

Enterprise edge strategy has outgrown the CDN conversation. Digital services are more distributed and increasingly shaped by AI, and the old model of managing delivery, security, and compute as separate layers is breaking down. The shift toward an integrated edge platform is now a strategic priority, not a future consideration.

Rethinking Edge Strategy for the AI Era: Why the Edge Needs More Than a Faster CDN

June 2026

Written by: Nikhil Batra, Senior Research Director, IDC Telecom and Enterprise ICT Research

Synopsis

Enterprise edge requirements have moved well beyond the traditional content delivery network (CDN) conversation. Digital services are now more distributed, application-led, and API-heavy, and increasingly shaped by AI-enabled experiences and automated interactions. Buyers are managing higher expectations on speed, uptime, security, and control across delivery environments that remain fragmented across tools, providers, and teams. The CDN-only frame no longer captures what enterprises need at the edge.

The market is moving with this shift. **IDC forecasts the worldwide managed edge services market, covering service provider edge, CDN edge, and on-premises edge deployments, to grow from US\$2.84 billion in 2024 to US\$7.82 billion in 2029, at a compound annual growth rate (CAGR) of 22.4%.**

This growth is tied to a broader change in how digital services are built and consumed. Organizations are supporting users, employees, partners, devices, and applications across more locations and across last-mile conditions that vary widely. Real-time transactions and media-heavy traffic have grown faster than many infrastructure plans assumed. Application programming interfaces (APIs) now connect customers, partners, devices, and internal systems at a scale that did not exist five years ago. As a result, edge delivery is becoming part of the application environment itself, not only a mechanism for accelerating content.

Asia/Pacific is forecast to be the fastest-growing region at 23.1% CAGR, slightly ahead of the Americas at 22.2%, and Europe, the Middle East, and Africa (EMEA) at 21.9% (see Figure 1).

AT A GLANCE

KEY STATS

- » The worldwide managed edge services market is forecast to grow from US\$2.84 billion in 2024 to US\$7.82 billion in 2029, at a CAGR of 22.4%.
- » Asia/Pacific is the fastest-growing region at 23.1% CAGR, followed by the Americas at 22.2% and EMEA at 21.9%.
- » The share of edge computing deployments incorporating AI is expected to rise from about 5% in 2023 to 60% by 2029.

