DELL Technologies

포스트 양자 암호화

시작하기

소개

양자 컴퓨팅은 근본적인 기술 재설계를 주도하여 엄청난 기회를 발굴하는 동시에 새로운 당면 과제도 마주하고 있습니다. 양자 컴퓨팅의 미래는 흥미롭지만 디지털 세상을 보호하는 암호화 시스템에 심각한 위협을 초래합니다.

양자 컴퓨팅이 부상하는 이유는 무엇입니까?

노트북, 스마트폰 또는 서버 등에 위치한 클래식 컴퓨터는 비트를 사용하여 정보를 처리하고, 이 비트는 0 또는 1의 상태로 존재합니다. 이 바이너리 모델은 수십 년에 걸친 발전을 이끌었지만 정보를 표현하고 조작하는 방법을 제한합니다. 양자 컴퓨터는 중첩 및 얽힘과 같은 원리를 통해 동시에 여러 상태로 존재할 수 있는 큐비트를 사용합니다. 이를 통해 양자 머신은 방대한 수의 가능한 솔루션을 병렬로 탐색할 수 있으며 특정 유형의 문제에 대한 컴퓨팅 이점을 제공합니다.

포스트 양자 암호화란 무엇입니까?

PQC(Post-Quantum Cryptography)는 디지털 시스템을 고전적 공격 및 양자 공격 모두로부터 보호하도록 설계된 새로운 세대의 알고리듬을 의미합니다. 특수 하드웨어가 필요한 양자 키 배포와 달리 PQC는 서버, 엔드포인트, 네트워크와 같은 오늘날의 기존 인프라스트럭처에서 실행되도록 설계되어 양자 시대에 대비하는 가장 실용적이고 확장 가능한 방법입니다.

조직이 양자 컴퓨팅으로 인해 직면하는 즉각적인 위험은 무엇입니까?

그 결과는 이론적 위험을 훨씬 넘어섭니다. 대비하지 못하는 조직은 기밀 지적 재산 노출, 금융 시스템 붕괴, 의료 데이터 침해, 국가 안보에 대한 위협에 직면하게 됩니다.

"Harvest Now, Decrypt Later" 전략은 이러한 시급성을 더욱 가중시킵니다. 공격자는 암호화된 데이터를 캡처해 두었다가 나중에 복호화 수단이 확보된 순간 복호화하면 되기 때문입니다. 암호학적으로 유의미한 양자 컴퓨터의 시대가 도래할 때면 이미 피해를 되돌릴 수 없을 것입니다.

"Harvest Now, Decrypt Later" - "Record Now, Decrypt Later"라고도 하며, 향후 암호학적으로 유의미한 양자 컴퓨터를 사용할 수 있게 되면 암호 해독을 목적으로 암호화된 데이터를 수집하고 저장하는 공격자의 행위입니다.

