DELL Technologies

백서

Post-Quantum Cryptography: Preparing for the Quantum Era

Dell Technologies 백서

목차

종합 개요

양자 컴퓨팅은 이론 연구에서 실제 현실로 빠르게 전환되고 있습니다. 한때 먼 미래로 여겨졌지만 하드웨어, 알고리듬, 투자의 발전으로 기존 컴퓨터로는 불가능했던 문제를 해결할 수 있는 머신의 도래를 가속화하고 있습니다. 이는 업계에 미치는 영향이 매우 큽니다. 신약 개발부터 기후 모델링, 글로벌 물류에 이르기까지 양자 컴퓨팅은 이전에는 이룰 수 없었던 혁신을 실현할 수 있을 것으로 전망됩니다.

그러나 이러한 혁신에는 혼란스러운 당면 과제가 수반됩니다. 바로 양자 컴퓨터가 디지털 경제를 보호하는 암호화 기반을 약화시킬 것이라는 점입니다. RSA 및 ECC(Elliptic Curve Cryptography)와 같은 알고리듬인 공개 키 암호화는 수십 년 동안 디지털 통신, 금융 시스템, 의료 기록 및 국가 보안을 보호해 왔습니다. 이러한 방법은 기존 컴퓨터로는 해결하기 어려운 수학적 문제를 사용합니다. 그러나 CRQC(Cryptographically Relevant Quantum Computer)가 등장함에 따라 이러한 문제를 효율적으로 해결할 수 있게 되어 오늘날의 보안 시스템은 철 지난 것이 되었습니다.

이러한 위협은 이론적인 것이 아닙니다. 일부 조직은 이미 HNDL(“Harvest Now, Decrypt Later”)이라는 전략을 사용하고 있습니다. 즉, 양자 컴퓨터가 발전함에 따라 암호화된 데이터를 해독할 수 있을 것이라는 기대감으로 이를 수집하는 것입니다. 현재 안전한 것으로 보이는 기밀 정보도 몇 년 후에는 취약해질 수 있습니다. 행동해야 할 때는 CRQC 시대가 도래했을 때가 아니라 바로 지금입니다.

이 백서에서는 양자 위협의 시급성을 설명하고, 새로운 PQC(Post-Quantum Cryptography) 분야를 살펴보며, 조직이 준비할 수 있는 방법에 대한 지침을 제공합니다. 이 백서는 NIST의 PQC(Post-Quantum Cryptography) 표준(FIPS 203, FIPS 204, FIPS 205)과 CNSA 2.0(Commercial National Security Algorithm Suite 2.0) 지침에 따라 공급망, 하드웨어, 펌웨어, 소프트웨어 및 파트너 생태계 전반에 보안 기능을 구축함으로써 양자 안전 미래를 구축하기 위한 Dell Technologies의 노력을 강조합니다. Dell Technologies의 목표는 명확합니다. 보안이나 신뢰를 저해하지 않고 혁신을 추진할 수 있도록 보장하는 것입니다.

용어

이 백서에서는 여러 가지 용어를 볼 수 있습니다. 본 백서의 이해를 돕기 위해 이러한 용어 중 일부를 간략하게 설명하고자 했습니다.

포스트 양자 암호화 – 새로운 알고리듬을 통해 양자 컴퓨터 공격으로부터 안전하게 보호할 수 있는 새로운 수학적 암호화 접근 방식입니다. 이러한 알고리듬은 기존 컴퓨터에서 실행되며 양자 공격뿐만 아니라 알려진 기존 암호학 공격에도 강합니다.

양자 회복탄력성 - 양자 회복탄력성은 암호화 관련 CRQC(Cryptographically Relevant Quantum Computer)가 있는 환경에서도 보안을 유지하도록 설계된 시스템, 알고리듬 또는 인프라스트럭처를 의미합니다. 양자 회복탄력성이 뛰어난 시스템은 PQC(Post-Quantum Cryptography) 또는 기존 공격과 양자 공격을 모두 견딜 수 있는 기타 보호 기능을 사용하여 향후 데이터의 기밀성, 무결성 및 신뢰성을 보장합니다. 양자 회복탄력성과 양자 안전성 등의 다른 용어도 혼용될 수 있습니다.

암호화 민첩성 - 암호 민첩성이라고도 하며, 조직의 시스템과 애플리케이션이 대대적인 재설계나 운영 중단 없이 암호화 알고리듬, 프로토콜 또는 키 길이를 빠르고 원활하게 전환할 수 있는 기능입니다.

HNDL("Harvest Now, Decrypt Later") - RNDL("Record Now, Decrypt Later")이라고도 하는 이 행위는 향후 CRQC(Cryptographically Related Quantum Computer)를 사용할 수 있게 되면 암호를 해독할 목적으로 암호화된 데이터를 수집하고 저장하는 공격자의 행위입니다.