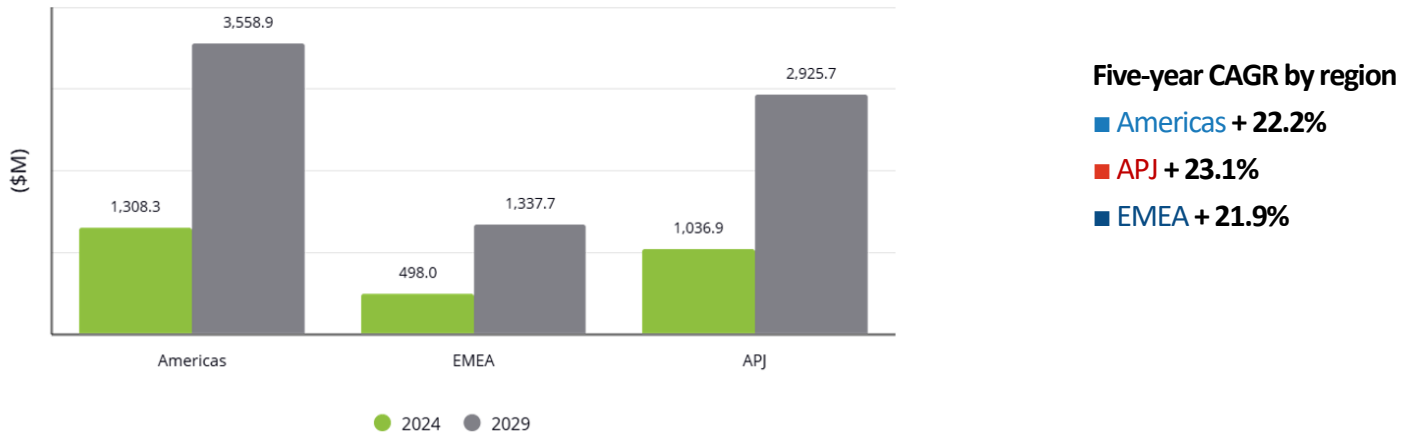
CHALLENGE

Enterprises are managing digital services across more regions, providers, and clouds while delivery, security, compute, and observability remain fragmented across separate tools and teams. The CDN-only model no longer addresses the full scope of edge requirements, particularly as AI-enabled services, real-time APIs, and data sovereignty mandates raise the bar on what the edge must carry, protect, and process.

WHAT'S IMPORTANT

From CDN to integrated edge platform: The edge conversation is shifting from caching and acceleration to an integrated operating model where delivery, application protection, edge compute, and observability share policy, telemetry, and routing logic. Organizations that treat these as one set of decisions, rather than stitching them together after the fact, will be better positioned for both resilience and growth.

AI changes the edge equation: AI-enabled services introduce less predictable traffic, new security risks such as prompt injection and model abuse, and inference workloads that need compute close to users. These requirements make the case for an integrated edge model more urgent than a CDN-only approach.

Figure 1: **Worldwide Enterprise Managed Edge Services Spend (by Region), 2024–2029**

Source: IDC Worldwide Managed Edge Services Forecast, 2024–2029

The drivers differ by region, though. Asia/Pacific is led by demands of mobile-first traffic, greenfield buildouts, and localization mandates across countries like Australia/New Zealand (ANZ), Singapore, China, India, and Indonesia. The Americas are primarily driven by enterprise AI inferencing and media requirements, at scale. EMEA growth is shaped more by regulation and resilience, especially from a GDPR and sovereign cloud point of view.

Segment wise, on-premises edge is the fastest-growing deployment model at 26.6% CAGR, reflecting enterprise demand for latency control, data sovereignty, and more direct management of workloads that cannot always be served efficiently from centralized cloud environments.

AI is one of the strongest forces shaping organizational edge and broader digital infrastructure strategy. AI-enabled experiences, inference calls, retrieval-heavy applications, and more automated application behavior are placing new demands on latency, routing, security inspection, and where processing happens. **IDC expects the share of edge computing deployments incorporating AI to rise from about 5% in 2023 to 60% by 2029.** That is not just a workload shift. It changes what edge environments are expected to carry, observe, protect, and optimize.

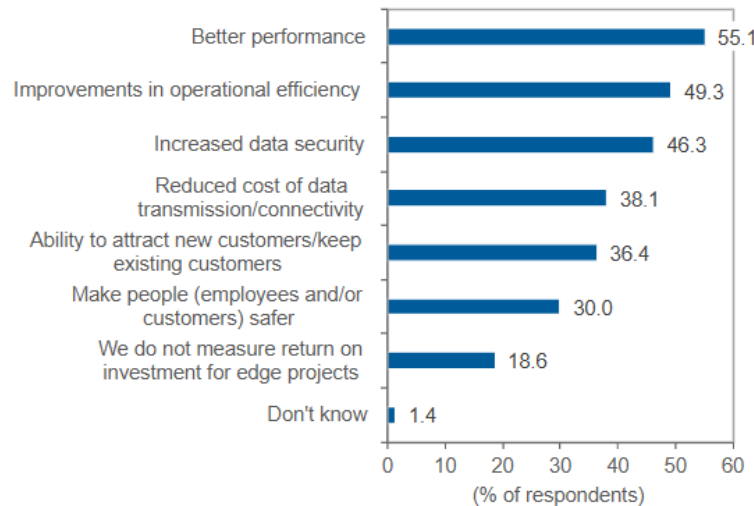
The edge is therefore moving closer to the center of digital operations. For some organizations, the business case remains defensive, centered on resilience, security, compliance, and cost control. For others, it is moving toward offense, where the edge becomes a way to support AI-enabled experiences, richer media, faster application response, and new customer interaction models. Treating this as a CDN problem misses where the edge now sits in the digital business.

