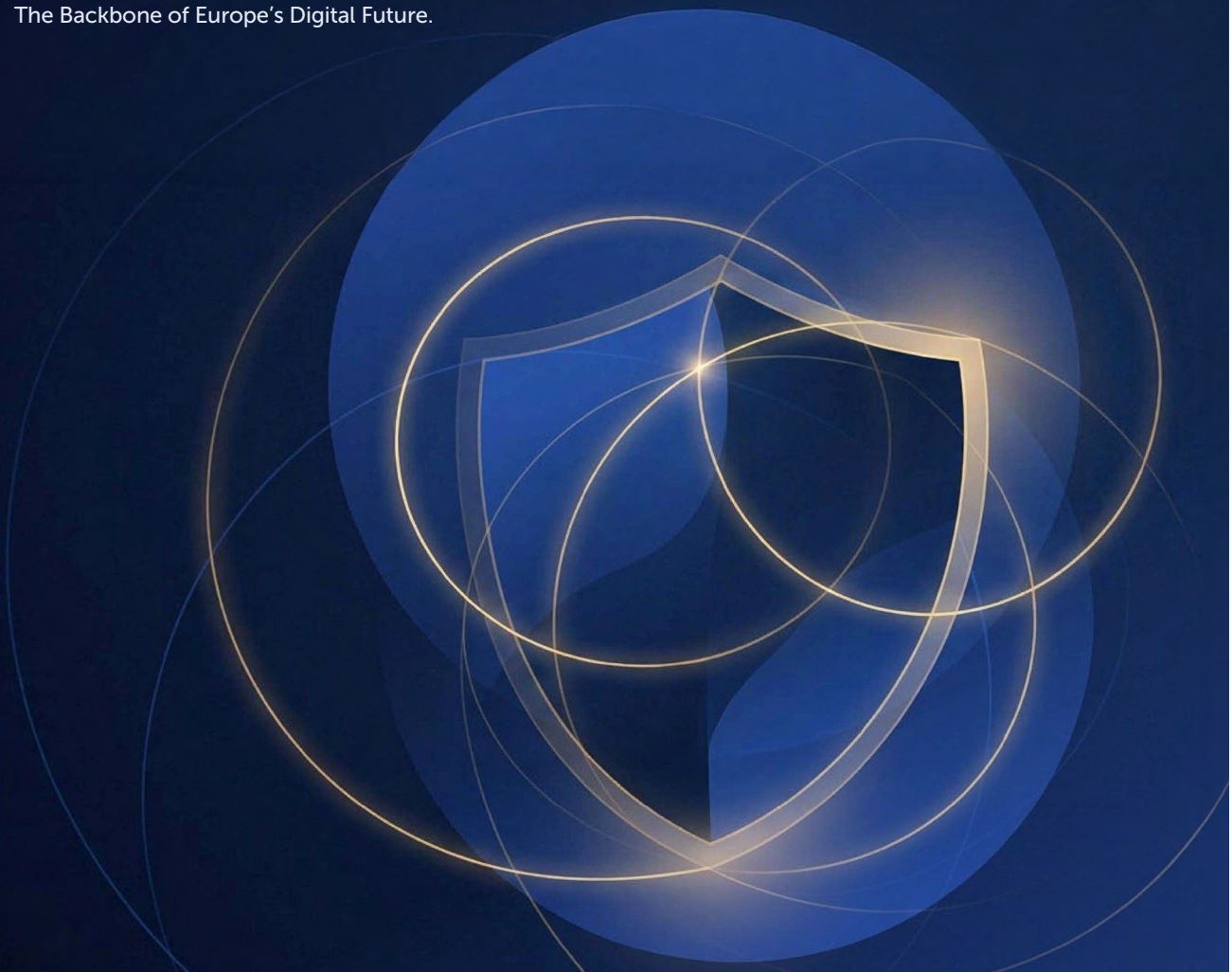
eunetworks.

The Backbone of Europe's Digital Future.

WHITE PAPER



The Quantum Threat Window: is yours open?

An executive guide to securing Layer 1 data centre interconnect traffic from the approaching threat of quantum computer attack. What leaders need to know – and do – before today's encrypted data becomes tomorrow's data breach.

Table of Contents

Executive Summary	02
The Quantum Threat Window in four questions	03
Introduction	04
Why Quantum Computers are changing the DCI threat landscape	06
Defining the Quantum Threat Window	07
How Post-Quantum Cryptography mitigates the risk	08
Layer 1 encryption complements higher-layer security measures	10
Why the threat is not theoretical	11
Governments, regulation and standards are translating this risk into action	12
How to close your Quantum Threat Window	14
Protect your critical data today. Prepare for tomorrow.	16
About the Authors	17
About euNetworks	17
Sources	18

Executive Summary

A future data breach can begin with traffic captured today.

The quantum security threat to data centre connectivity has a perception problem. It sounds like science fiction, feels technically complex and is easily dismissed as a future challenge. However, the response is not a problem to be deferred - it is an active, present-day priority.

Quantum computers will eventually break the public-key cryptography used to secure communications today. By intercepting and storing encrypted traffic now, adversaries can decrypt it as quantum capabilities mature - a strategy known as "store now, decrypt later". Consequently, the urgency of this threat is dictated not by the arrival date of quantum computers themselves, but by the lifespan of your data's confidentiality, the impact of disclosure and the time taken to migrate the systems protecting it. If critical intellectual property, strategic communications or regulated data will retain value into the 2030s, your Quantum Threat Window is open.

Until now, security teams have concentrated investment on the most common attack surfaces, including applications, identities and endpoints. However, as critical workloads increasingly distribute and bandwidth continues to scale, more sensitive and long-lived information is moving between geographically separated locations. This means a well-executed passive fibre tap may capture high-capacity traffic without creating an obvious alert or service disruption, making data centre interconnects (DCI) an increasingly lucrative target.

Recognising the risk, governments, regulators and standards bodies are raising expectations. The EU and UK have established PQC migration roadmaps, while NIS2 and DORA require relevant organisations to manage ICT security risk and apply appropriate controls to protect data in transit. While these frameworks do not mandate PQC or Layer 1 encryption, they increase the need to understand and manage how sensitive data is protected.

Layer 1 encryption with PQC-secured key establishment provides a comprehensive response, protecting all customer traffic carried across the link, with virtually no latency penalty. Crucially, protection must be crypto-agile, allowing algorithms to evolve with NIST and ETSI standards through software updates rather than costly hardware refresh cycles. For executives, leading this transition represents a strategic opportunity: it transforms regulatory compliance into a catalyst for building trust and demonstrating proactive security.

