

IBM lance de nouveaux services pour simplifier la sécurité du Cloud hybride

Une suite de services qui peut aider les entreprises à protéger les données, l'identité des utilisateurs et les applications sur des Clouds dispersés et sur des systèmes en local

CAMBRIDGE, Mass., le 25 mars 2021 : Aujourd'hui, IBM Security a annoncé des nouveaux services conçus pour aider les entreprises à gérer leur stratégie, leurs politiques et leurs contrôles de sécurité du Cloud dans les environnements de Cloud hybride. Ces services associent des technologies « Cloud natives », IBM et tierces à l'expertise d'IBM pour aider les entreprises à créer une approche de sécurité unifiée au sein de leurs écosystèmes Cloud.

Aujourd'hui, les entreprises exploitent un mélange de ressources Cloud et en local pour trouver un équilibre entre agilité, sécurité et réduction des coûts. Si la flexibilité du Cloud hybride peut offrir de nombreux avantages, beaucoup d'entreprises sont confrontées au défi de conserver une bonne visibilité et de gérer efficacement l'étendue des contrôles de sécurité dans cet environnement informatique dispersé. Les mauvaises configurations du Cloud ont été l'une des principales causes de violations de données selon le rapport 2020 sur le coût d'une violation de données^[1], représentant près d'une violation de données sur 5 étudiées.

Disponible dès aujourd'hui, la suite élargie de services de sécurité d'IBM pour le Cloud (IBM Security Services for Cloud) est conçue pour aider les entreprises à adopter une stratégie de sécurité cohérente dans leurs environnements Cloud hybride - avec l'aide de spécialistes d'IBM ayant l'expertise nécessaire pour gérer les contrôles de sécurité natifs sur Amazon Web Services, Google Cloud, IBM Cloud et Microsoft Azure, entre autres. Les services d'IBM peuvent aider les entreprises à évaluer la posture de sécurité du Cloud actuelle, ainsi qu'à créer et gérer les accès, les politiques et les contrôles techniques pour protéger les ressources Cloud nouvelles et existantes. Les services s'appuient sur l'IA et l'automatisation pour aider à identifier et à hiérarchiser les risques, à répondre aux menaces potentielles dans les environnements Cloud d'une entreprise, et à connecter ces données avec leurs opérations de sécurité plus larges et leurs systèmes en local.

*« La sécurité du Cloud peut sembler décourageante, ceux qui se défendent étant confrontés à une surface d'attaque étendue, à des modèles de responsabilité partagée et à des plateformes et outils Cloud qui évoluent rapidement », a déclaré **Vikram Chhabra, Global Director, Offering Management and Strategy, IBM Security Services**. « Nous ne pouvons pas supposer que les approches traditionnelles de la sécurité fonctionneront dans ce nouveau modèle d'exploitation - au contraire, la sécurité doit être modernisée spécifiquement pour l'ère du Cloud hybride, avec une stratégie basée sur les principes de « zero trust » qui associent contexte, collaboration et visibilité dans n'importe quel environnement Cloud. »*

Associer technologie et expertise pour simplifier la sécurité du Cloud

[IBM Security Services for Cloud](#) propose une approche ouverte et automatisée pour simplifier la sécurité du Cloud hybride, en réunissant une expertise en matière de sécurité, indépendamment du Cloud utilisé, et un ensemble intégré de solutions technologiques Cloud, propriétaires et tierces. Les services peuvent aider les clients à n'importe quelle étape de leur parcours de sécurisation du Cloud, qu'il s'agisse de conseiller les entreprises sur la façon de déplacer les données, les utilisateurs et les applications vers le Cloud, ou de fournir une surveillance continue des risques et une gestion des menaces relatives à leur architecture Cloud hybride existante.

Les nouveaux services comprennent :

Des services de sécurité « Cloud-native » : Nouveaux services de conseil et de sécurité managée qui peuvent fournir une visibilité, une gestion et une surveillance centralisées des contrôles de sécurité natifs sur tous les environnements Cloud - ce qui permet de réduire le risque de mauvaise configuration du Cloud, tout en fournissant des informations sur les risques et menaces potentiels. Les spécialistes d'IBM peuvent aider à concevoir et à mettre en œuvre des pratiques de sécurité pour les contrôles « Cloud-native » en fonction d'exigences commerciales et réglementaires spécifiques, et fournir un suivi et des rapports continus sur la façon dont les configurations sont optimisées dans l'ensemble de l'entreprise.