양자 컴퓨팅 및 암호화 위협

양자 컴퓨팅의 부상

CTO인 John Roese가 거의 1년 전에 작성한 블로그 게시물 Post-Quantum Cryptography: A Strategic Imperative for Enterprise Resilience에서 설명했듯이, 기존 컴퓨터는 노트북, 스마트폰, 서버 등 어디에서나 0이나 1의 상태로 존재하는 비트를 사용하여 정보를 처리합니다. 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.

양자 컴퓨팅의 잠재적 적용 분야는 놀랍습니다. 연구원들은 기존 컴퓨터로는 달성할 수 없는 정밀도로 분자 상호 작용을 시뮬레이션함으로써 제약 분야에서 획기적인 발전을 기대하고 있습니다. 기후 과학자들은 글로벌 시스템의 보다 정확한 모델을 구상하고 있으며, 에너지 부문에서는 전력망 및 스토리지를 최적화할 수 있는 잠재력을 주목하고 있습니다. 물류와 제조업조차도 양자 최적화 기술의 이점을 누릴 수 있습니다. 그 이점은 실질적이며 쉽게 얻을 수 있지만, 위험도 마찬가지입니다.

암호화가 위험에 처한 이유

암호화는 디지털 시대의 신뢰를 뒷받침합니다. 신용카드 번호를 입력하거나, 보안 웹사이트에 로그인하거나, 서명된 소프트웨어 업데이트를 받을 때 암호화는 기밀성, 신뢰성 및 무결성을 보장합니다. 이러한 보호 기능의 대부분은 RSA 및 ECC와 같은 알고리듬인 공개 키 암호화를 사용하며, 이러한 알고리듬은 기존 머신에서는 계산이 불가능하다고 여겨지는 수학적 문제에 기반합니다.

양자 컴퓨팅은 이러한 방정식을 변화시킵니다. **쇼어 알고리듬** 사용으로, 충분히 강력한 양자 컴퓨터는 RSA와 ECC의 강점인 인수 분해 문제와 이산 로그 문제를 해결할 수 있습니다. CRQC가 등장함에 따라, 소프트웨어 업데이트를 보호하는 디지털 서명, TLS 세션을 설정하는 키 및 디바이스를 인증하는 인증서가 모두 손상될 수 있습니다. 그 영향은 체계적이며 디지털 거래를 안전하게 만드는 메커니즘 자체를 위협합니다.

저장된 데이터 보호 또는 보안 통신을 보호하는 데 사용되는 AES와 같은 알고리듬인 대칭 암호화의 경우, 심각성은 낮지만 다른 문제가 있습니다. **그로버 알고리듬**은 양자 컴퓨터가 대칭 키의 유효 강도를 줄여 보안을 효과적으로 반감시킬 수 있도록 합니다. AES-256 등의 더 큰 키 크기로 전환하면 이 문제를 완화할 수 있지만, 이러한 조정이 필요하다는 사실 그 자체로 양자 위협이 광범위하다는 것을 알 수 있습니다.

시급성 및 결과

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. HNDL("Harvest Now, Decrypt Later") 전략은 이러한 시급성을 더욱 가중시킵니다. 지금은 공격자가 암호화된 데이터를 캡처하고 해독할 수단을 기다릴 수밖에 없지만 CRQC의 시대가 도래하면 이미 손해를 되돌릴 수 없게 될 것입니다.

포스트 양자 암호화 및 새로운 표준

포스트 양자 암호 정의

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.

PQC의 기반은 현재 알려진 바에 따르면 쇼어 알고리듬과 그로버 알고리듬 등의 양자 기술로는 해결 불가능한 일련의 수학적 문제입니다. 격자 기반 암호화, 해시 기반 서명, 코드 기반 체계 및 다변량 방정식은 가장 유망한 암호 체계입니다. 이러한 접근 방식은 RSA와 ECC가 제공했던 것과 동일한 신뢰성과 상호 운용성을 제공하기 위해 엄격한 테스트와 표준화 과정을 거치고 있습니다.

글로벌 표준화 노력 - 새로운 산업 표준

위협의 시급성을 인식한 정부와 표준 기관은 PQC를 전 세계적인 우선순위로 삼았습니다. 미국 NIST(National Institute of Standards and Technology)는 2016년에 PQC 프로젝트를 시작하여 암호화 연구 커뮤니티에 후보 알고리듬을 제안, 분석 및 개선할 것을 요청했습니다. 수년간의 테스트 끝에 NIST는 2024년 8월 최초의 표준화된 알고리듬 그룹을 발표했습니다.

- **CRYSTALS-**Kyber: 공개 키 암호화 및 키 설정을 위한 알고리듬
- **CRYSTALS-**Dilithium 및 SPHINCS+: 디지털 서명을 위한 알고리듬

내장형 펌웨어와 같은 경량 시스템을 포함하여 다양한 구현 요구 사항에 대한 다양성과 유연성을 제공하기 위해 더 많은 알고리듬이 검토 중입니다. 이러한 진화하는 표준화 프로세스를 통해 전 세계 조직은 양자 내성 솔루션을 채택할 수 있는 명확한 경로를 마련할 수 있습니다.

