Club des Experts de la Sécurité de l'Information et du Numérique

Baromètre de la cyber-sécurité des entreprises

Vague 2 - Janvier 2017

À : Alain Bouillé
De : Emmanuel Kahn, Agathe Martini
OpinionWay, 15 place de la République, 75003 Paris

Sommaire

CONTEXTE ET 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 de grandes entreprises.
- Le CESIN a lancé en 2015 sa première grande enquête auprès de ses membres pour connaître
  - la **perception de la cyber-sécurité et de ses enjeux** au sein des entreprises membres du CESIN
  - **la réalité** concrète de la sécurité informatique des grandes entreprises.
- L'enquête, renouvelée cette année, met à jour les résultats sur la perception et la réalité de la cyber-sécurité, et apporte de nouvelles données sur l'impact de la transformation numérique des entreprises.

MÉTHODOLOGIE

Méthodologie

Méthodologie

Étude quantitative réalisée auprès de **141 membres du CESIN**, à partir du fichier membre du CESIN (280 contacts)

Mode d'interrogation

L'échantillon a été interrogé par Internet sous système **CAWI** (*Computer Assisted Web Interview*)

Dates de terrain

Du **10 novembre** au **5 décembre 2016**

afaq ISO 20252 Étude marketing et d'opinion AFNOR CERTIFICATION

Certification

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

MESSAGES CLÉS

Messages clés (1/2)

Les enseignements à retenir

1. Le **nombre de cyber-attaques constatées est en hausse**, et pratiquement plus aucune entreprise n'y échappe.

   Le **ransomware** est cette année encore la cyber-attaque la plus fréquente, et de façon encore plus marquée que l'année dernière, loin devant les attaques par déni de service et les attaques virales générales. Dans le même temps, deux types d'attaques sont moins fréquentes qu'en 2015 : les attaques ciblées et le vol de données personnelles.
   Le **social engineering** et les **vulnérabilités résiduelles** permanentes touchent une entreprise sur deux et viennent compléter le tableau des cyber-risques auxquels les entreprises sont les plus exposées..

2. Face à ces risques, de nombreuses **solutions techniques** sont implantées. Au-delà des antivirus, VPN, filtrage web et AntiSPAM, on note aussi la mise en place de log management et de supervision sécurité : la détection est un enjeu majeur de la cyber-sécurité.
   Globalement, les solutions techniques sont tout de même jugées perfectibles et restent **inadaptées aux besoins de près d'un tiers des entreprises**. Parallèlement, un quart des entreprises a souscrit une cyber-assurance, un taux en augmentation par rapport à l'année dernière.

Messages clés (2/2)

Les enseignements à retenir

3. Dans ce contexte, la **transformation numérique** apporte elle aussi son lot de risques. Pour presque toutes les entreprises, elle a notamment un impact sur la gestion des données sensibles.

   - Le **Cloud**, déjà très répandu dans les entreprises, pose la question du **contrôle des accès**, **du stockage à l'étranger**, **de la confidentialité** des données et **d'un éventuel non-effacement des données.** Le Cloud nécessite ainsi des outils de sécurisation spécifiques.
   - Les **pratiques des salariés** mettent aussi à mal la cyber-sécurité, notamment le BYOD. Dans ce cadre, la **sensibilisation** des salariés aux cyber-risques est **en progression**, et plus de la moitié des entreprises a mis en place des procédures pour tester l'application des recommandations par les salariés.
   - Les **nouveaux usages du numériques**, en particulier les objets connectés mais aussi le machine to machine, représentent également un risque pour les entreprises.

   Globalement, les solutions techniques proposées par le marché pour faire face à ces risques liés à la transformation numérique n'ont pas encore convaincu les entreprises.

4. Pour l'avenir, la **confiance dans la capacité des entreprises** à faire face aux cyber-risques reste **limitée**. Les investissements à venir dans la cyber-sécurité portent encore majoritairement sur l'acquisition de solutions techniques, même si près d'une entreprise sur deux envisage d'augmenter ses effectifs alloués à la cyber-sécurité. **L'enjeu de demain sera ainsi avant tout humain** : replacer **la gouvernance de la cyber-sécurité** au bon niveau, pour mieux agir.

RÉSULTATS

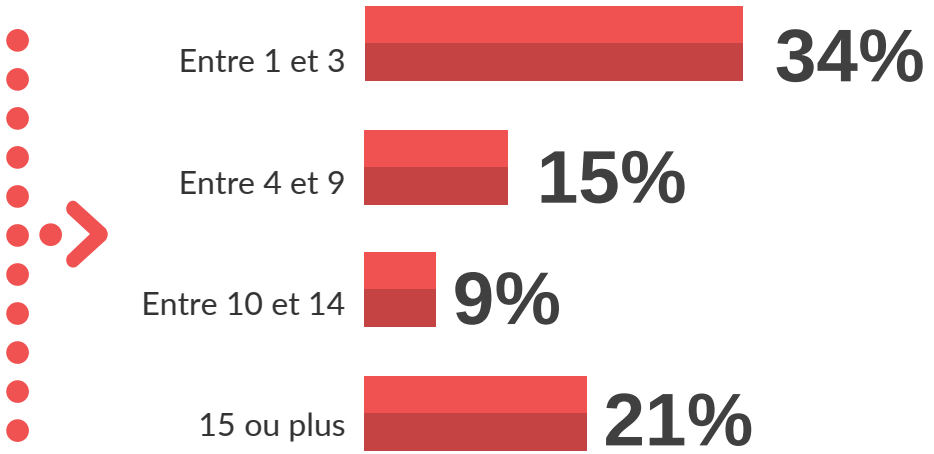
1. DES CYBER-ATTAQUES EN HAUSSE

Un grand nombre d'entreprises touchées par des cyber-attaques cette année

Q5. Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?
Base : ensemble (141 répondants)

