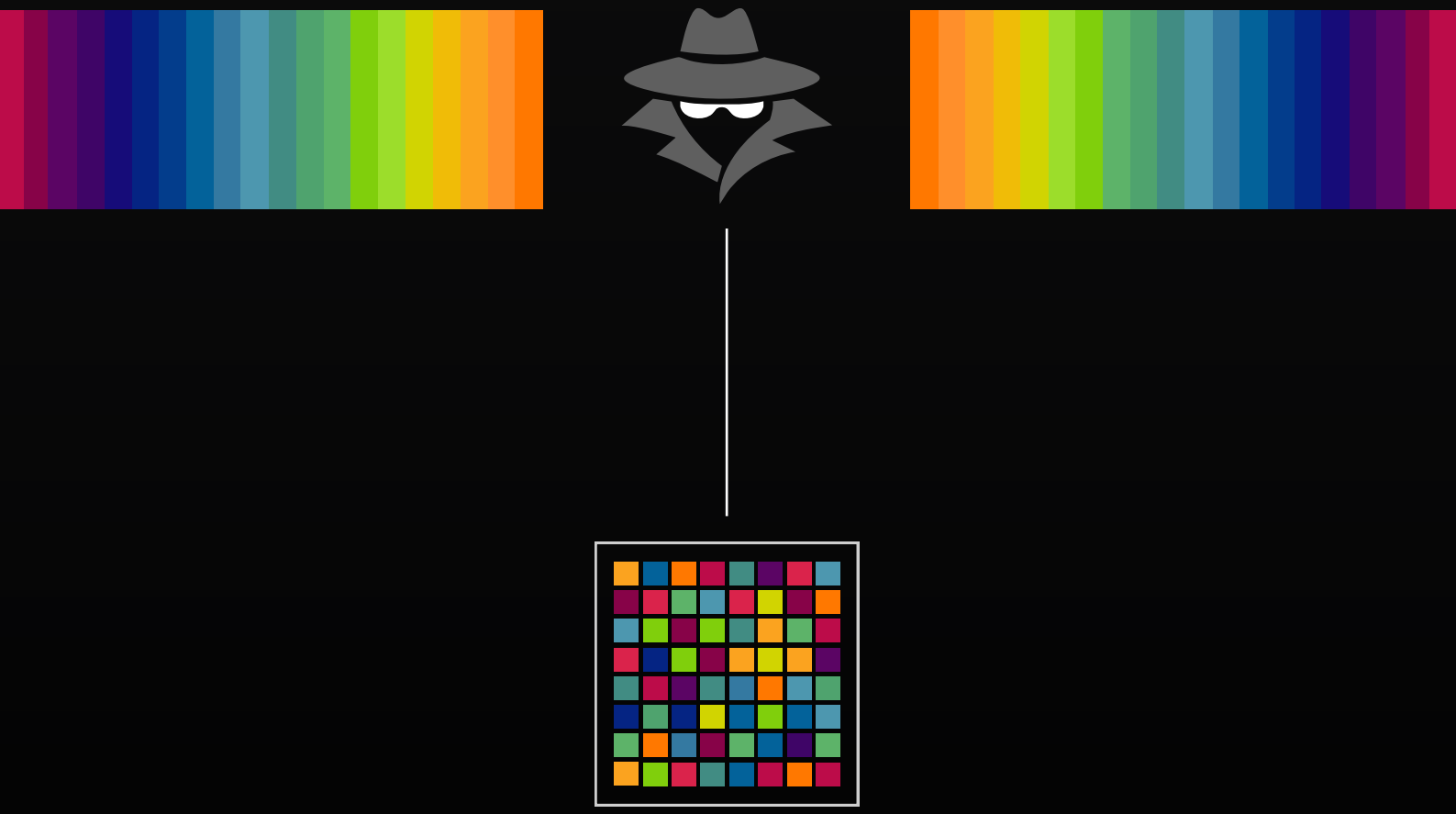
CyberRidge

How to Mitigate the Risk of HNDL Attacks

Protecting Data-in-Transit From Post Quantum Computing



Agenda

01 The Harvest Gap: Securing the Future of Data-in-Transit

02 What is an HNDL Attack?

03 How is Data Harvested?

04 How to Assess Your Enterprise Risk to Harvesting?

05 How to Implement HNDL Protection?

06 How to Measure the Success of an HNDL Solution

07 Beyond the Algorithm: Building Perpetual Resilience

08 About CyberRidge

The Harvest Gap: Securing the Future of Data-in-Transit

As quantum computing advances, a silent threat is compromising the long-term confidentiality of our most sensitive data. "Harvest Now, Decrypt Later" (HNDL) attacks allow adversaries to intercept and store encrypted traffic today, waiting for the inevitable arrival of cryptographically advanced quantum computers to unlock it. For those securing the data traversing across fiber optic backbones, the risk is not theoretical; the active exfiltration of intellectual property and national security assets is already happening.

"There is nothing you can do to protect data already harvested, so act now to minimize and manage the risk of a 'Harvest Now, Decrypt Later' (HNDL) data breach, even if the danger doesn't feel imminent."

