quantropi®

Bring it on.

Digital Quantum Key Distribution (D-QKD)

Eliminating HNDL Risk with Out-of-Band, Quantum Safe Keys

The Quantum Threat is No Longer Future Tense

'Harvest Now, D
Boosts Quantur

Nancy Liu | Editor
September 27, 2022 3:30 PM

Quantum computing development roa
quantum security journey and prepa
recommend.

"Harvest now, decrypt later" re
organizations today, anticipating
maturity level capable of renderin

The consulting firm surveyed over 4
computing benefits and found that ove
for "harvest now, decrypt later" attacks.

"It's encouraging to see th
aware of the securit
in Del
decrypt
quantur

BORDER GATEWAY PROTOCOL —

Strange snafu misroutes domestic US Internet traffic through China Telecom

Telecom with ties to China's government misdirected traffic for two and a half years.

DAN GOODIN - 11/6/2018, 8:05 AM

DATA CENTER NEWS

Harvest now, decrypt later attacks put encrypted data in the hands of hackers

Quantum computers are still under development and seen as future technology, but they already cause danger to encrypted data. Seeing a high potential to be able to crack cryptographic keys in the long-term, cybercriminals are intensifying what are known as "harvest now, decrypt later" attacks to accumulate huge quantities of encrypted data and decrypt them once quantum technology is developed enough.

"Current encryption systems are still hard to break, so they are beneficial for ensuring your privacy," said Marijus Briedis, CTO at NordVPN. "Nevertheless, cybercriminals already target encrypted data even if they cannot crack the decryption. Even though quantum computing is still in the future, it will take years until the global community adapts to the new standard of encryption, so we have to plan the transition to quantum-resistant algorithms now."

CYBERWARFARE

Cyber Insights 2022: Nation-States

By Kevin Townsend
January 20, 2022

by Christopher Burgess
Contributing Writer

Global trends will increase nation-state threats for the US in next 20 years

ress releases

Harvest Now, Decrypt Later Attacks Pose a Security Concern as Organizations Consider Implications of Quantum Computing

NEW YORK, Sept. 20, 2022 — Just over half of responding professionals at organizations considering quantum computing benefits believe that their organizations are at risk for "harvest now, decrypt later" (HNDL) cybersecurity attacks (50.2%), according to a new Deloitte poll.

