Informationsdokument

Postkvantumkryptografi: Förberedelser för kvanteran

Informationsdokument från Dell Technologies

Innehållsförteckning

Översikt

Kvantberäkningar utvecklas snabbt från teoretisk forskning till praktisk verklighet. Tack vare framsteg inom hårdvara, algoritmer och investeringar är det som en gång sågs som avlägset snart här, med maskiner som kan lösa problem som klassiska datorer inte klarar. Konsekvenserna för branschen är stora. Kvantdatorer kommer att möjliggöra innovationer som tidigare var utom räckhåll, inom allt från läkemedelsutveckling till klimatmodellering och global logistik.

Men det här genombrottet medför en betydande utmaning: Kvantdatorer kommer att underminera de kryptografiska grunder som skyddar den digitala ekonomin. Kryptografi med offentlig nyckel – algoritmer som RSA och kryptografi med elliptiska kurvor (ECC) – har skyddat digital kommunikation, finansiella system, patientjournaler och nationell säkerhet i årtionden. De här metoderna förlitar sig på matematiska problem som är svårlösta för klassiska datorer. Men med kryptografiskt relevanta kvantdatorer (CRQC) kan sådana problem lösas effektivt, vilket gör dagens säkerhet föråldrad.

Hotet är inte teoretiskt. Vissa angripare använder redan en taktik som kallas ”skörda nu, dekryptera senare” (HNDL – harvest now, decrypt later), där de samlar in krypterade data idag i väntan på att kunna dekryptera dem när kvantdatorerna blir tillräckligt kraftfulla. Känslig information som upplevs säker nu kan vara sårbar om bara några år. Det gäller att agera idag, och inte när CRQC-datorerna redan är här.

Det här informationsdokumentet förklarar hur brådskande kvanthotet är, utforskar det framväxande fältet för postkvantumkryptografi (PQC) och ser närmare på hur organisationer kan förbereda sig. Det belyser Dell Technologies satsningar på att bygga en kvantsäker framtid – och införliva säkerhet i hela vår leveranskedja, hårdvara, fasta mjukvara, mjukvara och vårt partnerekosystem – genom att anpassa verksamheten efter NIST:s standarder för postkvantumkryptografi (PQC) – FIPS 203, FIPS 204 och FIPS 205 – och Commercial National Security Algorithm Suite 2.0-riktlinjerna (CNSA 2.0). Dell har ett tydligt mål: att se till att innovationsarbetet kan fortsätta utan att äventyra säkerhet eller förtroende.

Termer

I det här dokumentet kommer du att stöta på ett antal termer. Här förklarar vi några av dem så att dokumentet ska vara lättare att förstå.

Postkvantumkryptografi – En ny matematisk metod för kryptografi, med nya algoritmer som ska vara säkra mot attacker från kvantdatorer. Algoritmerna körs på klassiska datorer och är motståndskraftiga mot både kvantattacker och kända klassiska kryptografiattacker.

Kvantresilient – Kvantresilient avser system, algoritmer eller infrastrukturer som är utformade för att vara motståndskraftiga och förbli säkra även vid angrepp från kryptografiskt relevanta kvantdatorer (CRQC-datorer). Ett kvantresilient system använder postkvantumkryptografi (PQC) eller andra skydd som står emot både klassiska attacker och kvantattacker, vilket säkerställer datasekretess, -integritet och -autenticitet långt in i framtiden. Andra termer som kvantresilient och kvantsäker används också med samma innebörd.

Kryptografisk agilitet (kryptoagilitet) – Förmågan hos en organisations system och applikationer att snabbt och smidigt byta kryptografiska algoritmer, protokoll eller nyckellängder utan att det behövs stora omarbetningar eller driftstörningar.

”Skörda nu, dekryptera senare” (HNDL, harvest now, decrypt later) – Kallas även ”record now, decrypt later” och innebär att angripare samlar in och lagrar krypterade data idag med avsikt att dekryptera dem i framtiden när kryptografiskt relevanta kvantdatorer (CRQC) finns tillgängliga.

Kvantdatorer och hotet mot kryptering

Kvantdatorernas framväxt

Som vi beskrev i vårt blogginlägg Post-Quantum Cryptography: A Strategic Imperative for Enterprise Resilience som vår CTO John Roese skrev för nästan ett år sedan, bearbetar klassiska datorer (i bärbara datorer, smartphones, servrar osv.) information med hjälp av bitar, som är antingen nollor eller ettor. Den här binära modellen har drivit årtionden av framsteg, men den begränsar hur information kan representeras och manipuleras. Kvantdatorer använder kvantbitar (qubits), som kan representera flera tillstånd samtidigt genom principer som superposition och sammanflätning. Det gör det möjligt för kvantdatorer att utforska ett stort antal möjliga lösningar parallellt, vilket medför en beräkningsfördel för vissa typer av problem.

