CIO CSO COMPUTERWOCHE VOICE OF DIGITAL

IT-SECURITY.

SOUS LE SIGNE DE LA SOUVERAINETÉ EUROPÉENNE EN MATIÈRE DE DONNÉES.

En collaboration avec notre partenaire d'étude exclusif

mimecast

SOMMAIRE

EMPREINTE

Élaboration du questionnaire :
Bernd Hohlweg (Mimecast),
Halime-Merve Ersan (Mimecast),
Matthias Teichmann (Foundry)

Révision finale /
Rédacteur en chef du
Rapport d'étude final :
Matthias Teichmann

Analyses / commentaires :
Oliver Schonschek, Bad Ems

Hébergement / coordination :
Travail sur le terrain :
Armin Rozsa (Foundry)

Partenaire d'étude :
Mimecast France SARL
4 Rue De Marivaux
75002 Paris
France
www.mimecast.com/fr

Graphique :
Patrick Birnbreier, Munich

Conception de la couverture
avec une illustration de
© shutterstock / pancha.me

Relecture :
Elke Reinhold, Munich

Interlocuteur :
Matthias Teichmann
matthias.teichmann@foundryco.com

Foundry
(formerly IDG Communications)

Adresse :
IDG Tech Media GmbH
Georg-Brauchle-Ring 23
D-80992 Munich
Allemagne
Téléphone : +49 89 36086 0
Fax: +49 89 36086 118
E-Mail: info@idg.de

Représentant autorisé :
Maria Savvidou

Tribunal d'enregistrement :
Tribunal d'instance de Munich,
HRB 99110

Numéro d'identification de la taxe
sur la valeur ajoutée :
DE 811 257 834

Informations supplémentaires
à l'adresse :
www.foundryco.com

INTRODUCTION

Le rôle des fournisseurs de services de sécurité informatique a considérablement évolué. Alors qu'auparavant, il s'agissait uniquement de se défendre contre les attaques techniques, les fournisseurs de solutions de sécurité informatique agissent désormais en tant que partenaires stratégiques pour des concepts de sécurité et de conformité holistiques dans un contexte de cybermenaces mondiales croissantes, de numérisation accrue et de modèles de travail hybrides. Ils aident les entreprises à construire des infrastructures informatiques résilientes et à mettre en œuvre les exigences réglementaires – telles que le RGPD ou NIS2 – sur le plan technique et organisationnel.

Un partenaire de confiance en matière de sécurité informatique doit garantir la transparence, la traçabilité et la sécurité juridique du traitement des données. En raison des incertitudes géopolitiques, cela est remis en question et le choix d'un tel prestataire de services est donc de plus en plus important. La souveraineté des données et la conformité aux normes européennes de protection des données peuvent-elles être garanties, si par ex. des lois américaines telles que la CLOUD Act permettent aux autorités américaines d'accéder aux données dans certaines circonstances, même si elles sont stockées en Europe ?

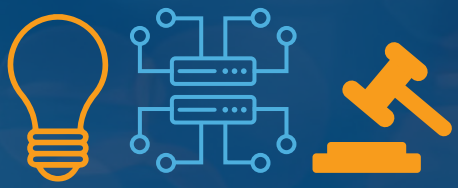
Dans ce contexte, les critères de sélection d'un fournisseur de solutions de sécurité informatique par les entreprises sont-ils en train d'évoluer ? Lesquels sont déterminants : l'expertise technologique ou la souveraineté des données et la conformité ?

RAPPORT DE GESTION

Aperçu des principales conclusions

Le contrôle de l'infrastructure des données est essentiel

29 % des entreprises considèrent que les compétences professionnelles de leur personnel sont très importantes pour la souveraineté numérique. Près des deux tiers des entreprises affirment même que l'infrastructure des données doit être contrôlée.



