Ponemon INSTITUTE

L’état des architectures de sécurité SD-WAN, SASE et Zero Trust

Sponsorisé par Aruba

Réalisé indépendamment par le Ponemon Institute LLC

Date de publication : Avril 2021

L’état des architectures de sécurité SD-WAN, SASE et Zero Trust

Présenté par le Ponemon Institute, avril 2021

Partie 1. Introduction

L’objet de cette recherche est d’obtenir d’importantes informations sur l’utilisation du SDN (Software-defined Networking ou mise en réseau définie par logiciel) dans des architecture SD-WAN (réseau local étendu), SASE (service d'accès sécurisé Edge) et Zero Trust. Sponsorisé par Aruba, le Ponemon Institute a interrogé 1 826 professionnels de la sécurité et de la mise en réseau dans les régions Amérique du Nord, EMEA, Asie-Pacifique et LATAM. Dans le contexte de cette recherche, les technologies mentionnées plus haut sont définies comme suit.

- **SD-WAN** simplifie la gestion et le fonctionnement d’un réseau WAN en dissociant le matériel réseau de son mécanisme de contrôle et en virtualisant les services de transport.

- **SASE et Zero Trust** sont des architectures de sécurité utilisées pour mettre en œuvre les contrôles de sécurité.

Les résultats qui suivent révèlent l’état d’adoption et de mise en œuvre.

- **Le choix d’une architecture SASE haut de gamme est préférable.** Soixante-dix pour cent des participants sont prêts à choisir un fournisseur jugé être parmi les meilleurs lorsqu’ils déploient la sécurité SD-WAN cloud pour une architecture SASE.

- **Les organisations qui sont convaincues que leur architecture de sécurité est efficace sont en tête dans le déploiement de Zero Trust, SASE et SD-WAN.** Près de la moitié des organisations performantes (48 % des participants) ont déployé ou déploieront Zero Trust comparé à 35 % des participants dans l'échantillon global. Quarante-trois pour cent des participants représentant des organisations performantes ont déployé ou déploieront SASE comparé à 24 % des participants dans l’échantillon global.

- **L'Amérique du Nord arrive en tête dans le déploiement de Zero Trust, SD-WAN et SASE.** Quarante-trois pour cent des participants nord-américains ont déployé Zero Trust comparé à 33, 31 et 26 % (respectivement) des participants représentant les régions EMEA, APAC et LATAM. Ces chiffres sont identiques à ceux du déploiement de SD-WAN et SASE, comme indiqué dans le rapport.

- **L’architecture de sécurité Zero Trust est plus connue que les architectures SD-WAN et SASE.** Soixante-deux pour cent des participants sont familiers ou très familiers avec Zero Trust. Vient ensuite la familiarité avec l’architecture de sécurité SASE (45 % des participants).

- **L’adoption des architectures Zero Trust et SASE est appelée à croître.** Cinquante-sept pour cent des participants affirment que leurs organisations ont déployé ou déploieront Zero Trust et 49 % des participants indiquent que leurs organisations ont déployé ou déploieront l'architecture SASE.

- **L’équipe réseau joue un rôle prépondérant dans le déploiement de SD-WAN.** Quarante-six pour cent des participants affirment que l’équipe réseau joue le rôle le plus important dans le déploiement des solutions SD-WAN et bénéficie des conseils de l’équipe de sécurité. Trente-sept pour cent des participants affirment que l’équipe de sécurité joue un rôle prépondérant dans le déploiement et reçoit des conseils de l’équipe réseau.

- **Quel type de fournisseur les organisations engageraient-elles lorsqu'elles mettent en œuvre des services de sécurité cloud tels qu'un pare-feu en tant que service basé dans le cloud ou un CASB ?** Quarante-quatre pour cent des participants affirment que leurs organisations utiliseraient les fournisseurs de pointe qui se consacrent aux services de sécurité cloud.

Partie 2. Principaux résultats

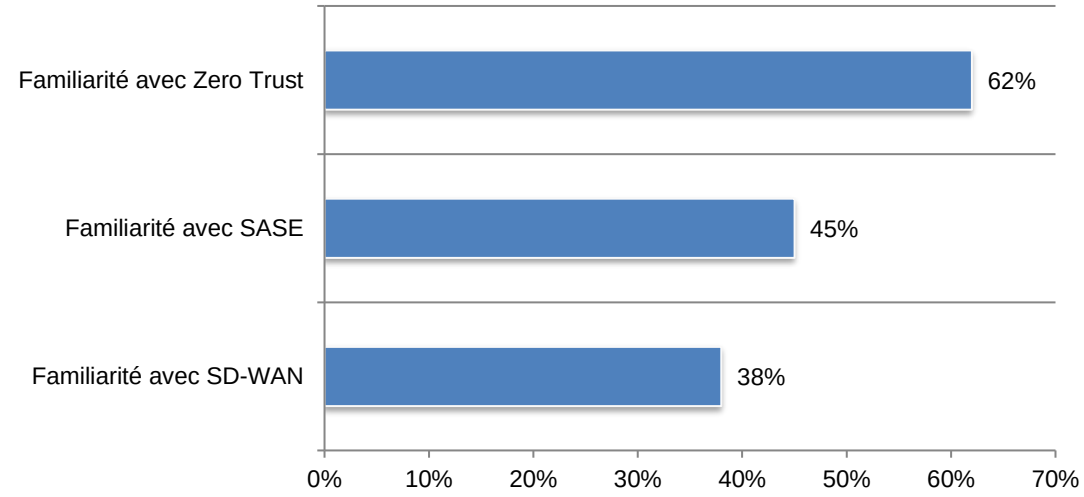
Dans cette section, nous vous proposons une analyse des résultats de la recherche. Les résultats complets et audités sont présentés dans l'annexe de ce rapport. Les sujets suivants ont été abordés dans ce rapport.

- La familiarité et le déploiement de SD-WAN, de la sécurité cloud, de l'architecture SASE et de l'architecture de sécurité Zero Trust
- Différences régionales
- Les pratiques des organisations dotées d'une architecture et mise en œuvre de sécurité extrêmement efficaces

La familiarité et le déploiement de SD-WAN, de la sécurité cloud, de l'architecture SASE et de l'architecture de sécurité Zero Trust

