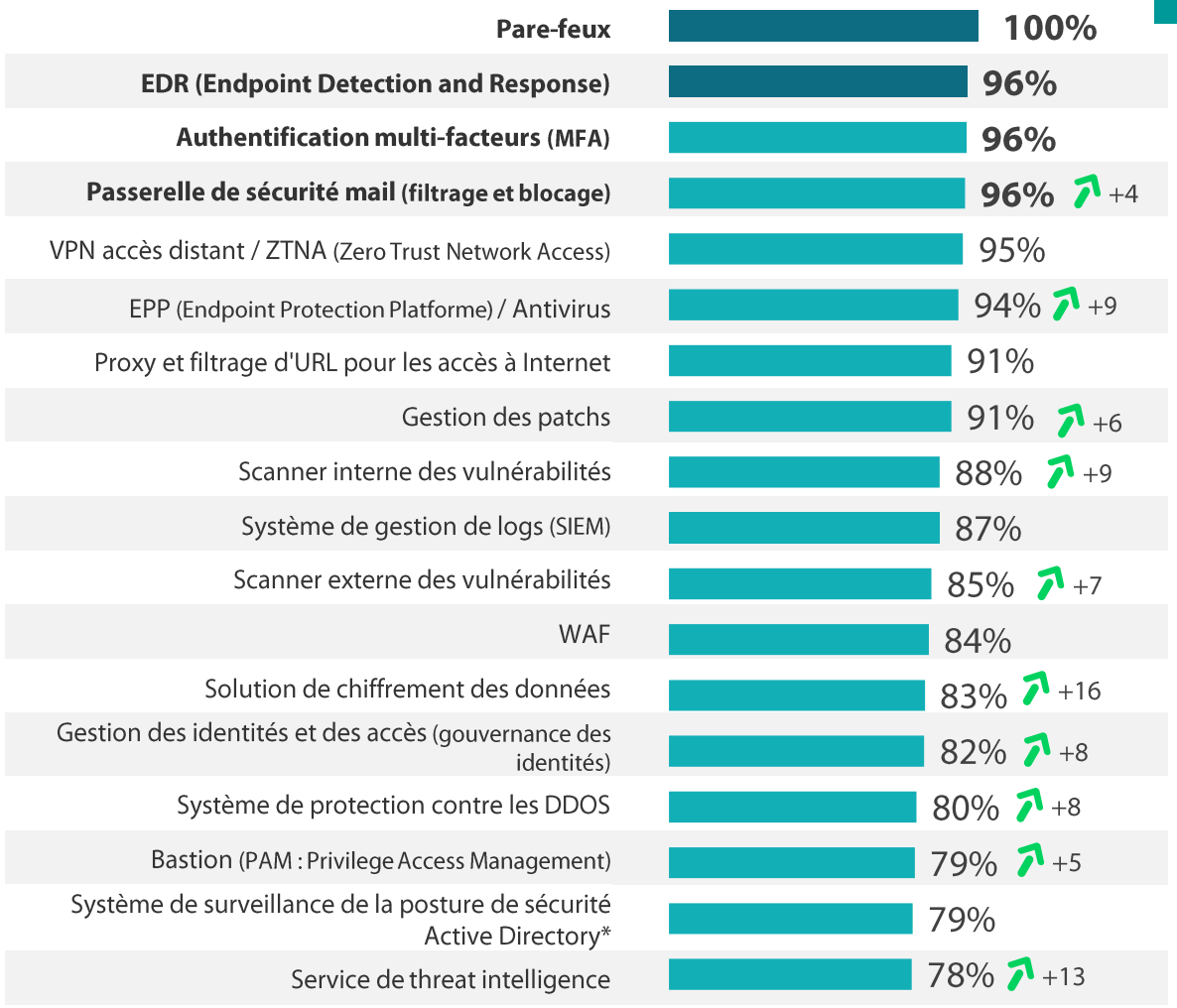
Q13. Pour chacune des solutions suivantes, estimez-vous qu'elle est très efficace, plutôt efficace, plutôt pas efficace ou pas du tout efficace ?
Base : ensemble



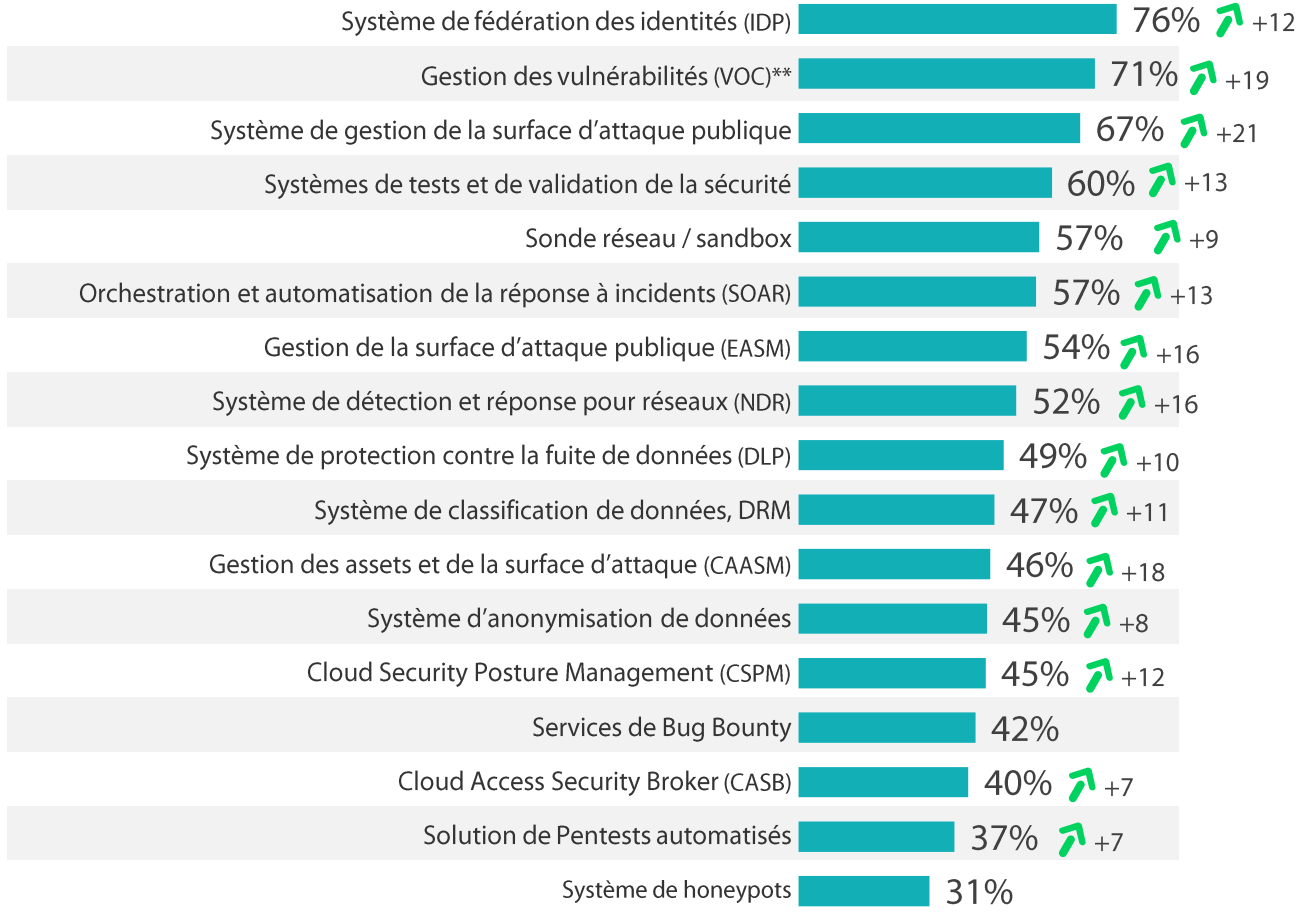
Les pares-feux, l'EDR et le MFA occupent toujours la tête des solutions déployées dans les entreprises. Les passerelles de sécurité mail progressent et rejoignent ce podium. De manière globale, les entreprises se protègent plus.

401 personnes

Q13. Pour chacune des solutions suivantes, estimez-vous qu'elle est très efficace, plutôt efficace, plutôt pas efficace ou pas du tout efficace ? *Base : ensemble - plusieurs réponses possibles*



Solution déployée



"opinionway pour CESIN

*Nouvel item
** item modifié

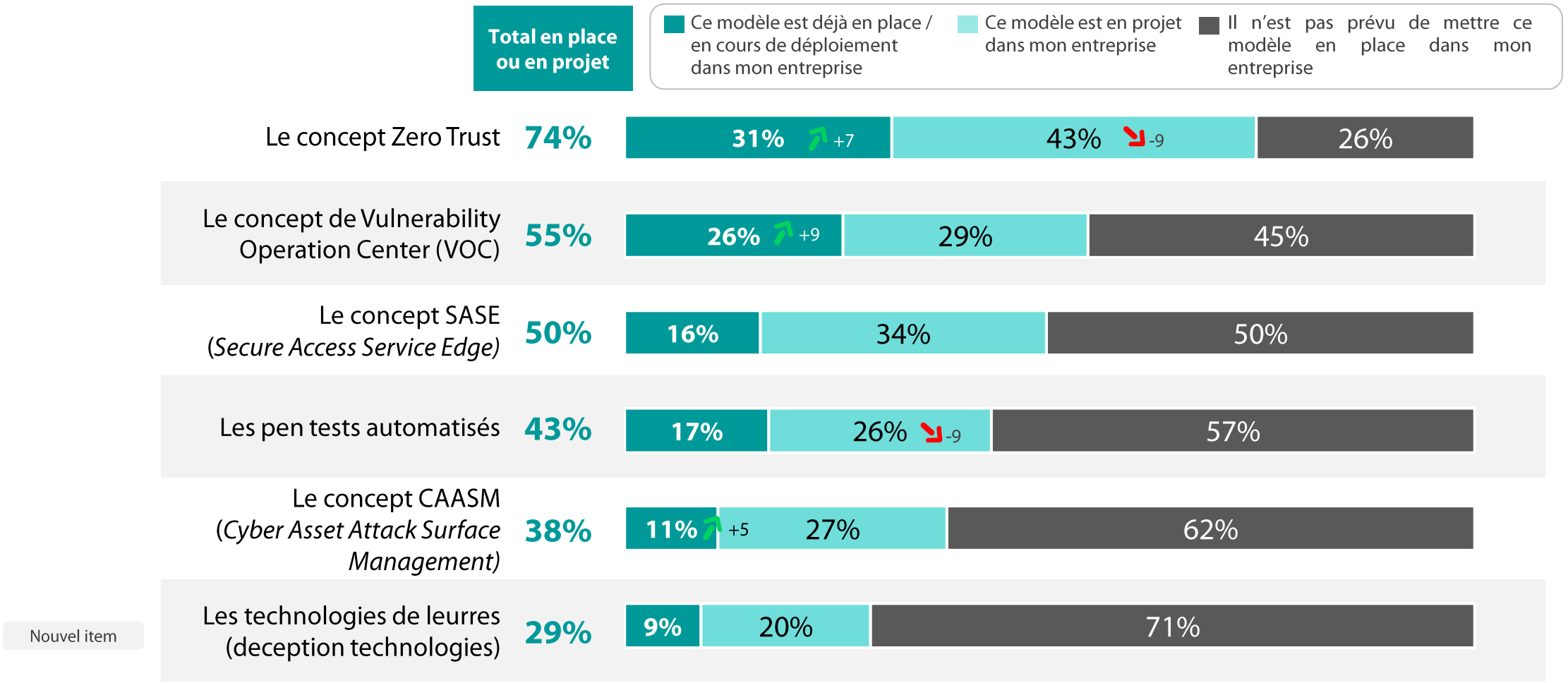
Évolution statistiquement significative par rapport à la vague précédente
Évolution à interpréter avec prudence au vu de l'ajout d'items

Le Zero Trust et le VOC sont davantage mis en place ou en cours de déploiement cette année, de même que le CAASM dans une moindre mesure, qui avait déjà débuté son ascension l'année dernière.

401 personnes

Q28b. Quelle est votre vision des concepts suivants ?

Base : ensemble

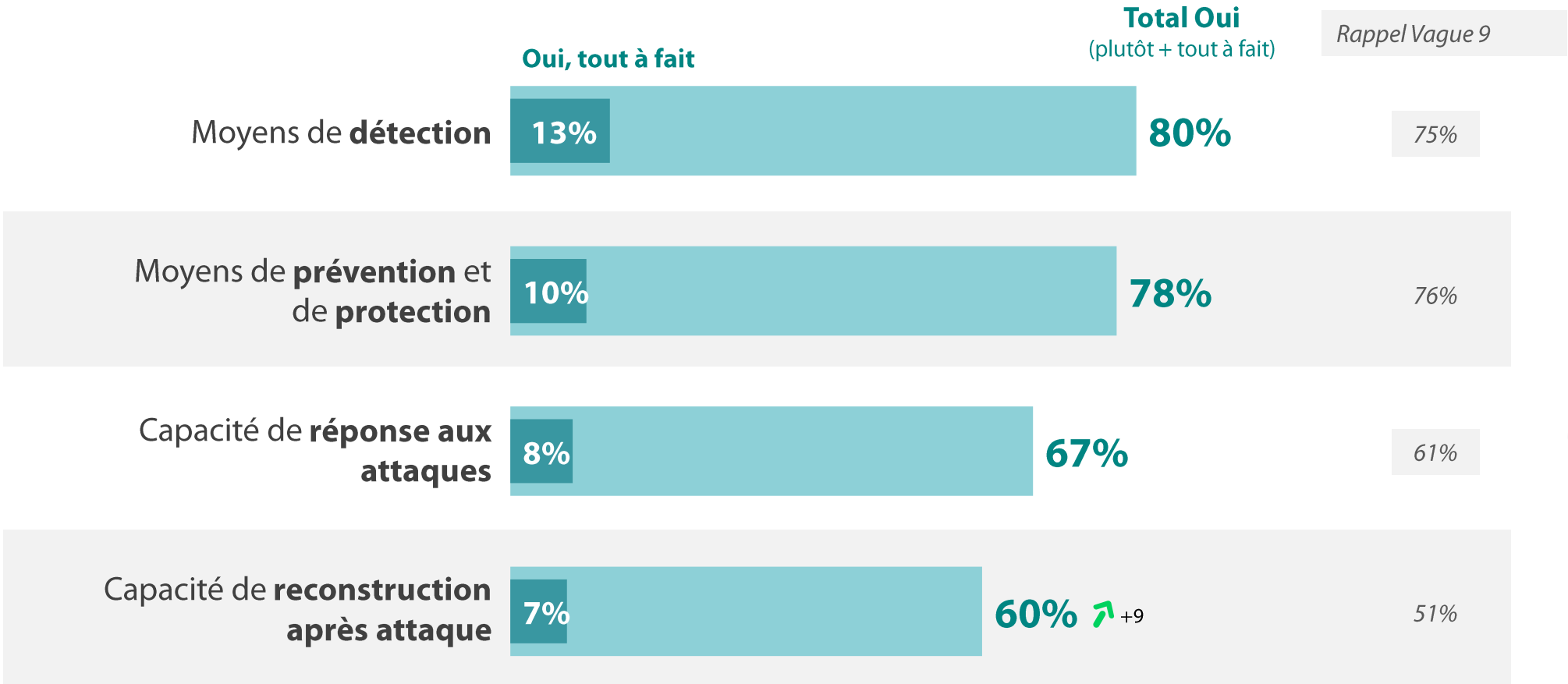


Nouvel item

Si les entreprises ont toujours davantage confiance en leur capacité en amont de l'attaque (détection et prévention) plutôt qu'en aval (réponse et reconstruction), elles sont tout de même plus sereines cette année concernant leur reconstruction.

