

Optical Encryption Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031)

Industry: Technology, Media & Telecom (TMT)

URL: <https://www.mordorintelligence.com/industry-reports/optical-encryption-market>

Optical Encryption Market Size and ShareMarket OverviewStudy Period | 2020 - 2031 |

Market Size (2026) | USD 5.27 Billion |

Market Size (2031) | USD 7.96 Billion |

Growth Rate (2026 - 2031) | 8.62 % |

Fastest Growing Market | Asia Pacific |

Largest Market | North America |

Market Concentration | Medium |

Major Players*Disclaimer: Major Players sorted in no particular order

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Optical Encryption Market Analysis by Mordor IntelligenceThe Optical Encryption Market size was valued at USD 4.85 billion in 2025 and estimated to grow from USD 5.27 billion in 2026 to reach USD 7.96 billion by 2031, at a CAGR of 8.62% during the forecast period (2026-2031).

The optical encryption market is valued at USD 4.85 billion in 2025 and is projected to reach USD 7.43 billion by 2030, registering an 8.91% CAGR. Rapid adoption of quantum-safe architectures, soaring AI bandwidth requirements, and line-rate performance above 800 Gbps propel investment in Layer 1 encryption platforms. Hardware-based designs remove software vulnerabilities, satisfy zero-trust mandates, and align with sovereign-cloud rules that compel in-flight key control. Hyperscale data-center operators accelerate 400 G and 800 G coherent upgrades, while telecom carriers refresh metro rings to enable multi-terabit data-center interconnects using integrated AES-256-GCM encryption.[1]Ciena Corporation, "WaveLogic 6 Extreme Product Brief," [ciena.com](https://www.ciena.com)Silicon-photonics integration cuts power budgets and lifts port densities, supporting loss-less AI/LLM workflows that cannot tolerate packet-level retransmissions. Finalization of NIST's post-quantum standards FIPS 203-205 creates a clear compliance target, reinforcing demand for crypto-agile optical hardware.

Key Report Takeaways* By encryption layer, Layer 1 solutions held 45.60% of the optical encryption market share in 2025 and are expanding at a 11.55% CAGR through 2031.

* By data rate, the 40-100 Gbps category accounted for 37.35% of the optical encryption market size in 2025, while the >100 Gbps segment is advancing at an 17.4% CAGR to 2031.

* By component, hardware appliances captured 41.10% revenue share in 2025; coherent and pluggable modules record the fastest 15.85% CAGR.

* By deployment mode, on-premise carrier-owned systems controlled 56.20% of the optical encryption market size in 2025, whereas cloud and network-as-a-service models are growing at a 16.5% CAGR.

* By end-user vertical, datacenter and cloud led with 51.20% revenue share in 2025 and is forecast to rise at a 14.9% CAGR through 2031.

* By geography, North America commanded 40.60% share in 2025; Asia Pacific is the fastest-growing region at 9.62% CAGR.

Note: Market size and forecast figures in this report are generated using Mordor Intelligence's proprietary estimation framework, updated with the latest available data and insights as of 2026.

Market Trends and Insights Drivers Impact Analysis of Optical Encryption Market*Driver | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeline |

Multi-terabit metro DCI build-outs | +2.1% | Global, with concentration in North America and Asia Pacific | Medium term (2-4 years) |
Zero-trust mandates across critical infrastructure | +1.8% | North America and EU, expanding to Asia Pacific | Short term (≤ 2 years) |
MACsec bottlenecks pushing Layer 1 upgrades | +1.4% | Global data-center markets | Short term (≤ 2 years) |
Post-quantum crypto-agile transport pilots | +1.2% | Government and BFSI sectors worldwide | Long term (≥ 4 years) |
Source: Mordor Intelligence |

Multi-terabit Metro DCI Build-outs Drive Coherent AdoptionHyperscale operators interconnect distributed AI campuses with multi-terabit metro rings, shifting to coherent optics that embed AES-256-GCM at 400 G and 800 G. Ciena's WaveLogic 6 Extreme enables 1.6 Tbps per wavelength while trimming per-bit power use by 50%. Optical circuit switching inside data centers removes copper bottlenecks and hands encryption to the physical layer, ensuring loss-less gradient exchange during model training. Regional carriers replicate this model to monetize existing dark fiber by offering encrypted bandwidth slices. Resulting scale economics lower cost per secured bit and accelerate Layer 1 penetration across colocation and enterprise campuses.