Closing the quantum threat window requires treating DCI as part of the security perimeter. True quantum resilience depends on an integrated chain of controls rather than a single cipher. This paper explains how euNetworks uniquely combines software, hardware and real-time network insight to deliver comprehensive protection against the quantum threat.

Urgency is dictated by the lifespan of your data's confidentiality.

The Quantum Threat Window in four questions

01

How long must your data remain confidential?

Quantum threat is determined by the lifetime of your data, not by when a powerful quantum computer might arrive. Encrypted traffic captured today could be stored and targeted for decryption as quantum capabilities mature. If intellectual property, financial records, strategic information or personal data such as biometric and genomic records will remain sensitive into the 2030s - or for a lifetime - intercepting it today creates the risk of a future data breach.

02

Why are high-capacity DCI routes becoming attractive targets?

Cloud adoption, distributed AI, data-centre replication and sovereignty requirements are moving growing volumes of long-lived sensitive data between locations. A single high-capacity interconnect can aggregate numerous critical data flows, while a well-executed interception may avoid detection. This combination of scale, value and limited awareness of an attack makes DCIs an increasingly high value target, and turns the physical route into a cybersecurity concern.

03

Where are the critical blind spots in your security perimeter?

Security investment has rightly concentrated on the most common attack surfaces, including applications, identities and endpoints. Private DCI has mostly been considered lower risk and procurement decisions made primarily on capacity and service availability. This can leave organisations with limited network records and visibility of the exact physical route, its hand-offs, potential interference and how the data is protected.

04

How does euNetworks close these perimeter gaps and future-proof your transport?

euNetworks uniquely combines software, hardware and real-time network insight to deliver comprehensive protection against the quantum threat. Together, these capabilities make routes verifiable, physical interference detectable and your traffic secure.

Introduction

Data Centre Interconnectivity is now a frontline segment of the security perimeter.

Security investment has followed the most common attack vectors. As the Verizon 2026 Data Breach Investigations Report[1] illustrates, breaches overwhelmingly (63%) originate in software, identities, and human behaviour. Consequently, security teams have concentrated their resources on the observable attack surfaces: applications, users, and endpoints.

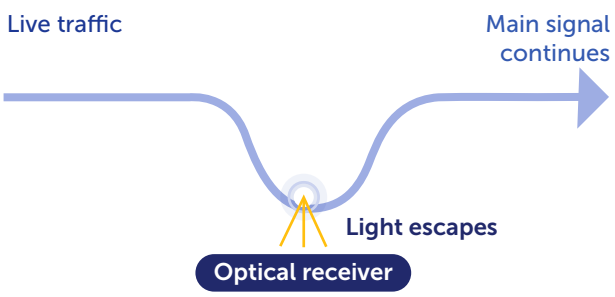
To defend this stack, organisations deploy layered controls. Data at rest is encrypted, identity and access controls govern access, TLS protects application sessions, IPsec secures network tunnels, and MACsec protects Ethernet links. These controls are essential and can overlap as complementary layers of defence. However, each operates at a different layer and within a defined scope, protecting a particular application, session, network path or link depending on its deployment. In practice, these controls are configured through applications, systems and endpoints the organisation can directly control, and their coverage may not extend to every traffic flow or underlying physical segment.

In contrast, DCIs often traverse infrastructure operated by network providers and intermediaries, placing the physical path outside the organisation's direct control. Where the security of that infrastructure is assumed rather than independently verified, the physical transport layer has become a security blind spot.

How a fibre can be tapped

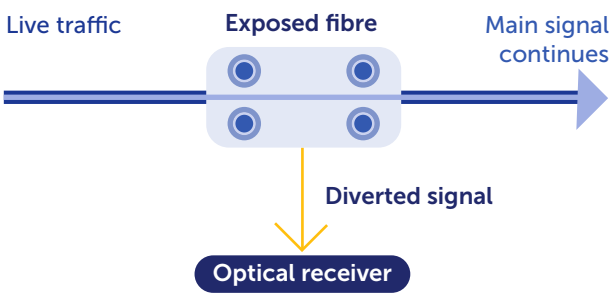
With physical access to a fibre, splice enclosure or patching point, an attacker can bend a fibre, or insert a low-ratio optical splitter or coupler, so that a controlled fraction of its light escapes to a receiver. The original signal can remain within its optical power budget, so the service may stay up and ordinary availability alarms may not fire. The copied signal can be recorded - what it reveals depends on the encryption applied.

Bend attack



A tight bend allows a small amount of light to leak towards a receiver.

Clip-on Coupler



A coupler placed around an exposed fibre diverts part of the signal to a receiver.