Kvantdatorernas potentiella tillämpningar är extraordinära. Forskare förutser genombrott inom läkemedel genom simulering av molekylära interaktioner med en precision som klassiska datorer inte kan uppnå. Klimatforskare föreställer sig mer exakta modeller av globala system, medan energisektorn ser potential att optimera elnät och energilagring. Även inom logistik och tillverkning kan man dra nytta av kvantoptimeringstekniker. Fördelarna är reella och inom räckhåll – men det gäller även riskerna.

Därför är kryptering i riskzonen

Kryptering utgör grunden för förtroendet i den digitala tidsåldern. När du anger ett kreditkortsnummer, loggar in på en säker webbplats eller tar emot en signerad mjukvaruuppdatering säkerställs sekretess, autenticitet och integritet genom kryptering. För större delen av skyddet används kryptografi med offentlig nyckel – algoritmer som RSA och ECC som baseras på matematiska problem som anses vara omöjliga att beräkna för klassiska datorer.

Med kvantdatorer förändras denna ekvation. Med **Shors algoritm** kan en tillräckligt kraftfull kvantdator lösa de problem med faktorisering och diskreta logaritmer som gör RSA och ECC så kraftfulla. CRQC-datorer kommer att kunna äventyra digitala signaturer som skyddar mjukvaruuppdateringar, nycklar som upprättar TLS-sessioner och certifikat som autentiserar enheter. Effekten är systemisk och hotar just de mekanismer som gör digitala transaktioner säkra.

Symmetrisk kryptografi – algoritmer som AES som används för att skydda lagrade data eller säker kommunikation – står inför en annan, men mindre allvarlig, utmaning. **Grovers algoritm** gör det möjligt för en kvantdator att minska symmetriska nycklars effektiva styrka på ett sätt som halverar deras säkerhet. Även om detta kan mildras genom en övergång till större nyckelstorlekar som AES-256, understryker justeringen hur genomgripande kvanthoten är.

Brådska och konsekvenser

Konsekvenserna sträcker sig långt bortom teoretiska risker. Om organisationer misslyckas med att förbereda sig riskeras exponering av känslig immateriell egendom, störningar i finansiella system, intrång i hälso- och sjukvårdsdata och hot mot den nationella säkerheten. Strategin ”skörda nu, dekryptera senare” gör läget ännu mer brådskande: Angripare behöver bara samla in krypterade data idag och vänta på att de ska kunna dekryptera dem. När CRQC-datorerna är här är skadan redan oåterkallelig.

Postkvantumkryptografi och kommande standarder

Definition av postkvantumkryptografi

Postkvantumkryptografi (PQC) avser en ny generation algoritmer som utformats för att skydda digitala system mot både klassiska angrepp och kvantattacker. Till skillnad från kvantnyckeldistribution, som kräver specialiserad hårdvara, är PQC utformat för att köras på dagens klassiska infrastruktur – servrar, slutpunkter, nätverk – och är därför det mest praktiska och skalbara sättet att förbereda sig för kvanteran.

Grunden till PQC är en uppsättning matematiska problem som, så vitt vi vet, står emot kvantteknik som Shors och Grovers algoritmer. Gitterbaserad kryptografi, hash-baserade signaturer, kodbaserade scheman och multivariata ekvationer är de mest lovande metoderna. De testas noga och standardiseras för att säkerställa att de ger samma tillförlitlighet och interoperabilitet som RSA och ECC en gång gjorde.

Det globala standardiseringsarbetet – kommande branschstandarder

Eftersom hotet är så brådskande har regeringar och standardiseringsorgan gjort PQC till en global prioritet. U.S. National Institute of Standards and Technology (NIST) lanserade sitt PQC-projekt 2016 och uppmanade då forskare inom kryptografi att föreslå, analysera och förfina möjliga algoritmer. Efter flera års tester presenterade NIST den första gruppen av standardiserade algoritmer i augusti 2024:

- **CRYSTALS –**Kyber för kryptering med offentlig nyckel och nyckeletablering
- **CRYSTALS –**Dilithium och SPHINCS+ för digitala signaturer

Ytterligare algoritmer undersöks fortfarande för att tillhandahålla mångfald och flexibilitet för olika implementeringsbehov, inklusive lätta system som inbyggd fast mjukvara. Genom den fortlöpande standardiseringsprocessen kan organisationer i hela världen få en tydlig plan för införandet av kvantresistenta lösningar.

NIST-standarder – FIPS 203, 204, 205

I augusti 2024 slutförde U.S. National Institute of Standards and Technology (NIST) de första PQC-algoritmerna:

- FIPS 203 (ML-KEM) – baserat på CRYSTALS-Kyber, en nyckelinkapslingsmekanism. Tillhandahåller IND-CCA2-säkerhet, vilket innebär att chiffertexter förblir oskiljbara även vid adaptiva attacker med vald chiffertext.
- FIPS 204 (ML-DSA) – baserat på CRYSTALS-Dilithium, en algoritm för digitala signaturer. Ger stark EUF-CMA-säkerhet (existentiell oförfalskbarhet under attacker med valda meddelanden), vilket är standardkravet för digitala signaturer.
- FIPS 205 (SLH-DSA) – baserat på SPHINCS+, ett hash-baserat signatursystem. Valt som en konservativ reservlösning som inte är beroende av gitterproblem.