Zero-trust Mandates Accelerate Layer-1 IntegrationGovernment frameworks now presume breach and require continuous verification, making hardware encryption a default rather than an add-on. The U.S. CNSA 2.0 and the EU's NIS2 point directly at quantum-resistant keys, steering budgets toward devices that encrypt transparently at line rate. Broadcom's Emulex Secure Fibre Channel adapters illustrate how hardware telemetry blocks ransomware while maintaining full throughput.[2]Broadcom Inc., "Emulex Secure Fibre Channel HBAs," broadcom.com Financial institutions adopt similar designs to serve high-frequency trading where microsecond delays erase profits. This compliance-driven spending decouples demand from ordinary technology refresh cycles and sustains premium pricing for certified optical gear.

MACsec Bottlenecks Push Layer-1 UpgradesAt speeds beyond 100 Gbps, MACsec introduces latency and frame expansion that strain switch buffers. Operators facing congestion now off-load encryption to coherent optics that operate outside the Ethernet pipeline. The design frees up forwarding ASIC capacity, supports 800 G trunk links, and simplifies instrumentation because encryption is no longer intertwined with L2 management. Vendors that bundle encryption with DSP silicon gain bill-of-materials leverage and defend margins against commoditized grey optics. The shift compresses multi-layer security into a single photonic stage, enhancing observability without packet reassembly.

Post-quantum Crypto-agile Transport PilotsNIST's endorsement of ML-KEM and ML-DSA standards clears uncertainty around algorithm choice, letting transport vendors bake them into firmware.[3]National Institute of Standards and Technology, "FIPS 203, 204, 205 Final Standards," nist.gov ETSI's TS 104 015 hybrid-key protocol enables seamless fall-back to classical curves during migration.[4]European Telecommunications Standards Institute, "TS 104 015 Hybrid Key Exchange," etsi.org Government networks in the Middle East and Asia Pacific demonstrate dual-stack operation that rotates keys without halting traffic, proving business-case viability for crypto-agile optics. Early adopters report smoother audits and longer asset lifecycles because hardware need not be swapped when algorithms evolve. These pilots create reference architectures that lower perceived risk for mainstream enterprises

Restraints Impact Analysis of Optical Encryption Market*Restrainer | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeline |

High capex of coherent 400 G+ optics | -1.9% | Global, pronounced in cost-sensitive markets | Medium term (2-4 years) |
Fragmented regulatory certification | -1.3% | Worldwide, jurisdiction dependent | Short term (≤ 2 years) |
Scarcity of entropy sources at line rate | -0.8% | High-security segments globally | Long term (≥ 4 years) |
Supply-chain choke-points in DSPs | -1.1% | Global, centered in Asia manufacturing hubs | Medium term (2-4 years) |
Source: Mordor Intelligence |

High Capex of Coherent 400 G+ Optics Coherent transceivers still command premiums over direct-detect modules because they require indium phosphide PICs and advanced DSPs. Coherent Corp.'s move to 6-inch InP wafers aims for a 60% die-cost reduction, but commercial volumes remain 18 months away. Material export restrictions on gallium and germanium further elevate input costs, squeezing margins for suppliers that lack vertical integration. Smaller carriers may defer upgrades or adopt bandwidth-on-demand services instead of outright purchases, tempering near-term unit shipments even as long-term economics improve.

Fragmented Regulatory Certification Requirements Optical encryption vendors juggle FIPS 140-3 Level 3 in the United States, Common Criteria NDcPP in Europe, and divergent national schemes in Asia Pacific. Hardware redesigns to satisfy mandatory multi-factor authentication and zeroization features extend certification by up to 18 months. Firms with global customer bases must maintain parallel SKUs, inflating R&D overhead and complicating supply-chain forecasting. Harmonization efforts lag, keeping barriers high for smaller entrants and slowing multi-region rollouts.

*Our forecasts treat driver/restraint impacts as directional, not additive. The impact forecasts reflect baseline growth, mix effects, and variable interactions.

Optical Encryption Market Segment Analysis By Encryption Layer: Hardware Dominance Drives Layer 1 Leadership Layer 1 commanded 45.60% market share in 2025 and is growing at 11.55% CAGR, the strongest rate among all layers. PacketLight's DWDM portfolio shows how quantum key distribution integrates directly into coherent channels while staying within FIPS 140-3 boundaries. The optical encryption market size for Layer 1 platforms is projected to expand steadily as hyperscalers adopt 800 G line cards. Hardware-rooted key stores, tamper evidence, and deterministic latency remain decisive advantages. Enterprises retain Layer 2 MACsec appliances for legacy 10-25 G links, but those deployments plateau amid performance ceilings. Layer 3 IPsec persists in niche WAN scenarios where application awareness outweighs raw speed; nevertheless, its incremental latency discourages adoption in AI training clusters that demand microsecond determinism.