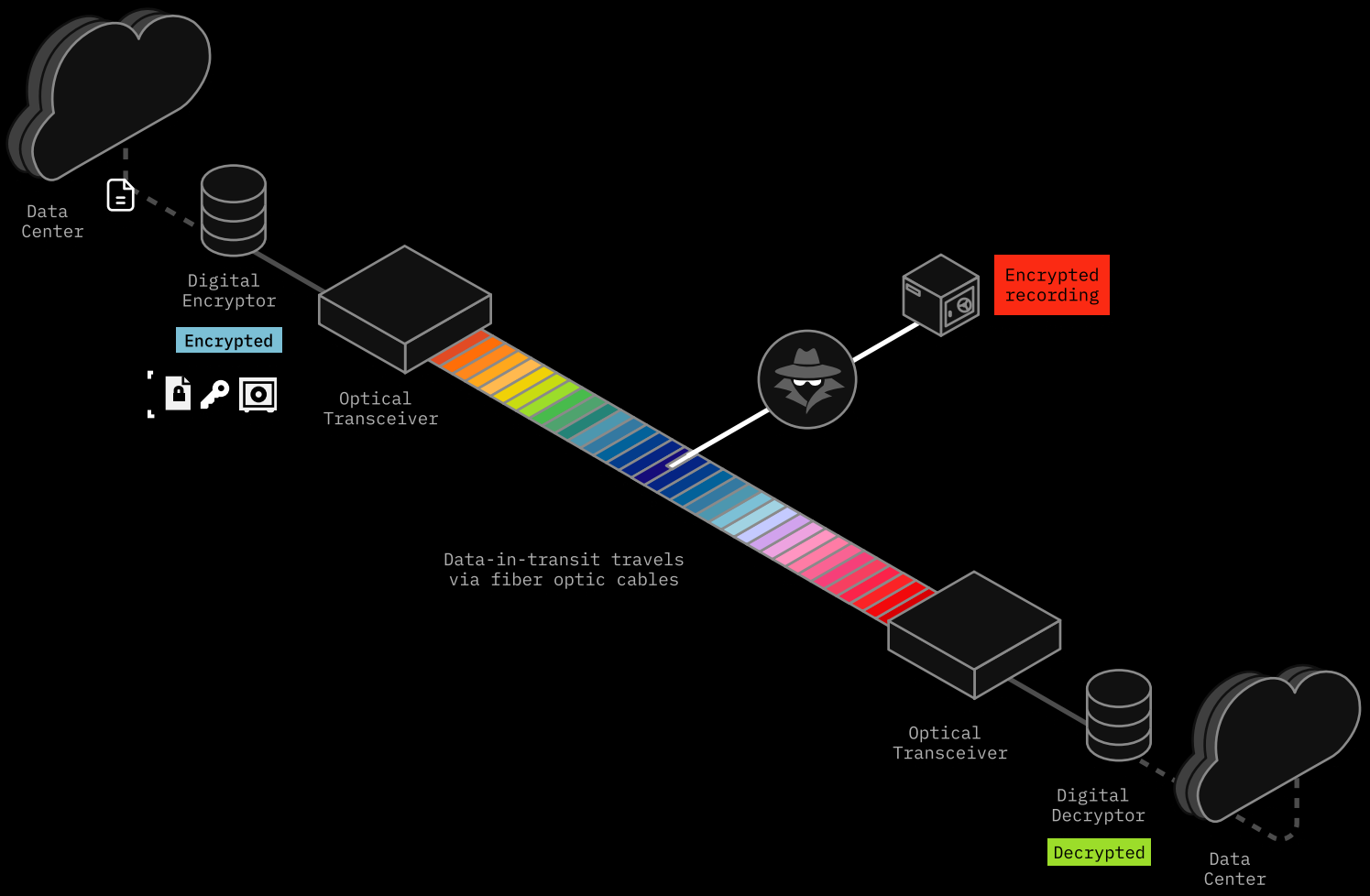
Gartner, '"Harvest Now, Decrypt Later" Attacks Aren't Just a Postquantum Problem', March 2026

This CyberRidge Whitepaper explores the different methods of how data is harvested, how to assess your enterprise risk to various attack vectors, the multi-layered approach that is recommended for securing data-in-transit, and finally, how to measure the effectiveness of your security program.

What is an HNDL Attack?