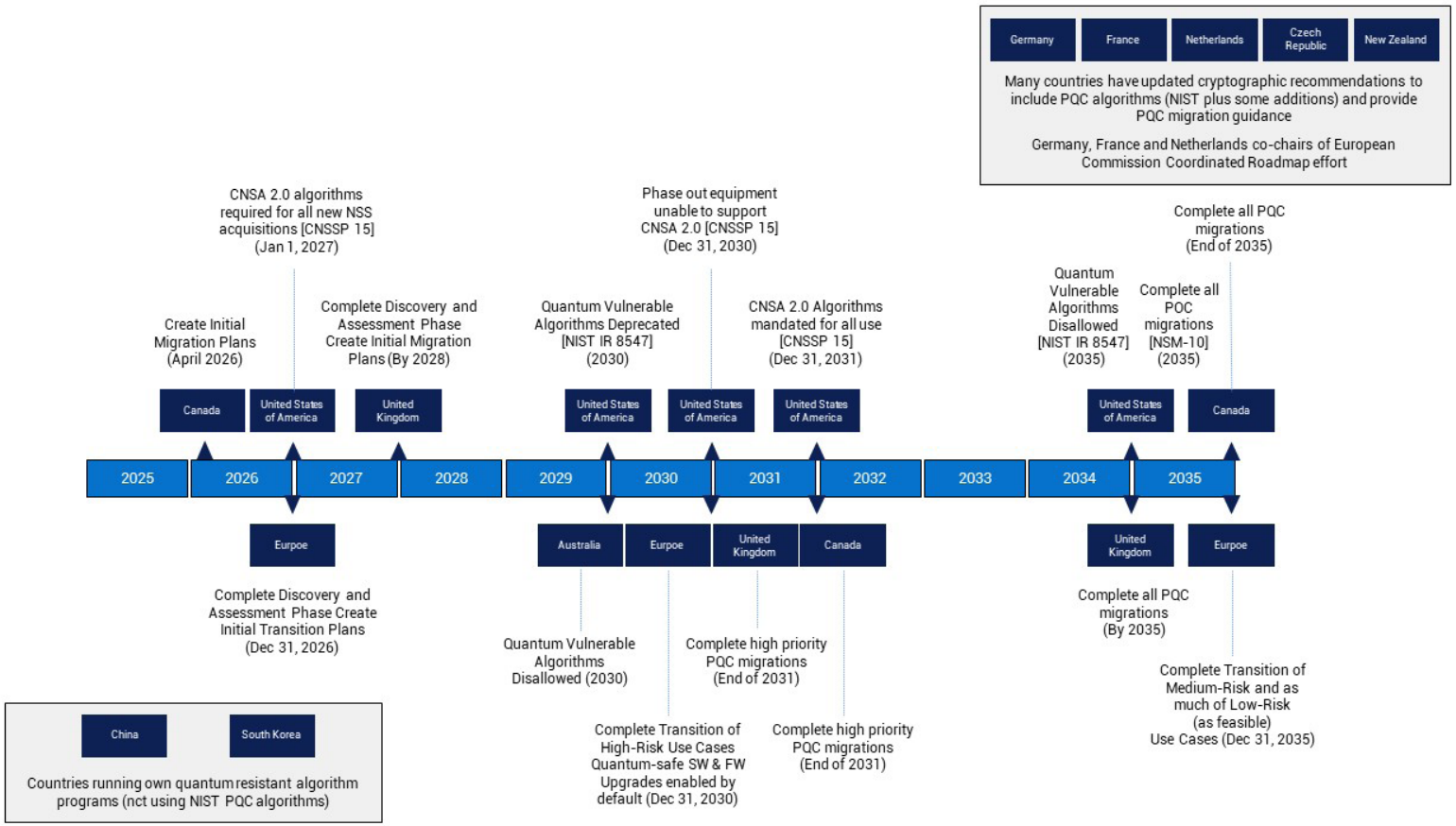
조직은 어떻게 PQC로의 전환을 준비해야 합니까?

양자 시대에도 안전한 미래를 향한 여정은 단거리 경기가 아닌 마라톤과 같으며, 계속해서 진화하는 여정입니다. 사전 예방적이고 계층화된 단계적 접근 방식은 조직이 위험을 관리하고, 리소스를 조정하고, 장기적으로 회복탄력성이 뛰어난 보안 태세를 구축하는 데 도움이 됩니다. Dell은 모든 단계에서 고객을 지원하는 기술과 지침을 제공합니다. 조직의 PQC 전환 계획 수립을 안내하는 주요 단계입니다.

PQC 전환 일정

위협의 시급성을 인식한 정부와 표준 기관은 PQC를 전 세계적인 우선순위로 삼았습니다. 미국 연방 정부는 양자 내성 암호화 알고리듬 채택의 중요성을 깨닫고 여러 연방 기구에 PQC 요구 사항을 제시하기 시작했습니다. 여기에는 NSM-10(National Security Memorandum 10), CNSA 2.0(Commercial National Security Algorithm Suite), OMB M-2302(Office of Management and Budget Memorandum 23-02), NIST IR 8547(National Institute of Standards and Technology Interagency Report 8547) 등이 있습니다.

전 세계의 다른 조직도 PQC 전환에 대한 지침을 설정했습니다. 이러한 날짜는 임의적인 것이 아니며, 복잡한 IT 생태계 전반에 걸쳐 암호화를 재설계, 검증 및 배포하는 데 필요한 리드 타임을 반영합니다. 기업은 이를 정부에서 부과하는 의무 이상의 것으로 간주해야 하며, 이는 양자 회복탄력성을 향한 전 세계적 변화의 실질적인 지표입니다. 아래는 국가별 규정 중 일부입니다.



암호화 관련 위협의 인벤토리 및 감사

첫 번째 우선 과제는 현재의 암호화 환경을 이해하는 것입니다. 이 기본 단계를 통해 전체 마이그레이션 전략과 관련된 정보를 얻을 수 있습니다.