The Current Edge Model Struggles to Deliver the Outcomes Organizations Want

Organizations now judge their edge and CDN investments by business outcomes, and performance sits at the top of the list. IDC's *Edge View Survey, 2025* highlights (Figure 2) that 'application and service performance' ranks as the top success metric for edge implementations (55.1%), ahead of operational efficiency improvements (49.3%) and data security (46.3%). However, older edge architecture and deployment models struggle to deliver against these metrics. Providing digital services across multiple regions, clouds, APIs, and user environments, while still meeting user expectations for speed, availability, security, and cost, is hard to sustain when delivery, security, compute, and visibility are managed as separate layers.

Figure 2: **How Organizations Measure Edge Success**

Q.How does your organization measure the ROI of edge projects?



Source: IDC's *Edge View Survey, 2025* (n = 600)

This gap between performance expectations and operational realities shows up as a recurring set of operating pressures, spread across every layer of the edge model, and most organizations are dealing with several of them at once. Six deserve closer examination:

- » **Uneven application and workload performance across regions.** Organizations are seeing more variability across geographies, providers, and last-mile conditions, making transaction response times and API behavior harder to predict. For customer-facing applications, performance inconsistency is not a technical issue — it directly affects conversion, satisfaction, and trust.
- » **Fragmented delivery and security operations.** CDN, distributed denial-of-service (DDoS) protection, web application and API protection (WAAP), bot management, and network policy are still often managed through separate tools, vendors, and teams. Some CDN providers have responded by bundling security services, but many enterprise operating models have not caught up. The result is fragmented ownership and slower response when something fails. Fully managed services are increasingly becoming a core part of edge architecture strategy. Enterprises now expect providers not only to deliver infrastructure, but also to take operational ownership.

- » **Limited visibility across the delivery path.** When a service degrades, operations teams must isolate the fault across application, origin, cloud, network, CDN, API gateway, and security layers. Without a shared view, each team works from its own data, extending mean time to resolution and increasing friction between application, networking, security, and cloud teams.
- » **Rising cost pressure from traffic growth.** Media traffic, API volumes, and always-on services are pushing more load through the delivery chain than older peak-hour models assumed. Egress costs, origin load, and routing efficiency are now part of the same conversation as performance and experience, and finance teams are asking harder questions about whether the delivery model remains cost-efficient at scale.
- » **Resilience risk is moving into mainstream planning.** The risk now extends well beyond a single cloud or network outage. Provider concentration, cable cuts, regional internet disruption, and subsea infrastructure dependency are all raising the business impact of delivery failure. The practical question is shifting from “Which CDN is fastest?” to “How do we absorb disruption, reroute traffic, and maintain service continuity when upstream infrastructure is affected?”. **The business cost of an hour of disruption has increased sharply over the last three to five years.**
- » **Data sovereignty is becoming part of edge architecture.** Edge strategy now must account for where traffic traverses, where user data is processed, where logs are stored, and which provider can support in-country or regional delivery requirements. For regulated industries, this makes edge design part of compliance architecture, not just a performance decision.

What used to be manageable as separate layers is becoming harder to operate as digital delivery becomes more distributed and exposed.

Organizations that get this layer right can address both defense and offense: They can reduce delivery risk and cost while also supporting AI-enabled services, media-heavy experiences, and API-driven business models with greater confidence.

Beyond the CDN-Only Mindset

The CDN discussions were anchored around caching, acceleration, and offload. While those capabilities still matter, they no longer define the full enterprise requirements. The workload at the edge now includes interactive applications, partner APIs, bot and machine traffic, AI-linked services, richer media, and security inspection. This shifts the discussion from CDN capacity alone to the digital operating model enterprises need. IDC sees this as a move toward a more integrated edge platform model. The requirement is not simply to buy more edge services from the same provider. It is to bring delivery, security, edge compute, observability, orchestration, and automation into a more unified operating layer.

