Contact presse :
Florence Lièvre
Tél. : +33 1 47 54 50 71
Email : florence.lievre@capgemini.com

Près des deux tiers des entreprises considèrent l'informatique quantique comme la menace de cybersécurité la plus critique d'ici 3 à 5 ans

Six « early adopters[1]» sur dix des technologies résistantes au quantique prédisent que le « Q-day, quand les ordinateurs quantiques pourront casser les algorithmes cryptographiques actuels, arrivera d'ici 5 à 10 ans

Paris, le 10 juillet 2025 – Un rapport du Capgemini Research Institute publié aujourd'hui, intitulé *Future encrypted : Why post-quantum cryptography leads the new cybersecurity agenda* *(Un avenir chiffré : pourquoi la cryptographie post-quantique s'impose dans la nouvelle stratégie de cybersécurité),* souligne que les progrès rapides de l'informatique quantique menacent de rendre obsolètes les algorithmes de chiffrement actuels. Les attaques « *harvest-now, decrypt-later*[2] », ainsi que le durcissement des réglementations et l'évolution du paysage technologique, ont accru l'importance de la sécurité quantique. Cependant, malgré une prise de conscience croissante, de nombreuses organisations sous-estiment encore les risques liés à l'informatique quantique, ce qui pourrait entraîner de futures violations de données et des sanctions réglementaires.

Selon le rapport, environ deux tiers (65%) des organisations sont préoccupées par l'augmentation des attaques « *harvest-now, decrypt-later* ». Un utilisateur précoce sur six pense que le « Q-day » arrivera dans les cinq ans, tandis qu'environ six sur dix pensent qu'il arrivera dans une décennie.

« Se préparer au déploiement de l'informatique quantique ne se limite pas à prédire une date, mais à gérer un risque irréversible. Chaque actif chiffré aujourd'hui pourrait devenir une faille de sécurité demain si les organisations tardent à adopter des dispositifs de sécurité adaptés à l'ère quantique. Une transition anticipée permettra de garantir la continuité des activités, la conformité réglementaire et la confiance à long terme, » déclare Marco Pereira, à la tête de la Cybersécurité des services *Cloud Infrastructure* du groupe Capgemini. *« Les mesures visant à la sécurité quantique prises aujourd'hui ne constituent pas des dépenses discrétionnaires mais un investissement stratégique, qui peut transformer un risque imminent en un avantage concurrentiel. Les organisations qui reconnaissent ce fait à un stade précoce seront les mieux préparées contre les cyberattaques futures. »*

Bien que les ordinateurs quantiques actuels ne soient pas encore capables de casser les systèmes de cryptage largement utilisés, les industries à haut risque telles que la défense et la banque sont à l'avant-garde de l'adoption de solutions résistantes au quantiques. En revanche, les secteurs axés sur la consommation, comme les produits de consommation et le commerce de détail, montrent moins d'urgence dans la préparation à la menace.

[1] Les « early adopters », qui représentent 70% des répondants à notre enquête, sont des organisations qui travaillent actuellement sur des solutions quantiques sûres ou qui prévoient de le faire au cours des cinq prochaines années.

[2] Les attaques « Harvest-now, decrypt-later » reposent sur l'acquisition de données actuellement illisibles avec la possibilité de les déchiffrer après le « Q-Day ».

La migration vers la cryptographie post-quantique préférée aux autres solutions de cybersécurité
La plupart des entreprises interrogées (70%) protègent leurs systèmes contre les menaces quantiques émergentes en adoptant une combinaison appropriée d'algorithmes de chiffrement capables de résister aux attaques quantiques.

Elles considèrent la cryptographie post-quantique (PQC) comme la meilleure option pour faire face aux risques de sécurité quantique à court terme, car elle fournit une approche complète de la sécurisation des données. Près de la moitié de ces 'early adopters' explorent, évaluent la faisabilité ou ont commencé à déployer des pilotes de solutions PQC. Pour 70% d'entre elles, les obligations réglementaires constituent un moteur clé de la transition vers la cryptographie post-quantique.

Tandis que les 'early adopters' avancent vers la sécurité quantique, 30% des entreprises interrogées ignorent encore la menace quantique. Elles peinent à allouer un budget et des compétences internes suffisants pour assurer la transition cryptographique.

Méthodologie du rapport
Le *Capgemini Research Institute* a mené une enquête auprès de 1 000 entreprises dont le chiffre d'affaires annuel est d'au moins 1 milliard de dollars, dans 13 secteurs et 13 pays d'Asie-Pacifique, d'Europe et d'Amérique du Nord. L'enquête mondiale a été réalisée en avril-mai 2025. Environ 70% de l'échantillon de ce rapport est appelé « early adopters ». Ce segment travaille ou prévoit de travailler sur des solutions quantiques sûres au cours des cinq prochaines années. Les résultats de l'enquête ont été complétés par des entretiens approfondis avec seize dirigeants de l'industrie.

À propos de Capgemini
Capgemini, partenaire de la transformation business et technologique de ses clients, les accompagne dans leur transition vers un monde plus digital et durable, tout en créant un impact positif pour la société. Le Groupe, responsable et multiculturel, rassemble 340 000 collaborateurs dans plus de 50 pays. Depuis plus de 55 ans, ses clients lui font confiance pour répondre à l'ensemble de leurs besoins grâce à la technologie. Capgemini propose des services et solutions de bout en bout, allant de la stratégie et du design jusqu'à l'ingénierie, en tirant parti de ses compétences de pointe en intelligence artificielle et IA générative, en cloud, et en data, ainsi que de son expertise sectorielle et de son écosystème de partenaires. Le Groupe a réalisé un chiffre d'affaires de 22,1 milliards d'euros en 2024.

*Get The Future You Want** | www.capgemini.com

**Capgemini, le futur que vous voulez*

À propos du Capgemini Research Institute
Le *Capgemini Research Institute* est le groupe de réflexion interne de Capgemini sur tout ce qui touche au numérique. L'Institut publie des recherches sur l'impact des technologies numériques sur les grandes organisations traditionnelles. L'équipe s'appuie sur le réseau mondial d'experts de Capgemini et travaille en étroite collaboration avec des partenaires universitaires et technologiques. L'Institut dispose de centres de recherche dédiés à Paris, en Inde, au Royaume-Uni, à Singapour et aux États-Unis. Il était récemment classé n°1 au monde pour la qualité de ses recherches par des analystes indépendants six années consécutives – une première.
Pour plus d'informations : https://www.capgemini.com/researchinstitute/