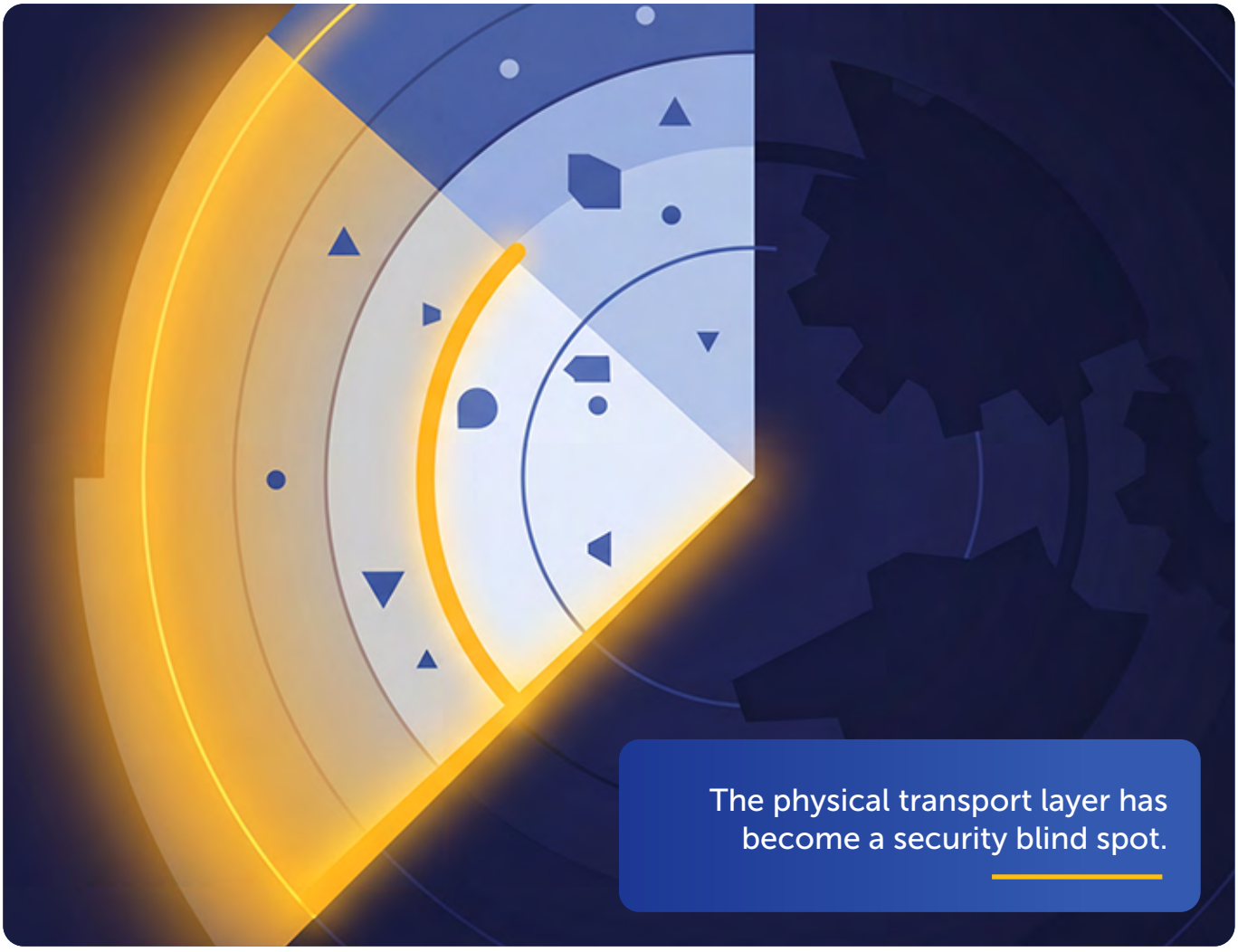
Some fibre tapping techniques can copy optical traffic without interrupting the service or generating a security-log event. The service operates normally while the data is siphoned, leaving the victim unaware and the incident unreported. Historically, CTOs and CISOs also viewed private circuits as inherently secure. Physical interception appeared specialist, expensive and difficult to target - how would an adversary identify the correct fibre?

Consequently, Layer 1 encryption has not always been prioritised where private infrastructure or higher-layer encryption was considered sufficient to manage the perceived risk.

The risk can no longer be ignored. The hybridisation of cloud architectures, distributed AI inference, and strict data sovereignty mandates mean vast volumes of highly sensitive, long-lived data are moving continuously across multiple domains. Bandwidths have been growing exponentially over the last decade and are now measured in hundreds of gigabits per second. At the same time, the organisations responsible for the data in transit have limited visibility of its precise route, physical exposure, or the controls applied at each hand-off.

This, combined with quantum threat, has forced a paradigm shift in how organisations should address data security risk. Regulations concur - timelines have been set for mitigation roadmaps, and standards are evolving to support this transition.

Organisations should reconsider the assumption that private infrastructure is automatically secure; Data Centre Interconnectivity is now a frontline segment of the security perimeter.



Why Quantum Computers are changing the DCI threat landscape

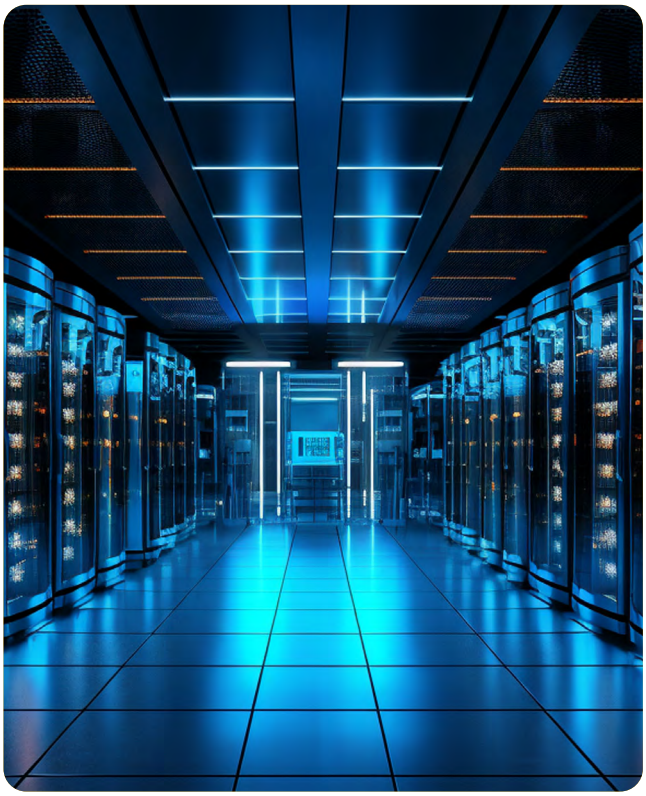
Quantum computers transform passive physical interception from a specialised espionage tactic into a scalable, lucrative operation.

Where Layer 1 encryption is enabled on a DWDM connection between data centres, traffic is commonly protected using a strong symmetric cipher such as AES-256. To encrypt data at one endpoint and decrypt it at the other, both endpoints must securely establish a shared secret. This is traditionally achieved using a key-agreement mechanism such as Diffie-Hellman, whose security relies on the difficulty of solving a mathematical problem known as the discrete logarithm problem. Solving this problem is considered infeasible for classical computers.

Quantum computing threatens this key-agreement process rather than AES-256 itself. Quantum computers use qubits and properties such as superposition and interference. By running algorithms that exploit these properties, they can solve certain mathematical problems far more efficiently than classical computers. One of these is Shor's algorithm, which can solve the discrete logarithm problem underpinning Diffie-Hellman. A quantum computer could therefore use a recorded Diffie-Hellman exchange to recover the shared secret, derive the encryption key and decrypt captured traffic.

The point at which a sufficiently capable quantum computer becomes capable of breaking widely deployed public-key cryptography is commonly called "Q-Day". Although its timing remains uncertain, the latest Global Risk Institute survey[2] assessed a cryptographically relevant quantum computer as "quite possible" within 10 years.

The question is not when Q-Day arrives, but how long your data must stay confidential.



For information that must remain confidential over this period, that possibility makes "store now, decrypt later" a rational attack strategy. High-capacity DCI links aggregate large volumes of potentially valuable traffic onto individual physical routes, making selected links attractive collection targets for adversaries.

