Hype Cycle for Enterprise Communication Services, 2026

8 July 2026 - ID G00853211 - 153 min read

By: Khurram Shahzad

Initiatives: Strategy, Risks and Opportunities

Enterprise communication services are evolving rapidly due to AI, new business models and as-a-service growth. This Hype Cycle helps CSP product leaders evaluate emerging innovations to make urgent roadmap decisions and maintain market competitiveness.

Analysis

What You Need to Know

The Hype Cycle for enterprise communication services assesses the maturity, adoption and business impact of emerging and established enterprise communication services. The 2026 Hype Cycle reflects a rapidly evolving landscape driven by advances in AI, edge computing, cloud and security, as well as new business models and service delivery paradigms. Currently there are multiple services such as network monetization APIs, LEO D2D services, CSP industry vertical solutions, sovereign AI and cloud, 5G private mobile networks, GPUaaS, agentic SMB service bundles, cross-cloud networking and machine customers in telecom that are clustered together at Peak of Inflated Expectations. Communications service provider (CSP) product leaders face a constant barrage of emerging technologies and trends and should use this Hype Cycle to:

- Validate the benefit and/or impact of technologies on current, emerging, and future products and services roadmaps.
- Create detailed product roadmaps that outline the timelines and strategies for launching offerings in the market.
- Develop consensus within product, business, IT, network and infrastructure teams on the technologies, features and capabilities required to offer these products and services.
- Avoid investing resources in overhyped ideas that will have low impact or are too far away from adoption.

The Hype Cycle

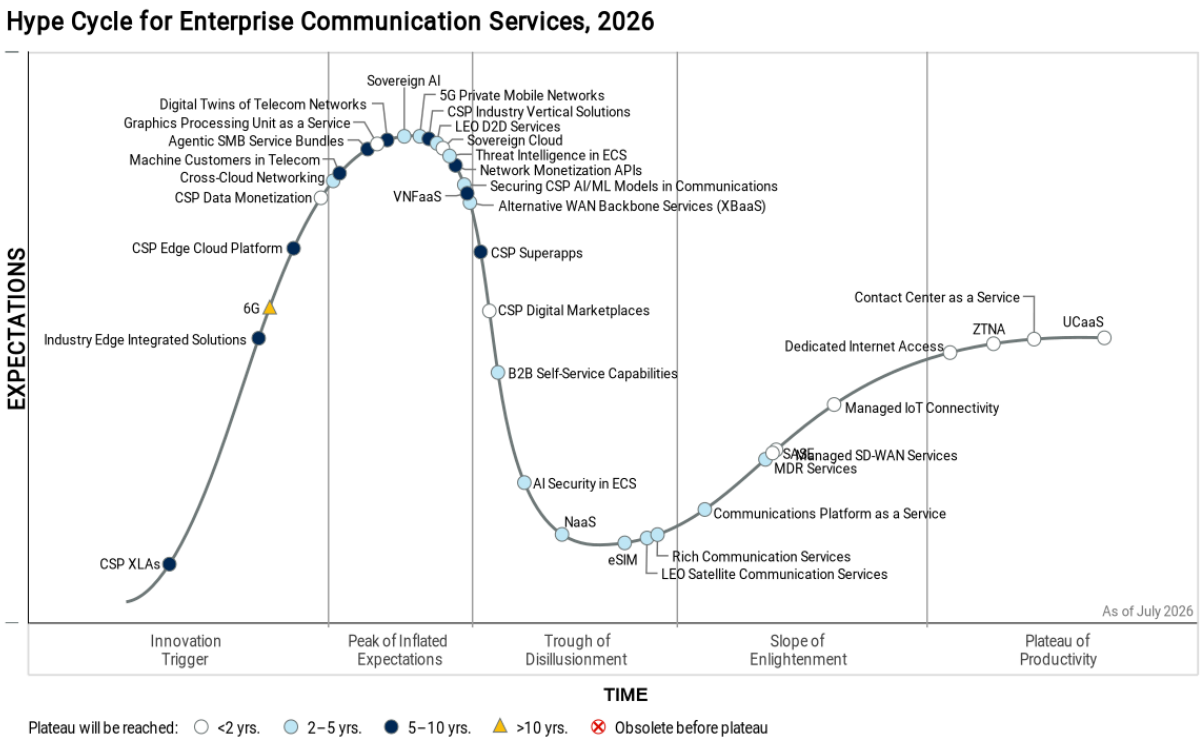
B2B services remain a strategic pillar for CSP growth, but success hinges on adapting to rapidly evolving enterprise requirements, shifting buying behaviors and accelerating technology innovation. Enterprise communication services now extend far beyond traditional connectivity, collaboration and security to include advanced AI-driven security, edge computing, AI-driven automation and new as-a-service models.

The CSP growth opportunity is reinforced by rising enterprise IT spending, particularly as organizations invest in AI infrastructure, such as accelerated servers and GPU as a service, to support next-generation workloads and meet increasing demand for local sovereign solutions. Despite ongoing macroeconomic and geopolitical uncertainties, IT spending is projected to increase, driven by the need for digital transformation, operational resilience and cost optimization. [1] Enterprises are prioritizing scalable, agile and consumption-based communication services that align with cloud-first and hybrid strategies. Geopolitical dynamics, especially in regions such as Europe and Asia, are fueling demand for sovereign cloud and AI solutions, while edge computing is gaining traction as organizations address latency, privacy, security and business continuity requirements.

CSPs are responding by developing flexible management models and self-service capabilities that enable enterprises to provision, manage and optimize services through digital marketplaces and unified platforms. The rise of B2B self-service, CSP superapps and digital marketplaces enables organizations to access a broad portfolio of networking, IoT, AI and security solutions through a seamless, on-demand experience.

Competitive pressures continue to intensify as nontraditional players, including IT service providers, hyperscalers, LEO satellite operators and alternative WAN backbone service providers (XBaaS providers), expand their presence in the enterprise communications market. To differentiate and drive sustainable growth, CSPs must innovate rapidly and deliver integrated, value-added solutions that address evolving enterprise requirements for agility, security and participation in digital ecosystems. They must also continuously update their product roadmaps to address current and emerging enterprise needs and maintain a competitive advantage.

Figure 1: Hype Cycle for Enterprise Communication Services, 2026



The Priority Matrix

The 2026 Priority Matrix reveals that while many transformational and high-value enterprise communication services remain clustered in the two- to 10-year horizon, the most immediate competitive advantages lie in high-impact innovations that will reach mainstream adoption in less than two years. Disruptive solutions such as managed IoT connectivity, SASE, ZTNA, DIA, managed SD-WAN services, CSP data monetization, GPUaaS and CSP digital marketplaces are already reshaping the traditional CSP portfolio for enterprises and small and midsize businesses (SMBs) and driving immediate innovation in connectivity, security and agility.

For CSP product leaders, these maturing, near-term services represent table stakes for remaining competitive in the market. However success will come to those who aggressively commercialize and scale these high-impact services today. For longer-term roadmap planning and continued differentiation, CSP product leaders should focus on services projected to reach mainstream adoption within two to five years, particularly AI-driven and as-a-service offerings. CSP product leaders should proactively plan for 5G private mobile networks, CPaaS, NaaS, LEO satellite communication services, sovereign AI, AI security in ECS, MDR services, securing CSP AI/ML models, threat intelligence in ECS, eSIM, RCS, LEO D2D services, B2B self-service capabilities and cross-cloud networking.

