Enterprise Strategy Group™ by TechTarget

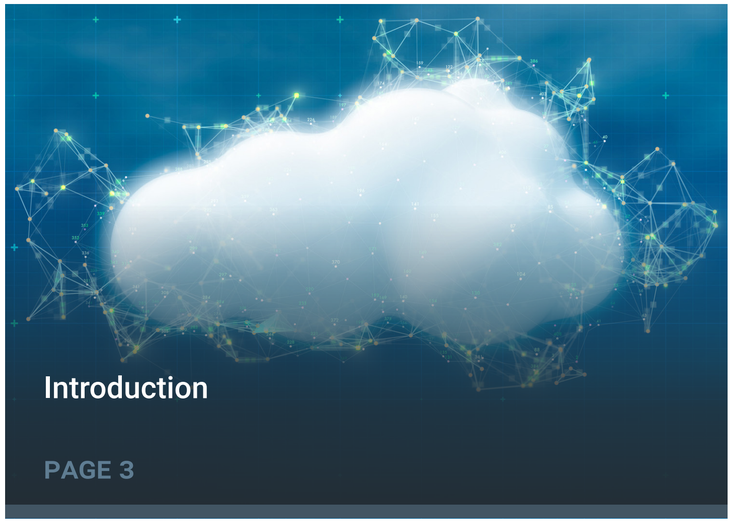
L’état de la gestion hybride et multi-cloud en Europe :

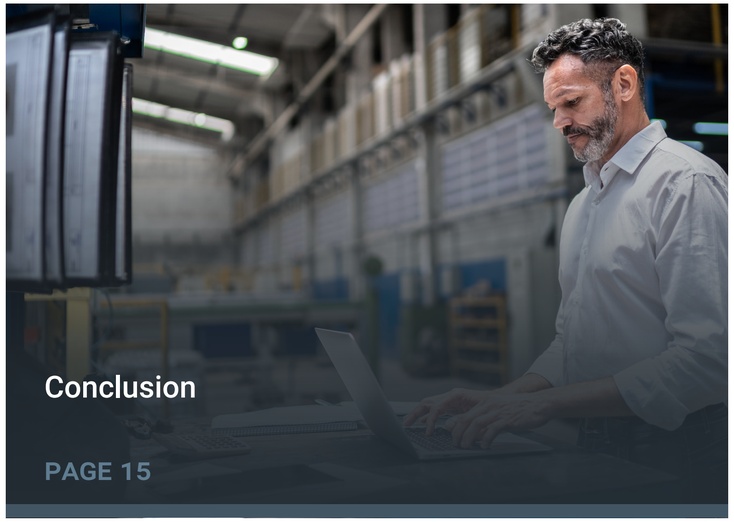
Où sont les lacunes et pourquoi il est essentiel d'améliorer

infoblox

Cet eBook d’Enterprise Strategy Group a été commandé par Infoblox et est distribué sous licence par TechTarget, Inc.

LE SOMMAIRE





« Il existe **des mesures spécifiques et réalisables que chaque organisation peut mettre en œuvre** pour améliorer ses opérations hybrides et multi-cloud et les résultats commerciaux associés. »

Introduction

Les objectifs

Une étude de marché primaire récemment réalisée par TechTarget's Enterprise Strategy Group et Infoblox a confirmé qu'il existe des mesures spécifiques et réalisables que chaque organisation peut mettre en œuvre pour améliorer ses opérations hybrides et multi-cloud et ses résultats commerciaux associés.

L'objectif de cet eBook est d'examiner plus en profondeur comment les réponses des individus et des organisations en Europe se comparent à celles de leurs homologues dans le reste du monde. Nous cherchons également à comprendre si les avantages de devenir un leader hybride et multi-cloud sont aussi marqués en Europe en comparant ces organisations leaders à leurs homologues moins matures dans la région.

Principales conclusions

Les organisations en Europe dont les opérations hybrides et multi-cloud sont plus matures, surpassent nettement leurs homologues :

Les leaders sont plus efficaces : ils ont réduit les coûts liés au cloud de 50 % de plus que les organisations émergentes au cours de l'année dernière grâce à une meilleure gestion.

Les leaders commercialisent leurs produits plus rapidement : 76 % se disent généralement les premiers à entrer sur leurs marchés, contre seulement 12 % des organisations naissantes.

Les leaders satisfont les utilisateurs du cloud : en ce qui concerne les charges de travail hébergées dans le cloud, ils sont 2,9 fois plus susceptibles de dépasser leurs objectifs de satisfaction de leurs employés (61 % contre 21 %) et 2,3 fois plus susceptibles de dépasser leurs objectifs de satisfaction de leurs clients (58 % contre 25 %).

Comment les organisations européennes se distinguent de leurs homologues en matière de maturité hybride et multi-cloud

L'état actuel de la maturité de la gestion hybride et multi-cloud

Pour évaluer l'état du marché, Enterprise Strategy Group a créé une enquête axée sur les personnes, les processus et les technologies en place permettant aux organisations de gérer leurs environnements cloud. Les réponses à ces questions ont permis à Enterprise Strategy Group de déterminer le degré d'alignement de toutes les organisations participantes sur un éventail de bonnes pratiques. Les organisations les plus matures sont désignées comme Leaders, suivies par *Convergentes, Émergentes* et *Naissantes.*