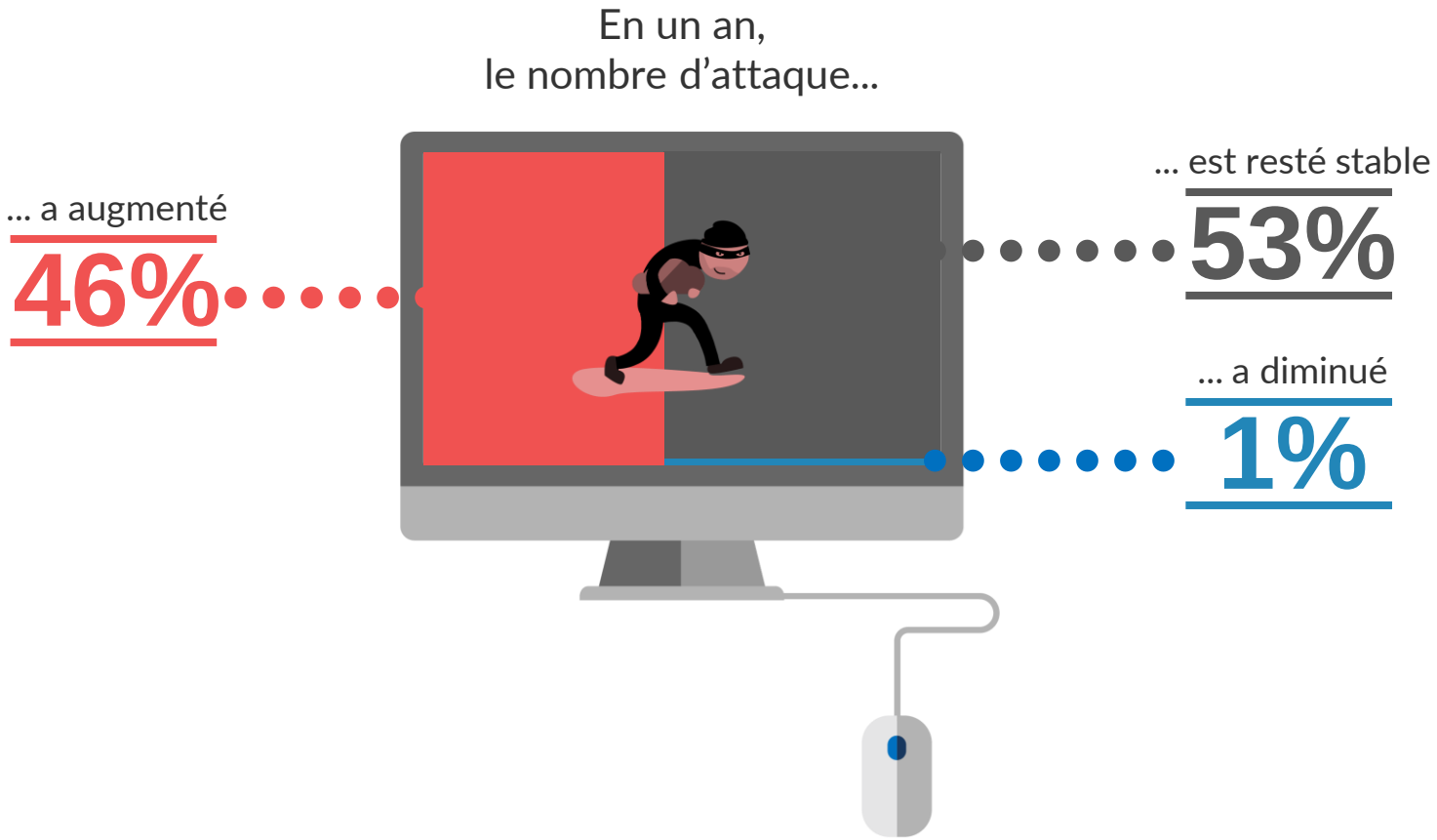
80%

des entreprises ont constaté au moins une cyber-attaque



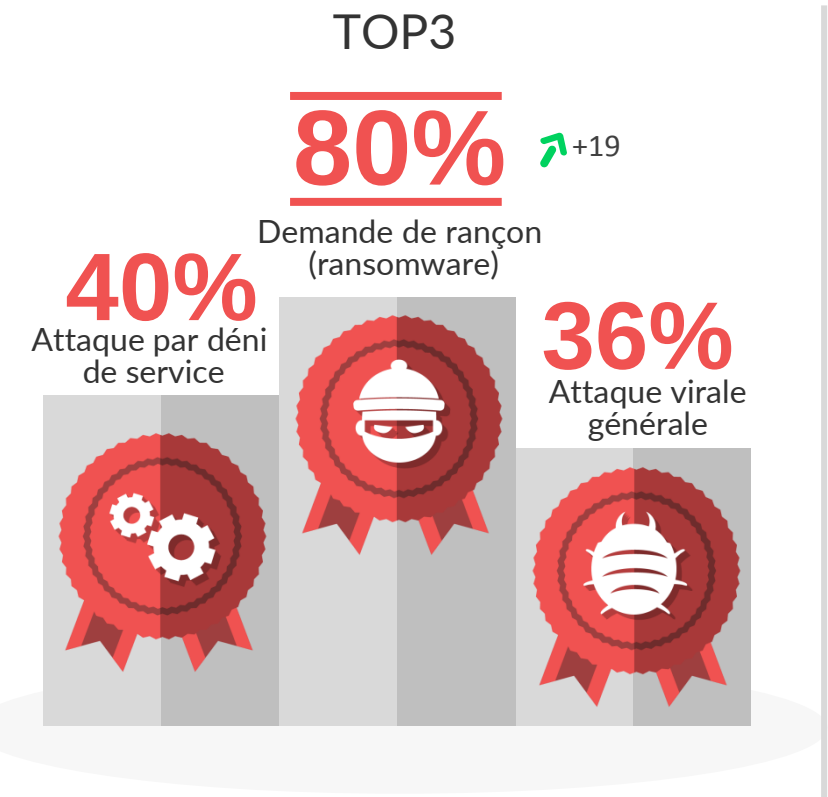
En un an, le nombre de cyber-attaques a augmenté pour près d'une entreprise sur deux

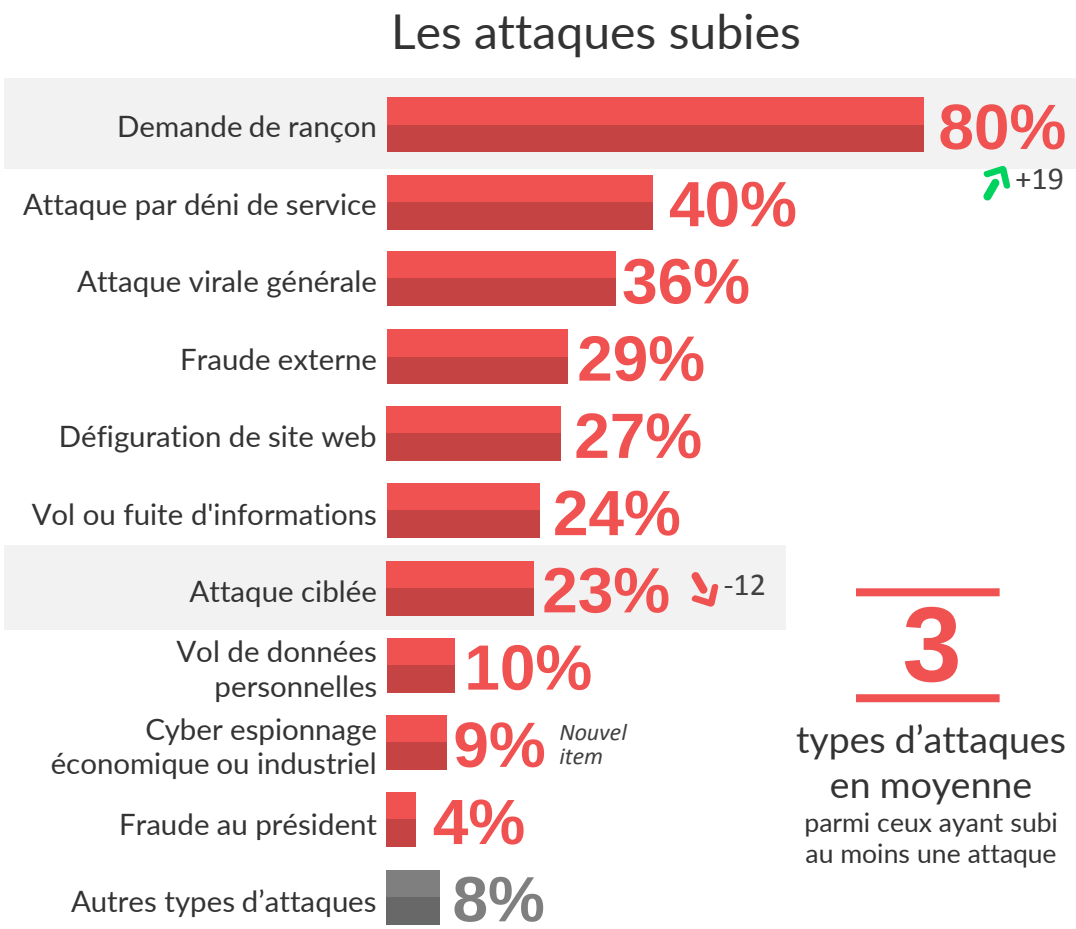
Q5BIS. Et par rapport à l'année dernière, ce nombre d'attaques constatées dans votre entreprise… ?
Base : ensemble (141 répondants)



Parmi les cyber-attaques constatées, le ransomware est la plus subie et de façon plus marquée encore qu'il y a un an

Q6. Quel(s) type(s) de cyber-attaque(s) votre entreprise a-t-elle constaté(s) au cours des 12 derniers mois ?
Base : ont constaté une attaque (113) / Plusieurs réponses possibles