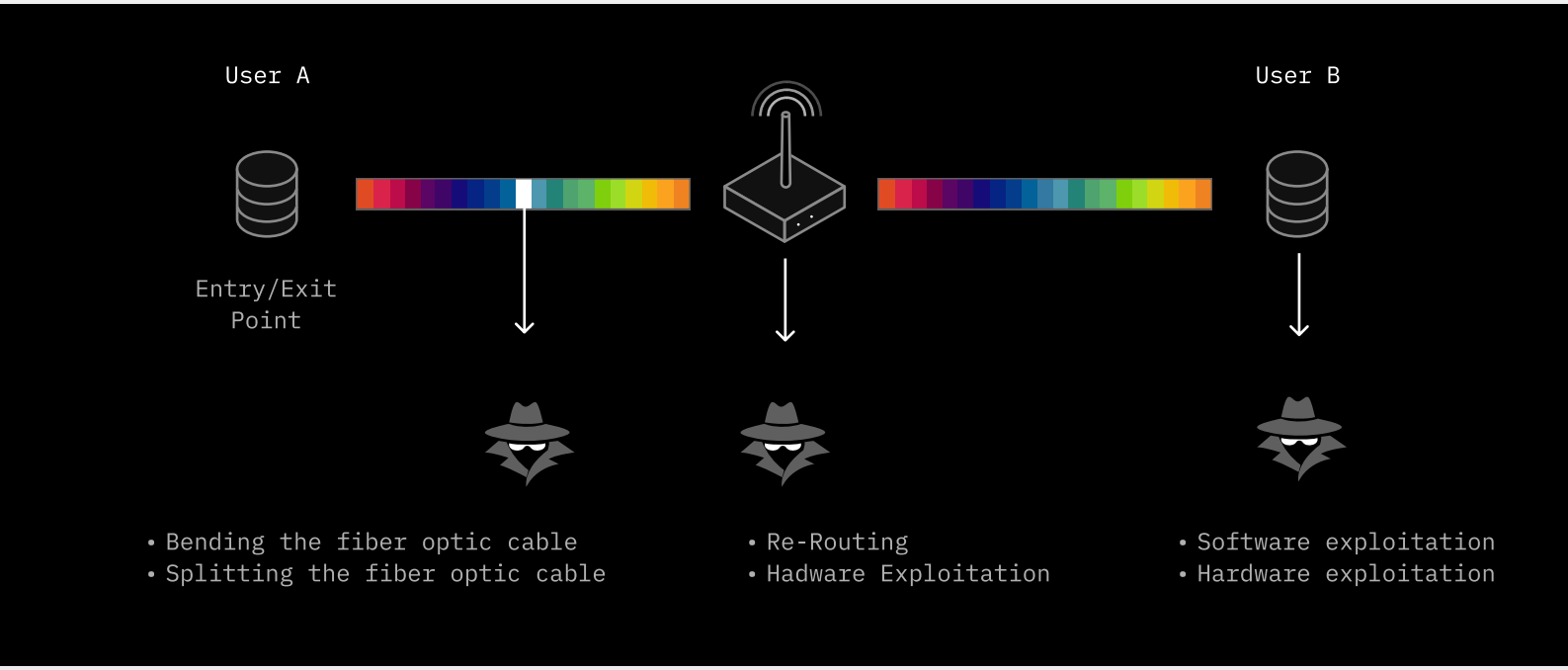
An HNDL (**Harvest Now, Decrypt Later**) attack is a long-game cybersecurity compromise where an adversary intercepts and stores encrypted data today, with the intent of decrypting it in the future. While the data is currently protected by modern encryption (like AES-256 or RSA), the attacker waits out the "Harvest Gap"; the period between the moment data is captured and the moment quantum computing becomes advanced enough to break that encryption. And this deadline is continuously closing in, as time marches forward on the one hand, and technological advancements bring it closer on the other.

Aware of the restraints that quantum computing currently imposes on them, Adversaries target high-value, "long-lived" data (such as state secrets, intellectual property, or medical records) that will still be sensitive or valuable in five to ten years. With the ability to harvest the data today, the data is stored within massive archives of stolen traffic, waiting for a quantum computer to decrypt the data and render it in plain text. Entirely overcoming cryptography's complex mathematical defenses



How is Data Harvested?

There is a lingering myth that fiber cables are inherently more secure than copper. Unfortunately, there have been more than enough incidents to shatter this perception and demonstrate how easily traffic can be diverted or physically siphoned. Attackers can use a range of different methods to obtain unauthorised access to data transmissions, regardless of the applicable equipment. These are the common methodologies used by adversaries to harvest and compromise data.



Digital Tapping: Invisible Redirection

Digital tapping focuses on manipulating how data flows through the network without ever touching a physical cable.

- **Re-routing**: Attackers exploit routing protocols (like BGP) or perform Man-in-the-Middle (MITM) attacks to trick the network into sending traffic through a rogue server. Once the data passes through the attacker's "checkpoint," it is cloned and stored before being passed to its original destination, leaving the sender and receiver completely unaware.
- **Hardware Exploitation**: By exploiting software vulnerabilities in routers and switches, adversaries gain administrative control. This allows them to install "logic taps" that mirror all traffic to an external storage site, effectively turning your own infrastructure against you.
- **Signal Interception and Sniffing**: Once traffic is diverted, attackers use Sniffing tools, software or hardware protocol analyzers, to "listen" to the traffic. They capture the digital "fingerprint" of the data, stripping away transport headers to reveal the encrypted payload. This payload is then indexed and moved to high-capacity storage arrays, where it sits in the "Digital Vault" for future decryption.

Physical Tapping: Siphoning the Light

Physical tapping is surprisingly "low-tech" and inexpensive, requiring only physical access to the line.

