

PLEINS FEUX SUR LA SÉCURITÉ

La clé de la stratégie de cloud hybride d'une entreprise

Sommaire

Les entreprises informatiques modernes qui abordent avec une vision holistique leur infrastructure informatique, y compris les modèles sur site et dans le cloud, seront mieux positionnées pour combattre les vulnérabilités de sécurité. Aujourd'hui, les entreprises font face à plus d'incertitude que jamais auparavant. Alors que le nombre et la complexité des cybermenaces ne cessent d'augmenter, le besoin d'une disponibilité numérique sécurisée est primordial. Cependant, les entreprises ont du mal à adapter leurs stratégies en matière d'infrastructures pour mieux soutenir leurs clients et les charges de travail de plus en plus complexes sans sacrifier la sécurité.

En janvier 2020, IBM a publié une étude qu'elle avait commandée à Forrester Consulting en septembre 2019, pour évaluer la façon dont les entreprises développent et mettent en œuvre leurs stratégies en matière d'infrastructure informatique. Forrester a mené une enquête en ligne auprès de 350 décideurs informatiques d'entreprises internationales de divers secteurs pour explorer ce sujet. Nous avons constaté que les entreprises créent des environnements de cloud hybride avec différents clouds publics, des clouds privés hébergés et des infrastructures sur site.

Les entreprises informatiques investissent largement dans leur infrastructure pour surmonter les défis de sécurité d'aujourd'hui et de demain.

Les entreprises s'attachent non seulement à répondre aux demandes croissantes sur l'infrastructure informatique existante, mais aussi à assurer la sécurité lors de l'implémentation de nouvelles technologies.

58 %

déclarent que répondre aux demandes croissantes sur l'infrastructure informatique *existante* est une de leurs 5 grandes priorités cette année.

56 %

étendent ou mettent en œuvre de *nouvelles* technologies d'infrastructure cette année.

77 %

considèrent la *sécurité* comme une préoccupation essentielle lors de l'achat d'une infrastructure.

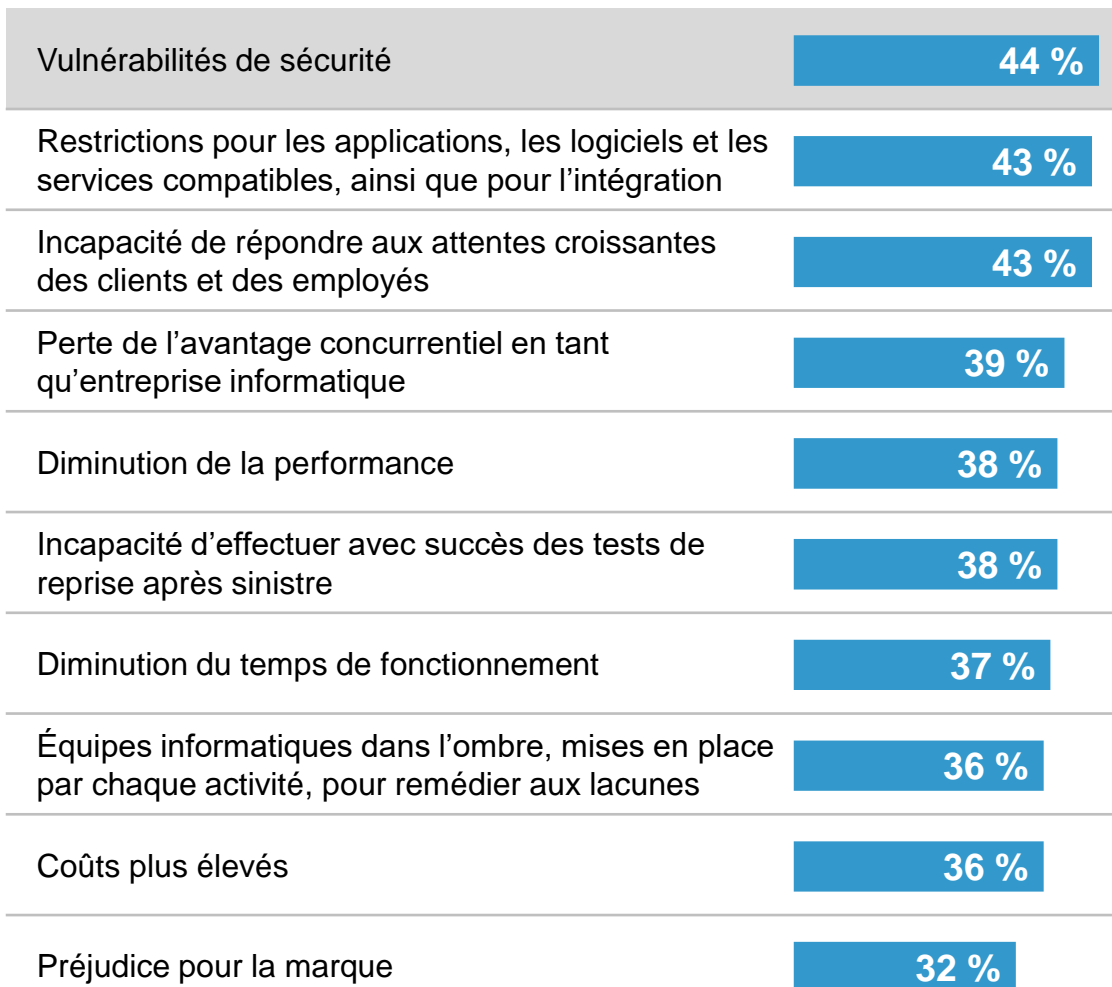
Dans les périodes d'incertitude, avec l'alourdissement et l'évolution des charges de travail, les entreprises informatiques doivent aborder la sécurité de manière holistique en parallèle de l'adaptation de leur infrastructure.