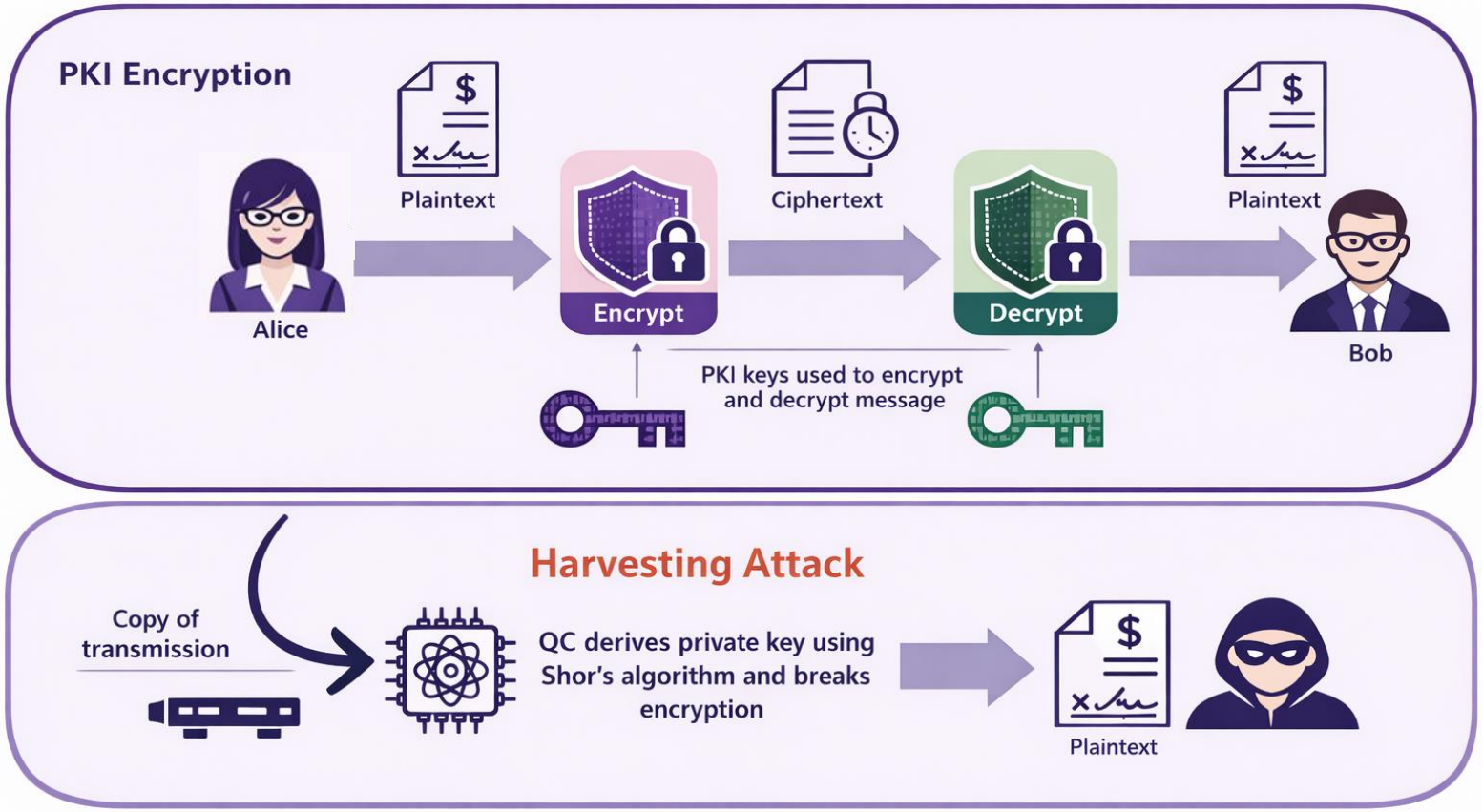
In HNDL attacks, threat actors "harvest" data from unsuspecting organizations, anticipating that data can be decrypted later — when quantum computing reaches the maturity to render some existing cryptographic algorithms obsolete.

Deloitte.

quantropi

Harvesting Attack (HNDL): The Zero Day Threat

- Adversaries are recording encrypted traffic **now**
- Decryption will occur once quantum capabilities mature (Harvest Now, Decrypt Later)
- IPSec/IKEv2, TLS, and PKI-based systems are all exposed
- **Even PQC algorithms may be broken in the future**



Any key exchange performed in-band is vulnerable to future decryption.

