DELL Technologies

Livre blanc

Cryptographie post-quantique : préparer l'ère quantique

Livre blanc Dell Technologies

Sommaire

Présentation générale

L'informatique quantique passe rapidement de la recherche théorique à la réalité pratique. Autrefois considérées comme un horizon lointain, les avancées en matière de matériel, d'algorithmes et d'investissement accélèrent l'arrivée de machines capables de traiter des problèmes que les ordinateurs classiques ne peuvent résoudre. Les implications pour l'industrie sont profondes. De la découverte de médicaments à la modélisation climatique en passant par la logistique mondiale, l'informatique quantique promet de libérer des innovations jusqu'ici hors de portée.

Toutefois, cette avancée s'accompagne d'un défi majeur : les ordinateurs quantiques vont saper les fondements cryptographiques qui protègent l'économie numérique. La cryptographie à clé publique (algorithmes comme le chiffrement RSA et la cryptographie à courbe elliptique, ou ECC) protège les communications numériques, les systèmes financiers, les dossiers médicaux et la sécurité nationale depuis des décennies. Ces méthodes reposent sur des problèmes mathématiques insolubles pour les ordinateurs classiques. Pourtant, avec l'avènement des ordinateurs quantiques cryptographiquement pertinents (CRQC), ces mêmes problèmes peuvent être résolus efficacement, rendant la sécurité actuelle obsolète.

Cette menace n'est pas une simple théorie. Certaines organisations utilisent déjà une tactique connue sous le nom de « Récolter maintenant, déchiffrer plus tard » (HNDL), qui consiste à collecter des données chiffrées aujourd'hui dans l'espoir de les déchiffrer une fois que les ordinateurs quantiques seront arrivés à maturité. Les informations sensibles qui semblent sécurisées aujourd'hui risquent d'être vulnérables dans quelques années. Aussi, n'attendez pas que les CRQC soient sur le marché pour agir.

Ce livre blanc explique l'urgence de la menace quantique, explore le domaine émergent de la cryptographie post-quantique (PQC) et fournit des conseils sur la façon dont les organisations peuvent se préparer. Il souligne l'engagement pris Dell Technologies pour construire un avenir quantiquement sûr, en intégrant la sécurité dans sa chaîne logistique, son matériel, ses firmwares, ses logiciels et son écosystème de partenaires, en s'alignant sur les normes de cryptographie post-quantique (PQC) du NIST (FIPS 203, FIPS 204 et FIPS 205) et sur la Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). L'objectif de Dell est clair : garantir que l'innovation peut aller de l'avant sans sacrifier la sécurité ou la confiance.

Terminologie

Tout au long de ce document, vous rencontrerez un certain nombre de termes. Nous avons essayé de décrire certains de ces termes afin de faciliter la compréhension du document.

Cryptographie post-quantique : nouvelle approche mathématique de la cryptographie, avec de nouveaux algorithmes, conçue pour être protégée contre les attaques informatiques quantiques. Ces algorithmes fonctionnent sur des ordinateurs classiques et résistent à la fois aux attaques quantiques et aux attaques cryptographiques classiques connues.

Résistant aux quanta : fait référence aux systèmes, algorithmes ou infrastructures conçus pour rester sécurisés même en présence d'ordinateurs quantiques cryptographiquement pertinents (CRQC). Un système résistant aux quanta utilise la cryptographie post-quantique (PQC) ou d'autres protections qui résistent aux attaques classiques et quantiques, garantissant ainsi la confidentialité, l'intégrité et l'authenticité des données à l'avenir. Les termes « résistant aux quanta » et « quantiquement sûr » sont utilisés de manière interchangeable dans le présent document.

Agilité cryptographique (parfois appelée crypto-agilité) : capacité des systèmes et applications d'une entreprise à changer rapidement et en toute transparence d'algorithmes cryptographiques, de protocoles ou de longueurs de clés sans nécessiter de reconceptions majeures ou de perturbations opérationnelles.

« Récolter maintenant, déchiffrer plus tard » (Harvest Now, Decrypt Later, ou HNDL, également appelé « Enregistrer maintenant, déchiffrer plus tard ») : action par laquelle les acteurs malveillants collectent et stockent, dès aujourd'hui, des données chiffrées dans le but de les déchiffrer plus tard, lorsque les ordinateurs quantiques cryptographiquement pertinents (CRQC) seront disponibles.

Informatique quantique et menace sur le chiffrement

L'essor de l'informatique quantique

Comme l'a décrit il y a près d'un an notre directeur technique John Roese dans notre billet de blog, Post-Quantum Cryptography: A Strategic Imperative for Enterprise Resilience, les ordinateurs classiques (ordinateurs portables, smartphones ou serveurs) traitent les informations à l'aide de bits, qui existent à l'état 0 ou 1. Ce modèle binaire a alimenté des décennies de progrès, mais il limite la façon dont l'information peut être représentée et manipulée. Les ordinateurs quantiques utilisent des qubits, qui peuvent exister dans plusieurs états simultanément grâce à des principes tels que la superposition et l'enchevêtrement. Cela permet aux machines quantiques d'explorer un grand nombre de solutions possibles en parallèle, offrant ainsi un avantage de calcul pour des classes spécifiques de problèmes.