NIST 표준 – FIPS 203, 204, 205

2024년 8월 미국 NIST(National Institute of Standards and Technology)는 첫 번째 PQC 알고리듬을 확정했습니다.

- FIPS 203(ML-KEM) - 주요 캡슐화 메커니즘인 CRYSTALS-Kyber를 기반으로 합니다. IND-CCA2 보안을 제공하여 적응성이 뛰어난 선택 암호문 공격을 받더라도 암호문을 구별할 수 없습니다.
- FIPS 204(ML-DSA) – 디지털 서명 알고리듬인 Crystals-Dilithium을 기반으로 합니다. 디지털 서명의 표준 요구 사항인 강력한 EUF-CMA 보안을 제공합니다(선택 메시지 공격을 받아도 실질적으로 위조가 불가능함).
- FIPS 205(SLH-DSA) – 해시 기반 서명 체계인 SPHINCS+를 기반으로 합니다. 격자 문제에 종속되지 않는 보수적인 대체 방안으로 선정되었습니다.

필수 로드맵

양자 내성 암호화 알고리듬 채택의 중요성을 깨닫고 미국 연방 정부는 연방 기관에 PQC 요구 사항을 발표하기 시작했습니다. 여기에는 NSM-10(National Security Memorandum 10), CNSA 2.0(Commercial National Security Algorithm Suite), NIST(National Institute of Standards and Technology) IR(Interagency Report) 8547, OMB M-2302(Office of Management and Budget Memorandum 23-02) 등이 포함됩니다.

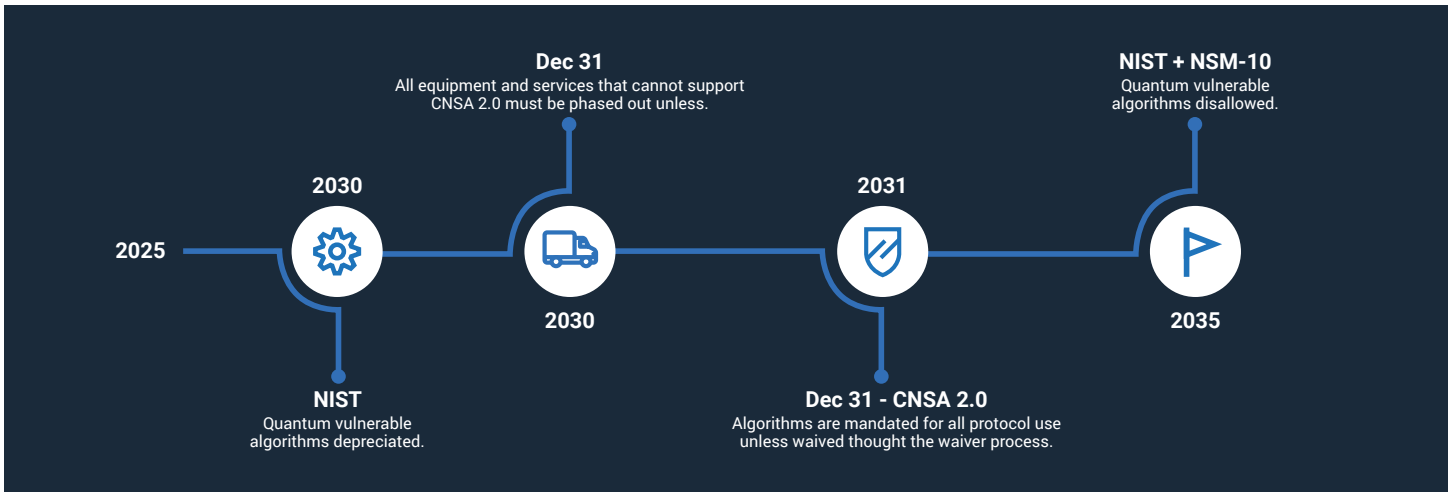
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodologies.