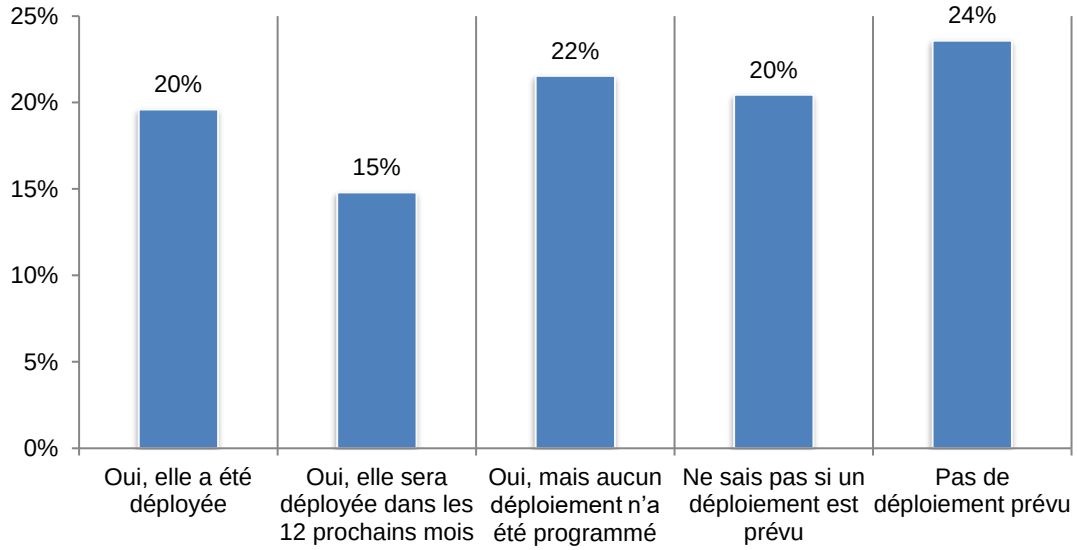
L'architecture de sécurité Zero Trust est plus connue que les architectures SD-WAN et SASE. Comme le montre la Figure 1, 62 % des participants sont familiers ou très familiers avec Zero Trust. Vient ensuite la familiarité avec l'architecture de sécurité SASE (45 % des participants). Seulement 38 % des participants affirment être familiers ou très familiers avec les solutions SD-WAN.

Figure 1. Familiarité avec Zero Trust, SD-WAN et SASE
Réponses « Très familier » et « Familier » combinées



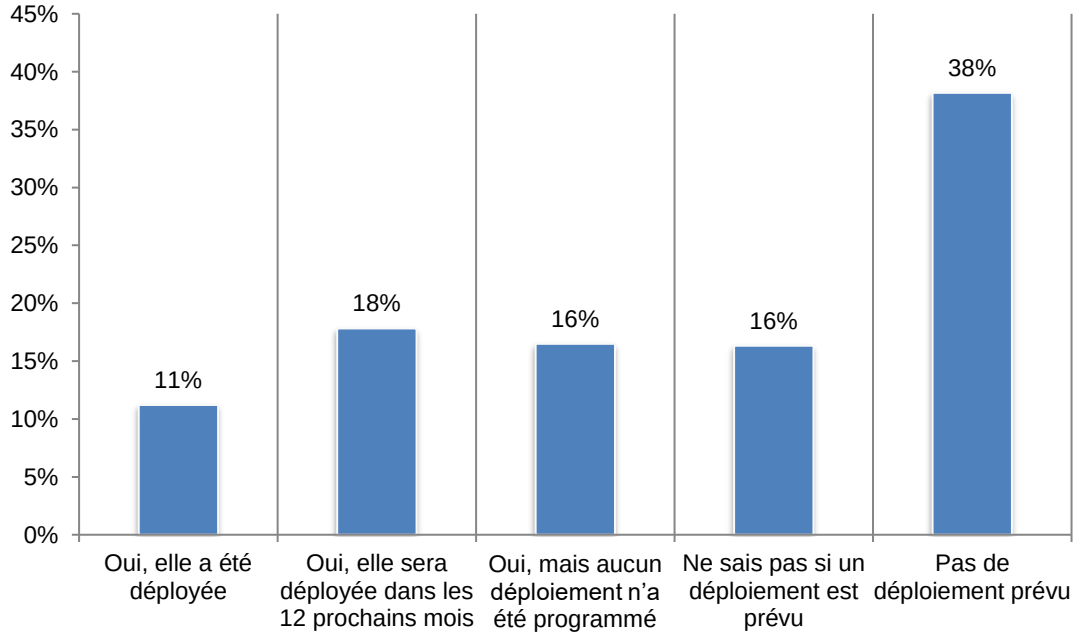
La majorité des organisations ont déployé ou envisagent de déployer l'architecture de sécurité Zero Trust. D'après la Figure 2, 57 % des participants affirment que Zero Trust a été déployé (20 %), qu'il sera déployé au cours des 12 prochains mois (15 %) ou qu'il sera déployé à l'avenir (22 %).

Figure 2. Votre organisation a-t-elle déployé ou envisage-t-elle de déployer l'architecture de sécurité Zero Trust ?



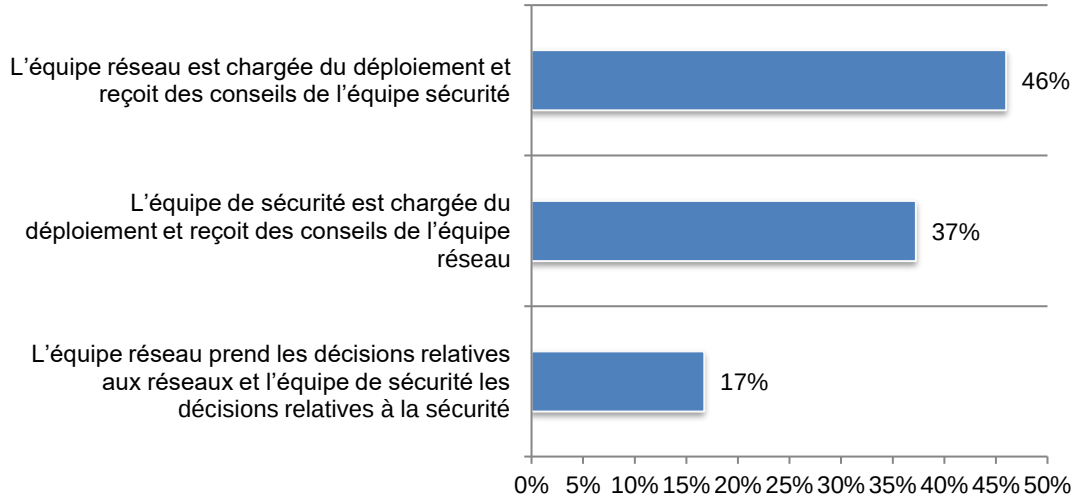
Quarante-cinq pour cent des participants affirment que leurs organisations ont déployé ou envisagent de déployer les solutions SD-WAN. D'après la Figure 3, 11 % des participants affirment qu'elles ont été déployées, 18 % des participants affirment qu'elles seront déployées dans les 12 prochains mois et 16 % des participants affirment qu'elles seront déployées à l'avenir.

Figure 3. Votre organisation a-t-elle déployé ou envisage-t-elle de déployer les solutions SD-WAN ?