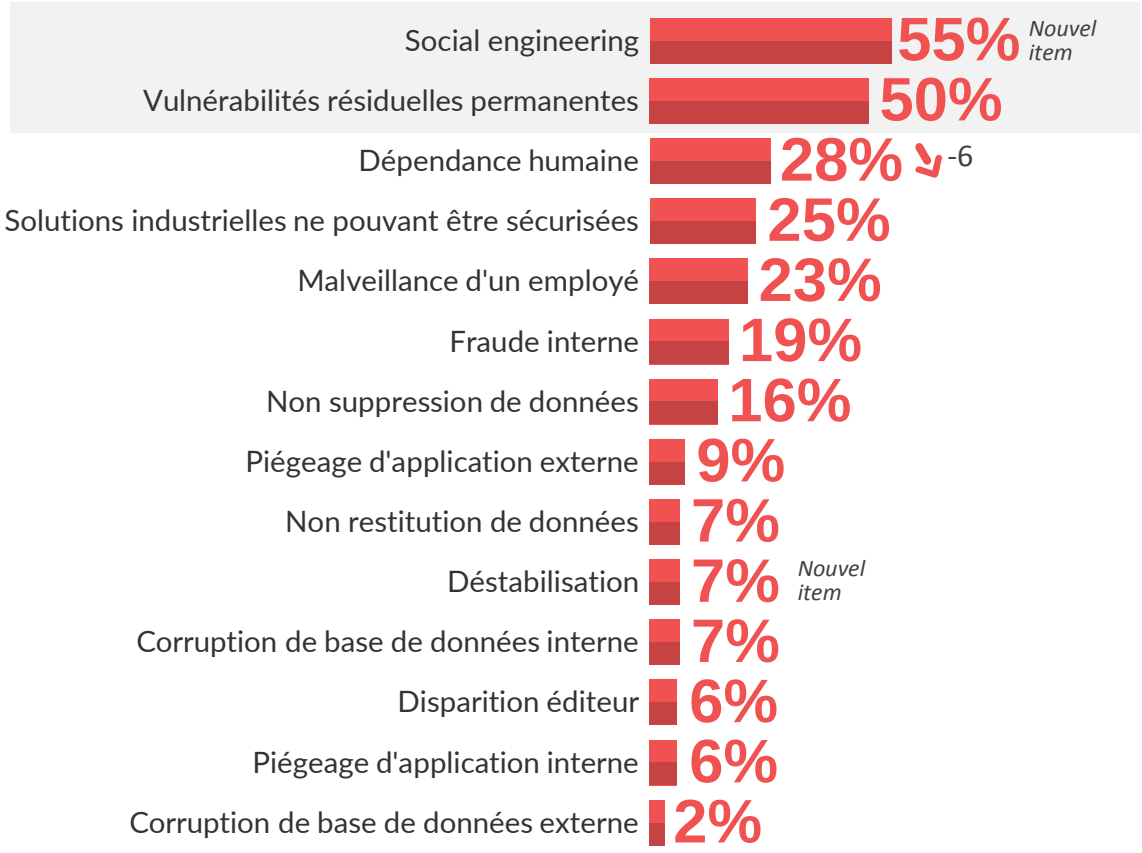




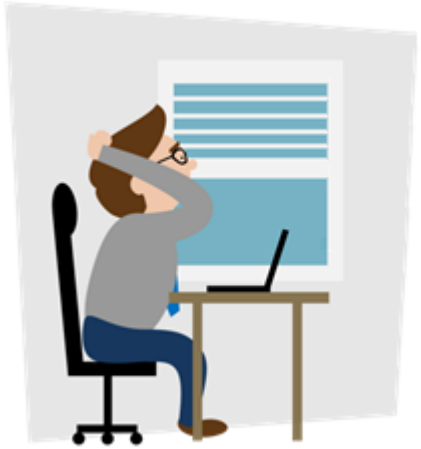
3
types d'attaques en moyenne
parmi ceux ayant subi au moins une attaque

Au-delà des cyber-attaques, un grand nombre d'entreprises est confronté à des risques, social engineering et vulnérabilités résiduelles en particulier

Q6BIS. Parmi les éléments suivants liés à la cyber-sécurité, quels sont ceux auxquels votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?
Base : ensemble (141 répondants) / Plusieurs réponses possibles



89% ont connu au moins un élément

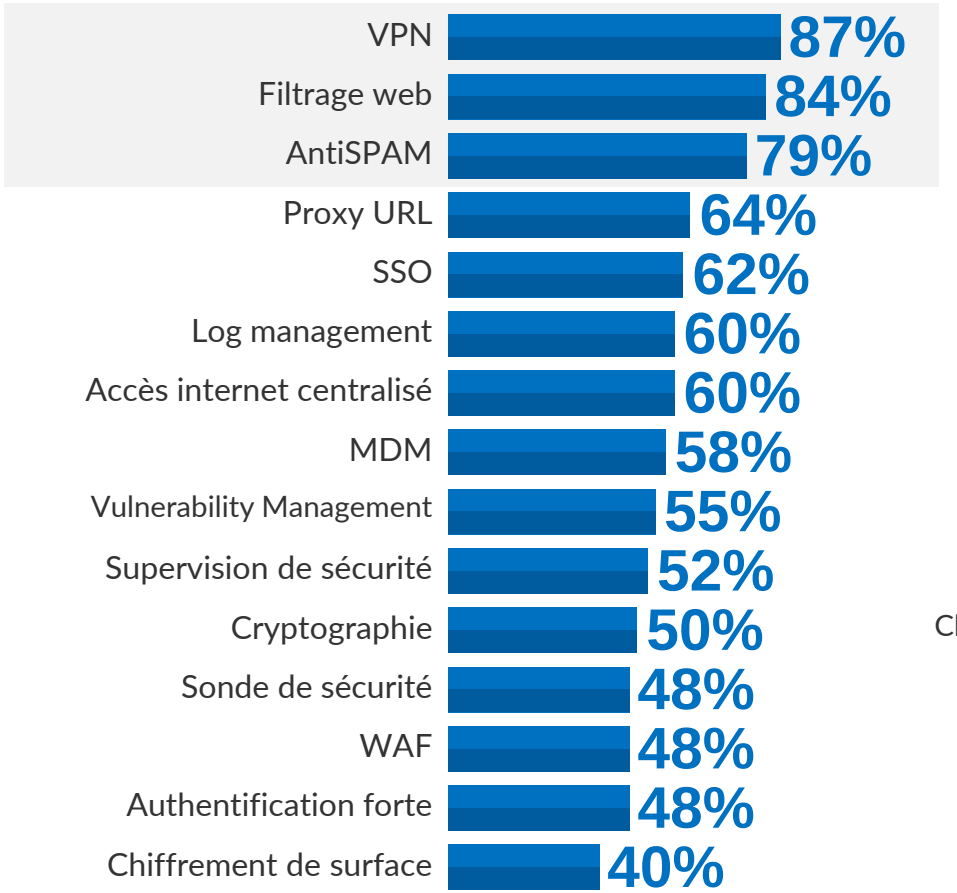


3 éléments en moyenne

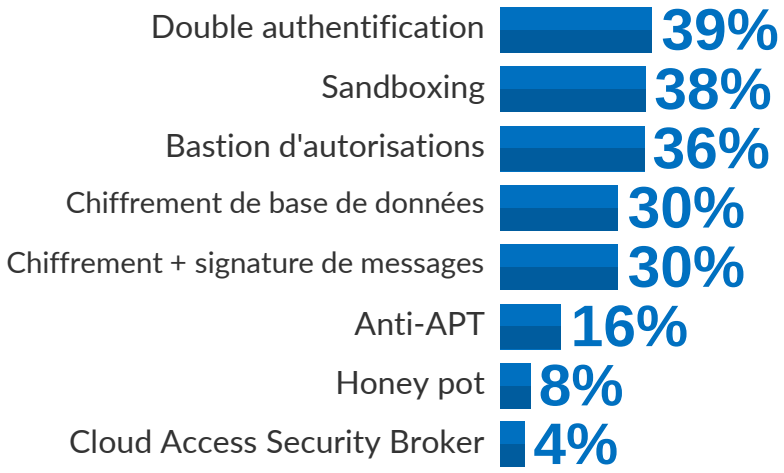
2. FACE AUX CYBER-RISQUES, DES SOLUTIONS TECHNIQUES À L'EFFICACITÉ RELATIVE

Les entreprises s'équipent de nombreuses solutions pour faire face aux cyber-risques, VPN, filtrage web et antiSPAM en tête

Q8. Parmi les solutions de protection suivantes, quelles sont celles qui ont été mises en place dans votre entreprise, en plus des antivirus et pare-feu ? *Base : ensemble (141 répondants) / Plusieurs réponses possibles*