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

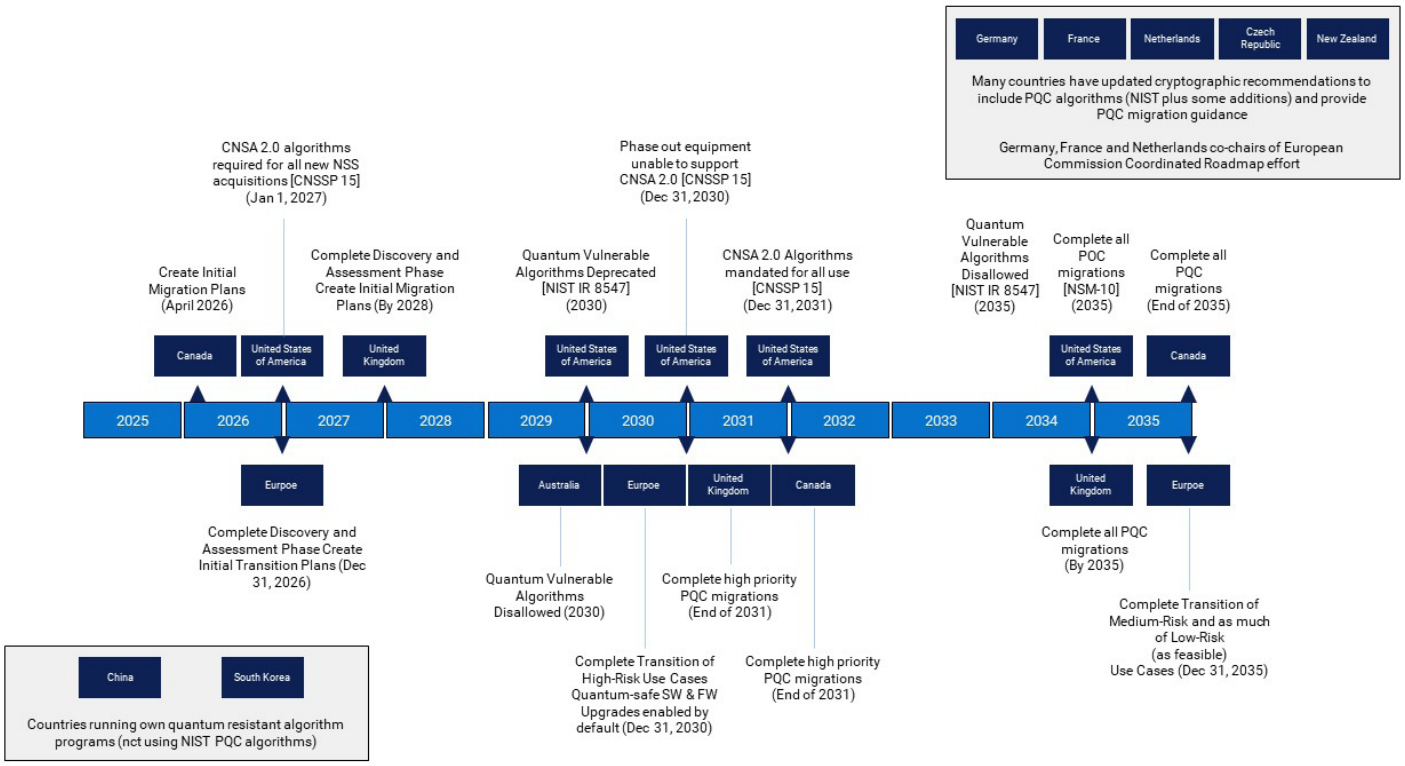
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

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

2022년 9월 NSA가 발표한 CNSA 2.0은 포스트 양자 암호화 알고리듬에 대한 첫 번째 권장 사항을 소개합니다. CNSA 2.0은 NSS(National Security Systems) 전반에 걸쳐 양자 내성 알고리듬을 도입하기 위한 명확한 기한을 정하고 있으며, 자체적인 전환을 준비하는 기업에 강력한 지침 역할을 합니다.



전 세계의 다른 조직도 PQC 전환에 대한 지침을 설정했습니다. 아래는 국가별 규정 중 일부입니다.



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.

업계 협업

NIST 및 NSA 외에도 Dell은 상호 운용성과 도입을 주도하는 업계 컨소시엄과 표준 그룹에 적극적으로 참여하고 영향력을 행사하고 있습니다. Trusted 컴퓨팅 그룹은 PQC를 TPM(Trusted Platform Module) 표준에 통합하고 있습니다. IETF는 PQC 알고리듬을 TLS, X.509 인증서와 같은 산업 프로토콜에 통합하는 데 많은 노력을 기울이고 있습니다. OASIS KMIP(Key Management Interoperability Protocol) 위원회는 주요 관리 프레임워크를 위한 PQC를 활성화하고 있습니다. FIDO Alliance는 PQC가 인증 및 디바이스 온보딩 표준에 미치는 영향을 연구하고 있으며, SAFECode와 같은 조직은 마이그레이션을 준비하기 위한 방안을 업계에 알리기 위해 노력하고 있습니다.

NIST NCCoE(National Cyber Security Center of Excellence)는 NIST가 도메인 중심 프로젝트를 통해 업계, 학계 및 정부 기관과 협력할 수 있도록 지원하는 기관입니다. NCCoE는 다음과 같은 여러 가지 사항에 중점을 두고 있습니다.

- 암호화 탐색 - 마이그레이션해야 하는 암호화와 먼저 마이그레이션할 항목의 우선순위를 지정하는 방법을 식별합니다.
- 상호 운용성 - 널리 사용되는 암호화 기능과 프로토콜이 새로운 PQC 알고리듬을 통합하고 다양한 공급업체의 구현이 상호 운용되도록 합니다.
- 암호 민첩성 - 암호화 민첩성이라고도 하며, 시스템 인프라스트럭처를 크게 변경하지 않고도 새로운 암호화 프리미티브 및 알고리듬을 신속하게 조정하도록 지원하는 정보 시스템을 개발하는 데 중점을 둡니다.