In metro and long-haul builds, Ciena's WaveLogic Encryption enables per-wavelength protection without external shelves, cutting rack space by 30%. Operators report simplified provisioning because DSP firmware automatically negotiates encryption parameters, boosting operational agility. The optical encryption market continues to shift budget from higher OSI layers to the photonic plane, reinforcing hardware vendors' pricing power while compressing value for software-only suppliers.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. By Data Rate: 40-100 Gbps Leads While above 100 Gbps Accelerates The 40-100 Gbps segment accounted for 37.35% of the optical encryption market size in 2025 as 100 G coherent pluggables reached volume production. Established telco networks use these rates for metro aggregation and edge cloud on-ramps. Coherent Corp.'s industrial-temperature 100 G ZR QSFP28-DCO extends reach into harsh environments, allowing encryption at cell-tower hubs without HVAC expense. Nonetheless, >100 Gbps lanes post an 17.4% CAGR as hyperscalers transition to 400 G and 800 G for GPU clust

er interconnects. Marvell's COLORZ 800 reduces capital cost of 800 G DCI links by up to 75%, collapsing the price gap that once hampered uptake.

Under 10 Gbps links survive in brownfield control networks and industrial IoT where traffic bursts remain modest. The 10–40 Gbps tier addresses campus backbones and 25 G PON, but incremental revenue migrates upward as AI workloads reshape traffic profiles. Accordingly, suppliers reallocate R&D toward 1.6 T road-maps backed by DSP nodes at 3 nm, further tipping momentum toward higher speeds.

By Component: Hardware Appliances Lead While Coherent Modules Accelerate Dedicated appliances captured 41.10% market share in 2025 as public-sector buyers favor tamper-proof chassis with integrated HSMs. The optical encryption market share may erode gradually, however, as coherent pluggables accelerate 15.85% CAGR on the back of silicon-photonics economies. Ciena's WaveLogic Nano and Marvell's 3 nm PAM4 chips demonstrate embedded security directly inside optical modules, delivering line-rate encryption without external blades. Software orchestration gains importance as fleet sizes rise; vendors now ship quantum-ready key servers that spin new post-quantum credentials in minutes.

Component miniaturization reduces power by up to 20%, an important metric as the Department of Energy anticipates tripling U.S. data-center electricity demand by 2028. Vendors that own DSP intellectual property can pivot faster to new algorithms, reinforcing entry barriers while trimming supply-chain exposure.

By Deployment Mode: On-premise Dominance Meets Cloud Acceleration Carrier-owned, on-premise systems held 56.20% share in 2025, reflecting telco need for physical control and regulatory accountability. Yet cloud and network-as-a-service models are growing at 16.5% CAGR as hyperscalers lease managed dark fiber and retain customer-managed keys. Ciena's Managed Optical Fiber Networks platform lets providers expose photonic APIs while customers manage encryption and telemetry. Hybrid deployment gains traction among utilities and logistics firms that combine on-site gateways with cloud-hosted key managers to balance latency and compliance.

Edge appliances remain relevant where indigenous data laws restrict foreign cloud use. Sovereign clouds in Europe and Asia South rely on regional key escrow, ensuring traffic never leaves jurisdiction unencrypted. This architectural diversity sustains revenue across OEMs, integrators, and emerging as-a-service brokers.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. **By End-user Vertical:** Datacenter Dominance Drives AI Demand Datacenter and cloud stakeholders generated 51.20% of 2025 revenue and will climb at 14.9% CAGR, reflecting AI training clusters that move petabytes between GPUs every second. Marvell's PCIe Gen 6 over optics demo shows host-to-GPU encryption at 64 GT/s with no retrain penalties, a prerequisite for exascale model convergence. BFSI institutions pilot quantum-safe optics to shield high-value FX trades, while government agencies mandate FIPS 140-3 Level 3 for classified transport. In energy, Hitachi Energy's quantum-secured grid in Oman illustrates how utilities protect SCADA flows at line rate.

Healthcare adoption grows as tele-diagnostics leverage homomorphic encryption to process MRI images in the cloud without exposing raw data. Retail and e-commerce focus on payment latency, integrating photonic encryption into edge POPs to keep tap-to-approval below 150 ms. Each vertical's distinct latency, compliance, and key-management needs diversify supplier road-maps and dilute reliance on any single customer cohort.