En nödvändig handlingsplan

USA:s federala regering inser vikten av att införa kvantresistenta krypteringsalgoritmer och har börjat utfärda PQC-krav till federala myndigheter. Det inbegriper bland annat 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 och Office of Management and Budget Memorandum 23-02 (OMB M-2302).

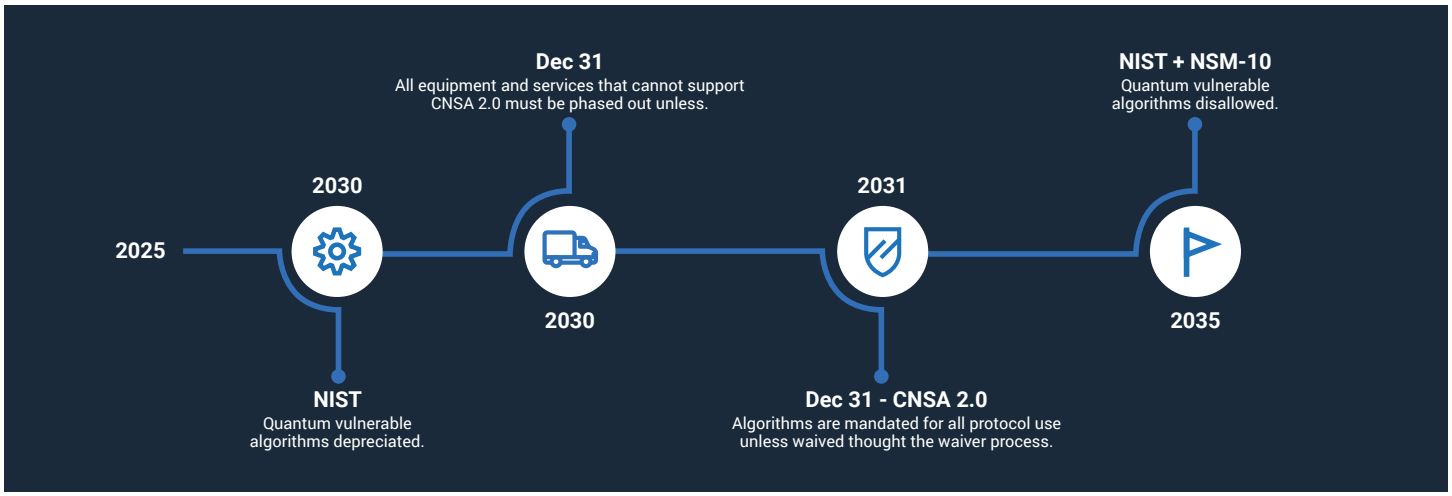
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

