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

Baromètre de la cyber-sécurité des entreprises

Vague 3 - Janvier 2018

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

"opinionway

CESIN

Sommaire

CESIN

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, avec OpinionWay, 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 chaque 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.

CESIN

MÉTHODOLOGIE

Méthodologie

Méthodologie

Étude quantitative réalisée par OpinionWay auprès de **142 membres du CESIN**, à partir du fichier membre du CESIN (343 contacts).

Mode d'interrogation

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

Dates de terrain

Du **21 novembre** au **27 décembre 2017**.

Certification

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

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.

MESSAGES CLÉS

Messages clés (1/2)

Les enseignements à retenir

1. La majorité des entreprises sont toujours touchées par des cyber-attaques. Dans près d'un cas sur deux, **les attaques ont des impacts concrets sur le business** des entreprises touchées : indisponibilité du site, arrêt de la production, etc.
   Le **ransomware** est cette année encore la cyber-attaque la plus fréquente, loin devant les attaques virales générales et la fraude externe ou les vols d'information. Dans le même temps, deux types d'attaques sont moins fréquentes qu'en 2017 : les attaques par déni de service et la défiguration de site web.
   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 **souscription de plus en plus courante aux cyber-assurances** : +14 points par rapport à l'an dernier. Pour s'informer sur la cyber-sécurité, les entreprises mobilisent tout un écosystème d'acteurs, **l'ANSSI étant considéré comme le plus légitime**.
   Globalement, les solutions techniques sont jugées plus efficaces, mais restent **perfectibles** et **pas totalement adaptées à l'actualité des cyber-attaques**.

Malgré la prégnance des cyber-attaques, la sécurité représente moins de 5% du budget IT dans près des deux tiers des entreprises.

Messages clés (2/2)

Les enseignements à retenir

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

   - Le **Cloud**, déjà très répandu dans les entreprises et utilisé de plus en plus dans sa forme hybride privé/public, pose notamment la question du **de la confidentialité** 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. Les failles de sécurité sont ainsi le premier défi à relever dans l'IoT en entreprise. Dans ce cadre, **les salariés sont plutôt bien sensibilisés** aux cyber-risques, mais **peu proactifs** : et plus de la moitié des entreprises a ainsi mis en place des procédures pour tester l'application des recommandations par les salariés.

   Globalement, les solutions techniques proposées par le marché pour faire face à ces risques liés à la transformation numérique se montrent de plus en plus adaptées, mais ne convainquent toujours pas près d'une entreprise sur deux.

4. La **GDPR** ajoute un **coût financier** aux entreprises, mais aussi surtout une **charge supplémentaire** pour le RSSI, qui cumule parfois la fonction de DPO. D'autant plus que la plupart des entreprises n'ont pas terminé leurs chantiers de mise en conformité GDPR. La GDPR est cependant bien perçue par les entreprises, qui y voient un **réel moyen de renforcer la protection des données**.

5. Alors que les enjeux pour demain seront plus humains que techniques, la mise en conformité GDPR a déjà permis de **refonder la gouvernance de la cyber-sécurité** dans une entreprise sur deux.

RÉSULTATS

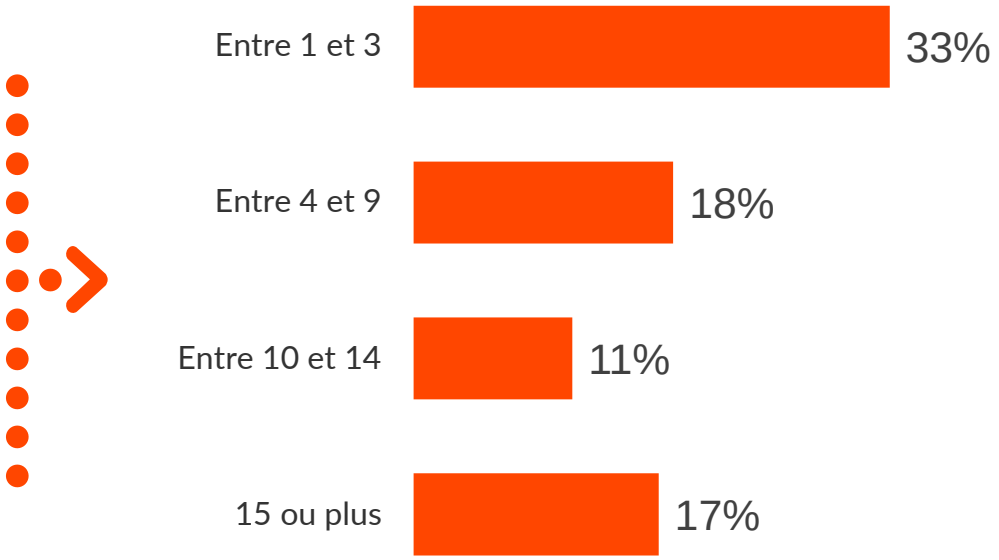
1. DES CYBER-ATTAQUES QUI CONTINUENT D'AUGMENTER

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 (142 répondants)*

79%

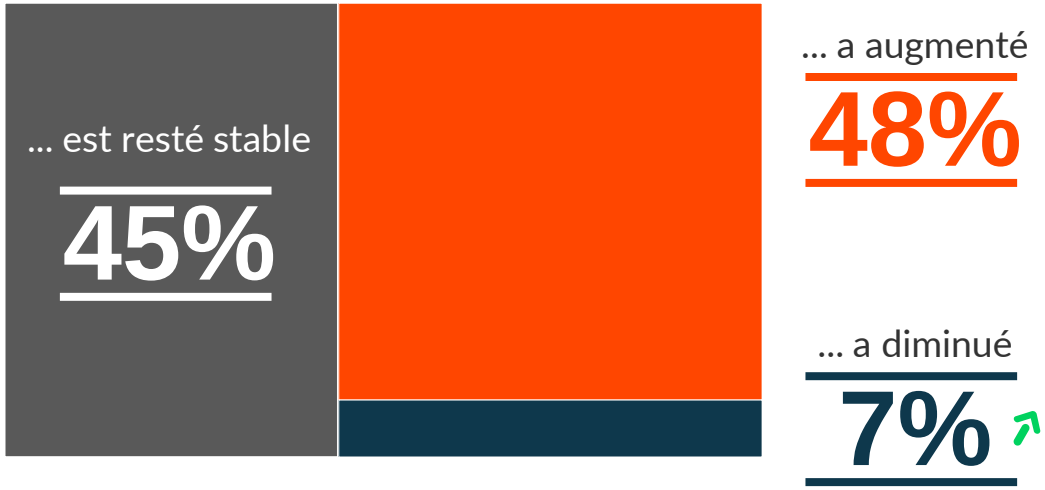
des entreprises ont constaté au moins une cyber-attaque



Le nombre de cyber-attaques constatées augmente encore pour près d'une entreprise sur deux

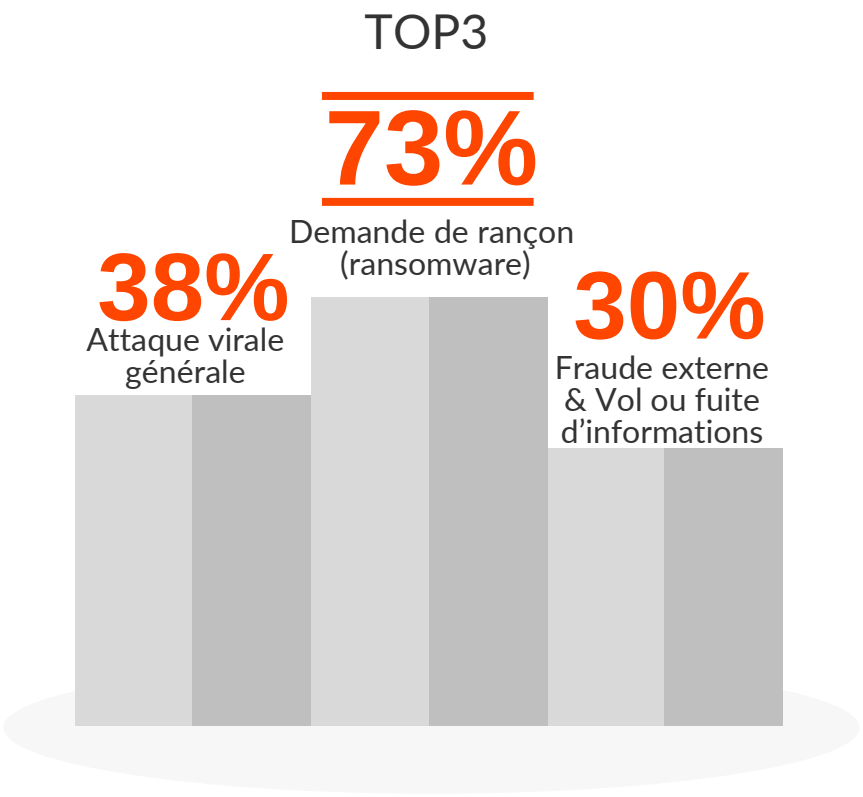
Q5BIS. Et par rapport à l'année dernière, ce nombre d'attaques constatées dans votre entreprise… ? *Base : ensemble (142 répondants)*

En un an, le nombre d'attaques…



Le ransomware reste la cyber-attaque la plus courante, loin devant les autres

Q6. Quel(s) type(s) de cyber-attaque votre entreprise a-t-elle constaté(s) au cours des 12 derniers mois ? *Base : ont constaté une attaque (112 répondants) / Plusieurs réponses possibles*