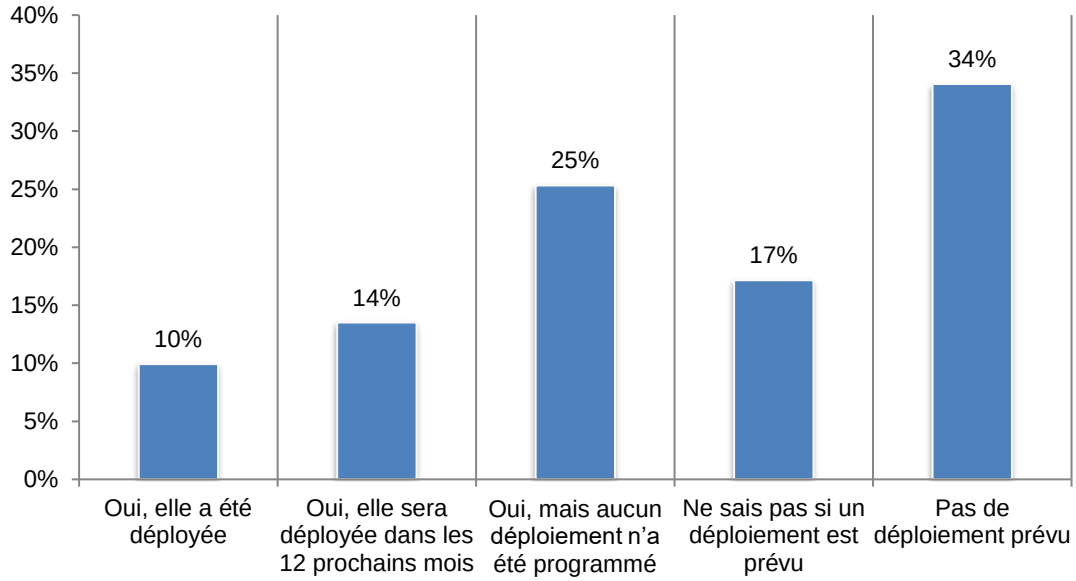
L'équipe réseau joue un rôle prépondérant dans le déploiement de solutions SD-WAN. Comme le montre la Figure 4, 46 % des participants affirment que l'équipe réseau a plus d'influence et bénéficie des conseils de l'équipe de sécurité. Dix-sept pour cent seulement affirment que l'équipe réseau prend les décisions relatives aux réseaux et l'équipe de sécurité les décisions relatives à la sécurité.

Figure 4. Qui aura le plus d'influence sur le déploiement de SD-WAN ?



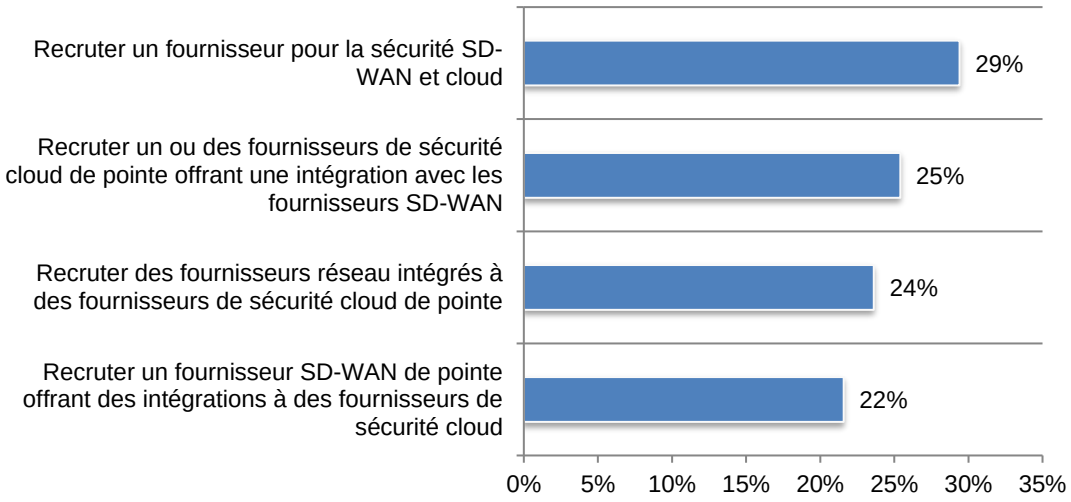
Près de la moitié des participants affirment que leurs organisations ont déployé ou déploieront l'architecture de sécurité SASE. D'après la Figure 5, 49 % des participants affirment avoir déployé (10 %), qu'ils déploieront dans 12 mois (14 %) ou qu'ils déploieront à l'avenir (25 %).

Figure 5. Votre organisation a-t-elle déployé ou envisage-t-elle de déployer l'architecture de sécurité SASE ?



La sélection d'un fournisseur de pointe pour le déploiement de la sécurité SD-WAN et cloud pour une architecture SASE est préférable. Comme indiqué, 71 % des participants affirment que leurs organisations préfèrent engager un ou des fournisseurs de sécurité qui proposent une intégration avec les fournisseurs SD-WAN (25 %), des fournisseurs réseau intégrés à des fournisseurs de sécurité cloud de pointe (24 %) et un fournisseur SD-WAN de pointe offrant des intégrations à des fournisseurs de sécurité cloud (22 %).

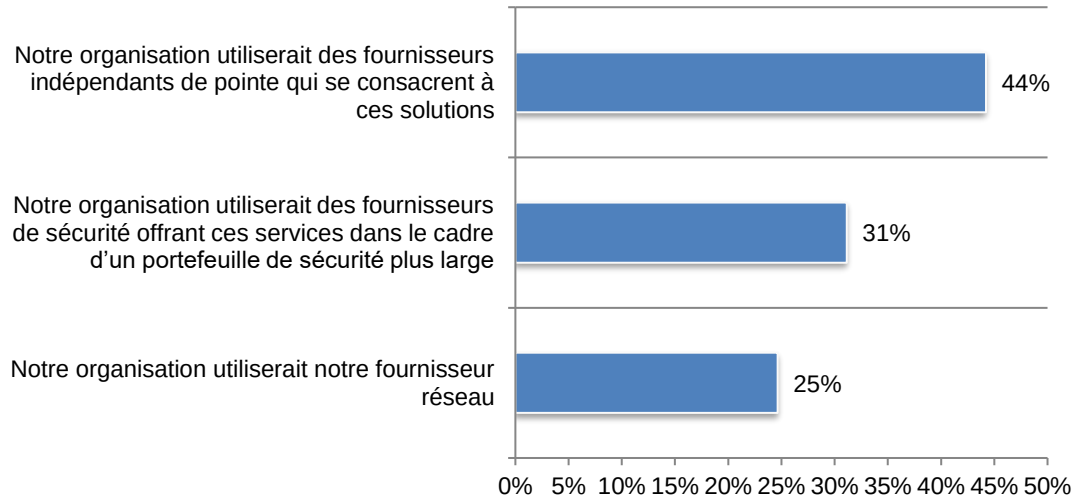
Figure 6. Si votre organisation déploie la sécurité SD-WAN et cloud-pour une architecture SASE, comment les fournisseurs seront-ils sélectionnés ?
Un seul choix est autorisé



L'équipe réseau prendra, en toute probabilité, les décisions concernant l'architecture des solutions de sécurité. Quarante-deux pour cent des participants affirment qu'au sein de leurs organisations, c'est l'équipe réseau qui prend ces décisions, 31 % d'entre eux pensent que c'est l'équipe de sécurité qui s'en charge et 27 % affirment que l'équipe réseau et l'équipe de sécurité prennent ensemble les décisions concernant l'architecture/les produits de solutions de sécurité.