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

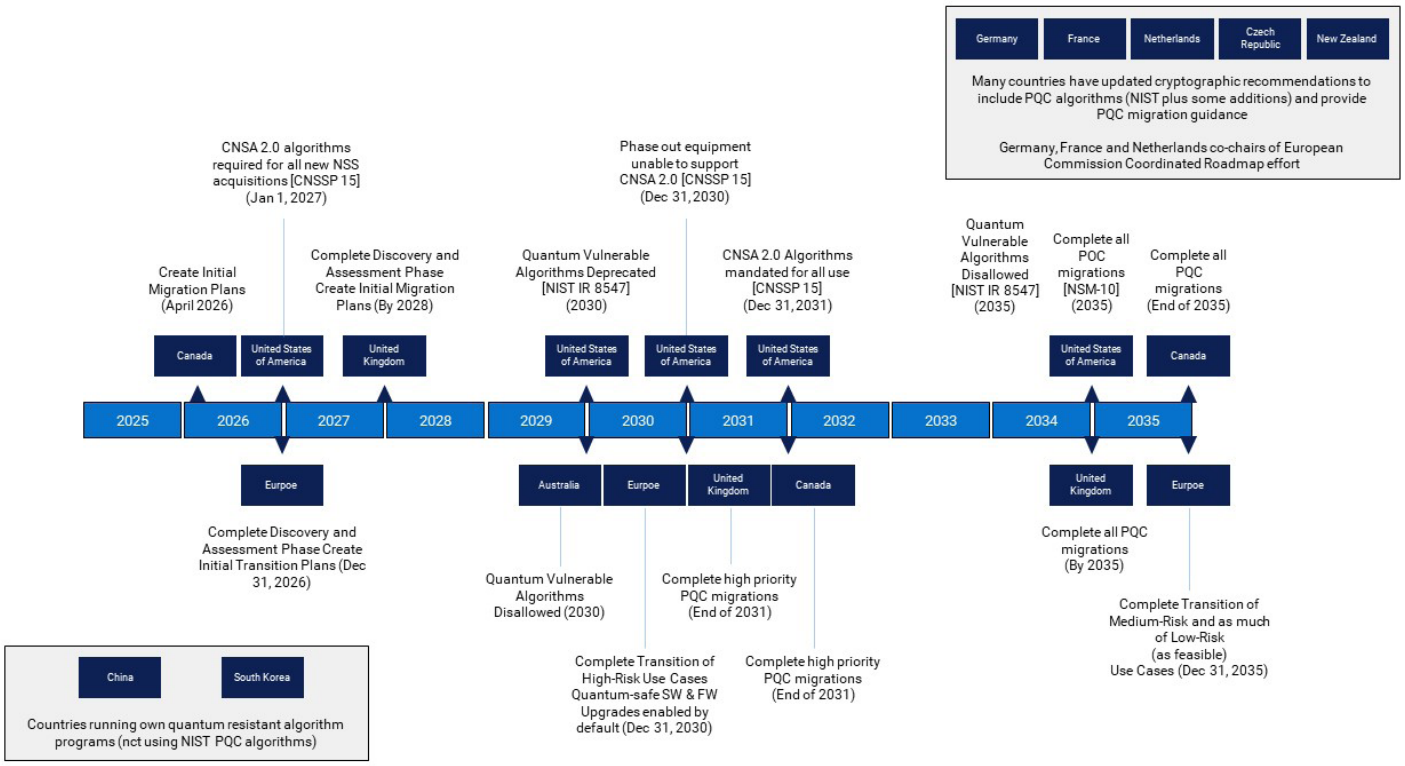
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

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

Med CNSA 2.0, som tillkännagavs av NSA i september 2022, introduceras de första rekommendationerna för postkvantumkryptografiska algoritmer. CNSA 2.0 fastställer tydliga tidsfrister för införandet av kvantresistenta algoritmer i National Security Systems (NSS), och fungerar som vägledning för företag som förbereder sina egna övergångar:



Andra organisationer runt om i världen har också utarbetat riktlinjer för PQC-övergången. Här nedan anges några av de olika landskraven.



De här datumen är inte slumpmässiga – de återspeglar de ledtider som krävs för att omarbeta, validera och distribuera kryptografi i komplexa IT-ekosystem. Företag bör inte betrakta dem som enbart myndighetskrav, utan som praktiska indikatorer på den globala övergången mot kvantresiliens.

Branschsamarbete

Utöver NIST och NSA påverkar och deltar Dell aktivt i branschkonsortier och standardgrupper som arbetar för interoperabilitet och implementering. Trusted Computing Group integrerar postkvantumkryptografi i TPM-standarden (Trusted Platform Module). IETF driver mycket av arbetet med att integrera PQC-algoritmerna i branschprotokoll, till exempel TLS- och X.509-certifikat. OASIS-kommittéerna för Key Management Interoperability Protocol (KMIP) möjliggör användning av PQC inom nyckelhanteringsramverk. FIDO Alliance studerar PQC-teknikens inverkan på standarder för autentisering och enhetsregistrering, medan organisationer som SAFECode arbetar med att utbilda branschen om migreringsberedskap.

NIST National Cyber Security Center of Excellence (NCCoE) är en struktur som gör det möjligt för NIST att arbeta med industrin, den akademiska världen och myndigheter genom domänfokuserade projekt. De har fokuserat på ett antal saker, till exempel:

- Kryptografisk identifiering – Identifiera vilken kryptografi som behöver migreras och hur man prioriterar vad som ska migreras först.
- Interoperabilitet – Säkerställa att populära kryptografiska funktioner och protokoll införlivar de nya PQC-algoritmerna och att implementeringar från olika leverantörer fungerar tillsammans.
- Kryptoagilitet – Fokusera på att utveckla informationssystem som uppmuntrar stöd för snabba anpassningar av nya kryptografiska primitiver och algoritmer utan att göra genomgripande ändringar av systemets infrastruktur. Kallas även kryptografisk agilitet.

De här projekten bidrar till att utforma och utveckla de riktlinjer och standarder som skapas, och hjälper till att säkerställa att det finns exempel på branschlösningar för de standarder och riktlinjer som tillhandahålls. Dell har deltagit i NCCoE Migration to PQC-projektet sedan starten.

Idag är PQC inte bara ett forskningsämne – det är en standard under utveckling med konkreta algoritmer, tidslinjer och implementeringsvägar. Organisationer som börjar förbereda sig nu kan undvika de kostnader, störningar och risker som uppstår vid en sista-minuten-satsning. Övergången handlar inte bara om överensstämmelse, utan om att säkerställa intakt förtroende, sekretess och integritet när kvantdatorer omformar det digitala landskapet.