Table 1: Priority Matrix for Enterprise Communication Services, 2026

(Enlarged table in Appendix)

Benefit	*Years to Mainstream Adoption*			
	Less Than 2 Years	*2 to 5 Years*	*5 to 10 Years*	*More Than 10 Years*
Transformational	SASE Sovereign Cloud	Communications Platform as a Service eSIM	Agentic SMB Service Bundles Industry Edge Integrated Solutions Network Monetization APIs	
High	Managed IoT Connectivity UCaaS	5G Private Mobile Networks AI Security in ECS B2B Self-Service Capabilities LEO Satellite Communication Services MDR Services Rich Communication Services Securing CSP AI/ML Models in Communications Sovereign AI Threat Intelligence in ECS	CSP Edge Cloud Platform CSP Industry Vertical Solutions Machine Customers in Telecom VNFaaS	6G
Moderate	Contact Center as a Service CSP Data Monetization CSP Digital Marketplaces Dedicated Internet Access Graphics Processing Unit as a Service Managed SD-WAN Services ZTNA	Alternative WAN Backbone Services (XBaaS) Cross-Cloud Networking LEO D2D Services	CSP Superapps CSP XLAs Digital Twins of Telecom Networks	
Low		NaaS		

Source: Gartner (July 2026)

On the Rise

CSP XLAs

Analysis By: Amol Nerlekar, Susan Welsh

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Communications service provider (CSP) experience-level agreements (XLAs) measure quality and effectiveness of services, applications and supporting processes. CSP XLAs leverage a combination of digital experience monitoring (DEM), sentiment analysis and service-level metrics to drive better end-user services, outcomes and application-level experience. They aim to address evolving B2B needs for enhanced service performance as organizations increase cloud adoption.

Why This Is Important

The interconnected services and systems of CSPs are often assessed against technical and performance metrics using agreed service-level agreements (SLAs) provided to customers. XLAs, offered in conjunction with or as a replacement of SLAs, allow CSPs to measure and provide observability on end-to-end digital user experiences. In addition to covering technical metrics, XLAs focus on positive user experiences that offer competitive differentiation.

Business Impact

XLAs differentiate CSPs' services from competitors' by helping define, meet and demonstrate achievement of evolving customer requirements for enhanced experiences and outcomes across different services, applications and support options. The enhanced experiences also improve customer satisfaction, loyalty and customer lifetime value (CLV). By setting and monitoring measures for XLAs, CSPs can detect areas for improvement and service optimization, make decisions, and take corrective actions.

Drivers

- **Service quality and customer experience:** CSPs must enhance service quality and customer experience as client expectations evolve. Traditional IT or network performance metrics miss the true end-user experience, focusing only on technical aspects rather than how users actually feel about the service. For instance, a system may be technically available, but slow logins and high inconsistent response times can still frustrate users, even if SLAs aren't breached. XLAs address this gap by measuring outcomes like user satisfaction and ease of use.
- **Business outcomes:** As CSPs prioritize business outcomes for B2B customers, enterprises need performance measures based on business results captured throughout the user journey. This is likely to drive XLA adoption. While some IT service management companies now offer XLAs, most CSPs have not yet adopted them, though some offer application-level quality of experience (QOE) measures.
- **Demand for executive-level visibility and metrics:** XLAs deliver more executive-level metrics that can help CSPs bridge the gap between the intended business performance improvements and the services that are delivered and measured. XLAs enable IT systems, networks and services to be mapped directly to business KPIs, allowing the creation of service deals that contract for defined business outcomes. XLAs deliver more executive-level metrics like productivity improvement, Net Promoter Score, etc.
- **Technical feasibility:** XLAs are now more feasible, as the state of monitoring and management technology has evolved. B2B customers are increasingly seeing the use of XLAs in IT services. These customers may begin to expect XLAs from their CSPs as well, to ensure a positive employee experience with the CSP-provided services.
- **Optimization and AIOps:** Data-driven decision making requires XLAs to detect areas of improvement and optimize services. AI adoption in BSS systems to advance customer-centricity and enhance customer journeys enables implementing XLAs. XLAs will also support the progression of AIOps over time.

Obstacles

- **Measurement and risk management:** Because good experience is subjective and varies widely, XLAs must be flexible and customizable, which makes them harder to scale and manage. CSPs should also combine qualitative and quantitative metrics and track all user touchpoints to capture the complete user journey.

- **Cultural shift:** Adopting XLAs requires CSPs to shift their focus from technical metrics to user experience. Vendors rarely highlight the workplace changes needed for better UX, and network teams are typically trained to prioritize system uptime over user satisfaction or productivity.
- **Data management:** XLAs need data from multiple sources like analytics, surveys and sentiment analysis, but CSPs often find it challenging to create a comprehensive data view to support them.
- **Cost and time to implement:** CSPs would need to invest in more D&A tools and UX research to support XLAs, increasing both costs and implementation time.
- **Monitoring environment:** XLA analytics often need multiple dashboards, but customers usually prefer a single, unified monitoring platform (either their own or one from CSP partners).
- **Financial risk:** XLAs are harder for CSPs to consistently meet, and if they become binding, they can lead to service credits, lost revenue and extra strain on CSP teams.

User Recommendations

- Identify and implement the right tools to gather the needed data, working with partners that have a strong track record in process mapping, analytics and digital experience monitoring.
- Establish a baseline of customer sentiment by correlating existing network KPIs (latency, throughput) with qualitative data, such as Net Promoter Score, to understand exactly how technical thresholds translate into user frustration.
- Start with relatively simple, proactive XLAs by working with leading customers to explore which experience measurements matter to them. Define methods and metrics to measure and track XLAs and improve actionable insights.
- Assess the risk potential of offering such XLAs as commitments.
- Configure XLAs that measure end-to-end user experience. Focus on an initial list of parameters that are meaningful measurements of experience (for a range of users) and can be compiled for each customer. This approach avoids creating detailed, custom XLAs for each customer and helps you manage XLAs and control risks.

Gartner Recommended Reading

Infographic: The Five Essential Components of an XLA

Establishing XLAs When Engaging With IT Service Providers

Industry Edge Integrated Solutions

Analysis By: Pablo Arriandiaga, Enrique Hernandez-Valencia

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Industry edge integrated solutions are whole-product offerings that address business outcomes across specific verticals by combining on-premises infrastructure, platforms, applications and services with packaged business capabilities (PBCs) for edge environments. Leveraging industry marketplaces, PBC libraries and composition tools, these solutions overcome latency and security hurdles to address industrial AI challenges such as IT/OT convergence, reliability, autonomy and cost optimization.

Why This Is Important

Generic horizontal edge services fail to deliver industry-specific outcomes. Scaling industrial AI across diverse operational environments requires bridging siloed IT, operational technology (OT) architectures, IoT and local data sources. To avoid custom technical debt, enterprises demand tailored, vertically integrated edge solutions bundling infrastructure with PBCs to ensure low latency, security and data sovereignty for real-time analytics and process optimization.

Business Impact

Industry edge integrated solutions:

- Accelerate ROI and shift buyer engagement toward high-value, outcome-based implementations by deploying industry-tailored packaged business capabilities.
- Simplify complex technology integrations — combining edge computing with other technologies such as industrial AI, private 5G and IoT — across diverse IT and OT environments.
- Enable real-time optimization for physical environments, powering use cases such as autonomous operations, predictive maintenance and smart check-outs.

Drivers

- Edge computing is part of a broader digitalization ecosystem evolving toward extensible platforms that utilize PBCs to enable specific industry scenarios. Processing high-frequency telemetry data locally directly addresses “data gravity,” drastically reducing cloud egress and bandwidth costs while guaranteeing the ultralow latency required to rapidly scale industrial AI.
- The convergence of IT and OT demands preintegrated solutions that bridge historical silos and modernize legacy “brownfield” facilities. This unified architecture reduces the complexity of deploying edge computing alongside IoT, computer vision or autonomous systems. Ultimately, it guarantees critical business continuity, enhances personnel safety and transforms customer experiences during intermittent cloud connectivity.
- Buyers prioritize vendors who align edge architectures directly with vertical-specific capabilities, metrics and KPIs to demonstrate quantifiable ROI. This accelerates the shift toward vertically integrated solutions and acts as a catalyst for product servitization, allowing industrial OEMs to shift from capital expenditure (capex) hardware sales to outcome-based or recurring operational expenditure (opex) services.
- Integrated solutions accelerate enterprises’ time to market and agility by eliminating integration errors commonly encountered in previous general-purpose IIoT deployments. By shifting to vertically tailored architectures, these solutions deliver immediate economies of scale in deployment times and ROI, while addressing strict data residency and sovereignty regulations.
- A diverse mix of technology providers — including hyperscalers, communications service providers, system integrators, network equipment providers and OT specialists — actively promote these solutions. By collaborating within broader ecosystems, vendors orchestrate horizontal, vertical and industrial AI synergies to solve complex security challenges.