이러한 프로젝트는 만드는 지침과 표준을 알리고 개발하는 데 도움이 되며, 제공하는 표준 및 지침에 대한 모범적인 업계 솔루션이 있는지 확인하는 데 도움이 됩니다. Dell은 NCCoE PQC 마이그레이션 프로젝트가 시작된 이래로 이 프로젝트에 참여해 왔습니다.

오늘날의 PQC는 단순한 연구 주제가 아니라 구체적인 알고리듬, 일정 및 도입 경로를 갖추고 발전 중인 표준입니다. 지금 준비를 시작하는 조직은 뒤늦게 급히 준비하면서 발생할 수 있는 비용, 운영 중단, 위험을 방지할 수 있습니다. 이러한 전환은 단순히 규정 준수에 관한 것이 아니라, 양자 컴퓨팅이 디지털 환경을 재편함에 따라 신뢰, 기밀성 및 무결성이 그대로 유지되도록 보장하는 것입니다.

지금 행동해야 하는 이유

위협의 즉시성

양자 컴퓨팅을 기술이 완전히 실현되었을 때 대처하면 되는, 멀리 있는 위험 정도로 보는 관점에 솔깃할 수 있습니다. 현실적으로 그 위험은 이미 시작되었습니다. 금융 거래, 의료 기록, 지적 재산 또는 정부 통신과 같은 기밀 정보의 경우, 지금은 안전하게 암호화될 수 있지만 양자 머신이 RSA 또는 ECC를 무력화시키는 임계점에 도달하면 해당 데이터도 소급적으로 노출될 수 있습니다. 그러면 과거 통신 및 기록의 전체 백로그가 순식간에 위험에 처할 수 있습니다.

긴 기술 주기

최신 IT 생태계는 쉽게 또는 빠르게 혁신되지 않습니다. 역사적으로 SHA-1에서 SHA-2로, DES/3DES에서 AES로의 전환과 같은 단일 알고리듬 교체에는 10년 이상이 소요되었습니다. 이러한 알고리듬은 운영 체제, 애플리케이션, 네트워크 디바이스 및 하드웨어에 깊이 내장되어 있습니다. 이를 교체하려면 데이터 센터에서 클라우드 플랫폼, 엣지 디바이스에 이르는 환경 전반에서 재설계, 검증, 테스트 및 배포가 필요합니다. 많은 조직에서, 이러한 교체는 양자 컴퓨팅이 실제 위협을 초래하기까지 남은 기간보다 훨씬 더 오래 걸릴 것입니다. 이것이 바로 규제 기관, 표준 기관 및 보안 리더가 즉각적인 준비를 강조하는 이유입니다. CRQC가 널리 보급될 때까지 기다리다가는 체계적으로 전환할 시기를 놓치게 됩니다.

조치를 취하지 않을 경우 발생할 수 있는 위험

마이그레이션을 지연하면 기술적 노출을 넘어 다음과 같은 결과가 발생합니다.

- 데이터 보안 위험: 양자 컴퓨터가 발전함에 따라 의료 기록, 재무 기록 또는 국방 정보와 같이 오래 보존해야 하는 데이터가 소급적으로 손상될 수 있습니다.
- 소프트웨어 신뢰성 및 무결성 위험: 지금의 서명 방식으로 서명한 소프트웨어를 양자 컴퓨터가 발전된 후에도 계속 사용하면 소프트웨어의 신뢰성과 무결성이 악성 코드로 인해 손상될 수 있습니다.
- 운영 위험: 공공 서비스, 운송망, 응급 서비스와 같은 중요한 인프라스트럭처 시스템은 업그레이드하기가 매우 어렵습니다. 지금 계획하지 않으면 나중에 운영 중단이 발생할 수 있습니다.
- 규제 및 규정 준수 위험: **CNSA 2.0**과 같은 프레임워크는 규정 준수를 위한 명확한 일정을 수립했습니다. 대비하지 못하는 조직은 노출 위험뿐만 아니라 정부 또는 업계의 기대치를 충족하지 못할 위험도 있습니다.
- 평판 및 재무 위험: 해결되지 않은 암호화 취약성으로 인한 침해는 브랜드 신뢰에 지속적인 피해를 입히고 상당한 재정적 손실을 초래할 수 있습니다.

사전 예방적 조치의 사례

사전 예방적 준비는 단순히 방어적인 움직임이 아니라 장기적인 회복탄력성을 강화할 수 있는 기회입니다. 조직은 암호화 인벤토리를 수행하고, 대칭 키 길이를 업그레이드하며, PQC 지원 솔루션을 시범 운영하고, 양자 내성 오퍼링을 제공하는 공급업체와 협력함으로써 신뢰의 연속성을 보장할 수 있습니다. 초기 수용자는 미래 지향적인 운영을 수행하고 규정 준수를 유지하며 고객, 파트너 및 규제 기관에 리더십을 입증할 수 있는 더 유리한 입지를 확보하게 됩니다.