우수한 보안 태세

양자 미래에 대비하는 첫 번째 단계는 이미 구축된 보안 태세를 강화하는 것입니다. 조직은 최소 권한 액세스 적용, 다단계 인증 구현, 엄격한 패치 관리 유지 등 강력한 보안 태세 모범 사례를 활용해야 합니다. 그 외에도 두 가지 고려 사항이 있습니다. 더 높은 암호화를 사용하는 새로운 시스템이 기존 시스템과 상호 운용될 수 있도록 약한 암호화를 비활성화하는 것이 중요할 수 있습니다. 또한 신규 시스템의 경우 Grover 알고리듬으로 인해 보안 여유도가 감소하는 것을 상쇄하기 위해 대칭 암호화에는 AES-256, 다이제스트에는 SHA-384 이상으로 최소 보안 강도를 상향하는 것이 중요합니다. 이러한 조치는 현재의 위험을 줄이는 것뿐만 아니라 미래의 마이그레이션을 복잡하게 만드는 암호화 부채의 백로그를 최소화합니다.

암호화 자산의 인벤토리 및 감사

모든 마이그레이션 계획의 초석은 가시성입니다. 조직은 애플리케이션, 디바이스 및 워크플로 전반에서 공개 키 암호화가 사용되는 위치와 방법을 식별하는 포괄적인 암호화 인벤토리를 수행해야 합니다. 여기에는 TLS 인증서, VPN, 이메일 시스템, 코드 서명 메커니즘, 고객 데이터, 아카이빙된 데이터 등이 포함됩니다. 식별된 후에는 비즈니스 중요도, 민감도 및 수명에 따라 자산의 우선순위를 지정해야 합니다. 의료 기록 또는 기밀 아카이브와 같이 오래 보존되는 데이터는 Harvest Now, Decrypt Later 위협에 가장 취약하므로 가장 시급히 처리해야 합니다.

PQC 시범 운영 및 실험

인벤토리가 명확하면 PQC 지원 기술로 실습 실험을 시작하여 성능과 통합을 검증할 수 있습니다.

암호화 환경을 파악한 후, 조직은 통제된 환경에서 PQC 솔루션 테스트를 시작해야 합니다. IT 팀은 이러한 솔루션을 실험실에서 시범 운영함으로써 대규모 배포 전에 성능, 상호 운용성 및 관리 용이성을 검증할 수 있습니다. 전체 시스템을 전면 재정비할 필요 없이 암호화 알고리듬을 전환할 수 있는 이러한 암호화 민첩성을 구축하는 것은 장기적인 회복탄력성과 마이그레이션 용이성에 매우 중요합니다.

상호 운용성 접근 방식 채택

PQC 표준이 자리를 잡으면 운영 환경 배포 계획 수립을 시작할 수 있습니다. 하이브리드 접근 방식은 양자 안전 환경으로 이어지는 가교 역할을 합니다.

표준이 발전함에 따라 하이브리드 모델이 미래의 대비책이 될 수 있습니다. 많은 공급업체가 이미 기존 알고리듬과 양자 내성 알고리듬을 단일 구현으로 결합한 하이브리드 암호 제품군을 지원하고 있습니다. 이러한 이중 접근 방식은 나중에 하나의 알고리듬이 손상되더라도 보호 연속성을 제공합니다. 기업은 이제 하이브리드 전략을 도입함에 따라, 인프라스트럭처 공급업체의 제품 로드맵 및 이정표에 맞춰 내부 일정을 조정해야 합니다. 이를 통해 양자 안전 알고리듬이 표준화됨에 따라 조직은 중단 없이 도입을 확장할 수 있습니다.

전체 마이그레이션 및 지속적인 검증 실행

최종 목표는 완전히 통합되고 지속적으로 검증된 양자 안전 기업이 되는 것입니다.

전체 마이그레이션 및 지속적인 검증 실행

궁극적인 목표는 기업 전반에서 PQC로 완전히 전환하는 것입니다. 이는 일회성 이벤트가 아니라 지속적인 검증 및 적응 프로세스가 될 것입니다. 조직은 새로운 표준과 구현을 지속적으로 테스트하면서 PQC를 IT 스택의 모든 계층에 통합하여 상세한 마이그레이션 계획을 실행해야 합니다. 기존의 컴퓨터와 양자 컴퓨터로 구성된 하이브리드 환경을 사용하면 고객이 공격 시나리오를 시뮬레이션하고, 암호화 무결성을 검증하고, 진화하는 위협에 맞서 시스템의 회복탄력성을 유지할 수 있습니다.