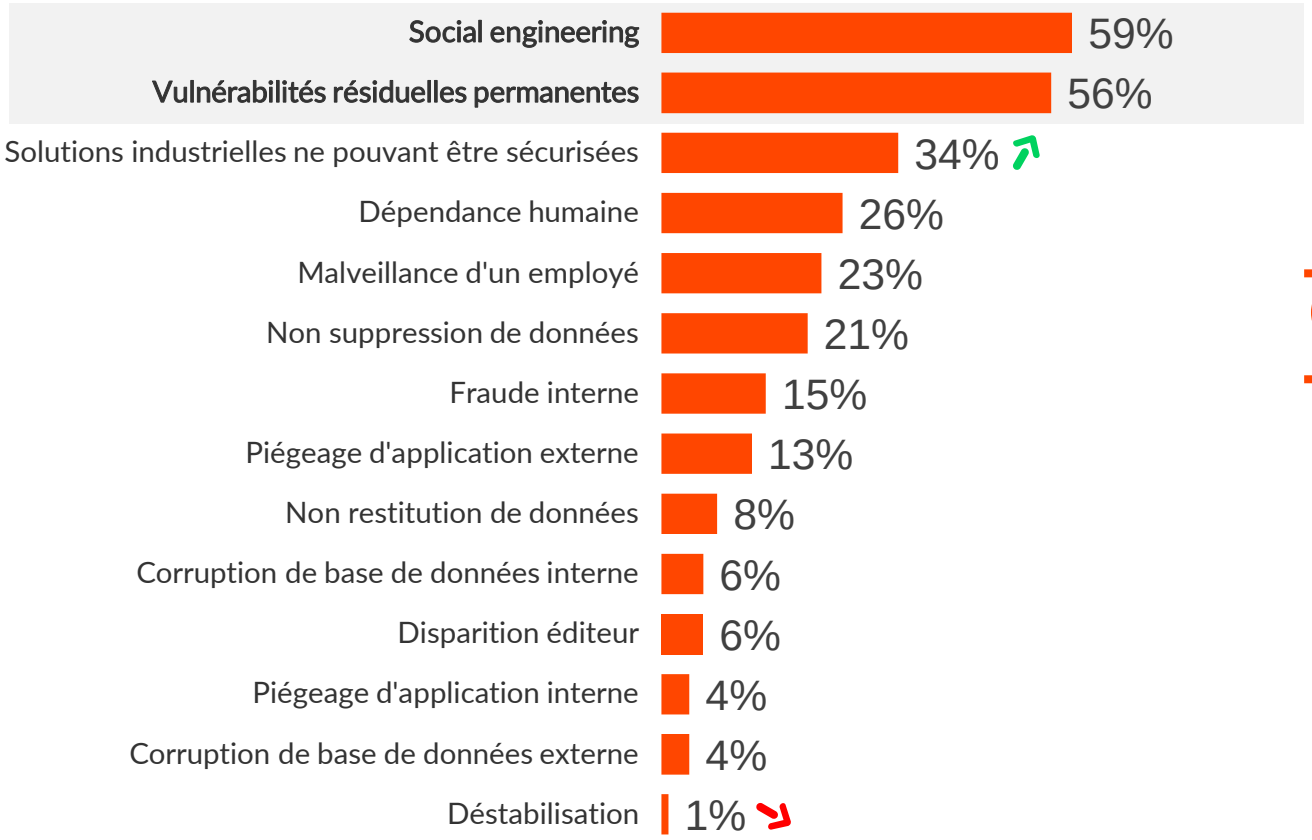


Évolution statistiquement significative vs. 01/2017

Social engineering et vulnérabilités résiduelles continuent de générer des risques, ainsi que des équipements industriels difficilement sécurisables

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 (142 répondants) / Plusieurs réponses possibles*

Les cyber-risques rencontrés



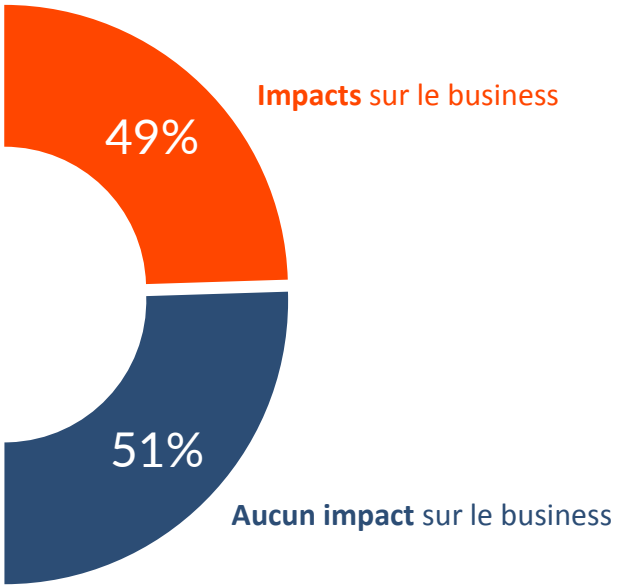
92% ont connu au moins un élément

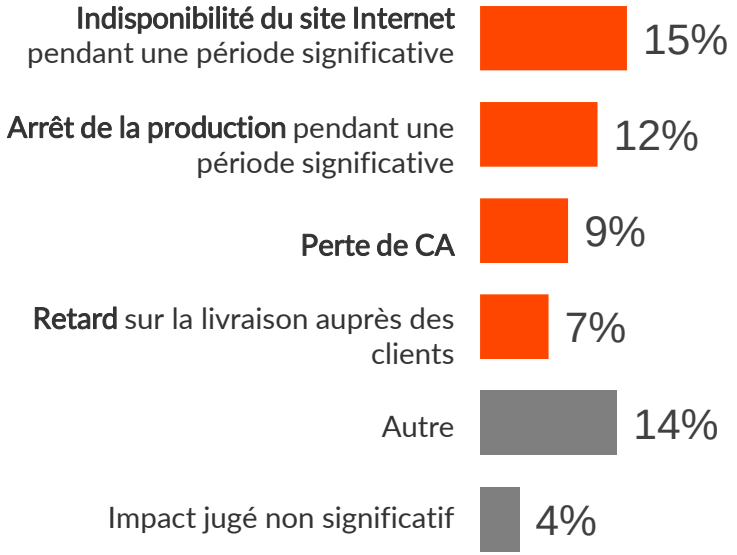
3,0 éléments en moyenne

↗ ↘ Évolution statistiquement significative vs. 01/2017

Des cyber-attaques qui dans un cas sur deux ont un impact concret sur le business des entreprises touchées

Q30. Quel a été l'impact des cyber-attaques sur votre business ? *Base : ensemble (134 répondants) / Plusieurs réponses possibles*



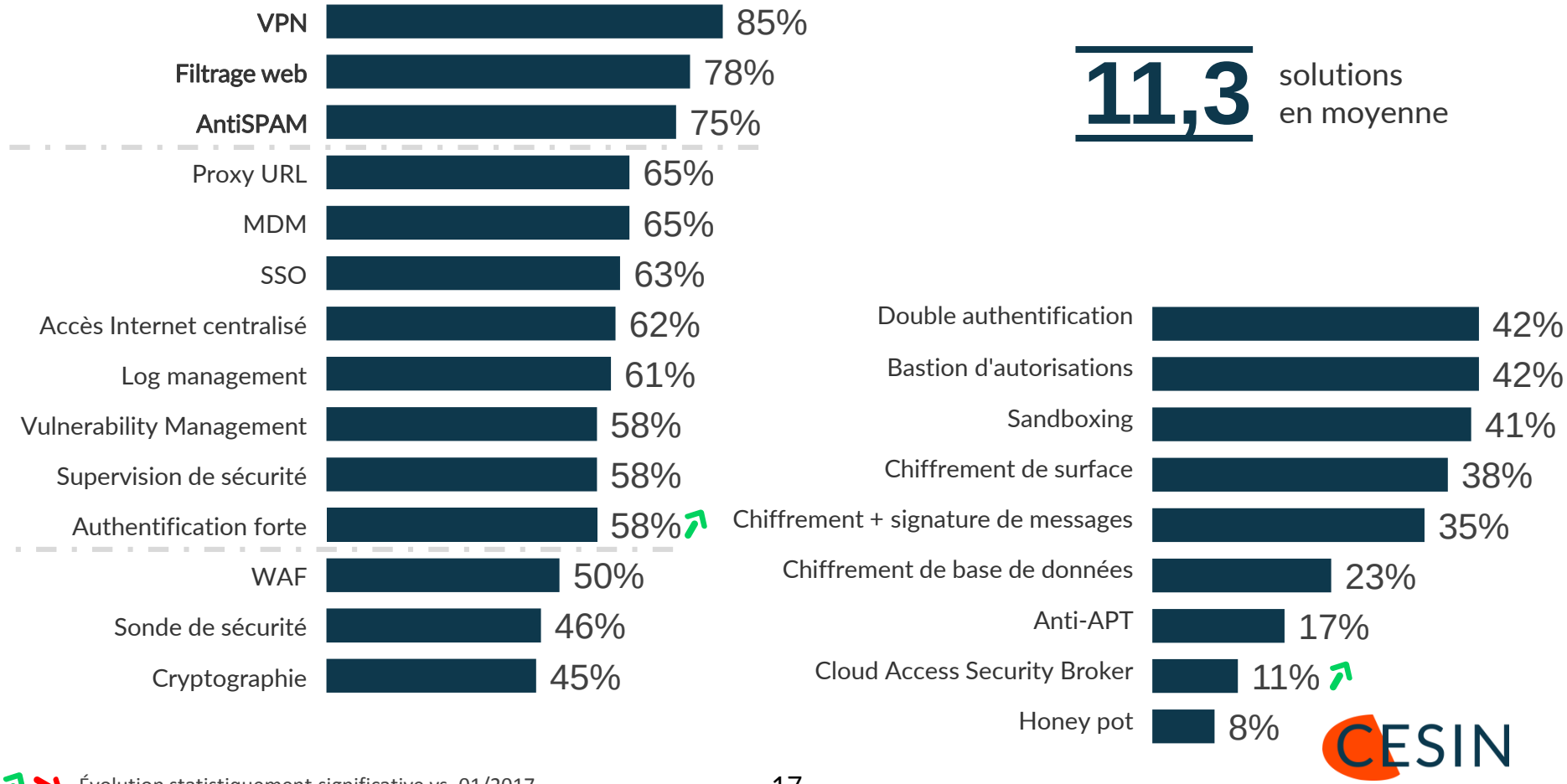


2. FACE AUX CYBER-RISQUES, DES SOLUTIONS TECHNIQUES QUI GAGNENT EN EFFICACITÉ MAIS RESTENT PERFECTIBLES

CESIN

Les entreprises déploient une dizaine de solutions techniques en moyenne , VPN, filtrage web et antiSPAM en tête