A modern edge platform needs to do four things differently from a standalone CDN or a traditional set of adjacent services:

- » **Shared control across delivery and protection.** Enterprises need a consistent way to manage routing, security policy, and mitigation across their delivery environment. An integrated control layer lets organizations apply policy, adjust routing, manage protection, and respond to changes from one place.
- » **Compute closer to the point of interaction.** More digital services now need logic to run closer to users, devices, or data sources. This includes edge compute and AI inferencing use cases where cloud round trips add cost, latency, or compliance exposure. Running AI models closer to where data is generated reduces latency, lowers bandwidth costs, supports privacy requirements, and improves operational resilience.
- » **Make observability part of the operating layer.** Observability is no longer just a reporting feature. It is now part of how enterprises manage performance, risk, customer experience, and cost across distributed digital services. IDC's *Enterprise Connectivity and Telecom Survey, 2025*, highlights that unified observability was one of the top 3 buying criteria for organizations, who now expect real-time, granular, business-relevant reporting as part of the core solution, rather than a bolted add-on.
- » **Secure the edge with AI-augmented real-time capabilities.** Security has become a foundational layer of modern edge platforms rather than a standalone perimeter function. Enterprises now expect L3–L7 DDoS mitigation, API security, bot management, and web application firewall (WAF) capabilities as part of the core edge architecture. As applications and APIs become increasingly distributed, organizations are prioritizing platforms that can deliver real-time threat detection, consistent policy enforcement, automated mitigation, and centralized visibility.

The integrated edge platform is therefore less about replacing the CDN than about expanding the operating model around it. Enterprises still need fast and efficient delivery, but they also need security, compute, observability, and automation to work together. That is the shift beyond the CDN-only mindset.

AI Raises the Stakes at the Edge

AI adds a new level of complexity to enterprise edge strategy and makes the move beyond CDN-only models more urgent. Traditional CDN architectures still deliver on caching and acceleration, but AI-enabled services create more dynamic traffic, more API dependency, and more real-time decisioning. The edge now needs to do more than move content closer to users. It needs to help route, secure, observe, and manage digital interactions as they happen.

AI Changes the Nature and Direction of Edge Traffic

AI services behave differently from traditional web or media workloads. They are more request-driven and data-dependent. For example, a customer interaction may trigger an inference call, a retrieval request, a policy check, and an API response in near real time. This creates a different type of pressure on the edge, where the platform needs to route traffic that is less predictable than conventional content delivery.

AI Readiness is the Leading Driver of Infrastructure Investment in 2026

IDC's Future Enterprise Resiliency and Spending Survey 2026 confirms the shift in spending priorities. **45.1%** of respondents cited preparing for **greater use of AI in the business as the top driver of infrastructure spending increase**, ahead of improving organizational resiliency (34.4%), reducing IT operating costs (29.6%), and launching new applications requiring greater performance (27.9%).

Source: IDC's Future Enterprise Resiliency and Spending Survey (FERS), Wave 9 (December 2025, n = 999)

AI and generative AI (GenAI) are already increasing demand on edge networks because training and inference are compute- and data-intensive. This is where a CDN-only approach starts to show its limitations. Caching and acceleration can improve delivery efficiency, but they do not provide enough control over API behavior, inference-linked requests, policy decisions, and traffic anomalies. AI increases the need for an edge model that brings together delivery, security, compute, and visibility in a unified framework.

AI Inference at the Edge

Running inference at the edge changes the economics and architecture of enterprise AI. Instead of round-tripping every request to a centralized cloud, organizations can process latency-sensitive workloads such as fraud scoring, visual inspection, and personalized recommendations, closer to users and devices. The trade-off is operational: edge inference requires model life-cycle management, device-level security, and orchestration between edge and cloud that most enterprises have not yet built. IDC believes that getting this right is a prerequisite for scaling AI beyond pilot use cases.