L'expertise et la protection des données sont essentielles, même sans certification

75 % des entreprises recherchent des fournisseurs de solutions de sécurité informatique disposant d'une expertise, la conformité est importante pour 68 % des entreprises. Mais seules 8 % des entreprises souhaitent que les fournisseurs de solutions de sécurité informatique soient certifiés.

Les entreprises de toutes tailles sont attentives à la géopolitique et à la souveraineté des données

En France, plus de neuf entreprises sur dix confirment que leur choix d'un fournisseur de solutions de sécurité informatique est influencé par les questions relatives à la souveraineté des données et la géopolitique.

1

Une infrastructure de données sécurisée est plus importante que les compétences professionnelles

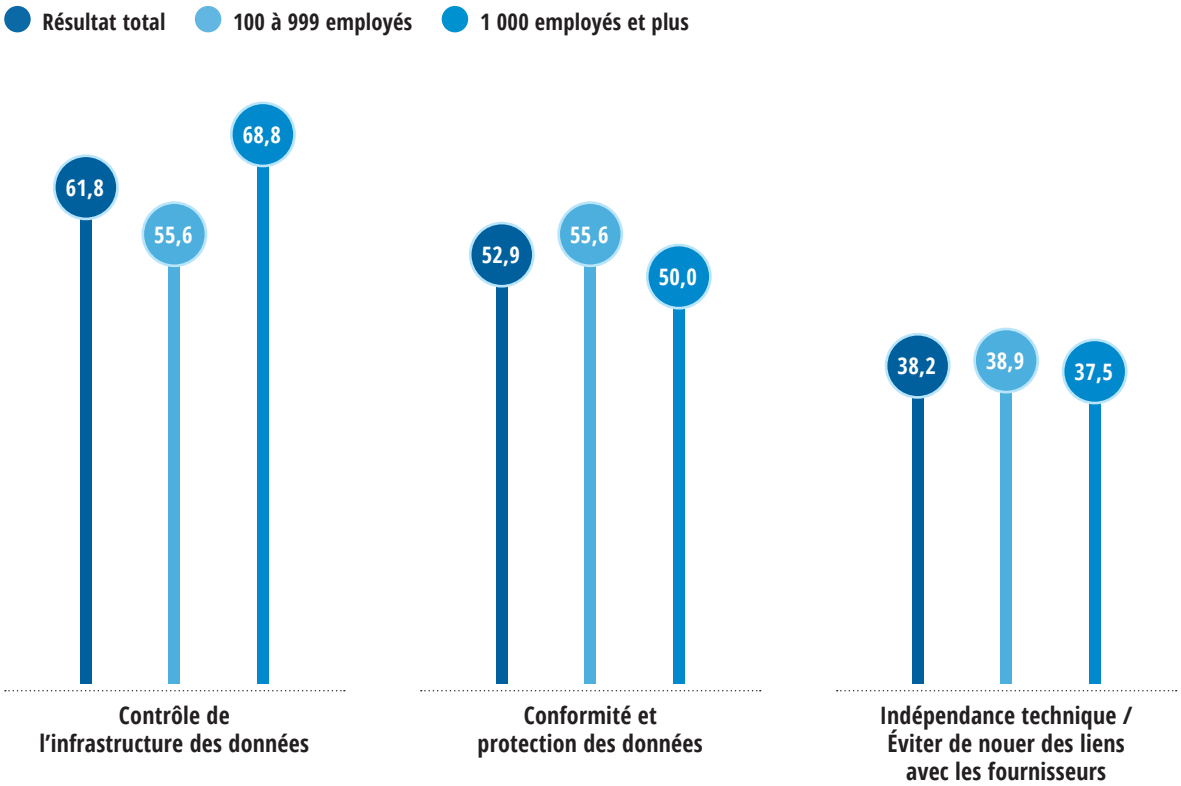
Pour les entreprises interrogées en France, le contrôle de l'infrastructure des données, la conformité et la protection des données ainsi que l'indépendance technique sont les trois critères les plus importants pour évaluer et maintenir la souveraineté numérique au sein de leur organisation. La compétence professionnelle du personnel, la continuité des activités et la qualité des partenariats arrivent loin derrière.