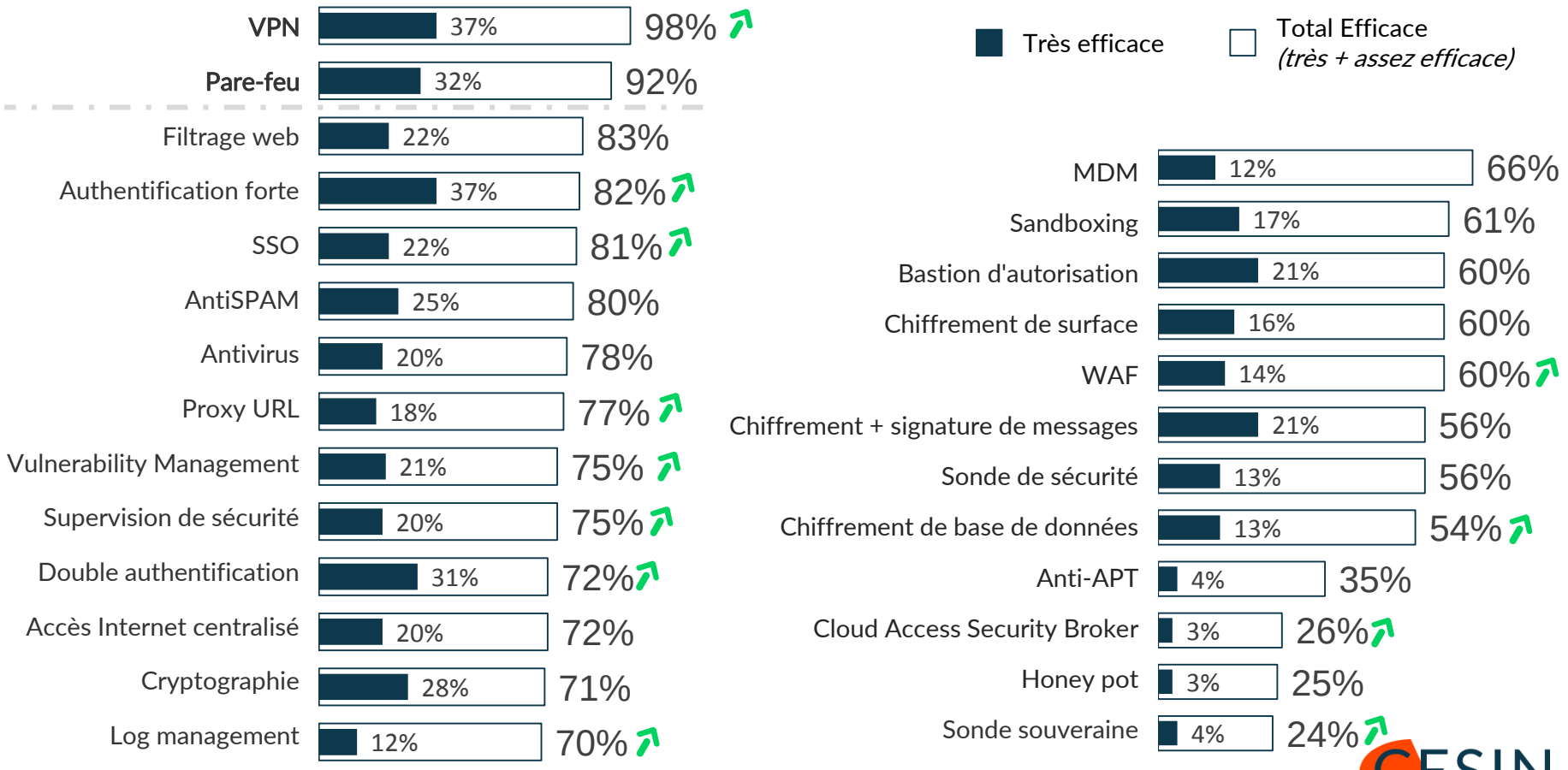
Q8. Parmi les solutions de protection suivantes, quelles sont celles qui ont été mises en place dans votre entreprise, en plus des antivirus et pare-feu ? *Base : ensemble (142 répondants) / Plusieurs réponses possibles*



Évolution statistiquement significative vs. 01/2017

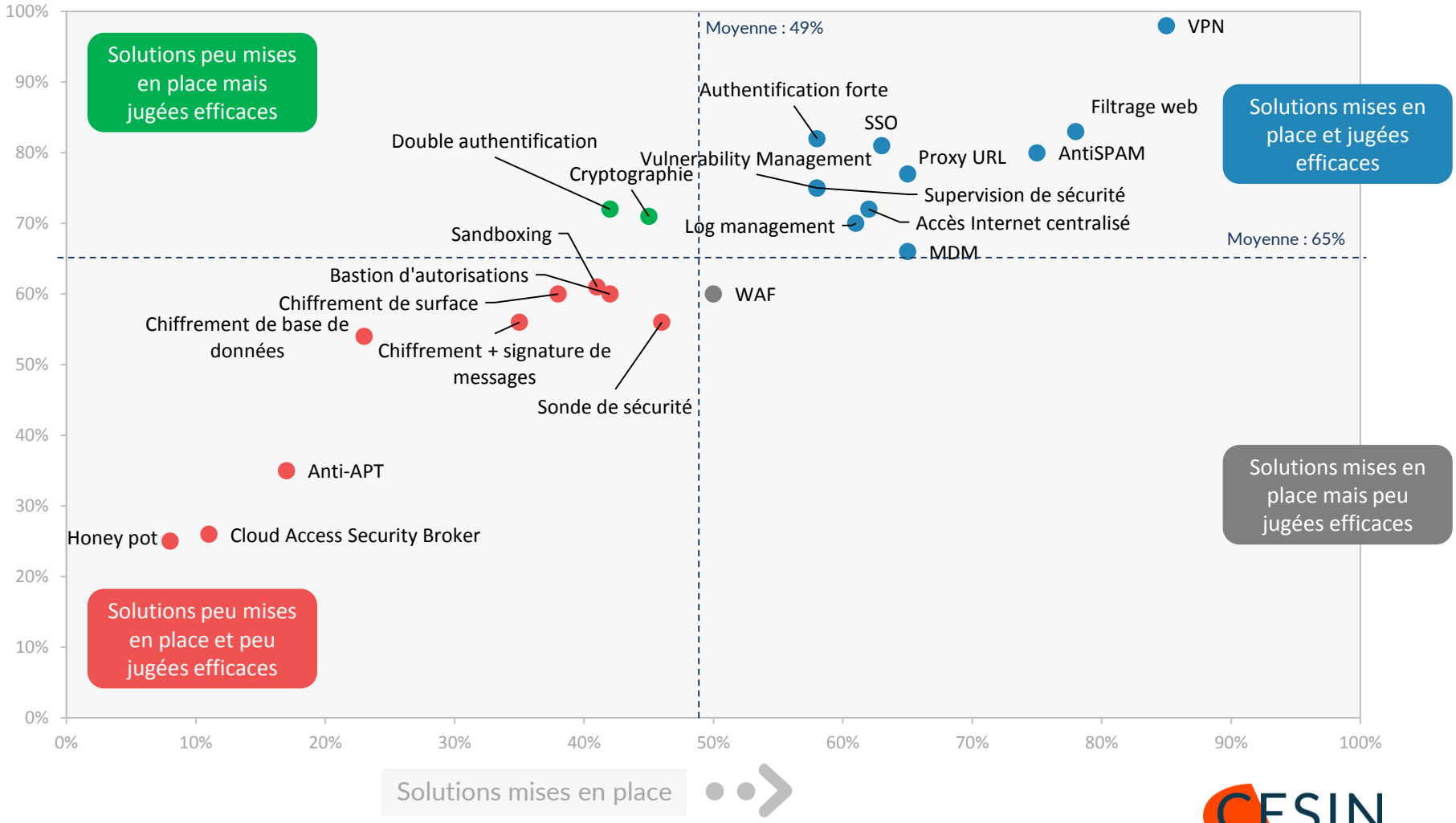
Des solutions techniques dont l'efficacité perçue tend à augmenter