Renforcez la sécurité face aux incertitudes par une stratégie de modernisation de l'infrastructure de votre entreprise :

- Actualisez sans cesse votre stratégie pour la protéger des vulnérabilités de sécurité
- Conservez l'infrastructure sur site comme élément de votre stratégie de sécurité holistique
- Tirez parti de l'infrastructure sur site pour améliorer la sécurité des charges de travail et des applications critiques.

Principaux risques d'un retard dans l'actualisation de l'infrastructure

(liste des 10 premières réponses uniquement, classées de 1 à 5)



Échantillon : nombre variable de décideurs du monde entier en ce qui concerne les environnements d'infrastructures informatiques

Source : étude menée par Forrester Consulting pour le compte d'IBM, septembre 2019

© 2020 Forrester. Reproduction interdite.

La non-actualisation régulière de l'infrastructure introduit des menaces

38 % des décideurs affirment que leur entreprise a échoué aux tests de récupération après sinistre à cause d'un retard de l'actualisation.

61 % ont reporté l'actualisation de leur infrastructure plusieurs fois au cours des cinq dernières années.

Conservez l'infrastructure sur site comme élément de votre stratégie de sécurité holistique

Les entreprises continuent de diversifier leur infrastructure avec des plateformes de cloud non public, y compris sur site. L'infrastructure sur site reste fondamentale et constitue un élément essentiel d'une stratégie de cloud hybride sécurisé et résilient.

9/10

Conviennent que l'infrastructure sur site est un élément essentiel des stratégies de cloud hybride de leur entreprise.