Därför är det hög tid att agera

Hotets omedelbara natur

Det kan vara frestande att se kvantdatorer som en avlägsen risk, något som kan åtgärdas när tekniken är fullt utvecklad. I verkligheten har klockan redan börjat ticka. Känslig information – finansiella transaktioner, patientjournaler, immateriella tillgångar eller myndighetskommunikation – kan vara säkert krypterad idag, men när kvantdatorer når kapacitet att knäcka RSA eller ECC kan dessa data exponeras i efterhand. Det innebär att en mängd historiska meddelanden och register plötsligt kan vara i fara.

Långa teknikcykler

Det är varken snabbt eller enkelt att ändra moderna IT-ekosystem. Historiskt har byten av enstaka algoritmer, till exempel övergången från SHA-1 till SHA-2 eller DES/3DES till AES, tagit över 10 år att slutföra. Algoritmerna är djupt inbäddade i operativsystem, applikationer, nätverksenheter och hårdvara. För att ersätta dem krävs omarbetning, validering, testning och distribution i miljöer som sträcker sig från datacenter till molnplattformar och kantenheter. För många organisationer kommer detta att ta flera år – betydligt längre tid än vad som återstår innan kvantdatorer utgör ett verkligt hot. Det är därför tillsynsmyndigheter, standardiseringsorgan och säkerhetsledare betonar vikten av omedelbara förberedelser. Att vänta tills CRQC-datorer är allmänt tillgängliga lämnar ingen tid för en ordnad övergång.

Risker med passivitet

Konsekvenserna av att fördröja migreringen går långt bortom teknisk exponering:

- Datasäkerhetsrisk: Långlivade data som patientjournaler, finansiella register eller försvarsrelaterad information kan kompromitteras retroaktivt när kvantdatorerna mognar.
- Risk för mjukvarans äkthet och integritet: Mjukvarans autenticitet och integritet kan äventyras av skadlig kod om den är signerad med dagens signeringsmetoder och fortfarande används när kvantdatorerna blir tillräckligt kraftfulla.
- Operativa risker: Kritiska infrastruktursystem – som el och vatten, transportnätverk och räddningstjänst – är kända för att vara svåra att uppgradera. Underlåtenhet att planera idag kan medföra driftstörningar senare.
- Regel- och efterlevnadsrisk: Ramverk som **CNSA 2.0** har fastställt tydliga tidsramar för efterlevnad. Organisationer som underlåter att förbereda sig riskerar inte bara exponering utan också bristande efterlevnad av myndighets- eller branschförväntningar.
- Risk för anseende och ekonomi: Ett intrång till följd av kryptografiska sårbarheter som inte åtgärdats kan leda till bestående skador på förtroendet för varumärket liksom betydande ekonomiska förluster.

Fördelarna med proaktiva åtgärder

Proaktiva förberedelser är inte bara ett defensivt drag, utan en möjlighet att stärka den långsiktiga motståndskraften. Genom att utföra kryptografiska inventeringar, uppgradera symmetriska nyckellängder, testa PQC-förberedda lösningar och samarbeta med leverantörer som erbjuder kvantresistenta produkter kan organisationer säkerställa kontinuerligt förtroende. Tidiga användare är bättre positionerade för att framtidssäkra driften, upprätthålla efterlevnad och visa prov på ledarskap för kunder, samarbetspartner och tillsynsmyndigheter.

Dells strategi för postkvantumkryptografi

På Dell anser vi att teknik driver mänskligheten framåt, och säkerhet är grunden för dessa framsteg. Som företag säkerställer Dell Technologies att dess portfölj, IT-infrastruktur och livscykelsupportsystem är väl förberedda för övergången till kvantresistenta algoritmer. Här är några exempel på åtgärder som vidtas för att förbereda övergången:

- Identifiera specifika områden och syften där kryptografi används i produkter, tjänster, IT-infrastruktur och supportsystem för att formulera omfattande övergångsplaner.
- Förbättra den interna kunskapen om postkvantumkryptografiska algoritmer (PQC), med hänsyn till implementeringsaspekter och designprinciper relaterade till kryptoagilitet för att underlätta en smidig övergång till PQC-algoritmer.
- Utvärdera prestanda, tillämplighet och lämplighet för PQC-algoritmer i olika användningsfall som är relevanta för Dell Technologies mångsidiga portfölj.

Med tanke på PQC-övergångens komplexitet kan uppgraderingar av kryptografiska användningsfall fasas in i Dell Technologies erbjudanden. Ur ett dataperspektiv prioriteras övergången för användningsfall som kan vara sårbara för ”skörda nu, dekryptera senare”-attacker, till exempel kryptering av in-flight data eller data vid vila.