Les applications potentielles de l'informatique quantique sont extraordinaires. Les chercheurs prévoient des percées dans le secteur pharmaceutique en simulant les interactions moléculaires avec une précision que les ordinateurs classiques ne peuvent atteindre. Les climatologues envisagent des modèles plus précis des systèmes mondiaux, tandis que le secteur de l'énergie entrevoit un potentiel d'optimisation des réseaux et du stockage d'énergie. Même la logistique et la fabrication peuvent bénéficier des techniques d'optimisation quantique. Les avantages sont réels et à portée de main – mais les risques aussi.

Pourquoi le chiffrement est menacé

À l'ère numérique, le chiffrement est à la base même de la confiance. La cryptographie garantit la confidentialité, l'authenticité et l'intégrité lorsque vous saisissez un numéro de carte de crédit, accédez à un site Web sécurisé ou recevez une mise à jour logicielle signée. Ces protections reposent majoritairement sur la cryptographie à clé publique, des algorithmes tels que les chiffrements RSA et ECC qui sont basés sur des problèmes mathématiques considérés comme non réalisables du point de vue du calcul pour les machines classiques.

L'informatique quantique change la donne. En utilisant l'**algorithme de Shor**, un ordinateur quantique suffisamment puissant peut résoudre les problèmes de factorisation et de logarithme discret qui donnent aux chiffrements RSA et ECC toute leur force. Dès que les CRQC existeront, les signatures numériques qui protègent les mises à jour logicielles, les clés qui établissent les sessions TLS et les certificats qui authentifient les terminaux risqueront tous d'être compromis. L'impact sera systémique, menaçant les mécanismes mêmes qui sécurisent les transactions numériques.

La cryptographie symétrique (des algorithmes tels qu'AES, utilisés pour protéger les données stockées ou sécuriser les communications) est confrontée à un défi différent, quoique moins grave. L'**algorithme de Grover** permet à un ordinateur quantique de réduire la force effective des clés symétriques, réduisant ainsi de moitié leur sécurité. Même si ce problème peut être atténué par le passage à des tailles de clés plus importantes, telles qu'AES-256, cet ajustement souligne le fléau omniprésent que représentent les menaces quantiques

Urgence et conséquences

Les conséquences vont bien au-delà du risque théorique. Les entreprises incapables de se préparer sont exposées à des problèmes de propriété intellectuelle sensibles, à des perturbations des systèmes financiers, à des violations des données de santé et à des menaces pour la sécurité nationale. La stratégie « Récolter maintenant, déchiffrer plus tard » aggrave l'urgence : les adversaires n'ont plus qu'à capturer les données chiffrées aujourd'hui et à attendre les moyens de les déchiffrer. Dès que les CRQC arriveront sur le marché, les dégâts seront déjà irréversibles.

Cryptographie post-quantique et normes émergentes

Définition de la cryptographie post-quantique

La cryptographie post-quantique (PQC) désigne une nouvelle génération d'algorithmes conçus pour sécuriser les systèmes numériques contre les attaques classiques et quantiques. À la différence de la distribution de clés quantiques (qui nécessite du matériel spécialisé), la PQC est conçue pour fonctionner sur l'infrastructure classique actuelle (serveurs, terminaux, réseaux), ce qui en fait le moyen le plus pratique et évolutif de se préparer à l'ère quantique.

La PQC repose sur un ensemble de problèmes mathématiques qui, au mieux des connaissances actuelles, résistent aux techniques quantiques comme les algorithmes de Shor et Grover. La cryptographie basée sur les treillis, les signatures basées sur le hachage, les schémas basés sur le code et les équations multivariées représentent les familles les plus prometteuses. Ces approches sont rigoureusement testées et standardisées afin de garantir la même fiabilité et la même interopérabilité que les chiffrements RSA et ECC.

Normes sectorielles émergentes : le défi de la standardisation mondiale

Conscients de l'imminence de la menace, les gouvernements et les organismes de normalisation ont fait de la PQC une priorité mondiale. Ainsi, aux États-Unis, le NIST (National Institute of Standards and Technology) a lancé son projet PQC en 2016, appelant la communauté de la recherche cryptographique à proposer, analyser et affiner des algorithmes candidats. Après des années de tests, le NIST a annoncé le premier groupe d'algorithmes standardisés en août 2024 :

- **CRYSTALS-**Kyber, pour le chiffrement à clé publique et l'établissement de clés
- **CRYSTALS-**Dilithium et SPHINCS+, pour les signatures numériques

D'autres algorithmes sont à l'étude afin de fournir diversité et flexibilité face aux différents besoins d'implémentation, y compris les systèmes légers tels que les firmwares intégrés. Ce processus de standardisation, en évolution constante, permet aux entreprises du monde entier d'adopter des solutions résistantes aux quanta.