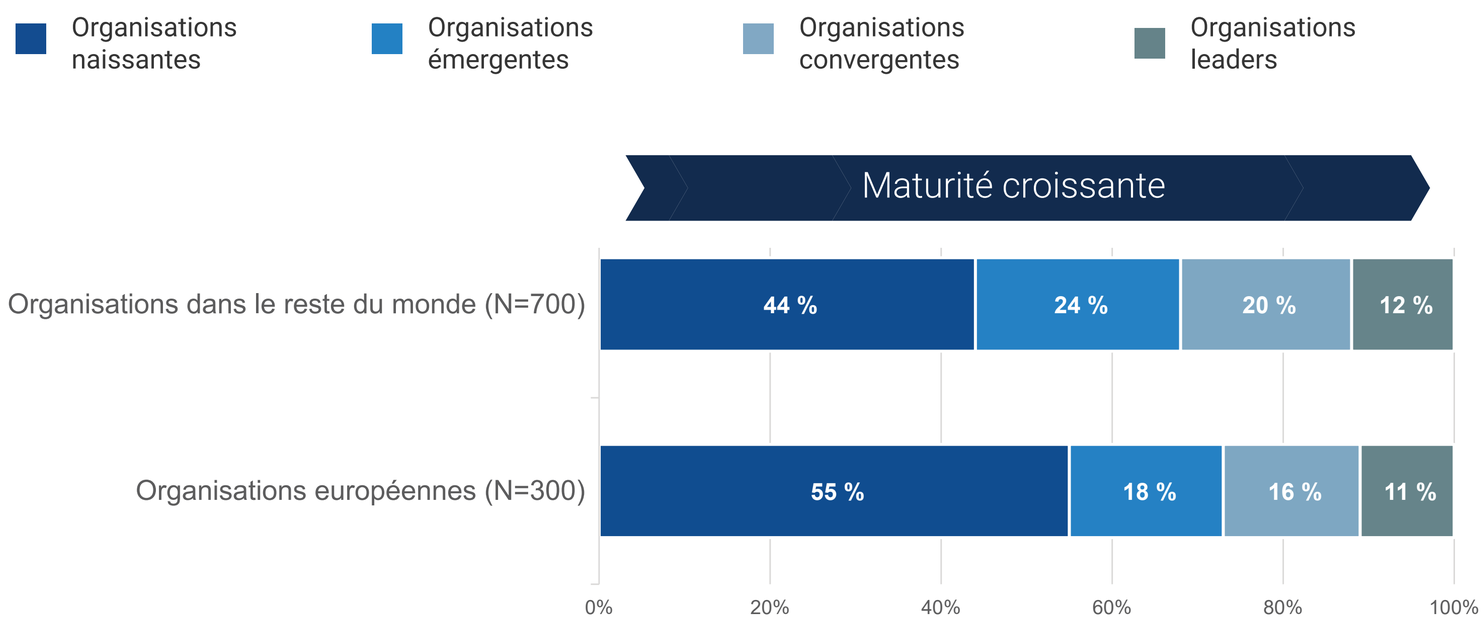
L'analyse d'Enterprise Strategy Group a utilisé un système de notation par points dans lequel les organisations ont été évaluées selon la présence (ou l'absence) d'attributs et de pratiques de gestion mature du cloud. Des points de maturité leur étaient ensuite accordés ou non, dans une limite maximale de 105 points.

Les attributs et pratiques évalués comprennent :

- L'organisation a-t-elle mis en place une équipe transverse chargée de la plateforme cloud, composée de spécialistes du réseau, de la sécurité et de l'exploitation du cloud ?
- L'organisation exploite-t-elle des solutions de mise en réseau de niveau entreprise et adaptables au différents types de cloud ?
- L'organisation adopte-t-elle une approche de défense en profondeur des solutions de sécurité, y compris l'utilisation du DNS pour un large éventail de cas d'utilisation liés à la sécurité ?
- L'entreprise automatise-t-elle intelligemment un large éventail de flux de travail NetOps et SecOps dans le cloud ?

La comparaison du niveau de maturité des organisations en Europe par rapport au reste du monde montre que, bien qu'il y ait un certain degré de cohérence à travers le monde, les organisations européennes sont bien plus susceptibles d'être dans la cohorte la moins mature (55 % contre 44 %), ce qui signifie que le degré de maturité hybride et multi-cloud des organisations européennes est, dans l'ensemble, plus faible.

Les organisations par maturité de gestion hybride et multi-cloud.



RETOUR AU SOMMAIRE

Qu'est-ce qui distingue une organisation leader hybride et multicloud de ses homologues ?

Le modèle de maturité hybride et multicloud d'Enterprise Strategy Group comporte de multiples facettes, couvrant les personnes, les processus et les technologies. Nous résumons ci-dessous les principales différences entre les organisations leaders et les autres cohortes de maturité :

Mise en place d'une équipe convergente chargée de la plateforme cloud :
La convergence du réseau et de la sécurité au sein du centre d'excellence des opérations cloud d'une organisation peut apporter des avantages significatifs en matière d'efficacité, d'agilité et de sécurité. En éliminant les silos traditionnels entre ces deux équipes, l'organisation peut favoriser une meilleure collaboration et un meilleur alignement des objectifs, ce qui permet de rationaliser les processus et d'accélérer la prise de décision. Dans le contexte du modèle de maturité, les questions permettant d'évaluer les progrès d'une organisation comprennent les mesures spécifiques prises pour faire converger les équipes, comme la création de rôles hybrides couvrant ces disciplines ou l'augmentation de la fréquence de la collaboration, la propension de l'organisation à déployer des outils communs utilisés par ces deux équipes, et la mise en place d'une équipe transverse d'ingénierie de cloud ou de plateforme axée sur la satisfaction des exigences de l'organisation en matière d'évolutivité, de fiabilité, de sécurité et de performance dans les environnements cloud.

Utilisation de solutions de mise en réseau d'entreprise adaptables à différents types de cloud :
Ces solutions, telles que les DNS, DHCP et IPAM (DDI) fournis par des tiers, offrent des capacités de gestion robustes, permettant un provisionnement, une allocation et un suivi efficaces des ressources réseau dans des environnements cloud dynamiques. En tirant parti d'outils conçus pour les opérations multicloud, par opposition aux outils fournis par les fournisseurs de services cloud (CSP) qui ne fonctionnent que sur l'infrastructure d'un seul fournisseur, les organisations peuvent renforcer la cohérence entre les clouds et gagner en agilité, en fiabilité et en performances. Les capacités de gestion centralisée et de reporting fournies par ces solutions offrent une meilleure visibilité et un meilleur contrôle de l'infrastructure réseau, simplifiant ainsi les efforts de conformité et réduisant les frais opérationnels.

Adoption d'une approche de défense en profondeur des solutions de sécurité cloud :
Le modèle de maturité préconise qu'une organisation ne dépende pas uniquement des outils de sécurité et de surveillance mis à disposition par les fournisseurs IaaS. En effet, chaque organisation a ses propres politiques de sécurité, obligations réglementaires et/ou normes de gouvernance différentes qui peuvent nécessiter des mesures de sécurité supplémentaires allant au-delà de ce que proposent les fournisseurs de services cloud. En particulier, l'utilisation du DNS dans un éventail de cas d'utilisation liés à la sécurité (comme l'application de politiques d'utilisation acceptables, la détection et le blocage de malwares, l'examen des incidents ou la traque des menaces) est un attribut organisationnel récompensé dans le modèle de maturité.

Automatisation des flux de travail NetOps et SecOps dans le cloud :
L'automatisation accroît l'efficacité opérationnelle en réduisant les efforts manuels et les erreurs humaines, ce qui permet aux organisations de déployer, de gérer et de faire évoluer l'infrastructure réseau et les services de sécurité plus rapidement et de manière plus cohérente. Cette agilité permet de répondre plus vite à l'évolution des besoins et des menaces de sécurité, et améliore également la productivité, tant au sein des équipes techniques que pour les parties prenantes telles que les développeurs.

