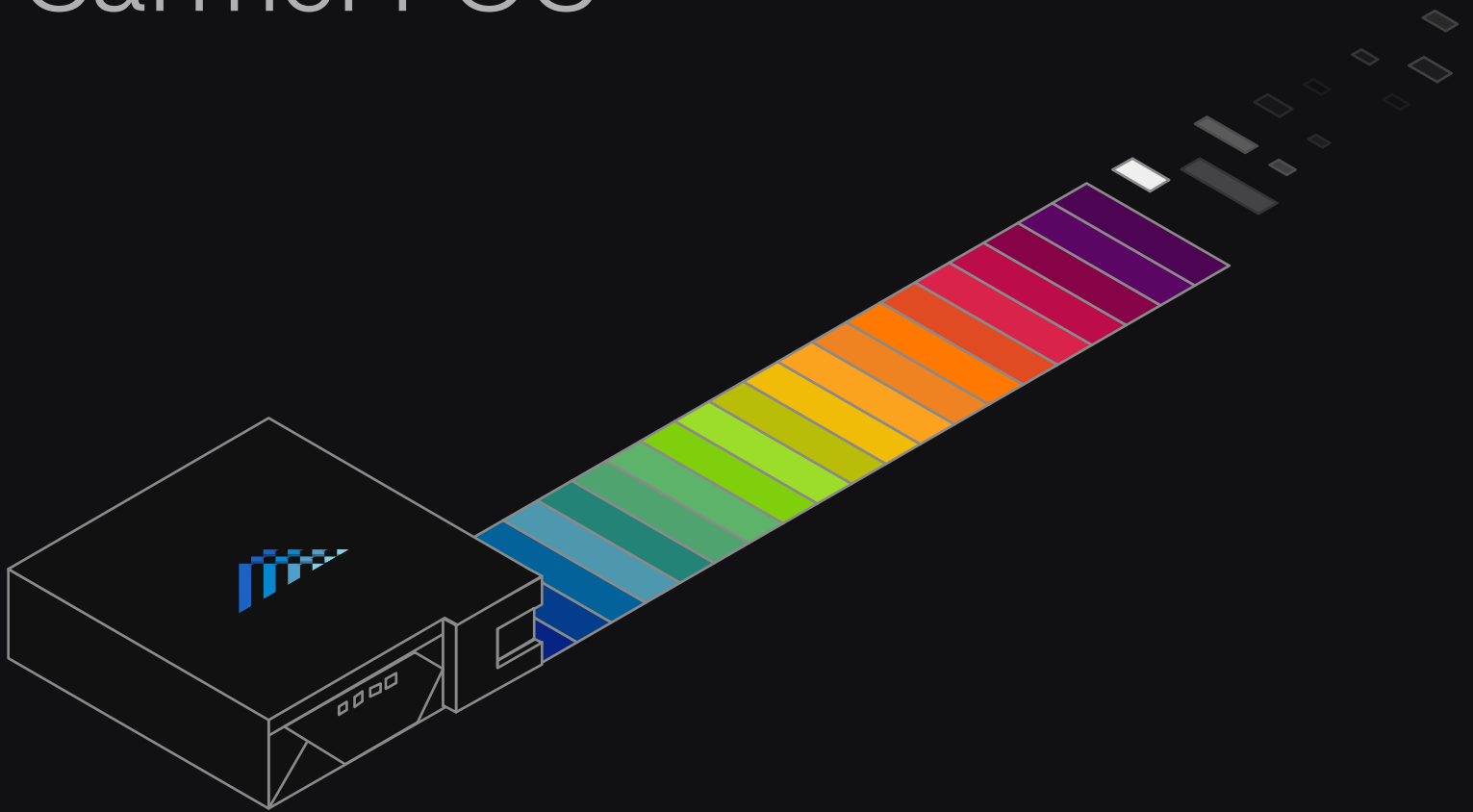


Photonic-Layer Security at a Tier1 Telco: Testing CyberRidge's Carmel POC



Global telecommunications providers are increasingly focused on the "Harvest Gap" – the window in which intercepted data can be exfiltrated today and decrypted by future quantum computers. As part of its broader evaluation of approaches to this challenge, the Telco tested CyberRidge's Carmel system in its optical network lab environment in Eschborn (around 13 kilometers from Frankfurt), examining whether photonic-layer security could meet harvest-proof and infrastructure performance requirements.

The POC demonstrated that CyberRidge's photonic-layer approach can secure data-in-transit on high-capacity topology.

By combining harvest-proof technology with precisely managed noise levels, the system rendered data physically unrecordable across the tested link, addressing the "Harvest Now, Decrypt Later" threat while preserving latency and distance characteristics suitable for Tier-1 operations.