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 (142 répondants)*



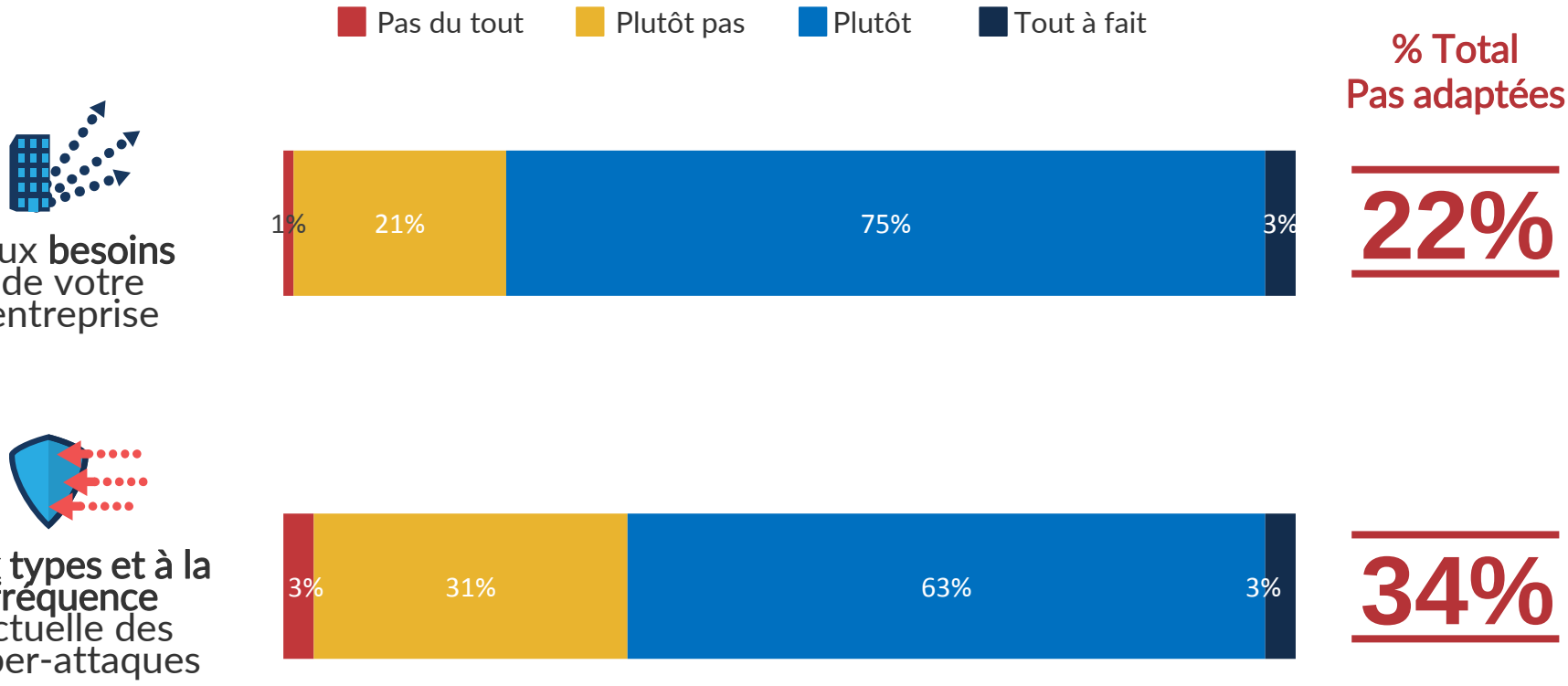
Évolution statistiquement significative vs. 01/2017

Globalement, les solutions mises en place sont celles jugées efficaces, sauf la cryptographie et la double authentification, peu utilisées malgré leur intérêt perçu



Pour autant, les solutions techniques proposées ne sont pas encore totalement en phase avec l'actualité des cyber-attaques

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 (142 répondants)*



Évolution statistiquement significative vs. 01/2017

Dans ce contexte, de plus en plus d'entreprises souscrivent une cyber-assurance

Q9. Par ailleurs, votre entreprise a-t-elle souscrit une cyber-assurance ? *Base : ensemble (142 répondants)*

40% ↗

15%

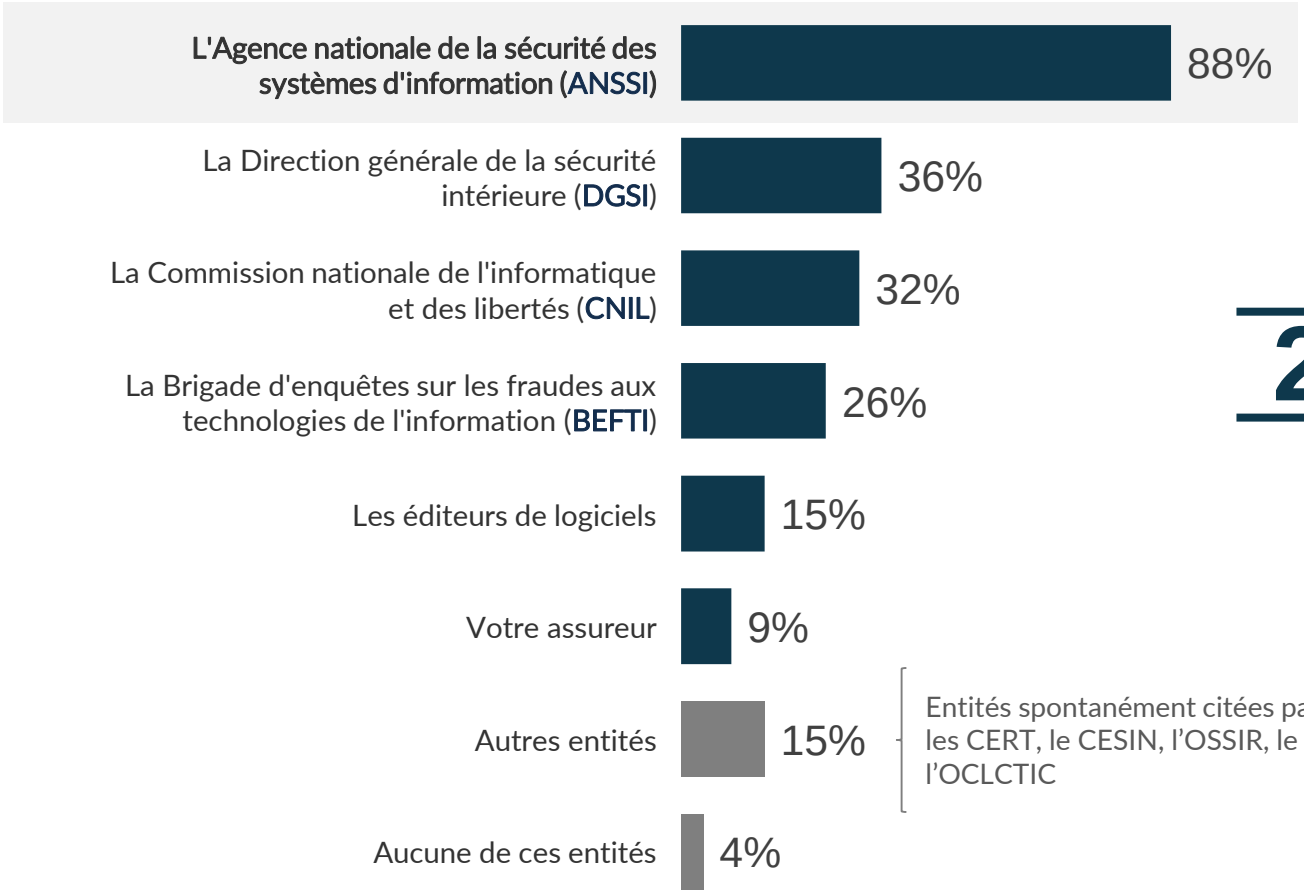
22%

↗↘ Évolution statistiquement significative vs. 01/2017

CESIN

Et les RSSI s'informent auprès de tout un écosystème d'acteurs, l'ANSSI leur semblant le plus légitime

Q31. Quelles entités vous semblent les plus légitimes pour vous conseiller sur la gestion des cyber-risques ? *Base : ensemble (142 répondants) / Plusieurs réponses possibles*



2,3 entités citées en moyenne

Entités spontanément citées par les répondants : les CERT, le CESIN, l'OSSIR, le Clusif, le NIST, l'OCLCTIC

3. D'AUTANT PLUS QUE LA TRANSFORMATION NUMÉRIQUE MULTIPLIE LES RISQUES

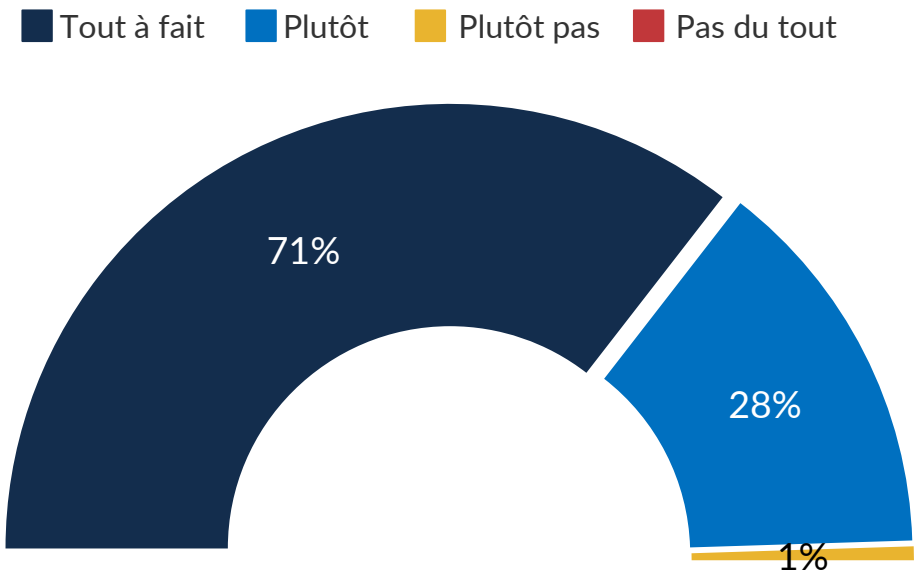
CESIN

La transformation numérique a un réel impact sur la sécurité des systèmes d'information

Q2BIS. Dans votre entreprise, la transformation numérique a-t-elle un impact sur la sécurité des systèmes d'information et des données ? *Base : ensemble (142 répondants)*