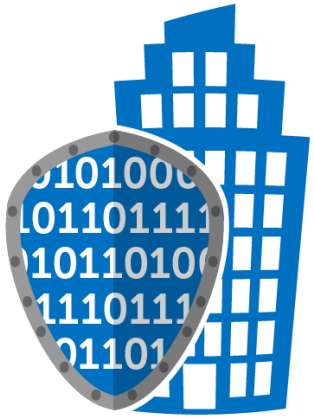


11 solutions en moyenne



Parmi les solutions de protection, la cyber-assurance est encore peu utilisée mais en nette progression

Q9. Par ailleurs, votre entreprise a-t-elle souscrit une cyber-assurance ?
Base : ensemble (141 répondants)

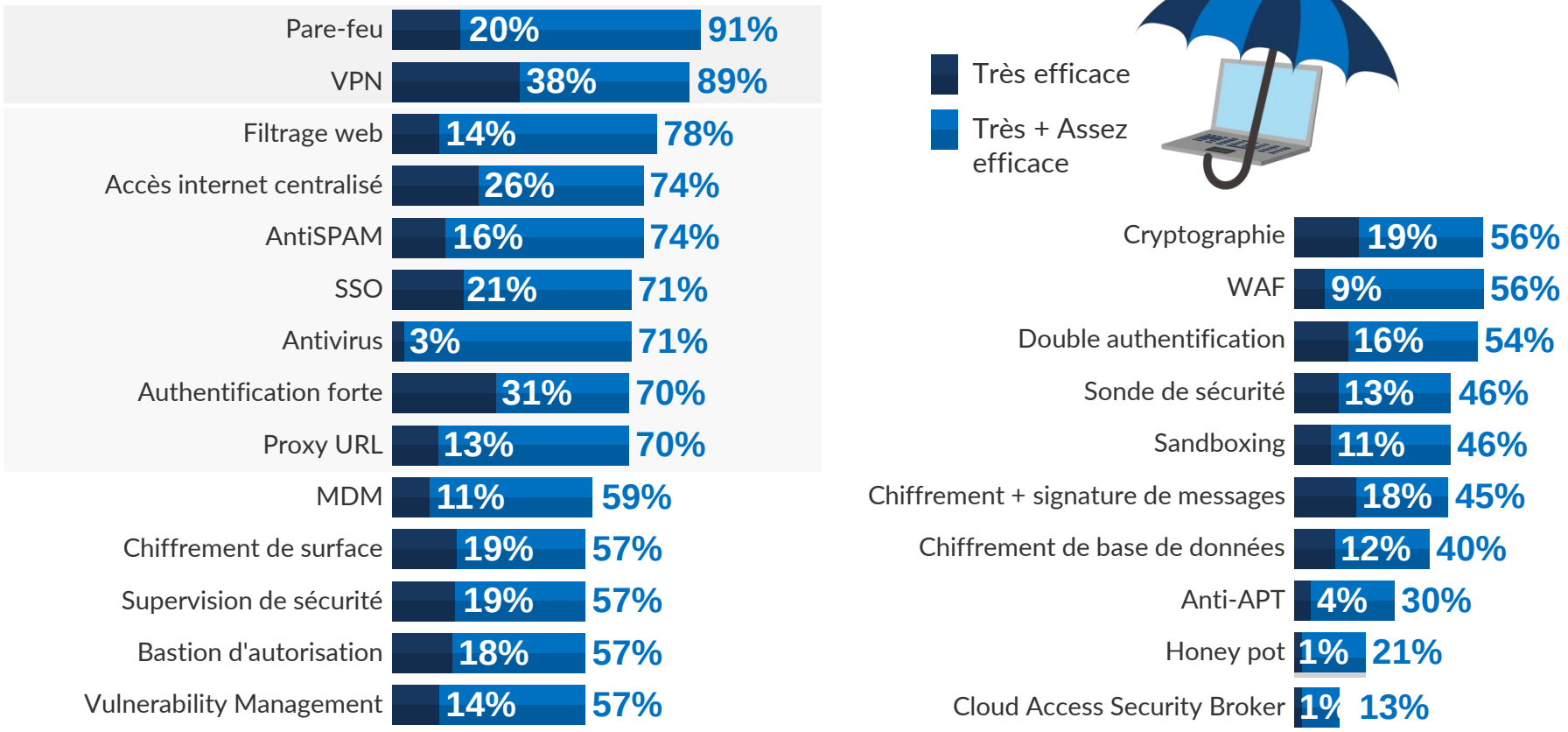


26% ↗ +7

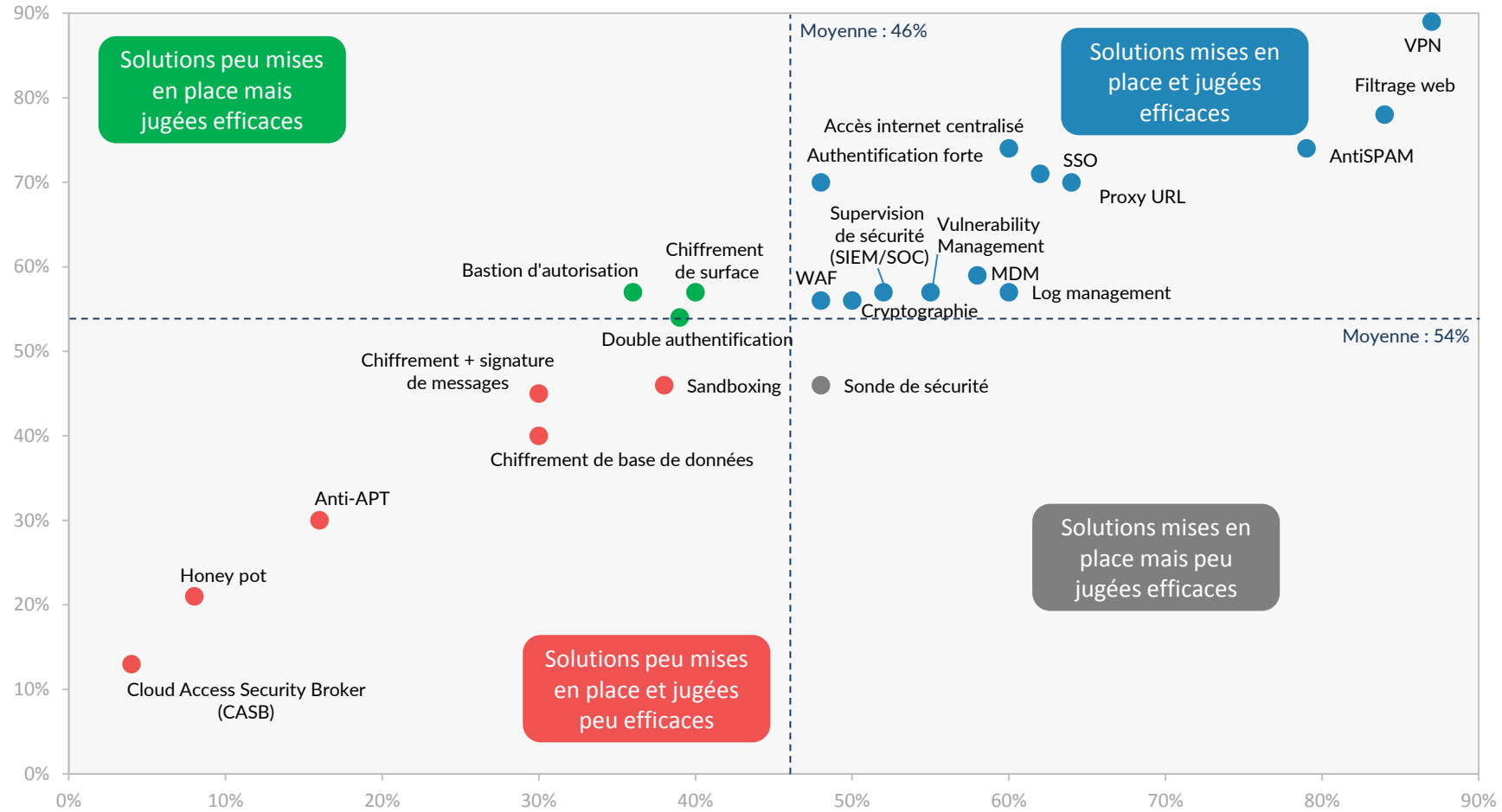
17% ↗ +4

Certaines solutions techniques sont jugées plus efficaces que d'autres : pare-feu et VPN sont plébiscités