Les grandes entreprises avec au moins 1 000 employés citent encore plus souvent (69 % des réponses) le contrôle de l'infrastructure de données en tant que critère le plus important pour la souveraineté numérique. Seuls 56 % des petites entreprises ayant entre 100 et 999 employés partagent cet avis. Les places n° 2 et n° 3 parmi les critères les plus importants pour la souveraineté numérique sont toutefois plus appréciées par les petites entreprises.

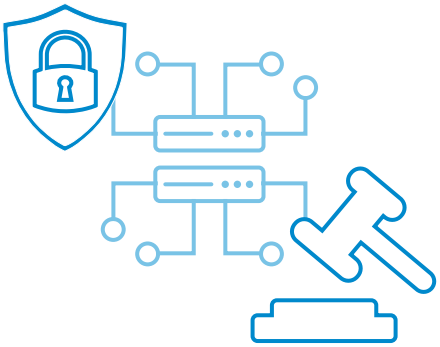
La protection des données et la conformité occupent la deuxième place chez les petites entreprises ayant jusqu'à 999 employés, avec 56 % des réponses, tandis que ces critères n'obtiennent que 50 % des réponses chez les grandes entreprises.

Veuillez indiquer les trois critères les plus importants pour évaluer et préserver la souveraineté numérique dans votre organisation.

Données en pourcentage. Plusieurs réponses possibles. Base : n = 102



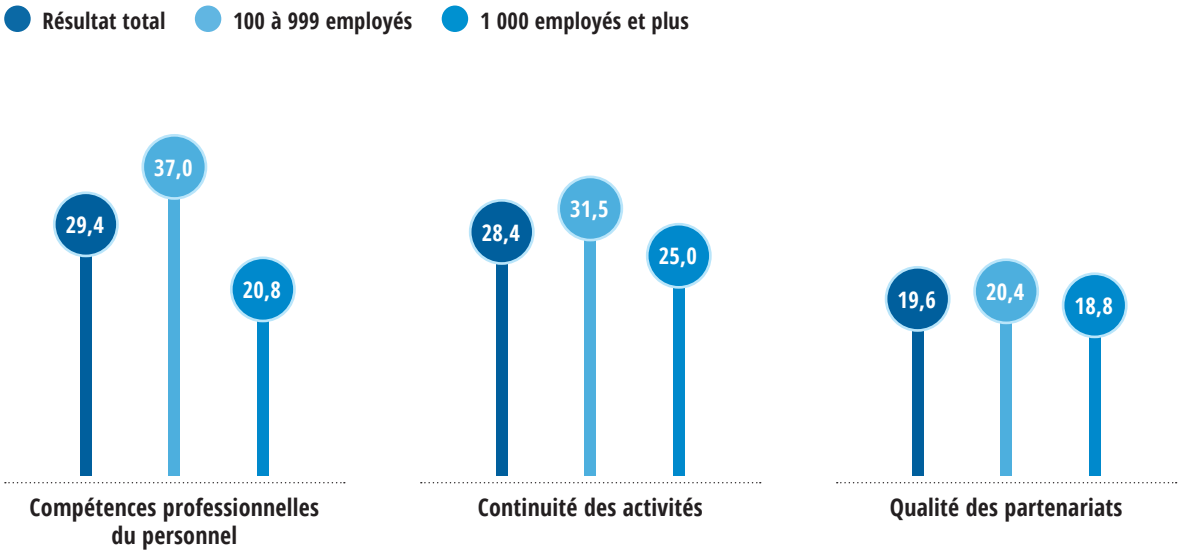
Les critères de la compétence professionnelle, de la continuité des activités et de la qualité des partenariats occupent plutôt les dernières places. Dans ce contexte, il ne faut toutefois pas oublier qu'un personnel compétent et des partenariats de haute qualité peuvent jouer un rôle important pour une infrastructure de données sécurisée, l'indépendance vis-à-vis des fournisseurs ainsi que le respect de la protection des données et de la conformité.



