

IBM dévoile une technologie résistante aux ordinateurs quantiques (Quantum-Safe) de bout en bout pour protéger les données les plus précieuses des gouvernements et des entreprises

La compagnie présente la feuille de route d'IBM Quantum Safe ainsi qu'un portefeuille de technologies visant à simplifier et à permettre une migration complète afin de sécuriser les données critiques contre des potentielles attaques dans le futur



ARMONK, NY / ORLANDO, FL, le 10 mai 2023 : IBM (NYSE : IBM) a annoncé aujourd'hui, lors de sa conférence annuelle Think à Orlando, en Floride, la nouvelle technologie IBM Quantum Safe (résistante aux ordinateurs quantiques) : un ensemble complet d'outils et de fonctionnalités, associé à l'expertise approfondie d'IBM en matière de sécurité, conçu comme une solution de bout en bout à mettre à la disposition des organisations, y compris des organismes gouvernementaux, qui préparent leur transition vers l'ère post-quantique, avec une sécurité résistante aux ordinateurs quantiques.

La technologie quantique progresse rapidement. Les systèmes quantiques sont en passe de résoudre des problèmes non résolus jusqu'à présent et bénéfiques pour les entreprises et la science, mais ces progrès présentent également des risques en matière de sécurité. Au fur et à mesure que les ordinateurs quantiques progresseront, ils parviendront à casser les protocoles de sécurité les plus largement utilisés dans le monde.

Consciente de ce risque, IBM a mis à profit sa vaste expertise en matière de cryptographie, d'informatique quantique et d'infrastructures critiques pour développer la technologie IBM Quantum Safe (résistante aux ordinateurs quantiques).

Cet ensemble de fonctionnalités est conçu pour aider les clients à se préparer à l'ère post-quantique via :

- **L'IBM Quantum Safe Explorer** qui permet aux entreprises d'analyser le code source et le code objet afin de localiser les actifs cryptographiques, les dépendances et les vulnérabilités, et d'établir une nomenclature cryptographique ([CBOM](#)). Cela permet aux équipes de visualiser et d'agréger les risques potentiels en un seul emplacement central.

- **L'IBM Quantum Safe Advisor** qui permet de créer une vue dynamique ou opérationnelle de l'inventaire cryptographique pour guider la remédiation, et analyse la posture cryptographique et la conformité pour hiérarchiser les risques.
- **L'IBM Quantum Safe Remediator** qui permet aux organisations de déployer et de tester des modèles basés sur les bonnes pratiques de remédiation à la menace quantique afin de comprendre les impacts potentiels sur les systèmes et les actifs lorsqu'elles se préparent à déployer des solutions résistantes aux ordinateurs quantiques.

IBM dévoile également sa feuille de route IBM Quantum Safe afin d'aider ses clients à comprendre cette transition en matière de sécurité et de les accompagner dans cette démarche. Il s'agit du premier plan d'IBM qui décrit les étapes technologiques vers une technologie résistante aux ordinateurs quantiques de plus en plus avancée, conçue pour aider les organisations à répondre aux futures normes et exigences cryptographiques grâce à la crypto-agilité, et à protéger les systèmes contre les vulnérabilités émergentes.

Ce parcours comprend trois actions clés :

- **Découvrir** : identifier l'utilisation de la cryptographie, analyser les dépendances et générer une nomenclature de cryptographie (CBOM).
- **Observer** : analyser la posture cryptographique des vulnérabilités et hiérarchiser les mesures correctives en fonction des risques.
- **Transformer** : remédier et atténuer grâce à la crypto-agilité et à l'automatisation intégrée.

*« En tant que leader de l'informatique quantique, IBM reconnaît l'importance de répondre de manière globale aux besoins critiques de ses clients qui envisagent également de transformer leur cryptographie pour l'ère quantique », a déclaré **Ray Harishankar, IBM Fellow and lead for IBM Quantum Safe technology** .*

« Notre nouvelle suite de technologies résistantes aux ordinateurs quantiques et les étapes de notre feuille de route sont conçues pour l'évolution continue de la sécurité résistante aux ordinateurs quantiques en tandem avec l'informatique quantique utile, et comprend également les solutions pour aider les industries à naviguer dans ce changement efficacement et facilement. »

L'année dernière, le gouvernement des États-Unis a publié de nouvelles exigences et lignes directrices invitant les agences fédérales à entamer la transition vers la sécurité résistante aux ordinateurs quantiques. Le National Institute of Standards and Technology (NIST) a sélectionné quatre algorithmes résistants aux ordinateurs quantiques en vue de leur standardisation, dont trois ont été [développés par IBM](#), en collaboration avec des universitaires et des industriels.

Ensuite, la National Security Agency (NSA) a annoncé de nouvelles exigences pour les systèmes de sécurité nationale afin qu'ils passent à des algorithmes résistants aux ordinateurs quantiques d'ici 2025, et la Maison Blanche a publié des exigences pour les agences fédérales afin qu'elles soumettent un inventaire cryptographique des systèmes qui pourraient être vulnérables à des ordinateurs quantiques impactant la cryptographie.

« Alors que l'ère de l'informatique quantique se rapproche rapidement de la réalité, il est impératif que des technologies résistantes aux ordinateurs soient également déployées pour protéger les systèmes et les données

*classiques d'aujourd'hui », a déclaré **Patrick Moorhead, CEO and founder of Moor Insights & Strategy** .*
« Ce dont le monde a besoin pour sécuriser les données à l'ère quantique, c'est d'une expertise en matière de technologie quantique de classe mondiale et de cryptographie avancée, ainsi que des décennies d'expérience en matière de développement de produits pour les infrastructures critiques. C'est sur ces piliers qu'IBM excelle, et maintenant, avec une feuille de route Quantum Safe pour mener l'industrie et de nouvelles technologies vers une migration simplifiée, je suis impatient de voir progresser les transitions vers une sécurité résistante aux ordinateurs quantiques dans le monde entier. »

La feuille de route et la technologie Quantum Safe d'IBM permettront aux organisations de découvrir leur paysage cryptographique actuel afin qu'elles puissent commencer à aborder les changements qui pourraient être nécessaires pour prospérer dans l'ère post-quantique.

Pour en savoir plus sur la technologie Quantum Safe (résistante aux ordinateurs quantiques) d'IBM ou pour demander une démonstration : <https://www.ibm.com/quantum/quantum-safe>.

Contacts Presse :

Weber Shandwick pour IBM

IBM

Gaëlle Dussutour

Tél. : + 33 (0)6 74 98 26 92

dusga@fr.ibm.com

Louise Weber / Jennifer Tshidibi

Tél. : + 33 (0)6 89 59 12 54 / + 33 (0)6 13 94 26 58

ibmfrance@webershandwick.com