Geography Analysis North America Optical Encryption Market North America retained 40.60% revenue share in 2025, underpinned by federal zero-trust directives and hyperscale AI cluster builds that demand secure 800 G waves. Domestic chip supply-chain incentives hasten adoption of co-packaged optics, anchoring much of the D

SP value chain onshore. Canada's quantum-communication field tests and Mexico's expanding colocation market add incremental demand, but the United States remains the dominant buyer and R&D hub.

APAC Optical Encryption MarketAsia Pacific is the fastest-growing region at 9.62 % CAGR through 2031. China channels multibillion-dollar state funding into quantum-secure backbone builds, while Japan's 402 Tbps fiber milestone proves regional depth in photonics research. India's data-center capacity more than doubles between 2025 and 2028, spurring procurement of 100 G-ZR pluggables with built-in AES-256. South Korea extends 5 G transport to rural areas using encrypted 25 G PON, and ASEAN nations leverage regional manufacturing capacity to localize photonic assembly.

Europe and Middle East Optical Encryption MarketEurope's share contracts despite world-class labs, penalized by fragmented certification regimes. National pilots such as Finland's Telia-VTT quantum-secure network validate technology but stop short of continent-wide consensus. The EuroQCI program aims to harmonize procurement, yet roll-out lags Asian and North American peers. Middle East growth outpaces Europe on a smaller base, buoyed by UAE's fiber-to-satellite quantum key distribution demo at GITEX 2024. Saudi Arabia's Vision 2030 earmarks sovereign-cloud encryption as critical infrastructure, creating fresh runway for vendors with Arabic localization and local-key-custody options.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Regulatory LandscapeOptical encryption adoption is increasingly shaped by formal post-quantum and telecom security requirements rather than voluntary best practice. NIST finalized the first three post-quantum cryptography standards, FIPS 203, FIPS 204, and FIPS 205, in August 2024, creating a concrete reference point for crypto-agile optical platforms and key-management designs used in government, defense, and regulated infrastructure.

In the United States, cryptographic module validation under FIPS 140-3 remains a central procurement gate for hardware-based encryption used in transport equipment, while federal migration governance tightened with White House Memorandum M-26-15 (June 2026), which directs agencies to submit post-quantum migration plans to OMB and ONCD. In Europe, ETSI publications such as TS 103 924 (catalog of optical network and device security requirements) and TS 103 996 (EUCC protection profile for optical network and device security) add structure to optical security certification expectations, while the UK updated Telecommunications Security Code of Practice 2026 (version 1.1) reinforces security duties under the Telecommunications (Security) Act 2021, elevating compliance scrutiny for public telecom providers and their encryption supply chains.

Value Chain AnalysisThe value chain starts with photonic and compute silicon inputs, including DSPs, indium phosphide and silicon photonics PICs, coherent optics sub-assemblies, and hardware security building blocks that support tamper resistance and key storage. OEMs and module vendors integrate these into Layer 1 optical transport platforms, coherent and pluggable modules, and encryption-capable line cards, with encryption commonly embedded at wire speed (for example AES-256-GCM in coherent DSP pipelines). Certification and conformance work (such as FIPS 140-3 validation in the United States and ETSI-aligned security requirements in Europe) becomes an additional downstream step that can force parallel SKUs and lengthen time-to-market.

Channels to market run through carrier and hyperscale procurement, systems integrators, and managed connectivity providers that package encrypted wavelengths or private connectivity services with customer-controlled keys. Recent commerciali

zation signals include Adtran and euNetworks launching the Quantum Shield quantum-safe private connectivity service in May 2026 using Adtran FSP 3000 encrypted optical transport technology for European enterprise customers, illustrating how services and orchestration sit alongside hardware in the go-to-market stack. Upstream constraints highlighted in the market context, notably supply-chain choke points in ultra-low-jitter DSPs and the high capex of 400G+ coherent optics, keep component sourcing and vendor vertical integration strategically important for optical encryption availability and pricing.

Competitive Landscape

The optical encryption market exhibits moderate concentration. Industry incumbents Nokia, Cisco, and Ciena bundle coherent transport, DSP, and security into integrated stacks. Nokia's agreed USD 2.3 billion purchase of Infinera consolidates DSP talent and PIC capacity under one roof. Ciena's WaveLogic 6 roadmap moves encryption into 3 nm ASICs, locking competitors out of performance leadership for at least one design cycle. Cisco leverages its routing footprint to cross-sell optical security blades, anchoring accounts with life-cycle services.