D'après la Figure 7, l'engagement d'un fournisseur lors de la mise en œuvre de services de sécurité cloud (par exemple pare-feu cloud en tant que service, agent de sécurité des accès au cloud, etc.) reflète le désir des organisations d'utiliser des fournisseurs de pointe indépendants qui se consacrent à ces solutions (44 % des participants), des fournisseurs de sécurité qui proposent ces services dans le cadre d'un portefeuille de sécurité plus large (31 % des participants) ou leur propre fournisseur réseau (25 % des participants).

Figure 7. Comment sont prises les décisions relatives aux fournisseurs lors de la mise en œuvre des services de sécurité cloud ?

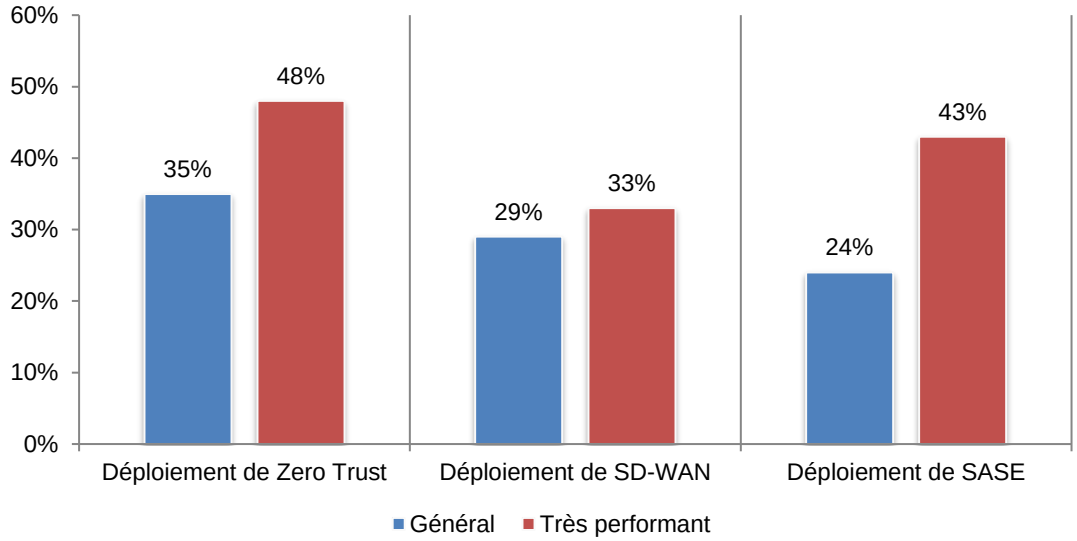


Les pratiques des organisations dotées d'une architecture et mise en œuvre de sécurité extrêmement efficaces

Dans cette section, nous proposons une analyse des résultats des participants qui ont déclaré que leurs organisations avaient confiance en l'efficacité de leur architecture et mise en œuvre de sécurité (22 % des participants). Nous considérons ces participants comme étant hautement performants.

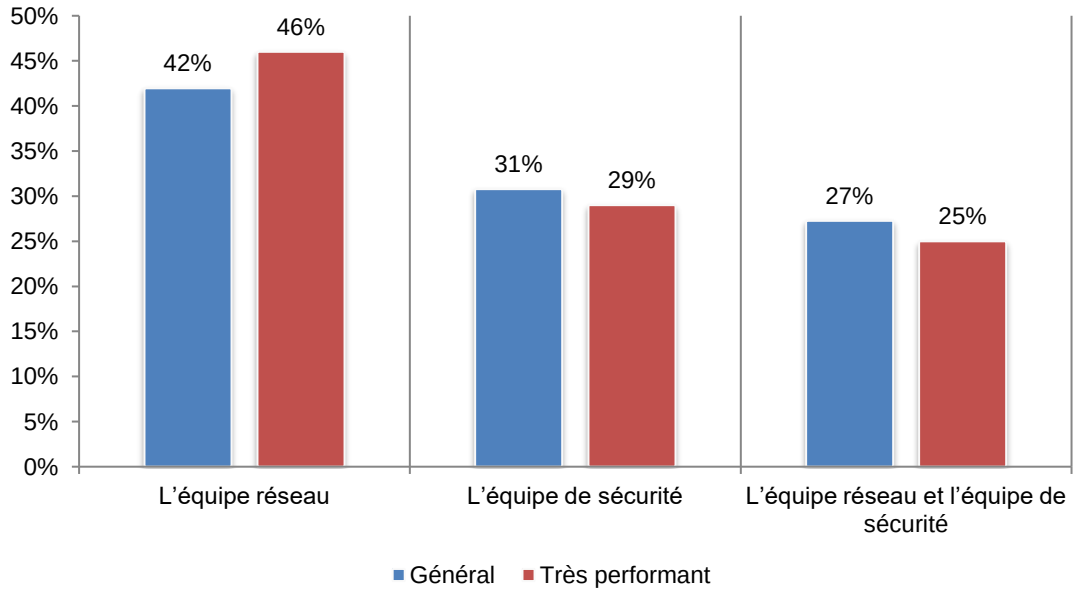
Les organisations hautement performantes sont plus à même de déployer Zero Trust, SD-WAN et SASE. D'après la Figure 8, près de la moitié des participants hautement performants (48 %) ont déployé Zero Trust contre 35 % seulement dans l'échantillon global des participants. Quarante-trois pour cent des participants hautement performants ont déployé SASE comparé à 24 % des participants dans l'échantillon global.

Figure 8. Déploiement de Zero Trust, SD-WAN et SASE
Réponses « Déployé » et « Sera déployé dans 12 mois » combinées



Les organisations performantes sont légèrement plus à même d'affirmer que c'est l'équipe réseau qui prend les décisions concernant l'architecture des solutions de sécurité, comme le montre la Figure 9.

Figure 9. Qui prend les décisions concernant l'architecture des solutions de sécurité ?

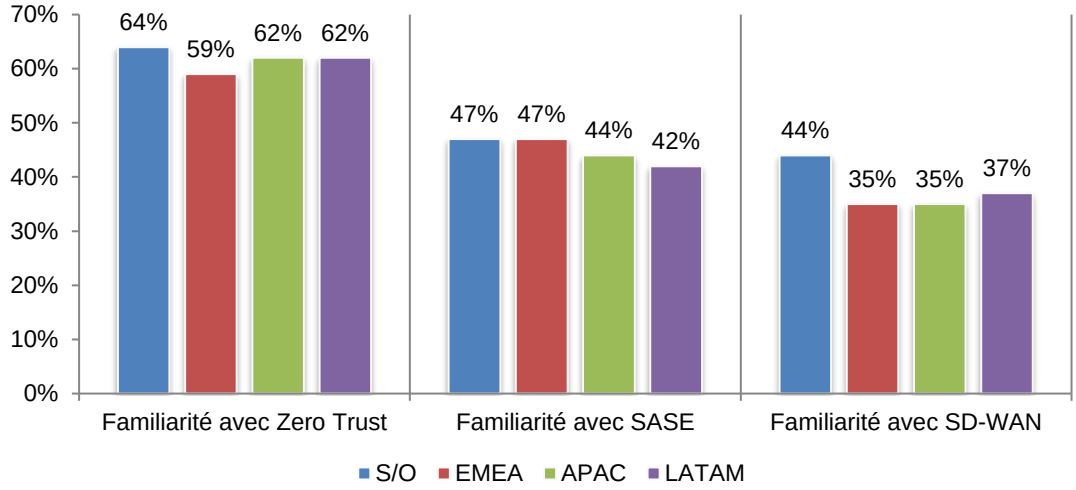


Différences régionales

Dans cette section, nous proposons une comparaison entre les quatre régions représentées dans cette recherche : Amérique du Nord (598 participants), EMEA (454 participants), Asie-Pacifique (402 participants) et LATAM (372 participants).