quantropi

Why Organizations Need Quantum-Safe Keying

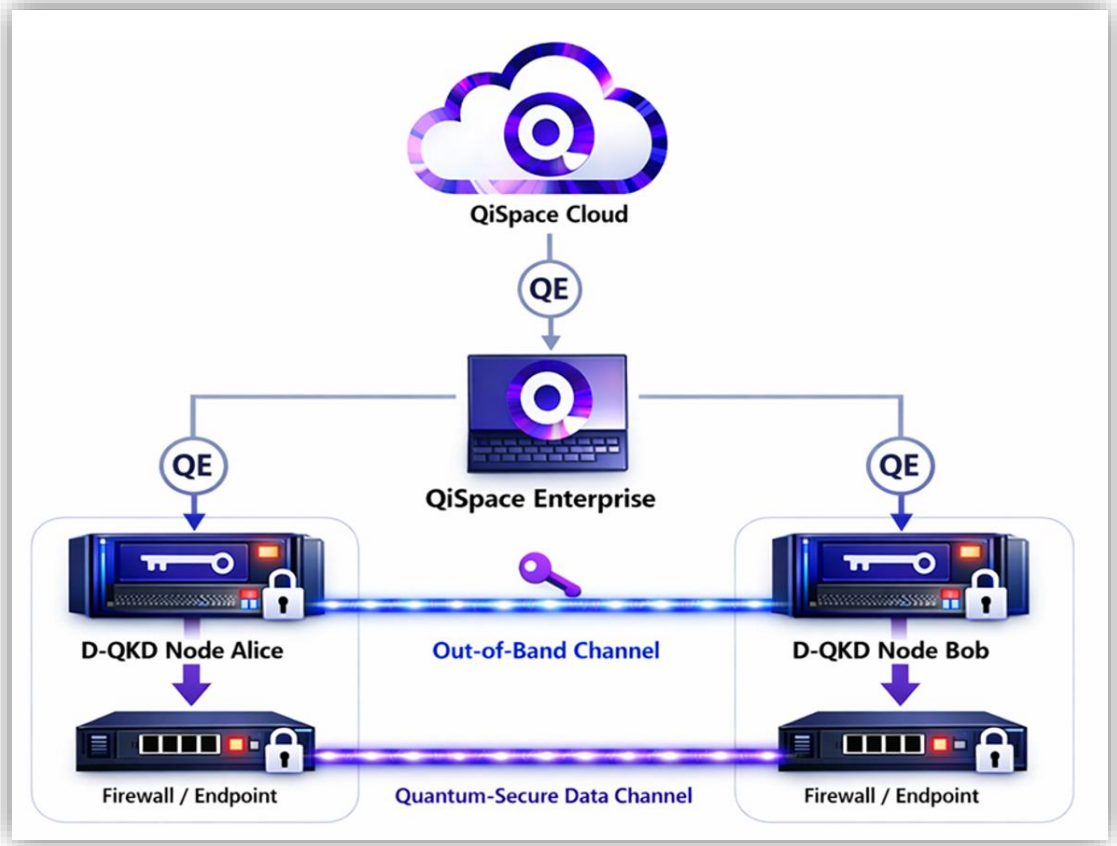
- Site to Site network links are prime targets for HNDL (IPSec, MACSec, OTNSec)
- IKEv2 and MKA key exchange remains in band
- Adding PQC **still** exposes key exchange material to harvesting
- If PQC is weakened or compromised later, today's traffic becomes decryptable

Customers need a solution that removes in-band exposure entirely.

quantropi

Introducing QiSpace™ Digital Quantum Key Distribution (D-QKD)

- Delivers keys out-of-band, not negotiated in-band
- Works seamlessly with IPSec, MACSec, OTNSec
- Works across any IP network infrastructure — no strict fiber dependencies, no distance limits
- Lightweight software only deployment
- Standards based: D-QKD Nodes implement ETSI-014 & SKIP interface standards
- Follows NSA published security guidance on securely implementing Pre-shared keys over digital networks