Challengers exploit silicon-photonics cost curves. Marvell delivers merchant 800G ZR/ZR+ modules to OEMs that lack in-house optics, broadening market access. Coherent's transition to 6-inch InP wafers shrinks die cost and allows fourfold output, key for meeting hyperscale volume. Broadcom embeds quantum-resistant algorithm agility inside Emulex HBAs, targeting ransomware mitigation in Fibre-Channel SANs.

Patent activity intensifies around photonic integration and post-quantum key exchange. Meta and Google file for hermetic PIC packaging and slanted-grating couplers to reduce insertion loss, reinforcing defensible moats. Start-ups pursuing quantum-random number generators and neuromorphic optical encryption carve niche niches beyond classical DSP scaling. Suppliers that combine vertical integration, NIST-validated algorithms, and low-power PICs stand best positioned to capture the next wave of AI-driven spending.

Optical Encryption Industry Leaders* Nokia Corporation

* Huawei Technologies Co. Ltd

* Broadcom Inc.

* Cisco System Inc.

* Ciena Corporation

* *Disclaimer: Major Players sorted in no particular order

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. Optical Encryption Market Companies Covered in this Report* Nokia Corporation

* Cisco Systems Inc.

* Huawei Technologies Co. Ltd

* Broadcom Inc.

* Juniper Networks Inc.

* Ciena Corporation

* Ribbon Communications

* Infinera Corporation

* ADVA Optical Networking SE

* Arista Networks Inc.

* Acacia Communications

* Thales Group

* Fujitsu Ltd.

* Lumentum Holdings Inc.

- * Marvell (Inphi)
- * PacketLight Networks
- * Microchip Technology Inc.
- * LightRiver Technologies
- * ID Quantique SA

Read Analysis of Optical Encryption Companies

Market Opportunities and Future Outlook

A primary whitespace is operationalizing quantum-safe transport without requiring dedicated dark fiber, by combining line-rate optical encryption with quantum-safe keying methods that work on lit DWDM infrastructure. A concrete market proof point is the May 2026 deployment in Malta by Terra Quantum AG, Mercury Cybersecurity, and Melita Business of a production-grade post-quantum secure optical network link connecting two commercial data centers, using a QKD hardware platform integrated into existing active DWDM fiber. This kind of deployment supports packaged offerings for metro DCI, colocation interconnect, and regulated enterprise backbones where customers want measurable quantum-safe posture while preserving photonic layer performance.

Another opportunity area sits in bridging compliance-driven post-quantum timelines with upgrade cycles for 400G/800G transport. White House Memorandum M-26-15 (June 2026) formalizes planning requirements for US federal migration to post-quantum cryptography, while NIST standards (FIPS 203-205 finalized in August 2024 and HQC selected in March 2025 for a future draft) provide a vendor roadmap for crypto-agile implementations. Vendors that align optical encryption hardware, key management, and certification artifacts to these reference points can reduce audit friction for government and critical infrastructure buyers, while ETSI optical security requirement and protection-profile work (TS 103 924 and TS 103 996) creates room for Europe-focused productization around standardized security controls and documentation packages.

Recent Industry Developments in Optical Encryption Market* May 2026: Adtran and euNetworks launched Quantum Shield quantum-safe private connectivity service in Europe, using Adtran FSP 3000 encrypted optical transport technology for enterprise customers. The service demonstrates how orchestration and security layers can be offered as a managed capability on existing fiber networks.

- * March 2026: Ciena and Quantum Computing Inc. demonstrated a quantum-secured communications architecture at OFC 2026 that combined quantum key distribution with high-speed optical encryption using PQC and AES-256-GCM. The demo validated hybrid keying approaches on transport-grade optics, supporting operator interest in crypto-agile upgrades that do not compromise line-rate throughput.

- * October 2025: Nokia launched a 50G PON solution on the Lightspan MF platform incorporating quantum-safe encryption for enterprise fiber broadband connectivity. Extending quantum-safe positioning into access networks broadens the addressable footprint for optical encryption capabilities beyond long-haul and metro transport.