401 personnes

Q14. Selon vous, votre entreprise est-elle préparée à gérer une cyberattaque de grande ampleur en termes de…?
Base : ensemble

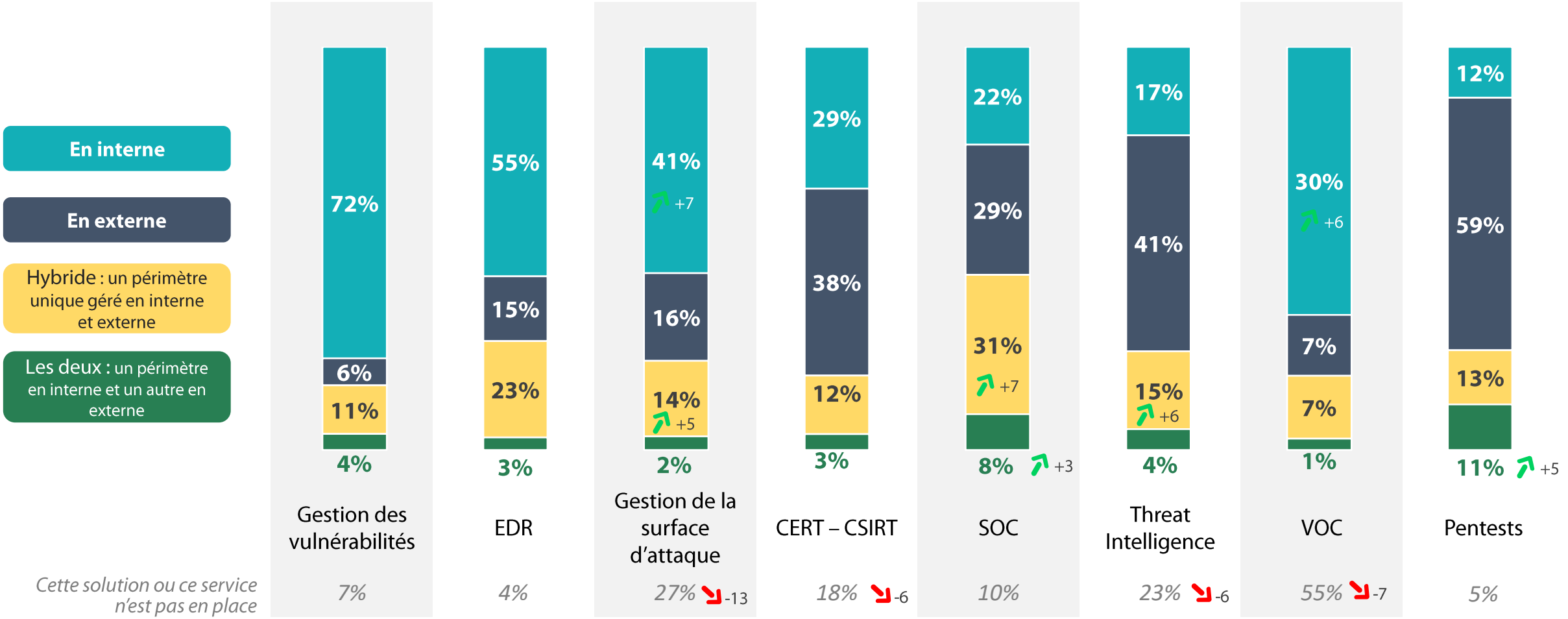


Une gestion différente en fonction des solutions : si les vulnérabilités, l'EDR, la surface d'attaque et le VOC sont principalement gérés en interne, les pentests, le threat intelligence, le CERT-CSIRT sont surtout externalisés, alors que le SOC combine gestion hybride, interne et externe.

401 personnes

Q30b. Comment opérez-vous les solutions et services ci-dessous ?

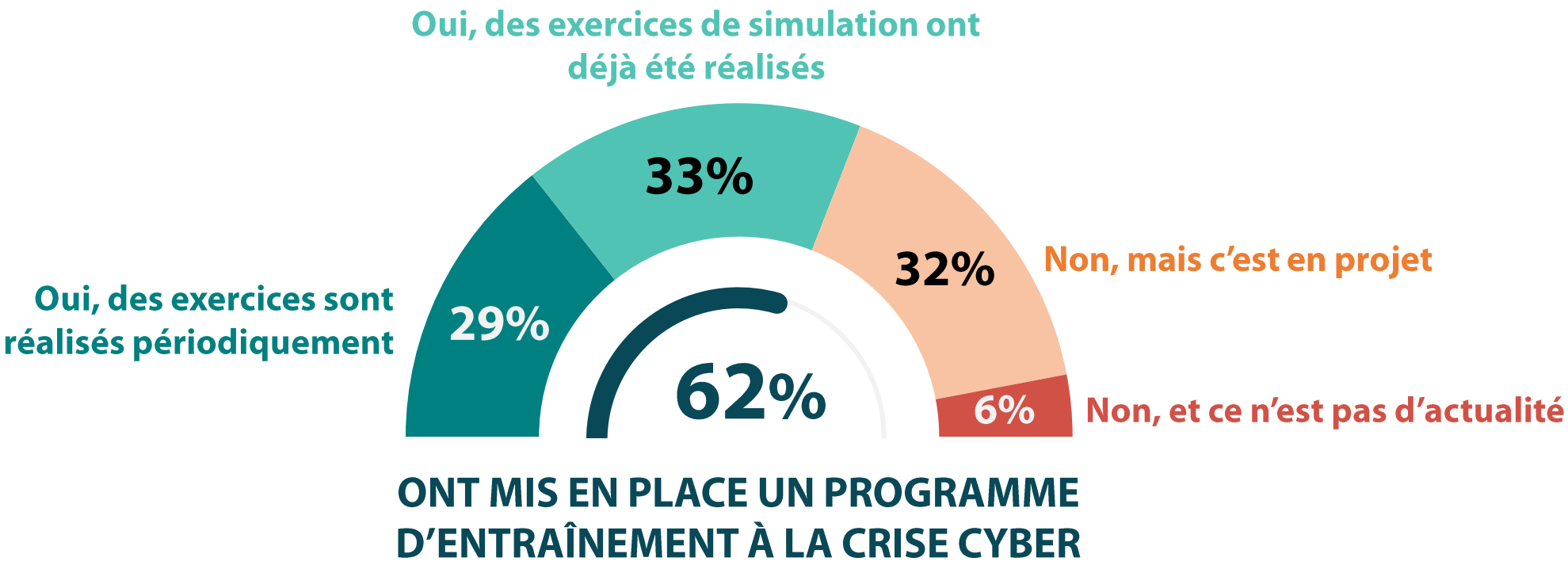
Base : ensemble – résultats hors solution non mise en place



6 entreprises sur 10 mettent en place un programme d'entrainement à la crise cyber, une proportion stable depuis l'année dernière.

401 personnes

Q15. Votre entreprise a-t-elle mis en place un programme d'entraînement à la crise cyber ?
Base : ensemble



Rappel Vague 9 : 57%

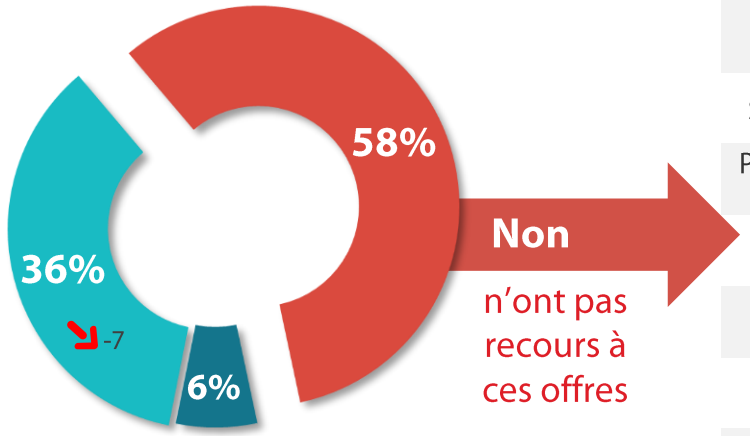
Le recours à des offres innovantes issues de startups concerne 4 entreprises sur 10. Pour les autres, le manque de budget explique leur réticence, de même que le manque de maturité des offres, en augmentation cette année. En revanche, de moins en moins d'entreprises considèrent cela comme une prise de risque.

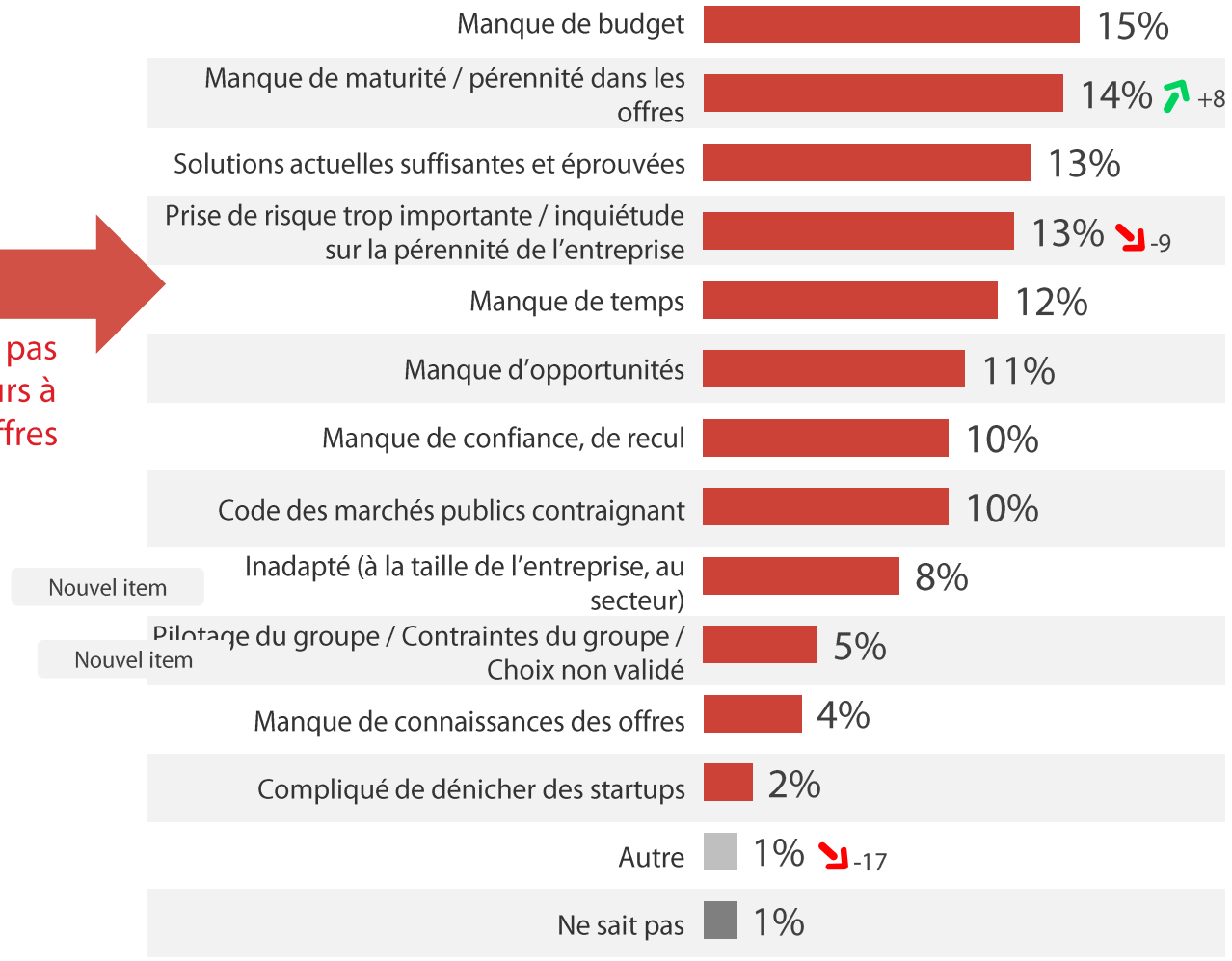
401 personnes

Q26. En matière de cybersécurité, recourrez-vous à des offres innovantes issues de startups ? *Base : ensemble*

Q26bis. Pour quelle(s) raison(s) ne le faites-vous pas ? *Base : ne fait pas appel à des offres issues de start-up – hors non-répondant (152)*

42% ont recours à des offres innovantes issues de startups



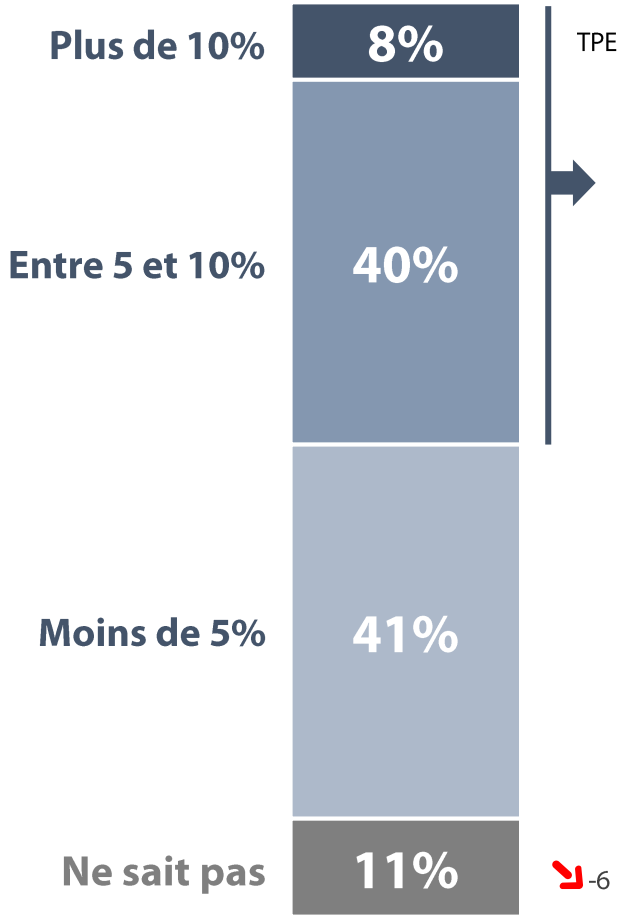


Évolution statistiquement significative par rapport à la vague précédente

Les budgets consacrés à la sécurité IT restent stables pour la 3ème année consécutive.