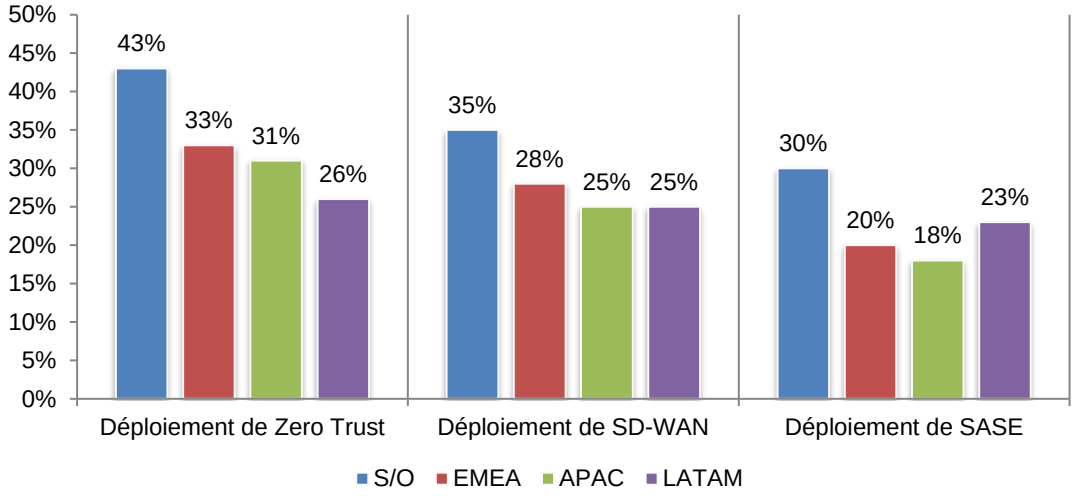
Au sein des régions, l'architecture de sécurité Zero Trust est plus connue que les architectures SD-WAN et SASE. Comme le montre la Figure 10, la plupart des participants sont familiers ou très familiers avec Zero Trust dans toutes les régions. Les participants des régions Amérique du Nord et EMEA sont légèrement plus familiers avec SASE que ceux des régions Asie-Pacifique ou LATAM. Les participants de la région Amérique du Nord sont plus familiers avec SD-WAN (44 % des participants).

Figure 10. Familiarité avec Zero Trust, SD-WAN et SASE
Réponses « Très familier » et « Familier » combinées



Le déploiement de Zero Trust, SD-WAN et SASE est plus élevé dans la région Amérique du Nord, comme l'indique la Figure 11.

Figure 11. Déploiement de Zero Trust, SD-WAN et SASE
Réponses « Déployé » et « Sera déployé dans 12 mois » combinées



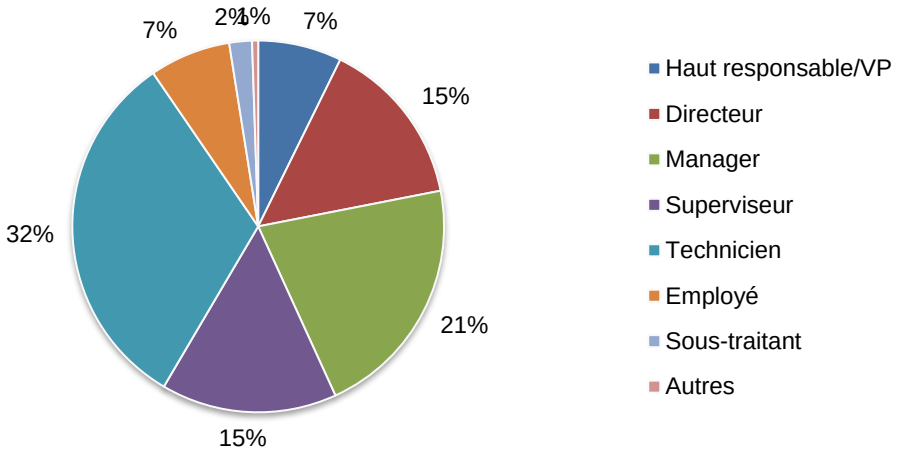
Partie 3. Méthodes

La base d'échantillonnage est composée de 51 248 informaticiens et professionnels de la sécurité dans les régions suivantes : Asie-Pacifique, EMEA, Amérique du Nord et LATAM. Comme le montre le Tableau 1, 2 040 personnes ont participé au sondage. Le filtrage a supprimé 214 sondages. Le dernier échantillon était composé de 1 826 sondages (soit un taux de réponse de 3,6 %).

Table 1. Exemple de réponse	Fréq	Pct%
Base d'échantillonnage totale	51 248	100,0 %
Total des résultats	2 040	3,9 %
Sondages rejetés ou filtrés	214	0,4 %
Échantillon final	1 826	3,6 %

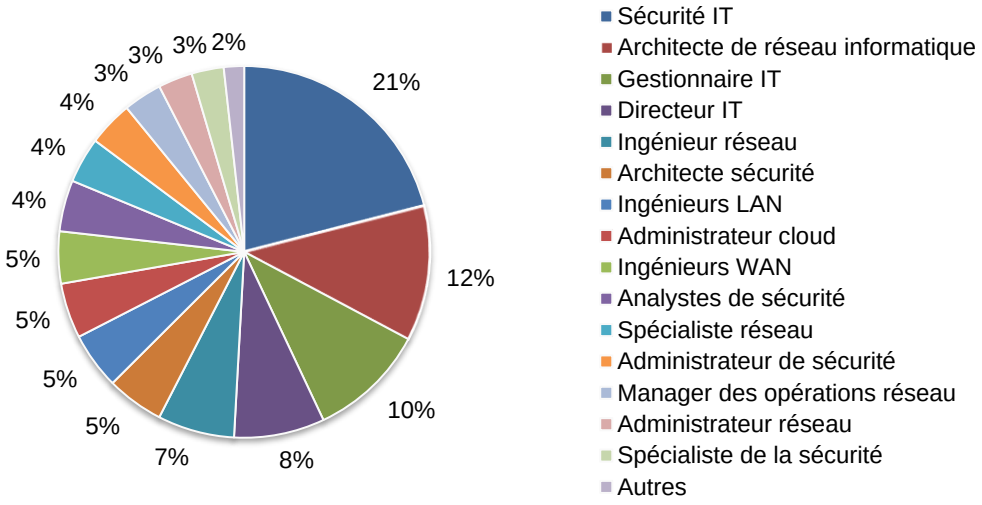
Le diagramme circulaire 1 indique le poste ou la fonction actuelle des participants au sein de leurs organisations. Cinquante-huit pour cent des participants ont déclaré qu'ils occupaient des postes de superviseurs ou des postes supérieurs alors que 32 % d'entre eux ont déclaré occuper des postes de techniciens.