포스트 양자 암호화에 대한 Dell의 접근 방식

Dell Technologies는 기술이 인류의 발전을 주도하며, 보안이 이러한 발전의 기반이라고 생각합니다. Dell Technologies는 기업으로서 포트폴리오, IT 인프라스트럭처 및 수명주기 지원 시스템이 양자 내성 알고리듬으로 전환할 수 있도록 준비하고 있습니다. 전환을 준비하기 위해 취해야 할 단계는 다음과 같습니다.

- 제품, 서비스, IT 인프라스트럭처 및 지원 시스템에 암호화가 사용되는 특정 영역과 목적을 파악하여 포괄적인 전환 계획을 수립합니다.
- PQC(Post Quantum Cryptography) 알고리듬에 대한 내부 지식을 향상하여 암호화 민첩성과 관련된 구현 측면과 설계 원칙을 고려하여 PQC 알고리듬으로의 원활한 전환을 촉진합니다.
- Dell Technologies의 다양한 포트폴리오와 관련된 다양한 활용 사례에서 PQC 알고리듬의 성능, 적용 가능성 및 적합성을 평가합니다.

PQC 전환의 복잡한 특성을 고려할 때, 암호화 활용 사례가 업그레이드되면 Dell Technologies 오퍼링에서도 단계적으로 이를 지원할 수 있습니다. 예를 들어, 데이터 관점에서는 전송 중인 데이터 또는 저장 상태 데이터 암호화와 같은 HNDL("Harvest Now, Decrypt Later") 공격에 취약할 수 있는 활용 사례에 대해 전환 우선순위를 둡니다.

기술 플랫폼을 고려하면 암호화 활용 사례의 전환에는 전체 제품 복구/교체 또는 제품 업그레이드가 포함될 수 있습니다. 이는 해당 제품과 제품 및 주변 시스템에서 암호화가 구현되는 위치와 방법에 따라 달라집니다.

향후 5년 동안 양자 내성 오퍼링의 릴리스는 고객이 2027년에서 2035년 사이에 정부 및 업계 협회에서 발표할 PQC 전환 일정을 충족할 수 있도록 지원하는 데 중점을 둘 것입니다.

고객은 Dell 어카운트 팀과 협력하여 제품별 세부 정보(예: 릴리스 로드맵 및 일정)를 확보하여 마이그레이션 계획에 반영해야 합니다. Dell은 향후 몇 달 이내에 PQC를 제품군과 제품에 통합하기 위한 보다 구체적인 일정을 제공할 예정이므로 계속 지켜봐 주시기 바랍니다.

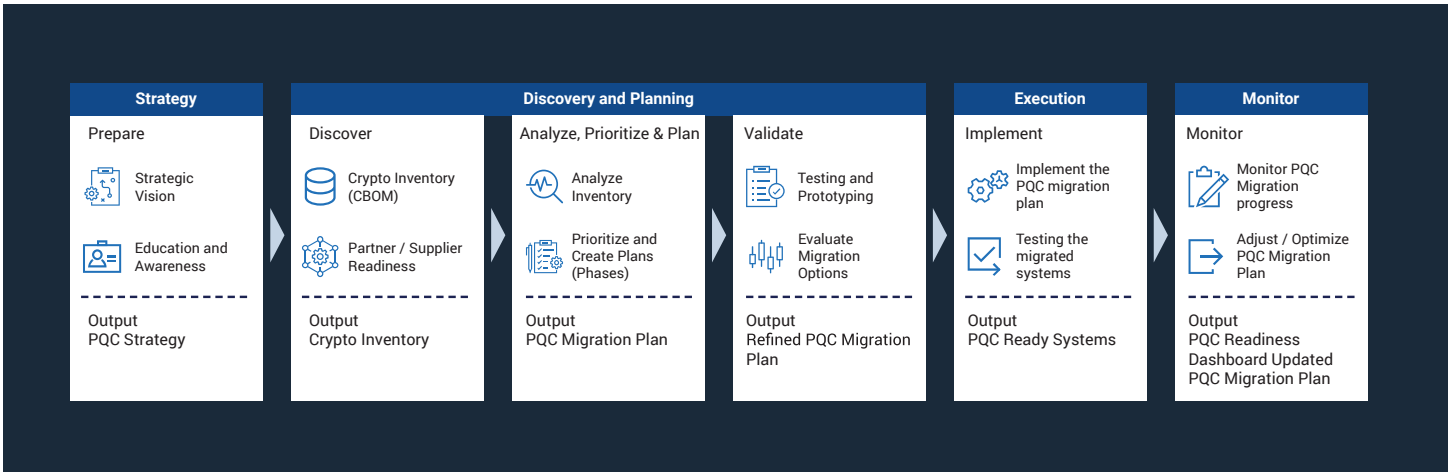
양자 회복탄력성 혁신에 대비

Dell의 목표는 고객이 새로운 표준을 준수하도록 지원할 뿐만 아니라 양자 시대에 안전하게 혁신할 수 있도록 지원하는 것입니다. AI 워크로드를 배포하거나, 하이브리드 클라우드 환경을 관리하거나, 엣지 인프라스트럭처를 현대화하려는 고객은 Dell 솔루션이 회복탄력성을 염두에 두고 설계된 것이라는 확신을 가질 수 있습니다. 보안 기능은 추가되는 것이 아니라 Dell 포트폴리오의 모든 계층에 엔지니어링되어 있으므로 조직은 포스트 양자 암호화로 안심하고 전환할 수 있습니다.