Les normes du NIST : FIPS 203, 204 et 205

En août 2024, le NIST a finalisé les premiers algorithmes PQC :

- FIPS 203 (ML-KEM), basé sur CRYSTALS-Kyber, un mécanisme d'encapsulation de clés. Il fournit une sécurité IND-CCA2, ce qui signifie que les textes chiffrés restent impossibles à distinguer, même en cas d'attaques adaptatives à texte chiffré choisi.
- FIPS 204 (ML-DSA), basé sur CRYSTALS-Dilithium, un algorithme de signature numérique. Il offre une sécurité EUF-CMA robuste (infalsification existentielle en cas d'attaques par message choisi), une exigence standard pour les signatures numériques.
- FIPS 205 (SLH-DSA), basé sur SPHINCS+, un schéma de signature basé sur le hachage. Il est sélectionné comme une solution de secours conservatrice, indépendant des problèmes de treillis.

Une feuille de route obligatoire

Conscient de l'importance de l'adoption d'algorithmes de chiffrement résistants aux quanta, le gouvernement fédéral américain a commencé à émettre des exigences PQC auprès des organismes fédéraux. Ces algorithmes comprennent notamment les suivants : National Security Memorandum 10 (NSM-10), Commercial National Security Algorithm Suite (CNSA 2.0), National Institute of Standards and Technology (NIST) Interagency Report (IR) 8547, Office of Management and Budget Memorandum 23-02 (OMB M-2302), etc.

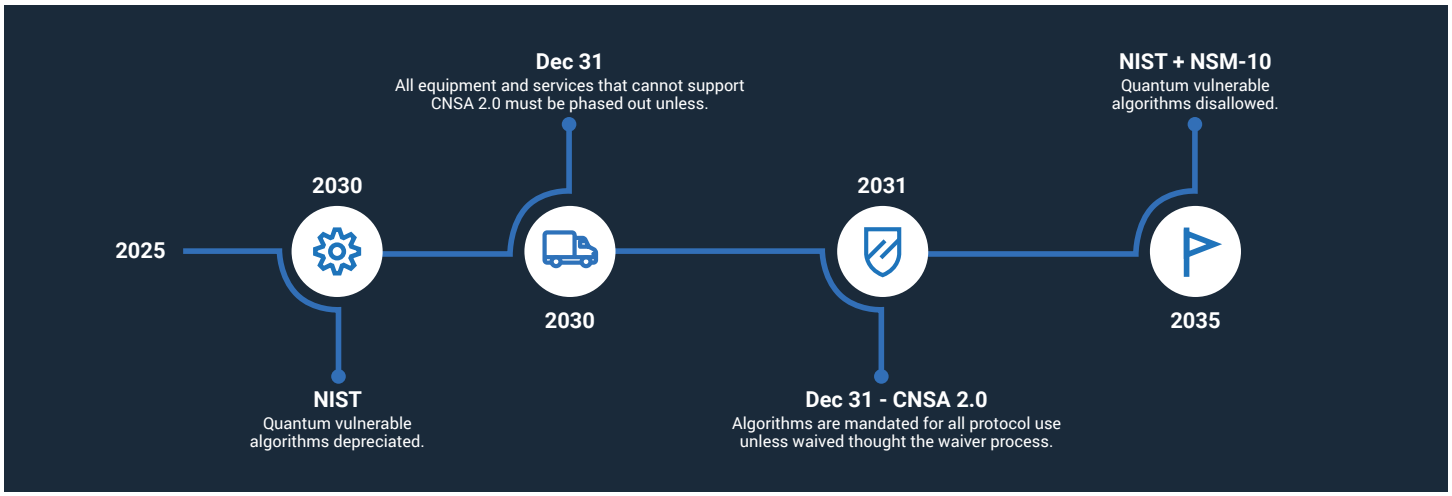
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)
Introduces the first recommendations post-quantum cryptographic algorithms