Obstacles

- The enterprise edge is highly distributed across thousands of sites, often constrained by limited physical space, power availability and intermittent network connectivity. Managing this scale requires skilled staff and dependable orchestration capabilities that take time to mature.
- Industry-vertical edge ecosystems remain immature, lacking common architectures. This risks creating siloed, vendor-specific implementations that increase vendor lock-in and require significant upfront capital and ongoing opex to maintain. Furthermore, deployments are complex and require specialized development frameworks and tools to optimize performance, resilience and industrial AI workloads.
- Integrating modern edge architectures with legacy OT and proprietary protocols introduces significant technical and cultural hurdles. Furthermore, managing diverse, heterogeneous edge devices complicates data governance and security, expands the attack surface and makes consistent policy enforcement difficult.

User Recommendations

- Identify the most viable edge computing use cases by mapping essential technical capabilities and potential adoption challenges directly to targeted business outcomes.
- Evaluate prospective edge architectures and integrated solutions by assessing their ability to meet specific data processing needs, ultralow latency requirements and stringent industry privacy regulations.
- Overcome the complexities of integrated edge deployments by engaging ecosystem partners to share best practices and establishing a cross-functional digital edge fusion team to bridge the critical IT and OT skills gap.
- Safely scale industrial AI inferencing and adapt to data drift by implementing a robust, end-to-end data management and security strategy built on a modular, extensible architecture that avoids vendor lock-in.

Sample Vendors

ABB; Barbara; Ericsson; Hewlett Packard Enterprise (HPE); Microsoft; Nokia; NTT DATA; Schneider Electric; Siemens; Verizon

Gartner Recommended Reading

Innovation Insight: Cross-Industry Edge Computing Solutions Unveiled

Innovation Insight: Industry Edge Enhances Manufacturing Excellence

Innovation Insight: Industry Edge Enhances Government Transformation

Innovation Insight: Industry Edge in Transportation and Automotive

Innovation Insight: Industry Edge Computing Enhances Retail Transformation

Innovation Insight: Industry Edge Enhances Power and Utilities Performance

Innovation Insight: Edge Computing Enhances Healthcare Provider Efficiency

Innovation Insight: Healthcare Industry Data Fabric Accelerates Innovation

Innovation Insight: Industry Edge Enhances Productivity in Communications and Media

Market Guide for Edge Computing

Market Guide for Edge Computing Platforms

6G

Analysis By: Kosei Takiishi

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

6G is the next generation of cellular technology after 5G, currently studied under ITU-R IMT-2030 and early 3GPP activities. Although not fully defined as of 2026, early commercialization is expected around 2029 by leading communications service providers (CSPs). 6G targets AI-native, sensing-enabled networks with near-terabit-per-second peak data rates, sub-millisecond latency, improved energy efficiency, and ubiquitous coverage enabled by integrated nonterrestrial networks.

Why This Is Important

- Beyond greater speeds and higher efficiency, 6G plans to improve 5G by supporting new capabilities that facilitate multitechnology integration and use cases, and learning from 5G commercial experiences.
- The proliferation of agentic and physical AI systems shifts connectivity requirements toward network-native intelligence, integrated sensing and deterministic ultra-low latency that exceed the architectural limits of 5G.
- 6G aims at enabling distributed AI inference and agentic workflows at the network edge, allowing autonomous systems, robotics and real-time digital-physical convergence to operate reliably beyond centralized cloud or best-effort connectivity models.

Business Impact

6G will enable new categories of services built around persistent AI agents, real-time digital-physical fusion, and wide-area sensing. Enterprises can expect more deterministic connectivity for immersive collaboration, autonomous operations, and mission-critical systems. For CSPs, 6G shifts the value proposition from connectivity alone toward AI-driven platforms combining communications, compute and sensing.

Drivers

- **Government and policy momentum:** National and regional governments increasingly view 6G as a long-term strategic infrastructure priority. Across major economies, public policies have emerged that emphasize spectrum planning, early standards engagement, and sustained public funding for 6G research and development. Regions including North America, Europe, and Asia/Pacific — encompassing countries such as China, South Korea, Japan and India — are advancing national or coordinated 6G initiatives to shape future wireless leadership and ecosystem positioning.
- **Standardization progress:** 3GPP held its first TSG-wide 6G workshop in March 2025 and confirmed that Release 20 will focus on 6G studies, with normative specification work expected from Release 21 (starting around 2027). This provides the first concrete industry timeline toward IMT-2030 submissions and early implementations.
- **AI-native network vision:** Industry consensus has strengthened around 6G being designed as an AI-native system. Major vendors and hyperscalers now position 6G around three pillars: connectivity, wide-area sensing, and high-performance compute. Announcements at MWC 2026 highlighted early prototypes and coalition-based roadmaps targeting commercial readiness from 2029 onward.
- **Ecosystem and investment dynamics:** Vendors, CSPs and semiconductor companies are accelerating 6G research to secure future intellectual property and ecosystem influence. Early lab validations in cmWave spectrum and AI-RAN architectures indicate a shift from exploratory research toward proof-of-concept systems.

Obstacles

- **Unproven monetization beyond 5G:** Persistent challenges in turning 5G capabilities into new revenue streams raise concerns about whether 6G will deliver sufficiently differentiated, scalable business value. New use cases enabled by 6G such as immersive XR and holographic telepresence might not result in additional monetization opportunities for CSPs.
- **Ecosystem influence risk:** The mobile industry has historically controlled its own specifications and standardization through tightly defined telecom-centric processes. While 6G discussions increasingly involve players from AI, cloud and vertical industries, it remains unclear whether these external perspectives will meaningfully influence requirements and architecture, or whether 6G standardization will continue to be driven primarily by traditional telecom priorities.
- **Risk of overcomplexity and delayed adoption:** Expanding the scope of 6G beyond connectivity — into sensing, compute, and intelligence — implies a pivot in the scope of the mobile services specifications, increasing standardization, deployment, and regulatory complexity.

User Recommendations

- Monitor discussion of the currently emerging 6G landscape carefully by tracking 3GPP working groups, requirement studies and emerging use cases. Active participation in these is essential if you want to lead critical technology for future 6G services.
- Prepare early trials and proofs of concept in the late 2020s with vendors to learn more about the capabilities of 6G, the required infrastructure and operation changes, and early use cases. Then, begin building skill sets.
- Collaborate with policymakers and regulators to influence spectrum strategy and standards alignment well ahead of commercialization.

Sample Vendors

Ericsson; Huawei; Nokia; NTT DOCOMO; Qualcomm; Samsung; SK Telecom

Gartner Recommended Reading

Emerging Tech Impact Radar: Communications

Market Trend: 6G AI-Native Networks, Use Cases and Spectrum Progress

CSP Edge Cloud Platform

Analysis By: Enrique Hernandez-Valencia

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

CSP edge cloud platforms integrate compute, storage and communications capabilities within the last miles of the CSP network to deliver digital services that leverage the CSP's network footprint and operational assets. They act as a service broker over multiple clouds, fixed/5G access and other telecom layers, and encompass capabilities for real-time and reliable distributed workloads, including elements of settlement, orchestration and placement of edge workloads across different locations.

Why This Is Important

Enterprise digitalization and AI are opening new business opportunities. CSPs can play a unique role in integrating communications and operational workloads, acting as essential service brokers that enable intelligent enterprise digitalization. This is critical for the monetization of 5G investments beyond basic connectivity, leveraging enterprise's techno/data sovereignty needs and repositioning themselves as they increasingly compete and partner with hyperscalers and system integrators (SIs).

Business Impact

- Adjacent value-added services such as critical compute and AI inferencing provide new business opportunities and revenue streams.
- These platforms leverage enterprise digital transformation and CSP assets to deliver cost-efficient, proximity-driven and highly reliable capabilities as an entry point into the enterprise AI infrastructure stack.
- They enable edge federation, delivering carrier-grade connectivity for edge-to-cloud offerings that require seamless handoffs between different CSPs, SIs or hyperscaler cloud providers.
- Edge cloud is the CSP entry point into the AI infrastructure stack. Without it, CSPs risk being relegated to pure connectivity pipes as AI workloads proliferate.
- Edge computers are increasingly sold as a component of private 5G PMN deals rather than stand-alone. It raises deals' average contract value (ACV) and stickiness.