전환을 위한 준비

포스트 퀀텀 암호화로의 전환은 수십 년 동안 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 마이그레이션의 전략 수립, 계획, 실행 및 모니터링에 도움이 되는 일련의 활동을 제시합니다.



오늘날의 보안 태세 준비

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 최신 시스템의 경우 그로버 알고리듬으로 인한 마진 감소를 방지하기 위해 대칭 암호화를 더 긴 키 길이인 AES-256 및 SHA-384 이상으로 업그레이드하는 것이 중요합니다. 이러한 조치는 현재의 위험을 줄이는 것뿐만 아니라 미래의 마이그레이션을 복잡하게 만드는 암호화 부채의 백로그를 최소화합니다.

암호화 자산 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 및 아카이빙된 데이터가 포함됩니다. 식별된 후에는 비즈니스 중요도, 민감도 및 수명에 따라 자산의 우선순위를 지정해야 합니다. 의료 기록 또는 기밀 아카이브와 같이 오래 보존되는 데이터는 HNDL(Harvest Now, Decrypt Later) 위협에 가장 취약하므로 가장 시급히 처리해야 합니다.

PQC 시범 운영 및 실험

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

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

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. 하이브리드 양자-기존 환경을 통해 고객은 공격 시나리오를 시뮬레이션하고, 암호화 무결성을 검증하고, 발전하는 위협에 대한 시스템의 회복탄력성을 유지할 수 있습니다.

협업 및 지식 공유

마지막으로, 어떤 조직도 혼자서 이 과제에 직면해서는 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.

PQC를 준비하는 작업은 단거리 뛰기가 아닌 마라톤을 하는 것과 같습니다. 현재의 방어 태세 강화, 암호화 자산 감사, PQC 시범 운영, 하이브리드 전략 도입, 전체 마이그레이션 실행 등 단계적 접근 방식을 통해 조직은 양자 회복탄력성을 향해 자신 있게 나아갈 수 있습니다. Dell의 파트너가 되시면 이 여정을 달성할 수 있을 뿐만 아니라, 신뢰를 강화하고 미래에도 혁신을 실현할 수 있습니다.

실제 적용 사례 및 이점

포스트 양자 암호화로의 전환은 단순한 규정 준수를 넘어 신뢰, 회복탄력성 및 장기적인 경쟁력에 직접적인 영향을 미치는 비즈니스 필수 과제입니다. 통신 공급업체, 금융 기관, 의료 조직 및 정부 기관의 경우, 양자 내성 알고리듬을 도입함으로써 중요한 디지털 인프라스트럭처를 현재와 미래의 위협으로부터 안전하게 보호할 수 있습니다.

통신

통신 네트워크는 글로벌 디지털화의 중추입니다. 긴급 서비스 및 IoT 연결부터 안전한 고객 통신에 이르기까지 모든 것을 지원합니다. 이 분야에서 양자 보안 침해가 발생할 경우, 4G 및 5G의 기반이 되는 SIM 프로비저닝, eSIM 온보딩 또는 인증 프로세스가 손상될 수 있습니다. 지금 하이브리드 및 양자 안전 암호화를 구축함으로써, 운영자는 고객 신뢰를 유지하고 데이터 프라이버시를 보호하며 여러 세대의 모바일 기술 전반에서 원활한 서비스 연속성을 보장할 수 있습니다.

금융 서비스

금융 산업은 사이버 공격자의 가장 큰 표적이 되고 있으며, 거래의 무결성은 암호화에 달려 있습니다. 포스트 양자에 대비한 기업은 양자 기반 사기 행위로부터 디지털 결제, 온라인 뱅킹 및 은행 간 송금을 보호할 수 있습니다. 또한 조기 도입은 규제 기관과 고객이 자산을 보호하고 시스템 안정성을 유지하기 위해 최선을 다하고 있음을 재확인시켜 줍니다. 이 부문에서는 미래에 대비한 암호화를 통해 규정 위반 및 평판 위험을 모두 줄일 수 있습니다.

의료

환자 기록, 게놈 데이터, 연동형 의료 디바이스가 모두 HNDL(Harvest Now, Decrypt Later) 공격의 위험에 노출되어 있습니다. 의료 부문은 기밀 의료 데이터에 필요한 장기간 보존 기간이라는 추가적인 과제에 직면해 있습니다. 지금 PQC로의 전환을 시작함으로써 병원과 의료진은 의료 기록을 지금뿐만 아니라 앞으로도 수십 년간 비공개로 유지할 수 있습니다. 이는 변화하는 데이터 보호 규정을 준수하면서 환자의 신뢰를 유지하는 데 필수적입니다.