401 personnes

Q18. Dans votre entreprise, quelle part du budget IT/digital est consacrée à la sécurité ?
Base : ensemble

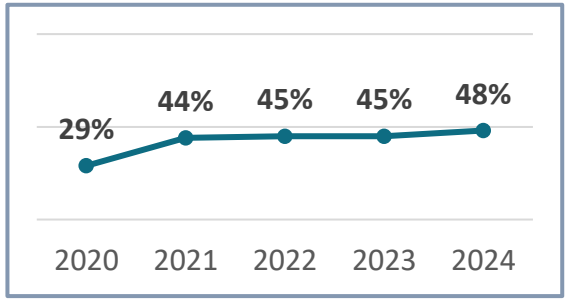


TPE / PME : 16%

5% ou plus du budget IT/digital est consacrée à la sécurité : 48%

Rappel Vague 9 : 45%

Rappel vagues précédentes



Les ¾ des entreprises identifient correctement leurs assets.

401 personnes

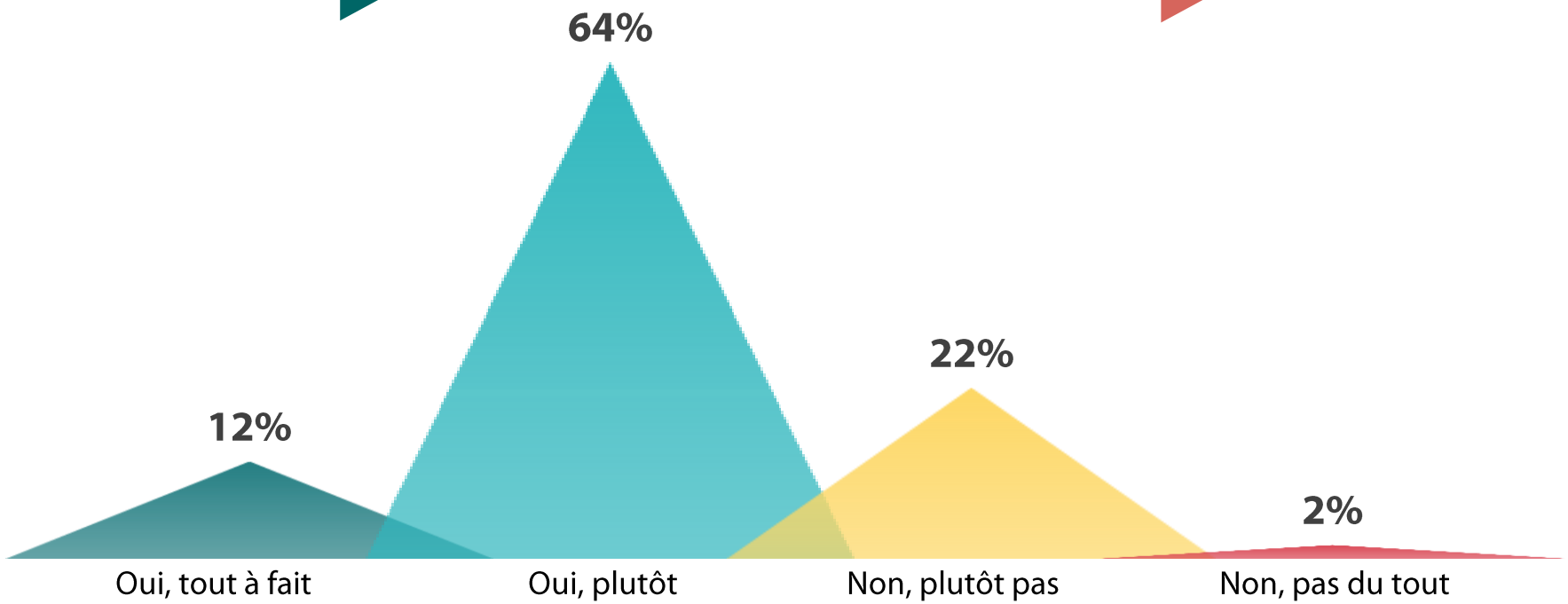
Nouvelle question en 2024

Q41 : Avez-vous une bonne identification de vos assets ?

Base : ensemble

76% Ont une bonne identification de leurs assets

N'ont pas une bonne identification de leurs assets **24%**



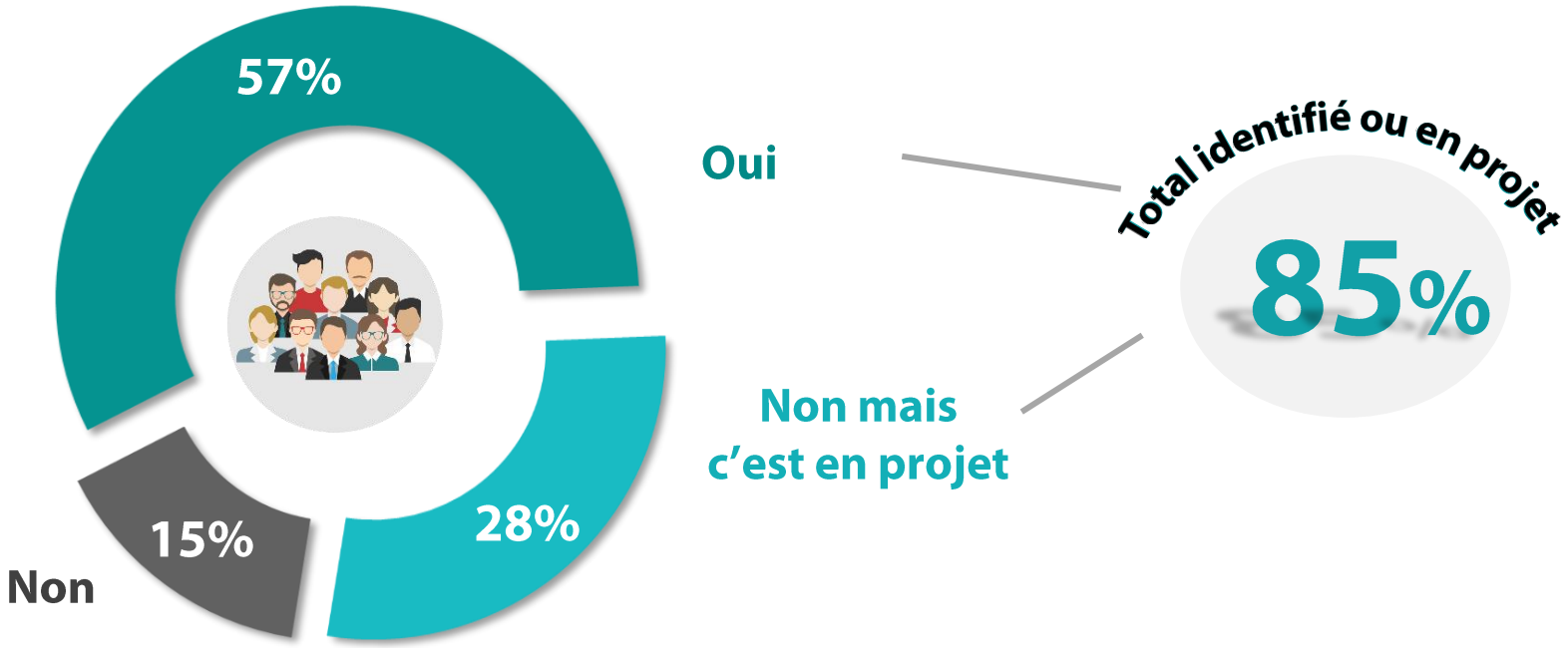
Il en est de même pour l'identification des assets critiques pour la grande majorité des entreprises : si plus de la moitié les identifient déjà, ¼ prévoit de le faire.

401 personnes

Nouvelle question en 2024

Q42 : Avez-vous clairement identifié et marqué les assets critiques (crown jewels) ?

Base : ensemble

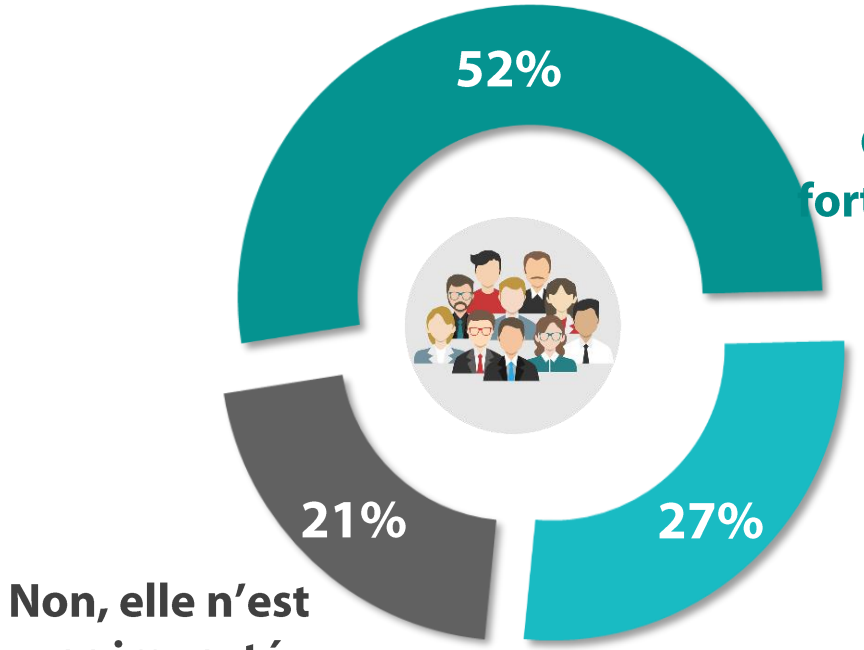


Les réglementations cyber (hors RGPD) ont une grande importance pour les entreprises : la majorité en est impactée, dont la moitié fortement.

401 personnes

Nouvelle question en 2024

Q46 : Votre société est-elle impactée par une ou plusieurs réglementations cyber (hors RGPD) ?
Base : ensemble



Oui, et elle est fortement impactée

Oui, mais elle est peu impactée

Non, elle n'est pas impactée

Total oui

79%

Grande entreprise : 85%

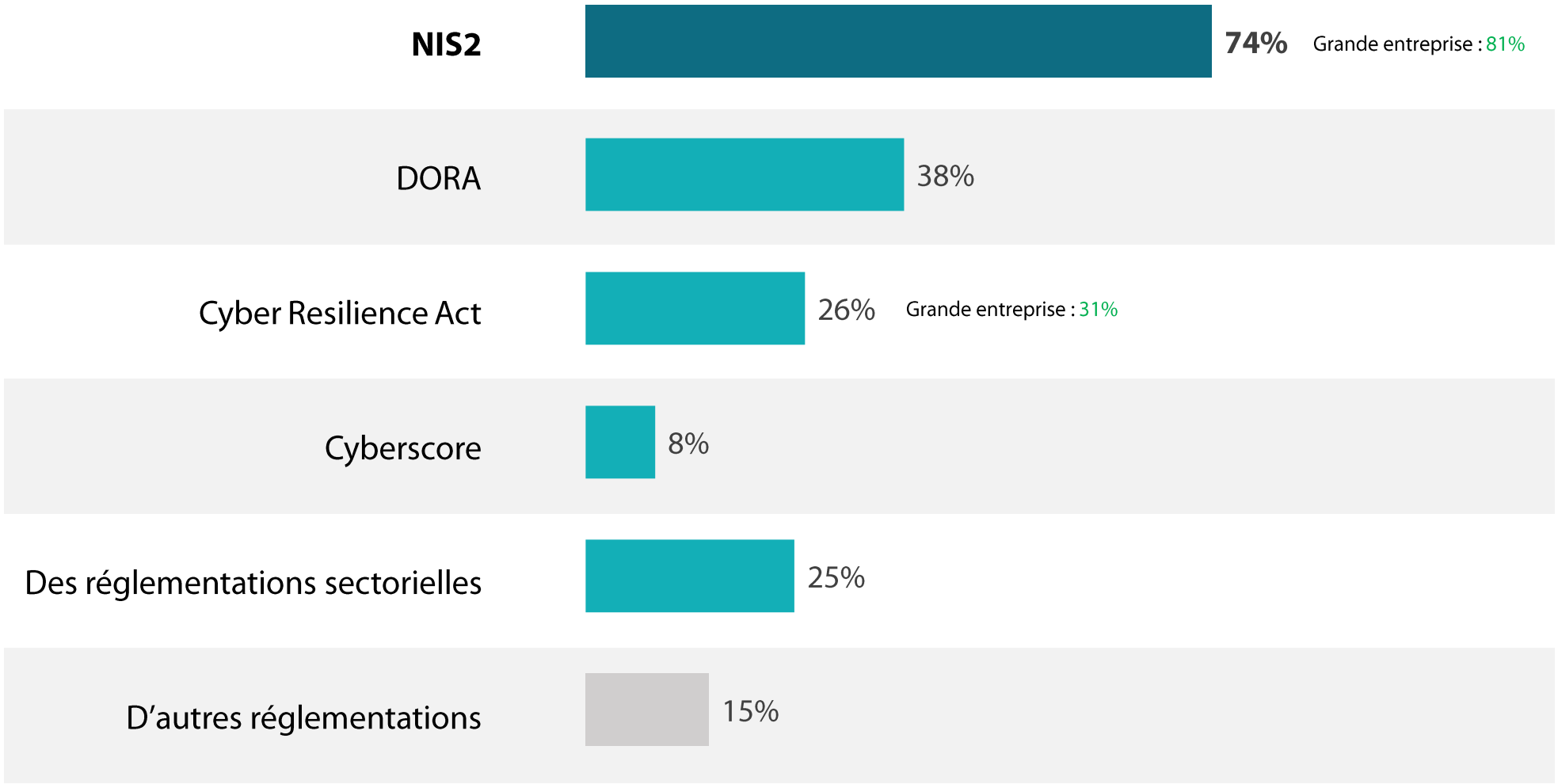
Dans le détail, c'est la réglementation NIS2 qui impacte principalement les entreprises, loin devant DORA et le Cyber Resilience Act. En parallèle, le Cyberscore reste minoritaire.