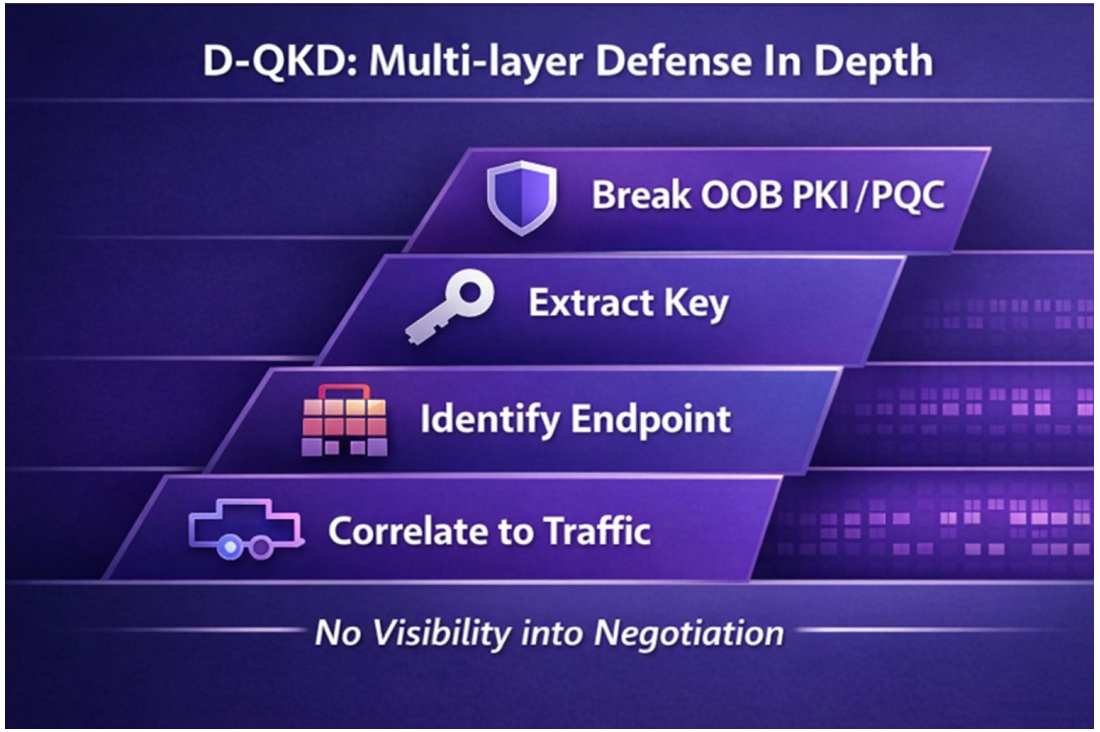
D-QKD eliminates HNDL attacks and PQC risks.

quantropi

Defense in Depth: Why D-QKD is Harder to Attack

To compromise D-QKD an attacker would need to target the out of band (OOB) channel. They would need to:

- Break the PKI/PQC protecting the OOB D-QKD transport
- Extract the delivered key
- Determine which firewall or endpoint it belongs to
- Correlate it to a specific in-band traffic flow
- Do all of this without any visibility into in-band key negotiation (because none exists)



Multi-layer protection makes compromise effectively impossible.

quantropi

Why have a STRONG Lock if you have a WEAK Key?

- Out-band-keying eliminates the possibility of an attacker compromising the AES-256 key exchange mechanism to access encrypted traffic
- The AES-256 algorithm itself is accepted as “Quantum safe” because even a Quantum-based attack cannot compromise the encryption mechanism (aka the “Lock”) to extract data
- An attacker must therefore seek other ways to obtain the Key
- AES-256 Keys are generated from Random Number sequences also referred to as “Entropy”
- **Cyber threats powered by AI/ML are now used to guess / predict / calculate AES-256 Keys because of weakness or predictability of the Random Number sequences**