Drivers

- **IT provider ambitions:** Many CSPs have the ambition to diversify revenue streams into adjacent IT services. CSP edge cloud platforms address critical infrastructure for enterprises such as high-performance computing and AI inferencing, targeting the industrywide trend toward real-time intelligence, digitalization, resiliency and industrial automation.
- **Leveraging network assets:** CSP edge cloud platforms leverage edge computing functionality used by CSPs to build the infrastructure and architecture of public 5G networks to deliver new edge services for consumers and enterprises, reducing both startup cost and total cost of ownership (TCO) for delivering edge services.
- **Enabling industrial digitalization:** Digitalization by industries requires high-performance infrastructure. The improved deterministic latency and performance of 5G networks combined with compute infrastructure deployed at the network edge make a compelling proposal by telcos. IoT devices are proliferating and generating massive amounts of data that need to be processed closer to the edge, creating new business opportunities for CSPs.
- **The rise of edge AI inferencing:** AI is moving to the enterprise edge as businesses leverage AI/ML-driven analytics for their digital transformation and data-driven decision making, creating demand for AI-enabled edge compute solutions.
- **Moving beyond IPTV content:** Content delivery networks (CDNs) are adding intelligent processing and improved proxy capabilities. These networking adjacent capabilities to both connectivity and residential IPTV services are motivating CSPs to consider whether the CDN business is becoming more valuable and should be reentered. Edge cloud gives them a way to test this opportunity without a heavy investment. Enterprise edge initiatives require an integrated approach for multiaccess compute interworking — such as edge federation. CSPs have assets in this domain that can be leveraged by CSP edge platforms — and relationships with SDOs to promote alignment to industry initiatives, such as the GSMA Operator Platform Group.
- **Addressing enterprise techno and data sovereignty:** Geopolitical tensions and stringent data residency regulations are forcing enterprises to process sensitive data locally, driving demand for sovereign, CSP-managed edge platforms over global public clouds.

Obstacles

- **Buyer readiness:** Most enterprise edge computing deployments are on-premises. Moving real-time applications to edge requires modifications to prevailing on-premises deployment models, something that most enterprises need help to undertake.
- **Increased operational complexity:** Managing thousands of distributed micro data centers is expensive. Many CSPs underestimate operating expenditure (opex) for edge life cycle management, security patching and hardware refresh.
- **Adopting cloud-like market strategies:** Developing effective go-to-market strategies for edge offerings, pricing and cloud-like business models requires CSPs to move beyond their comfort zone of basic connectivity, demanding significant changes to enterprise operating models.
- **Fierce competition from hyperscalers** (e.g., AWS Local Zones and AWS Outposts, Google Distributed Cloud, Microsoft Azure Local): Public cloud players are leveraging existing enterprise relationships and expanding their extensive service portfolio to the edge, raising the bar for edge capabilities, fragmenting the edge market, and hindering the critical mass needed for CSP platforms to mature.
- **Pace of technology change:** Key enabling capabilities, such as dynamic workload placement and edge federation, remain immature and lack the standardization necessary to drive widespread multioperator interoperability.

User Recommendations

- Create a roadmap that initially leverages enterprise needs for real-time and reliable compute and networking and the distributed communications assets.
- Expand from supporting CSP differentiators such as breadth of edge locations and networking to supporting roaming orchestration, steering, termination and settlement across multicloud, application workloads and slices.
- Implement asset management, provisioning and orchestration at scale at the 5G edge(s), including hybrid, public and private scenarios, by harmonizing the tooling for service orchestration, telemetry and assurance.
- Promote standardization and open APIs for undifferentiated capabilities in areas such as roaming and cross-settlement in organizations such as TM Forum, ETSI and GSMA to facilitate integration and ecosystem expansion.
- Factor into the business case the channel opportunities, such as resale, operations and support of hyperscaler edge cloud platform offerings.
- Collaborate with technology vendors, hyperscalers and application developers to identify the right business strategy (e.g., insource vs. outsource vs. joint venture) to build a robust edge ecosystem.
- Address the skills gap by investing in training and development programs to upskill the workforce in edge computing and AI cloud-native technologies.

Gartner Recommended Reading

Emerging Technologies: Revenue Opportunity Projection for Edge Computing

CSP Data Monetization

Analysis By: Kameron Chao, Susan Welsh

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

CSP data monetization is the practice of realizing net-new measurable and tangible economic benefits from data, combined with business models and techniques beyond standard connectivity products. It involves data, analytics and AI capabilities, ranging from identifying appropriate data to developing and marketing solutions of value to customers. Data monetization offers cross-industry collaboration opportunities for CSPs to many industries, such as finance, retail and healthcare.

Why This Is Important

Leveraging customer data under privacy compliance enables CSPs to grow beyond connectivity. Many have invested in data management and analytics, expanding monetization portfolios and using privacy-by-design and transparent governance to build trust. Data monetization will gain momentum over the next two years as CSPs develop new revenue streams, with 5G SA as a key enabler, supporting advanced use cases, real-time analytics and network slicing for tailored, high-value services.

Business Impact

CSPs amass vast data across networks, OSSs and BSSs. Addressing operational tech issues and structuring data management unlocks revenue and new business models. CSPs targeting sectors such as banking, retail and insurance with ecosystem approaches are better positioned for external data monetization. Embedding privacy-by-design and targeted governance reduces risk, supports premium pricing and boosts brand equity.

Drivers

- CSPs seeking more value amid flat core revenue increasingly view anonymized customer data as a monetizable asset. Leveraging aggregated and anonymized data unlocks new revenue streams while ensuring privacy compliance and trust.
- CSPs are exploring the economic potential of their data repositories. Treating data as an enterprise asset is now critical, requiring trust-based sharing across internal and external sources for collaborative and innovative monetization.
- Internal digital transformation in customer engagement is advancing rapidly in CSPs, outpacing other industries. This expertise can be packaged as value-added services for B2B clients, offering advanced analytics and customer insights.
- The growth of location-based service ecosystems, powered by 5G and analytics, creates new opportunities. Monetizing movement and traffic patterns supports industries like retail, transport and urban planning.
- Network APIs are key enablers, allowing CSPs to expose network capabilities to partners, developers and third-party ecosystems, facilitating innovative services and business models such as real-time connectivity and IoT enablement.
- Use cases are growing for personalized marketing and product bundling such as advertising, credit scoring and providing industries with population, location and consumption insights. Leading CSPs include Globe, Orange, Fundación Telefónica and Vodafone.
- CSPs leverage internal sales and buyer data to drive cross-sell and upsell, optimizing customer value and strengthening their position.
- Regulatory and competitive pressures from GDPR, CCPA, hyperscalers and OTTs are pushing CSPs to unlock new revenue streams, making compliance a catalyst for innovation, not just a constraint.

Obstacles

- Data protection legislation is maturing, requiring enterprises to address ethical implications of dataset use, sharing and privacy to maintain trust and comply with regulations.
- CSPs must create new business models for data monetization as they divest assets generating customer data insights, such as streaming and OTT.
- Internal misalignment prevents connecting use case experts with those who know where to find the right data.
- Data silos and lack of adaptive governance aligned to monetization goals are obstacles.
- Few vendors offer prepackaged solutions to accelerate CSP monetization initiatives.
- Legacy IT/networking integration, such as monolithic OSS/BSS stacks and proprietary interfaces, complicates real-time data streaming and enrichment.
- Consent management and opt-in/opt-out challenges make it harder to ensure compliance and user trust in data monetization.

User Recommendations

- Align data monetization with business strategy, targeting key market segments and reflecting organizational maturity.
- Evaluate and prioritize opportunities by assessing current technology, ecosystem potential and compliance with security and privacy regulations.
- Establish a proactive privacy and ethics framework with analytics, security and operations leaders. Develop robust consent management to protect user privacy.
- Design monetization platforms with advanced analytics, collaboration and BSS modernization for better integration.
- Develop a strategic roadmap for data monetization, focusing on data management, analytics, product life cycle, real-time support, security and partnerships.
- Ensure regulatory reporting and audit readiness with automated workflows and audit logs for compliance.
- Monetize aggregated and anonymized data, not raw subscriber data. A marketplace can be an effective choice for secure, compliant data monetization.