If captured traffic contains intellectual property, genomic records or strategic communications that remain sensitive for many years, its future decryption could have significant financial, operational or national-security consequences. The critical question is therefore not when Q-Day will arrive, but whether the data moving today must remain confidential beyond it.

Defining the Quantum Threat Window

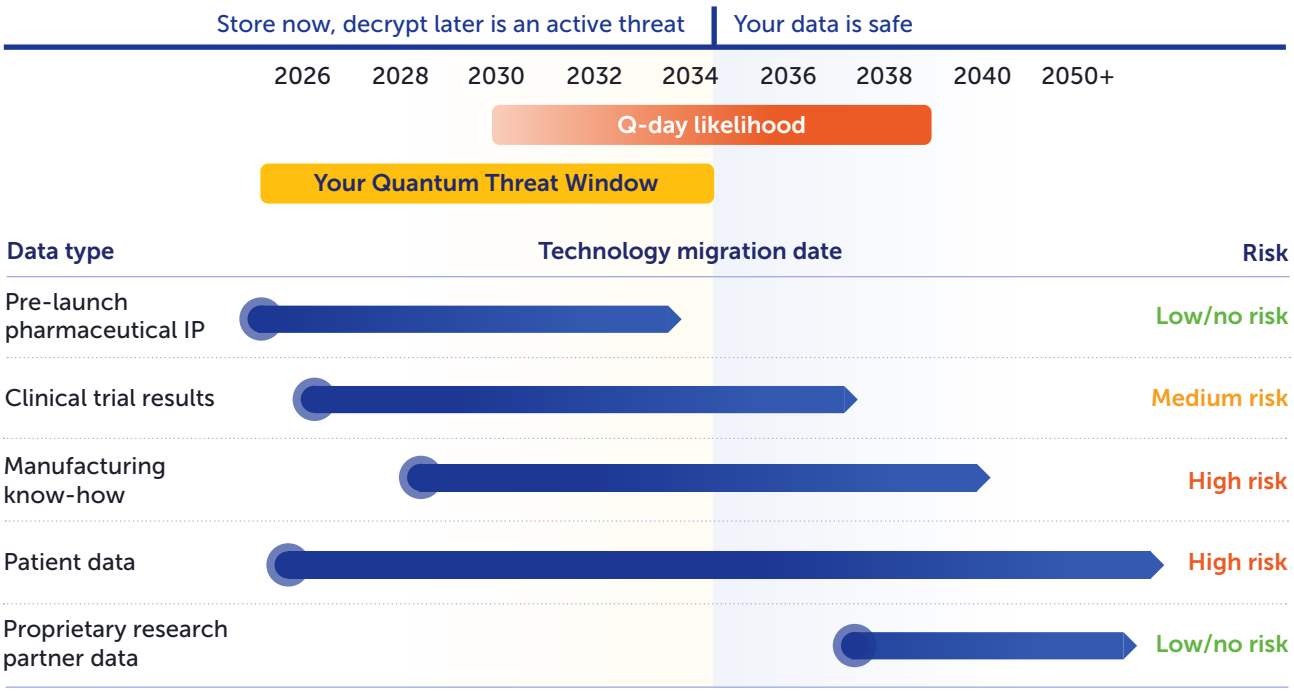
The Quantum Threat Window is the time between today and the moment a critical data flow is secured by quantum-resistant cryptography.

While this window remains open, encrypted data in transit can be intercepted, stored, and targeted for future decryption.

Consequently, the business case for investment should not depend on predicting when a sufficiently capable quantum computer will arrive. Instead, leaders should consider how long their data must remain confidential, the consequences of disclosure and how long migration will take. These factors determine whether the cost of upgrading today is justified by the risk of sensitive data being harvested now and decrypted later.

Deploying quantum-resistant protection closes the window for new traffic, but it cannot retroactively secure information that has already been captured. The immediate priority is therefore to identify high-value, long-lived data flows and close their quantum threat windows first.

Illustrative quantum risk profile for a life sciences organisation, based on data type and interception date



Risk is lowest where data loses its value before Q-Day or is protected by quantum-resistant cryptography before interception.

How Post-Quantum Cryptography mitigates the risk

Crypto-agility turns post-quantum security from a one-time technology replacement into a capability that can evolve with the threat landscape.

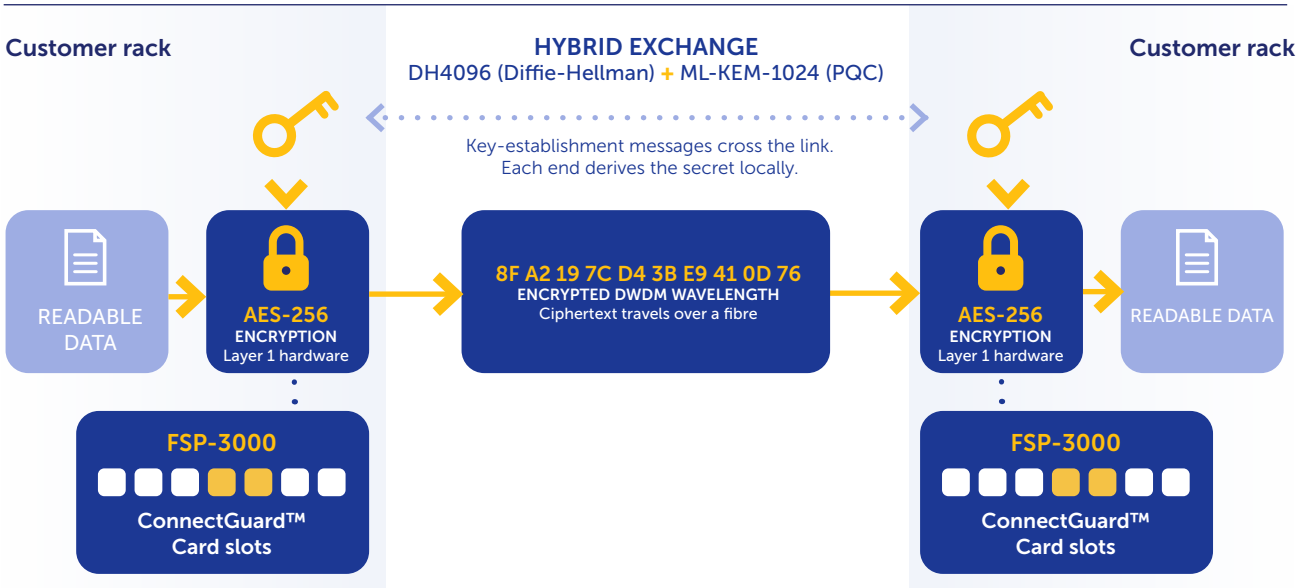
The opportunity presented to bad actors by "store now, decrypt-later" attacks is underpinned by the time and cost of migration. Procuring new hardware, integrating key-management systems and completing operational testing can take time and investment. Every delay extends the period during which valuable traffic can be collected, making high-capacity DCI routes an increasingly attractive target. Both NIST[3] and the UK NCSC[4] therefore emphasise the need to begin migration planning now.