The POC's Objectives

The POC was built to answer several operational questions:

Can a harvest-proof technology operate at the photonic layer across long-haul fiber, given different fibre-spools to simulate different wavelengths and transponder signals? How would it manage across the lab's various amplifiers and ROADMs, without modifying the underlying transport? Different harvest-proof approaches have different operational profiles, and the Telco wanted to characterize how a photonic-layer solution would behave on a representative long-haul topology.

The goal of the evaluation was to determine how CyberRidge's Carmel system performs at the photonic layer under realistic conditions. Could the technology maintain its "unrecordable" state while passing through existing amplifiers? How much of the existing ROADM infrastructure would need to be modified to support deployment? Would the added noise affect adjacent traffic or recoverability at the receiver? Ultimately, the POC was designed to characterize whether photonic-layer security could deliver the distance, flexibility, and physics-based protection relevant to a Tier-1 long-haul environment.

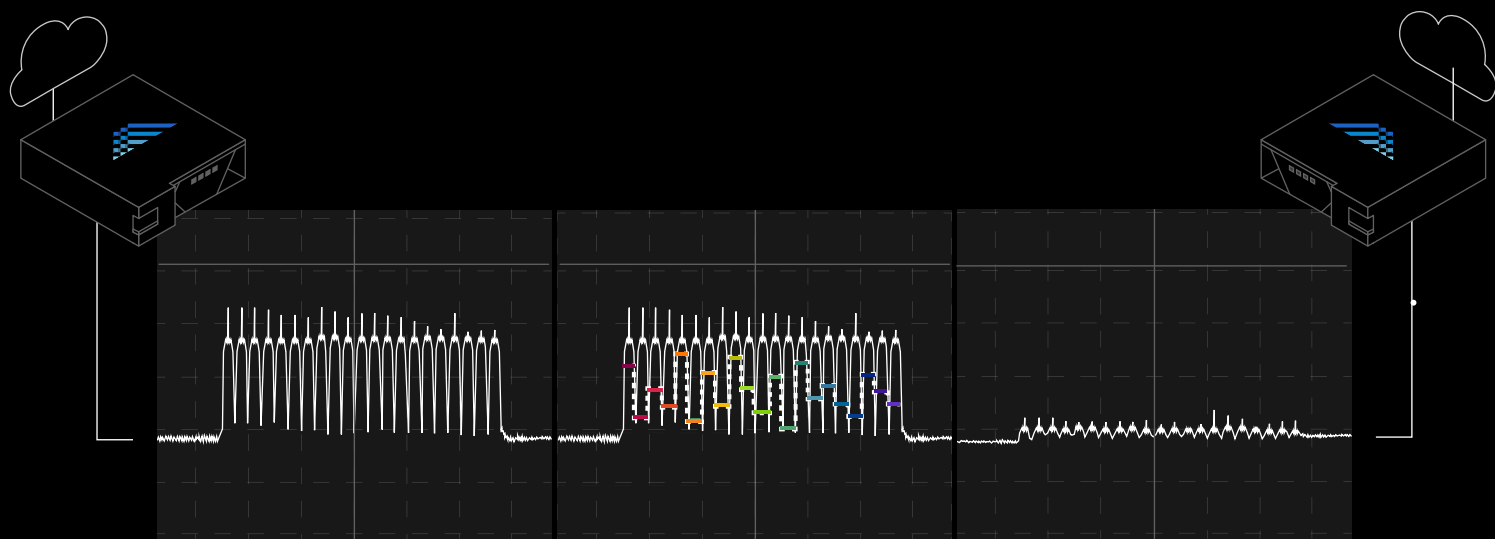
Let's jump into how it went down.

Harvest Proof Technology

The core of the CyberRidge solution is a shift from recordable, algorithm-based cryptography, to a three-layer physical defense that renders data unrecordable. Rather than making data hard to read, the approach is designed to make it physically uncapturable in transit.

The first layer utilizes a Mode-locked Pulse Laser to spread the optical signal across a wide spectral band. By dispersing the signal, the data footprint is expanded far beyond the reach of standard intercept tools. Once dispersed, the Dynamic Optical Encryptor applies Constantly-Changing Encryption (CCE). These keys change every fraction of a second and are embedded directly into the light stream. Because they exist only in transit and are never stored, there is no "master key" for an attacker to steal from a server.

Finally, the signal is aggressively attenuated and buried under a layer of added spontaneous optical noise. This creates a low Optical Signal-to-Noise Ratio (OSNR) that produces a signal too weak to extract any information. To any unauthorized tap or harvesting device, the signal appears as nothing more than random background noise. The combination of all three layers ensures the data is physically unrecoverable and the Harvest Gap is effectively closed. If an attacker cannot record the signal today, they have nothing to decrypt tomorrow, regardless of how powerful quantum computing becomes.