99% ↗

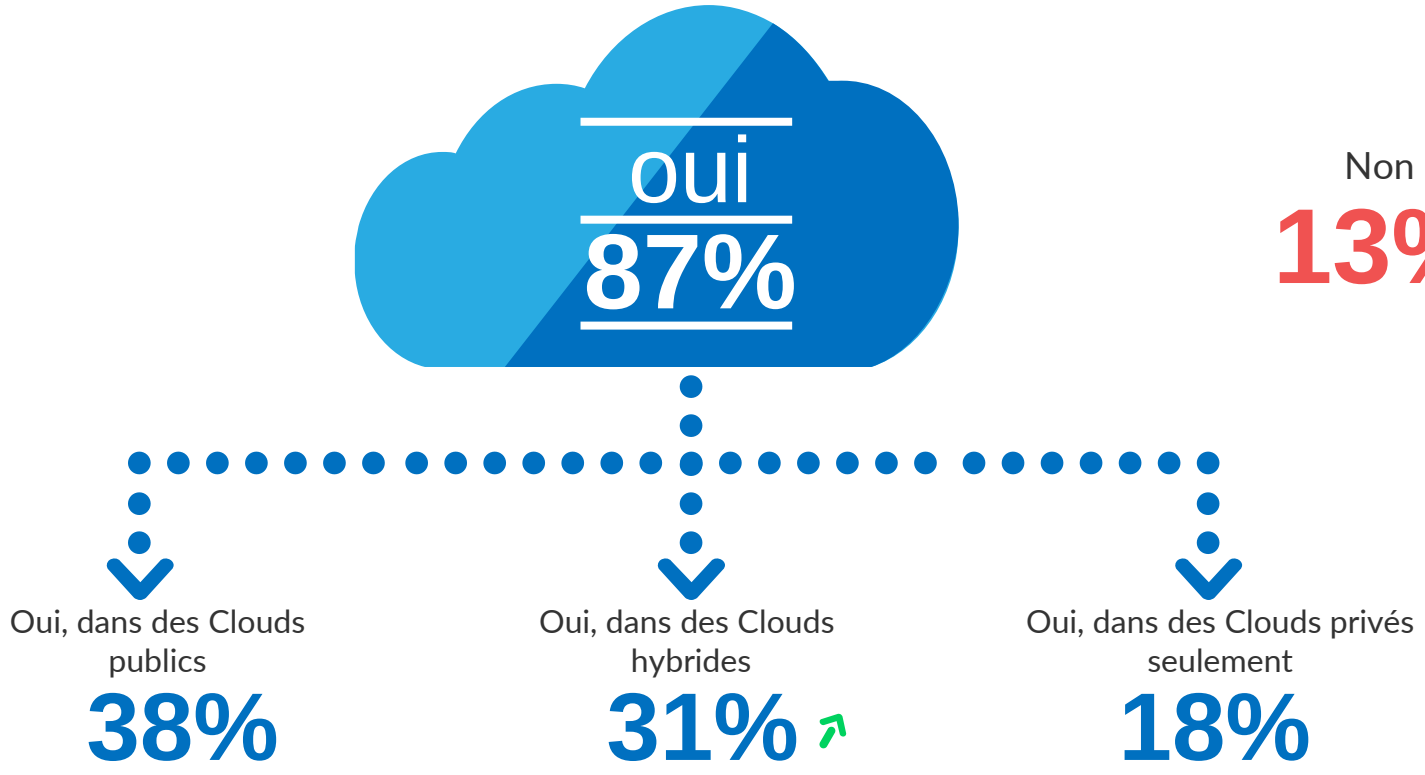
estiment que la transformation numérique a **un impact sur la sécurité** des systèmes d'information et des données



↗↘ Évolution statistiquement significative vs. 01/2017

Engagées dans la transformation numérique, la plupart des entreprises stockent leurs données dans un cloud, et de plus en plus dans des clouds hybrides

Q20. Certaines des données de votre entreprise sont-elles stockées dans un Cloud ? *Base : ensemble (142 répondants)*



Évolution statistiquement significative vs. 01/2017

Le cloud expose les entreprises à différents risques, notamment en ce qui concerne la confidentialité 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 (142 répondants)*

% Un risque fort	
53%	**Confidentialité** des données vis-à-vis de l'hébergeur
49%	Difficultés de contrôle des accès et audits
48%	Stockage des données dans des **datacenters à l'étranger**, hors du droit français
47%	Non-maîtrise de **l'utilisation** qui en est faite **par les salariés** de votre entreprise
43%	Non-maîtrise des **paramètres de sécurité** / chiffrement faible de la part de l'hébergeur
43%	**Non effacement** des données ↘
42%	Traitement **Big Data** à notre insu
37%	**Non restitution** des données ↘
30%	**Propagation systémique** des attaques et erreurs humaines
29%	**Non-alimentation du SOC** (interne ou externe) en données provenant du Cloud
24%	**Indisponibilité** des données
22%	**Attaque par rebond** depuis l'hébergeur
21%	**Piégeage** d'application hébergée
15%	**Corruption** de base de données
15%	**Disparition** de l'hébergeur ↘

↗ ↘ Évolution statistiquement significative vs. 01/2017

CESIN

Sécuriser ses données stockées dans un cloud requiert ainsi des outils spécifiques

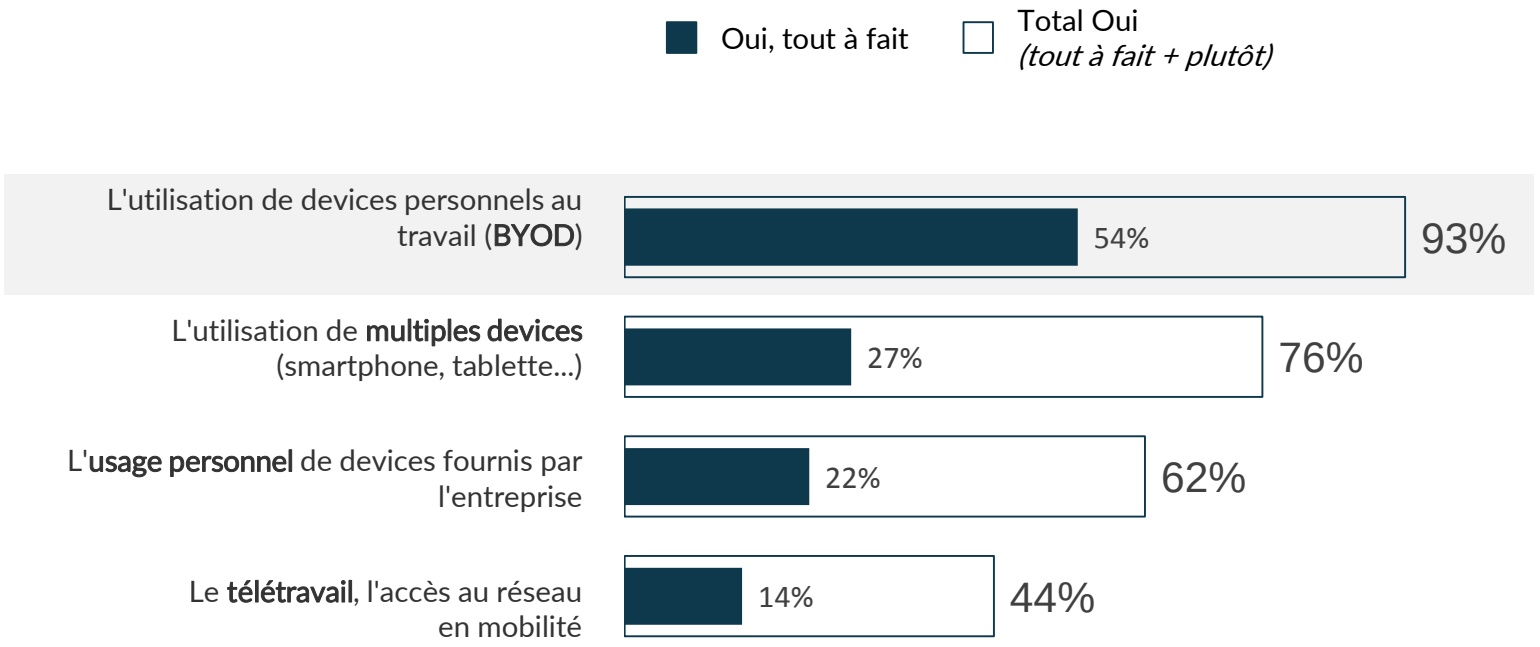
Q23. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?
Base : ensemble (142 répondants)

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

Évolution statistiquement significative vs. 01/2017

La transformation numérique induit également des risques liés aux usages des salariés de l'entreprise, en particulier la multiplicité des devices