Sample Vendors

Amazon Web Services; Amdocs; Comviva; Google; IBM; Intersec; Netcracker; Oracle; Salesforce; Virtusa

Gartner Recommended Reading

Market Trend: CSPs Embrace Data Monetization With Location Intelligence

Industry Case Studies for CIOs Supporting D&A and AI Initiatives

Research Roundup for State of Data and Analytics for CSPs

Essential Steps and Enabling Practices to Monetize Data

Toolkit: How to Get Started With Data Monetization

At the Peak

Cross-Cloud Networking

Analysis By: Jonathan Forest, Simon Richard

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cross-cloud networking (CCN) is an offering or feature explicitly designed to connect multiple public clouds with each other. CCN offerings aim to simplify cloud-to-cloud connectivity and reduce provisioning time compared with alternative legacy and do-it-yourself (DIY) methods. The service can be delivered by a third-party provider offering software defined cloud interconnect (SDCI) or by cloud provider offerings such as AWS Interconnect - multicloud or Google Cross-Cloud Interconnect.

Why This Is Important

AI is driving increased traffic, applications are more distributed across clouds, and organizations are seeking resilience against cloud outages. While there are DIY ways to support cloud-to-cloud traffic, CCN simplifies network connectivity using third-party service providers or directly with a cloud provider. Google's Cross-Cloud Interconnect was an early entry, and AWS has introduced Interconnect - multicloud, providing an open API standards-based connectivity from AWS to other clouds.

Business Impact

CCN offers simpler, faster, and more agile cloud-to-cloud network connectivity. The various options simplify organizations' ability to architect and provision intercloud connectivity compared with legacy and DIY options. This includes simplifying billing across cloud providers using SDCI as a third-party provider. It also limits the need for third-party vendors where Google Cross-Cloud Interconnect or AWS Interconnect - multicloud offer a solution delivered directly by cloud providers.

Drivers

- AWS Interconnect - multicloud with launch partner Google Cloud Platform marks the first time that there is a structured way for cloud providers to work directly together offering simplicity, rapid provisioning times, and agility for customers.

- There is increased AI-related cloud-to-cloud traffic where data residency is in one cloud and large language models (LLMs) are in another. Processes such as retrieval-augmented generation drive this increased traffic pattern.
- There is a desire for non-network teams to provision connectivity between clouds on demand, without needing deep knowledge from the network teams.
- There is a preference to use a third party to manage billing and network environments across cloud providers.
- CloudOps increasingly manages cloud networking within a single cloud provider, and this would extend that concept across multiple providers.
- There is an increased concern of cloud outages due to recent events, so there is less reliance on a cloud provider.

Obstacles

- AWS Interconnect - multicloud is newly launched, and other cloud providers still need time to develop their capabilities.
- Cloud-to-cloud traffic is nascent, as most traffic flows are between users and workloads in the cloud. Over time, there is also the risk of elevated egress costs when connecting between clouds.
- With the AWS interconnect - multicloud, customers have to work with each cloud provider and pay that cloud provider directly.
- SDCI vendors introduce a third party to manage all cloud connectivity. Customers, in general, are looking to reduce the number of vendors they work with.
- There is potential resistance from highly skilled DIY network teams who typically architect, implement, and operate connectivity end to end.
- There is the potential loss of network visibility with cloud provider solutions, which could require additional tooling.

User Recommendations

- When using CCN, establish governance to control which roles have the ability to provision or use cloud-to-cloud connectivity services.
- Leverage AWS Interconnect - multicloud if your organization relies primarily on AWS but wants to directly connect to GCP (and soon other clouds).

- Leverage SDCI where a third-party cloud-to-cloud provider is desired to manage the overall service and provide a single bill.
- Leverage Google Cross-Cloud Interconnect if your organization relies primarily on Google Cloud Platform but wants to directly connect to other clouds with management support.
- Track new cloud provider integrations with AWS Interconnect - multicloud.
- For DIY organizations, route cloud-to-cloud traffic through infrastructure deployed at a colocation facility. This is effectively still hairpinning, but it avoids the latency of bringing traffic back on-premises.

Sample Vendors

Alkira; Amazon Web Services; AT&T; BT Group; Console Connect; Equinix; Google Cloud Platform; Megaport; Orange Business; Tata Communications

Gartner Recommended Reading

AWS Unveils New Multicloud Connectivity Strategy: Advantages & Cautions

Machine Customers in Telecom

Analysis By: Susan Welsh, Khurram Shahzad

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Machine customers are nonhuman economic actors that obtain goods or services in exchange for payment. Examples of machine customers include AI agents, generative AI chatbots, smart appliances, connected cars and Internet of Things (IoT)-enabled factory equipment. Machine customers act on behalf of a human customer or an organization.

Why This Is Important

Machine customers are emerging as autonomous buyers of communication services that evaluate, procure and switch services in real time based on cost, performance, risk and intent. As AI agents and connected systems augment and ultimately replace humans in procurement loops, CSPs risk becoming invisible unless their networks, products and assurance models are programmable, machine readable, API driven and support high-frequency, autonomous transactions.

Business Impact

Machine customers fundamentally change how telecom services are consumed and monetized. They replace long-term, human-led contracts with high-frequency, outcome-driven transactions and micropurchases. This shifts revenue patterns, accelerates competition to milliseconds, increases volatility and creates new growth opportunities for CSPs that can support programmable, agent-first engagement models. CSPs that successfully integrate into agent-driven ecosystems will secure a sustainable competitive advantage in the evolving telecom landscape.

Drivers

- **Rise of agentic AI in procurement and machine customers:** Gartner predicts a shift from human-led buying to AI-based nonhuman actors that evaluate, negotiate, purchase and modify services in real time based on intent, cost and performance. Enterprises will increasingly delegate sourcing, negotiation and optimization of network services to autonomous AI agents acting without continuous human supervision.
- **Programmable connectivity as a competitive differentiator:** CSPs exposing intent-based APIs, real-time telemetry and automated provisioning are more likely to be selected by autonomous agents acting on behalf of enterprises.
- **Intent-based buying behavior:** Autonomous buyers are likely to prioritize business outcomes such as guaranteed latency, resilience, compliance or sustainability over traditional product tiers.
- **Growth of FinOps and optimization agents:** Cost-optimization, utilization and performance-balancing agents will be able to continuously reassess providers and shift demand dynamically, increasing pricing pressure and reducing long-term demand predictability for CSPs.
- **Emergence of monetization models and contracts tailored to machine customers:** Microtransactions, real-time dynamic pricing and machine wallets enable high-velocity, low-value purchases at massive scale. Machine customers may favor short-duration, usage-based “snacking” models aligned to real-time needs and dynamic consumption patterns rather than fixed-term agreements.
- **Expansion of physical AI and IoT:** Autonomous vehicles, robots, factories, drones and devices increasingly self-select, activate and scale connectivity services without human intervention.
- **Increased adoption of protocols, APIs and agent identity management:** Protocols such as Model Context Protocol (MCP), Agent-to-Agent (A2A) Protocol (Google), Universal Commerce Protocol (UCP), OpenAI ACP (Agent Commerce Protocol), Agent Payments Protocols (AP2), along with APIs for AI agent use and AI agent identity tools further enable machine-customer transactions.

Obstacles

- **Legacy OSS/BSS constraints:** Human-centric, batch-based systems lack the real-time responsiveness required for autonomous purchasing and modification.
- **Lack of intent-based APIs and autonomous enablement:** Machine customers require real-time, intent-based and event-driven interactions with end-to-end automation to support high-frequency transactions, which is currently not supported by the majority of CSPs.
- **Limited machine readiness of products:** Machine customers require a fundamental deconstruction of the traditional CSP product catalogs into composable, machine-readable components discoverable by AI agents.
- **Organizational misalignment:** Sales, GTM, support, legal and contract management, security, billing and revenue assurance and regulatory and compliance functions remain optimized for relationship-led engagement instead of algorithmic buyers.
- **Governance, risk and trust gaps:** CSPs struggle to balance autonomous decisioning with financial guardrails, security, compliance and accountability.