- **Entry/Exit Points:** Infrastructure is only as secure as its weakest door. Attackers target street cabinets, communication tunnels, and manholes. By posing as maintenance crews, they can install small, unobtrusive hardware (like a Raspberry Pi or dedicated optical sniffers) at these junction points to capture raw data streams.
- **Bending the Fiber Optic Cable**: This is the most common stealth technique. When a fiber cable is bent beyond a specific radius (typically 6.5–7.5 cm), "macrobending" occurs, where light leaks out of the core through the cladding. An attacker uses a clip-on coupler to catch this leaked light, capturing the signal without breaking the fiber or causing a detectable loss in signal strength.
- **Splitting the Fiber Optic Cable**: Using an optical splitter, an attacker physically cuts into the fiber and inserts a device that divides the light signal. While a portion continues to the intended destination, a small percentage is diverted to a recording device. This method is highly effective for high-volume harvesting on trunk lines and undersea cables.

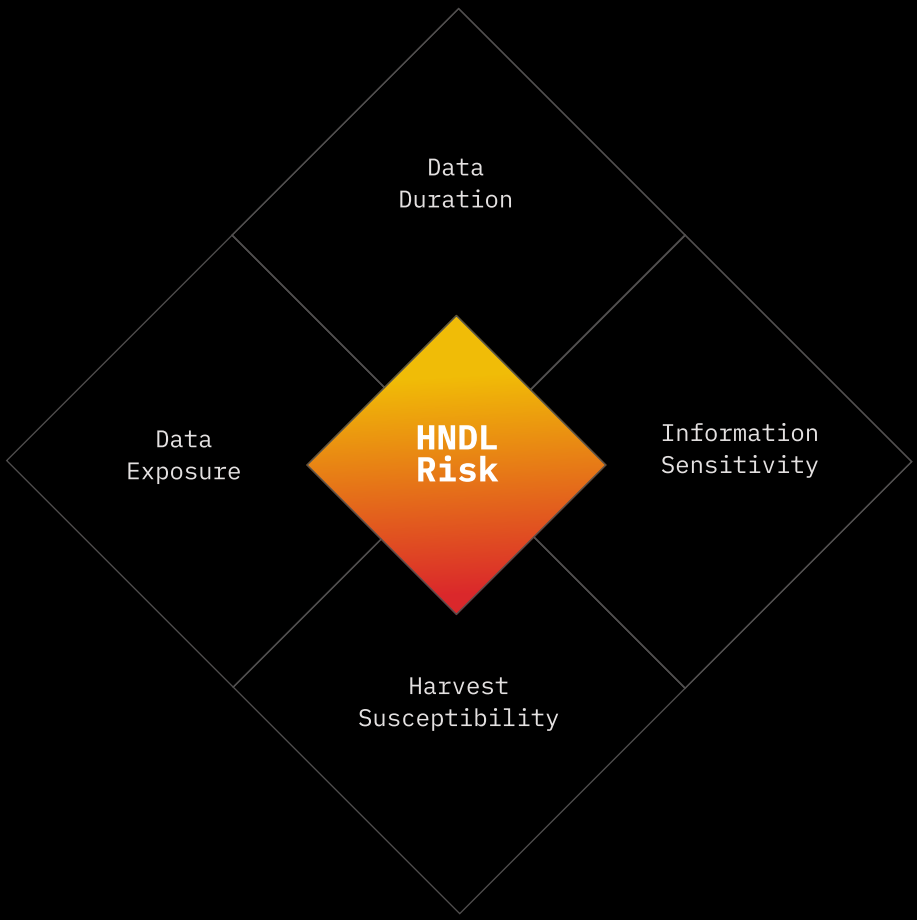
How to Assess Your Enterprise Risk to Harvesting?

Before deploying a solution, infrastructure leaders must quantify their exposure to the "Harvest Gap." Not all data requires the same level of protection, but for large-scale infrastructure and telecommunication providers, the risk is often systemic. To assess your risk, evaluate your data through the following four lenses:

1. Data Duration

The most critical factor in HNDL risk is the duration for which your data must remain confidential.

- **Short-lived data** For example, a single-use password has low HNDL risk.
- **Long-lived data** For example, intellectual property, blue-prints, 20-year government contracts, or medical records, face extreme risk. If your data must remain secret past 2029, the earliest year experts predict a 75% chance of decryption by quantum computers, it is a prime target for harvesting today.

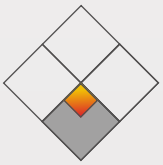


2. Information Sensitivity

Assess what the cost is if the data were to be breached. For infrastructure companies, this could mean the exposure of long-term strategic plans, grid vulnerabilities, or sensitive customer metadata. If the information retains its exploitative value if it falls into the wrong hands, it is currently under-protected by standard "recordable" encryption.

3. Data Exposure

As earlier established, fiber optic cables are not a closed loop and the presence of attack vectors makes data exposure a continual threat. The easier it is to exfiltrate or intercept data, the greater its risk. This risk is amplified with reliance on third-party carrier backbones that support public networks or lack data exfiltration controls.