« La protection des données et la conformité sont de plus en plus importantes,notamment dans les les grandes entreprises. »

Veuillez indiquer les trois critères les plus importants pour évaluer et préserver la souveraineté numérique dans votre organisation.

Données en pourcentage. Plusieurs réponses possibles. Base : n = 102



2

Les fournisseurs de solutions de sécurité informatique peuvent convaincre grâce à leur expertise et à la protection des données

Trois quarts des entreprises interrogées en France accordent une importance particulière à l'expertise technologique et à la connaissance des processus lors du choix d'un fournisseur de solutions de sécurité informatique. Pour 68 % des entreprises interrogées, la protection des données et la conformité des fournisseurs de solutions de sécurité sont particulièrement importantes. En revanche, les certifications ne jouent un rôle que pour 8 % des entreprises.

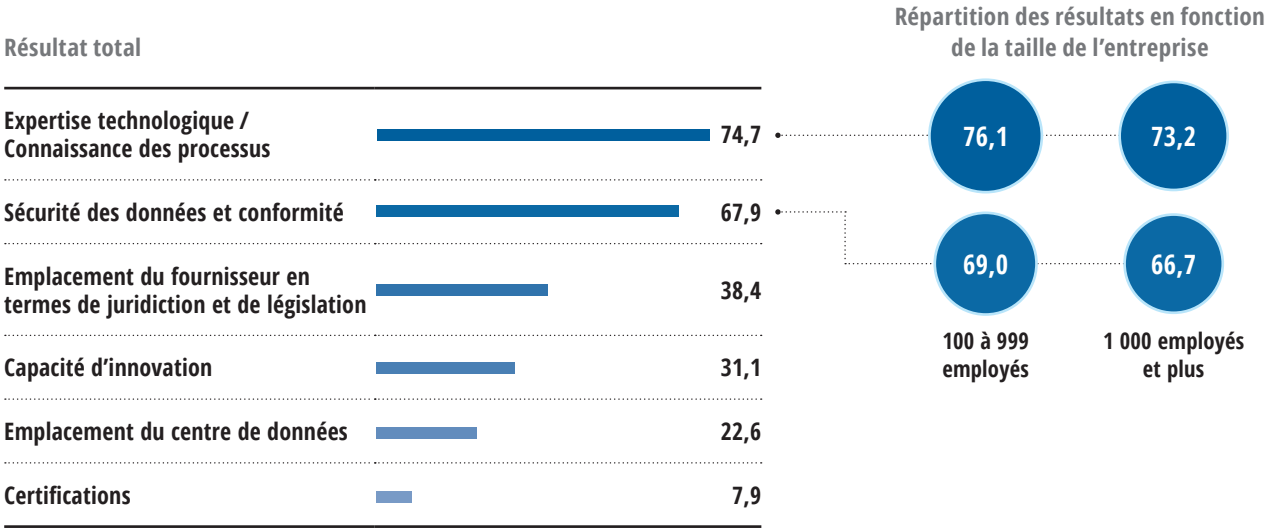
L'expertise en matière de technologie et de processus des fournisseurs de solutions de sécurité informatique est particulièrement importante pour les entreprises de toutes tailles.

La protection des données et la conformité occupent la deuxième place parmi les critères de sélection des fournisseurs de solutions de sécurité informatique, avec une moyenne de 68 % des réponses. Environ 40 % des entreprises considèrent que l'emplacement du fournisseur en termes de juridiction et de législation est un critère important, bien qu'il soit important pour la protection des données et la conformité. Selon l'enquête, les certifications ont une importance particulièrement faible, puisqu'elles ne sont citées en tant que critère de sélection que par 8 % des entreprises.