Table of Contents for Optical Encryption Industry Report1. INTRODUCTION

- * 1.1 Study Assumptions and Market Definition
- * 1.2 Scope of the Study

2. RESEARCH METHODOLOGY

3. EXECUTIVE SUMMARY

4. MARKET LANDSCAPE

- * 4.1 Market Overview
- * 4.2 Market Drivers
 - * 4.2.1 Multi-terabit metro DCI build-outs
 - * 4.2.2 Zero-trust mandates across critical infrastructure
 - * 4.2.3 MAC-sec bottlenecks pushing Layer-1 upgrades
 - * 4.2.4 Post-quantum "crypto-agile" transport pilots
 - * 4.2.5 AI/LLM GPU clusters demanding loss-less 800 G links
 - * 4.2.6 Sovereign cloud zones requiring in-flight key escrow
- * 4.3 Market Restraints
 - * 4.3.1 High capex of coherent 400 G+ optics
 - * 4.3.2 Fragmented regulatory certification (FIPS 140-3, ETSI 012)
 - * 4.3.3 Scarcity of entropy sources at line-rate speeds
 - * 4.3.4 Supply-chain choke-points in ultra-low-jitter DSPs
- * 4.4 Value Chain Analysis
- * 4.5 Regulatory Landscape
- * 4.6 Technological Outlook
- * 4.7 Porter's Five Forces Analysis
 - * 4.7.1 Threat of New Entrants
 - * 4.7.2 Bargaining Power of Buyers
 - * 4.7.3 Bargaining Power of Suppliers
 - * 4.7.4 Threat of Substitutes
 - * 4.7.5 Competitive Rivalry

5. MARKET SIZE AND GROWTH FORECASTS (VALUE)

- * 5.1 By Encryption Layer
 - * 5.1.1 Layer 1
 - * 5.1.2 Layer 2
 - * 5.1.3 Layer 3
- * 5.2 By Data Rate
 - * 5.2.1 less than 10 Gbps
 - * 5.2.2 10 - 40 Gbps
 - * 5.2.3 40 - 100 Gbps
 - * 5.2.4 above 100 Gbps
- * 5.3 By Component
 - * 5.3.1 Hardware Encryption Appliances
 - * 5.3.2 Coherent/Pluggable Modules and Optics
 - * 5.3.3 Key-Management / Orchestration Software
 - * 5.3.4 Managed Encryption Services
- * 5.4 By Deployment Mode
 - * 5.4.1 On-Premise (Carrier-Owned)
 - * 5.4.2 Cloud / Network-as-a-Service
 - * 5.4.3 Edge / Remote-Site Appliances
- * 5.5 By End-user Vertical
 - * 5.5.1 Datacenter and Cloud
 - * 5.5.2 BFSI
 - * 5.5.3 Government and Defense
 - * 5.5.4 Healthcare
 - * 5.5.5 Energy and Utilities
 - * 5.5.6 Retail and E-commerce
 - * 5.5.7 Other End-user Verticals
- * 5.6 By Geography
 - * 5.6.1 North America
 - * 5.6.1.1 United States
 - * 5.6.1.2 Canada
 - * 5.6.1.3 Mexico
 - * 5.6.2 South America
 - * 5.6.2.1 Brazil
 - * 5.6.2.2 Argentina
 - * 5.6.2.3 Rest of South America
 - * 5.6.3 Europe
 - * 5.6.3.1 Germany

- * 5.6.3.2 United Kingdom
- * 5.6.3.3 France
- * 5.6.3.4 Rest of Europe
- * 5.6.4 Asia Pacific
- * 5.6.4.1 China
- * 5.6.4.2 India
- * 5.6.4.3 Japan
- * 5.6.4.4 South Korea
- * 5.6.4.5 ASEAN
- * 5.6.4.6 Rest of Asia Pacific
- * 5.6.5 Middle East
- * 5.6.5.1 Saudi Arabia
- * 5.6.5.2 UAE
- * 5.6.5.3 Turkey
- * 5.6.5.4 Rest of Middle East
- * 5.6.6 Africa
- * 5.6.6.1 South Africa
- * 5.6.6.2 Rest of Africa