User Recommendations

- **Develop strategic positioning and portfolio assessment:** Define your CSP's evolving role in the machine economy value chain and evaluate your portfolio to identify capabilities and products best suited for autonomous consumption.
- **Adopt an agent-first mindset:** Expose network capabilities through intent-based APIs, real-time telemetry and machine-readable product catalogs. Deconstruct product bundles into composable services supporting algorithmic pricing, microtransactions and outcome-based models.
- **Design intent-based, automated offerings:** Productize high-frequency, low-duration services with automated provisioning and intent-based logic to provide AI agents with dynamic configuration suggestions based on stated goals rather than static catalogs.
- **Modernize OSS/BSS and operations:** Enable event-driven, autonomous provisioning, assurance and settlement at machine speed.
- **Evolve GTM and governance:** Build an autonomous GTM layer, policy-as-code controls and safe human-in-the-loop mechanisms for high-impact actions.

Gartner Recommended Reading

AI Vendor Race: Prepare Enterprise Network Services for Machine Customers, or Lose to Competitors Who Have

Is Your Network Ready for Autonomous Machine Customers?

Forecast Analysis: Enterprise IoT-Enabled Machine Customers, Worldwide

Emerging Tech: Use Machine Customers to Break Through Barriers to Innovation

Agentic SMB Service Bundles

Analysis By: Pablo Arriandiaga, Khurram Shahzad

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Agentic small and midsize business (SMB) service bundles are a CSP AI-driven service-packaging strategy that mixes connectivity, IT services, and third-party applications like security, productivity, business intelligence and data analytics, customer engagement, or accounting. Agentic SMB service bundles offer flexibility to SMB buyers to compose solutions tailored to their needs or their industry and make contracting and fulfillment an easy process to improve the customer experience.

Why This Is Important

SMBs represent a key growth opportunity in B2B for communication service providers (CSPs), yet have historically received less focus than large enterprises. Providers are now adopting sophisticated segmentation approaches that go beyond company size, designing AI-driven bundles that combine communications and IT services based on industry or business maturity. By aligning offerings more closely with SMB needs, CSPs deliver solutions that better fit the unique requirements of SMB customers.

Business Impact

- Increases average deal size and customer lifetime value via modular upsell options.
- Accelerates “click to cash” with self-service, tailored digital journeys.
- Enables hyperpersonalized offerings, not rigid packages.
- Boosts customer loyalty and reduces churn.
- Improves Net Promoter Scores in the competitive B2B market.
- Enhances indirect channel SMB enablement with tailored, composable solutions.
- Enables truly dynamic, industry-specific solutions that adapt to evolving SMB needs and market trends.

Drivers

- Agentic AI and multiagent systems (MAS) are driving the shift from manual configure, price, and quote (CPQ) processes to instant, hyperpersonalized solution builders that autonomously assemble optimal product combinations.
- Embedding AI and machine learning into digital engagement and life cycle management allows CSPs to anticipate SMB needs and dynamically adjust offerings, ensuring relevance and value throughout the customer journey.
- The widespread adoption of microservices, API-first, cloud-native, and headless (MACH) architectures enables CSPs to unbundle rigid catalogs into reusable, granular packaged business capabilities (PBCs).
- SMBs increasingly demand flexible, outcome-based integrated communications and technology services (ICTS) — including remote work, cybersecurity, and cloud solutions — making static connectivity bundles obsolete.
- Growing competition from digital-native providers and hyperscalers is compelling CSPs to evolve into platform businesses capable of rapidly orchestrating and monetizing dynamic partner ecosystems.
- The shift to SaaS has democratized access to applications for SMBs, making it essential for CSPs to respond with agile, modular bundles that seamlessly integrate connectivity, software, and IT services tailored to each business's stage and sector.
- Differentiation in the SMB market will increasingly depend on the ability to deliver agentic, composable bundles that adapt in real time to customized customer requirements.
- Pairing journey mapping with highly configurable, outcome-driven bundles enables CSPs to maximize returns on digital channel and customer experience investments.
- SaaS disruption of indirect channels enables CSPs to expand reach and enhance partner capabilities by empowering integrators and MSPs with flexible, value-added SMB bundles.
- Integrating communications, IT, and security tools into a single bundle enables SMBs to boost efficiency, collaboration, and business continuity with robust cloud-based services.

Obstacles

- Legacy business support systems (BSS) and operational support systems (OSS) are typically built on tightly coupled, monolithic architectures, hindering the rapid and dynamic creation of new services.
- Fragmented and siloed data environments restrict AI agents' ability to accurately interpret customer intent, assess product suitability, and continuously optimize service combinations.
- Transitioning to outcome-based or volumetric pricing models for composable bundles adds commercial complexity and often conflicts with traditional revenue assurance frameworks.
- Many CSPs still take a technology-first approach to SMBs, offering bundles as catalog items focused on price, not business needs. These solutions often fail to address real SMB challenges or deliver meaningful outcomes.
- Leading networking and IoT MNOs/MVNOs are evolving platforms for composable solutions, often via siloed partners. Large enterprises are prioritized, with SMBs usually targeted in later development phases.

User Recommendations

- Develop agentic SMB service bundles with a phased composability strategy. Start by upgrading service lines, then integrate them to address cross-functional needs like digital workplace and customer experience. Add industry-specific features for vertical markets.
- Implement MACH architecture to transform monolithic product catalogs into discoverable, API-driven microservices that can be dynamically assembled by autonomous systems.
- Deploy specialized AI agents to guide B2B customers through needs assessment, product composition, and automated contracting, delivering frictionless, personalized digital experiences.
- Establish an AI-ready data fabric to unify customer, operational, and network telemetry data, enabling composed products to adapt to changing business demands in real time.
- Adopt outcome-based and consumption-based pricing models that directly align the cost of composable services with the measurable business value delivered to SMBs.

Sample Vendors

Airtel; AT&T; Comcast; Deutsche Telekom; Orange Business; Proximus; Singtel; Softbank; Swisscom; Verizon

Gartner Recommended Reading

AI Vendor Race: Leverage Agentic AI to Create Composable Products for Growth in SMBs

How CSPs Can Achieve Maximum Growth From SMBs in 2025

Market Guide for CSP B2B Digital Marketplace Solutions

Case Study: Align Connectivity, Managed Network and Security Services

2025 Top Trend: Rise of CSP Digital Marketplaces

Digital Twins of Telecom Networks

Analysis By: Will Rice, Pulkit Pandey, Peter Liu

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

A digital twin of a telecom network is a virtual representation of the telecom network, which encapsulates logical data and AI models to emulate real, as well as simulated behavior. These real-time representations are used to improve network performance, asset maintenance, planning, base station information modeling, and other use cases. A digital twin of a telecom network can represent objects like physical network components, a single base station, rack, data center, or an end-to-end network.

Why This Is Important

Digital twins of telecom networks can be leveraged to assess a current situation and run simulation scenarios for planning, testing, and optimizing the network. They can also model scenarios to improve network performance in terms of better customer service/experience or reduced operating costs. Digital twins promise to become a central simulation tool for network planning and performance optimization, aiding human decision making, and enabling validation of AI decisions.

Business Impact

Digital twins of telecom networks:

- Enable communications service providers (CSPs) to enrich and simulate information for decision making.
- Identify network elements with common faults to shorten root cause analysis and even predict failures, as well as informing sourcing tactics toward equipment vendors.
- Optimize processes, such as monitoring, managing, and maintaining the supply chain.
- Support human oversight of AI-driven network operations, optimization, and maintenance.

Drivers

- Digital twins improves with network design, allowing for better network predictions, such as those related to capacity demands, issue resolution, and thus network performance optimization.
- Reduce operational costs through improved asset management, real-time remote monitoring, and predictive maintenance insights.
- Optimize resource allocation and planning through prediction and simulation based on real-time information.
- Increase and speed up experimentation of new business and operating models by enabling impact assessment related to requirements for different use cases, enterprise solutions, as well as validation of AI scenarios and operations.
- As CSPs move toward network-as-a-service (NaaS) models, they must manage multiple virtual networks on a single physical infrastructure. Digital twins provide the visibility needed to allocate resources dynamically and ensure SLAs are met for specific enterprise use cases.
- With rising energy costs, CSPs are under pressure to decarbonize. Digital twins can model power consumption across thousands of sites, allowing for the simulation of integration of renewable energy sources to reduce the carbon footprint.