317 personnes

Nouvelle question en 2024

Q47 : Et par quelle(s) réglementation(s) cyber votre société est-elle impactée ?

Base : votre société est impactée par une ou plusieurs réglementations cyber (hors RGPD) - plusieurs réponses possibles



Focus sur…

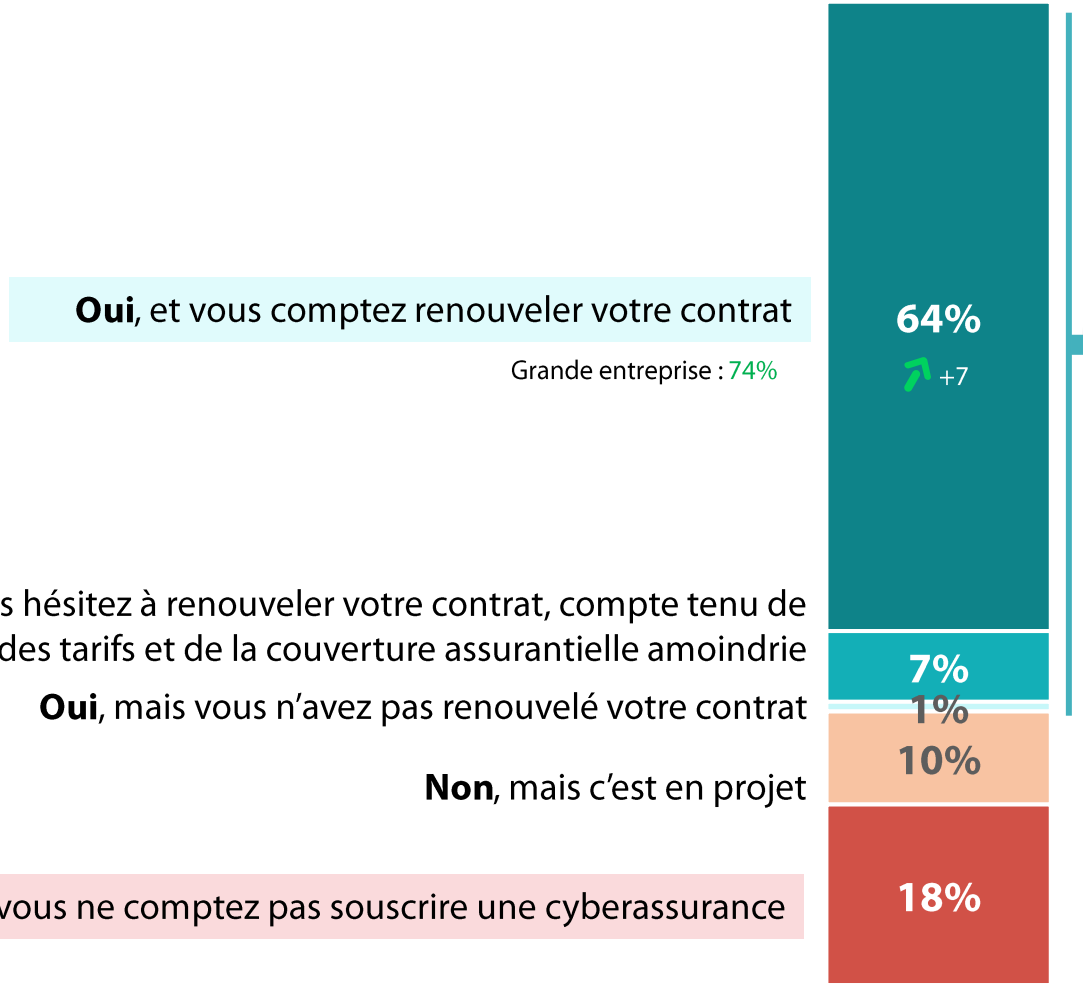
La cyberassurance

Les cyberassurances assoient leur présence sur le marché : si la proportion d'entreprises ayant souscrit une cyberassurance reste stable en 2024 (7/10), de plus en plus d'entreprises prévoient de renouveler leur contrat.

401 personnes

Q31. Avez-vous souscrit une cyberassurance ?

Base : ensemble



72% **Ont souscrit une cyberassurance**

Rappel Vague 9 : 70%

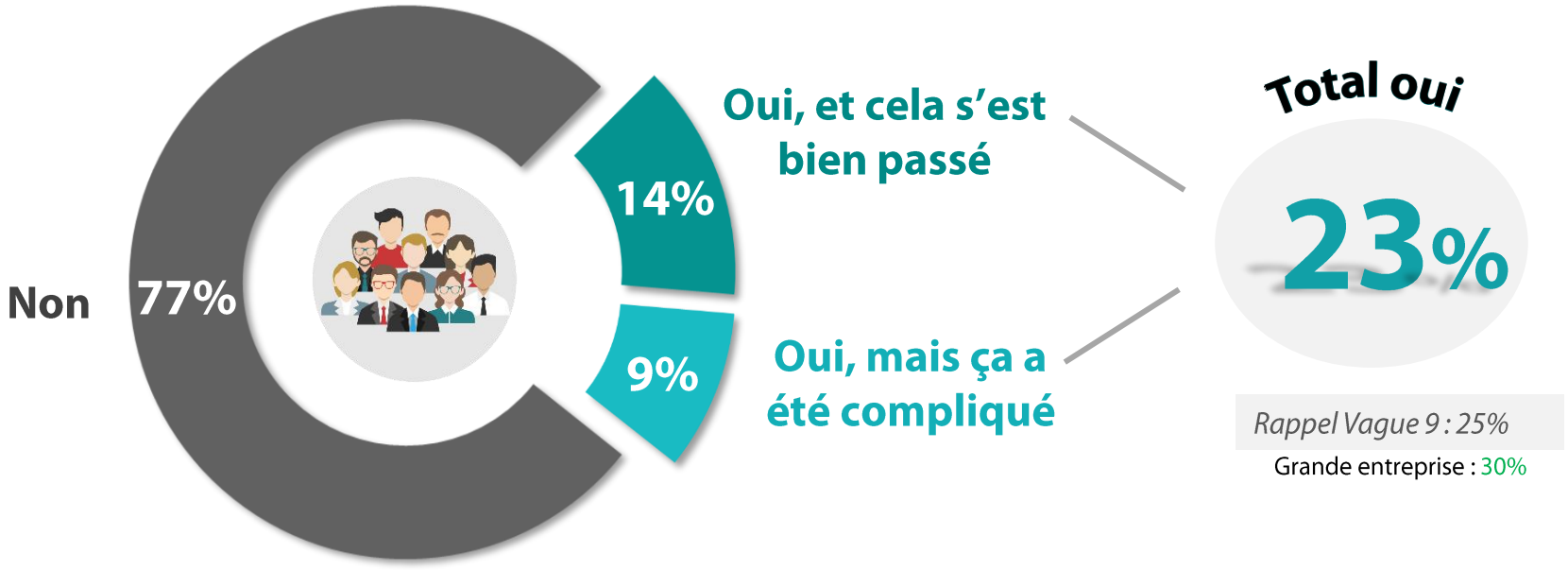
Grande entreprise : 80%

Pour autant, un quart seulement des entreprises a déjà fait appel à sa cyberassurance dans le cadre d'une attaque.

289 personnes

Q32. Votre entreprise a-t-elle déjà fait appel à sa cyberassurance dans le cadre d'une cyberattaque ?
Base : possède une cyberassurance ou projette d'en posséder une

Utilisation de la cyberassurance

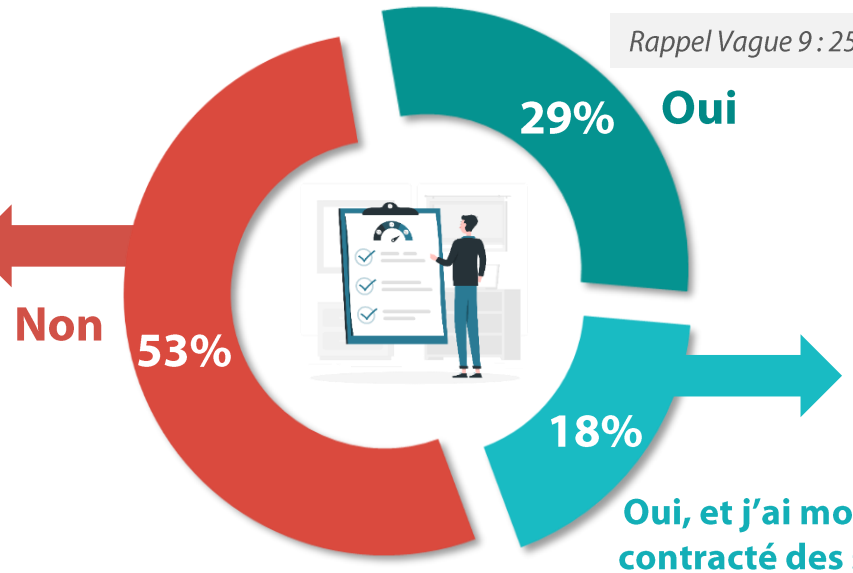


La perception du recours aux agences de notation par les cyberassureurs divise les entreprises : la moitié estimant que c'est une bonne idée favorise surtout l'opportunité de connaitre la vision des tiers sur leur société. Les autres ne sont pas convaincus de l'analyse et des scores réalisés par ces agences.

401 personnes

Q33. Les cyber-assureurs ont de plus en plus recours au service d'agences de notation. Est-ce une bonne chose selon vous ? *Base : ensemble*
Q33b. Et pour quelle raison avez-vous contracté les services de cyber-rating ? *Base : ont contracté des services de cyberrating (72)*
Q33bis. Pour quelles raisons ? *Base : estiment que ce n'est pas une bonne chose (212)*

Le recours au service d'agences de notation



Rappel Vague 9 : 25%

Rappel Vague 9 : 57%

Rappel Vague 9 : 18%

Parce que ces plateformes ne font par construction qu'une analyse très partielle du niveau de sécurité et fournissent un score par extrapolation **68%**

Parce que les critères et le mode de calcul des scores sont contestables du point de vue des priorités définies **63%**

Nouvel item — Parce qu'il y a trop d'opacité et d'instabilité dans les calculs de scores **55%**

Parce que les résultats ne sont pas fiables dans l'identification et l'assignation des assets **53%**

Parce que ces services constituent une forme de vente forcée de solution **38%**

Pour une autre raison **3%**

65% Pour connaître la vision cyber qu'ont des tiers sur ma société — Nouvel item

57% Je considère que c'est utile à ma surveillance — Nouvel item

49% Pour améliorer mon rating car c'est un indicateur demandé / suivi par mon Comité Exécutif — Nouvel item

42% Pour appréhender le niveau de sécurité de mes tiers — Nouvel item

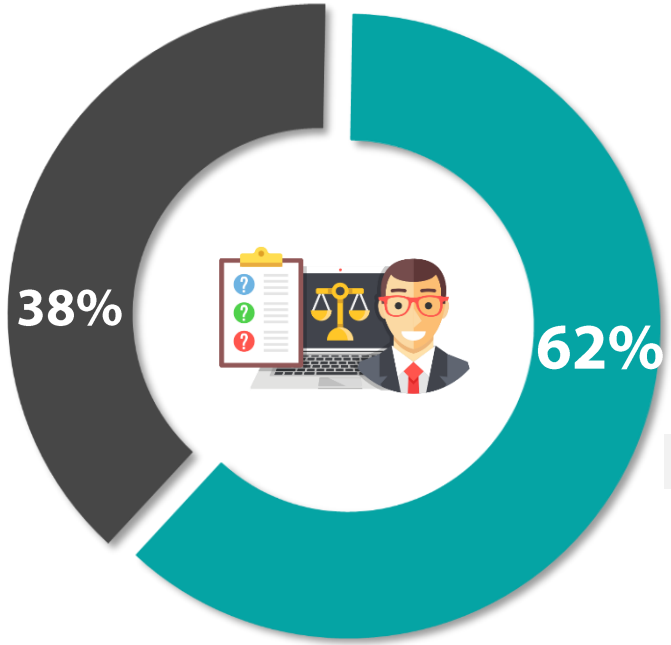
6% Autre raison

Près des 2/3 des entreprises portent plainte en cas de cyberattaque, dont près d'1/3 pour toutes les attaques.