Diagramme circulaire 1. Répartition des participants en fonction du niveau du poste



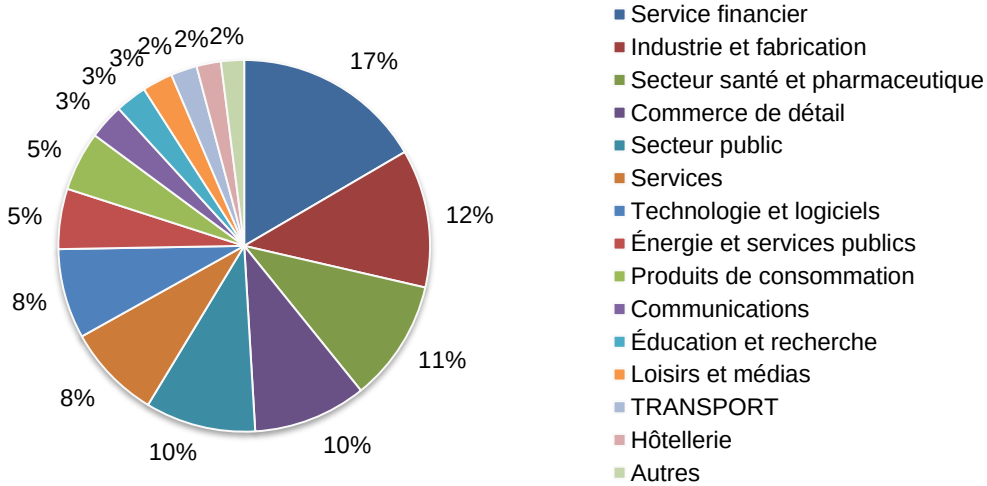
Le diagramme circulaire 2 identifie la fonction principale du participant. Vingt-et-un pour cent des participants ont indiqué qu'ils étaient des agents de sécurité IT, 12 % des architectes réseau, 10 % des responsables IT et 8 % des directeurs IT.

Diagramme circulaire 2. Répartition des participants en fonction du rôle principal au sein de l'organisation



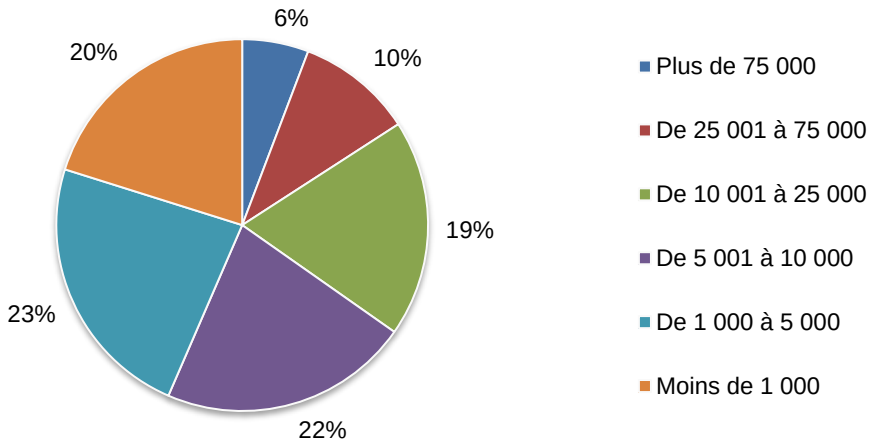
Le diagramme circulaire 3 indique la principale classification industrielle des organisations des participants. Ce graphique identifie les services financiers (17 % des participants) comme le segment le plus important, incluant les banques, l'assurance, le courtage, la gestion des investissements et le traitement des paiements. Suivent le secteur industriel/fabrication (12% des participants), le secteur santé et pharmaceutique (11% des participants), le secteur public et le secteur du détail (10% des participants chacun).

Diagramme circulaire 3. Répartition des participants en fonction de la classification principale au sein du secteur



D’après le diagramme circulaire 4, plus de la moitié (57 %) des participants appartiennent à des organisations de plus de 5 000 employés.

Diagramme circulaire 4. Répartition des participants en fonction du nombre d’employés au sein de l’organisation



Partie 4. Avertissements

Les résultats des sondages sont sujets à des limitations qui doivent être soigneusement prises en compte avant toute interprétation. Les éléments suivants font partie des limitations qui sont inhérentes à la plupart des sondages réalisés sur les sites Web.

Biais de non réponse : Les résultats actuels sont basés sur un échantillon des résultats des sondages. Nous avons envoyé des sondages à un échantillon représentatif de participants, ce qui s’est traduit par un grand nombre de réponses utilisables. Malgré les tests de non réponse, il est tout à fait possible que les non participants aient des avis très différents des personnes qui ont pris part aux sondages.

Biais d’échantillonnage : La précision dépend des informations de contact et de la mesure dans laquelle la liste est représentative des personnes qui sont des agents de sécurité informatique ou des professionnels de la mise en réseau dans diverses organisations des régions Asie-Pacifique, EMEA, Amérique du Nord et LATAM. Nous reconnaissons également que les résultats peuvent être biaisés par des événements extérieurs tels que la couverture médiatique. Nous reconnaissons enfin le biais occasionné par la compensation encourageant les participants à terminer cette recherche dans une période de temps bien définie.

Résultats auto déclarés : La qualité de la recherche est basée sur l’intégrité des réponses confidentielles reçues des participants. Bien qu’il soit possible d’intégrer un système de poids et contrepoids au processus du sondage, il est tout à fait possible qu’un participant n’ait pas fourni des réponses exactes.

Annexe : Résultats détaillés du sondage

Les tableaux suivants fournissent la fréquence ou la fréquence des pourcentages des réponses à toutes les questions contenues dans cette étude. Les réponses du sondage ont toutes été capturées en février 2021.