Obstacles

- A lack of demonstrable value and proven ROI for implementation of CSP network digital twins.
- Legacy systems often house data in incompatible formats across different domains, consolidating into a “single source of truth” can be a massive integration challenge to build a comprehensive, accurate and up-to-date DT.

User Recommendations

- Utilize proven digital twin capabilities from vendors to create and resolve “what-if” scenarios for your network optimization use cases.
- Strengthen the data collection capabilities for inventory management (discovering and reconciling management of physical and logical inventory between OSS and digital twin).
- Engage with business-unit peers to ensure the business case has clear metrics that the technology organization can support.
- Identify IT gaps and build a roadmap to drive organization learning, its investment plan for internal skills and partner selection strategy.
- Take a holistic view of digital twin network planning and implementation. Go beyond digital twins for individual physical objects (e.g., data center racks). Develop holistic models that are seamlessly integrated with the current business architecture to include support for processes and AI-decisions-related network capacity planning (simulation), deployment and life cycle management.

Sample Vendors

BluePlanet (Ciena); Ericsson; Huawei; Keysight; MarlinDT; Netcracker; Nokia; NTT DATA; NVIDIA; Oracle; VIAVI

Gartner Recommended Reading

Magic Quadrant for AI in CSP Customer and Business Operations

AI Predicts 2026: CSPs Turn AI-First by Necessity, Not Choice — Sovereignty and Security Predefine Success or Failure

Market Guide for AI Offerings in CSP Network Operations

Emerging Tech Impact Radar: CSP Technologies and Services

Assess the Potential of Emerging Technologies for CSPs

Graphics Processing Unit as a Service

Analysis By: Enrique Castera, Chirag Dekate, Jason Donham

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Definition:

Graphics processing unit as a service (GPUaaS) delivers on-demand access to GPU or other AI processors through a public cloud or specialized cloud models. GPUaaS offers elastic, consumption-based access to high-performance GPUs for workloads such as AI training and inference, data engineering, and graphic-intensive applications. This excludes on-premises or private cloud deployment.

Why This Is Important

GPUaaS is increasingly critical as GenAI, high-performance computing (HPC) and real-time inference workloads demand specialized, high-density GPU infrastructure. Most enterprises lack the skills and funding to build GPU-based supercomputing environments. With hyperscalers and neoclouds scaling next-gen GPUs and orchestration tools, enterprises can use GPUaaS to avoid the cost and complexity of building AI-optimized environments while gaining elastic access to advanced compute.

Business Impact

GPUaaS enables infrastructure and operations (I&O) leaders to utilize state-of-the art GPU resources at a fraction of the cost of a capital expenditure (capex) solution, which involves budgeting for the upfront cost of procurement, configuration, maintenance and depreciation. GPUaaS is a consumption-based model that offers access to hardware resources in a pay-as-you-go and highly scalable model. This service is also valuable for organizations that do not have a significant data center footprint to run GPU-dependent applications.

Drivers

- Explosive growth in GenAI, large-scale inference and advanced AI workloads continues to drive unprecedented demand for high-performance GPUs.
- Newer GPU architectures offer significantly lower cost per token for inference and training that enterprises cannot replicate via private hardware. Hyperscalers and neoclouds leverage massive scale to amortize the high capex of these chips.
- Demand for sovereign AI and regulated-market compliance is increasing reliance on GPUaaS providers capable of delivering regionally anchored GPU capacity. Neocloud growth in Europe and globally demonstrates rising demand from AI labs, GenAI-native startups, and research institutions for secure, locality-aligned GPU capacity, with enterprise adoption still emerging.
- Rising adoption of distributed and edge AI is accelerating GPUaaS demand. Low-latency inference, sovereign AI requirements and proximity-based workloads are pushing GPU capacity close to data sources.
- The shift toward full-stack AI platforms further accelerates GPUaaS growth. Enterprises now expect integrated environments that combine high-speed networking, orchestration, inference optimization and AI development tooling, making GPUaaS an enabler of end-to-end AI innovation, rather than a stand-alone compute service.
- Most enterprises lack the skill sets to maintain, manage and deliver GPU supercomputers. GPUaaS delivers integrated orchestration, scheduling, networking and life cycle management tools that simplify operations and improve GPU utilization across workloads.
- Improved availability of next-generation GPUs through hyperscalers and neocloud providers is driving broader enterprise adoption. Hyperscalers plan massive capacity expansions in 2026, making state-of-the-art hardware more accessible via consumption models.

Obstacles

- Even with scale-ups, next-gen GPU instances are available in limited regions, constraining placement and failover options.
- Limited availability of electrical capacity and GPUs, plus high capital costs and long lead times to add new datacenters, mean GPUaaS vendors may lack sufficient capacity to meet customer demands. An extreme undersupply of AI data center capacity has pushed wait times for 10MW+ power in major metros to 24 to 36 months. Grid delays effectively bar enterprises from building large-scale internal clusters near business hubs, forcing a reliance on GPUaaS providers that secured high-density capacity and power interconnections years in advance.
- Spot markets and provider pricing spread make opex forecasting difficult (e.g., H100 rental spikes and large gaps between neoclouds and hyperscalers).
- Differing managed stacks hamper workload portability and raise skills overhead when moving GPUaaS deployments across clouds.
- Many specialized clouds lack hyperscaler-grade networks. Securing high-throughput, multiregion inference may require extra overlay solutions.
- Diversification of hardware for AI, including new AI application-specific integrated circuits (ASICs) and custom chips from hyperscalers, will tighten GPU-only economics, challenging pure GPUaaS sustainability.

User Recommendations

- Default to CSPs for integrated AI stacks, governance, and ecosystems, unless a clear gap in features, prices or availability exists.
- Use neocloud GPUaaS when CSPs can't meet regional capacity/price/sovereignty or edge-latency needs.
- Prioritize elastic consumption options (fractional GPUs, serverless endpoints) to optimize costs for rightsizing inference and bursty demand.
- When comparing GPUaaS and CSPs, focus strategically on the provider's ability to deliver comprehensive AI portfolio comparisons and support your security, integration, skills, risk mitigation, cloud governance and data management requirements, ensuring these align with your long-term strategic goals and operational needs.
- Design for portability and exit through Kubernetes-based deployments and data egress plans; reduce stack lock-in across clouds.

Sample Vendors

Alibaba Cloud; Alphabet; Amazon Web Services (AWS); CoreWeave; Crusoe; Huawei; Lambda; Microsoft; Nebius; Oracle; OVHcloud; RunPod

Gartner Recommended Reading

Market Guide for Specialty Cloud Providers

Sovereign AI

Analysis By: Lydia Clougherty Jones, Mike Fang, Clementine Valayer

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Sovereign AI reflects a nation-state's ambition to develop and use AI without foreign assistance for sovereign objectives, including global AI dominance, global leadership, national security, cybersecurity, cultural preservation and economic competitiveness. As AI becomes key to economic growth, nation-states prioritize controlling their own AI, minimizing reliance on other countries for AI-ready data, operations, technology, talent and infrastructure.

Why This Is Important

Sovereign AI reflects nation-states' investment to develop AI with less foreign assistance, advancing AI adoption for their own use. While sovereign AI could enhance an individual state's military defense, AI use by other nations could undermine those national security efforts. Sovereign AI supports market innovation and growth. Global Sovereign AI Accelerates is a top trend in D&A for 2026. See Top Trends in D&A for 2026: Global Sovereign AI Accelerates.

Business Impact

Sovereign AI is an enterprisewide disruptor for U.S. entities and non-U.S. entities alike, regardless of geographic location, impacting almost all aspects of the data and model foundations required for optimal AI value. Nation-states accelerate sovereign AI through mechanisms such as tariff/trade policy, financial investment, funds appropriation, regulatory/deregulatory action and public/private transactions. Yet, sovereign AI is often confused with regional "x" sovereignty requirements, such as cloud, data, digital, technology, model sovereignty. Conflating sovereign AI with "x" sovereignty requirements leads to missed opportunity and undiagnosed threat.