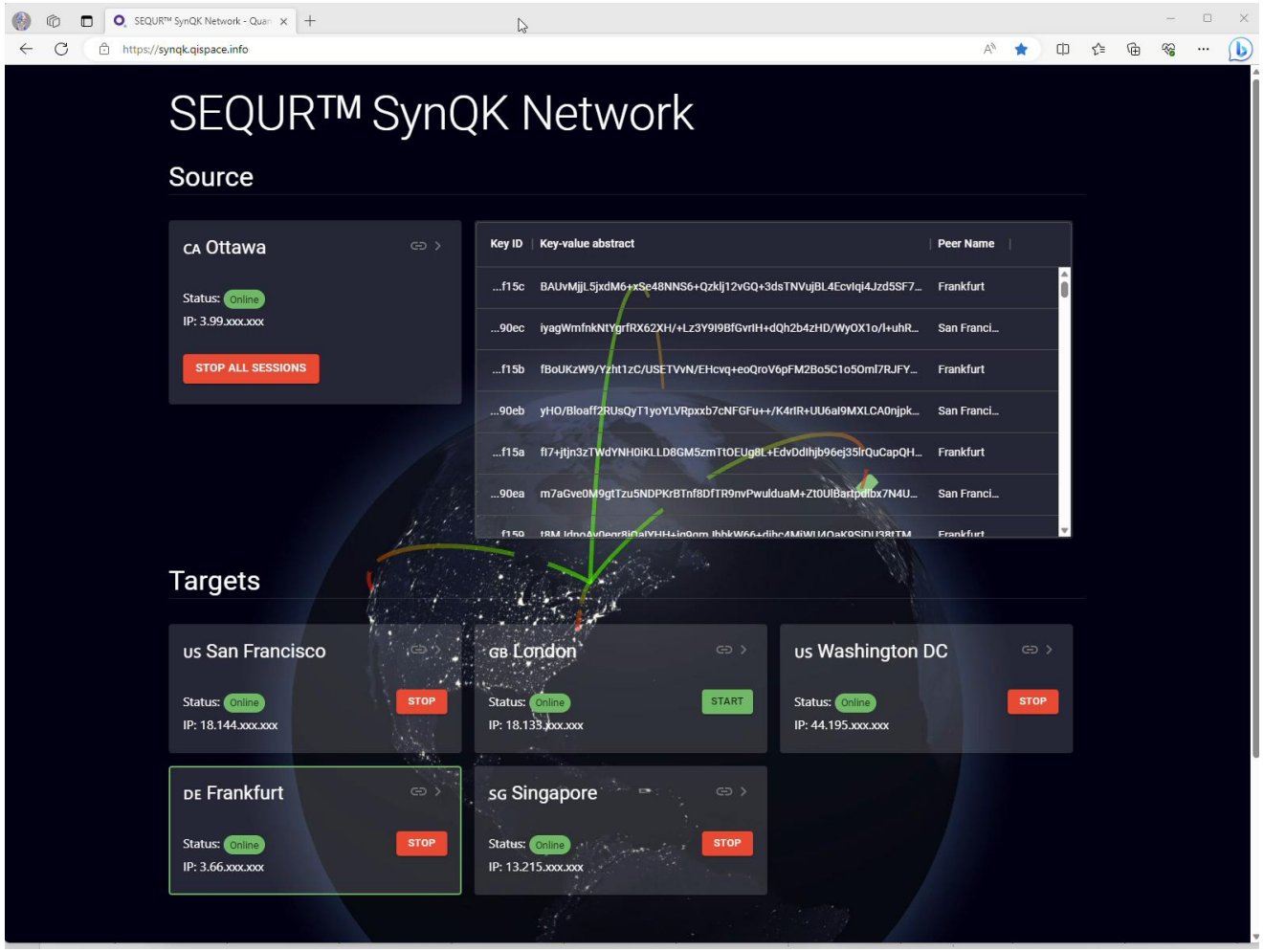
quantropi

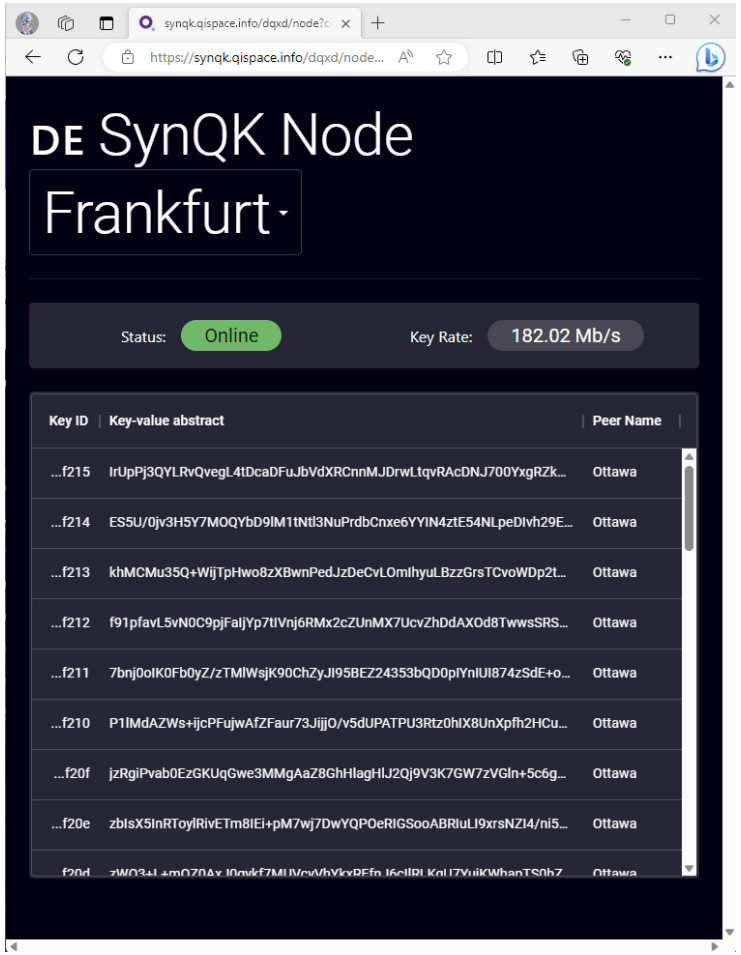
Quantropi's Quantum Entropy Differentiators

- **Entropy Sovereignty:** Customers have complete ownership and control over where their entropy is generated and how it is stored and used.
- **Multisource QRNG Generation:** QiSpace™ utilizes a multisource portfolio of industry leading quantum random number generators to ensure entropy source diversity and quality.
- **Quantum Secure Distribution:** QiSpace™ uses quantum secure symmetric encryption for transmissions to enable high-performance distribution, at gigabits per second, over existing internet infrastructure.
- **Entropy Expansion:** QiSpace™ provides platform resiliency against peak demand and flexibility for connection limited and offline endpoints.

quantropi

QiSpace™ D-QKD Powered by Strong Entropy Network





quantropi

Quantropi D-QKD vs. Photonic QKD

QiSpace™ D-QKD offers significant advantage over Photonic QKD:

- No expensive, specialized endpoint hardware
- No optical fiber requirements
- No distance limits
- No trusted nodes
- No limits on multi-node connections

Photonic QKD not recommended by US or EU intelligence agencies

Digital QKD brings quantum security to real-world infrastructure.

quantropi

Case Study: Deutsche Telekom Benchmark

Quantropi deployed QiSpace in the Deutsche Telekom Open QKD Lab **to test system compatibility and Enterprise-scale performance**.

- Concurrent AES-256 Sessions:
  - QiSpace™ D-QKD: **1.4 Million**
  - Toshiba: **1200**
  - ID Quantique: **12**
- Quantropi D-QKD keys passed NIST 800-22, ENT and Dieharder randomness tests essential for assuring cryptographic integrity