Ensemble, ces quatre attributs organisationnels déterminent la position d'une organisation donnée sur le modèle de maturité hybride et multi-cloud. Les organisations qui cherchent à accroître leur niveau de maturité doivent avant tout s'efforcer de s'aligner davantage sur ces principes.

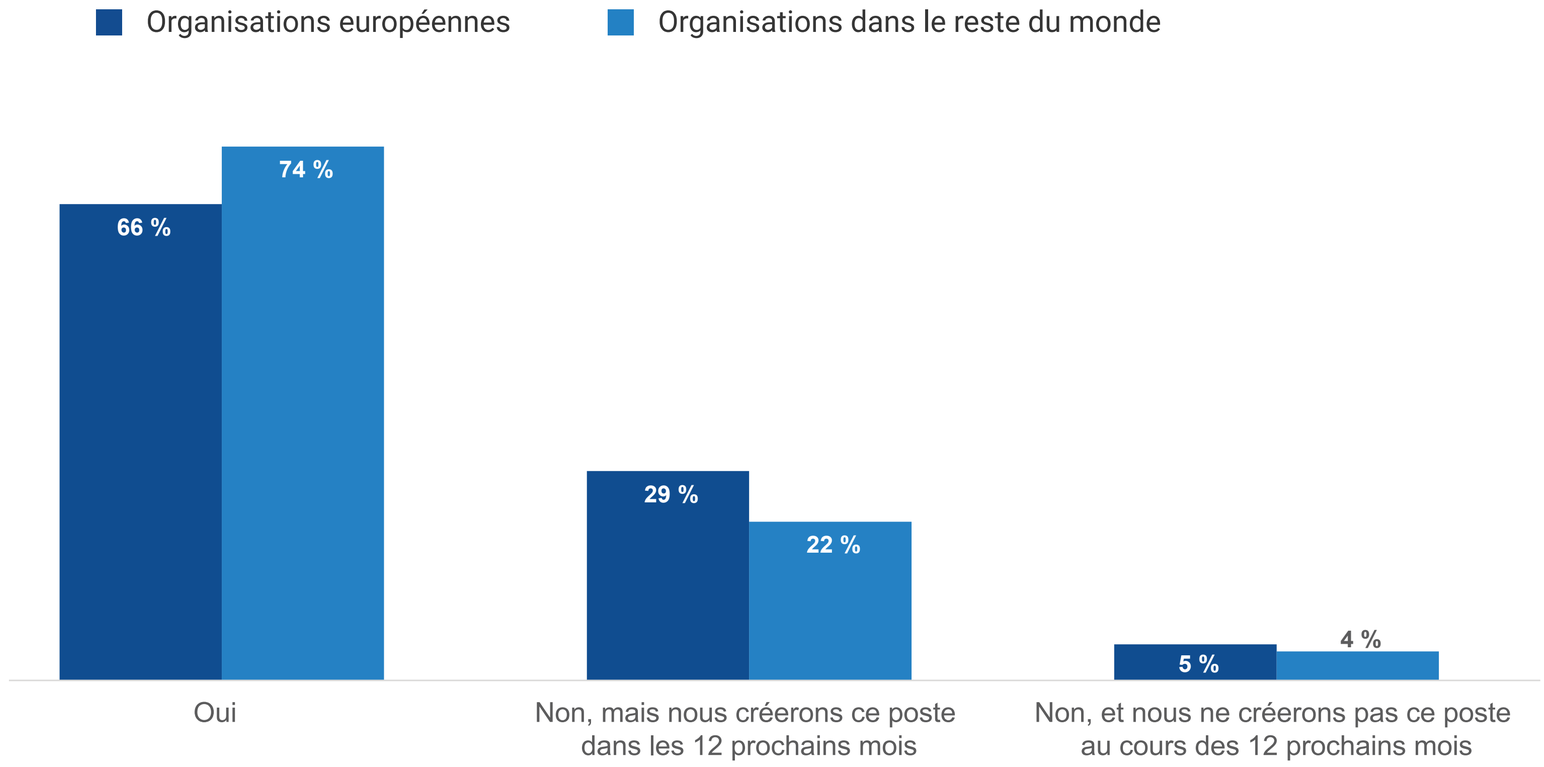
RETOUR AU SOMMAIRE

Les organisations européennes sont à la traîne dans leur transition vers l'ingénierie de plateforme

Les organisations dotées de topologies d'équipes d'ingénierie de plateforme obtiennent de meilleurs résultats dans le modèle de maturité, car elles tendent à promouvoir un environnement de développement plus rationalisé et plus évolutif. Les équipes d'ingénierie de plateforme cherchent à garantir un degré plus élevé de standardisation et d'automatisation des opérations cloud. Elles se concentrent sur la mise en œuvre des bonnes pratiques en matière de sécurité, de configuration réseau, de conformité et d'optimisation des performances de manière uniforme au sein de l'organisation, afin de créer des environnements cloud plus cohérents et plus fiables. Résultat : les équipes de développement et de production voient leur charge de travail réduite, ce qui leur permet de se consacrer à la livraison de fonctionnalités et d'innovations.

Comparées à leurs homologues des autres régions étudiées, les organisations européennes étaient moins susceptibles de déclarer employer actuellement des ingénieurs de plateforme (66 % contre 74 %). Sur une note positive, ces mêmes organisations étaient plus susceptibles de signaler la création de ces postes au sein de leur organisation au cours des 12 prochains mois (29 % contre 22 %), ce qui signifie que la région dans son ensemble est sur le point de rattraper la référence mondiale.

Votre organisation emploie-t-elle des collaborateurs à temps plein qui sont pleinement dédiés à l'ingénierie de plateforme ?