6. COMPETITIVE LANDSCAPE

- * 6.1 Market Concentration
- * 6.2 Strategic Moves
- * 6.3 Market Share Analysis
- * 6.4 Company Profiles (includes Overview, Core Segments, Financials, Strategy, Market Rank)*
 - 6.4.1 Nokia Corporation
 - 6.4.2 Cisco Systems Inc.
 - 6.4.3 Huawei Technologies Co. Ltd
 - 6.4.4 Broadcom Inc.
 - 6.4.5 Juniper Networks Inc.
 - 6.4.6 Ciena Corporation
 - 6.4.7 Ribbon Communications
 - 6.4.8 Infinera Corporation
 - 6.4.9 ADVA Optical Networking SE
 - 6.4.10 Arista Networks Inc.
 - 6.4.11 Acacia Communications
 - 6.4.12 Thales Group
 - 6.4.13 Fujitsu Ltd.
 - 6.4.14 Lumentum Holdings Inc.
 - 6.4.15 Marvell (Inphi)
 - 6.4.16 PacketLight Networks
 - 6.4.17 Microchip Technology Inc.
 - 6.4.18 LightRiver Technologies
 - 6.4.19 ID Quantique SA

7. MARKET OPPORTUNITIES AND FUTURE OUTLOOK

- * 7.1 White-space and Unmet-need Assessment

Optical Encryption Market Report Scope and Research Methodology
Market Definition and Coverage
 The optical encryption market is defined as hardware, embedded modules, software, and services that encrypt data while it is carried over fiber optic transport, including metro and long haul links used by operators and large enterprises.

Scope exclusions: We exclude encryption products that operate only on the electrical packet stream and do not sit on, or integrate with, the optical transport path.

Segments Covered in This Report* By Encryption Layer* Layer 1

- * Layer 2
- * Layer 3
- * By Data Rate* less than 10 Gbps
- * 10 - 40 Gbps
- * 40 - 100 Gbps
- * above 100 Gbps
- * By Component* Hardware Encryption Appliances
- * Coherent/Pluggable Modules and Optics
- * Key-Management / Orchestration Software
- * Managed Encryption Services
- * By Deployment Mode* On-Premise (Carrier-Owned)
- * Cloud / Network-as-a-Service
- * Edge / Remote-Site Appliances
- * By End-user Vertical* Datacenter and Cloud
- * BFSI
- * Government and Defense
- * Healthcare
- * Energy and Utilities
- * Retail and E-commerce
- * Other End-user Verticals
- * By Geography* North America* United States
- * Canada
- * Mexico
- * South America* Brazil
- * Argentina
- * Rest of South America
- * Europe* Germany
- * United Kingdom
- * France
- * Rest of Europe
- * Asia Pacific* China
- * India
- * Japan
- * South Korea
- * ASEAN
- * Rest of Asia Pacific
- * Middle East* Saudi Arabia
- * UAE
- * Turkey
- * Rest of Middle East
- * Africa* South Africa
- * Rest of Africa

Data Sources, Market Sizing, and ValidationDesk Research

Desk research was used to set the market boundaries and build the first set of assumptions on demand and supply. We relied on public references such as FCC and NTIA releases, NIST security publications, ITU-T and IEEE standards pages, and O ECD telecom indicators to understand network build activity and security expectations. We also reviewed operator and system integrator filings, investor presentations, and press releases to map how optical transport upgrades and security add-ons are being positioned.

To make the model practical, we used paid subscriptions focused on company financials and intelligence, along with patent databases and a news and financials service, to track product launches and estimate typical pricing direction. These inputs helped us shortlist realistic adoption curves by link type and by buyer group, then pressure-tested through interviews. The examples listed above are illustrative and not exhaustive, and many other public and internal reference points were used for data collection, cross-checks, and clarification.

Primary Interviews and Surveys

Primary work was done through expert interviews and structured surveys with telecom operators, data center network teams, optical equipment channel partners, and security decision-makers who influence encryption choices. We focused on validating where encryption is actually activated (line-side versus client-side, and in new builds versus retrofits), and how buyers think about tradeoffs such as latency, compliance needs, and upgrade timing. Coverage was kept global so regional differences in backbone expansion and cross-border data handling could be reflected in the final assumptions.

Distribution of primary research fieldwork respondents

Company type	Respondent position	Region
Top tier: 33%	CXOs: 12%	APAC: 44%
Mid tier: 47%	Functional/Unit leaders: 41%	EMEA: 32%
Smaller Players: 20%	Managers: 47%	Americas: 24%

Market-Sizing & Forecasting Sizing was built mainly using a top-down approach where optical transport spending and installed fiber link activity were reconstructed into an addressable pool, followed by applying penetration rates for optical-layer encryption attach. For corroboration, we then used selective bottom-up approximations, such as sampled deployments by major operator groups and typical average selling price ranges for line cards, pluggables, and software licenses, to confirm that totals stayed reasonable.