정부 및 중요 인프라스트럭처

국방 통신에서 에너지 분배 시스템에 이르기까지 정부와 인프라스트럭처 운영자는 운영 연속성 및 국가 보안을 위해 암호화를 사용합니다. 포스트 양자 암호화는 단기적인 공격뿐만 아니라 향후 악용을 목적으로 암호화된 통신을 전략적으로 수집하는 행위로부터 보호합니다. CNSA 2.0과 같은 프레임워크와 연계하면 양자 시대에 상호 운용 가능하며, 안전하고, 신뢰할 수 있는 정부 시스템을 유지할 수 있습니다.

더 광범위한 비즈니스 이점

PQC의 기술적 필요성은 분명하며, 비즈니스 타당성도 마찬가지로 강력합니다.

- 신뢰 및 브랜드 평판: 고객 및 파트너 데이터를 보호하는 데 있어 리더십을 보여줍니다.
- 규정 준수: NIST 표준 및 CNSA 2.0과 같은 정부 규정을 준수합니다.
- 운영 회복탄력성: 암호화가 손상되어 심각한 운영 중단이 발생할 위험을 줄입니다.
- 경쟁력 있는 차별화: 조직을 수동적인 추종자가 아닌 선제적 혁신가로 포지셔닝합니다.

지금 바로 행동했을 때 따르는 이점은 기술적 회복탄력성을 훨씬 뛰어넘습니다. PQC를 조기에 도입하는 조직은 위험을 줄일 뿐만 아니라 신뢰에 의존하는 디지털 경제에서 혁신, 규정 준수 및 경쟁 역량을 강화할 수 있습니다.

다음 단계 진행

양자 컴퓨팅의 등장은 세대를 초월하는 기회이자 전례 없는 보안 당면 과제를 나타냅니다. 암호학적으로 관련성이 있는 양자 컴퓨터가 정확히 어떻게 될지는 불확실하지만, 확실한 것은 이에 대비하려면 노력이 필요하다는 것입니다. 포스트 양자 암호화로 전환하려면 수년간의 조율된 계획, 투자 및 실행이 필요합니다. 양자 컴퓨터가 운영될 때까지 기다리는 것은 현실적인 선택이 아닙니다.

모든 조직의 첫 번째 단계는 암호화가 환경 전반 어디에서 어떻게 사용되는지 이해하는 것입니다. 이를 바탕으로 기업은 양자 안전 솔루션을 인벤토리화하고, 우선순위를 정하고, 시범 운영해야 합니다. 표준이 계속 변화하는 가운데, 기존 알고리듬과 포스트 양자 알고리듬을 결합한 하이브리드 암호화를 통해 회복탄력성을 즉시 확보할 수 있습니다. NIST의 PQC 표준 및 CNSA 2.0 일정과 같은 글로벌 프레임워크에 내부 로드맵을 맞춰 조정함으로써 조직은 규정 준수 및 상호 운용성을 향해 자신 있게 나아갈 수 있습니다.

Dell Technologies는 고객이 이러한 전환 과정을 원활하게 진행할 수 있도록 지원하기 위해 최선을 다하고 있습니다. Dell Technologies는 이러한 접근 방식을 통해 공급망 무결성, 하드웨어 내장형 보안 장치, 소프트웨어 기반 적응성의 기반을 제공합니다. 선도적인 보안 공급업체와의 파트너십과 업계 표준 기관에서의 적극적인 참여는 Dell 솔루션이 최신 요구 사항에 부합할 뿐만 아니라 실제 성능과 상호 운용성을 테스트하도록 보장합니다.

지금 바로 대비를 시작하십시오. 발견 및 위험 분석으로 시작하면, 신뢰할 수 있는 공급업체와 협력하고, 양자 안전 기술을 시범 운영할 수 있습니다. 지금 취하는 모든 단계는 미래의 운영 중단 위험을 줄여줍니다. 조기에 조치를 취하는 조직은 데이터와 시스템을 보호할 뿐만 아니라 디지털 신뢰가 가장 중요한 시대에 고객, 규제 기관 및 파트너의 신뢰를 얻을 수 있습니다.

회사 소개

Dell Technologies는 모든 사람이 첨단 기술을 쉽게 이용할 수 있고, 신뢰할 수 있으며, 역량을 강화할 수 있도록 최선을 다하고 있습니다. Dell Technologies는 사람과 조직이 혁신을 안전하게 활용하여 보다 안전하고 포용적이며 연결된 미래를 향해 나아갈 수 있도록 지원합니다.

Dell [product name] 솔루션에 대한 자세한 정보

Dell Technologies 전문가에게 문의

추가 리소스 보기

대화에 참여: #HashTag

DELL Technologies