4. Harvest Susceptibility

Current cryptographic standards are failing to keep pace with "harvesting" capabilities.

- **The RSA/ECC Trap**: Most current infrastructure relies on asymmetric encryption (RSA/ECC) that is mathematically proven to be broken by Shor's Algorithm.
- **The Recordability Flaw**: Even "strong" encryption like AES-256 remains **recordable**. An adversary does not need to break the math today; they only need to successfully siphon it to store the digital fingerprint.

If you carry high-sensitivity data with a 5+ year lifespan over geographically exposed fiber, your enterprise is currently operating within a critical "Harvest Gap." Taking a multi-layered approach of HNDL solutions, is the most guaranteed method for protection against future decryption.

How to Implement HNDL protection?

To protect data-in-transit against HNDL attacks, no single technology is a silver bullet. Resilience is found in layering mathematical defenses with physical-layer protections to ensure that even if one layer is bypassed, the data remains inaccessible.

Here is an analysis of the current solution landscape:

1. Data Exfiltration Controls

Traditional encryption (MACsec at Layer 2, IPsec/TLS at Layer 3) remains the foundation of network security, but it was designed for an era where "capture" was difficult and "compute" was limited, ensuring that encrypted data stayed encrypted. These protocols use symmetric (AES) and asymmetric (RSA/Diffie-Hellman) math to scramble data packets.

This solution is ubiquitous, and typically built into existing routers and switchers, making them relatively easy to install and implement with most modern line cards from vendors like Cisco or Juniper supporting MACsec at wire speed.

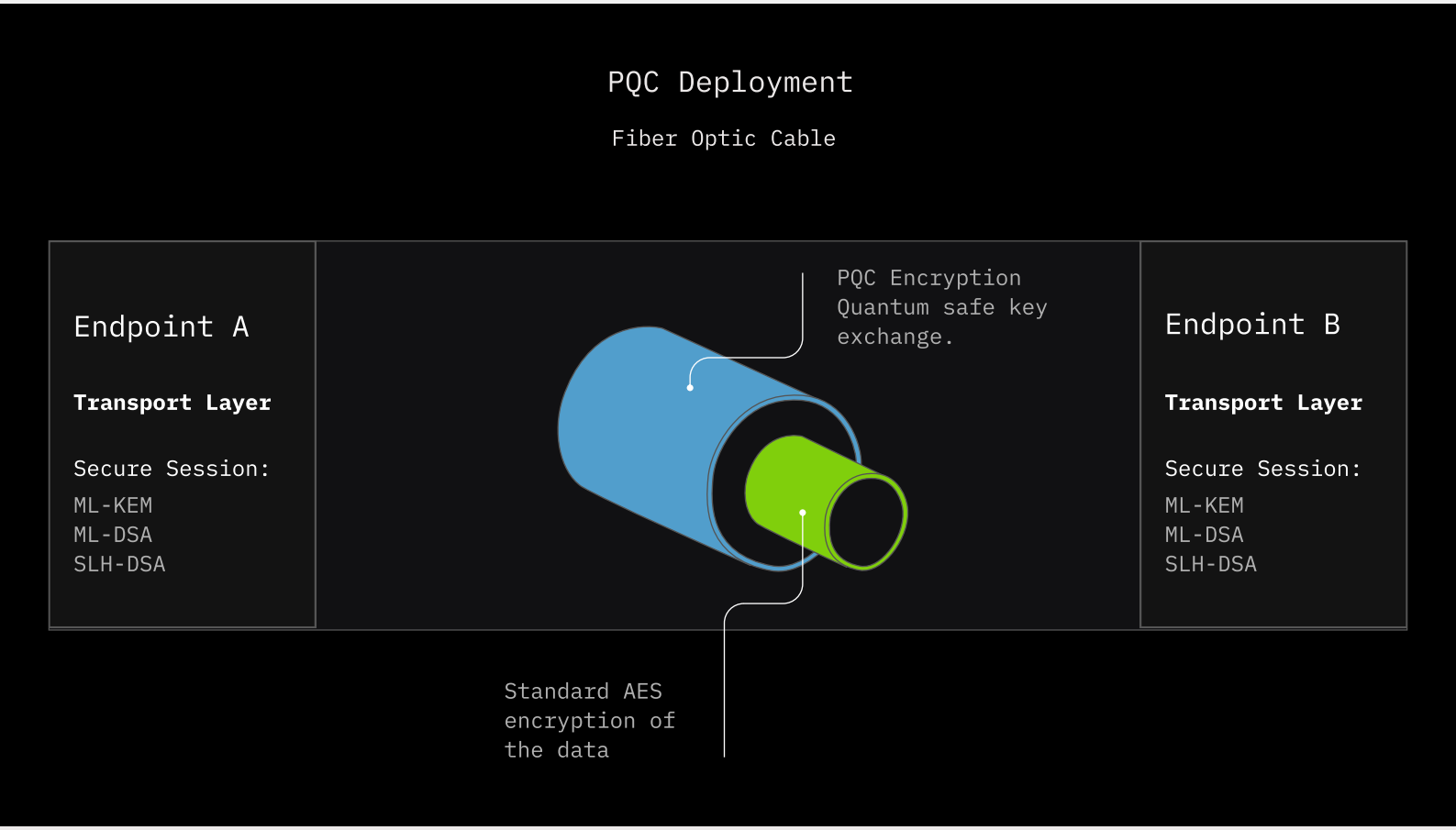
Yet, while these solutions will effectively stop casual eavesdropping and are low friction to install, they're fairly easy to decrypt and undermine. Depending on the algorithm, the "ciphertext" will produce a perfect digital copy of data, albeit locked data. This 'locked box' is susceptible to being harvested, and decrypted when a quantum compute 'key' can be forged.