RETOUR AU SOMMAIRE

Les organisations européennes sont à la traîne par rapport à leurs homologues en matière de sécurité et de convergence des outils de mise en réseau

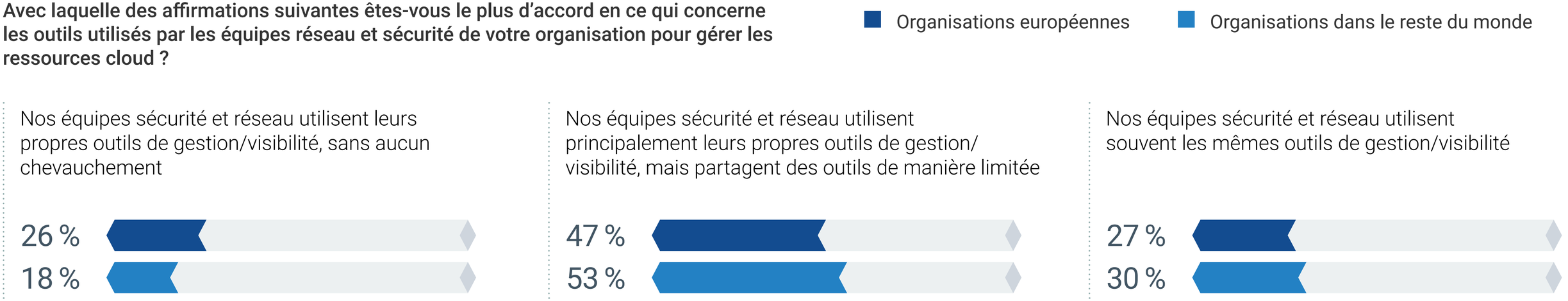
La convergence représente un domaine critique dans le modèle de maturité. Une équipe de plateforme centralisée en constitue l'un des aspects, l'autre étant la convergence des outils.

Lorsque les équipes chargées du réseau et de la sécurité utilisent un ensemble d'outils commun, cela simplifie la communication et la coordination, ce qui leur permet de collaborer plus facilement. Cette convergence permet également d'éviter les failles de sécurité qui peuvent résulter de l'utilisation d'outils et de processus disparates. En outre, l'utilisation d'outils communs permet également de rationaliser la réponse aux incidents et le dépannage, car toutes les équipes ont une vue cohérente de l'infrastructure de l'organisation.

Une fois de plus, les organisations européennes ont tendance à adopter une approche moins mature en ce qui concerne la convergence des outils de mise en réseau et de sécurité. Par rapport à leurs homologues des autres régions, elles étaient 44 % plus susceptibles d'adopter une approche complètement cloisonnée (26 % contre 18 %).

Les entreprises européennes seraient bien avisées de se demander s'il existe, dans leur environnement, des opportunités pour améliorer la cohérence des outils au sein de leurs équipes chargées des opérations cloud.

Avec laquelle des affirmations suivantes êtes-vous le plus d'accord en ce qui concerne les outils utilisés par les équipes réseau et sécurité de votre organisation pour gérer les ressources cloud ?



RETOUR AU SOMMAIRE

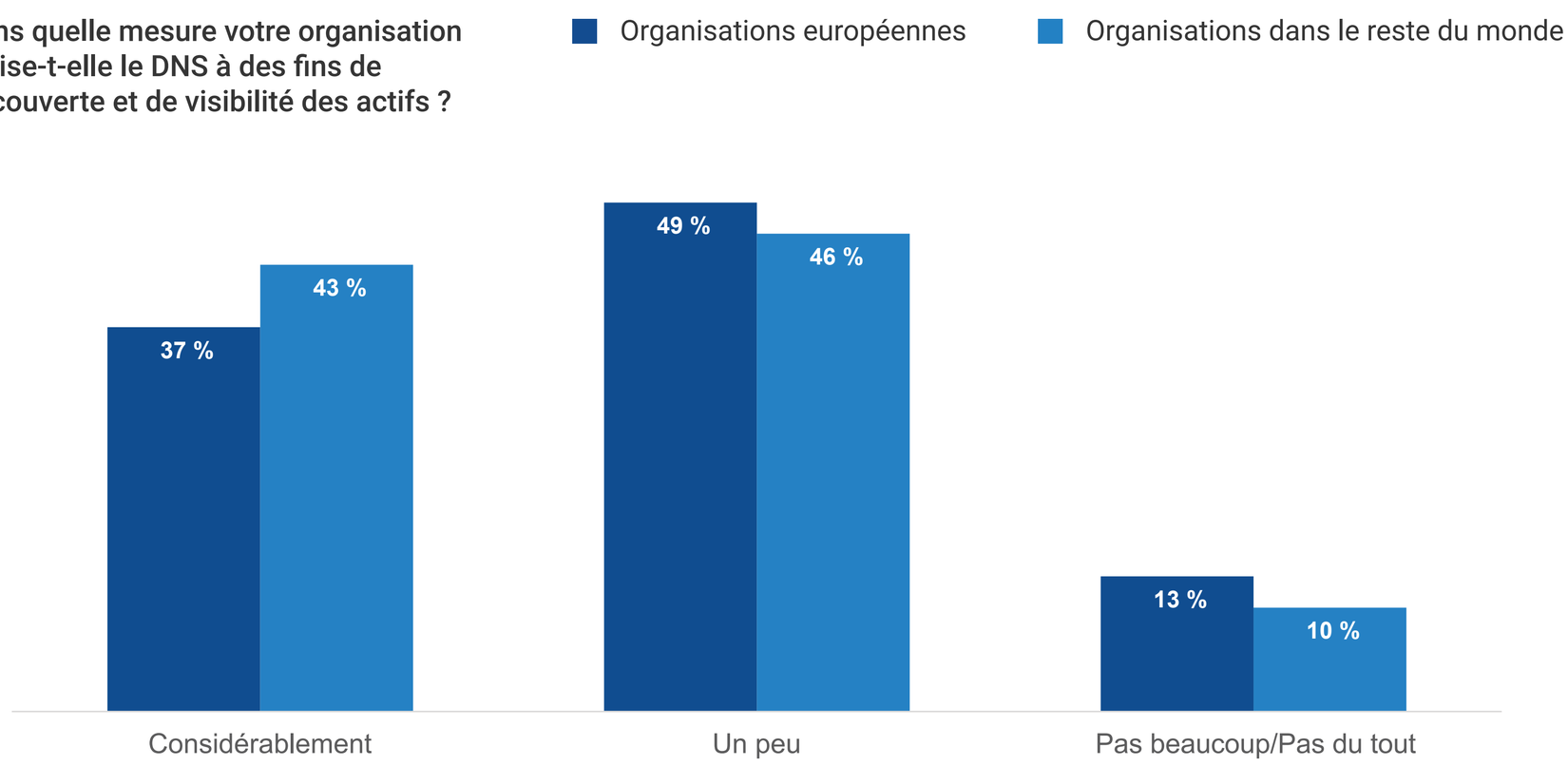
Les organisations européennes n'exploitent pas autant le DNS à des fins de découverte d'actifs que leurs homologues

L'intégration du DNS en tant que contrôle de sécurité primaire est une stratégie de cybersécurité logique en raison de son potentiel à contrecarrer un large éventail de menaces. En exploitant le DNS dans des cas d'utilisation liés à la sécurité, les entreprises peuvent détecter et bloquer efficacement les activités malveillantes au niveau du périmètre du réseau, notamment les infections par malware, les tentatives d'exfiltration de données et les attaques par phishing.