Q8BIS. Pour chacune des solutions suivantes, estimez-vous qu'elle est très efficace, plutôt efficace, plutôt pas efficace ou pas du tout efficace ? *Base : ensemble (141 répondants)*



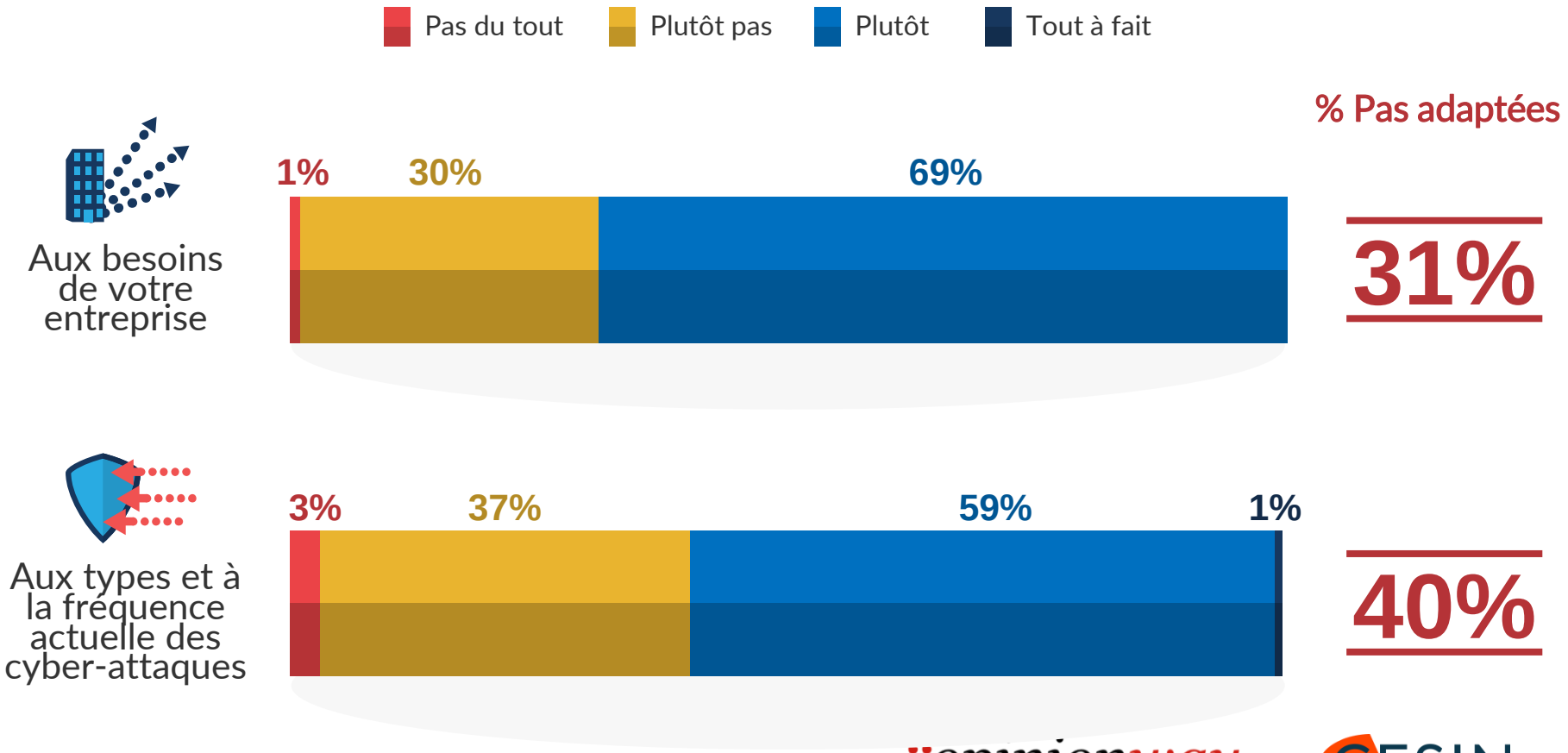
Globalement, les solutions mises en places sont celles jugées efficaces



Des solutions techniques qui restent inadaptées pour plus d'un tiers des entreprises

Q29. Pensez-vous que les solutions de protection disponibles sur le marché sont tout à fait, plutôt, plutôt pas ou pas du tout adaptées… ?

Base : ensemble (141 répondants)



3. LA TRANSFORMATION NUMÉRIQUE VIENT BOUSCULER LES ENJEUX DE LA CYBER-SÉCURITÉ

La transformation numérique est déjà un enjeu stratégique pour les entreprises

Q1. Dans votre entreprise, diriez-vous que la transformation numérique est un enjeu stratégique ?
Base : ensemble (141 répondants)

95%

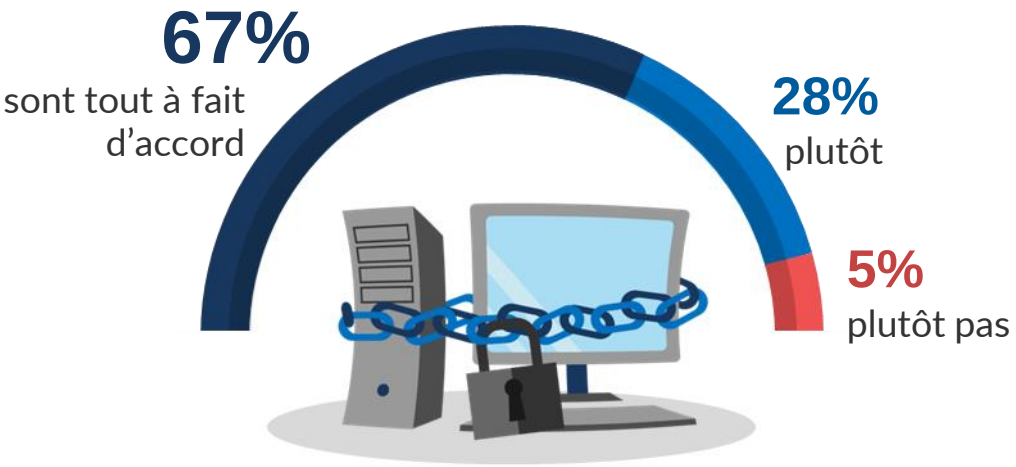
des membres du CESIN considèrent que **la transformation numérique est un enjeu stratégique**

La transformation numérique vient perturber la cyber-sécurité avec un impact sur les SI et les données sensibles

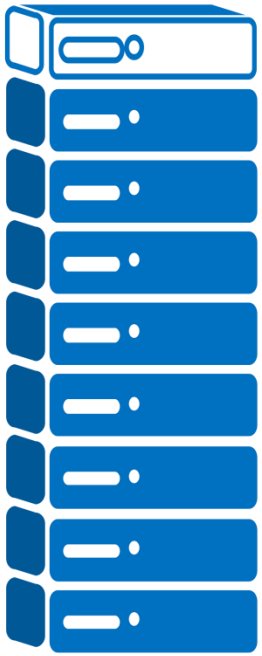
Q2BIS. Dans votre entreprise, la transformation numérique a-t-elle un impact sur la sécurité des systèmes d'information et des données ?
Base : ensemble (141 répondants)

95%

estiment que la transformation numérique a **un impact sur la sécurité** des systèmes d'information et des données



Q2TER. La transformation numérique a-t-elle un impact sur la gestion des données sensibles dans votre entreprise ?