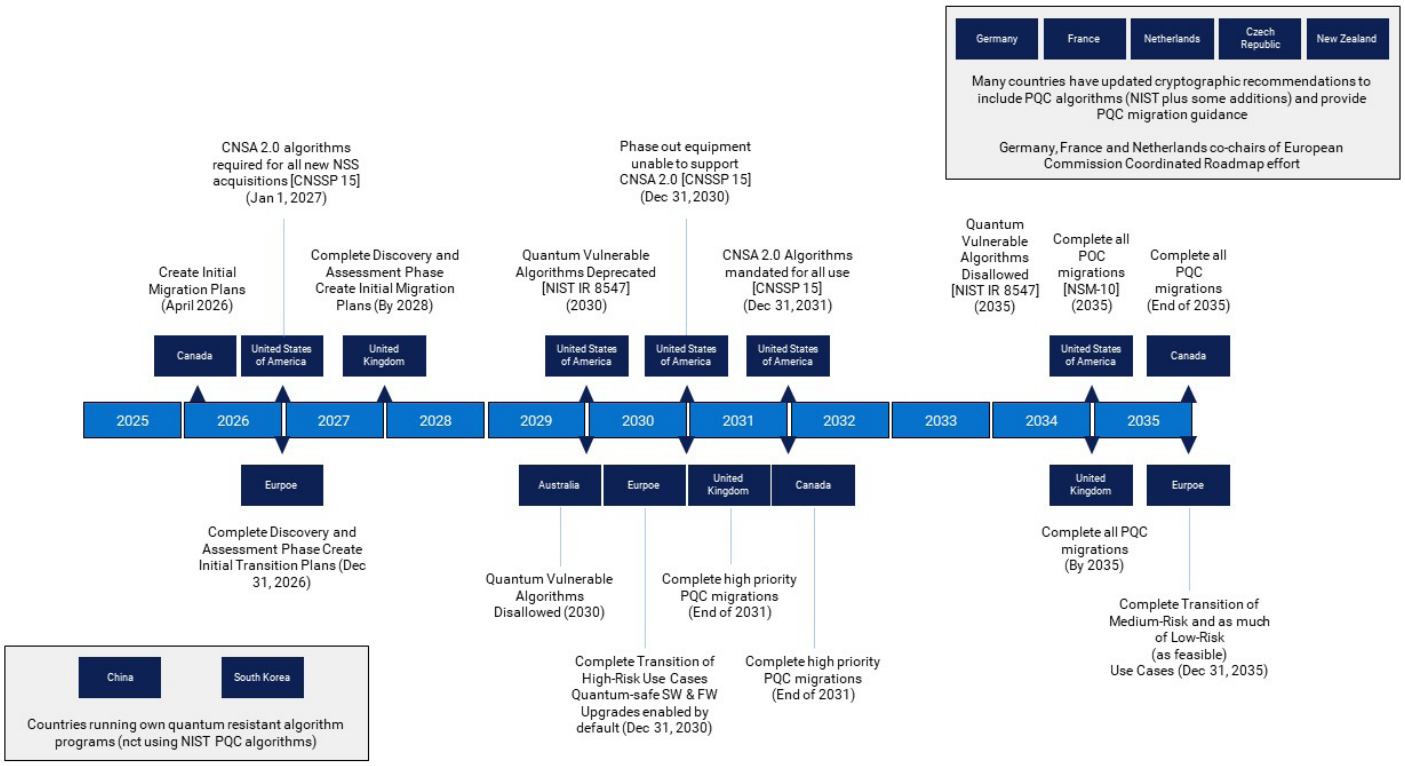
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

OMB Memorandum 23-02 (OMB M-23-02)
Provides detailed guidelines for federal agencies to how to comply with NSM-10

La CNSA 2.0, annoncée par la NSA en septembre 2022, introduit les premières recommandations pour les algorithmes cryptographiques post-quantiques. Elle fixe des échéances explicites pour l'adoption d'algorithmes résistants aux quanta dans les systèmes de sécurité nationale (NSS) et sert de guide efficace pour les entreprises préparant leurs propres transitions :



D'autres organisations dans le monde ont également établi des directives pour la transition vers la PQC. Vous trouverez ci-dessous quelques exemples de mandats nationaux.



Ces dates ne sont pas arbitraires, mais reflètent les délais requis pour reconcevoir, valider et déployer la cryptographie dans des écosystèmes IT complexes. Les entreprises doivent les considérer non pas comme de simples mandats gouvernementaux, mais comme des indicateurs pratiques de la transition mondiale vers la résilience quantique.

Collaboration dans le secteur

Au-delà du NIST et de la NSA, Dell participe activement aux consortiums industriels et aux groupes de normalisation qui favorisent l'interopérabilité et l'adoption, et y exerce son influence. Le Trusted Computing Group procède actuellement à l'intégration de la PQC dans la norme TPM (Trusted Platform Module). L'IETF participe pleinement à l'intégration des algorithmes PQC dans les protocoles industriels tels que le TLS et les certificats X.509. Les comités KMIP (protocole d'interopérabilité de gestion des clés) de l'OASIS permettent à la PQC de gérer les cadres de gestion des clés. La FIDO Alliance étudie l'impact de la PQC sur l'authentification et les normes d'intégration des appareils, tandis que des organisations comme SAFECode s'efforcent de sensibiliser le secteur à la préparation à la migration.

Le NCCoE (NIST National Cyber Security Center of Excellence) est la structure qui permet au NIST de travailler avec l'industrie, les universités et les agences gouvernementales via des projets axés sur le domaine. L'institut s'est concentré sur un certain nombre de choses telles que les suivantes :

- Découverte cryptographique : identifier les crypto-monnaies à migrer et hiérarchiser les éléments à migrer en premier.
- Interopérabilité : s'assurer que les fonctionnalités et protocoles cryptographiques courants intègrent les nouveaux algorithmes PQC, et veiller à l'interopérabilité des implémentations par les différents fournisseurs.
- Crypto-agilité (ou agilité cryptographique) : se concentrer sur le développement de systèmes d'information qui encouragent la prise en charge d'adaptations rapides de nouvelles primitives et algorithmes cryptographiques, sans apporter de modifications significatives à l'infrastructure du système.

Ces projets contribuent à informer/développer les directives et les normes créées et à s'assurer qu'il existe des exemples de solutions sectorielles pour les normes et les directives fournies. Dell participe au projet de migration du NCCoE vers la PQC depuis sa création.

À l'heure actuelle, la PQC n'est pas seulement un sujet de recherche : c'est une norme en développement, avec des algorithmes concrets, des calendriers et des parcours d'adoption. Les entreprises qui commencent à se préparer dès maintenant peuvent éviter les coûts, les interruptions et les risques de bousculade de dernière minute. La transition n'est pas simplement une question de conformité : il s'agit de s'assurer que la confiance, la confidentialité et l'intégrité restent intactes à l'heure où l'informatique quantique refaçonne le paysage numérique.