Les données montrent que les organisations européennes utilisent moins souvent le DNS de manière intensive à des fins de découverte et de visibilité des actifs cloud. L'utilisation du DNS pour la découverte de l'infrastructure permet aux équipes chargées de la sécurité d'identifier automatiquement tous les appareils et services actifs dans l'environnement cloud. La découverte basée sur le DNS permet d'identifier les dispositifs non autorisés ou indésirables qui peuvent présenter des risques de sécurité, ce qui permet de les isoler et de les atténuer plus rapidement. De même, elle facilite une meilleure surveillance des modèles de trafic et du comportement des utilisateurs, ce qui permet de détecter les activités suspectes telles que les mouvements latéraux des attaquants au sein du réseau. Les organisations européennes devraient se demander si elles utilisent pleinement le DNS pour optimiser les opérations de sécurité.

« La découverte basée sur le DNS aide à **identifier les dispositifs non autorisés ou indésirables susceptibles de présenter des risques de sécurité,** ce qui permet de les isoler et de les atténuer plus rapidement. »

Dans quelle mesure votre organisation utilise-t-elle le DNS à des fins de découverte et de visibilité des actifs ?



RETOUR AU SOMMAIRE

Pourquoi les entreprises européennes devraient se concentrer sur l’amélioration de leur maturité hybride et multicloud

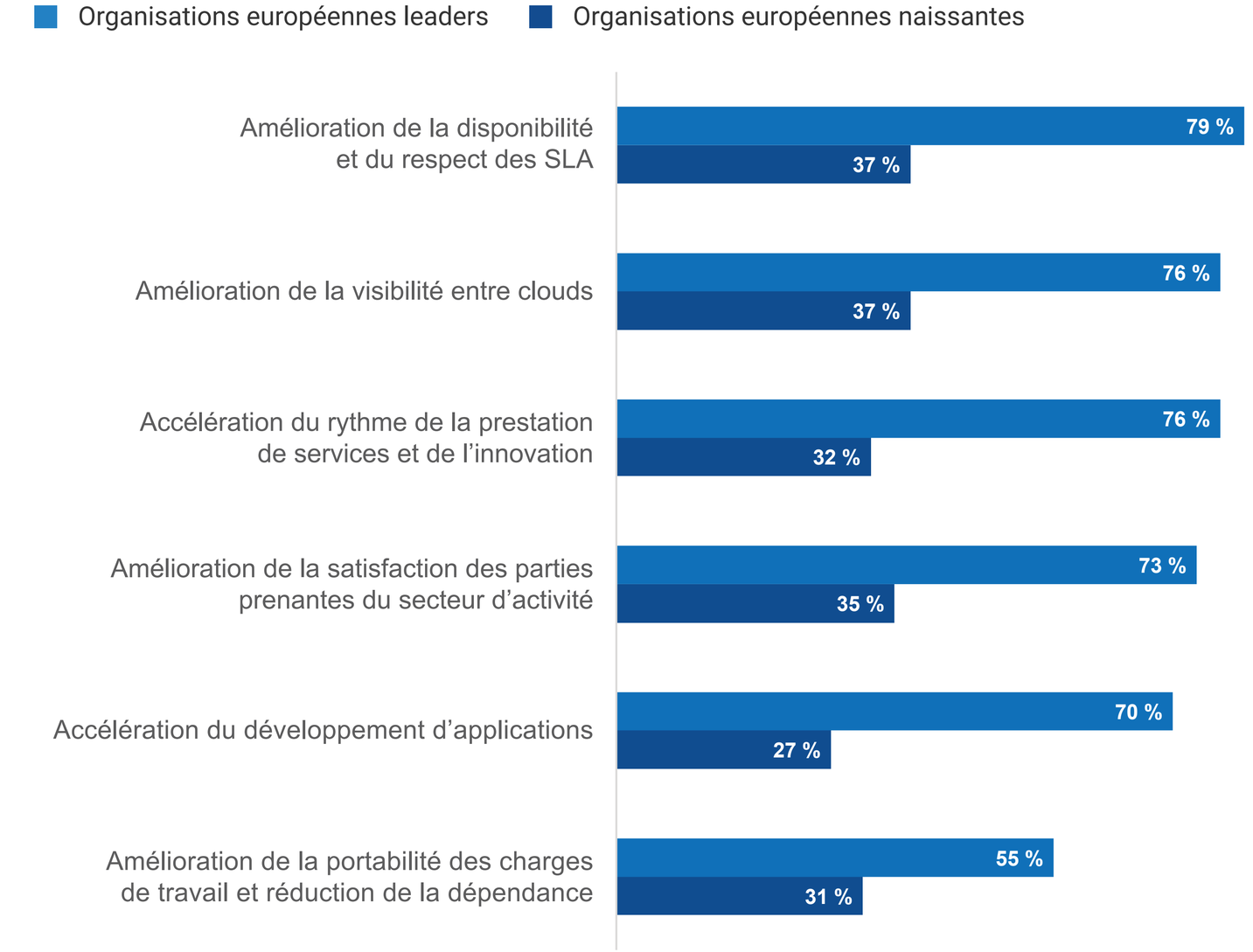
Les investissements technologiques des organisations leaders sont plus rentables

Dans le cadre de l'étude, il a été demandé aux personnes sondées si l'approche de leur organisation en matière de mise en réseau cloud et de technologies de sécurité améliorait considérablement les résultats ITOps et SecOps dans le cloud.

Les personnes sondées pouvaient répondre selon différents degrés, de « oui, de façon significative » à « pas du tout ». Lorsque le modèle de maturité est appliqué aux réponses à cette question, il devient rapidement évident que les organisations leaders en Europe tirent beaucoup plus de bénéfices de leurs investissements technologiques que leurs homologues dans la meme région. Plus précisément, elles déclarent plus souvent que leur approche du réseau cloud et de la technologie de sécurité permet de façon significative :

- L'amélioration de la disponibilité et du respect des SLA (79 % contre 37 % des organisations naissantes).
- L'amélioration de la visibilité sur tous les clouds (76 % contre 37 %).
- L'augmentation du rythme de la prestation de services et de l'innovation (76 % contre 32 %).
- L'amélioration de la satisfaction des parties prenantes des secteurs d'activité (73 % contre 35 %).
- L'accélération du développement des applications (70 % contre 27 %).
- Faciliter une meilleure portabilité des charges de travail et réduire la dépendance (55 % contre 31 %).

Le pourcentage des des personnes sondées déclarant que leurs solutions d'identité contribuent de manière significative à chaque bénéfice.



