SYNTHÈSE

2023 Sécurité du cloud hybride

perception vs. réalité

Avec 72 % des organisations ayant déployé une infrastructure de cloud hybride, la sécurité peut être difficile à assurer ; de nombreux outils traditionnels, conçus pour un monde sur site, ne peuvent tout simplement pas surveiller et protéger suffisamment cette infrastructure numérique moderne.

Pour connaître le véritable état de la sécurité du cloud hybride, nous avons analysé les données fournies par plus de 1 000 décideurs IT et Sécurité sur six marchés mondiaux clés : les États-Unis, le Royaume-Uni, la France, l'Allemagne, l'Australie et Singapour. Le résultat ? Il existe un important décalage entre la perception qu'ont les responsables IT et Sécurité de leur posture de sécurité et la dure réalité. Accédez ici au rapport complet, ou découvrez-en les points clés ci-dessous.

L'état de la sécurité du cloud hybride

La bonne nouvelle, c'est que 96 % des personnes interrogées considèrent que la sécurité du cloud est la responsabilité de tous, et que la quasi-totalité (**99 %**) des responsables IT et Sécurité avec lesquels nous nous sommes entretenus dans les régions EMEA, APAC et aux États-Unis estiment que, dans leur entreprise, les CloudOps et les SecOps travaillent à un objectif commun.

Il reste cependant encore beaucoup à faire. Pour **99 %** des personnes interrogées, la détection et la réponse aux vulnérabilités restent cantonnées aux équipes SecOps en raison d'un manque de culture de la sécurité. Beaucoup s'inquiètent également d'un manque de connaissances réelles sur la façon de sécuriser le cloud, plus de la moitié (**52 %**) affirmant que leur conseil d'administration ne comprend pas le modèle de responsabilité partagée.

Il n'est donc guère surprenant que **93 %** des responsables IT et Sécurité dans le monde prévoient une augmentation des attaques de sécurité dans le cloud au cours des 12 prochains mois, surtout si l'on considère que **90 %** d'entre eux ont déjà été victimes d'une cyberattaque réussie depuis le début de l'année 2022.

Un fossé grandissant en matière de visibilité : perception vs. réalité

31 % des responsables IT et Sécurité ont identifié une violation parce que :

- Les utilisateurs avaient constaté un ralentissement des performances des applications (**18 %**), probablement en raison d'un DoS ou d'une exfiltration des données en transit
- Les utilisateurs ne pouvaient plus accéder aux applications et aux ressources numériques (**9 %**)
- Des données propriétaires de l'organisation avaient été divulguées sur le dark web (**4 %**)

Outre le fait que les violations sont identifiées trop tard, près d'une sur trois n'est pas détectée par les outils de sécurité et de surveillance actuels. Face à ce sombre constat, rien d'étonnant à ce que les angles morts suscitent de plus en plus d'inquiétudes.

Autre constatation préoccupante, 1 RSSI sur 3 ne sait pas avec certitude où ses données les plus sensibles sont stockées, ni comment elles sont sécurisées. La visibilité semble souffrir d'un certain nombre d'importantes faiblesses, aggravées par une mauvaise compréhension de l'étendue des angles morts ; **70 %** des personnes interrogées admettent que le trafic chiffré circule librement dans leur cloud hybride, tandis que **35 %** d'entre elles déclarent avoir une vue limitée sur les conteneurs. Cette situation présente de graves risques pour l'entreprise, car le trafic chiffré ne peut pas être suffisamment analysé et les menaces liées aux logiciels malveillants ne peuvent pas être détectées avec les outils existants lorsque ces données circulent en interne, à l'externe et latéralement dans une organisation.

Voilà la disparité entre perception et réalité. Si **50 %** des responsables IT et Sécurité déclarent être sûrs, voire tout à fait sûrs d'être suffisamment sécurisés depuis leur site jusqu'au cloud, la réalité de la sécurité du cloud hybride est toute autre : non seulement des angles morts existent, mais ils sont nombreux dans les organisations du monde entier.