2. Post-Quantum Cryptography - PQC

A software-defined solution, PQC is aimed at replacing standard encryption and digital signature algorithms with lattice-based, code-based, or hash-based cryptography. All these methods produce mathematical problems that are resistant to quantum computing power and advanced decryption methods like Shor's Algorithm. Essentially providing a "math-based" shield against "math-based" quantum attacks. Over the coming years it is expected to become the mainstream solution through NIST standardization.

PQC is a highly scalable, inexpensive solution that doesn't require any new fiber infrastructure. Typically, it integrates easily within existing systems and is easily maintained with software updates. The main risk to PQC is the very method through which it protects. It is betting on a future where there are no further mathematical breakthroughs (quantum or classical) that will be able solve its complex problems. This is where it remains vulnerable in a post-quantum future. Also importantly, PQC produces recordable ciphertext that can be harvested. If an adversary captures PQC-encrypted data today and the algorithm is found to have a flaw in the post-quantum era, the data can still be compromised retroactively.

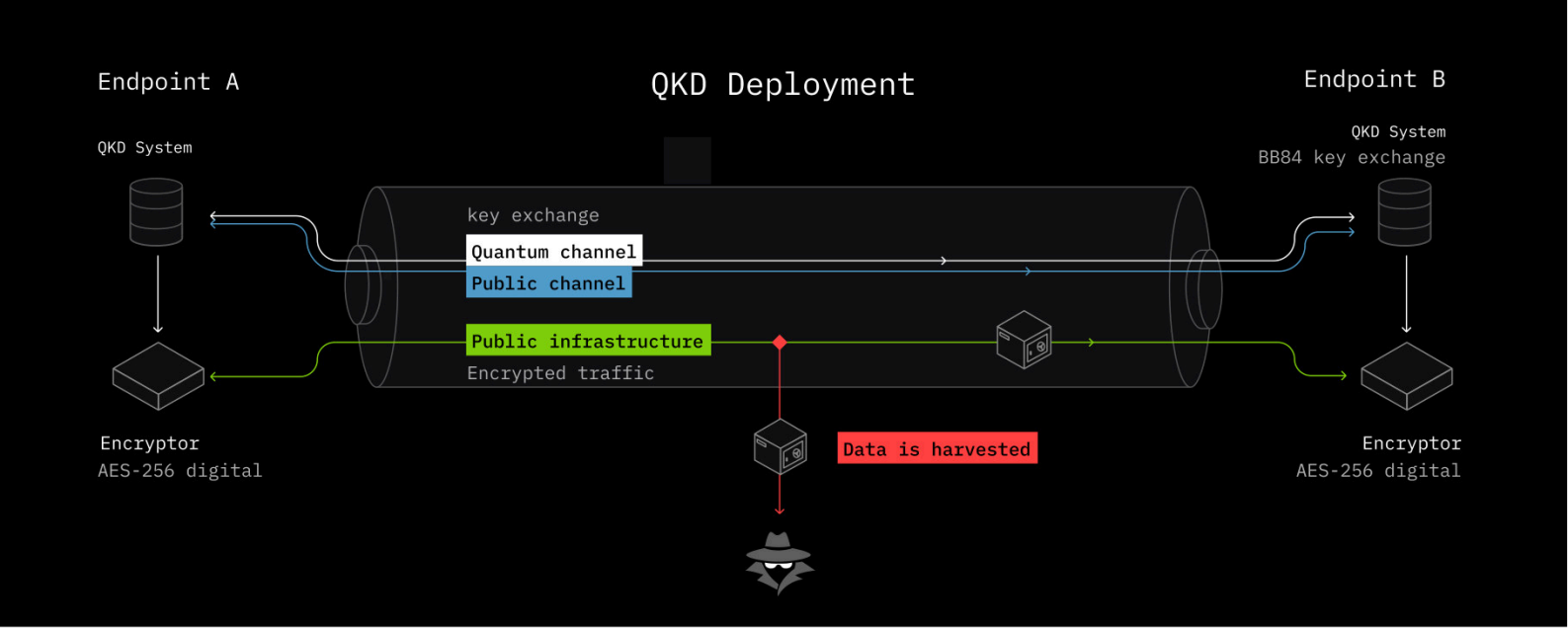
Additional risk factors include the possibility of PQC encrypted keys being leaked and falling into the wrong hands. The data is exposed without even having to wait for quantum advances. Finally, there is also the concern of added latency because of the intensive processing power required.