Pourquoi il est temps d’agir

Une menace immédiate

Il peut être tentant de considérer l’informatique quantique comme un risque lointain, qui sera résolu une fois que la technologie sera pleinement mise en œuvre. En réalité, le compte à rebours a déjà démarré. Les informations sensibles (transactions financières, dossiers médicaux, propriété intellectuelle ou communications gouvernementales) peuvent aujourd’hui être cryptées de manière sécurisée, mais dès lors que les machines quantiques seront en mesure de briser les chiffrements RSA ou ECC, ces données pourront être exposées rétroactivement. En conséquence, c’est une longue accumulation de communications et d’enregistrements qui pourrait soudainement être menacée.

Des cycles technologiques longs

Les écosystèmes IT modernes ne se transforment pas facilement ou rapidement. Par le passé, les remplacements d’algorithmes uniques, tels que la transition de SHA-1 à SHA-2 ou de DES/3DES à AES, ont pris plus de dix ans. Ces algorithmes sont profondément intégrés aux systèmes d’exploitation, aux applications, aux périphériques réseau et au matériel. Leur remplacement nécessite une reconception, une validation, des tests et un déploiement dans des environnements allant des datacenters aux plates-formes Cloud, en passant par les périphériques. Pour de nombreuses entreprises, ce processus prendra des années, soit bien plus de temps que la fenêtre restante avant que l’informatique quantique ne constitue une menace réelle. C’est pourquoi les législateurs, les organismes de normalisation et les responsables de la sécurité insistent sur une préparation immédiate. Attendre que les CRQC soient disponibles à grande échelle ne vous laissera pas le temps de procéder à une transition ordonnée.

Les risques de l’inaction

Retarder la migration a des conséquences qui vont au-delà de l’exposition technique :

- Risques pour la sécurité des données : les données à long terme, telles que les antécédents médicaux, les dossiers financiers ou les informations de défense, peuvent être compromises rétroactivement une fois les ordinateurs quantiques arrivés à maturité.
- Risques liés à l’authenticité et à l’intégrité des logiciels : l’authenticité et l’intégrité des logiciels peuvent être compromises par un code malveillant s’ils sont signés avec les méthodes de signature actuelles et s’ils sont toujours utilisés une fois les ordinateurs quantiques arrivés à maturité.
- Risques opérationnels : les systèmes d’infrastructure essentiels, tels que les services publics, les réseaux de transport et les services d’urgence, sont notoirement difficiles à moderniser. Si l’on ne planifie pas tout de suite, les opérations risqueront d’être perturbées demain.
- Risques liés à la réglementation et à la conformité : des cadres tels que la **CNSA 2.0** ont établi des délais clairs en matière de conformité. Les entreprises qui échouent à se préparer risquent non seulement d’être exposées, mais aussi de décevoir les attentes de leur gouvernement ou de leur secteur.
- Réputation et risque financier : toute violation résultant de vulnérabilités cryptographiques non résolues pourrait altérer la confiance vis-à-vis de la marque, ainsi qu’entraîner des pertes financières importantes.

Encourager l’action proactive

Une préparation proactive n’est pas seulement un geste défensif, mais également l’occasion de renforcer la résilience à long terme. En menant des inventaires cryptographiques, en mettant à niveau les longueurs de clés symétriques, en pilotant des solutions compatibles PQC et en s’engageant avec des fournisseurs qui proposent des offres résistantes aux quanta, les organisations peuvent maintenir la confiance. Les primo adoptants sont mieux placés pour assurer des opérations évolutives, maintenir la conformité et faire preuve de leadership auprès des clients, des partenaires et des organismes de réglementation.

L’approche de Dell en matière de cryptographie post-quantique

Chez Dell, nous pensons que la technologie est le moteur du progrès humain et que la sécurité en est le fondement. En tant qu’entreprise, Dell Technologies veille à ce que son portefeuille, son infrastructure IT et ses systèmes de support du cycle de vie soient bien préparés pour la transition vers des algorithmes résistants aux quanta. Mesures prises pour préparer la transition :

- Identifier les domaines et objectifs spécifiques où la cryptographie est utilisée dans les produits, les services, l’infrastructure IT et les systèmes de support afin de formuler des plans de transition complets.
- Améliorer les connaissances internes sur les algorithmes de cryptographie post-quantique (PQC), en tenant compte des aspects de mise en œuvre et des principes de conception liés à l’agilité cryptographique, afin de faciliter une transition en douceur vers les algorithmes PQC.
- Évaluer les performances, l’applicabilité et l’adéquation des algorithmes PQC dans divers cas d’utilisation pertinents pour la gamme diversifiée Dell Technologies.

Étant donné la nature complexe de la transition vers la PQC, les mises à niveau des cas d’utilisation cryptographiques peuvent être progressivement intégrées aux offres Dell Technologies. Du point de vue des données, par exemple, les efforts de transition doivent se focaliser sur les cas d’utilisation vulnérables aux attaques « Récoler maintenant, déchiffrer plus tard », tel que le chiffrement à la volée ou au repos des données.