Stage 1

Spread

Mode-locked Pulse laser disperses signal across multi-terahertz spectrum → Hundreds of wavelengths

Stage 2

Encrypt

Dynamic Optical Encryptor applies Constantly-Changing Encryption (CCE) → Keys change every fraction of a second → Embedded in light, never stored

Stage 3

Bury

Noise Loader adds spontaneous optical noise → Signal buried below optical noise floor → Negative OSNR achieved → Information-theoretically unrecoverable (Shannon theorem)

Stage 4

Reconstruct

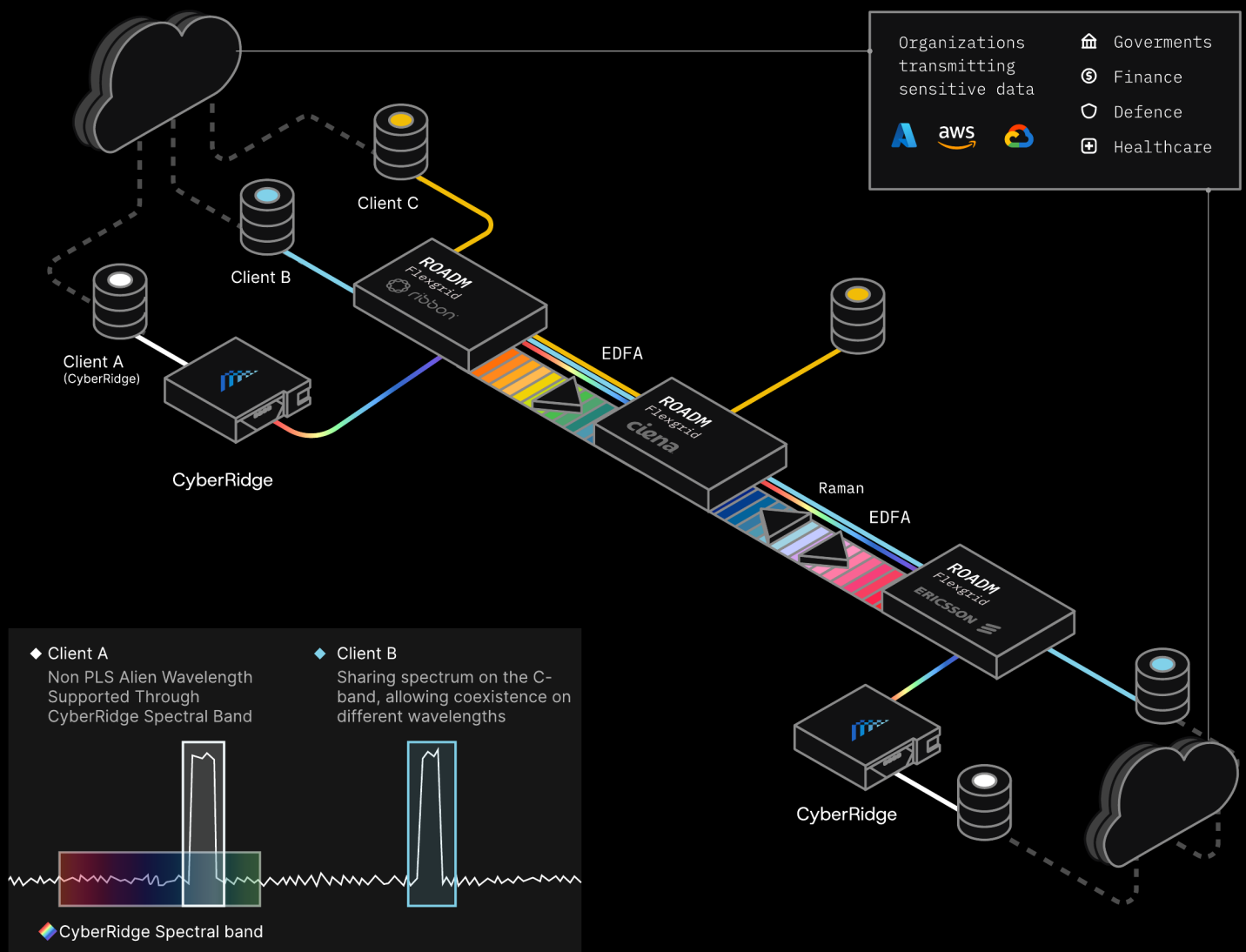
Authorized Carmel receiver with exact photonic key reverses process → Only works at exact microsecond → Attackers see noise; receiver sees perfect data-in-tact.