Deutsche Telekom / Quantropi Publication

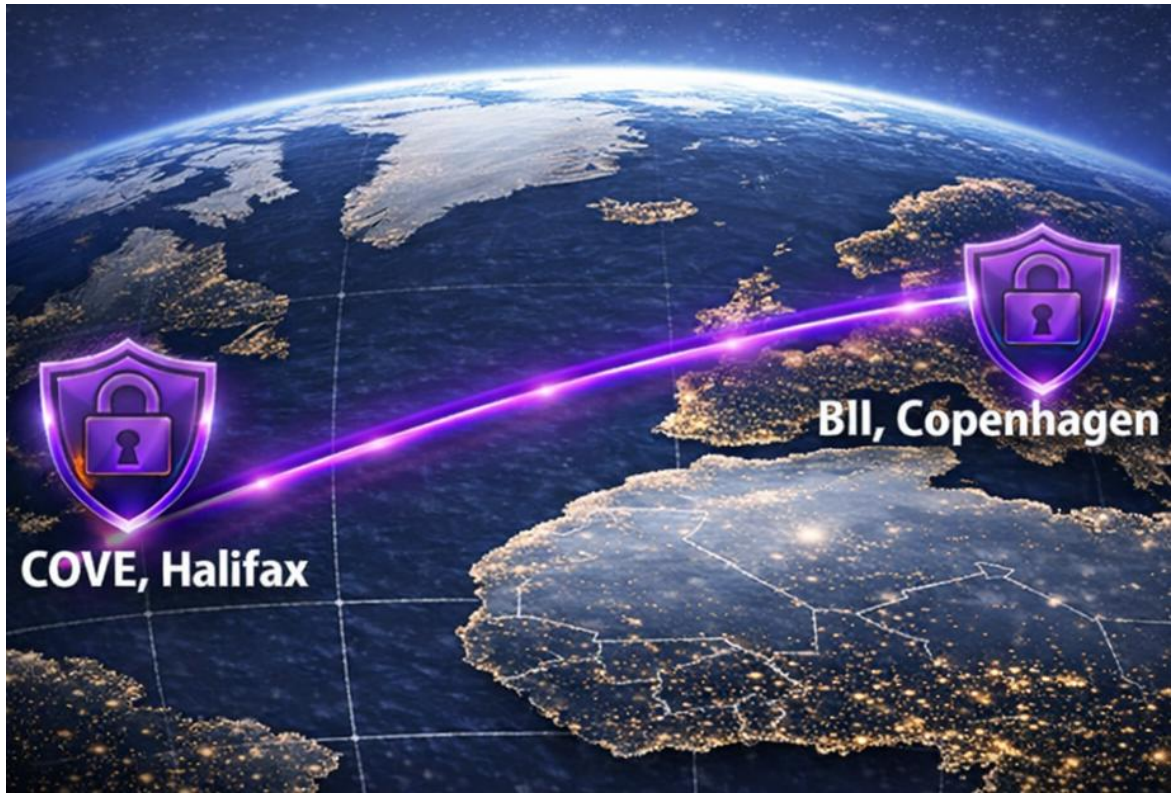
QiSpace dramatically outperformed photonic QKD solutions for a fraction of the cost with no distance limitations.

Case Study: NATO Transatlantic Quantum-safe Networking

Quantropi installed QiSpace in two NATO network locations to create **the first NATO Quantum-safe transatlantic network.**

- The Quantropi solution integrated directly with NATO's existing Palo Alto Networks firewalls
- The connection spanned over 5000 km between Halifax, Canada and Copenhagen, Denmark
- Quantum entropy source used for strong cryptographic key generation

Quantropi Delivers First NATO Quantum Safe Network Connection



Proven quantum security capability for sensitive networks and global operations.

quantropi

Case Study: Nokia Optical Network Integration

Quantropi delivered QiSpace as a **quantum security overlay for Nokia fiber networks** at the Numana technology testbed.

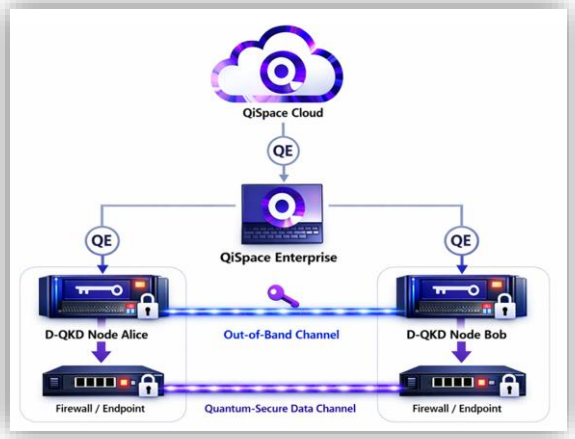
- Kirq by Numana is Canada's only quantum-safe tech testbed that simulates real world conditions and networks
- Quantropi's D-QKD solution was deployed to upgrade existing Nokia fiber network to complete Quantum Security without specialized equipment or dedicated fiber
- Quantum security demonstrated at full network bandwidth up to fiber capacity of 800 Gbps