Protection from quantum threat is achieved using Post-Quantum Cryptography (PQC[5]) protection of the vulnerable key exchange. An encrypted DWDM connection typically uses two complementary cryptographic mechanisms: an efficient symmetric cipher such as AES-256 for the data stream, and a separate mechanism for key establishment. AES-256 is already considered resistant to quantum attack. The key-establishment mechanism therefore allows the equipment at each end of the connection to securely derive or exchange the symmetric keys required to encrypt and decrypt the data stream.

The primary quantum vulnerability lies within this second process. Post-quantum cryptography replaces or augments quantum-vulnerable public-key algorithms with mechanisms based on mathematical problems believed to resist both classical and quantum attack.

The resulting shared secret is used to derive the AES-256 keys that encrypt and decrypt the data stream.

Adtran's ConnectGuard card integrates AES-256 encryption and PQC key exchange, occupying two slots in the FSP 3000 chassis which sit at each end of a customer DWDM data centre interconnect:



PQC key establishment therefore mitigates the "store now, decrypt-later" risk for newly protected traffic. An adversary may intercept and store encrypted traffic, but PQC is designed to prevent the underlying cryptographic keys from being recovered by a quantum computer and used to decrypt it.

As well as the latest PQC algorithms, modern DWDM platforms offer crypto-agility. This means cryptographic algorithms and security policies can be updated through software or firmware, extending platform longevity and reducing the need for hardware replacement.

NIST defines crypto-agility around this ability to replace and adapt cryptography across software, hardware, firmware, protocols and infrastructure while maintaining secure operations. To support this operational discipline, the Security Director software from Adva Network Security (an Adtran company) automates cryptographic configuration and policy checks.[6] Extending this management tool to the S-Flex™ and CryptoMux™ platforms brings these agile capabilities directly to encrypted optical transport.[7]

To support this continuous evolution, organisations rely on standardisation bodies like ETSI and NIST.

Following a rigorous multi-year competition, NIST recently standardised the first quantum-resistant algorithms. This includes NIST's FIPS 203 (ML-KEM),[8] which specifies a key-encapsulation mechanism standard and is currently utilised in Adtran's solutions. This public approach ensures data is protected by transparent, globally peer-reviewed mathematics rather than "black box" cryptography.

Together, AES-256 traffic encryption, standardised PQC key establishment and crypto-agility provide complementary controls that can support staged migration and allow supported algorithms and policies to evolve while reducing the risk of premature hardware replacement.

Crypto-agility shifts the investment principle from purchasing a fixed cryptographic implementation to deploying an adaptable foundation that can evolve over time.

Data is protected by transparent, globally peer-reviewed mathematics rather than 'black box' cryptography.

Layer 1 encryption complements higher-layer security measures

Layer 1 creates defence in depth by inherently protecting all data, with no latency penalty.

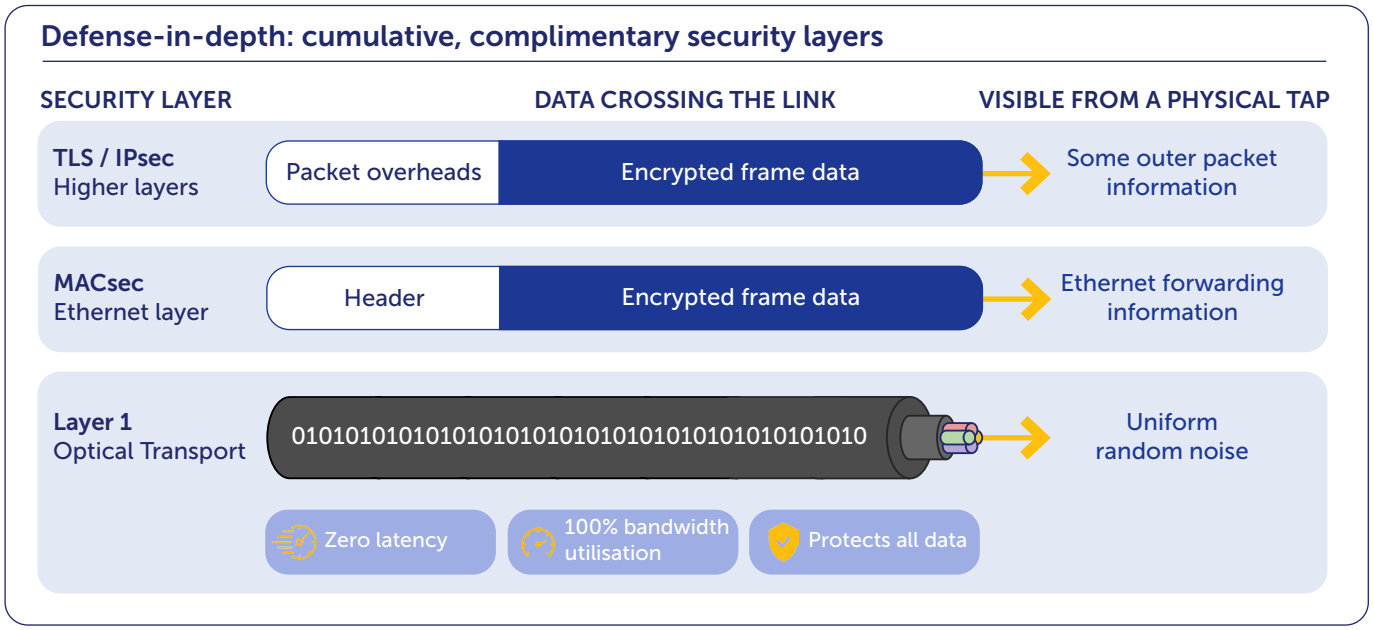
PQC can be applied higher in the network stack - it is not unique to Layer 1. However, securing data exclusively at upper OSI layers introduces distinct operational trade-offs. Protocols like IPsec and TLS inspect packets, encrypt payloads, and attach additional headers. These expanded packet sizes consume additional bandwidth and increase transport costs, while the required computational processing can introduce 5-10 microseconds of latency.