RETOUR AU SOMMAIRE

Une inspection plus approfondie des résultats du développement d'applications

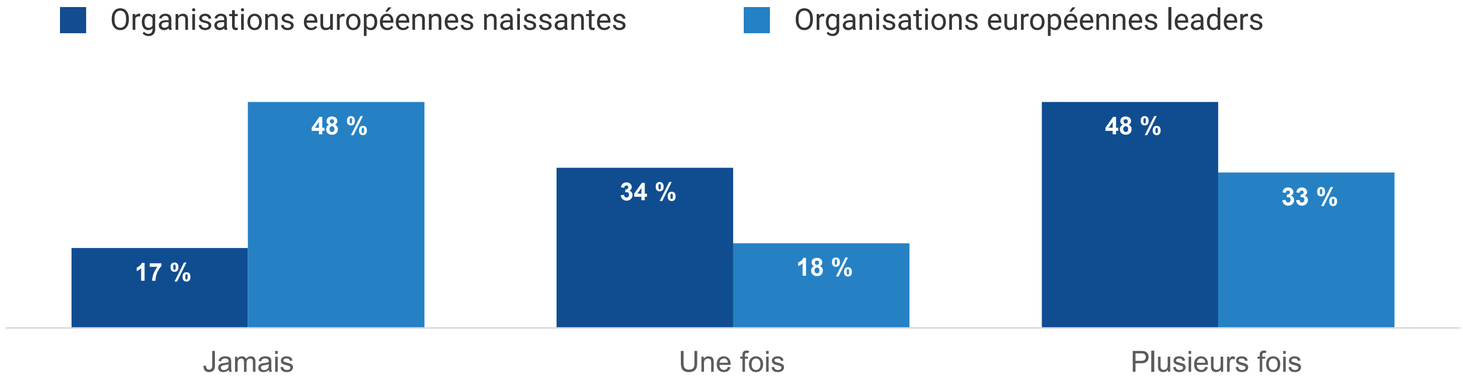
Non seulement les personnes sondées dans les organisations européennes leaders ont déclaré que leurs solutions de sécurité et de mise en réseau cloud contribuaient à améliorer les résultats du développement d'applications, mais leurs résultats étaient également *objectivement supérieurs* à ceux de leurs homologues moins matures dans la région.

Il a été demandé aux personnes sondées combien de fois, au cours de l'année écoulée, un projet de développement d'application avait été retardé parce que l'équipe informatique ou de sécurité avait besoin de plus de temps pour inspecter les services cloud sur lesquels reposait le projet. 48 % des organisations leaders européennes ont déclaré n'avoir jamais retardé ou interrompu l'avancement de l'équipe de développement sur de nouvelles applications ou fonctionnalités parce que l'équipe informatique ou de sécurité avait besoin de plus de temps pour inspecter les services cloud utilisés. Seules 17 % des organisations naissantes pouvaient en dire autant.

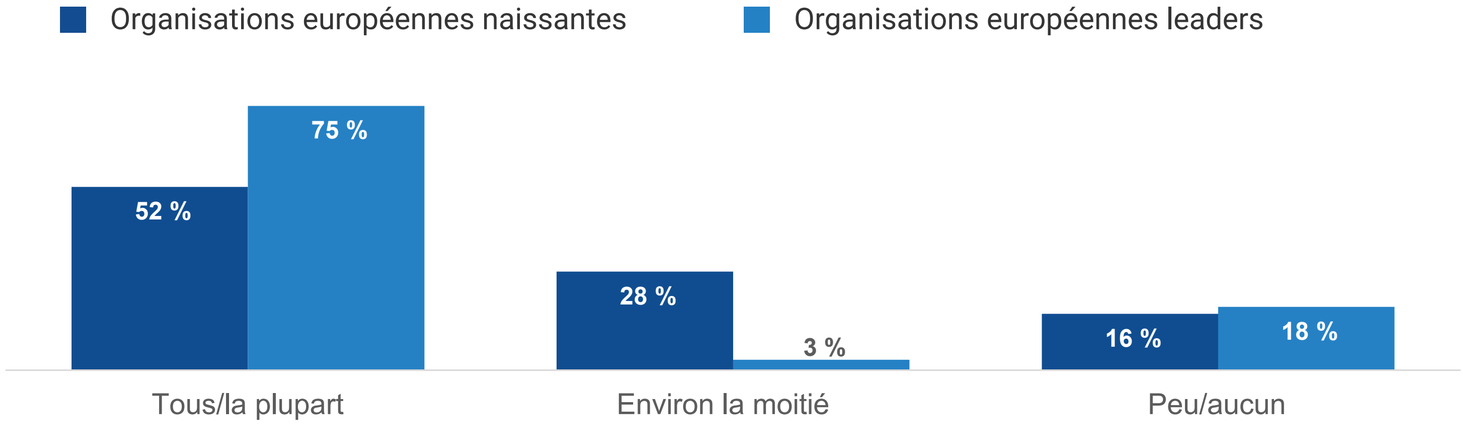
Les personnes sondées ont également été invités à réfléchir à toutes les applications développées en interne par leur organisation et à estimer la proportion dans laquelle le code a pu être mis en production « à la demande ». 75 % des organisations européennes leaders ont déclaré que les développeurs pouvaient intégrer le code en production pour la plupart ou la totalité de leurs applications (contre 52 % des organisations naissantes).

Ces deux preuves montrent à quel point les organisations leaders sont bien plus préparées à donner à leurs équipes de développement les moyens dont elles ont besoin.

Au cours des 12 derniers mois, combien de fois un projet de développement d'application a-t-il été retardé parce que l'équipe informatique ou de sécurité avait besoin de plus de temps pour inspecter les services cloud sur lesquels reposait le projet ?



Si l'on considère toutes les applications développées en interne par votre organisation, dans quelle proportion le code peut-il être mis en production « à la demande » ?



RETOUR AU SOMMAIRE

Les organisations leaders disposent d'environnements cloud plus efficaces et plus résilients

Les organisations leaders ont également fait état de résultats radicalement différents en ce qui concerne la rentabilité, la fiabilité et la sécurité de leurs environnements cloud :

la rentabilité

Réduction 50 % plus importante

Toutes les organisations sondées ont été invités à estimer dans quelle mesure leurs solutions de surveillance et de visibilité du cloud les aidaient à réduire leurs coûts liés au cloud (par rapport à l'absence de ces solutions), et les organisations leaders ont fait état d'une réduction de 50 % plus importante.