3. Quantum Key Distribution – QKD

QKD shifts the security from the mathematical encryption of data to the physics based distribution of keys. Its quantum physics follows a basic rule; if you measure a quantum particle, you disturb it. Therefore any attempt by an attacker to measure, and thus harvest, the photons disturbs their state, causing the system to detect it immediately. Deployed by using a hardware based solution, single photons are sent across dedicated fiber links. The quantum physics design makes it immune to key hacking. The hacked bits are revealed and cannot be used for the key.

The downside to QKD are its deployment limitations within standard infrastructure set-ups. It has severe distance limitations, typically <100km (incompatible with amplifiers), and it requires expensive, dedicated quantum hardware installations. Additionally, it's important to note that because QKD does not encrypt the data, but only the key, the actual data payload is still sent using traditional "recordable" encryption, meaning the payload itself can still be harvested.



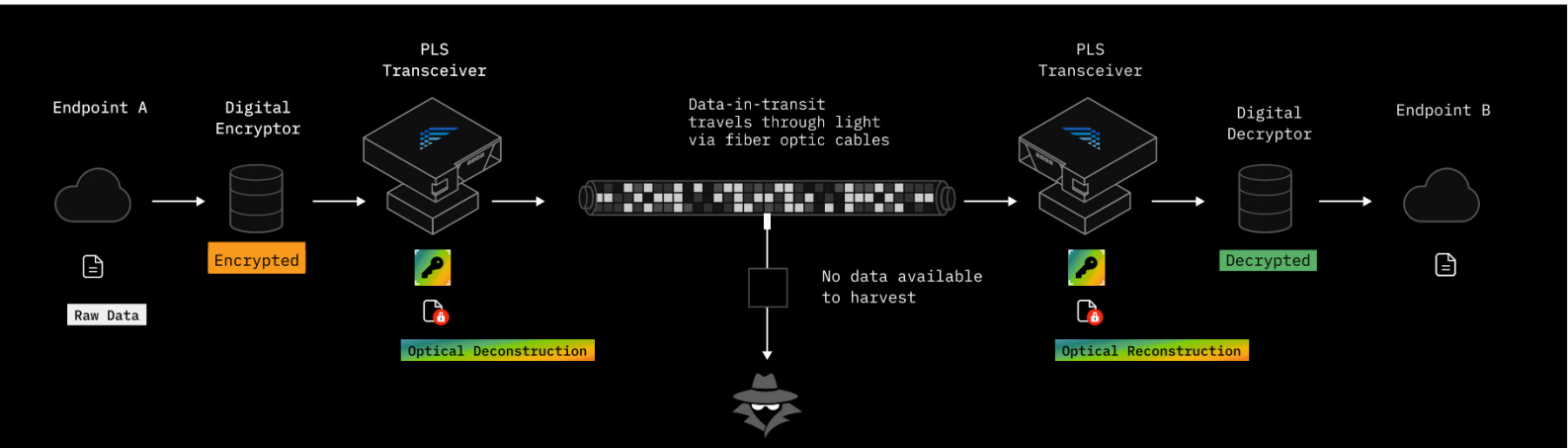
4. Photonic Layer Security – PLS

PLS takes a whole new approach to protecting data in transit with its focus on protecting the medium, rather than the message. Meaning, that instead of using mathematical based encryption to protect the data or the keys, it operates at the Layer 1 photonic level to transform data into optical noise.

There are numerous advantages to this; Firstly, it makes the signal physically unrecordable, if an adversary cannot capture a reconstructible digital fingerprint of the data, that means there is nothing available for them to harvest, nothing to store, and nothing to decrypt, even in a highly advanced post-quantum future.

Secondly, it carries almost zero latency. Since processing happens at the photonic level, as an optical solution data is transformed at the speed of light. There is no encryption delay or packet overhead to slow down the transfer of data.

Finally, its infrastructure requirements are very low. Using a transmission box which substitutes standard line cards, it works over existing DWDM/Fiber infrastructure, therefore no modifications to the fiber infrastructure are required.



Comparison Table of HNDL Solutions

	Photonic Layer Security (PLS)	QKD	PQC
Technology	Analog light manipulation	Quantum Mechanic Laws	Digital Key Algorithms
Main Claim to Fame	Eliminates HNDL at the physical layer	Physics drives absolute key secrecy	Resiliency provided; easy to implement software based
Encryption Scope	Delivers full high-speed **payload & keys** encryption	Delivers encryption **Keys Only** (data encryption - classical AES)	
Hardware Solution Scope	Complete encryption & transmission system (replacing the existing transmission system)	Requires dedicated quantum hardware + Key Management Software (Must use existing transmission system)	Software only
Network Integration	"Plug-And-Play" integration with existing & legacy infrastructure	Requires a dedicated fiber / wavelength	Requires an extensive software migration
What's visible to a fiber-tapping attacker?	Nothing! (optical noise)	Signal is recordable & Metadata visible	Signal is recordable & Metadata visible
Time to PQR (post-quantum readiness)	< 1 Week	~ Weeks	~ Years
Link Distance	No Limitation (operates with In-line EDFAs)	Up to 100 km (Incompatible with in-line EDFAs)	No limitation (a non-physical method)
Latency	No added latency (Analog light manipulation)	–	Adds significant latency (heavy DSP algorithms)
Additional Features	Energy efficient, No metadata	Inherent wiretapping detection	Software only, flexible

How to Measure the Success of an HNDL Solution

Success in mitigating HNDL attacks isn't just about "checking a box" but rather by quantifiably measuring risk reduction across the infrastructure. The following two standards are widely used for assessing an organization's post-quantum security posture.