Key inputs used in the model included optical transport upgrade cycles, growth in data center interconnect capacity, share of links carrying regulated or sensitive traffic, typical encryption enablement rates by link type, and pricing movement as higher-speed coherent solutions become common. Where local data was thin, assumptions were bridged using comparable operator footprints and supplier channel checks, then adjusted only after the logic was validated in interviews.

Forecasts were produced using scenario analysis anchored on backbone build plans and security policy adoption, with a light multivariate regression used as a consistency check against traffic growth and capex cycles. Final numbers were converted to USD using average annual exchange rates for the year being sized, which reduced timing noise in multi-country totals.

Data Validation & Update Cycle Validation was done by triangulating outputs against independent signals such as optical transport equipment shipment commentary, public capex guidance from major carriers, and the pace of data center interconnect expansions. If a region or year showed a jump that could not be explained by these signals, the assumptions were re-opened and the relevant interview themes were revisited before sign-off.

Each model pass goes through multi-step internal checks where one analyst reviews inputs, another reviews calculations, and a final review checks whether the story matches the numbers. Reports refresh annually, and interim updates are made when a material event changes demand, pricing, or supply conditions. Right before delivery, a fresh pass is performed so clients receive the most current view available.

Mordor Intelligence's Optical Encryption Market Size Measured Against Other Published Estimates It is normal to see different market sizes for optical encryption, even when the titles look similar, because the counted products and the activation point in the network can vary. Differences also come from how pricing is treated for high-speed coherent optics, and from whether the study assumes fast adoption across all link types or limits uptake to the most security-sensitive routes.

Key gap drivers in this space usually include whether Layer 2 and Layer 3 encryption features are bundled into the same total, whether only optical transport (OTN and line-side) is counted, and how services and software are added to hardware revenue. Currency timing can also shift totals when suppliers sell globally, and refresh cadence matters because network upgrade plans can change quickly after new regulations or major breaches.

Benchmark comparison

Source | Market Size | Gaps in Research Methodology |

Mordor Intelligence | USD 4.85 B (2025) |

Industry Publisher A | USD 4.08 B (2025) | This figure looks lower because it typically limits revenue to optical-transport encryption hardware and may not fully count key management software and managed service revenue that is bundled into deployments.

Global Consultancy B | USD 6.16 B (2025) | This figure looks higher when Layer 2 and Layer 3 encryption feature revenue is added broadly across network upgrades, and when average selling prices are assumed to hold up at higher-speed ports for longer.

The spread mainly comes from whether the total includes only optical-path encryption, or also adds adjacent packet-layer security features, and from how quickly upgrades are assumed to turn into paid encryption activations. By counting Layer 1, 2, and 3 only when the function is delivered on optical transport equipment or integrated coherent modules, and then refreshing attach-rate assumptions through recurring operator and channel checks, the sizing stays tied to the optical-layer demand pool, a treatment applied by Mordor Intelligence.

Key Questions Answered in the Report What is driving the strong growth of the optical encryption market? Demand for quantum-safe security, AI-led bandwidth surges, and zero-trust mandates that favor hardware-based Layer 1 solutions are collectively pushing the market toward an 8.62% CAGR through 2031.

Which segment currently leads in revenue? Layer 1 hardware platforms dominate with 45.60% market share in 2025 because they encrypt at line rate and remove software vulnerabilities.

Why is Asia Pacific the fastest-growing region? Large-scale quantum-technology funding, 6 G trials, and aggressive data-center builds give Asia Pacific a 9.62% CAGR, outpacing all other regions.

How are coherent pluggable modules changing the competitive landscape? Silicon-photonics pluggables cut cost and power, posting a 15.85% CAGR that challenges traditional chassis-based appliances and expands supplier diversity.

What role do post-quantum standards play in adoption? NIST's final FIPS 203-205 standards remove algorithm uncertainty, prompting enterprises to budget for crypto-agile optical hardware compliant with future regulatory audits.

Are high capital costs still a barrier? Yes, coherent 400 G+ optics remain expensive, but initiatives like Coherent's 6-inch InP wafers are expected to lower die costs by 60% within two years, easing adoption for cost-sensitive buyers.

Related Reports Explore More ReportsReport on Fiber Optic Cable IndustryFiber Optic Component MarketOptical Interconnect Industry OverviewReport on Optical Transceiver IndustryIndustry Outlook of Optical Transport NetworkIndustry Trends in Optical Wavelength ServicesIndustry Outlook of Passive Optical Network (PON) EquipmentPhysical Internet Market SizeTelecom Service Assurance Industry OverviewIndustry Trends in Telecom Services