Après tout, l'emplacement d'un fournisseur est important pour environ 40 % des entreprises. Cependant, sans certifications, il est difficile de vérifier la protection des données et la conformité d'un fournisseur de solutions de sécurité informatique.

Parmi les critères suivants, lesquels sont les plus importants pour votre entreprise lors du choix d'un fournisseur de solutions de sécurité informatique approprié ?

Données en pourcentage. Base en fonction de la réponse n = 61 - 87



La géopolitique et la souveraineté des données influencent le choix du fournisseur de solutions de sécurité informatique

Seuls 5 % des entreprises interrogées en France affirment que les développements géopolitiques actuels et la question de la « souveraineté des données » n'ont aucune influence sur le choix d'un fournisseur de solutions de sécurité informatique par leur entreprise. En revanche, 95 % des entreprises interrogées soulignent explicitement l'importance de la souveraineté des données et de la géopolitique ou elles la confirment.

Dans les grandes entreprises avec au moins 1 000 employés, ce chiffre atteint même 96 %, la décision de choisir un fournisseur de solutions de sécurité informatique étant influencée par les débats actuels relatifs à l'évolution géopolitique et à la souveraineté des données. Avec 44 %, le consentement est particulièrement fort parmi les grandes entreprises.

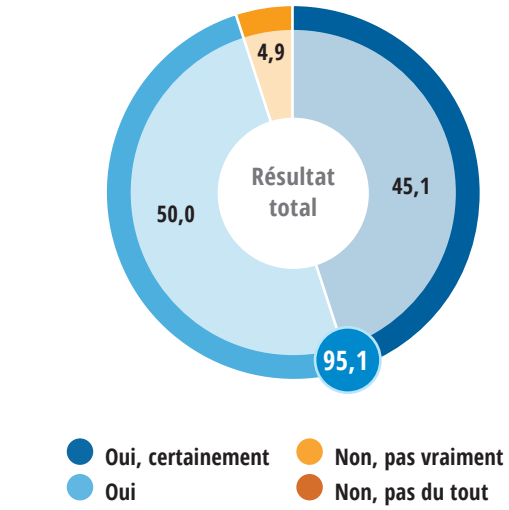
Dans les petites entreprises, 94 % des entreprises interrogées considèrent ou confirment explicitement que leur décision concernant les fournisseurs de solutions de sécurité informatique est influencée par la géopolitique et les questions relatives à la souveraineté des données.

En France, ni les petites ni les grandes entreprises ne considèrent que la géopolitique et la souveraineté des données jouent un rôle lors du choix d'un fournisseur de solutions de sécurité informatique.

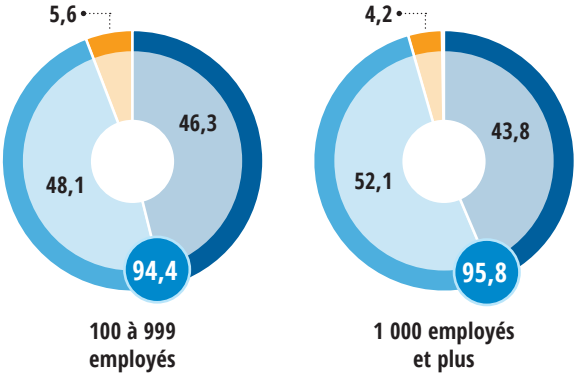
Ce résultat montre clairement à quel point les développements géopolitiques et les questions relatives à la souveraineté des données influencent le choix des fournisseurs de solutions de sécurité informatique en France.

Les développements géopolitiques actuels ainsi que le thème de la « souveraineté des données » ont-ils une influence sur le choix d'un fournisseur de solutions de sécurité informatique par votre entreprise ?

Données en pourcentage. Base : n = 102



Répartition des résultats en fonction de la taille de l'entreprise



CONCLUSION

La protection des données et le désir de souveraineté numérique influencent la recherche de fournisseurs de solutions de sécurité informatique

Même si l'expertise d'un fournisseur de solutions de sécurité informatique est particulièrement importante, les entreprises françaises attachent beaucoup d'importance à la souveraineté des données, à la protection des données et à la conformité. Cependant, à cet égard, des certifications ne sont pas particulièrement requises.