- **Une gestion de la posture de sécurité du Cloud :** Nouveaux services de conseil et de sécurité managée qui peuvent aider les clients à concevoir et à mettre en œuvre une solution de gestion de la posture de sécurité du Cloud (CSPM) pour assurer la gouvernance et la conformité des fournisseurs de services Cloud. Ces nouveaux services peuvent offrir une solution unique pour la conception d'un cadre de politique de conformité et de gouvernance, l'intégration du système CSPM et les services managés - en fournissant des recommandations exploitables et une automatisation pour aider à résoudre les problèmes liés à la conformité, ainsi que les activités continues de surveillance et de remédiation.
- **La sécurité des conteneurs :** Services de sécurité pour les environnements de conteneurs des clients, depuis le conseil et l'intégration de systèmes jusqu'à la gestion des menaces, la gestion de la vulnérabilité et les services de sécurité managée pour le cycle de vie complet des conteneurs. Voici les caractéristiques de ce service qui vient d'être amélioré :
 - Les consultants d'IBM peuvent évaluer les environnements de conteneurs existants, analyser les processus DevSecOps, revoir la conception des applications et les besoins en solutions, et aider les clients à établir une feuille de route pour leurs déploiements futurs.
 - [IBM Managed Security Services](#) (les services de sécurité managés d'IBM) peut fournir une visibilité, une gestion et une surveillance centralisées des conteneurs par le biais d'un tableau de bord unique - rassemblant des images, des registres, les orchestrateurs et les fournisseurs de services Cloud.
 - L'intégration avec la gestion des vulnérabilités d'IBM Security X-Force Red permet d'identifier, d'analyser et de classer des milliers de vulnérabilités liées aux conteneurs dans les environnements des clients afin de donner la priorité à la remédiation.
- **La stratégie de sécurisation du Cloud :** Services de conseil améliorés pour l'évaluation de la sécurité et la stratégie de sécurité hybride et multi-cloud, basés sur des cadres sectoriels tels que la matrice des contrôles du Cloud (CCM : Cloud Controls Matrix) de la CSA. Ces services peuvent désormais aider les entreprises à évaluer la posture de sécurité des applications et des services Cloud, y compris les recommandations pour faire face aux risques. Grâce à des techniques exclusives, les services peuvent fournir une stratégie personnalisée et une feuille de route de la maturité de la sécurité adaptée aux besoins commerciaux et réglementaires spécifiques du client.

Ces services s'appuient sur les capacités et l'expertise existantes d'IBM pour aider les clients dans leur parcours de sécurisation du Cloud. Les services de gestion des menaces IBM X-Force peuvent aider les clients à gérer le cycle de vie des menaces de sécurité à travers la détection, l'investigation et la réponse. IBM propose

également des services de sécurité pour le Cloud Access Security Broker (CASB : Agent de sécurité des accès au Cloud), qui aident les organisations à protéger les environnements Cloud grâce à une approche intégrée de la planification et de la mise en œuvre d'une solution CASB.

Pour en savoir plus sur IBM Security Services for Cloud : www.ibm.com/security/services/cloud-security-services

Ressources additionnelles :

- L'outil [IBM Security Services Cloud Assessment](#) peut aider les organisations à mesurer leur maturité en matière de sécurité du Cloud et à quantifier les risques.
- IBM organisera un webinaire le 1^{er} avril pour passer en revue les considérations stratégiques et opérationnelles relatives à la sécurité du Cloud.

À propos d'IBM Security

IBM Security offre aux entreprises l'une des gammes de produits et services de sécurité les plus performantes et intégrées du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère plus de 150 milliards d'évènements de sécurité par jour dans plus de 130 pays, et possède plus de 10 000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur <https://www-03.ibm.com/security/fr-fr/>, suivez IBM Security sur Twitter ou consultez [le blog IBM Security Intelligence](#).

Contacts presse :

Weber Shandwick pour IBM

IBM

Gaëlle Dussutour

Tél. : + 33 (0) 6 74 98 26 92

dusga@fr.ibm.com

Robin Legros / David Boutet

Tél. : + 33 (0)6 68 04 57 83 / +33 (0)6 6 63 45

03 79

ibmfrance@webershandwick.com

[1] Benchmark study of 524 companies who experienced a data breach, conducted by Ponemon Institute and sponsored, analyzed and reported by IBM Security