190 personnes

Q8. Avez-vous porté plainte à la suite de la cyberattaque / des cyberattaques dont votre entreprise a été victime ?
Base : ont constaté une attaque

47% des entreprises ont subi au moins une cyberattaque en 2023



Rappel Vague 9 : 59%

pour **toutes les attaques** : **29%**

pour **certaines attaques** : **33%**

03

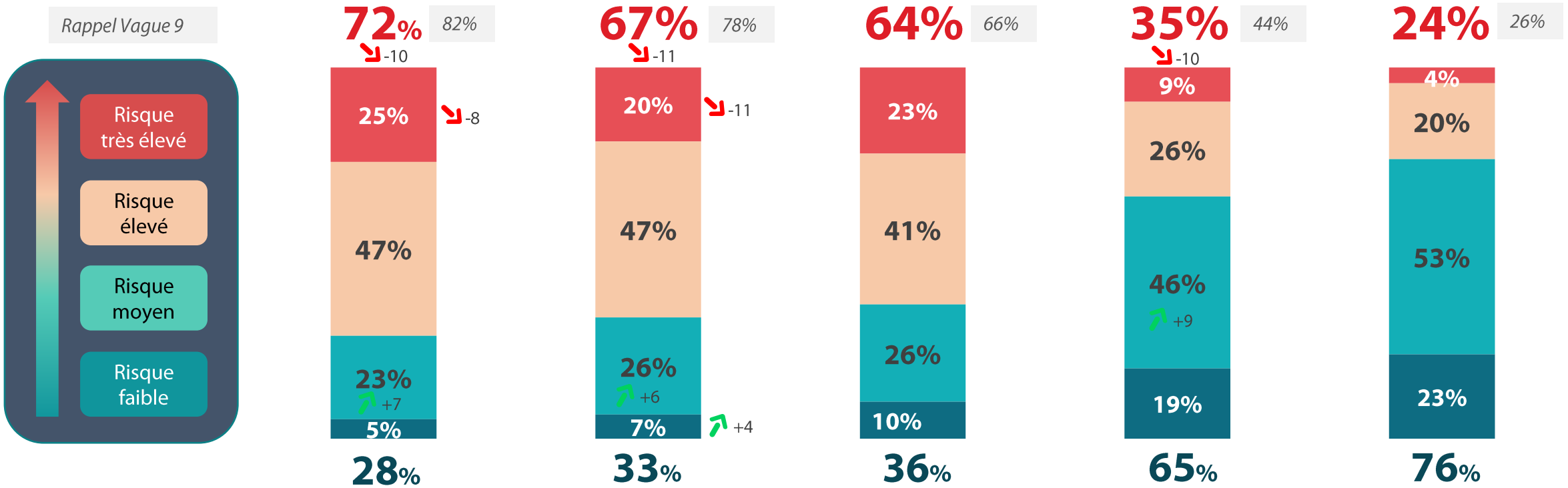
Des risques plus contenus concernant les usages numériques grâce une sensibilisation et une formation des collaborateurs efficaces

Le niveau de risques des usages numériques des salariés recule cette année concernant le Shadow IT et les partages de données via le collaboratif cloud (bien que le risque reste élevé), ainsi que pour l'usage à des fins personnelles des devices de l'entreprise.

401 personnes

Q23. Comment évaluez-vous le niveau de risque induit par les usages suivants du numérique par les salariés ?

Base : ensemble



Le recours massif aux services cloud non approuvés (Shadow IT)

La gestion des partages de données par les utilisateurs eux-mêmes dans le cas du collaboratif cloud

L'utilisation de devices personnels pour se connecter aux applications de l'entreprise (BYOD)

L'usage à des fins personnelles des devices fournis par l'entreprise (COPE)

Item modifié

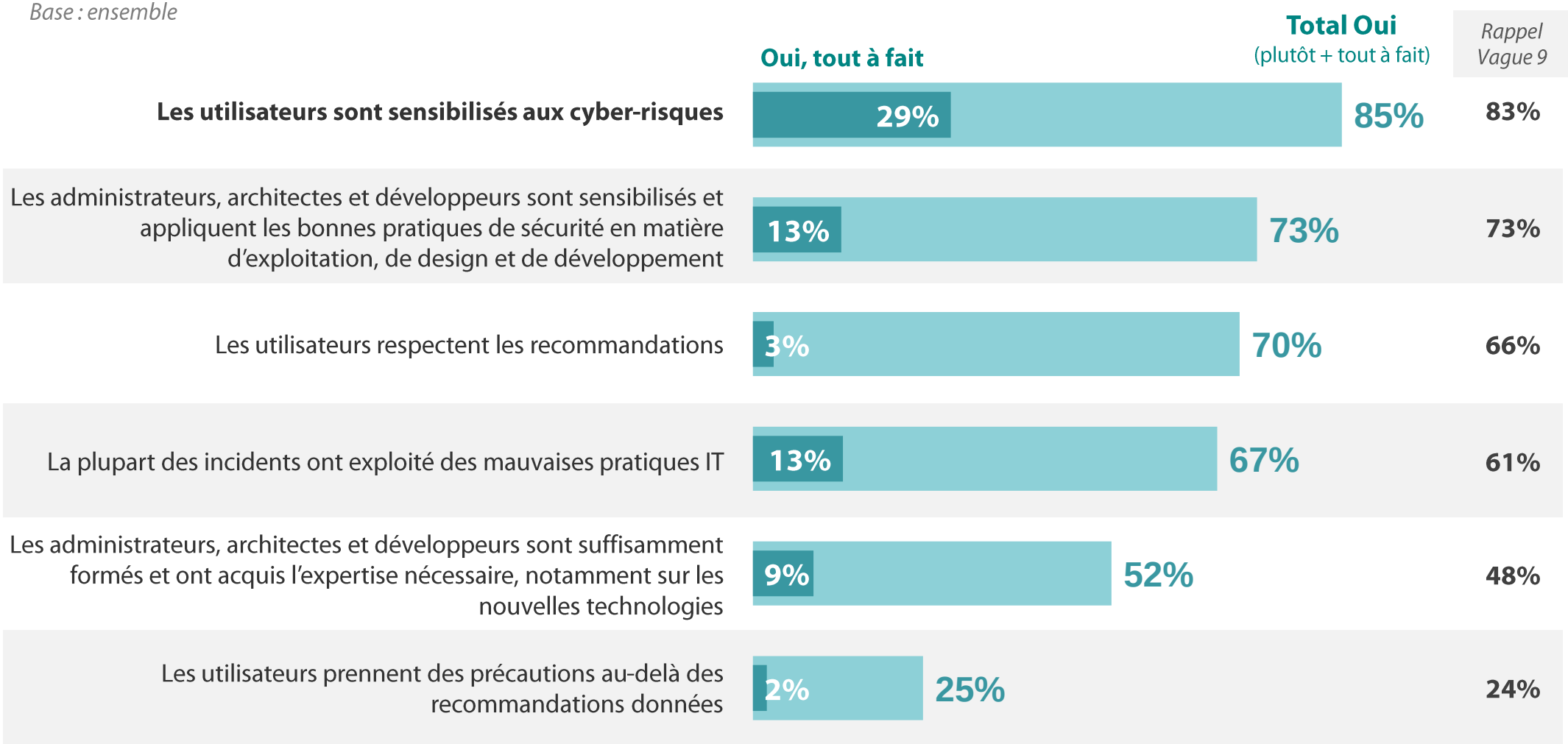
Le télétravail, l'accès au réseau en mobilité

La sensibilisation et la formation de l'ensemble des collaborateurs (utilisateurs, administrateurs, architectes et développeurs) à la cybersécurité reste stable cette année, les entreprises ayant particulièrement confiance en la sensibilisation aux risques cyber.

401 personnes

Q19. En ce qui concerne la sensibilisation et la formation des salariés à la cybersécurité, pensez-vous que ?

Base : ensemble



Focus sur…

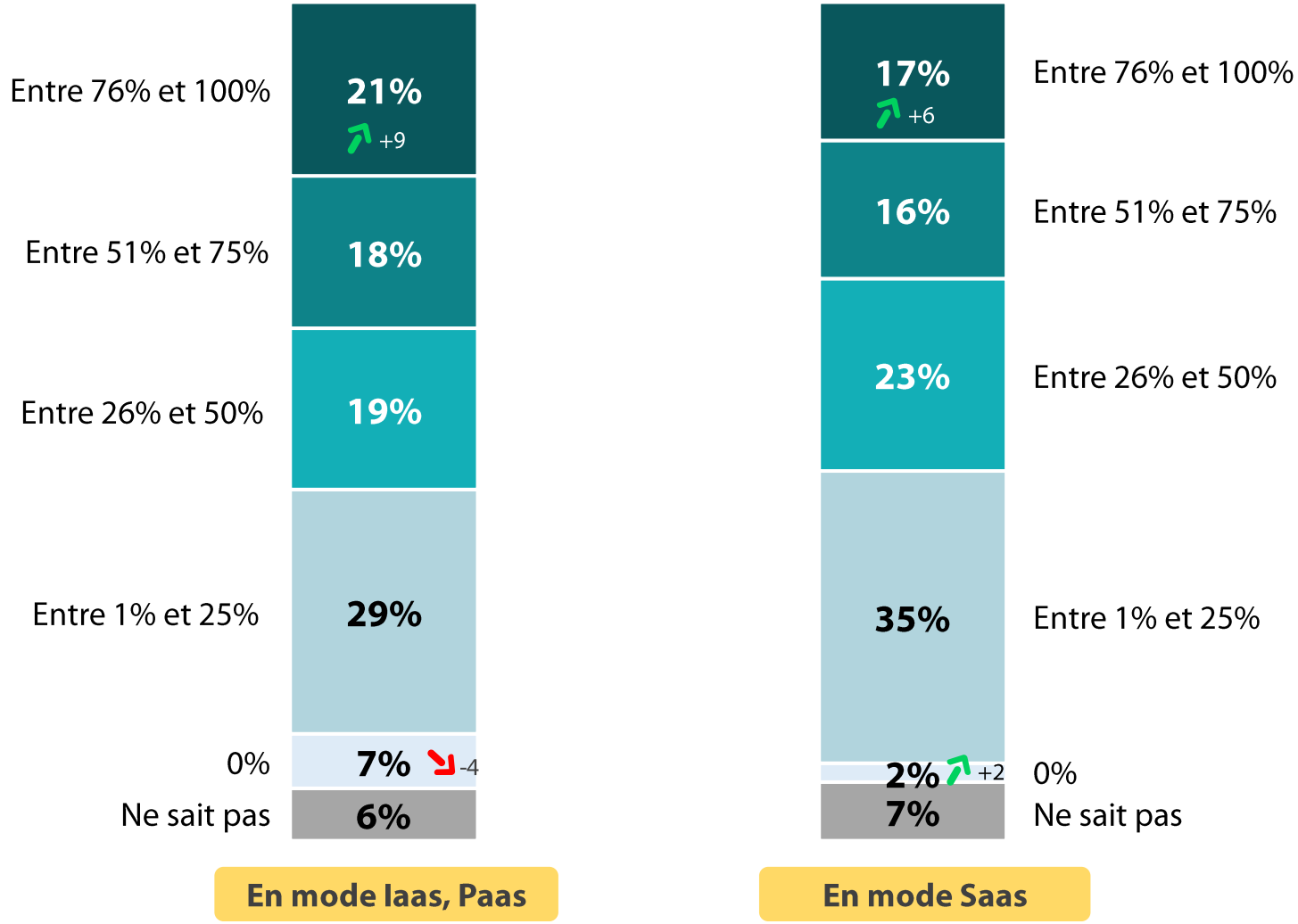
Le Cloud

Pour les deux modes Iaas/Pass et Saas, le cloud est adopté par moins de 50% du SI dans la majorité des entreprises. On notera la progression de ceux l'adoptant à plus de 75%.

401 personnes

Q20b. Quelle est la part d'adoption du Cloud dans votre SI, que ce soit en mode Iaas, Paas ou Saas ?

Base : ensemble



Les risques de l'utilisation du Cloud résident principalement dans la maitrise des sous-traitants (bien qu'en recul depuis 2023), la difficulté de mener des audits et le contrôle des accès par les administrateurs (en baisse également). La mauvaise visibilité de l'inventaire des ressources du Cloud est moins risquée cette année pour les entreprises (alors que c'était le 3ème risque en 2023).

401 personnes

Q21. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ?

Base : ensemble

Rappel classement 2023		% Un risque fort	
↘ -9	1	40%	**Non maîtrise de la chaîne de sous-traitance de l'hébergeur**
		37%	**Difficulté de mener des audits (test d'intrusion, contrôle des configurations, visite sur site)**
↘ -7	2	36%	**Difficulté de contrôler les accès par des administrateurs de l'hébergeur**
		34%	Expertise encore trop rare, attendue de la part des architectes et des administrateurs
	5	34%	Stockage des données dans des datacenters à l'étranger, hors du droit français
	4	34%	Stockage des données en France/Europe mais assuré et/ou opéré par des prestataires étrangers où la loi du pays d'origine s'applique également
		33%	Maîtrise difficile de l'utilisation qui en est faite par les salariés de votre entreprise
		32%	Défaut de cloisonnement entre les différents clients de l'hébergeur
		31%	Indisponibilité des données / de l'application due à une attaque de l'hébergeur
↘ -10	3	31%	Mauvaise visibilité de l'inventaire des ressources qu'il y a dans le cloud
		29%	Confidentialité des données vis-à-vis de l'hébergeur
↘ -7		29%	Non-maîtrise des paramètres de sécurité / chiffrement faible de la part de l'hébergeur (l'hébergeur gère les clés de déchiffrement)
		26%	Forte fréquence des nouvelles versions mises en ligne avec des potentielles évolutions non contrôlées des principes ou paramètres de sécurité
		25%	Propagation systémique des attaques et erreurs humaines qui surviendraient au niveau de l'hébergeur
		25%	Difficulté ou impossibilité d'alimenter le SIEM par des logs provenant du Cloud
↘ -10		23%	Non-effacement des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
↘ -7		23%	Attaque par rebond depuis l'hébergeur
↘ -7		22%	Non-effacement des données au cours de l'usage, les suppressions et purges opérées par le client n'étant pas réellement effectives
		22%	Traitement et exploitation des données par l'hébergeur à l'insu de ses clients
		21%	Non-restitution des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
		15%	Piégeage d'une application hébergée

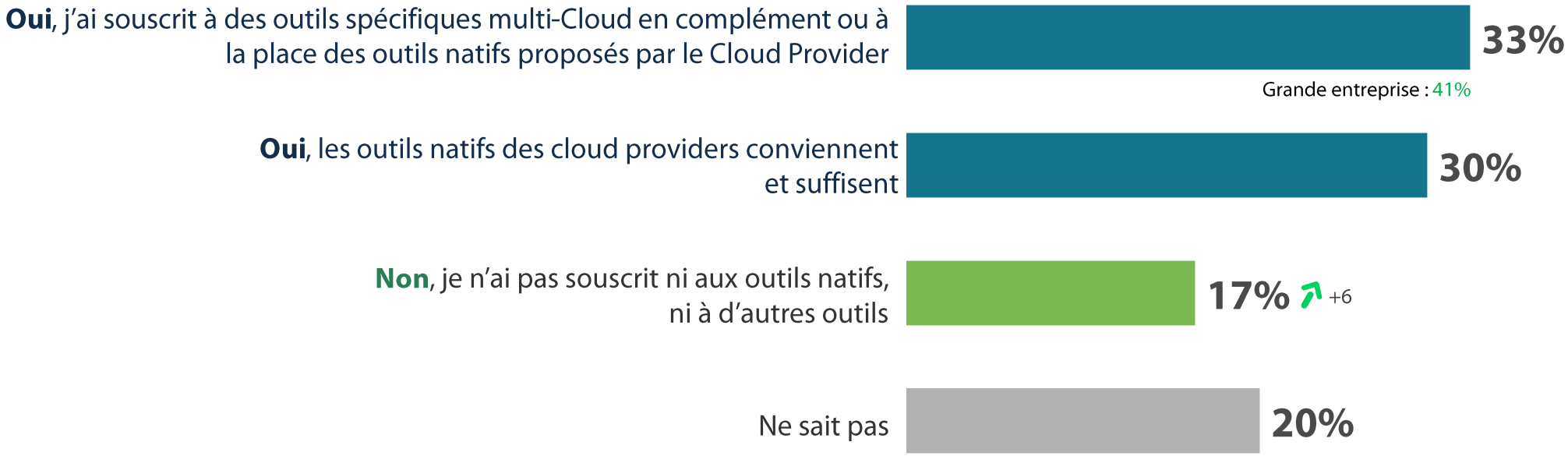
Près des 2/3 des entreprises estiment que la sécurisation des données stockées dans le Cloud nécessite des outils spécifiques, dont 1/3 ayant souscrit des outils supplémentaires à cet effet.