Par Oliver Schonschek

Même si l'on entend régulièrement dans les débats que le Règlement Général sur la Protection des Données (RGPD) empêche la compétitivité des entreprises européennes en comparaison avec des entreprises d'autres régions du monde qui sont soumises à des politiques de confidentialité moins strictes, les entreprises interrogées en France sont d'un avis différent : 22 % affirment que le RGPD est un obstacle, mais 34 % l'infirment.

De même, 35 % des entreprises françaises ne considèrent pas que l'accent mis sur la souveraineté numérique et les exigences en matière de conformité freine les innovations technologiques, tandis que 21 % seulement le confirment. 42 % des entreprises françaises ne considèrent pas non plus la souveraineté numérique en tant qu'illusion, contre seulement 23 % qui le pensent.

La situation est également intéressante en matière de sécurité informatique. Dans ce domaine, 95 % des entreprises sont attentives aux développements géopolitiques et aux questions relatives à la souveraineté des données. La protection des données et la conformité font partie des critères de sélection les plus importants lors de la recherche d'un fournisseur de solutions de sécurité informatique. En revanche, moins d'un tiers des entreprises interrogées recherchent une capacité d'innovation en matière de sécurité informatique chez le fournisseur de leur choix.

Pour près de 40 % des entreprises interrogées, l'emplacement des fournisseurs de solutions de sécurité informatique joue un rôle important, cependant les certifications jouent un rôle secondaire. Les entreprises devraient examiner elles-mêmes comment elles souhaitent se convaincre de la protection des données et de la conformité, alors que seulement 8 % d'entre elles considèrent les certifications en tant que critère important lors de la recherche de fournisseurs de solutions de sécurité informatique.

L'importance potentielle de l'emplacement du fournisseur ou du centre de données pour le niveau de protection des données garanti par la loi ne semble pas non plus être suffisamment prise en compte, puisque seuls 38 et 23 % des entreprises françaises interrogées y font attention.

Seuls 29 % des entreprises estiment que l'Europe doit tabler davantage sur la mise en place de ses propres infrastructures cloud indépendantes afin de garantir la souveraineté de ses données, tandis que 39 % des entreprises interrogées ne partagent pas cet avis.

Cependant, celles qui partagent cet avis devraient également évaluer plus précisément la question de l'emplacement ou demander des mesures de sécurité supplémentaires afin de garantir un niveau de protection des données conforme aux normes européennes.

Par conséquent, cela montre que : Les fournisseurs de solutions de sécurité basés en Europe, la protection des données, la souveraineté des données et la géopolitique jouent un rôle important pour les entreprises françaises, notamment dans les domaines de la sécurité informatique et de l'informatique en nuage. Cela ne devrait pas évoluer à l'avenir, à moins que des changements géopolitiques ne surviennent, lesquels, selon l'enquête, font partie des facteurs clés qui influencent les décisions des entreprises en matière de sécurité informatique.

« Dans ce domaine, 95 % des entreprises sont attentives aux développements géopolitiques et aux questions relatives à la souveraineté des données. La protection des données et la conformité font partie des critères de sélection les plus importants. »

PROFIL DE L'ÉTUDE

Éditeur ..... CIO, CSO et COMPUTERWOCHE

Partenaire d'étude exclusif ..... Mimecast France SARL

Population statistique ..... Responsables (informatiques) de haut niveau dans les entreprises françaises de 100 employés et plus : personnes impliquées dans les processus de décision stratégiques (informatiques) au niveau C ; décideurs et experts du domaine informatique (sécurité), de la gestion des risques ou du domaine financier

Génération des participants ..... Invitation personnelle par e-mail via la base de données exclusive des entreprises de CIO, CSO et COMPUTERWOCHE et, afin de respecter les quotas, via des panels d'accès en ligne externes