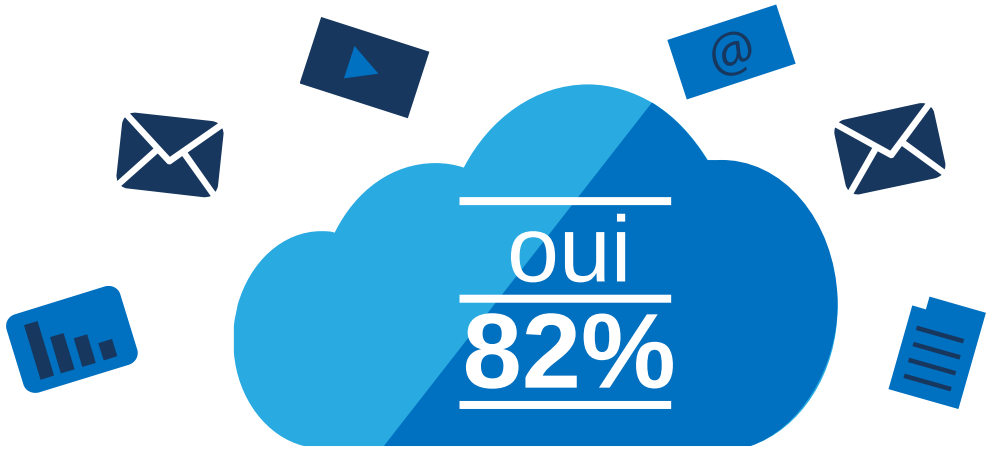
Et pour

89%

Elle a **un impact sur la gestion des données sensibles** de l'entreprise

Engagées dans la transformation numérique, la plupart des entreprises stockent leurs données dans un Cloud

Q20. Certaines des données de votre entreprise sont-elles stockées dans un Cloud ?
Base : ensemble (141 répondants)



Non
18%

Oui, dans des Clouds publics
43%

Oui, dans des Clouds hybrides
20%

Oui, dans des Clouds privés seulement
19%

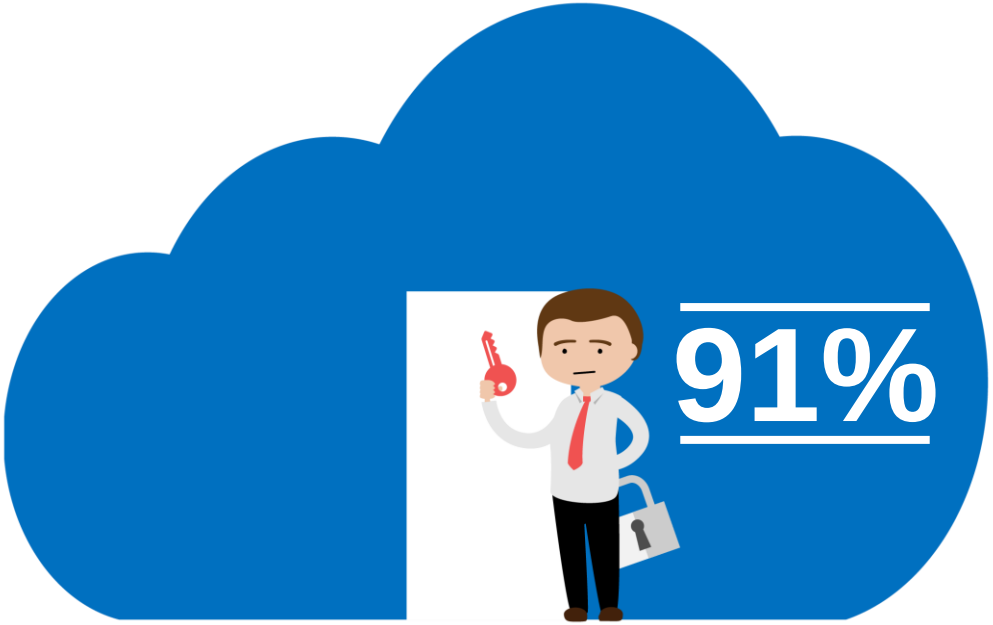
Le Cloud expose les entreprises à de nombreux risques, notamment en raison du moindre contrôle des données

Q22. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ? *Base : ensemble (141 répondants)*

- 57% Difficulté de **contrôle des accès** et audits
- 55% Stockage des données dans des **datacenters à l'étranger**, hors du droit français
- 55% **Non effacement** des données
- 50% **Confidentialité** des données vis-à-vis de l'hébergeur
- 47% **Non restitution** des données
- 42% Non-maîtrise des **paramètres de sécurité** / chiffrement faible de la part de l'hébergeur
- 42% Non-maîtrise de **l'utilisation** qui en est faite **par les salariés** de votre entreprise
- 36% Traitement **Big Data** à notre insu
- 30% **Indisponibilité** des données
- 28% **Non-alimentation du SOC** (interne ou externe) en données provenant du Cloud
- 26% **Propagation systémique** des attaques et erreurs humaines
- 24% **Disparition** de l'hébergeur
- 23% **Attaque par rebond** depuis l'hébergeur
- 20% **Piégeage** d'application hébergée
- 15% **Corruption** de base de données

Sécuriser le Cloud nécessite de mettre en œuvre des outils spécifiques

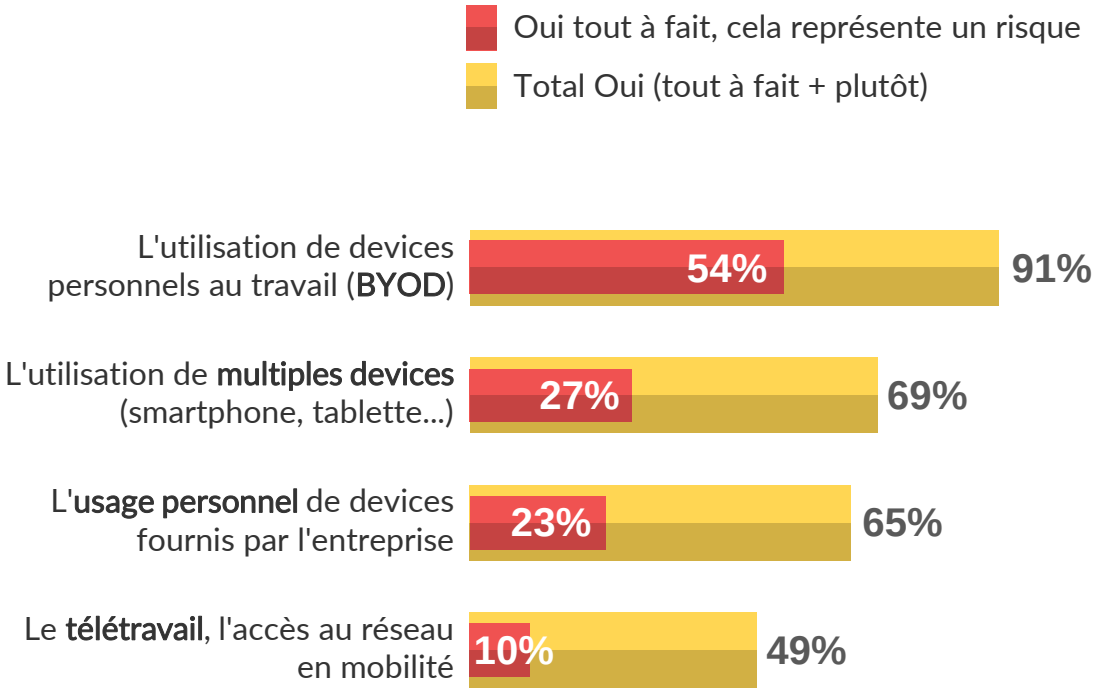
Q23. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?
Base : ensemble (141 répondants)



estiment que la sécurisation des données stockées dans le Cloud requiert des outils ou dispositifs spécifiques

La transformation numérique induit des risques liés aux usages des salariés de l'entreprise – le BYOD en particulier

Q24. À vos yeux, les usages suivants du numérique par les salariés représentent-ils un risque pour la cyber-sécurité des entreprises ?
Base : ensemble (141 répondants)



La sensibilisation des salariés aux cyber-risques progresse, mais reste largement perfectible

Q15. En ce qui concerne la cyber-sécurité, pensez-vous que les salariés de votre entreprise… ?
Base : ensemble (141 répondants)

65% ↗ +6
pensent que les salariés sont sensibilisés aux cyber-risques

58% ↗ +6
pensent que les salariés respectent les recommandations

14% ↘ -1
pensent que les salariés prennent des précautions au-delà des recommandations données

Plus d'une entreprise sur deux a mis en place des procédures de vérification du respect des recommandations de cyber-sécurité