La résilience

3,3 fois plus susceptibles de dire qu'ils peuvent se remettre d'une panne en quelques minutes plutôt qu'en quelques heures ou jours

- Toutes les organisations sondées ont été invités à estimer combien de fois au cours de l'année écoulée, les charges de travail critiques hébergées dans le cloud avaient été interrompues ou avaient vu leurs performances se détériorer considérablement. 75 % des organisations leader ont déclaré n'avoir jamais (33 %) été confrontées à une interruption des charges de travail critiques hébergées dans le cloud au cours des 12 derniers mois, ou y avoir été confrontées une seule fois (42 %) (contre 44 % des organisations naissantes).
- Lors des interruptions de charges de travail, les organisations leaders détectent les problèmes et s'en remettent plus rapidement : elles étaient 4,1 fois plus susceptibles de détecter des interruptions en temps réel ou quasi réel (33 % contre 8 %) et 3,3 fois plus susceptibles de dire qu'elles pouvaient rétablir le service en quelques minutes plutôt qu'en quelques heures ou jours (36 % contre 11 %).
- En ce qui concerne la sécurité, au cours des 12 derniers mois, 72 % des organisations leaders ont déclaré n'avoir jamais été confrontées (45 %) ou n'avoir été confrontées qu'une seule fois (27 %) à une attaque réussie contre des charges de travail critiques hébergées dans le cloud (contre 56 % des organisations naissantes).

RETOUR AU SOMMAIRE

Les organisations leaders accélèrent leur mise sur le marché grâce à des solutions qui plaisent à leurs utilisateurs

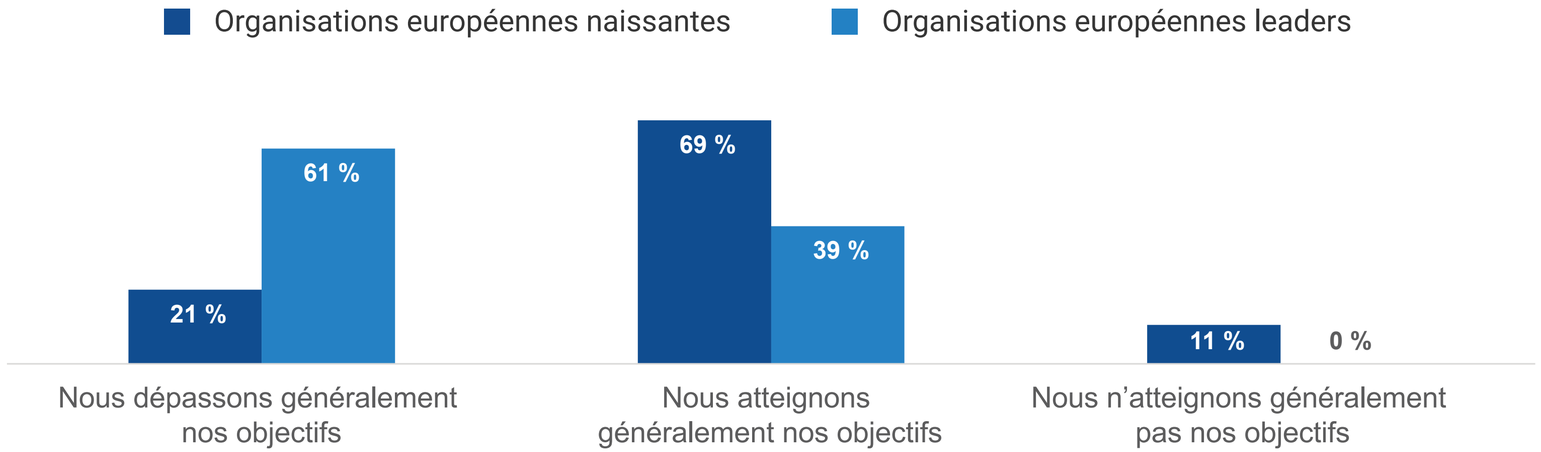
Enfin, l'étude montre que les avantages des organisations leaders en matière d'agilité et de résilience contribuent à leur réussite de manière quantifiable et tangible.

Toutes les personnes sondées ont été invités à se prononcer sur les performances de leur organisation en matière de délai de commercialisation. Les organisations européennes leaders étaient bien plus susceptibles que leurs homologues moins avancés de connaître le succès : 76 % ont déclaré qu'elles étaient généralement les premières à entrer sur leur marché, contre 11 % seulement pour les organisations naissantes.

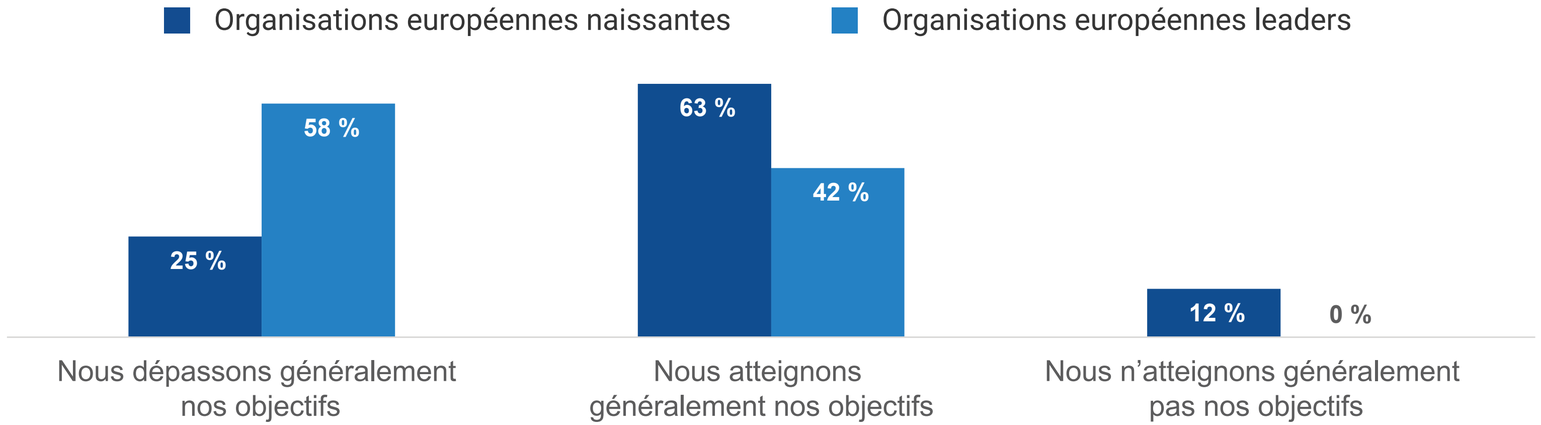
Et les solutions mises sur le marché répondent aux attentes des utilisateurs :

- Les organisations leaders étaient 2,9 fois plus susceptibles de dire qu'elles dépassaient généralement leurs objectifs de satisfaction des employés en ce qui concerne les charges de travail gérées par l'informatique et hébergées dans le cloud (61 % contre 21 %).
- Les organisations leaders étaient 2,3 fois plus susceptibles de dire qu'elles dépassaient généralement leurs objectifs de satisfaction des clients en ce qui concerne les charges de travail gérées par l'informatique et hébergées dans le cloud (58 % contre 25 %).