401 personnes

Q22b. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?
Base : ensemble

… 63% estiment que la sécurisation des données stockées dans le Cloud requiert des outils spécifiques

Grande entreprise : 70%



La moitié des entreprises se sent concernée par le sujet de la souveraineté et le Cloud de Confiance, dans les mêmes proportions que l'année précédente.

401 personnes

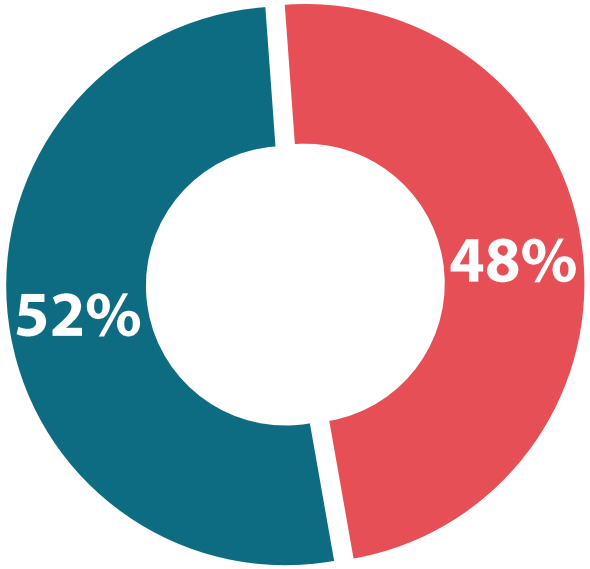
Q35. De nombreuses initiatives ont récemment vu le jour en matière de souveraineté et de Cloud de Confiance. Vous sentez-vous concerné par ces sujets ?

Base : ensemble

Souveraineté et Cloud de Confiance

Oui, c'est un sujet de préoccupation pour mon entreprise

TPE / PME : 71%



Non, mon entreprise ne se sent pas concernée par ces sujets

04

Une adaptation nécessaire des entreprises pour accompagner les transformations numériques, dont l'essor de l'IA

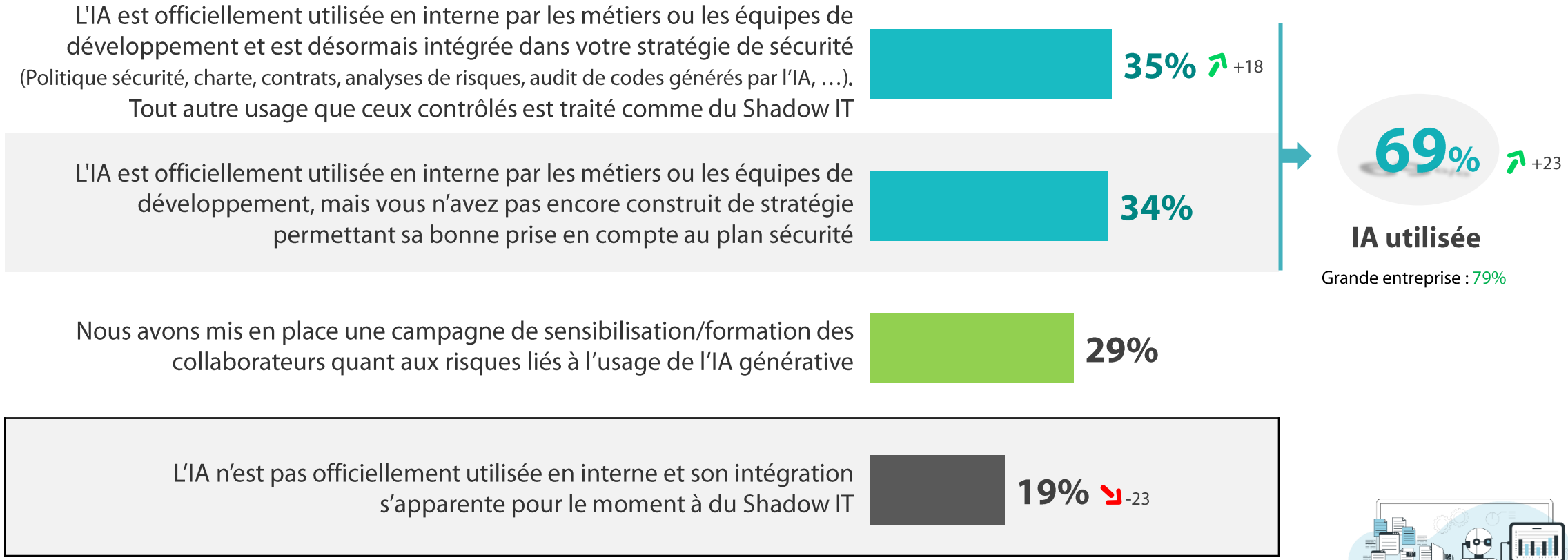
Le recours à l'IA a fortement progressé depuis 2023 pour concerner aujourd'hui 7 entreprises sur 10, dont 1/3 l'ayant officiellement intégrée dans la stratégie de sécurité.

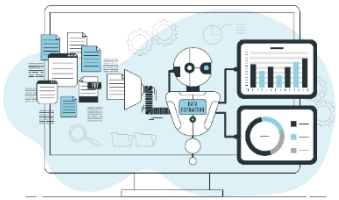
401 personnes

Question modifiée en 2024

Q39. L'IA, déjà plus ou moins utilisée dans certaines solutions cyber, s'est imposée dans nos SI avec notamment un grand nombre d'initiatives autour de l'IA générative. Quelle est la place de l'IA aujourd'hui dans votre organisation ?

Base : ensemble





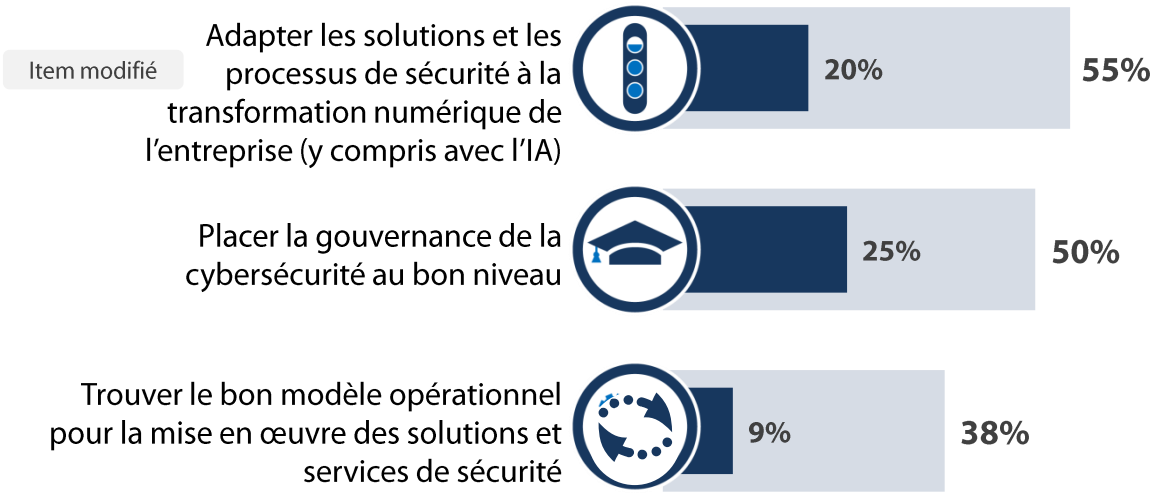
L'adaptation des solutions et des processus de sécurité aux transformations numériques reste essentielle dans ce contexte de développement de l'IA, premier enjeu identifié pour l'avenir de la cybersécurité.

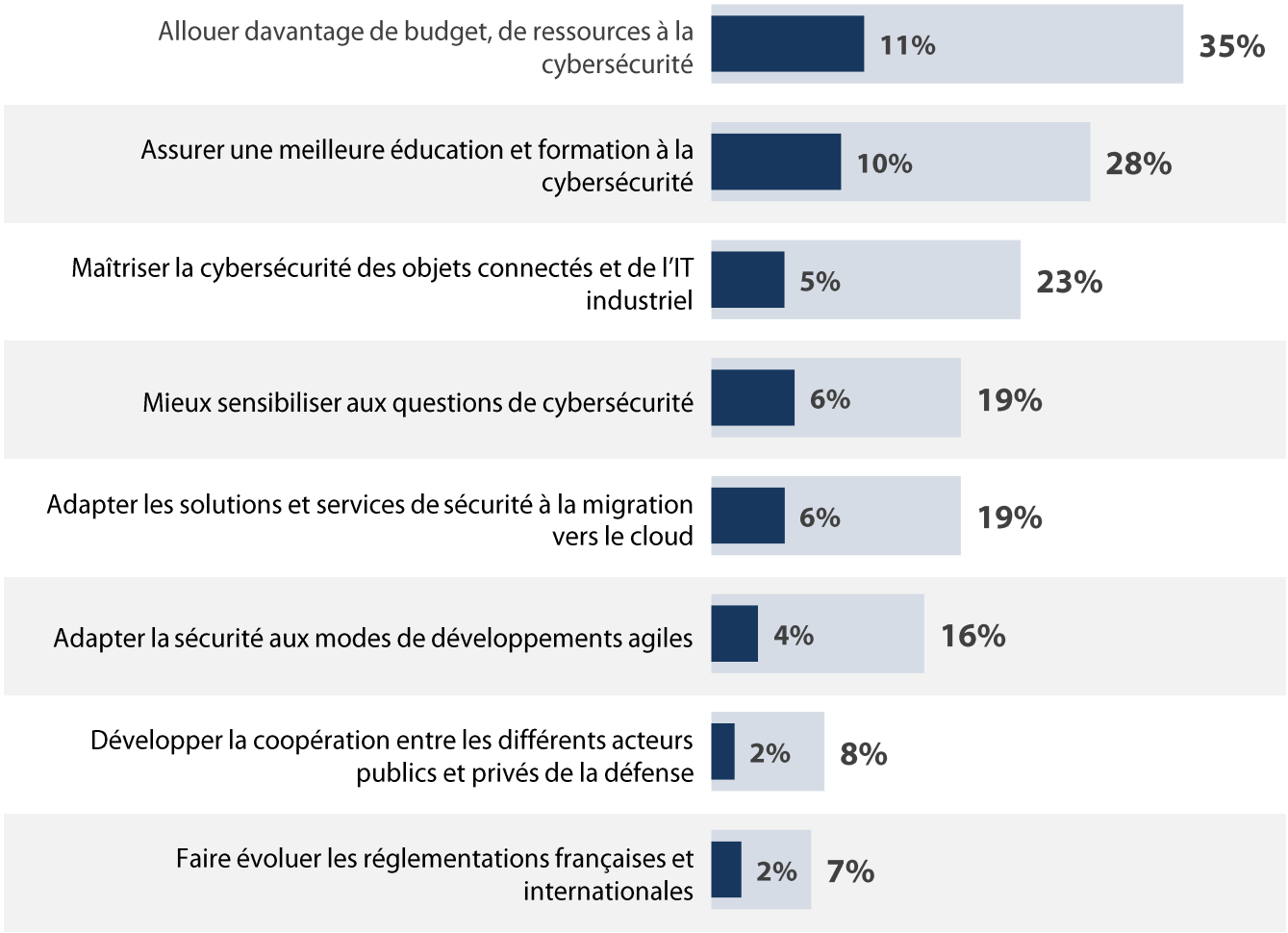
401 personnes

Q27. Parmi les enjeux suivants, quels sont selon vous les trois enjeux de demain pour l'avenir de la cybersécurité des entreprises ?

Base : ensemble

TOP3 des enjeux



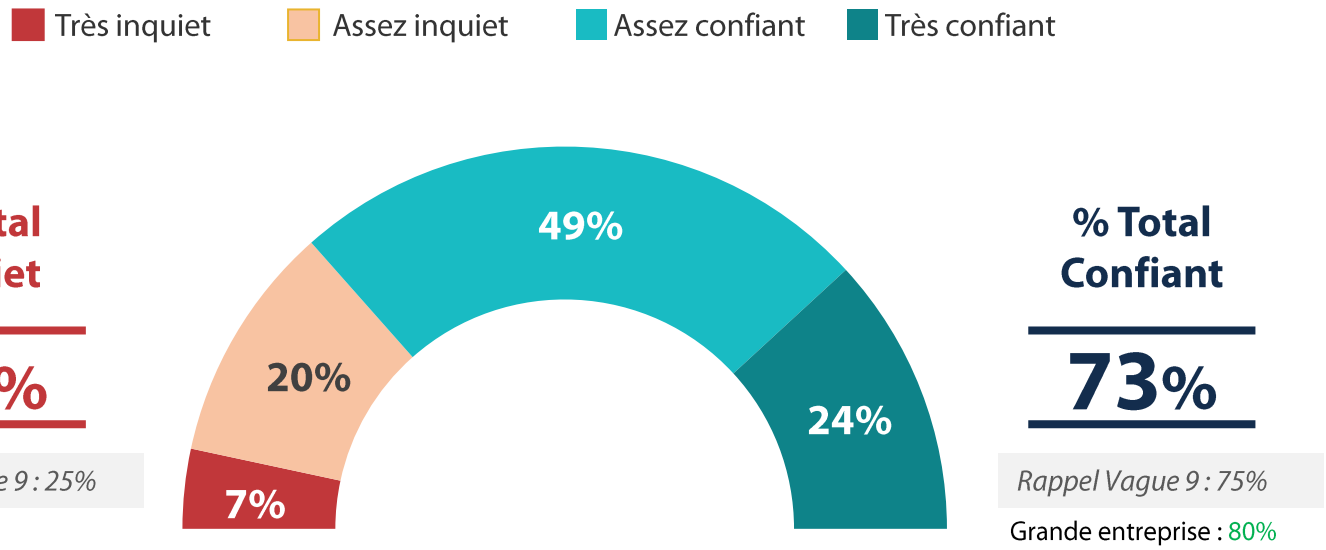


¾ des entreprises ont confiance en leur COMEX pour mesurer l'ampleur des enjeux de la cybersécurité, dans les mêmes mesures qu'en 2023.