Période examinée ..... du 30 mai au 6 juin 2025

Méthode ..... enquête en ligne (CAWI), 114 entretiens terminés et qualifiés

Mise en œuvre ..... Équipe de recherche personnalisée de CSO, CIO et COMPUTERWOCHE

STATISTIQUES DES ÉCHANTILLONS

Répartition sectorielle
Plusieurs réponses possibles

Énergie	12,7 %
Approvisionnement en eau et assainissement	2,9 %
Fabrication et distribution de produits chimiques	11,8 %
Fabrication de machines, de véhicules et d'appareils électriques/électroniques	17,6 %
Technologie de l'information et de la communication (TIC) - Gestion des services	45,1 %
Infrastructure digitale	7,8 %
Fournisseurs numériques (par ex. places de marché en ligne, réseaux sociaux)	3,9 %
Production, transformation et distribution de produits alimentaires	7,8 %
Autres commerces de gros et de détail (à l'exception des produits alimentaires)	2,9 %
Médias, industrie du papier et de l'impression	2,9 %
Construction, artisanat	1,0 %
Banques et assurances et infrastructure des marchés financiers	10,8 %
Transports, logistique et circulation (y compris les services postaux et de messagerie)	2,0 %
Espace / Infrastructure spatiale-terrestre	2,0 %
Services aux entreprises	10,8 %
Administrations publiques	6,9 %
Secteur de la recherche, instituts de recherche	3,9 %
École, université, enseignement supérieur	3,9 %
Fabrication de dispositifs médicaux	1,0 %
Santé et secteur de la santé (par ex. hôpitaux, prestataires de soins de santé, produits pharmaceutiques, recherche médicale)	7,8 %
Gestion des déchets / élimination	1,0 %
Autre secteur d'activités	2,0 %

Taille de l'entreprise
En France

100 à 249 employés	17,6 %
250 à 499 employés	12,7 %
500 à 999 employés	22,5 %
1 000 à 4 999 employés	25,5 %
5 000 à 9 999 employés	7,8 %
10 000 employés et plus	13,7 %

Dépenses annuelles
Systèmes informatiques

Inférieures à 1 million d'euros	6,9 %
De 1 à moins de 10 millions d'euros	38,2 %
De 10 à moins de 100 millions d'euros	17,6 %
100 millions d'euros et plus	10,5 %
Je ne sais pas / Aucune réponse	4,9 %

Achats de logiciels via
AWS Marketplace

oui	54,9 %
non	36,3 %
je ne sais pas	8,8 %

À PROPOS DE MIMECAST

Mimecast est une entreprise leader dans le domaine de la cybersécurité qui révolutionne la façon dont les entreprises gèrent les risques humains. La plateforme de gestion des risques humains en réseau, contrôlée par l'IA et compatible avec l'API, a été spécialement conçue pour protéger les organisations contre l'éventail des cybermenaces. En intégrant une technologie de pointe à une approche centrée sur l'humain, notre plateforme améliore la visibilité et fournit des perspectives stratégiques.

Notre plateforme permet de prendre des mesures décisionnelles pertinentes et renforce la capacité des entreprises à protéger leurs environnements de collaboration. Elle sécurise les données critiques et implique activement les employés afin de réduire les risques et d'augmenter la productivité. Plus de 42 000 entreprises dans le monde font confiance à Mimecast pour garder une longueur d'avance sur le paysage des menaces en constante évolution.

Des risques d'initiés aux menaces externes, les clients obtiennent davantage avec Mimecast. Visibilité accrue. Agilité accrue. Contrôle accru. Sécurité accrue.

mimecast

Interlocuteur :
Katia De Medici, Marketing Manager, Southern Europe
kdemedici@mimecast.com

Mimecast France SARL
4 Rue De Marivaux
75002 Paris
France
Site internet : www.mimecast.com/fr