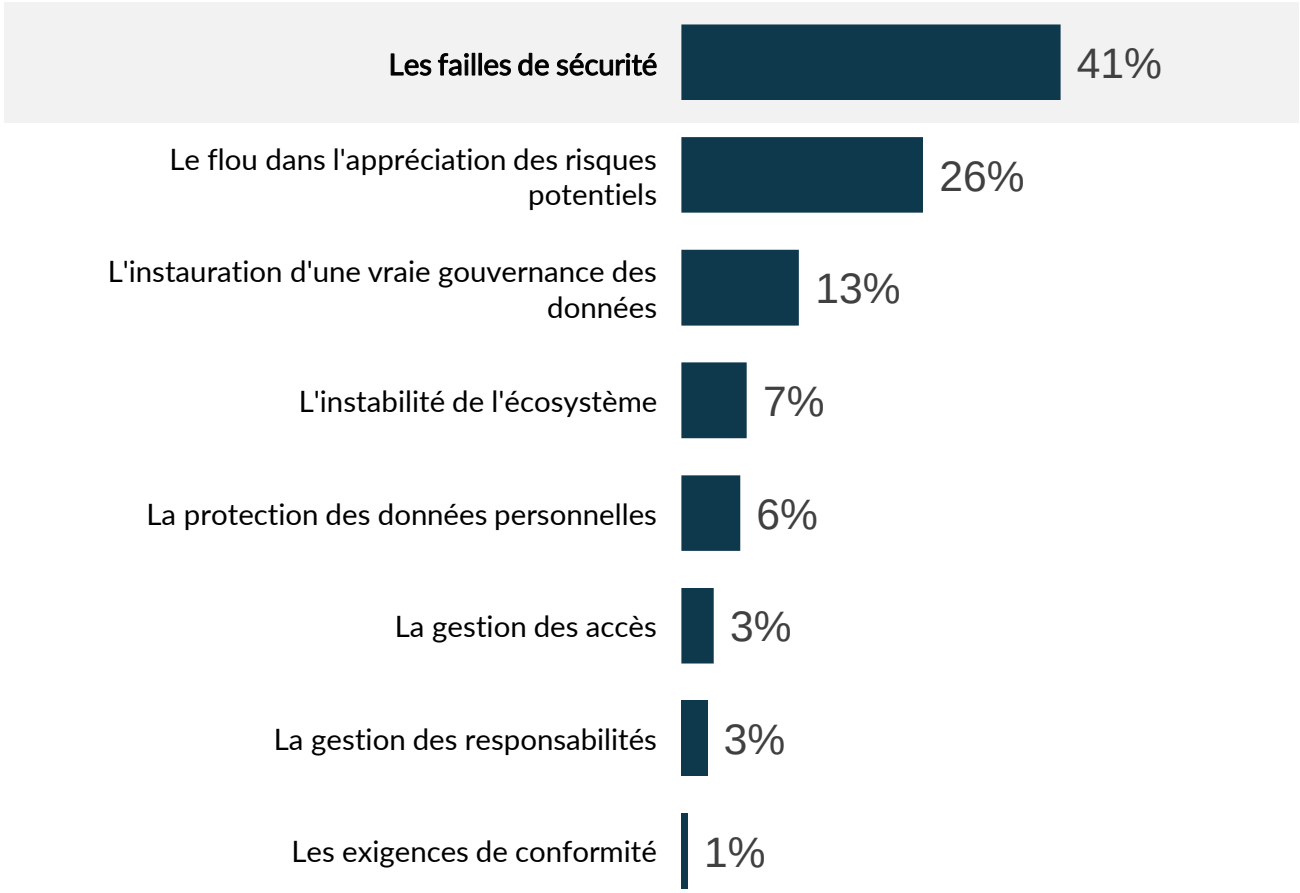
Q24. À vos yeux, les usages suivants du numérique par les salariés représentent-ils un risque pour la cyber-sécurité des entreprises ? *Base : ensemble (142 répondants)*



Évolution statistiquement significative vs. 01/2017

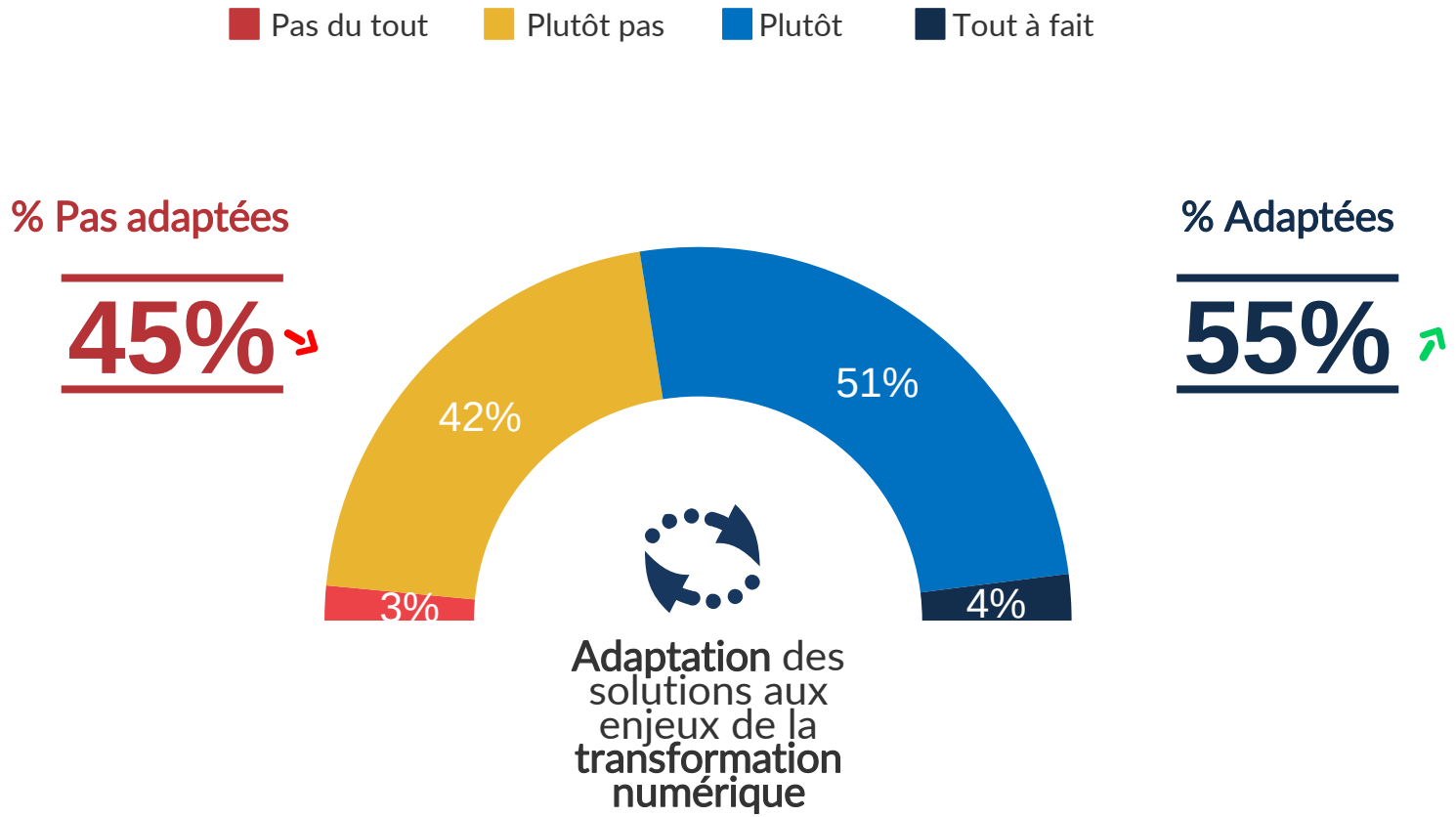
L'IoT génère plusieurs défis à relever, et tout d'abord les failles de sécurité

Q36. D'après vous, quel est le principal défi à relever pour le RSSI en ce qui concerne l'IoT (*Internet of Things*) en entreprise ?
Base : ensemble (142)



Face aux cyber-risques liés à la transformation numérique, les solutions semblent de plus en plus adaptées mais restent perfectibles

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 (142 répondants)*



Évolution statistiquement significative vs. 01/2017

Les salariés restent plutôt sensibilisés aux cyber-risques, mais se montrent peu pro-actifs

Q15. En ce qui concerne la cyber-sécurité, pensez-vous que les salariés de votre entreprise… ? *Base : ensemble (142 répondants)*

73%
pensent que les salariés **sont sensibilisés** aux cyber-risques

59%
pensent que les salariés **respectent les recommandations**

19%
pensent que les salariés **prennent des précautions au-delà des recommandations** données

Évolution statistiquement significative vs. 01/2017

Près de deux entreprises sur trois ont 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 (142 répondants)*

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

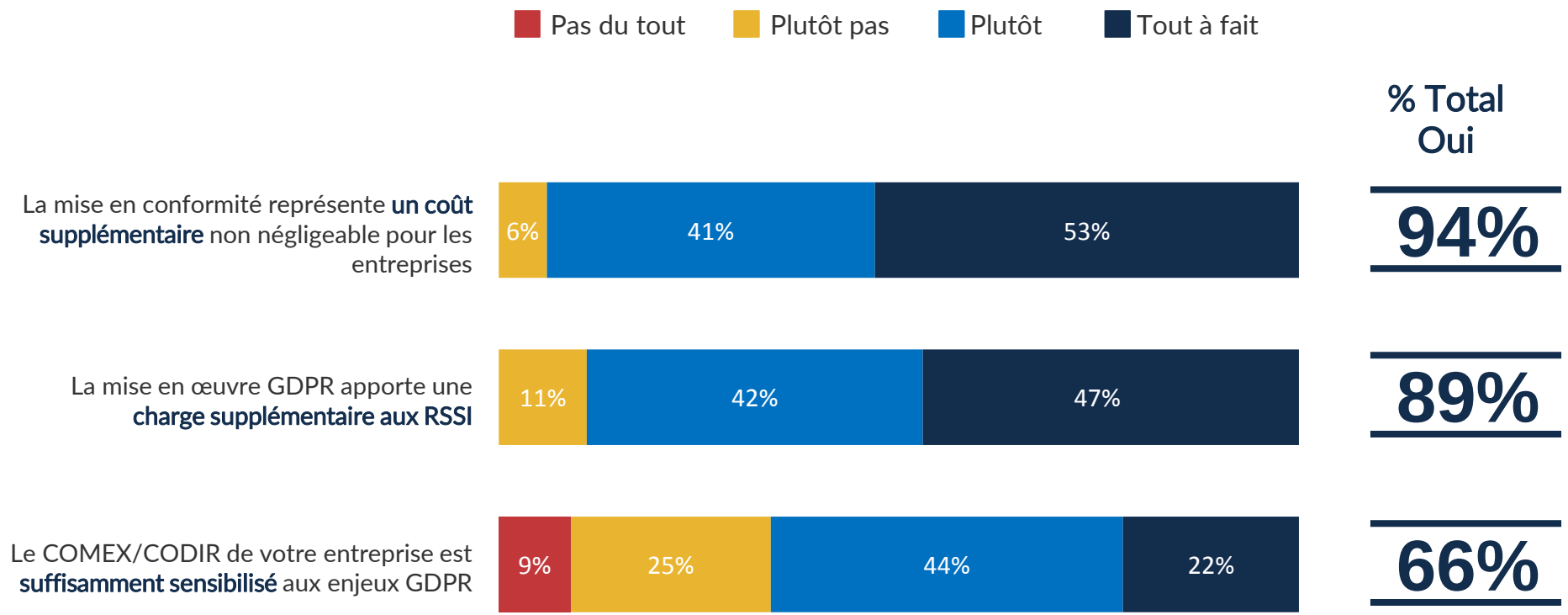
Évolution statistiquement significative vs. 01/2017