401 personnes

Q24. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble

La **prise en compte des enjeux** de la cybersécurité au sein du COMEX de votre entreprise

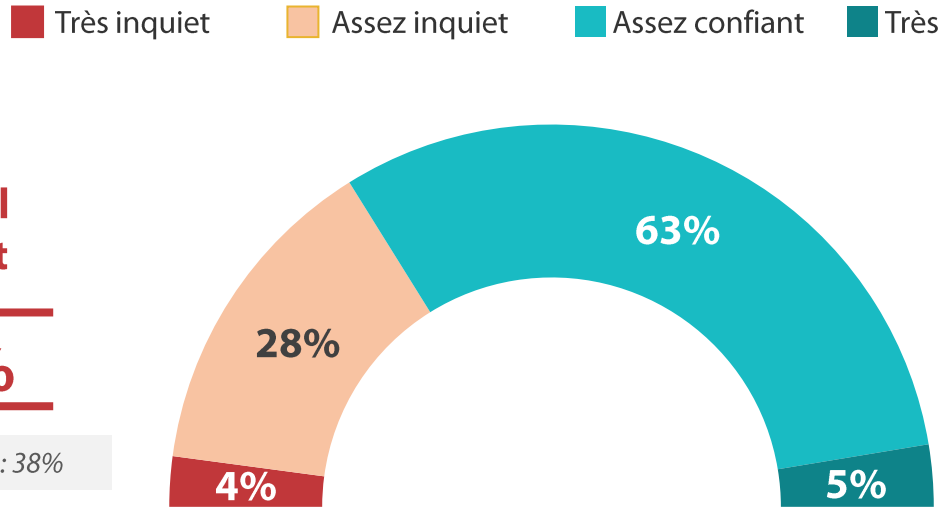


Au-delà de la prise en compte des enjeux, 7 entreprises sur 10 ont confiance en leur capacité à faire face aux risques cybers.

401 personnes

Q24. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble

La **capacité** de votre entreprise à **faire face aux cyber-risques**



% Total Inquiet

32%

Rappel Vague 9 : 38%

% Total Confiant

68%

Rappel Vague 9 : 62%

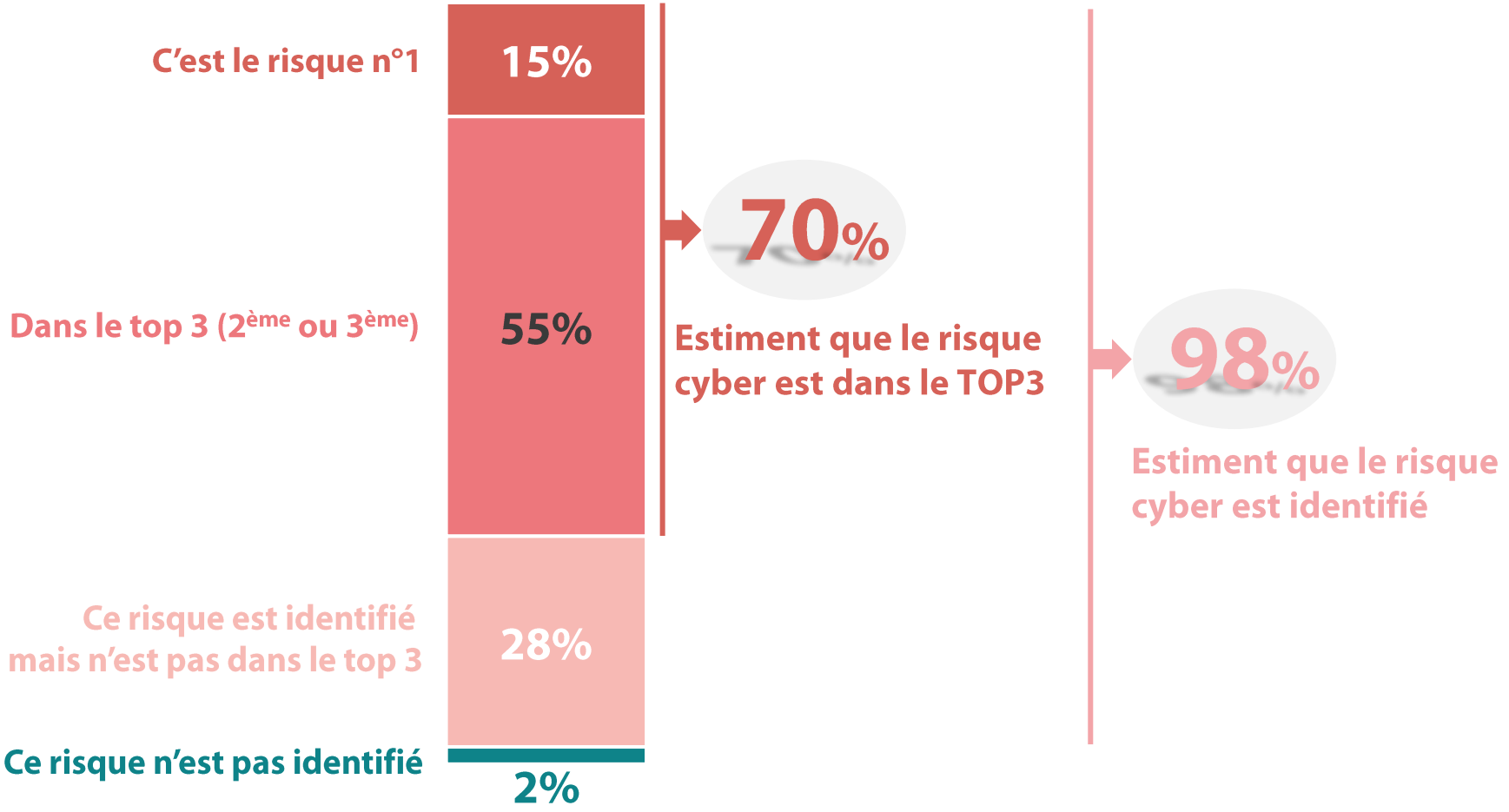
Grande entreprise : 75%

La quasi-totalité des entreprises identifient d'ailleurs le risque cyber dans leur cartographie des risques, dont 7/10 le positionnent même dans le TOP3.

401 personnes

Nouvelle question en 2024

Q48 : Comment le risque cyber est-il positionné dans la cartographie des risques de votre entreprise ?
Base : ensemble



Pour faire face au risque cyber, près de la moitié des entreprises envisagent d'augmenter leurs effectifs alloués à la cybersécurité, bien qu'elles soient moins nombreuses qu'en 2023 à le prévoir.

401 personnes

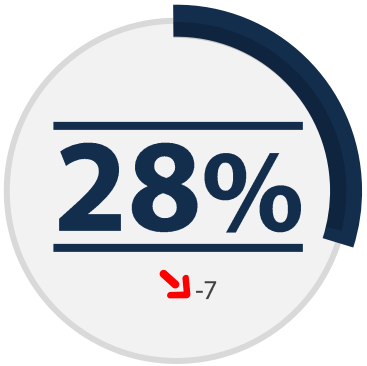
Q17. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ?
Base : ensemble

45% prévoient d'augmenter les effectifs alloués à la protection contre les risques cyber

Grande entreprise : 52%

Nouvel item

d'**augmenter les effectifs** alloués à la gouvernance de la protection contre les cyber-risques



d'**augmenter les effectifs** alloués à la cybersécurité opérationnelle de la protection contre les cyber-risques

d'**augmenter les effectifs** alloués à la culture sécurité, la sensibilisation, la formation

De même, la volonté d'acquérir de nouvelles solutions et d'augmenter les budgets est en baisse cette année.

401 personnes

Q17. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ?
Base : ensemble

d'**augmenter les budgets** alloués à la protection contre les cyber-risques

d'**acquérir de nouvelles solutions techniques** destinées à la cybersécurité

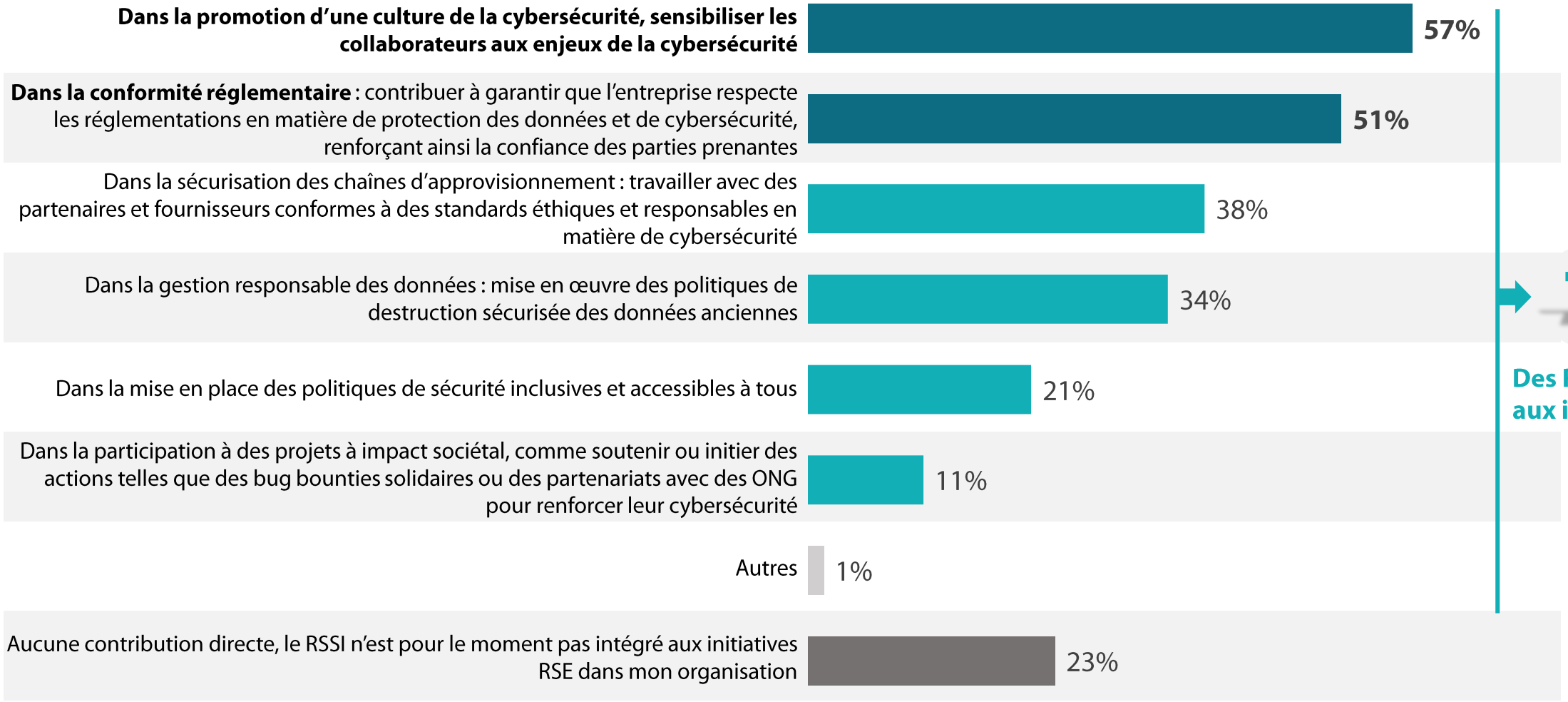
Les ¾ des RSSI sont intégrés aux initiatives RSE de leur entreprise, notamment via la promotion d'une culture de la cybersécurité et la conformité réglementaire.

401 personnes

Nouvelle question en 2024

Q49 : Dans quelle mesure votre rôle contribue, ou pourrait contribuer aux objectifs de responsabilité sociétale et environnementale (RSE) de votre organisation ?

Base : ensemble - plusieurs réponses possibles



La synthèse

Synthèse (1/4)

Un nombre de cyberattaques stable depuis 2023, avec peu d'innovations concernant les méthodes et les impacts des attaques

Dans les mêmes proportions que l'année dernière, une entreprise sur deux a subi au moins une cyberattaque réussie en 2024 (47%).

Les stratégies demeurent similaires à l'année précédente, le phishing, spear phishing et smishing constituant cette année encore les vecteurs principaux d'attaque (60%), suivis par l'exploitation d'une faille (47%) et le déni de service (41%).

En conséquence de ces attaques, les vols de données ont augmenté en 2024 (42%, +11 points), et le déni de service reste stable (36%). L'usurpation d'identité (34%) complète le trio des impacts principaux. En parallèle, les données chiffrées par un ransomware diminuent (9%, -9 points).

Les tiers sont également sources d'incidents, principalement via des mauvaises pratiques (28%). Pour s'en protéger, les entreprises misent surtout sur les clauses sécurité dans les contrats (85%), ainsi que sur des questionnaires de sécurité (74%).

Le risque de cyberespionnage reste important pour les entreprises, 37% le considérant élevé.

Synthèse (2/4)

Une confiance renouvelée dans les moyens de défense emblématiques : les pares-feux, l'EDR et le MFA.

Les solutions et services de sécurité sont toujours adaptés aux besoins des entreprises pour 84% des RSSI. Si la plupart des solutions mesurées gagnent en efficacité cette année, les trois solutions plébiscitées assoient leur position : les pares-feux, l'EDR et le MFA, tant en termes d'efficacité que de déploiement dans les entreprises.

Les concepts Zero Trust et Vulnerability Operation Center (VOC) sont davantage mis en place dans les entreprises (respectivement 31%, +7 points et 26%, +9 points), de même que le Cyber Asset Attack Surface Management (CAASM) (11%, +5 points).

Les entreprises ont une bonne identification de leurs assets (76%) et de leurs assets critiques (crown jewels) (57%).

La grande majorité des entreprises sont impactées par les réglementations cyber (79%, dont 52% fortement), notamment par NIS2 (74% des entreprises concernées).

Des cyberassurances bien implantées dans le marché de la cybersécurité

La majorité des entreprises ont souscrit une cyberassurance (72%), dont 64% prévoient de renouveler leur contrat (+7 points). Près d'un quart d'entre elles (23%) ont d'ailleurs fait appel à cette cyberassurance dans le cadre d'une attaque.