AI Raises the Security and Visibility Bar

AI-linked traffic also changes the risk profile. Inference-linked workflows increase the need to understand what is normal, what is abnormal, and what needs action. A CDN-only approach may show traffic volumes and delivery performance, but it is less suited to managing the combined view of application behavior, API exposure, and security events.

Observability becomes more important because AI-linked services are harder to troubleshoot when delivery and security data sit in different tools. IDC expects observability to become a key enterprise buying requirement, with GenAI and ML increasingly embedded in observability workflows to improve reporting, reduce reaction time, and accelerate fault determination.

AI is therefore reshaping both what enterprises need from the edge and how edge environments are managed, strengthening the case for an integrated model over a CDN-only approach. That case becomes concrete when applied to the use cases enterprises are now scaling.

Where the Integrated Edge Model Starts to Pay Off

A traditional CDN-led approach handles delivery and acceleration well but breaks down when enterprises try to operate it across workloads such as AI inferencing, application security, anti-DDoS and real-time analytics. As edge environments become more distributed, the operational case for an integrated, managed edge model grows stronger.

This is where the integrated edge platform earns its place. It brings delivery, security, edge compute, observability, and orchestration into one operating layer — so that policy, telemetry, and incident response work from a shared foundation rather than across disconnected tools. Enterprises increasingly rely on service providers, including communications service providers, hyperscalers, and CDN providers, to deliver this integrated layer without having to build specialist teams in every region.

IDC has identified five domains — security, inferencing, media, IoT, and data sovereignty — as major areas where edge computing use cases are developing, and integrated, managed edge services are playing a critical role:

Edge Category	Key Trends	Industry Use Cases	Where the Integrated Platform Pays Off
Security at the edge	Zero trust architecture, AI-powered threat detection and automated response, 5G-related vulnerabilities, supply chain risks, quantum-resistant encryption planning	Real-time video surveillance and analytics, industrial control system (ICS) and operational technology protection, access control, autonomous systems security, Smart City security	A shared control plane enforces policy consistently across CDN, DDoS, WAAP, and bot management — eliminating the drift that separate tools produce. Combined telemetry surfaces anomalies that single-tool views miss, and AI-driven policy tuning reduces false positives across the whole layer.
Inferencing at the edge	Distributed and agentic AI inference, specialized compact models, edge-to-cloud-to-edge model life cycle, AI-optimized silicon, lightweight inference runtimes	Autonomous vehicles, healthcare diagnostics and patient monitoring, manufacturing predictive maintenance, financial services fraud detection, real-time video analytics, retail vision-based inventory and checkout	Edge compute hosts inference alongside delivery, which a CDN alone cannot do. Orchestration manages model deployment across distributed nodes, and AI-aware security inspects inference traffic for prompt injection and abuse.
Media at the edge	CDN evolution into edge delivery services, content-aware encoding, media over QUIC, CMCD, and CMSD standards, live streaming growth above 20% annually	Augmented reality (AR) and virtual reality (VR) experiences, multiplayer cloud gaming, live sports and entertainment streaming, personalized and targeted advertising, real-time video monitoring	Edge compute runs personalization, ad insertion, and content-aware encoding close to viewers, beyond what caching alone can do. Integrated DDoS and WAAP absorb peak attack volume during live events, while observability tracks quality of experience in real time.
IoT at the edge	Massive Internet of Things (IoT) scale, edge-AI synergy, mobile edge computing (MEC) expansion with 5G and 6G, decentralized local data processing	Smart healthcare wearables, industrial automation and predictive maintenance, Smart Cities and traffic management, remote asset monitoring, autonomous mobility	Edge compute filters and acts on telemetry locally rather than backhauling to a central cloud. Integrated zero trust and device identity scale to large fleets, and observability correlates device and network behavior in one view.
Data sovereignty at the edge	Regulatory scrutiny across more than 144 countries with data protection laws, localization mandates, hybrid cloud compliance, data governance frameworks, in-country delivery requirements	Financial data localization, healthcare and pharmaceutical compliance, government data management, industrial IoT residency, regulated industry edge architectures	Delivery, processing, and logging run within the same in-country footprint, simplifying audit and residency guarantees that multivendor stacks struggle to provide. A single policy layer keeps traffic, data, and audit trails inside required geographies.