D'une manière générale, comment votre organisation se comporte-t-elle en matière de satisfaction des utilisateurs finaux employés avec les charges de travail cloud gérées par l'informatique ?



D'une manière générale, comment votre organisation se comporte-t-elle en termes de satisfaction des clients avec les charges de travail cloud gérées par l'informatique ?



RETOUR AU SOMMAIRE

Conclusion

L'analyse des réponses des participants européens met en lumière deux points clés. Tout d'abord, dans l'ensemble, les organisations européennes ont un retard modéré à rattraper par rapport à leurs homologues du monde entier. Bien que l'écart ne soit pas insurmontable, il est constant dans des domaines tels que la création d'équipes de plateforme, la convergence des outils de mise en réseau et de sécurité du cloud et l'utilisation du DNS pour améliorer la gestion et la sécurité des actifs. Deuxièmement, les efforts pour combler ces lacunes porteront leurs fruits pour les organisations de la région. Les organisations leaders de la région font régulièrement état de résultats techniques et commerciaux considérablement meilleurs associés à leurs environnements cloud. Les responsables de la stratégie du cloud en Europe auraient tout intérêt à hiérarchiser les investissements et à mettre en place des processus adaptés au modèle de maturité de gestion hybride et multicloud décrit dans cet eBook.

Comment Infoblox peut aider

Infoblox allie la mise en réseau et la sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et les innovateurs émergents, Infoblox offre une visibilité et un contrôle en temps réel sur les personnes et les appareils se connectant au réseau d'une organisation afin d'accélérer son fonctionnement et d'arrêter les menaces plus tôt.

EN SAVOIR PLUS

infoblox®

MÉTHODOLOGIE DE RECHERCHE ET DÉMOGRAPHIE DES PERSONNES SONDÉES

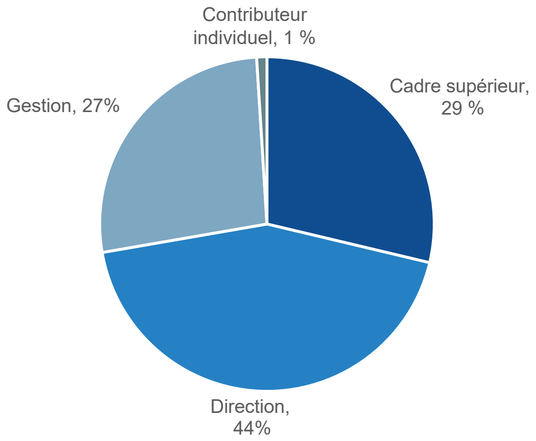
Pour recueillir les données de ce rapport, Infoblox a demandé à Enterprise Strategy Group de mener une enquête en ligne complète auprès de 1 000 décideurs et influenceurs dans le domaine des réseaux et de la sécurité, qui connaissent bien l'environnement de cloud public de leur organisation.

Les organisations représentées couvrent les secteurs privés et publiques du monde entier, notamment basées en Amérique du Nord (États-Unis et Canada), en Europe occidentale (France, Allemagne, Espagne et Royaume-Uni) et dans la région Asie-Pacifique (Australie, Inde, Japon, Nouvelle-Zélande et Singapour). L'enquête a été réalisée entre le 15 décembre 2023 et le 17 janvier 2024. La marge d'erreur au niveau de confiance de 95 % pour cet échantillon est de + ou - 3 points de pourcentage.

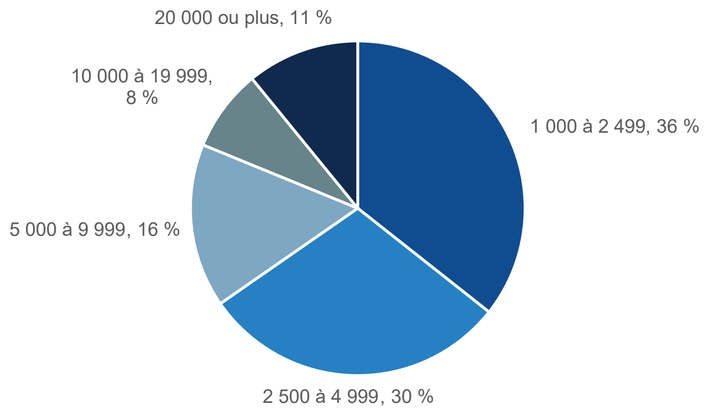
Les données démographiques des répondants basés en Europe sont affichées ici.

Remarque : les chiffres ayant été arrondis, leur somme indiquée dans les figures et les tableaux du présent rapport est susceptible de ne pas totalement correspondre.

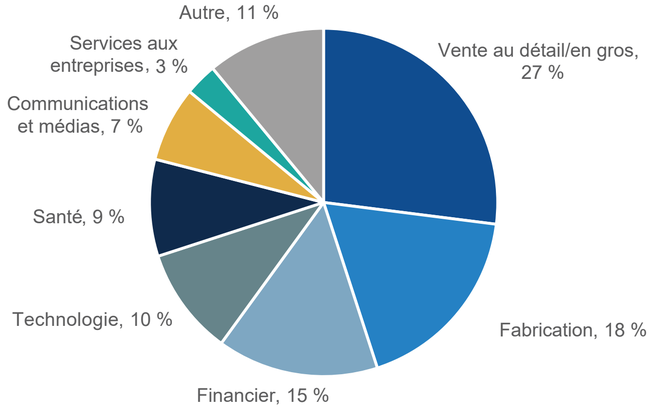
Lequel des énoncés suivants décrit le mieux votre titre et votre niveau de poste actuels ? (Pourcentage des répondants, N=300)



Combien d'employés votre organisation compte-t-elle dans le monde ? (Pourcentage des répondants, N=300)



Quel est le principal secteur d'activité de votre organisation ? (Pourcentage des répondants, N=300)



RETOUR AU SOMMAIRE

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group est une société intégrée d'analyse, de recherche et de stratégie technologiques qui fournit des renseignements sur le marché, des informations exploitables et des services de contenu de commercialisation à la communauté technologique mondiale.