Le recours aux agences de notation par les cyberassureurs continue de diviser les entreprises. 47% estiment que c'est une bonne chose, notamment car cela leur permet de connaitre la vision cyber qu'ont des tiers sur leur société (65% des entreprises concernées), alors que 53% affirment que ce n'est pas une bonne idée car sceptiques concernant les analyses et scores réalisés par les agences.

En parallèle, 62% des entreprises ont porté plainte à la suite d'une attaque cyber, un chiffre stable par rapport à 2023.

Synthèse (3/4)

Des comportements individuels moins risqués grâce à la sensibilisation et la formation permanente des collaborateurs

Si les usages numériques des salariés constituent toujours un risque pour les entreprises, ce risque diminue en 2024 pour le Shadow IT (72%, -10 points), la gestion des partages de données par les utilisateurs dans le collaboratif cloud (67%, -11 points) et l'usage à des fins personnelles des devices fournis par l'entreprise (COPE) (35%, -10 points).

Une amélioration des risques obtenue notamment grâce à la sensibilisation et la formation de l'ensemble des collaborateurs à la cybersécurité (85% des utilisateurs sont sensibilisés).

Le Cloud, un enjeu de sécurité réel pour les entreprises

L'adoption du Cloud dans les SI concerne moins de 50% des SI dans la majorité des entreprises, que ce soit en mode Iaas / Paas ou en mode Saas.

L'utilisation du Cloud représente un risque pour les entreprises, principalement dû à la non-maîtrise de la chaine de sous-traitance de l'hébergeur, bien que ce risque recule depuis 2023 (40%, -9 points). La difficulté de mener des audits (37%) et la difficulté de contrôler les accès par les administrateurs de l'hébergeur (36%, -7 points) participent également aux risques prioritaires du Cloud.

La sécurisation des données stockées dans le Cloud requiert d'ailleurs des outils spécifiques pour 63% des RSSI, dont 33% ont souscrit des outils spécifiques en complément des outils natifs du Cloud Provider.

Synthèse (4/4)

Des transformations numériques impliquant nécessairement une adaptation des entreprises, notamment pour prendre en compte l'essor de l'IA

Le recours à l'IA se démocratise dans les entreprises. 69% des entreprises l'utilisent aujourd'hui (soit une augmentation de +23 points depuis 2023), dont 35% (+18 points) qui l'ont officiellement intégrée dans leur stratégie de sécurité.

L'adaptation des solutions et des processus de sécurité aux transformations numériques reste ainsi l'enjeu principal pour l'avenir de la cybersécurité (55%).

Les RSSI démontrent toujours une confiance envers leur entreprise pour prendre en compte les enjeux de la cybersécurité (73%) et pour faire face aux risques cyber (68%).

Le risque cyber est d'ailleurs positionné au sein de la cartographie des risques de la quasi-totalité des entreprises (98%), dont 70% le placent dans le TOP3 des risques.

Malgré ces risques bien présents à l'esprit des entreprises, les prévisions d'augmentation des effectifs alloués à la protection contre les risques cyber reculent cette année (28%, -7 points pour une augmentation de budget alloué à la gouvernance de la protection contre les risques cyber et 34%, -13 points pour la cybersécurité opérationnelle de la protection contre les risques). De même, la volonté d'acquérir de nouvelles solutions techniques et d'augmenter les budgets est en baisse cette année.

En parallèle, 77% des RSSI sont intégrés aux initiatives RSE de leur entreprise, notamment via la promotion d'une culture de la cybersécurité (57%) et via la conformité réglementaire (51%).

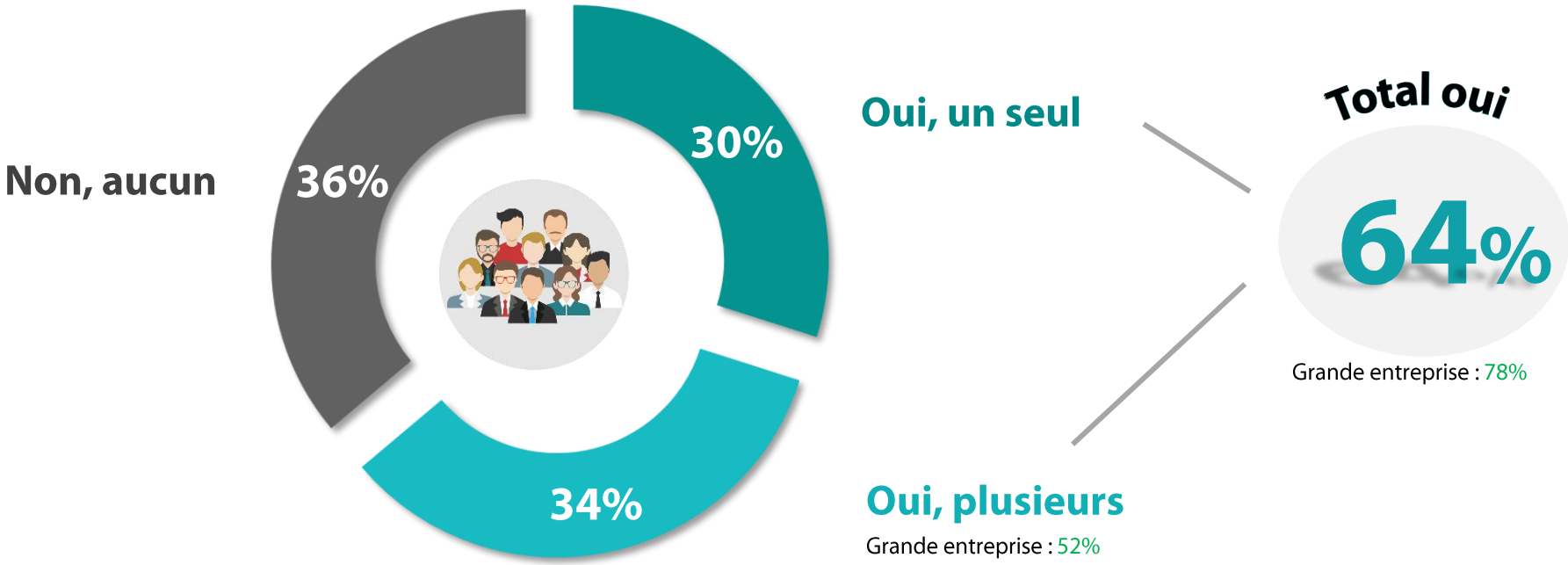
Les annexes

2/3 des entreprises ont intégré des alternants cette année, dont 1/3 qui en a recruté plusieurs.

401 personnes

Nouvelle question en 2024

Q44 : Au cours des 12 derniers mois, avez-vous intégré des étudiants en alternance ?
Base : ensemble



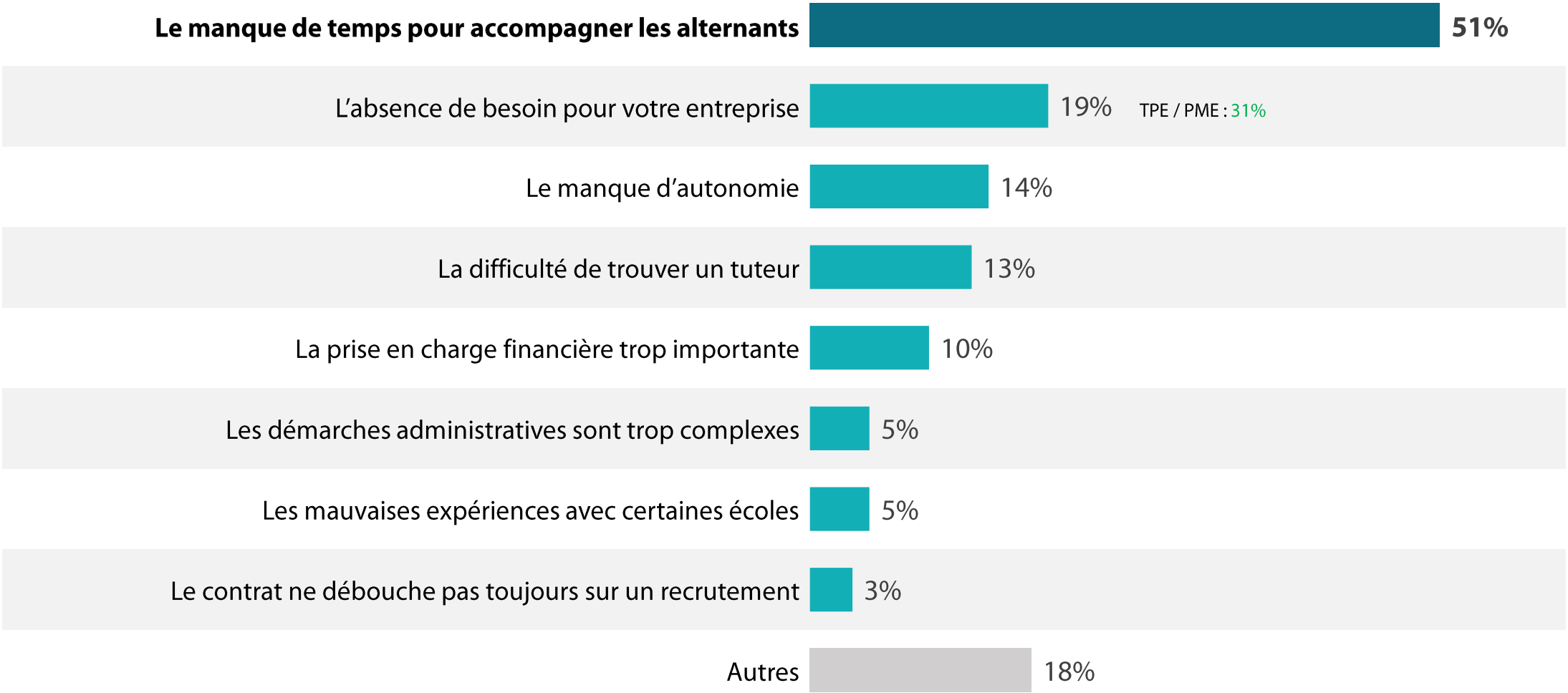
Pour ceux qui n'ont pas recruté d'alternants, le manque de temps représente le principal frein au passage à l'acte.

145 personnes

Nouvelle question en 2024

Q45 : Pour quelles raisons n'avez-vous pas recruté des alternants ?

Base : n'ont pas recruté d'alternants - plusieurs réponses possibles



WE ARE DIGITAL !

Fondé en 2000 sur cette idée radicalement innovante pour l'époque, OpinionWay a été précurseur dans le renouvellement des pratiques de la profession des études marketing et d'opinion.

Forte d'une croissance continue depuis sa création, l'entreprise n'a eu de cesse de s'ouvrir vers de nouveaux horizons pour mieux adresser toutes les problématiques marketing et sociétales, en intégrant à ses méthodologies le Social Média Intelligence, l'exploitation de la smart data, les dynamiques créatives de co-construction, les approches communautaires et le storytelling.

Aujourd'hui OpinionWay poursuit sa dynamique de croissance en s'implantant géographiquement sur des zones à fort potentiel que sont l'Europe de l'Est et l'Afrique.

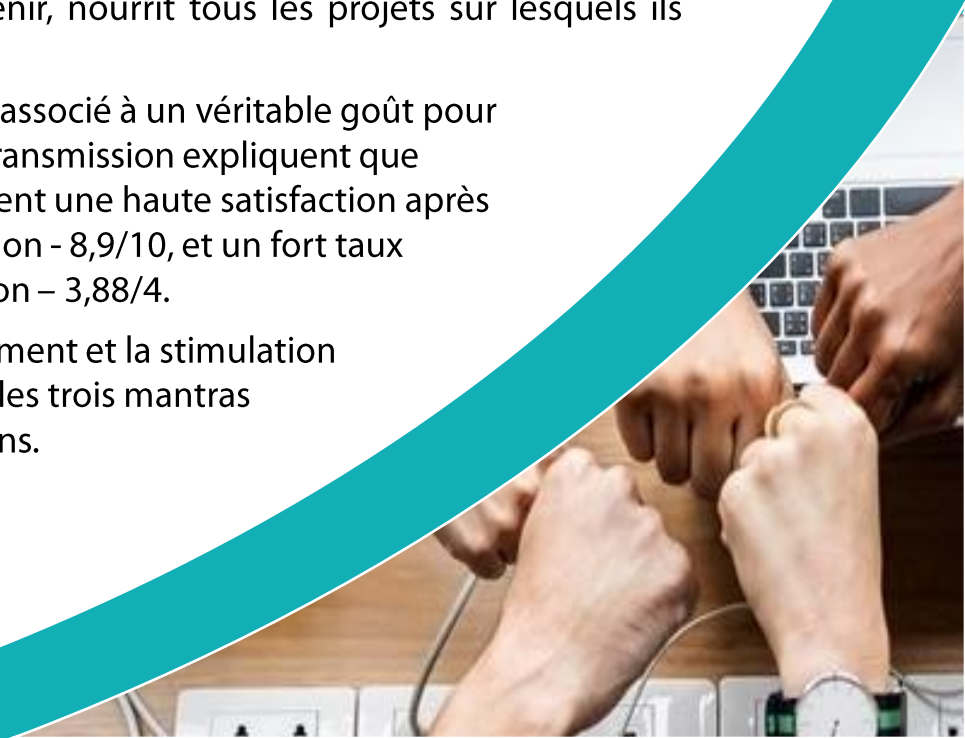
RENDRE LE MONDE INTELLIGIBLE POUR AGIR AUJOURD'HUI ET IMAGINER DEMAIN

C'est la mission qui anime les collaborateurs d'OpinionWay et qui fonde la relation qu'ils tissent avec leurs clients.

Le plaisir ressenti à apporter les réponses aux questions qu'ils se posent, à réduire l'incertitude sur les décisions à prendre, à tracker les insights pertinents et à co-construire les solutions d'avenir, nourrit tous les projets sur lesquels ils interviennent.

Cet enthousiasme associé à un véritable goût pour l'innovation et la transmission expliquent que nos clients expriment une haute satisfaction après chaque collaboration - 8,9/10, et un fort taux de recommandation – 3,88/4.

Le plaisir, l'engagement et la stimulation intellectuelle sont les trois mantras de nos interventions.



RESTONS CONNECTÉS !

www.opinion-way.com

Envie d'aller plus loin ?

Recevez chaque semaine nos derniers résultats d'études dans votre boite mail en vous abonnant à notre

newsletter !

opinionway

15 place de la République
75003 Paris

PARIS
CASABLANCA
ALGER
VARSOVIE
ABIDJAN