Across all five areas, the failure mode of a fragmented stack is the same — integration friction. The integrated edge platform addresses this by collapsing those decisions into a single operating layer and makes advanced edge capabilities accessible to enterprises that cannot build them in-house.

Tata Communications Edge Distribution Platform: A Network-Led Approach to Integrated Edge

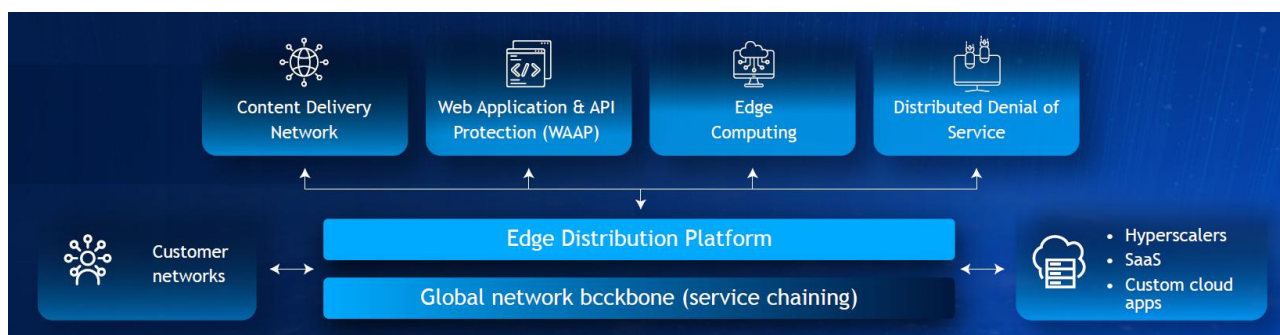
Tata Communications' approach to the integrated edge brings content delivery, DDoS mitigation, web application and API protection, edge compute, analytics, orchestration, and managed operations under its Edge Distribution Platform (EDP). Aligned with its broader Digital Fabric strategy, EDP handles delivery, security, and edge compute for distributed digital services, anchored on Tata Communications' global backbone, and positioned for organizations looking to consolidate these functions under a single management interface.

The Edge Distribution Platform Architecture

The EDP proposition is built on four core domains where Tata Communications has established capability and a right to compete: global network reach, programmable edge compute, managed security, and life-cycle-led enterprise services. The platform is powered by 65+ Super-PoPs, extendable to 300+ across the Tata Communications global network, and an underlying backbone capacity of 300Tbps. These four domains are realized through seven integrated capabilities that operate under a shared control plane and are delivered as a managed service.

Figure 3 shows how these elements fit together.

Figure 3: ***Tata Communications Edge Distribution Platform Architecture***



Source: Tata Communications, 2026

The seven elements of EDP are:

- » **Content delivery network.** A global CDN for live and on-demand content delivery, with smart caching, modern streaming protocol support, token-based security, and IPv4 and IPv6 support across the Tata Communications footprint.
- » **DDoS protection.** Globally distributed mitigation across volumetric, protocol, and application-layer attacks, covering more than 60 attack vectors from L3 to L7, with the service provider claiming sub-60-second response on volumetric attacks and real-time threat intelligence feeding the mitigation logic.