När du ser över din teknikplattform kan övergången av ett kryptografiskt användningsfall innebära en fullständig produktförnyelse eller produktuppgradering. Det beror på produkten i fråga samt var och hur kryptografin är implementerad i produkten och i de omgivande systemen.

Lanseringen av kvantresistenta erbjudanden kommer att vara i fokus under de kommande fem åren och framåt, för att säkerställa att kunderna kan möta myndigheters och branschorganisationers tidslinjer för PQC-övergången som infaller mellan 2027 och 2035.

Kunder bör samarbeta med sitt Dell-kontoteam för att få produktspecifik information (t.ex. lanseringsplaner och tidslinjer) som kan införlivas i migreringsplanerna. Håll utkik – Dell kommer att utfärda mer specifika tidslinjer för PQC-integrering i sina produktlinjer och produkter under de kommande månaderna.

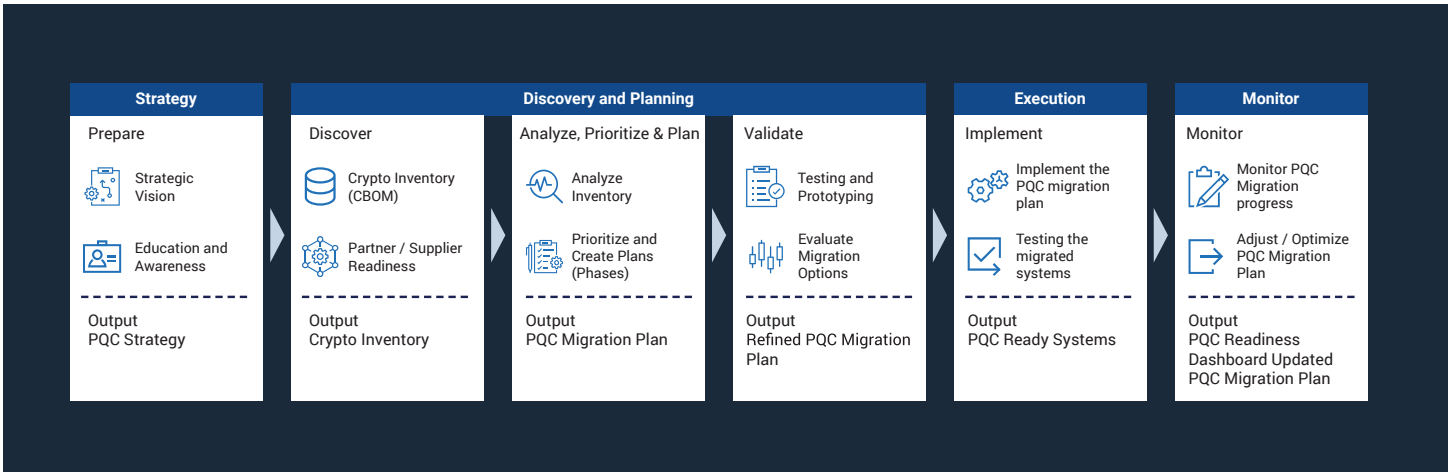
Förbereder för kvantresilient innovation

Dell har inte bara som mål att hjälpa kunder att följa nya standarder, utan också att ge dem möjlighet att arbeta innovativt på ett säkert sätt i kvanteran. Oavsett om de distribuerar AI-arbetsbelastningar, hanterar hybridmolnmiljöer eller moderniserar kantinfrastrukturen kan kunderna lita på att Dells lösningar är utformade med motståndskraft i åtanke. Säkerhet är inget som läggs till i efterhand, utan är inbyggt i varje lager av Dells portfölj så att organisationer kan hantera övergången till postkvantumkryptografi på ett tryggt sätt.

Förberedelser för övergången

Övergången till postkvantumkryptografi blir en av de största infrastrukturförändringarna på årtionden. Övergången berör nästan alla aspekter av IT, från servrar och lagring till slutpunkter, molnplattformar och nätverksprotokoll. För att lyckas krävs förutseende, planering och ett disciplinerat genomförande. På Dell Technologies ser vi vägen framåt som en stegvis resa, där omedelbara säkerhetsförbättringar balanseras med långsiktig beredskap för PQC-implementering.

Dell är redo att hjälpa dig med din strategi för implementering av PQC. Vi rekommenderar en fasad migreringsplan och vi har skisserat en uppsättning aktiviteter som hjälper dig att planera, genomföra och övervaka PQC-migreringen.



Förbereda dagens säkerhetsställning

God säkerhetshygien

Det första steget i att förbereda sig för kvantteknikens framtid är att stärka de försvar som redan finns på plats. Organisationer bör använda bästa praxis för säkerhetshygien, till exempel att tillämpa åtkomst med minsta behörighet, implementera multifaktorautentisering och upprätthålla strikt korrigeringshantering. Det finns två ytterligare aspekter att ta hänsyn till. Det kan vara viktigt att inaktivera svagare kryptografi så att nya system med mer kraftfull kryptografi kan interagera med äldre system. Det är också viktigt att symmetrisk kryptografi för nyare system uppgraderas till längre nyckellängder – AES-256 och SHA-384 eller högre – för att motverka de minskade marginaler som introduceras av Grovers algoritm. Åtgärderna minskar inte bara riskerna idag utan minimerar också den kryptografiska eftersläpning som annars skulle försvåra morgondagens migrering.