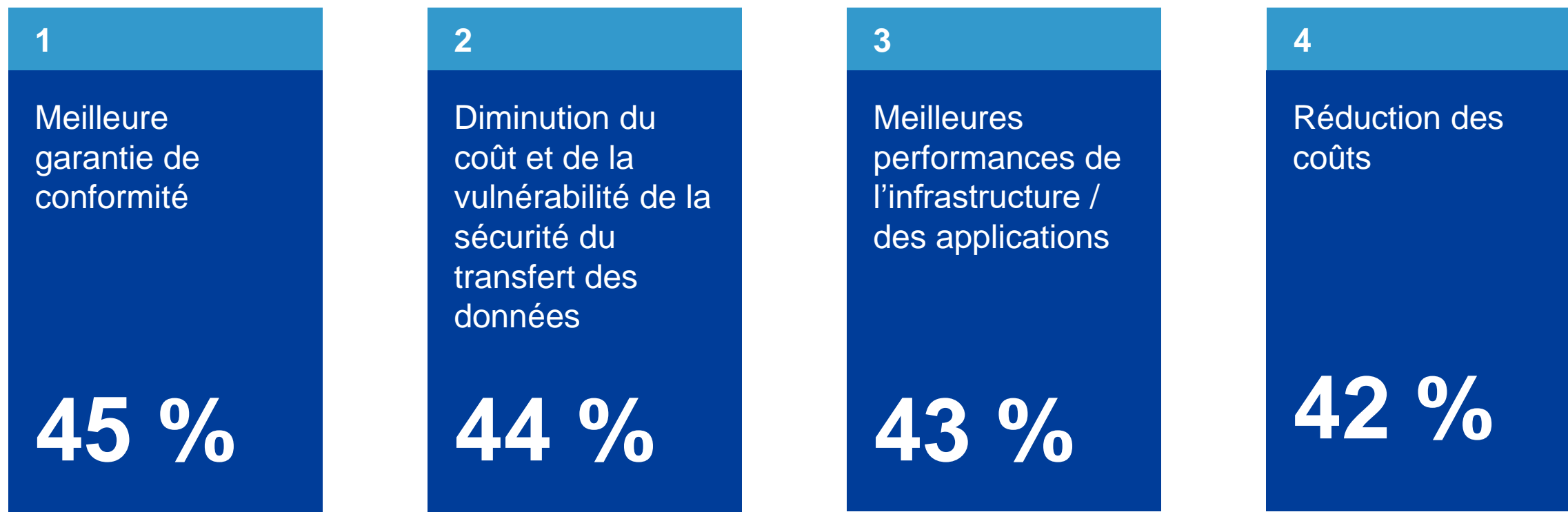


40 %

affirment que le fait que le cloud public ne réponde pas aux **besoins en matière de sécurité** est la raison pour laquelle ils maintiennent une infrastructure en dehors de la plateforme de cloud public.

Tirez parti de l'infrastructure sur site pour améliorer la sécurité des charges de travail et des applications critiques.

Raisons les plus souvent mentionnées de l'utilisation de ressources pour certaines charges de travail et applications :



Principales recommandations



Accordez la priorité à l'actualisation de l'infrastructure. Établissez une stratégie claire et holistique en matière d'infrastructure qui reconnaît le besoin de charges de travail sur site et qui s'attache aux problèmes de sécurité comme moteur principal des décisions d'actualisation. Même les entreprises qui ont du mal à survivre à cause de la pandémie doivent faire de l'actualisation de leur infrastructure en matière de sécurité une priorité.



Établissez une stratégie pour les données afin de prendre des décisions réfléchies sur les charges de travail — ceci afin de promouvoir la sécurité et la performance. Évitez le piège de ne considérer que les coûts pour prendre des décisions relatives aux charges de travail. Gardez l'impact de l'emplacement des données en haut de la liste, en optimisant les performances globales en fonction de la gestion des problèmes de sécurité et de latence via les données et les charges de travail importantes associées sur la même plateforme.



Développez un plan d'affaires irréfutable. La performance est particulièrement critique, car elle a un impact significatif sur l'expérience client (CX) et sur la perception de la marque. Les dirigeants qui ne souhaitent pas effectuer des actualisations complètes peuvent tirer parti des options d'actualisation de l'infrastructure qui dépendent de l'abonnement afin de pouvoir être plus flexibles à l'avenir en cas de changements de leur stratégie.



Télécharger
l'étude
complète

Méthodologie

Dans cette étude, Forrester a mené une enquête en ligne auprès de 350 décideurs du monde entier en ce qui concerne les environnements d'infrastructures informatiques afin d'évaluer la façon dont les entreprises développent et mettent en œuvre leurs stratégies en matière d'infrastructure. Les participants à l'enquête comprenaient des décideurs informatiques dans les domaines de l'infrastructure et des opérations, de la gestion ou de la maintenance des applications, et/ou du développement des logiciels. Les questions posées aux participants portaient sur les environnements utilisés pour les différentes charges de travail et sur l'investissement dans l'infrastructure. Une indemnisation financière a été versée aux personnes interrogées pour les remercier de leur participation à l'enquête. L'étude a commencé en août 2019 et s'est achevée en septembre 2019.

À PROPOS DE FORRESTER CONSULTING

Forrester Consulting propose des services de conseil indépendants et objectifs, basés sur un travail de recherche, pour aider les dirigeants à réussir dans leurs entreprises. Que ce soit lors de sessions courtes d'échange ou lors de la construction de projets sur mesure, les équipes conseil de Forrester vous mettent en contact avec des analystes qui mobilisent leur expertise pour répondre aux défis de votre secteur. Pour en savoir plus, consultez forrester.com/consulting.

© 2020, Forrester Research, Inc. Tous droits réservés. Toute reproduction non autorisée est strictement interdite. Les informations fournies s'appuient sur les meilleures sources disponibles. Les avis exposés sont le reflet d'une évaluation à un moment donné et peuvent évoluer. Forrester®, Technographics®, TechRankings, Forrester Wave, RoleView, TechRadar, Total Economic Impact et le logo CX sont des marques commerciales de Forrester Research, Inc. Toutes les autres marques commerciales appartiennent à leurs entreprises respectives. Pour des informations complémentaires, rendez-vous sur forrester.com.

Directrice de projet :

Cynthia Hicks,
Emma Van Pelt, Consultante en impact
sur le marché

Contribution à l'étude :

Groupe de recherche pour les directeurs
informatiques de Forrester