Le Zero Trust séduit, mais l'adoption reste difficile

Pour la troisième année consécutive, nous avons également interrogé des responsables IT et Sécurité au sujet du Zero Trust et nous avons identifié un certain nombre d'évolutions quant à la perception de ce cadre de sécurité.

Cela reste un sujet de discussion clé dans le secteur à l'avenir car, si **80 %** des RSSI admettaient que le Zero Trust allait être une grande tendance en 2022, ce chiffre est passé à **96 %** en 2023 et au-delà. D'autres résultats mettent en évidence des conclusions similaires,

Définition de l'observabilité avancée : l'amélioration de la performance des outils de sécurité et d'observabilité traditionnels grâce à de l'intelligence et des données pertinentes tirées du réseau pour éliminer les angles morts, ce qui permet aux équipes d'atténuer de manière proactive les risques de sécurité et de conformité liés au cloud hybride, de réduire les coûts et la complexité.

puisque **87 %** des personnes interrogées déclarent en 2023 que leur conseil d'administration discute du Zero Trust comme d'une priorité – un chiffre qui a augmenté de **29 %** par rapport à 2022.

Pourtant, les discussions toujours plus nombreuses autour du Zero Trust s'accompagnent d'un scepticisme croissant quant à la réalité de sa mise en œuvre. Nombreux sont ceux qui ne savent pas comment concevoir et déployer le Zero Trust. La tendance croissante au scepticisme dans la région EMEA – où **77 %** des responsables IT et Sécurité considéraient en 2021 que le Zero Trust était réalisable, un chiffre qui a chuté à **53 %** en 2022 et est maintenant inférieur à la moitié (**44 %**) en 2023 – en est l'illustration. Cette incertitude est probablement due au fait que seulement **34 %** des organisations ont la visibilité nécessaire pour mettre en œuvre le Zero Trust.

La puissance de l'observabilité avancée

Les responsables IT et Sécurité reconnaissent que la visibilité fait partie intégrante du Zero Trust. Nous avons d'ailleurs découvert que si **89 %** des personnes interrogées en 2022 considéraient l'observabilité avancée comme assez à fortement liée au Zero Trust, **100 %** considèrent que les deux sont fortement liés en 2023.

Il est important de noter que l'observabilité avancée est de plus en plus reconnue comme une solution pour sécuriser le cloud hybride. Lorsqu'on leur avait montré la définition complète de l'observabilité avancée en 2022, **89 %** des responsables IT et Sécurité dans le monde avaient reconnu qu'il s'agissait d'un élément important de la sécurité du cloud. Ce chiffre est désormais passé à **97 %**, tandis que **20 %** de personnes interrogées en plus cette année par rapport à l'année dernière affirment que leur conseil d'administration aborde le sujet de l'observabilité avancée comme une priorité pour sécuriser le cloud hybride.

Le cloud hybride est un espace complexe, mais avec la majorité des organisations qui adoptent cette infrastructure, il est crucial que les responsables IT et Sécurité aient une vision fidèle à la réalité de leur posture de sécurité. La course est lancée pour obtenir une visibilité sur toutes les données en mouvement, combler le fossé entre la perception et la réalité, et éradiquer les angles morts critiques sources d'inquiétudes dans le cloud.

À propos de Gigamon

Gigamon offre un flux d'observabilité avancée qui exploite l'intelligence du réseau pour améliorer la performance des outils de sécurité et la visibilité ; ce qui permet aux services informatiques d'assurer la gouvernance de la sécurité et de la conformité, d'accélérer l'analyse des causes des goulets d'étranglement en matière de performance, et de réduire les coûts opérationnels associés à la gestion des infrastructures informatiques hybrides et multi-clouds. Résultat : les entreprises peuvent concrétiser toute la promesse de la transformation cloud. Gigamon compte plus de 4 000 clients dans le monde, dont plus de **80 %** des entreprises du classement Fortune 100, 9 des 10 plus grands fournisseurs de réseaux mobiles et des centaines de gouvernements et d'établissements d'enseignement. Pour en savoir plus, visitez gigamon.com/fr.

Téléchargez le rapport complet pour découvrir les résultats de votre région gigamon.com/enquete-cloud-securite

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

09.23_01