Reduction in HNDL exposures

The main aim of your HNDL strategy is to reduce the detection of exposed data that is recordable. Where the objective is to transition from a state where 100% of your fiber traffic is harvestable ciphertext to a state where 0% of your sensitive long-term data can be digitally reconstructed. This exposure rate should ideally be dropped to zero.

Increase post-quantum ready use cases

The journey to a quantum-ready state is long and should be tracked. This "Quantum Migration" progress should cut across diverse use cases, from Data Center Interconnects (DCI) to edge street cabinets. The aim is to increase the percentage of active and mission-critical network links that have post quantum security coverage.

These two measures of success should be conducted over a series of tests to confirm that results are moving in the right direction.

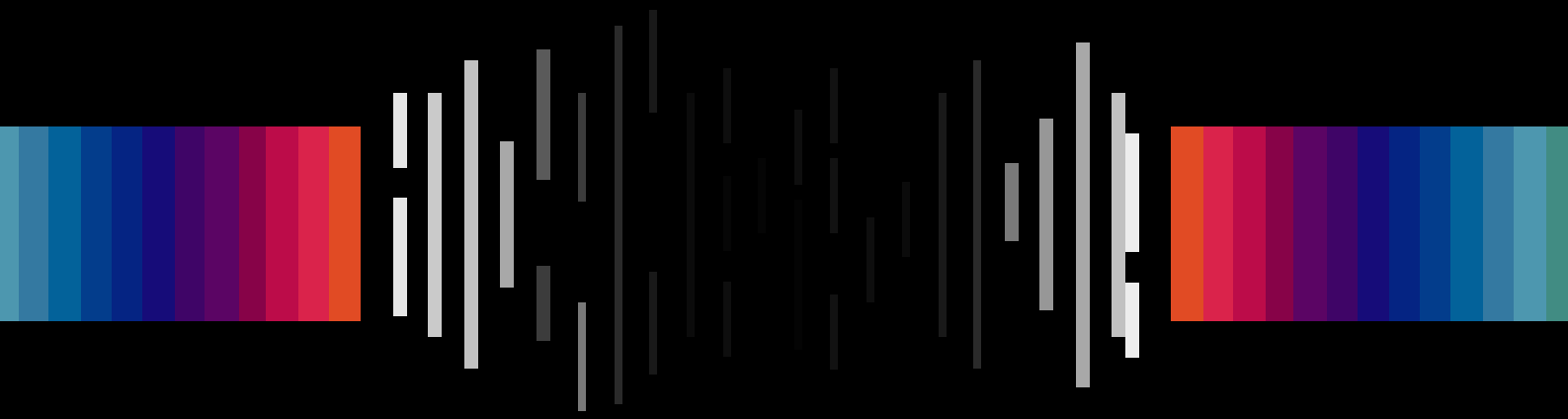
Beyond the Algorithm: Building Perpetual Resilience

As both technology and mathematics progress, even our most advanced defenses face an inevitable expiration date. History has shown that cryptographic algorithms and their associated parameters eventually become deprecated as computing power scales; even PQC is no exception. Relying solely on mathematical complexity means accepting a cycle of constant maintenance, vulnerability patches, and eventual replacement.

To achieve true long-term security, infrastructure leaders must move beyond an encryption-only strategy. A robust defense-in-depth posture requires layering agile software defenses with physical-layer innovations that are immutable to technological shifts. By integrating Photonic Layer Security, organizations can ensure that their data-in-transit is not just difficult to decrypt, but physically impossible to record.

The goal is perpetual protection. A security architecture where the confidentiality of your data is guaranteed by the laws of physics, ensures it remains secure today, tomorrow, and throughout the post-quantum era.

CyberRidge



About CyberRidge

CyberRidge is a deep-tech company delivering a post quantum, harvest proof solution that represents a true paradigm shift for securing data-in-transit. Founded in 2022, it leverages patented photonic layer security (PLS) technology through its flagship Carmel platform.

Operating at the physical layer, it manipulates light to make data in transit physically unrecordable using physics rather than algorithms, interception and recording become impossible. Designed as a plug-and-play solution for rapid deployment, it integrates seamlessly into existing DWDM infrastructures with zero added latency, ensuring mission-grade protection against harvest- now-decrypt -later threats, even in the face of future quantum computing or other advances.

www.cyber-ridge.com info@cyber-ridge.com