Inventera och granska kryptografiska tillgångar

Hörnstenen i alla migreringsplaner är insyn. Organisationer måste genomföra en omfattande kryptografisk inventering där man identifierar var och hur kryptografi med offentlig nyckel används i applikationer, enheter och arbetsflöden. Det inkluderar TLS-certifikat, VPN, mejlsystem, kodsigneringsmekanismer och arkiverade data. När tillgångarna har identifierats bör de prioriteras utifrån affärskritikalitet, känslighet och livslängd. Data med lång livslängd – som patientjournaler eller sekretessbelagda arkiv – bör behandlas med högsta prioritet, eftersom de är mest sårbara för ”skörda nu, dekryptera senare”-hotet.

Testa och experimentera med PQC

När det kryptografiska landskapet har kartlagts bör organisationer börja testa PQC-lösningar i kontrollerade miljöer. Genom att testa de här lösningarna i labb kan IT-teamen validera prestanda, interoperabilitet och hanterbarhet före storskalig distribution. Att bygga upp den här kryptoagiliteten – förmågan att byta kryptografiska algoritmer utan att göra om hela system – är avgörande för långsiktig motståndskraft och smidig migrering.

Anta en interoperabilitetsstrategi

Medan standarderna mognar erbjuder en hybridmodell en brygga till framtiden. Många leverantörer stöder redan hybridkrypteringssviter som kombinerar klassiska och kvantresistenta algoritmer i en enda implementering. En sådan dubbel strategi säkerställer kontinuerligt skydd även om en av algoritmerna senare komprometteras. Företag bör börja införa hybridstrategier nu och anpassa sina interna tidsplaner efter infrastrukturleverantörens produktplaner och milstolpar. På så sätt kan organisationer skala upp implementeringen utan störningar i takt med att kvantsäkra algoritmer når standardisering.

Utför fullständig migrering och kontinuerlig validering

Slutmålet är en fullständig övergång till postkvantumkryptografi (PQC) i hela företaget. Det är ingen engångshändelse utan en pågående validerings- och anpassningsprocess. Organisationer bör genomföra detaljerade migreringsplaner där PQC införlivas i varje lager av IT-stacken samtidigt som nya standarder och implementeringar testas löpande. Med hybridlabb som kombinerar klassisk och kvantbaserad teknik kan kunder simulera attackscenarier, validera kryptografisk integritet och säkerställa att deras system förblir motståndskraftiga mot nya hot.

Samarbete och kunskapsdelning

Slutligen bör ingen organisation stå ensam inför denna utmaning. Branschkonsortier, akademiska forskare och statliga myndigheter samlar sin kunskap för att påskynda PQC-övergången. Genom att delta i standardiseringsgrupper, arbetsgrupper och pilotprogram kan företag hålla jämna steg med bästa praxis och nya krav. Dells aktiva engagemang i initiativ som NIST NCCoE PQC-projektet säkerställer att våra kunder kan dra direkt nytta av denna samlade expertis.

Förberedelserna för PQC är ett maraton, inte ett sprintlopp. Genom att en fasad strategi – stärka dagens försvar, granska kryptografiska tillgångar, testa PQC, anta hybridstrategier och genomföra en fullständig migrering – kan organisationer tryggt övergå till kvantresiliens. Med Dell som partner är den här resan inte bara genomförbar utan också en möjlighet att stärka förtroendet och möjliggöra innovation långt in i framtiden.

Faktiska användningsområden och fördelar

Övergången till postkvantumkryptografi är mer än en fråga om efterlevnad – det är ett måste för företaget med direkt inverkan på förtroende, motståndskraft och långsiktig konkurrenskraft. För telekomleverantörer, finansinstitut, hälso- och sjukvårdsorganisationer och myndigheter säkerställer införandet av kvantresistenta algoritmer att kritisk digital infrastruktur förblir skyddad mot både dagens och framtidens hot.

Telekommunikation

Telekomnätverk är ryggraden i den globala digitaliseringen. De är nödvändiga inom allt från räddningstjänst och IoT-uppkoppling till säker kundkommunikation. Ett kvantintrång i den här sektorn skulle kunna kompromettera SIM-provisionering, eSIM-aktivering eller de autentiseringsprocesser som ligger till grund för 4G och 5G. Genom att driftsätta hybrida och kvantsäkra krypteringslösningar redan idag kan operatörer upprätthålla kundernas förtroende, skydda datasekretessen och säkerställa sömlös kontinuitet i tjänster över generationer av mobil teknik.