4. UNE GESTION DES RISQUES COMPLIQUÉE PAR LA MISE EN CONFORMITÉ GDPR

CESIN

La mise en conformité génère un coût financier pour les entreprises, mais aussi une charge pour les RSSI

Q32. Concernant la mise en conformité GDPR, diriez-vous que… ? *Base : ensemble (142)*



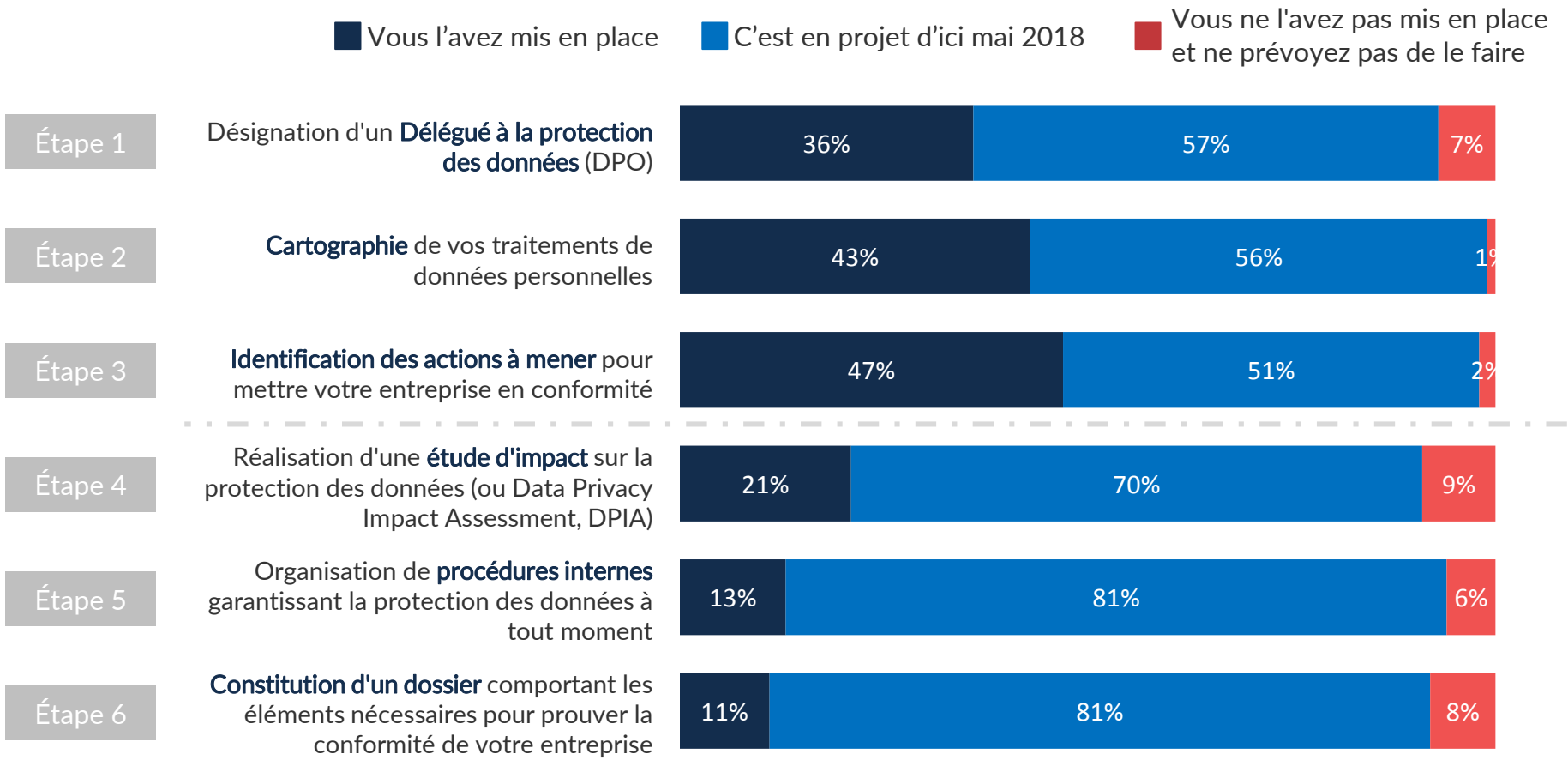
Une gestion d'autant plus complexe que le cumul des fonctions de RSSI et de DPO est estimé compatible par plus d'un tiers des répondants

Q34. Pensez-vous que le poste de RSSI est compatible avec la fonction de DPO ? *Base : ensemble (142)*

estiment que la **fonction de DPO** peut être assurée **par un RSSI**

Si les premières étapes de la mise en conformité GDPR ont été mises en place dans plus d'un tiers des entreprises, il reste beaucoup à faire d'ici mai 2018

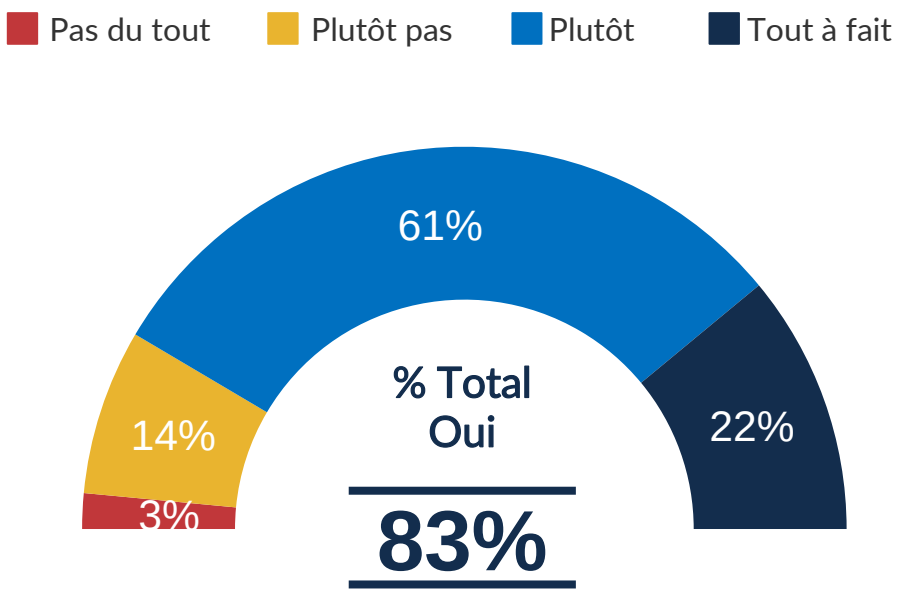
Q33. Dans le cadre de la mise en conformité GDPR, votre entreprise a-t-elle effectué les actions suivantes ? *Base : ensemble (142)*



Pour autant, la plupart des entreprises reconnaissent que la GDPR permettra de mieux renforcer la protection des données

Q32. Concernant la mise en conformité GDPR, diriez-vous que… ? *Base : ensemble (142)*

« La mise en conformité GDPR permettra de réellement renforcer la protection des données personnelles »



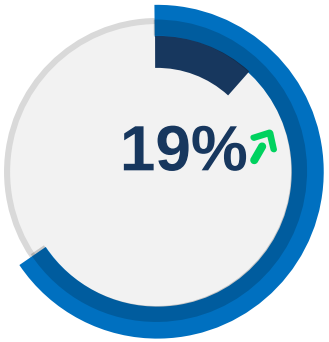
4. ACCOMPAGNER L'ÉLAN IMPULSÉ PAR LA GDPR POUR REFONDER LA GOUVERNANCE DES DONNÉES

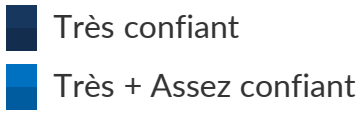
CESIN

Pour l'avenir, une confiance dans la capacité à faire face aux cyber-risques réelle et en hausse

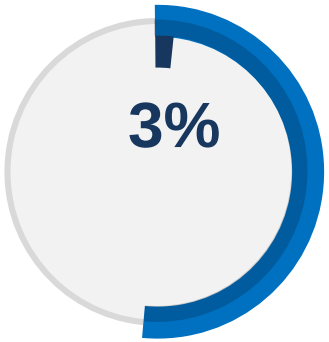
Q26. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (142 répondants)

71%
La **prise en compte des enjeux** de la cyber-sécurité au sein du COMEX votre entreprise





63%
La **capacité** de votre entreprise à faire face aux cyber-risques



La plupart des entreprises envisagent d'investir davantage dans la cyber-sécurité, notamment en augmentant les effectifs dédiés

Q11BIS. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ? *Base : ensemble (142 répondants)*

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

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

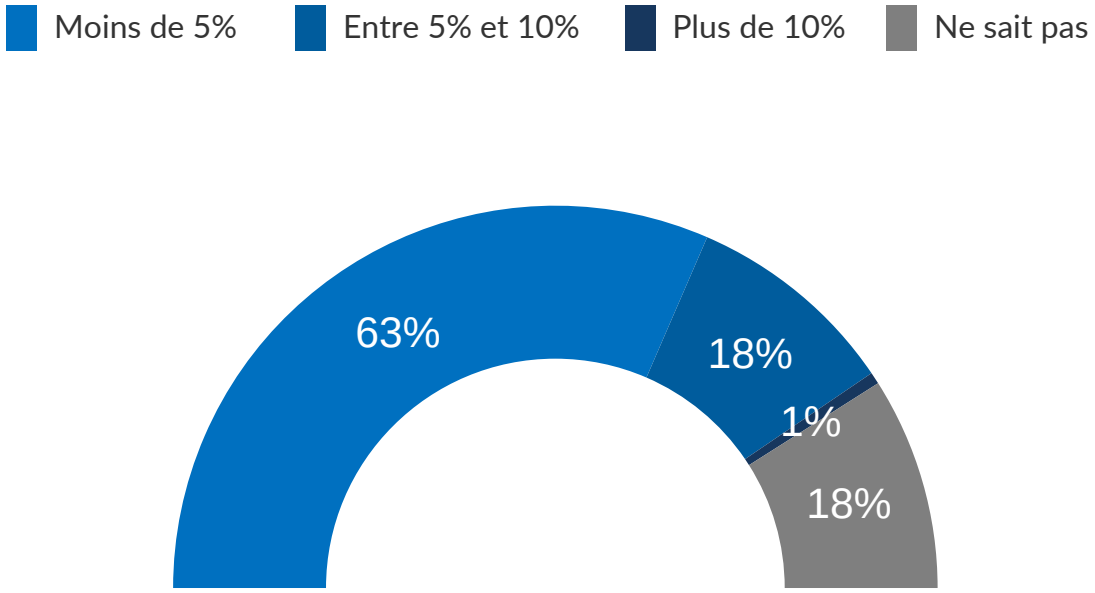
d'**augmenter les effectifs** alloués à la protection contre les cyber-risques