협업 및 지식 공유

어떤 조직도 이 문제를 혼자 감당해서는 안 됩니다.

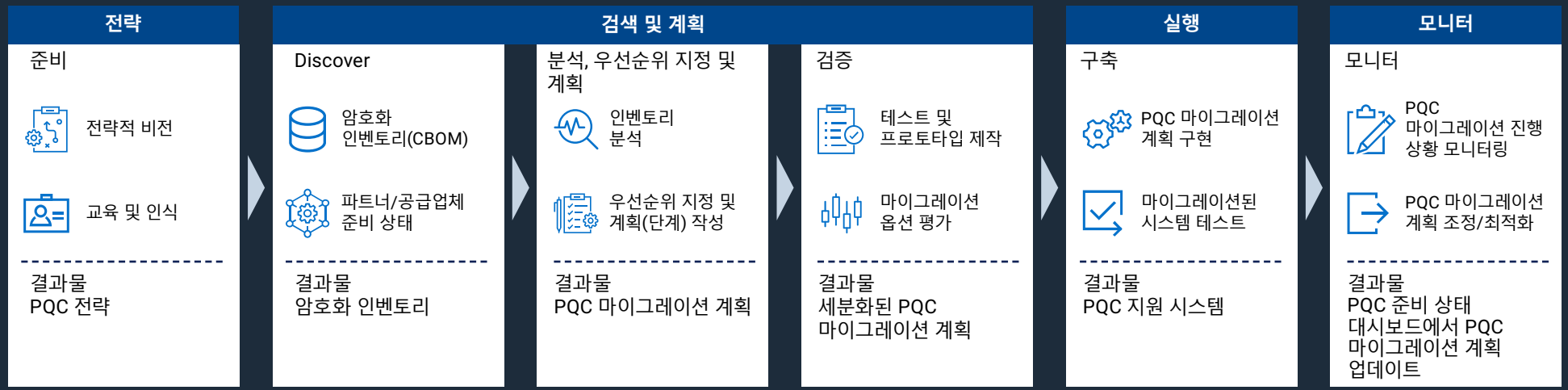
업계 컨소시엄, 학술 연구원 및 정부 기관은 PQC 전환을 가속화하기 위해 지식을 모으고 있습니다. 표준 그룹, 실무 그룹, 시범 프로그램 참여를 통해 기업은 모범 사례와 새로운 요구 사항을 충족할 수 있습니다. Dell은 NIST NCCoE PQC 프로젝트와 같은 이니셔티브에 적극적으로 참여하여 고객이 이러한 집단적 전문 지식을 직접 활용할 수 있도록 합니다.

결론

양자 시대는 더 이상 먼 미래가 아니라, 당장의 미래 지향적 사고를 바탕으로 한 조치를 필요로 하는 임박한 현실입니다. 기술의 변화에 대비하는 것은 가장 귀중한 자산인 데이터를 보호하는 전략에 있어 필수 과제입니다. 앞서 설명한 것처럼 인벤토리 및 감사부터 전체 마이그레이션까지의 단계적 접근 방식이 양자 시대에도 안전한 미래를 향한 가장 명확한 길입니다.

PQC로의 전환은 향후 수십 년 간 가장 중요한 인프라스트럭처 변화 중 하나가 될 것입니다. 이러한 전환은 서버 및 스토리지에서 엔드포인트, 클라우드 플랫폼, 네트워크 프로토콜에 이르기까지 IT의 거의 모든 측면에 영향을 미칩니다. 성공에는 예측, 계획, 그리고 체계적인 실행이 필요합니다. Dell Technologies는 미래를 단계적인 여정, 다시 말해 즉각적인 보안 개선과 PQC 도입을 위한 장기적인 준비 사이의 균형을 맞추는 여정으로 보고 있습니다.

Dell은 PQC 구현 전략을 지원할 준비가 되어 있습니다. 단계별 마이그레이션 계획을 권장하며 PQC 전환의 전략 수립, 계획, 실행 및 모니터링에 도움이 되는 일련의 활동을 제시하였습니다.



Copyright © Dell Inc.. All Rights Reserved. Dell Technologies, Dell 및 기타 상표는 Dell Inc. 또는 해당 자회사의 상표입니다. 기타 상표는 해당 소유주의 상표일 수 있습니다.