Réponse de sondage	S/O	EMEA	APAC	LATAM	Total
Base d'échantillonnage totale	16 248	12 445	11 891	10 664	51 248
Total des résultats	663	501	456	420	2 040
Sondages rejetés	65	47	54	48	214
Échantillon final	598	454	402	372	1 826
Taux de réponse	3,7 %	3,6 %	3,4 %	3,5 %	3,6 %
Pondérations d'échantillons	32,7 %	24,9 %	22,0 %	20,4 %	100,0 %

Partie 1. Filtrage

S1. Qu'est-ce qui décrit le mieux votre rôle au sein de votre organisation ?	S/O	EMEA	APAC	LATAM	Total
Je suis plutôt un professionnel de la sécurité	41 %	35 %	36 %	30 %	36 %
Je suis plutôt un professionnel des réseaux	27 %	37 %	39 %	42 %	35 %
Je suis un professionnel de la sécurité et des réseaux	32 %	28 %	25 %	28 %	29 %
Aucune des réponses ci-dessus (stop)	0 %	0 %	0 %	0 %	0 %
Total	100 %	100 %	100 %	100 %	100 %

Partie 2. Utilisation de SD-WAN, sécurité cloud, architecture SASE et architecture de sécurité Zero Trust

Q1. À quel point êtes-vous familier avec l'architecture de sécurité Zero Trust ?	S/O	EMEA	APAC	LATAM	Total
Très familier	34 %	30 %	28 %	27 %	30 %
Familier	30 %	29 %	34 %	35 %	32 %
Un peu familier	27 %	30 %	28 %	17 %	26 %
Pas familier	9 %	11 %	10 %	21 %	12 %
Total	100 %	100 %	100 %	100 %	100 %

Q2. Votre organisation a-t-elle déployé ou envisage-t-elle de déployer l'architecture de sécurité Zero Trust ?	S/O	EMEA	APAC	LATAM	Total
Oui, elle a été déployée	24 %	19 %	18 %	15 %	20 %
Oui, elle sera déployée dans les 12 prochains mois	19 %	14 %	13 %	11 %	15 %
Oui, mais aucun déploiement n'a été programmé	23 %	19 %	20 %	24 %	22 %
Ne sais pas si un déploiement est prévu	16 %	25 %	27 %	15 %	20 %
Pas de déploiement prévu	18 %	23 %	22 %	35 %	24 %
Total	100 %	100 %	100 %	100 %	100 %

Q3. À quel point êtes-vous familier avec les solutions SD-WAN ?	S/O	EMEA	APAC	LATAM	Total
Très familier	21 %	16 %	13 %	17 %	17 %
Familier	23 %	19 %	22 %	20 %	21 %
Un peu familier	32 %	23 %	30 %	33 %	30 %
Pas familier	24 %	42 %	35 %	30 %	32 %
Total	100 %	100 %	100 %	100 %	100 %

Q4. Votre organisation a-t-elle déployé ou envisage-t-elle de déployer les solutions SD-WAN ?	S/O	EMEA	APAC	LATAM	Total
Oui, elle a été déployée	15 %	9 %	11 %	8 %	11 %
Oui, elle sera déployée dans les 12 prochains mois	20 %	19 %	14 %	17 %	18 %
Oui, mais aucun déploiement n'a été programmé	11 %	20 %	23 %	14 %	16 %
Ne sais pas si un déploiement est prévu	18 %	12 %	19 %	16 %	16 %
Pas de déploiement prévu	36 %	40 %	33 %	45 %	38 %
Total	100 %	100 %	100 %	100 %	100 %

Q5. Qui a ou aura le plus d'influence sur le déploiement des solutions SD-WAN ?	S/O	EMEA	APAC	LATAM	Total
L'équipe de sécurité est chargée du déploiement et reçoit des conseils de l'équipe réseau	40 %	34 %	38 %	36 %	37 %
L'équipe réseau est chargée du déploiement et reçoit des conseils de l'équipe sécurité	45 %	47 %	50 %	42 %	46 %
L'équipe réseau prend les décisions relatives aux réseaux et l'équipe de sécurité les décisions relatives à la sécurité	15 %	19 %	12 %	22 %	17 %
Total	100 %	100 %	100 %	100 %	100 %

Q6. À quel point êtes-vous familier avec l'architecture de sécurité SASE ?	S/O	EMEA	APAC	LATAM	Total
Très familier	24 %	18 %	17 %	19 %	20 %
Familier	23 %	29 %	27 %	23 %	25 %
Un peu familier	30 %	28 %	25 %	28 %	28 %
Pas familier	23 %	25 %	31 %	30 %	27 %
Total	100 %	100 %	100 %	100 %	100 %

Q7. Votre organisation a-t-elle déployé ou envisage-t-elle de déployer l'architecture de sécurité SASE ?	S/O	EMEA	APAC	LATAM	Total
Oui, elle a été déployée	12 %	8 %	9 %	10 %	10 %
Oui, elle sera déployée dans les 12 prochains mois	18 %	12 %	9 %	13 %	14 %
Oui, mais aucun déploiement n'a été programmé	23 %	28 %	27 %	24 %	25 %
Ne sais pas si un déploiement est prévu	15 %	21 %	18 %	15 %	17 %
Pas de déploiement prévu	32 %	31 %	37 %	38 %	34 %
Total	100 %	100 %	100 %	100 %	100 %

Q8. Si votre organisation déploie la sécurité SD-WAN et cloud-pour une architecture SASE, comment les fournisseurs seront-ils sélectionnés ? Veuillez choisir une seule réponse.	S/O	EMEA	APAC	LATAM	Total
Recruter un fournisseur pour la sécurité SD-WAN et cloud	29 %	28 %	31 %	30 %	29 %
Recruter des fournisseurs réseau intégrés à des fournisseurs de sécurité cloud de pointe	23 %	27 %	25 %	19 %	24 %
Recruter un fournisseur SD-WAN de pointe offrant des intégrations à des fournisseurs de sécurité cloud	25 %	24 %	18 %	17 %	22 %
Recruter un ou des fournisseurs de sécurité cloud de pointe offrant une intégration avec les fournisseurs SD-WAN	23 %	21 %	26 %	34 %	25 %
Total	100 %	100 %	100 %	100 %	100 %

Q9. Qui prend les décisions concernant l'architecture/les produits de solutions de sécurité ?	S/O	EMEA	APAC	LATAM	Total
L'équipe réseau	40 %	48 %	38 %	42 %	42 %
L'équipe de sécurité	33 %	29 %	33 %	27 %	31 %
L'équipe réseau et l'équipe de sécurité	27 %	23 %	29 %	31 %	27 %
Total	100 %	100 %	100 %	100 %	100 %

Q10. Comment sont prises les décisions relatives aux fournisseurs lors de la mise en œuvre des services de sécurité cloud (par exemple pare-feu cloud en tant que service, agent de sécurité des accès au cloud, etc.) ? Veuillez choisir la réponse la plus pertinente	S/O	EMEA	APAC	LATAM	Total
Notre organisation utiliserait des fournisseurs indépendants de pointe qui se consacrent à ces solutions	47 %	41 %	43 %	45 %	44 %
Notre organisation utiliserait notre fournisseur réseau	23 %	26 %	28 %	22 %	25 %
Notre organisation utiliserait des fournisseurs de sécurité offrant ces services dans le cadre d'un portefeuille de sécurité plus large	30 %	33 %	29 %	33 %	31 %
Total	100 %	100 %	100 %	100 %	100 %