Layer 2 MACsec provides line-rate encryption with minimal added latency, but does not conceal all Ethernet frame information - the Ethernet header must remain visible so network equipment can forward each frame to its destination. Therefore, an adversary tapping the physical line could analyse this information to infer aspects of network architecture and identify which entities are communicating.

Operating directly at the hardware level, Layer 1 encryption resolves these challenges. Because DWDM is fundamentally a point-to-point physical connection rather than a packet-switched network, the data does not need to navigate complex routing webs and therefore all data can be encrypted. Consequently, Layer 1 encrypts the raw, continuous bitstream without appending overhead headers. This guarantees 100% bandwidth utilisation - even at 400G or 800G line rates - while adding virtually zero latency, ensuring real-time data replication remains uninterrupted.

To an attacker analysing the physical cable, the link appears as uniform, random noise, completely obscuring the organisation's internal network topology.

By providing protocol-independent protection across the optical transport link, Layer 1 encryption complements TLS, IPsec and MACsec and adds another control to a broader defence-in-depth security architecture.



Why the threat is not theoretical

Although the public record does not conclude that terrestrial fibre tapping is widespread, it confirms that data collection is real, credible physical access points exist and adversaries are increasingly surveying critical cables.

Public awareness of covert fibre tapping is limited, partly because the activity is designed to avoid detection and intelligence investigations may remain classified. Nevertheless, the available public evidence establishes three points relevant to the DCI threat landscape.

High-capacity communications are already being intercepted

In 2015, the UK Intelligence and Security Committee publicly described[9] GCHQ bulk interception systems accessing selected internet 'bearers' - the high-capacity communications links that make up the internet. This provided official confirmation that communications carried over selected high-capacity links can be accessed and subjected to filtering and selection, although the public report does not establish the physical interception method used.

Network infrastructure contains identifiable physical points of vulnerability

ENISA's assessment[10] of subsea cable security concludes that tapping a modern cable on the seabed is highly unlikely because of the engineering challenge, but states that tapping at cable landing stations is more feasible. This distinction matters for data-centre connectivity because the most credible access point may be a hand-off, patch panel, shared facility, splice location etc., rather than the deepest part of the cable.

There is current hostile interest

In April 2026, then UK Defence Secretary John Healey warned[11] that Russian GUGI units operating around critical undersea infrastructure were 'designed to survey underwater infrastructure during peacetime, and be prepared to sabotage it in conflict'. The same statement described UK and allied monitoring of activity over cables and pipelines. Reconnaissance is not proof of interception, but it is authoritative evidence that communications infrastructure is an active geopolitical target.

Governments, regulation and standards are translating this risk into action

Governments are not waiting for certainty about when a cryptographically relevant quantum computer will arrive.

Government and regulatory guidelines are based on two facts: "store now, decrypt-later" creates a risk today, and replacing vulnerable cryptography across complex technology estates will take time.

Across Europe, organisations are required to establish post-quantum transition plans. As part of this, public bodies and critical infrastructure operators must identify vulnerable systems, prioritise them based on risk and data lifespan, and prepare to adopt standardised, tested PQC solutions as they mature.

The EU Roadmap for the Transition to Post-Quantum Cryptography[12] recommends a phased transition schedule. By the end of 2026, countries should establish national roadmaps and begin planning for high and medium-risk systems. By the end of 2030, the transition for high-risk systems must be complete, planning and pilots for medium-risk systems should be finished, and quantum-safe software and firmware upgrades should be enabled by default. Finally, by the end of 2035, the transition must be completed across all remaining risk categories.

The UK NCSC roadmap also sets out a phased transition. Organisations must complete their discovery and initial migration planning by 2028. By 2031, they must migrate their highest-priority systems and finalise plans for the remainder, with the goal of completing the entire transition by 2035.

The EU and UK dates are government policy benchmarks rather than statutory deadlines. Regulated industries, however, may already be accountable for quantum risk even where regulation does not use the term "post-quantum cryptography". For example, the NIS2[13] directive requires essential entities to manage risks around cryptography, encryption, and supply chains. Similarly, DORA[14] enforces strict requirements for financial entities regarding encryption, cryptographic keys, and third-party ICT risks.

Neither DORA nor NIS2 mandates PQC or a particular algorithm. However, regulated organisations are already required to ensure that their controls remain appropriate as threats and technology evolve. In practice, this means crypto-agility across DCI is the essential capability to support long-term resilience and help organisations adapt their cryptographic controls as standards, threats and regulatory expectations evolve.

In the United States, federal purchasing power is accelerating this timeline globally. On June 22, 2026, President Trump signed two complementary Executive Orders: "Securing the Nation Against Advanced Cryptographic Attacks"[15], which mandates that all federal high-value assets transition key establishment to PQC by 2030, and "Ushering in the Next Frontier of Quantum Innovation"[16], which targets quantum hardware development by 2028. Because US federal procurement rules apply to major technology vendors, hyperscalers like Google and Microsoft[17] are aligning their own infrastructure and R&D roadmaps to these same deadlines, setting a de facto global timeline for the connectivity ecosystem.

For executives, leading this transition represents a strategic opportunity: it transforms regulatory compliance into a catalyst for building trust and demonstrating proactive security.

'Store now, decrypt-later' creates a risk today.

Governmental and Regulatory PQC Planning and Migration Milestones:

	2024	2025	2026	2028	2030	2031	2035
Plan priority systems	NIS2* [18]	DORA* [19]	EU† [20] DE† [21]	UK† [22]			
Migrate priority systems					EU, DE, US† [23]	UK	
Plan remaining systems					EU, DE	UK	
Migrate remaining systems						DE	UK, US, EU

* NIS2 and DORA require relevant organisations to maintain risk-based cryptographic controls and update them as standards and threats evolve. Neither explicitly mandates PQC.

† Governmental roadmaps provide guidance and target milestones, not general statutory deadlines.

The strategic message for CTOs and CISOs is therefore straightforward: identify critical data flows and how they are protected, establish the migration plan within the next two years, protect the highest-risk connections by the beginning of the next decade, and complete the wider transition by 2035.

How to close your Quantum Threat Window

euNetworks combines route intelligence, data-insight, infrastructure ownership and quantum-resilient security to serve as your strategic digital infrastructure partner.