Évolution statistiquement significative vs. 01/2017

CESIN

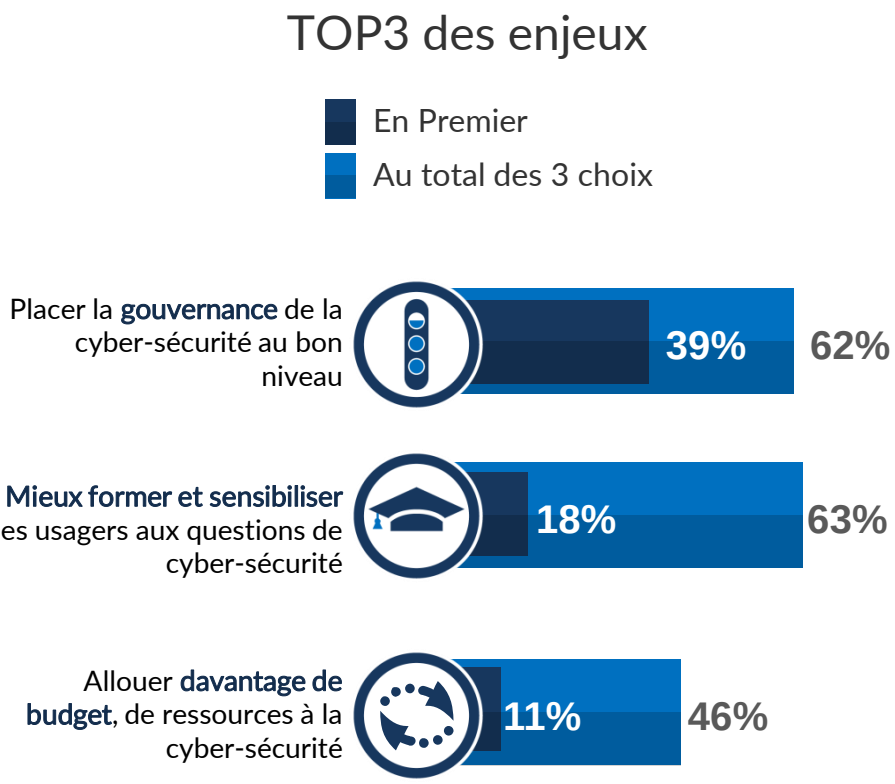
Des investissements envisagés qui font écho à la faible part du budget IT actuellement consacré à la sécurité

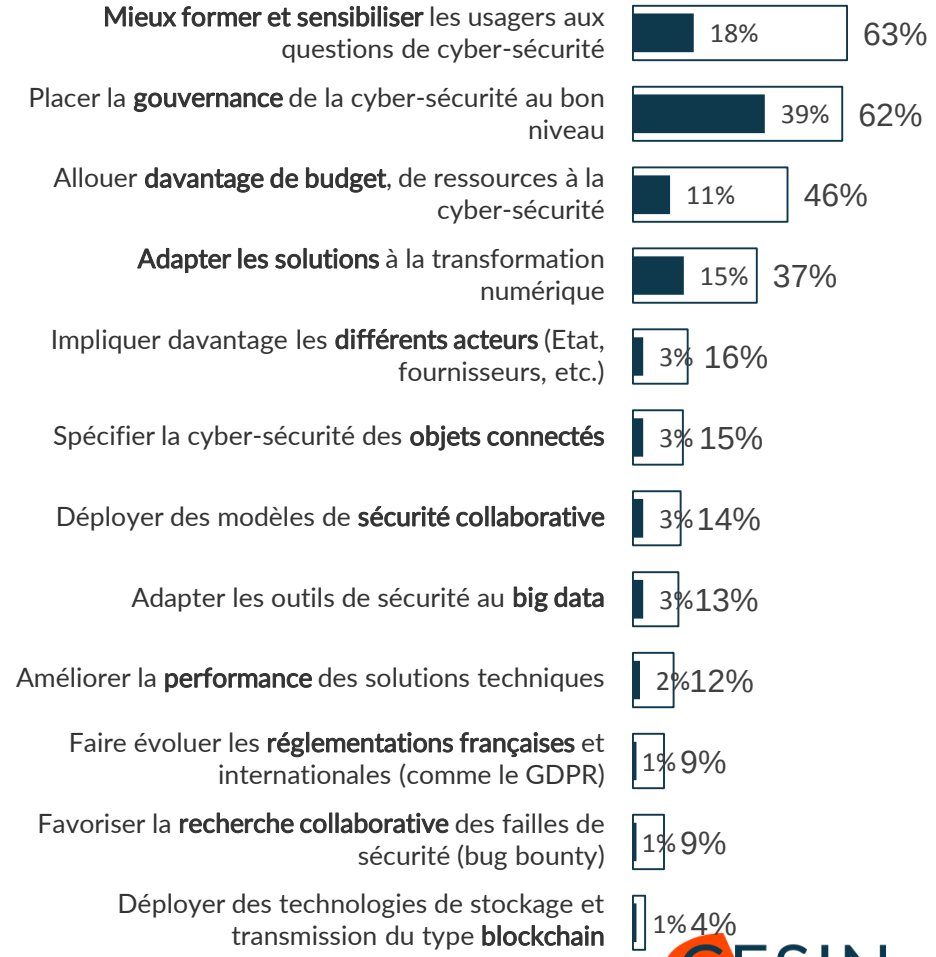
Q37. Dans votre entreprise, quelle part du budget IT est consacrée à la sécurité ? *Base : ensemble (142 répondants)*



Pour demain, l'enjeu reste humain plus que technique : former, sensibiliser, refonder la gouvernance de la cyber-sécurité

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 (142 répondants)*



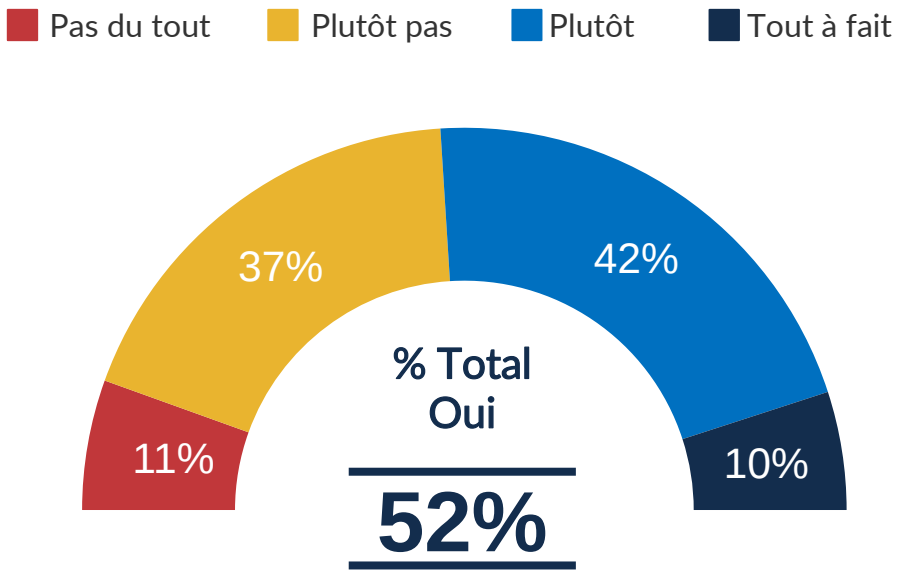


Évolution statistiquement significative vs. 01/2017

Un changement de gouvernance déjà initié par une entreprise sur deux à l'occasion de la mise en conformité GDPR

Q32. Concernant la mise en conformité GDPR, diriez-vous que… ? *Base : ensemble (142)*

« La mise en place du GDPR **a changé la gouvernance de l'entreprise** en matière de protection de l'information »

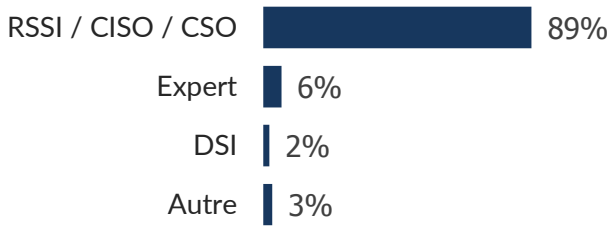


ANNEXES

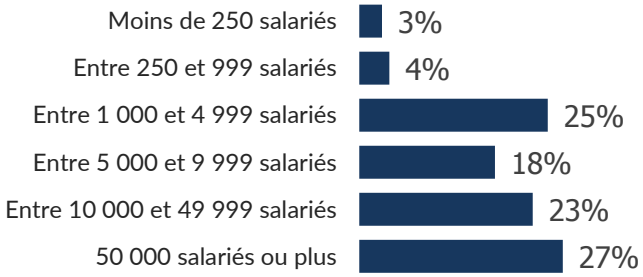
Profil des répondants

142 membres du CESIN ont participé à cette enquête

Fonction des répondants :



Nombre de salariés de l'entreprise :



Secteur d'activité de l'entreprise :