Q15BIS. Avez-vous mis en place des procédures pour tester l'application des recommandations par les salariés dans des situations concrètes, comme des audits, campagnes de faux phishing, contrôles internes, etc. ?
Base : ensemble (141 répondants)

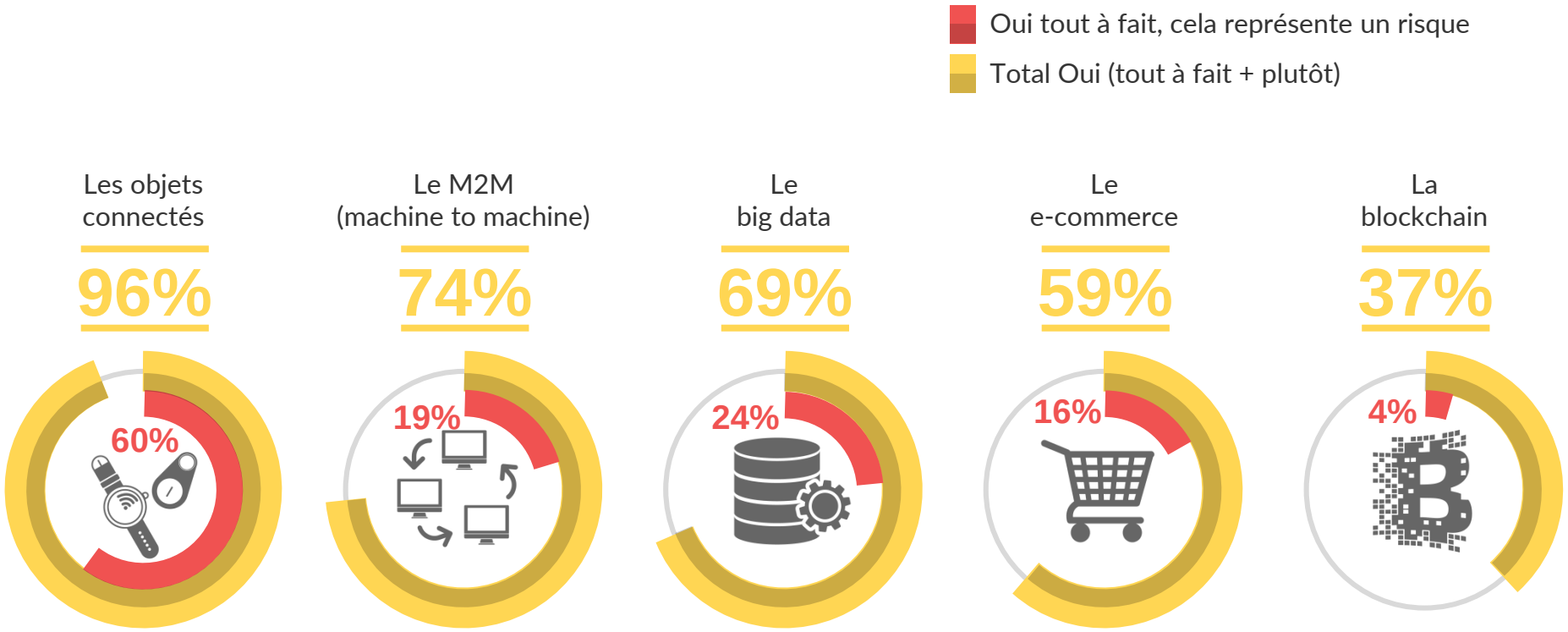
57%

ont mis en place des procédures pour tester l'application des recommandations par les salariés

Les nouveaux usages liés à la transformation numérique apportent leurs lots de risques – les objets connectés en particulier

Q24BIS. Et les usages suivants liés à la transformation numérique représentent-ils un risque pour la cyber-sécurité des entreprises ?

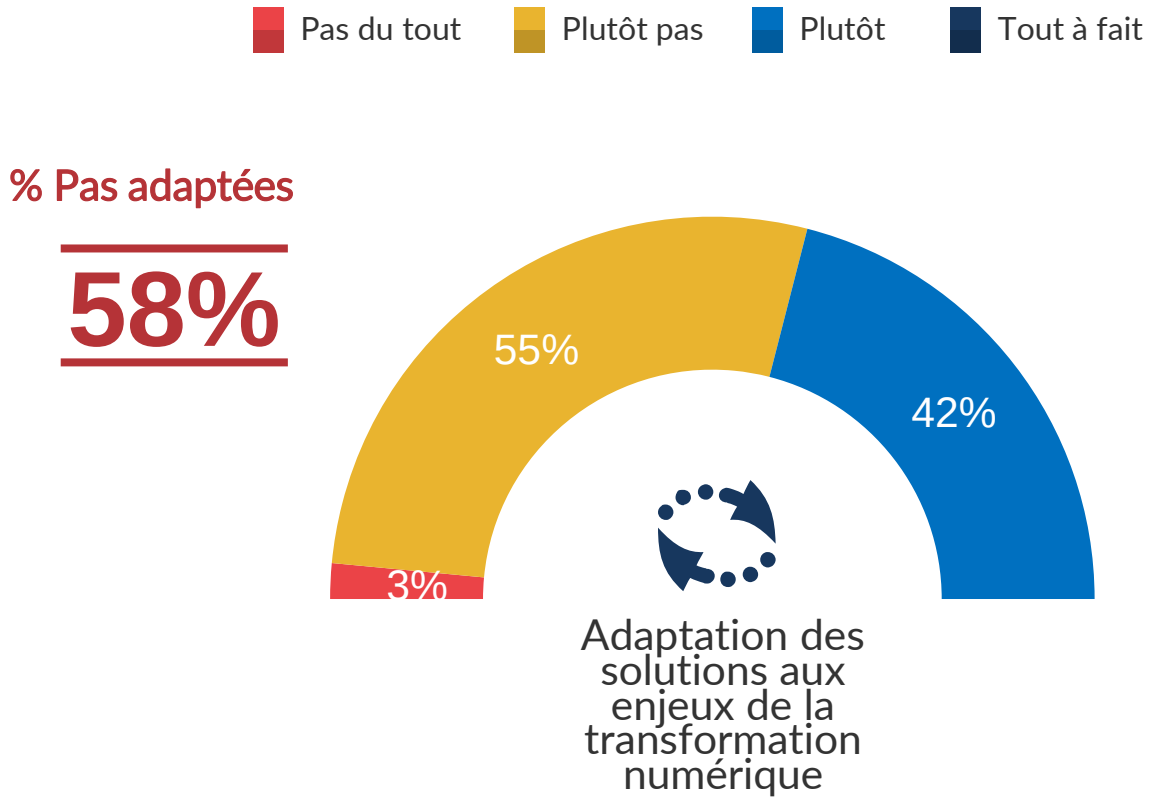
Base : ensemble (141 répondants)



Face aux cyber-risques liés à la transformation numérique, plus d'une entreprise sur deux considère que les solutions du marché ne sont pas adaptées

Q29. Pensez-vous que les solutions de protection disponibles sur le marché sont tout à fait, plutôt, plutôt pas ou pas du tout adaptées… ?