Once an organisation has established how long its critical data must remain secure and where that data travels, there are four questions every CTO and CISO should ask:

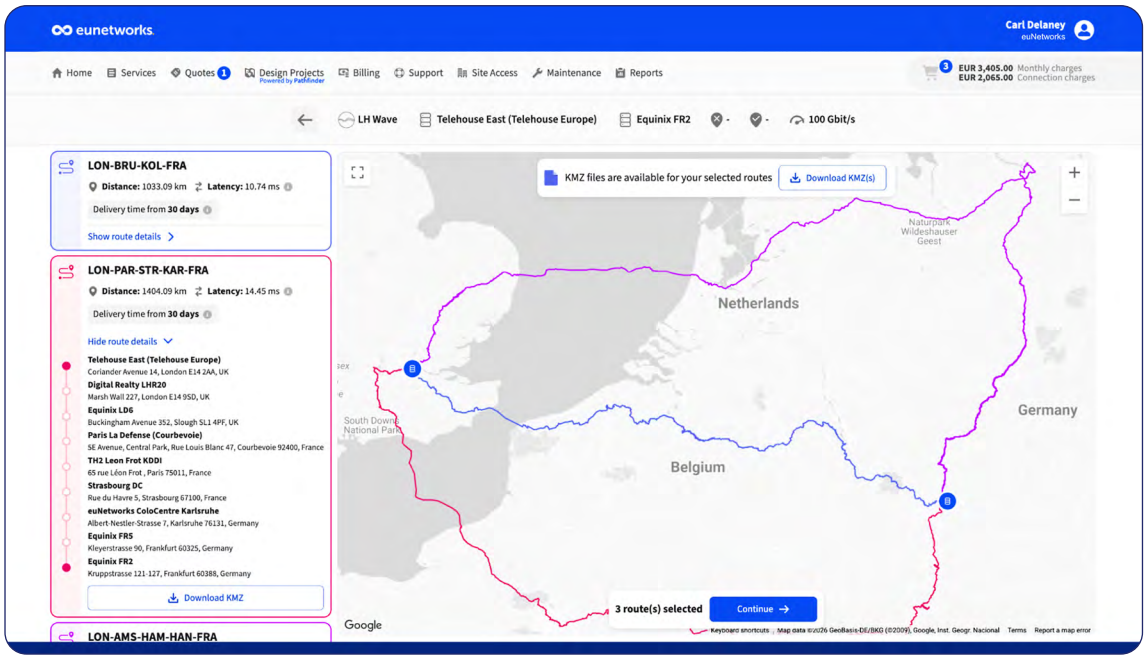
1. Can I trace the complete physical route?
2. How is data protected throughout its journey?
3. Can that protection adapt as threats and standards evolve?
4. Would I know if the physical infrastructure were being interfered with?

Trace the exact route with Pathfinder

As connectivity becomes part of the security architecture, understanding the physical route is critical. Organisations need to know exactly where their data travels and who controls the infrastructure carrying it.

Pathfinder is an online self-service route design tool that sits within euNetworks' Customer Portal, providing users with instant visibility of their routes. Available for wavelength and fibre services, it provides access to more than 700,000 validated route options, detailed route information and up-to-date downloadable KMZ files - both pre-sale and after delivery.

This enables customers to evaluate risk, plan network diversity and make faster operational decisions using a consistent source of route data. euNetworks' extensive ownership and control of the underlying infrastructure supports accurate records, disciplined route management, clear accountability and faster investigation of changes or incidents.



Quantum Shield is euNetworks' market-leading Layer 1 security proposition

Knowing the route is foundational, but it is not sufficient. Security also requires the ability to detect abnormal events on that infrastructure and to protect the information even if an interception attempt succeeds. This is why physical and cyber security can no longer be separate conversations.

To proactively address the quantum security threat, euNetworks - in partnership with Adtran - developed the market's first quantum-safe enabled private connectivity solution, Quantum Shield.[24]

Quantum Shield delivers trusted, private connectivity to protect critical data against today's cyber threats and tomorrow's security challenges. Designed for organisations handling highly sensitive information or operating critical infrastructure, it functions as an advanced security layer integrated directly into euNetworks' Private Connect Managed Optical Fibre Network (MOFN) solution.

What is Private Connect MOFN?

Private Connect MOFN provides private, managed network infrastructure for organisations seeking enhanced security, scalability and control over their data. It functions as a bespoke private network, with dedicated devices, control over day-one capacity, high-performance and flexible managed opex.

Quantum Shield is offered as an additional security layer to Private Connect MOFN. By combining the inherent security of a dedicated managed fibre network with quantum-resistant crypto-agile encryption at Layer 1, Quantum Shield ensures all traffic is automatically secured without impacting latency or throughput.

The underlying infrastructure is powered by Adtran's FSP 3000 optical transport platform and S-Flex™ technology to support high-capacity, encrypted data centre interconnect (DCI) services anywhere on the euNetworks footprint. To safeguard this traffic, the system pairs standard AES-256 ciphers with NIST-aligned Post-Quantum Cryptography (PQC) for key establishment. This highly crypto-agile design ensures the network meets immediate security needs while remaining fully adaptable as global cybersecurity standards evolve.

The S-Flex™ solution - capable of bandwidths up to 400G - boasts credentials that include industry-first approval by the Federal Office for Information Security (BSI) for EU/NATO Restricted traffic and information classified up to "Verschlusssache - Nur für den Dienstgebrauch" (VS-NfD) - "For Official Use Only". SAP deployed this exact technology between its data centres in Walldorf and St. Leon-Rot, Germany, to protect replication, backup, and operational traffic.[25]

Beyond advanced encryption, Quantum Shield actively monitors the physical integrity of the network using Adtran's Advanced Link Monitoring (ALM). This provides continuous assurance by instantly detecting and precisely locating any fibre-tapping attempts. By pairing customer-controlled, quantum-resistant data protection with real-time physical layer transparency, Quantum Shield provides a comprehensive defence against both immediate intrusions and future attacks enabled by quantum computing. This uniquely positions organisations to confidently strengthen their cyber resilience and prepare for strict, evolving regulatory requirements.

Protect your critical data today. Prepare for tomorrow.

The quantum threat to data centre interconnectivity is a present-day data protection issue.

Quantum computers are expected to break the public-key methods used to establish encryption keys, allowing traffic captured now to be decrypted later. If your critical data moving today must remain confidential into the 2030s then your Quantum Threat Window is open.