Deployment Ease

While CyberRidge's internal technology is highly sophisticated, the POC showed its deployment is remarkably simple, even when using complex, multiple network equipment. Key operational highlights included:

- **Universal Compatibility:** CyberRidge was integrated into a topology featuring both EDFA and Raman amplifiers, alongside flexgrid ROADMs. This setup mirrored a standard, high-capacity optical network, demonstrating compatibility with the optical transport and fiber infrastructure used in the test environment.
- **Standard Interfaces:** Supports standard client 100GbE interfaces, ensuring it slots directly into current workflows.
- **Alien Wavelength Support:** Can be deployed as an "alien wavelength" over existing third-party line systems without needing to replace the underlying DWDM equipment.

By acting as a direct replacement for standard line cards, CyberRidge's plug-and-play installation enabled a high-security upgrade in a routine hardware addition.



Long Distance Transfer with Zero Latency

A significant challenge for Tier-1 operators is securing expansive infrastructure – particularly subsea and long-haul terrestrial routes – without compromising on performance. Any harvest-proof solution deployed on these routes has to coexist with standard optical amplifiers and the realities of multi-hundred-kilometer reach.

CyberRidge's Carmel system addresses this requirement by operating at the photonic layer with a robust optical signal. During the POC, the system maintained a secure, harvest-proof link over 205 km, passing through EDFA and Raman amplifiers as well as multiple flex-grid ROADMs.

Critically, this extended reach does not come at the cost of speed. Inline digital encryption typically introduces latency, which is a concern for telcos sensitive to jitter and delays. In the POC, physical-layer security via CyberRidge introduced negligible added latency despite the noise loading. This ensures that mission-critical, time-sensitive services like financial transactions, voice calls, and real-time signaling remain unaffected. For the tested topology, this demonstrated that long-haul fiber routes can be made physically unrecordable while maintaining wire-speed performance.

Noise, Turned From a Bug to a Feature

In traditional optical networking, "noise" is the enemy. If noise levels are too high, the signal remains recordable and vulnerable to interception. However, what is less realized is that if the noise level is too low, the data risks becoming impossible to recover at the receiver end, leading to dropped packets and service instability. In reality, managing noise is a delicate balancing act where both risks need to be minimized.

CyberRidge reframes this dynamic. Its technology, which involves taking a clear signal and aggressively burying it under added spontaneous optical noise, makes it physically unrecordable during transit. The key to this "noise-as-a-feature" model is the precise control that is enabled over the optical equipment.

The system attenuates both the data and the noise in tandem, keeping the signal "hidden" from interceptors while ensuring it remains perfectly recoverable for the authorized receiver. Crucially, this control ensures that CyberRidge coexists harmoniously on the same fiber as other traffic.

Proving Resilience: Attacker Simulations

To prove the resilience of the Carmel hardware against real-world interception, two distinct attacker simulations were demonstrated.

- 1. Naive Attacker – In this scenario, an attacker uses a simple optical tapping equipment to bleed off a portion of the light signal from the fiber. The threshold of accessibility to conduct this type of attack is extremely low, the optical tapping equipment can be easily and simply sourced on the web, while the level of knowledge required to execute the attack is not high.

To mitigate this concern CyberRidge employs a Noise Loader that generates spontaneous optical noise, burying the actual data signal deep below the "noise floor." The Optical Signal-to-Noise Ratio (OSNR) is intentionally degraded for anyone without the optical key, unable to distinguish the data from the background noise. The hardware literally cannot "lock on" to the signal and the attacker is all but able to harvest nothing but scrambled noise.



Fig 03
A site for purchasing a clip-on coupler. They can typically be bought on the internet for anywhere between \$500 – \$2500 per unit.

- 2. The Rogue Transceiver – This simulation addresses a more extreme threat: what if an adversary manages to get their hands on a CyberRidge Carmel unit itself? This explores a "Man-in-the-Middle" (MITM) scenario where the attacker uses the same high-end hardware as the defender to reverse the process and uncover the signal. However, even with the correct hardware, CyberRidge relies on an Air-Gapped CPU that produces Constantly-Changing Encryption (CCE) keys. These keys are unique to the authorized link, leaving the attacker without the specific optical key required to synchronize the de-noising and decryption process. Therefore, the rogue Carmel unit doesn't transition the traffic from the analog (optical) domain back to the digital domain.

POC Findings

For telecommunications companies managing expansive land and sea infrastructure, CyberRidge offers a definitive advantage in securing the physical layer. By combining harvest-proof technology with optimal noise levels, it renders data physically unrecordable without the latency penalties that often plague traditional encryption.

The system also held up under the two attacker simulations run during the POC, both naive optical tapping and the rogue-transceiver scenario. Taken together, the results characterize how a photonic-layer approach to the "Harvest Gap" performs under realistic Tier-1 conditions, and provide a basis for further evaluation alongside other harvest-proof technologies under consideration.



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.