Quantropi Announces NOKIA Quantum Safe Integration

Carrier-grade quantum security trusted by Telecommunications OEMs.

quantropi

QiSpace™ D-QKD Vendor Support



paloalto NETWORKS

cisco

HPE juniper networking

FORTINET

NOKIA

ciena

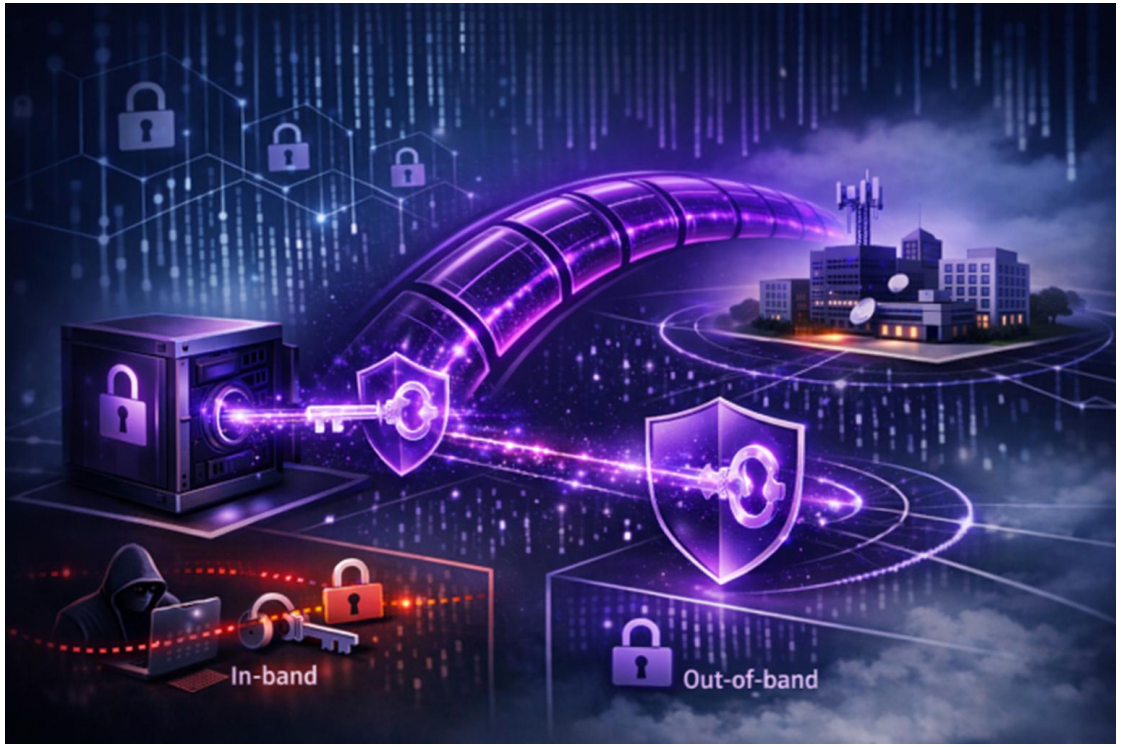
ribbon

Quantum-safe solution for Leading Manufacturers.

quantropi

Summary: Why Choose D-QKD

- Software only deployment, works on existing physical, virtual, and cloud environments
- Eliminates HNDL risk
- Removes in-band key-exchange exposure
- Future-proofs against potential PQC weaknesses
- Compatible with existing infrastructure from Cisco, Ciena, Fortinet, Nokia, and Palo Alto
- Delivers quantum-grade entropy at scale
- Proven, standards-based, and operationally simple



D-QKD is the most practical path to quantum-safe communications today.

quantropi

Bring it On.

Contact Information

Email: sales@quantropi.com

Website: www.quantropi.com

LinkedIn: https://www.linkedin.com/company/quantropi/