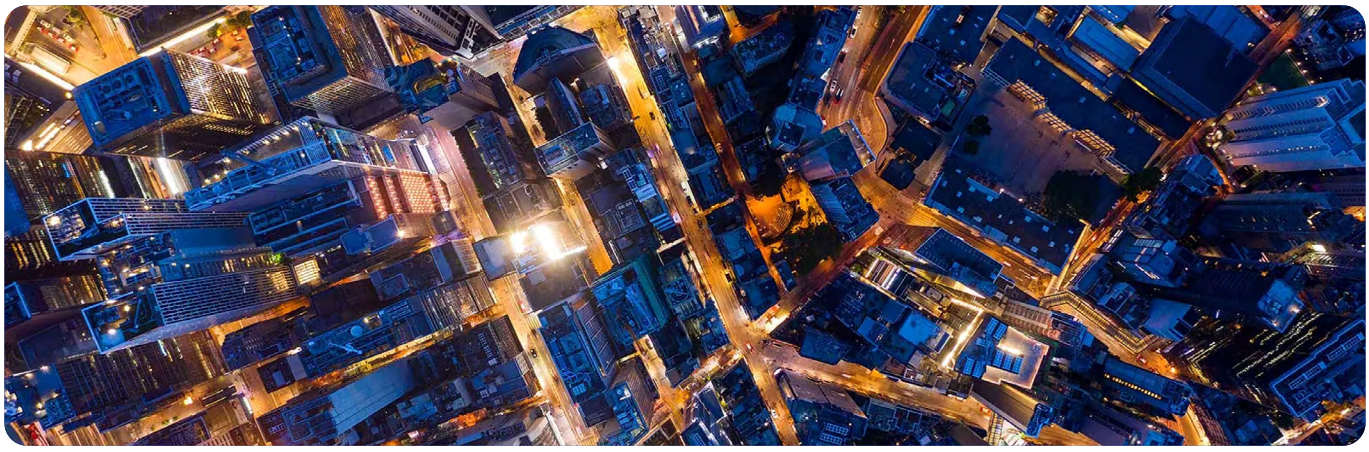
Security investment has rightly concentrated on applications, identities and endpoints. DCI matters because it concentrates large volumes of high-value data on physical routes that often sit outside an organisation's direct control. A passive fibre tap can copy that traffic without interrupting the service or triggering the alerts security teams usually rely on.

Route visible.
Traffic quantum-resistant.
Interference detectable.

The need to act is growing as data volumes rise, migration takes time and government roadmaps call for organisations to identify vulnerable cryptography and prioritise their highest-risk systems. Traffic already harvested cannot be protected retrospectively, so waiting for certainty only extends the period in which critical data can be collected.

Closing the window starts with the most valuable and long-lived data flows. Organisations should know where those flows travel, verify the physical route, encrypt the complete optical link using AES-256 with PQC-secured key establishment, maintain crypto-agility as standards evolve and monitor the fibre for interference. At Layer 1, these controls protect all traffic at full line rate with virtually no latency, while complementing TLS, IPsec and MACsec higher in the stack.

euNetworks brings these controls together. Its owned and operated European fibre infrastructure and Pathfinder route intelligence provide visibility of where critical data travels. Private Connect provides dedicated, controlled infrastructure, while Quantum Shield, built on Adtran's FSP 3000, combines customer-controlled AES-256 encryption, PQC-secured key establishment, crypto-agility and Advanced Link Monitoring.[25,26] Together, these capabilities make the route visible, the traffic quantum-resistant and physical interference detectable - closing the Quantum Threat Window for new traffic today while keeping protection ready for tomorrow's standards and threats.



About the Authors

Carl Delaney,
Head of Products at euNetworks

Sweta Patnaik, Product Manager,
Private Connect MOFN

Thank you to our technology partner, Adtran.

About euNetworks

euNetworks is a pan-European provider of bandwidth infrastructure services, with a network that's purpose-built to enable long-term Security, Data, AI and Cloud strategies. We're the leading connectivity partner for data centre companies and their customers in Europe, directly connecting over 600 data centres today. We own and operate 18 metropolitan city networks connected with a high capacity intercity backbone covering 53 cities in 17 countries. A leading provider of cloud connectivity, we directly connect to all major cloud platforms.

euNetworks delivers scalable solutions to a customer base that is at the centre of technology transformation, offering a targeted portfolio of metropolitan, private and long haul network services underpinned by Dark Fibre, Wavelengths, Ethernet and Internet technology. We proactively invest in our network to ensure Europe's demand for bandwidth is met today and into the future.

Sources

1. https://www.verizon.com/business/resources/reports/dbir/#2026DBIRNR
2. https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/
3. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
4. https://www.ncsc.gov.uk/paper/next-steps-in-preparing-for-post-quantum-cryptography
5. https://csrc.nist.gov/projects/post-quantum-cryptography
6. https://www.advasecurity.com/en/newsroom/press-releases/20250930-adva-network-security-launches-security-director-to-automate-cryptographic-operations
7. https://www.advasecurity.com/en/newsroom/press-releases/20260820-adva-network-security-extends-security-director-with-automated-crypto-management
8. https://csrc.nist.gov/pubs/fips/203/final
9. https://publicintelligence.net/uk-isc-mass-surveillance/
10. https://www.enisa.europa.eu/publications/undersea-cables
11. https://www.gov.uk/government/speeches/on-russian-submarine-activity-in-the-atlantic-joint-statement-to-the-osce
12. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation- roadmap-transition-post-quantum-cryptography
13. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
14. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
15. https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/
16. https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/
17. https://www.microsoft.com/en-us/security/blog/2026/06/30/microsoft-advances-quantum-safe-security-as-the-risk-timeline-shifts/
18. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm
19. https://finance.ec.europa.eu/news/commission-launched-4-week-have-your-say-feedback-two-delegated-regulations-under-dora-2023-11-27_en?utm
20. https://digital-strategy.ec.europa.eu/en/policies/post-quantum-cryptography?utm
21. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile
22. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
23. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
24. https://eunetworks.com/news/eunetworks-launches-new-quantum-safe-private-connectivity-service-powered-by-adtrans-encrypted-optical-transport-technology/
25. https://www.advasecurity.com/en/newsroom/press-releases/20260819-sap-strengthens-its-cloud-infrastructure-in-germany-with-bsi-approved-layer-1-encryption?utm_source=chatgpt.com
26. https://www.advasecurity.com/en/newsroom/press-releases/20250925-adva-network-security-scores-world-first-with-bsi-approved-400g-encryption-solution?utm_source=chatgpt.com

eunetworks.

Contact us:
info@eunetworks.com

Find out more

eunetworks.

The Backbone of Europe's Digital Future.