

# IBM muscle ses services de sécurité cloud

Protection, migration, intégration, gestion des accès, tests... IBM a annoncé cette semaine consolider ses [services de sécurité cloud](#).

« La sécurité cloud peut sembler décourageante, ses défenseurs étant confrontés à une surface d'attaque étendue, des modèles de [responsabilité partagée](#), des plateformes et des outils cloud en évolution rapide », a déclaré Vikram Chhabra, responsable mondial management et stratégie produit IBM Security Services. « Nous ne pouvons présumer que les approches héritées de sécurité fonctionnent avec ce modèle opérationnel », a ajouté le dirigeant. Selon lui, les professionnels du secteur ont intérêt à « moderniser la sécurité » pour l'adapter à « l'ère du cloud hybride », et opter pour une approche « [zero trust](#) ».

Que propose la multinationale américaine dans ce contexte ?

## Services gérés de sécurité cloud

L'offre étendue associe l'expertise conseil et technique du groupe en matière de sécurité, indépendamment des clouds utilisés (AWS, Microsoft Azure, Google Cloud, IBM Cloud...), à un ensemble intégré de solutions cloud, propriétaires et tierces.

Quels domaines couvrent les nouveaux services gérés de sécurité cloud d'IBM ?

La sécurité « native » dans le cloud, la gestion de la posture de sécurité et la sécurité des conteneurs. IBM dit également avoir renforcé ses services de conseil en stratégie de sécurité multicloud et hybride (infrastructure sur site et dans le cloud public/privé).

Pour ce faire, IBM déclare s'appuyer sur un ensemble de bonnes pratiques reconnues par l'industrie, dont la liste [Cloud Controls Matrix](#) de la Cloud Security Alliance.

(crédit photo : IBM)