Lorsque vous songez à votre plate-forme technologique, la transition d’un cas d’utilisation cryptographique peut impliquer une actualisation complète/un remplacement complet du produit ou une mise à niveau de ce dernier. Cela dépendra du produit en question, ainsi que de l’endroit et de la façon dont la cryptographie est implémentée dans ce produit et dans les systèmes environnants.

Ces cinq prochaines années, nous mettrons l’accent sur la commercialisation d’offres résistantes aux quanta afin de garantir que les clients puissent respecter les délais de transition vers la PQC publiés par les gouvernements et les associations professionnelles entre 2027 et 2035.

Les clients doivent collaborer avec leur équipe de compte Dell pour obtenir des détails spécifiques au produit (feuilles de route et calendriers de publication, par exemple) à intégrer dans leurs plans de migration. Dell fournira des échéances plus précises pour l’intégration de la PQC dans ses gammes de produits au cours des prochains mois.

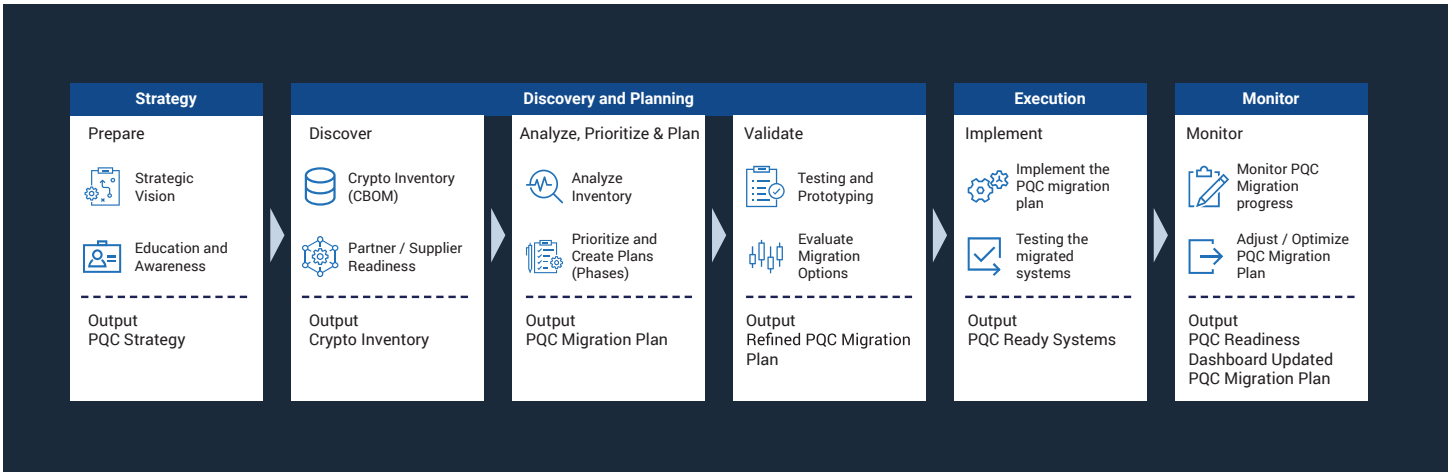
Se préparer à l’innovation résistante aux quanta

L’objectif de Dell n’est pas seulement d’aider les clients à se conformer aux normes émergentes, mais aussi de leur donner les moyens d’innover en toute sécurité à l’ère quantique. Qu’il s’agisse de déployer des charges applicatives d’IA, de gérer des environnements de Cloud hybride ou de moderniser leur infrastructure de périphérie, les clients peuvent avoir la certitude que les solutions Dell sont conçues dans un souci de résilience. La sécurité n’est pas pensée après la conception, mais intégrée à chaque niveau de la gamme Dell, permettant ainsi aux entreprises de gérer en toute confiance leur transition vers la cryptographie post-quantique.

Se préparer à la transition

La transition vers la cryptographie post-quantique sera l’un des changements d’infrastructure les plus importants depuis des décennies. Cette transition affecte presque tous les aspects de l’IT, des serveurs et du stockage aux terminaux, en passant par les plates-formes Cloud et les protocoles réseau. La réussite exige prévoyance, planification et exécution rigoureuse. Chez Dell Technologies, la voie à suivre prend la forme d’une transition progressive, qui assure l’équilibre entre des améliorations immédiates de la sécurité et une préparation à long terme pour l’adoption de la PQC.

Dell est prêt à vous aider à déployer votre stratégie d’implémentation de la PQC. Outre notre plan de migration progressive, nous avons défini un ensemble d’activités pour vous aider à élaborer des stratégies, planifier, exécuter et surveiller votre migration vers la PQC.