- » **Web application and API protection.** TLS 1.3 encryption between the edge and origin, integrated bot management, API traffic protection, and customizable rule sets for application-layer security, all managed from a unified control plane.
- » **Intelligent edge compute.** Edge functions for personalization, API handling, and lightweight inference, with ready-to-use templates so organizations can deploy logic at the edge without building custom infrastructure.
- » **Unified orchestration and visibility.** A single control plane managing petabyte-scale traffic at high concurrency, with AI-powered analytics, real-time anomaly detection, role-based control dashboards, and self-service onboarding for new applications and policies.
- » **Managed services and support.** Fully managed operations with 24 x 7 monitoring, life-cycle management, and engineering support — designed to take operational load off enterprise IT teams.
- » **Proactive defense.** Continuous vulnerability scanning, clear remediation service-level agreements (SLAs), and AI-based policy tuning, including an around-72-hour vulnerability-mitigation SLA at under 1% false positive rate.

The combined architecture supports 99.999% platform availability and 100% in-country delivery options across multiple regulated geographies — ensuring adherence to regulatory and data sovereignty requirements.

How EDP Applies AI Across the Stack

AI runs through both the workload and the operations side of EDP. The intelligent edge compute layer is built to host inferencing close to users, targeting real-time AI experiences and API-driven services. On the operations side, AI-driven analytics, anomaly detection, automated mitigation, and policy tuning underpin EDP's response speed and false-positive SLAs. Tata Communications plans to add functions-as-a-service capabilities in the next 12–18 months, aiming to extend the platform's edge programmability for developers.

The Tata Communications Advantage

- » **Network and security-led edge foundation.** Tata Communications' strongest starting point is the combination of its global network assets and security services capability. Most integrated edge providers come from one of these two starting points — few bring both. This gives EDP a clearer role where enterprises need performance, protection, and resilience considered together, particularly in regions requiring in-country delivery, provider diversity, or stronger control over traffic flows.
- » **Managed operations and simplification.** Tata Communications can lean on its long-standing managed services experience as the operational layer for EDP. Many organizations want advanced edge capabilities without building and running every operational layer themselves. EDP's value will be significant where Tata Communications can reduce onboarding effort, support migration, and help customers tune delivery and security policies after deployment.
- » **Network-led resilience in a more fragile delivery environment.** As digital services become more dependent on global routes, subsea infrastructure, regional internet stability, and third-party platforms, continuity planning is becoming part of the edge decision. Tata Communications' global backbone, Super-PoP footprint, and peering depth give enterprises a network-led option for strengthening delivery resilience across markets. This is relevant for organizations that need stronger path diversity and a resilient platform for critical applications and APIs.

Tech Buyer Considerations

Tata Communications is competing in a market where established CDN and edge providers already have strong brand recognition, mature self-service portals, and deeper developer ecosystems. EDP will therefore need to prove its differentiation through operating outcomes, not only platform architecture. Tech buyers should look closely at onboarding processes, migration support, regional performance, policy control, observability depth, and the maturity of edge compute solutions.

The road map, including functions-as-a-service capabilities, integration with multicloud connect and managed hosting services, should be treated as an emerging part of the EDP story rather than a fully mature capability today. It is strategically relevant because it can make edge compute programmable and easier to consume, but buyers should assess how these functions are packaged, governed, supported, and integrated into existing application workflows before treating them as a core adoption driver.

IDC's view is that Tata Communications' EDP is best understood as an integrated edge approach rather than a CDN replacement alone. Its right to win is strongest where enterprises want delivery, application protection, managed operations, unified visibility, and resilience to come together in a coordinated operational model. The main test will be execution: whether Tata Communications can make the platform simple enough to adopt, mature enough to operate at scale, and differentiated enough to stand out against CDN and edge providers with deeper developer-led market perception.