Q11. À quel point votre organisation est-elle confiante de l'efficacité de son architecture de sécurité et de sa mise en œuvre (1 = pas confiante à 10 = très confiante ?	S/O	EMEA	APAC	LATAM	Total
1 ou 2	5 %	8 %	11 %	9 %	8 %
3 ou 4	15 %	6 %	8 %	13 %	11 %
5 ou 6	25 %	15 %	8 %	25 %	19 %
7 ou 8	33 %	36 %	35 %	34 %	34 %
9 ou 10	22 %	35 %	38 %	19 %	28 %
Total	100 %	100 %	100 %	100 %	100 %
Valeur extrapolée	6,54	7,18	7,12	6,32	6,78

Q12. Pensez-vous qu'un seul fournisseur puisse répondre à tous vos **besoins en matière de sécurité** ?	S/O	EMEA	APAC	LATAM	Total
Oui	68 %	64 %	59 %	57 %	63 %
Non	27 %	30 %	37 %	36 %	32 %
Pas sûr	5 %	6 %	4 %	7 %	5 %
Total	100 %	100 %	100 %	100 %	100 %

Q13. Pensez-vous qu'un seul fournisseur puisse répondre à tous vos **besoins en matière de réseau** ?	S/O	EMEA	APAC	LATAM	Total
Oui	48 %	45 %	41 %	39 %	44 %
Non	45 %	47 %	53 %	55 %	49 %
Pas sûr	7 %	8 %	6 %	6 %	7 %
Total	100 %	100 %	100 %	100 %	100 %

Q14. Pensez-vous qu'un seul fournisseur puisse répondre à tous vos **besoins en matière de sécurité et réseau** ?	S/O	EMEA	APAC	LATAM	Total
Oui	57 %	52 %	50 %	47 %	52 %
Non	35 %	42 %	43 %	45 %	41 %
Pas sûr	8 %	6 %	7 %	8 %	7 %
Total	100 %	100 %	100 %	100 %	100 %

Partie 3. Votre rôle et vos caractéristiques organisationnelles

D1. Quel niveau correspond le mieux à votre poste actuel au sein de votre organisation ?	S/O	EMEA	APAC	LATAM	Total
Haut responsable/VP	8 %	6 %	7 %	8 %	7 %
Directeur	16 %	14 %	13 %	15 %	15 %
Manager	21 %	23 %	19 %	22 %	21 %
Superviseur	15 %	17 %	15 %	14 %	15 %
Technicien	30 %	31 %	35 %	33 %	32 %
Employé	7 %	8 %	8 %	5 %	7 %
Sous-traitant	2 %	1 %	3 %	2 %	2 %
Autres	1 %	0 %	0 %	1 %	1 %
Total	100 %	100 %	100 %	100 %	100 %

D2. Qu'est-ce qui décrit le mieux votre rôle principal au sein de l'organisation ?	S/O	EMEA	APAC	LATAM	Total
Administrateur cloud	5 %	6 %	3 %	5 %	5 %
Responsable de la protection des données	0 %	0 %	0 %	0 %	0 %
Directeur IT	7 %	8 %	9 %	8 %	8 %
Gestionnaire IT	11 %	8 %	9 %	13 %	10 %
Architecte de réseau informatique	12 %	10 %	13 %	12 %	12 %
Sécurité IT	20 %	19 %	23 %	23 %	21 %
Ingénieurs LAN	5 %	3 %	6 %	6 %	5 %
Administrateur réseau	3 %	3 %	2 %	4 %	3 %
Ingénieur réseau	6 %	7 %	8 %	6 %	7 %
Manager des opérations réseau	4 %	3 %	4 %	2 %	3 %
Spécialiste réseau	3 %	6 %	4 %	3 %	4 %
Administrateur de sécurité	5 %	3 %	5 %	2 %	4 %
Analystes de sécurité	6 %	5 %	2 %	4 %	4 %
Architecte sécurité	4 %	8 %	3 %	5 %	5 %
Spécialiste de la sécurité	3 %	3 %	3 %	2 %	3 %
Ingénieurs WAN	4 %	7 %	3 %	4 %	5 %
Autre (veuillez préciser)	2 %	1 %	3 %	1 %	2 %
Total	100 %	100 %	100 %	100 %	100 %

D3. Quel secteur décrit le mieux l'intérêt de votre organisation ?	S/O	EMEA	APAC	LATAM	Total
Agriculture et service de restauration	1 %	1 %	1 %	1 %	1 %
Communications	3 %	2 %	4 %	3 %	3 %
Produits de consommation	5 %	5 %	5 %	6 %	5 %
Défense et aérospatial	1 %	1 %	2 %	1 %	1 %
Éducation et recherche	2 %	2 %	4 %	3 %	3 %
Énergie et services publics	5 %	5 %	6 %	5 %	5 %
Loisirs et médias	2 %	2 %	3 %	4 %	3 %
Service financier	18 %	15 %	17 %	15 %	17 %
Secteur santé et pharmaceutique	11 %	12 %	9 %	10 %	11 %
Hôtellerie	2 %	2 %	2 %	3 %	2 %
Industrie et fabrication	12 %	15 %	11 %	10 %	12 %
Secteur public	9 %	10 %	9 %	11 %	10 %
Commerce de détail	10 %	10 %	9 %	10 %	10 %
Services	9 %	9 %	8 %	7 %	8 %
Technologie et logiciels	8 %	8 %	8 %	7 %	8 %
TRANSPORT	2 %	2 %	2 %	3 %	2 %
Autres	0 %	0 %	0 %	0 %	0 %
Total	100 %	100 %	100 %	100 %	100 %

D4. Quelle plage correspond le mieux au nombre d'employés à plein temps au sein de votre organisation ?	S/O	EMEA	APAC	LATAM	Total
Moins de 1 000	18 %	24 %	21 %	18 %	20 %
De 1 000 à 5 000	20 %	25 %	24 %	26 %	23 %
De 5 001 à 10 000	19 %	20 %	23 %	27 %	22 %
De 10 001 à 25 000	22 %	17 %	19 %	16 %	19 %
De 25 001 à 75 000	13 %	9 %	8 %	9 %	10 %
Plus de 75 000	8 %	5 %	5 %	4 %	6 %
Total	100 %	100 %	100 %	100 %	100 %

Pour toute question, veuillez contacter research@ponemon.org ou nous appeler au +1 800 887 3118.

Ponemon Institute

Encourager la gestion responsable des informations

Le Ponemon Institute est dédié à la recherche indépendante et à l'éducation qui encouragent les pratiques de gestion responsables des informations et de la confidentialité au sein de l'entreprise et du gouvernement. Notre mission consiste à mener des études empiriques de haute qualité sur les problèmes qui affectent la gestion et la sécurité des informations sensibles des personnes et des organisations.

En tant que membres d'**Insights Association**, nous nous conformons aux strictes normes qui régissent la confidentialité des données, la vie privée et la recherche éthique. Nous ne collectons pas d'informations personnellement identifiables auprès d'autres personnes (ou des informations pouvant identifier des entreprises dans nos recherches commerciales). En outre, nous adhérons à des normes de qualité strictes qui nous permettent de veiller à ce que les participants n'aient pas à répondre à des questions hors sujet, non pertinentes ou déplacées.