Préparer votre posture de sécurité dès aujourd'hui

Bonne hygiène de sécurité

La première étape de la préparation de l'avenir quantique consiste à renforcer les défenses déjà en place. Les entreprises doivent appliquer de strictes pratiques d'excellence en matière d'hygiène de sécurité, telles que l'application d'un accès du moindre privilège, la mise en œuvre d'une authentification multifacteur et la gestion rigoureuse des correctifs. Deux autres considérations sont également essentielles. Il peut être important de désactiver la cryptographie plus faible afin que les nouveaux systèmes dotés d'une cryptographie plus élevée puissent interagir avec les systèmes existants. Il est également important que la cryptographie symétrique, pour les systèmes plus récents, soit mise à niveau vers des longueurs de clé supérieures (AES-256 et SHA-384 ou supérieures) afin de contrer les marges réduites introduites par l'algorithme de Grover. Ces mesures réduisent non seulement les risques actuels, mais aussi le retard de dette cryptographique qui viendrait compliquer la migration future.

Actifs cryptographiques d'inventaire et d'audit

La visibilité est la pierre angulaire de tout plan de migration. Les entreprises doivent effectuer un inventaire cryptographique complet, en identifiant où et comment la cryptographie à clé publique est utilisée dans les applications, les périphériques et les workflows. Cela inclut les certificats TLS, les VPN, les systèmes de messagerie électronique, les mécanismes de signature de code et les données archivées. Une fois identifiés, les actifs doivent être hiérarchisés selon leur importance stratégique, leur sensibilité et leur durée de vie. Les données à long terme, telles que les dossiers médicaux ou les archives classifiées, doivent être traitées en priorité, car elles sont les plus vulnérables à la menace « Récolter maintenant, déchiffrer plus tard ».

Pilotage et expérimentation avec la PQC

Une fois le paysage cryptographique pleinement compris, les entreprises doivent commencer à tester les solutions de PQC dans des environnements contrôlés. En pilotant ces solutions dans des laboratoires, les équipes IT peuvent valider leurs performances, leur interopérabilité et leur facilité de gestion avant un déploiement à grande échelle. Développer cette agilité cryptographique (c'est-à-dire la possibilité de changer d'algorithmes cryptographiques sans remanier des systèmes entiers) est essentiel pour la résilience à long terme et la facilité de migration.

Adopter une approche d'interopérabilité

À mesure que les normes évoluent, un modèle hybride ouvre la voie vers l'avenir. De nombreux fournisseurs prennent déjà en charge des suites de chiffrement hybrides qui combinent des algorithmes classiques et résistants aux quanta en une seule implémentation. Cette double approche assure la continuité de la protection même si un algorithme est compromis par la suite. Dès maintenant, les entreprises doivent commencer à adopter des stratégies hybrides, tout en alignant leur calendrier interne sur les feuilles de route et les étapes de leur fournisseur d'infrastructure. À mesure que les algorithmes quantiquement sûrs sont standardisés, les entreprises peuvent ainsi faire évoluer leur adoption sans interruption.

Exécuter une migration complète et la validation continue

L'objectif ultime est une transition complète vers la PQC dans l'ensemble de l'entreprise. Il ne s'agira pas d'un événement ponctuel mais d'un processus continu de validation et d'adaptation. Les entreprises doivent mettre en œuvre des plans de migration détaillés, en intégrant la PQC dans chaque couche de leur infrastructure IT, tout en testant continuellement les nouvelles normes et mises en œuvre. À l'aide de laboratoires hybrides « quantiques-classiques », les clients peuvent simuler des scénarios d'attaque, valider l'intégrité cryptographique et s'assurer que leurs systèmes restent résistants aux menaces en constante évolution.

Collaboration et partage des connaissances

Aucune entreprise ne doit relever ce défi seule. Des consortiums industriels, des chercheurs universitaires et des organismes gouvernementaux mutualisent leurs connaissances pour accélérer la transition vers la PQC. La participation à des groupes de normalisation, des groupes de travail et des programmes pilotes permet aux entreprises de rester alignées sur les meilleures pratiques et les exigences émergentes. L'implication active de Dell dans des initiatives telles que le projet PQC du NIST NCCoE garantit que nos clients bénéficient directement de cette expertise collective.

Se préparer à la PQC est un effort sur le long terme. En adoptant une approche progressive (renforcement des défenses actuelles, audit des actifs cryptographiques, pilotage de la PQC, adoption de stratégies hybrides et exécution d'une migration complète), les entreprises évoluent en toute confiance vers la résilience quantique. Avec Dell en tant que partenaire, ce parcours n'est pas seulement réalisable : il constitue une opportunité de renforcer la confiance et de favoriser l'innovation pour l'avenir.

Applications et avantages concrets

La transition vers la cryptographie post-quantique est plus qu'un simple exercice de conformité, mais un impératif commercial qui a un impact direct sur la confiance, la résilience et la compétitivité à long terme. Pour les compagnies de télécommunications, les institutions financières, les établissements de santé et les administrations publiques, l'adoption d'algorithmes résistants aux quanta garantit la sécurité de l'infrastructure numérique stratégique contre les menaces actuelles et futures.

Télécommunications

Les réseaux de télécommunications sont l'épine dorsale de la numérisation mondiale. Ces réseaux sont à la base de tout, des services d'urgence à la connectivité IoT, en passant par les communications sécurisées avec les clients. Une faille quantique dans ce secteur pourrait compromettre le processus de provisionnement des cartes SIM, l'intégration des eSIM ou les mécanismes d'authentification qui sous-tendent les réseaux 4G et 5G. En déployant dès maintenant la cryptographie hybride et quantiquement sûre, les opérateurs peuvent maintenir la confiance des clients, protéger la confidentialité des données et assurer une continuité de service transparente à travers les générations de technologies mobiles.