"The edge is evolving into a strategic layer for intelligence, not just delivery. As enterprises embrace AI-driven, distributed applications, the ability to process, secure and optimise data closer to users is critical. AI is accelerating this shift by enabling real-time decisions, predictive performance and automated security. The future belongs to unified edge platforms that seamlessly combine performance, security and compute to deliver faster, smarter and more resilient digital experiences." – **Vaibhav Dutta, Vice President and Global Head-Cybersecurity Products & Services at Tata Communications**

Essential Guidance: Moving Toward the Next Phase of Edge Strategy

The next phase of enterprise edge strategy will be defined less by where content is cached and more by how delivery, security, compute, observability, and AI orchestration are operated together. Organizations should consider the following as they work through those decisions:

- » **Take an integrated view of edge, starting today.** As you evaluate your digital infrastructure strategy, avoid planning CDN, security, edge compute, and observability as separate decisions and trying to stitch them together afterwards. Plan for delivery, application and API protection, edge compute, and observability as one set of decisions, since they will increasingly need to share policy, telemetry, and routing logic.
- » **Evaluate managed services depth, not just platform features.** Most enterprises do not have deep technical expertise across security, compute, observability, and AI orchestration. Provider depth in managed services, including onboarding, migration, life-cycle support, policy tuning, and incident response, is where edge platform value compounds or fragments. Evaluate SLAs for detection, mitigation, and false-positive rates, and ask how the provider supports day 2 operations after the initial rollout.

- » **Build resilience into the procurement decision.** Provider concentration, cable cuts, regional internet disruption, and geopolitical exposure are now consistent, mainstream concerns. Buyers should think about where path diversity is needed, and how easily traffic, policy, and observability can move between providers if conditions change. Treat resilience as part of the platform decision, not a separate business continuity one.
- » **Plan for AI workload requirements before AI is in production.** AI-enabled services change the edge in three practical ways: traffic patterns become less predictable, prompt injection, model abuse, and API rate manipulation become new security concerns, and inference workloads need compute close to users. Evaluate edge compute for inferencing, AI-aware security inspection, and observability that can read AI traffic anomalies.
- » **Make data sovereignty part of the edge architecture.** For regulated industries and geographies with localization requirements, edge architecture is now part of compliance architecture. Map where traffic traverses, where data is processed, where logs are stored, and where audit trails are kept. In-country delivery, processing, and storage options should be evaluated together rather than treated as separate compliance decisions, especially for financial services, healthcare, government, and critical infrastructure workloads.
- » **Treat observability as a major buying criterion.** Real-time, business-relevant reporting across delivery, security, and edge compute should be a contractual expectation. Evaluate whether the provider's observability is designed for operations teams to act on through dashboards, alerts, and automation. Insist on end-to-end visibility of the delivery path, not just edge-side telemetry, so that troubleshooting can identify the root cause.

The enterprises that will get the most out of the next phase of edge strategy are those that treat it as one operating decision rather than several disconnected ones. That is what makes the integrated edge model practically valuable, and what makes provider selection a more strategic choice for enterprise buyers than it was when CDN was the dominant frame.

About the Analyst



Nikhil Batra, Senior Research Director, Telecom

Nikhil Batra is a Senior Research Director for the regional telecommunications team in IDC Asia/Pacific. Based in Australia, Nikhil focuses on Telecom Service Provider and tech vendor strategies, along with enterprise services across the A/P region. In his role, Nikhil works with the regional telecom teams to produce intelligence reports, market insights, and contributes to various consulting projects for leading regional telcos and tech vendors.

MESSAGE FROM THE SPONSOR

Tata Communications is redefining the edge with its Edge Distribution Platform (EDP) — bringing together performance, security, resilience, and intelligence into a unified, AI-driven platform. Built on a global network backbone, EDP enables enterprises to deliver faster, more secure and highly personalized digital experiences closer to users, agents, and workloads. As businesses embrace AI and distributed architectures, our platform provides the agility, visibility, and resilience needed to stay ahead.

Discover how EDP can transform your edge strategy: [Enterprise Edge Distribution Platform \(EDP\) | Secure Edge Computing](#)



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Asia/Pacific Headquarters

18 Cross Street
#11-01
Singapore 048423
65.6226.0330
Twitter: @IDC
blogs.idc.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2026 IDC. Reproduction without written permission is completely forbidden.