Base : ensemble (141 répondants)



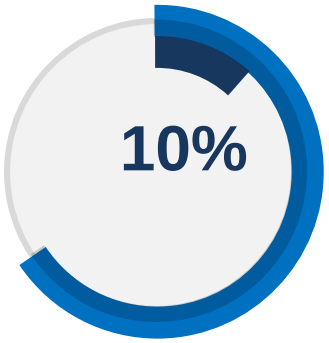
4. POUR DEMAIN, REFONDER LA GOUVERNANCE DE LA CYBER-SÉCURITÉ

Pour l'avenir, une confiance dans la capacité à faire face aux cyber-risques réelle mais limitée

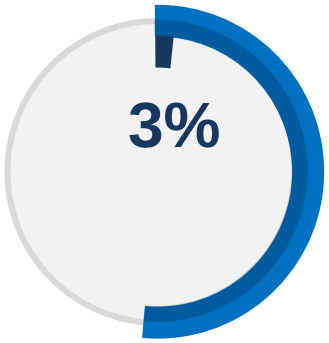
Q26. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (141 répondants)

Très confiant
Très + Assez confiant

67%
La prise en compte des enjeux de la cyber-sécurité au sein de votre entreprise



52% +5
La capacité de votre entreprise à faire face aux cyber-risques



La plupart des entreprises envisagent d'acquérir des solutions techniques pour assurer leur cyber-sécurité

Q11BIS. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ?
Base : ensemble (141 répondants)

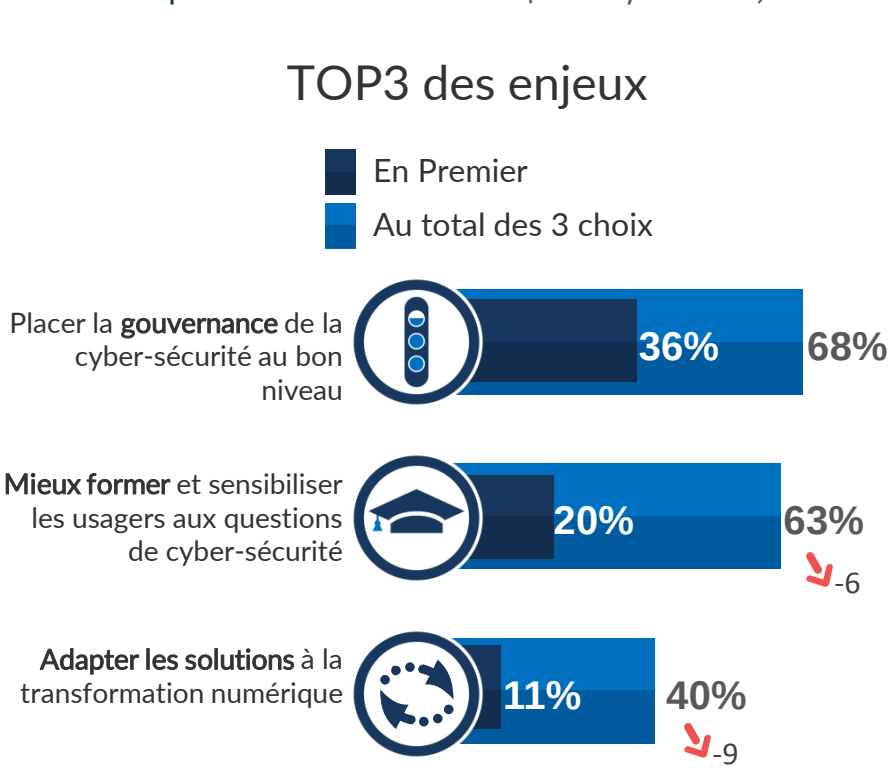
84%
d'acquérir de nouvelles solutions techniques destinées à la protection contre les cyber-risques

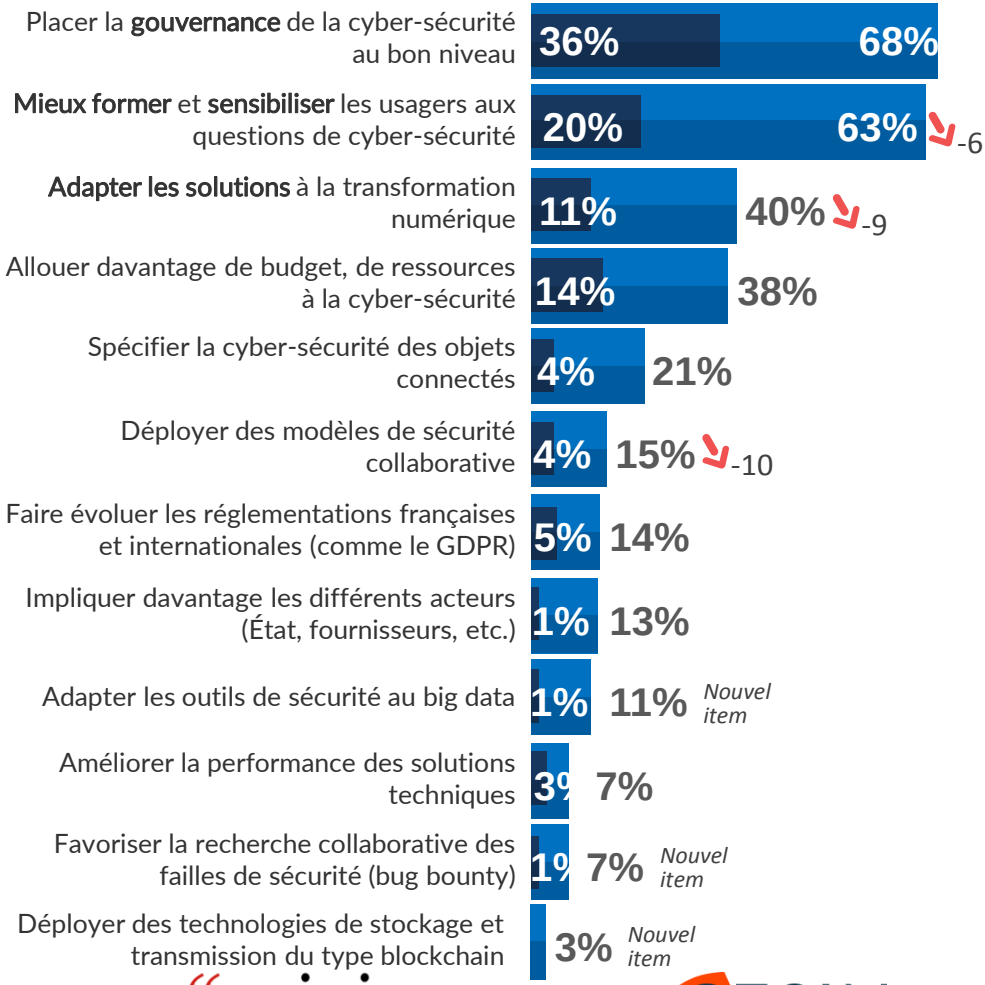
55%
d'augmenter les budgets alloués à la protection contre les cyber-risques

44%
d'augmenter les effectifs alloués à la protection contre les cyber-risques

Pour demain, l'enjeu sera moins technique : il s'agira plutôt de revoir la gouvernance de la cyber-sécurité pour mieux agir

Q28. Parmi les enjeux suivants, quels sont selon vous les trois enjeux de demain pour l'avenir de la cyber-sécurité des entreprises ? *Base : ensemble (141 répondants)*



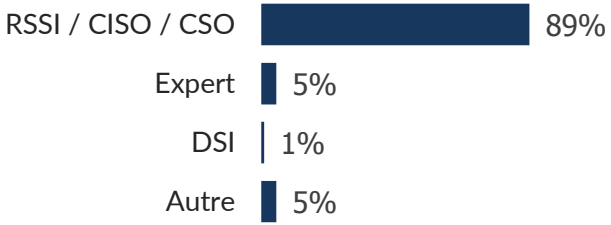


ANNEXES

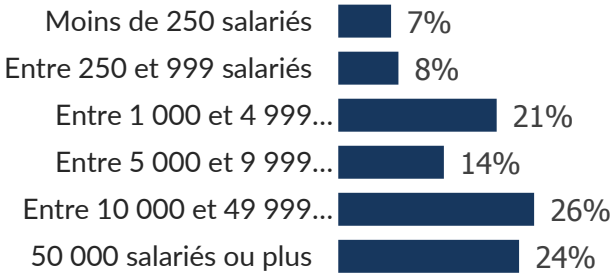
Profil des répondants

141 membres du CESIN ont participé à cette enquête

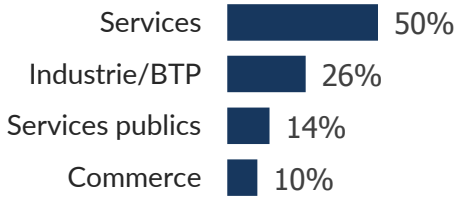
Fonction des répondants :



Nombre de salariés de l'entreprise :



Secteur d'activité de l'entreprise :



Entité en charge de la protection contre les cyber-risques

Q3. Dans votre entreprise, quelle est l'entité en charge du pilotage de la protection contre les cyber-risques ?
Base : ensemble (141 répondants) / Plusieurs réponses possibles