Finansiella tjänster

Finanssektorn är en av de mest utsatta för cyberattacker, och transaktionernas integritet är beroende av kryptografi. Genom postkvantberedskap skyddas digitala betalningar, internetbanktjänster och överföringar mellan banker mot kvantbaserat bedrägeri. Tidig implementering försäkrar också tillsynsmyndigheter och kunder om att institutioner är fast beslutna att skydda tillgångar och upprätthålla systemstabilitet. Framtidssäkrad kryptografi i den här sektorn minskar både regulatorisk exponering och risken för skadat anseende.

Hälso- och sjukvård

Patientjournaler, genomiska data och uppkopplade medicinska enheter är alla sårbara för ”skörda nu, dekryptera senare”-attacker. Hälso- och sjukvårdssektorn står inför ytterligare en utmaning: de långa lagringsperioder som krävs för känsliga medicinska data. Genom att påbörja övergången till PQC idag säkerställer sjukhus och leverantörer att patientjournaler förblir privata inte bara idag, utan flera årtionden in i framtiden. Det är avgörande för att bevara patientförtroendet och samtidigt möta föränderliga dataskyddsbestämmelser.

Myndigheter och kritisk infrastruktur

Från försvarskommunikation till energidistributionssystem förlitar sig myndigheter och infrastrukturoperatörer på kryptografi för kontinuerlig drift och nationell säkerhet. Postkvantumkryptografi skyddar inte bara mot angripare i närtid utan också mot strategisk insamling av krypterad kommunikation för framtida exploatering. Genom anpassning till ramverk som CNSA 2.0 kan statliga system förblir kompatibla, säkra och betrodda i kvanteran.

Bredare affärsfördelar

Det tekniska behovet av PQC är tydligt, och affärsargumentet är lika starkt:

- Förtroende och varumärkets anseende: Visar på ledarskap när det gäller att skydda kund- och partnerdata.
- Regelefterlevnad: Efterlever NIST-standarder och myndighetsmandat som CNSA 2.0.
- Motståndskraftig drift: Minskar risken för katastrofala driftstopp orsakade av knäckt kryptering.
- Konkurrenskraftig differentiering: Positionerar organisationer som proaktiva innovatörer snarare än reaktiva följare.

Fördelarna med att agera nu sträcker sig långt bortom teknisk motståndskraft. Organisationer som anammar PQC tidigt minskar inte bara riskerna utan stärker sin förmåga att arbeta innovativt, följa regelverk och konkurrera i en digital ekonomi där förtroende är helt avgörande.

Ta nästa steg

Framväxten av kvantdatorer innebär både en enorm möjlighet och en aldrig tidigare skådad säkerhetsutmaning. Den exakta tidslinjen för kryptografiskt relevanta kvantdatorer är visserligen fortfarande osäker, men vi vet att det krävs omfattande förberedelser. Övergången till postkvantumkryptografi kommer att ta år av samordnad planering, investeringar och genomförande. Det är inte ett praktiskt alternativ att vänta tills kvantdatorer är i drift.

Det första steget för varje organisation är medvetenhet – att förstå var och hur kryptografi används i deras miljö. Därifrån måste företag påbörja processen med att inventera, prioritera och testa kvantsäkra lösningar. Hybridkryptografi – som kombinerar klassiska algoritmer och postkvantalgoritmer – erbjuder en omedelbar väg till motståndskraft medan standarderna fortsätter att utvecklas. Genom att anpassa interna handlingsplaner till globala ramverk som NIST:s PQC-standarder och CNSA 2.0-tidslinjer kan organisationer gå mot efterlevnad och interoperabilitet med tillförsikt.

Dell Technologies strävar efter att hjälpa kunderna att hantera övergången på bästa sätt. Med vår strategi erbjuder vi en grund som säkerställer leverantörskedjans integritet, hårdvaruinbäddade skyddsmekanismer och mjukvarubaserad anpassningsförmåga. Våra samarbeten med ledande säkerhetsleverantörer och vår aktiva roll i branschstandardorgan säkerställer att Dells lösningar inte bara uppfyller de senaste kraven utan även är testade för prestanda och interoperabilitet i verkliga världen.

Påbörja förberedelserna idag. Börja med identifiering och riskanalys, samarbeta med betrodda leverantörer och testa kvantsäker teknik. Varje steg som tas nu minskar risken för störningar i morgon. Organisationer som agerar tidigt skyddar inte bara sina data och system utan kommer också att vinna kunders, tillsynsmyndigheters och partners förtroende i en tid då digitalt förtroende är oumbärligt.

Om oss

Dell Technologies strävar efter att göra avancerad teknik tillgänglig, tillförlitlig och möjliggörande för alla. Vi hjälper människor och organisationer att dra nytta av innovation på ett säkert sätt och visar vägen mot en säkrare, mer inkluderande och uppkopplad framtid.