Services financiers

L'industrie financière est l'une des cibles privilégiées des cyberadversaires, et l'intégrité des transactions repose sur la cryptographie. La préparation post-quantique protège les paiements numériques, les opérations bancaires en ligne et les virements interbancaires contre les fraudes quantiques. L'adoption précoce rassure également les organismes de réglementation et les clients sur le fait que les institutions s'engagent à protéger leurs actifs et à maintenir une stabilité systémique. La pérennisation de la cryptographie, dans ce secteur, réduit à la fois l'exposition aux réglementations et le risque réputationnel.

Services de santé

Dossiers des patients, données génomiques et appareils médicaux connectés sont tous exposés aux attaques « Récoler maintenant, déchiffrer plus tard ». Le secteur de la santé est confronté à un défi supplémentaire : les longues périodes de conservation requises pour les données médicales sensibles. En entamant leur transition vers la PQC dès aujourd'hui, les hôpitaux et les prestataires de soins veillent à ce que les dossiers médicaux restent confidentiels aujourd'hui et sur de longues décennies. Cela est essentiel pour préserver la confiance des patients tout en respectant l'évolution des réglementations en matière de protection des données.

Services publics et infrastructures essentielles

Des communications de défense aux systèmes de distribution d'énergie, les gouvernements et les opérateurs d'infrastructure s'appuient sur la cryptographie pour assurer la continuité des opérations et la sécurité nationale. La cryptographie post-quantique protège non seulement contre les adversaires à court terme, mais également contre la collecte stratégique de communications chiffrées pour une exploitation future. L'alignement avec des cadres tels que la CNSA 2.0 garantit que les systèmes gouvernementaux restent interopérables, sécurisés et fiables à l'ère quantique.

Avantages commerciaux accrus

Évidente d'un point de vue technique, la PQC offre également une solide valeur ajoutée :

- Réputation et confiance vis-à-vis de la marque : fait preuve de leadership dans la protection des données des clients et des partenaires.
- Conformité réglementaire : est conforme aux normes NIST et aux directives gouvernementales telles que la CNSA 2.0.
- Résilience opérationnelle : réduit le risque de pannes catastrophiques causées par une cryptographie défaillante.
- Différenciation concurrentielle : positionne les entreprises comme des innovateurs proactifs plutôt que comme des suiveurs réactifs.

Agir maintenant, ce n'est pas simplement faire preuve de résilience technique : les entreprises qui adoptent la PQC à un stade précoce non seulement réduiront les risques, mais renforceront également leur capacité à innover, à se conformer et à être compétitives dans une économie numérique qui repose sur la confiance.

Passer aux étapes suivantes

L'arrivée de l'informatique quantique représente à la fois une opportunité générationnelle et un défi de sécurité sans précédent. Même si le calendrier précis des ordinateurs quantiques cryptographiquement pertinents reste flou, une chose est sûre : la préparation exige un effort certain. La transition vers la cryptographie post-quantique nécessitera des années de planification, d'investissement et d'exécution coordonnés. Attendre que les ordinateurs quantiques soient opérationnels n'est pas une option réaliste.

La première étape, pour toute entreprise, consiste à comprendre où et comment la cryptographie est utilisée dans son environnement. À partir de là, les entreprises doivent commencer à inventorier, hiérarchiser et piloter des solutions quantiquement sûres. La cryptographie hybride (combinant des algorithmes classiques et post-quantiques) offre une voie immédiate vers la résilience, à l'heure où les normes ne cessent d'évoluer. En alignant les feuilles de route internes sur des cadres internationaux tels que les normes PQC du NIST et les échéances de la CNSA 2.0, les organisations peuvent progresser en toute confiance vers la conformité et l'interopérabilité.

Dell Technologies s'engage à aider ses clients à gérer cette transition. Grâce à notre approche, nous fournissons les bases de l'intégrité de la chaîne logistique, des protections matérielles intégrées et une adaptabilité logicielle. Nos partenariats avec des fournisseurs de sécurité de premier plan et notre rôle actif au sein des organismes de normalisation du secteur garantissent que les solutions Dell sont alignées sur les dernières exigences, mais également testées pour garantir des performances et une interopérabilité réelles.

Préparez-vous dès aujourd'hui. Commencez par la découverte et l'analyse des risques, faites appel à des fournisseurs de confiance et testez des technologies quantiquement sûres. Toutes les mesures prises aujourd'hui réduiront le risque de perturbation demain. Non seulement les entreprises qui agissent tôt sécuriseront leurs données et systèmes, mais gagneront également la confiance des clients, des organismes de réglementation et des partenaires, à une époque où la confiance numérique est primordiale.

À propos de nous

Dell Technologies s'engage à rendre les technologies avancées accessibles, fiables et habilitantes pour tous. Nous aidons les personnes et les organisations à tirer parti de l'innovation en toute sécurité, pour un avenir plus sûr, plus inclusif et plus connecté.