Drivers

- To increase their competitiveness and safeguard their future, an increasing number of nation states and independent political entities such as the EU are actively planning and building their own AI infrastructure and advanced AI capabilities with less dependence on foreign assistance. Across most global sovereign AI ambitions exists a desire for less dependencies and reliance on foreign entities.
- Known and unknown risks of harms to sovereign objectives and citizen welfare from unintended or irresponsible uses of AI drive sovereign states to increase control over the development of AI systems, and more so over generative AI (GenAI) use cases and artifacts.
- As nation-states advance these ambitions, enterprises are grasping the opportunity by shifting from “geo-agnostic” to “geo-aligned” technology decisions. This in turn furthers nation-state goals, including developing AI in their geographies with less foreign assistance.
- Need for nation-states to self-regulate, including how their data is used to train large language models (LLMs), is growing. For example, nation-states are increasingly using AI tools to make important government decisions, but clients report year over year that these decisions are often outsourced to private companies without public input or oversight. This lack of transparency and accountability drives sovereign states to develop the AI tools themselves to address concerns about unwanted biases and conflicts of interest in these critical decision-making processes.
- Nation-states desire to increase their independence from other nations and the foreign tech market, including to foster economic competitiveness and to remedy underrepresentation of cultural and linguistic inputs.
- Sovereign AI plays an important role in digital sovereignty as it focuses on the sovereign control of AI data and systems, including control over computing capacity, data storage, access to human resources and proprietary knowledge for AI application development. Digital sovereignty also can significantly impact sovereign AI development, with the availability of locally stored data, for example, to train AI models.
- Sovereign AI differs from “x” sovereignty, such as cloud/data/digital/technology/model sovereignty. Its core focus is being the developer and user of AI technologies, not the regulator of them. “x” sovereignty reflects state efforts to regulate data and AI use by its citizens, private industry and its economy.

- Combating threats to political stability from the proliferation of deepfakes can drive nation-states to adopt sovereign AI.
- Upskilling government workers today for a more AI-ready government workforce tomorrow will assist sovereign AI advancement.
- Demand to advance local and national defense, and cybersecurity strategies is increasing.
- Progressing and maintaining leadership in emerging technologies space will accelerate scaling AI.

Obstacles

- Preparation of an AI-ready IT infrastructure.
- Development of an AI-skilled government and private sector workforce.
- Modernization of government culture to embrace advanced analytics and automation.
- Limited capability of already-taxed IT infrastructure and fragmented business networks that would need to serve a sovereign AI system.
- Lack of the right AI-ready data for training LLMs, resulting in AI output with varying levels of utility.
- Lack of technically skilled humans to loop into the AI development and use life cycle, resulting in an increase of unintended negative outcomes from AI use and GenAI artifacts.
- Lack of AI-readiness across people, talent, data management techniques and enabling tools and technologies, impeding nation-states from accelerating AI adoption across government functions.
- Differences in political and cultural values create inconsistent AI-value versus AI-harms analysis, leading to unpredictable impacts on international trade and global markets.
- Legal, regulatory or fiscal policies that can undermine sovereign AI initiatives.
- Development of AI by nation-states across the world leads to a fragmentation and possible contradiction in the requirements for AI solutions, many of which cannot be met by either public or private sector.

User Recommendations

Given the wide variances across sovereign AI innovation to risk ratios, sovereign AI is impacting international relationships, global trade, local public/private partnerships and economic markets in unexpected ways.

As nation-states advance their sovereign AI ambitions, enterprises, regardless of a U.S. or non-U.S. location, must grasp the opportunity to balance sovereign AI restriction with high-value AI use cases. Use A Journey Guide Playbook to Balance Sovereign AI With High-Value AI Use Cases to ensure your organization is on the right path to confront, overcome and monetize the collision of geopolitics and technology, while deploying the most robust data and model foundations in alignment with the highest-value AI use cases, including those impacted by sovereign AI.

Sovereign states, and the vendors with whom they work, seeking a self-governed and controlled approach to the development of AI systems aligned with sovereign strategic objectives should:

- Start small and prioritize AI uses aligned with maximum advancement of their stakeholder and government business goals.
- Build an AI strategic roadmap that progresses from internal use cases to citizen-facing ones.
- Ensure the AI strategy identifies key value opportunities and risks.
- Develop early in the planning process a metric of success and include various metrics within the strategy to track successes and course-correct unwanted impacts.
- Cultivate public-private collaborations that foster and accelerate data and analytics, AI upskilling, technology innovation and adoption.
- Monitor and learn from sovereign AI already underway, including from Sovereign Australia AI, the European Commission, India, the United States, Canada and the United Kingdom.
- Collaborate with friendly sovereign states to accelerate the learning curve, sharing failure analysis and positive narratives of unexpected success.
- Use Gartner's Top Trends in D&A for 2026: Global Sovereign AI Accelerates to guide the nation toward AI development, creating tangible value and achieving competitive national leader status.

Gartner Recommended Reading

A Journey Guide Playbook to Align Sovereign AI With High-Value Use Cases and Agentic AI Workflows

Sovereign AI Series: Checklist for Enterprise AI Strategy With Sovereign AI Ambition

Sovereign AI Series: Define Enterprise Operating Model to Grasp the Sovereign AI Opportunity

Sovereign AI Series: Shift Your AI Gravity to Regional Autonomy

Sovereign AI Series: New U.S. LLM Content Mandates Will Not Slow Global AI Acceleration

How Sovereign AI Impacts Enterprise Opportunity and Creates Nonobvious Threat

5G Private Mobile Networks

Analysis By: Sylvain Fabre

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

5G private mobile networks (PMNs) provide mobile services specifically and exclusively to an enterprise or public organization and are based on the 3rd Generation Partnership Project (3GPP) R15 or above. A PMN is used to provide unified connectivity, optimized services and security to interconnect people and things for an enterprise. Deployments can be local or linked to a public network.

Why This Is Important

The importance of 5G private mobile networks lies in giving organizations direct control over wireless performance, security and economics where shared public networks or Wi-Fi cannot reliably meet operational requirements. It can also optimize connectivity costs for large areas; 5G requires far fewer radio nodes than Wi-Fi, which drastically reduces the expense of hardware and cabling.

Business Impact

5G PMN enables transformational use cases (e.g., factory digital twins, edge AI, and computer vision). Unlike 4G, 5G delivers strict deterministic connectivity, guaranteeing sub-20ms latency and massive uplink throughput for critical OT. It offers improved reliability, security and independence, supporting high-density endpoint connections with absolute performance guarantees to drive efficiency gains in automated industrial environments. 5G PMN is the enterprise's own infrastructure, with limited outside dependency. In practice, the business impact of 5G PMNs is highest in asset-intensive and mission-critical environments, and significantly lower where connectivity requirements can already be met with simpler alternatives.

Drivers

- Practical applications and vertical-specific integration are increasing. Beyond 3GPP, other bodies are now contributing, such as 5G Alliance for Connected Industries and Automation and 5G Automotive Association.
- Liberalization of the radio spectrum has opened up standard radio bands, often around 3.5 GHz, for use by 5G PMN networks.
- The requirement for full, reliable network coverage for machines, sensors and equipment, including indoor, outdoor, office and large industrial areas, at a lower cost than Wi-Fi, is a driver.
- Bridge to edge computing: 5G's deterministic high-bandwidth and low-latency profile supports embedding edge AI and compute for demanding industrial use cases.
- Shift to NaaS and OpEx: Vendors and SIs now offer flexible, OpEx-based network-as-a-service models, drastically lowering upfront CapEx barriers.
- Some enterprises in specific verticals or those adopting specific use cases deploy private networks because they want to run their network more independently, as their own infrastructure, with limited outside dependency, such as long-term commitment from public network operators.
- Data sovereignty: Strict physical and logical isolation ensures sensitive data remains on-premises, giving defense and regulated clients absolute control.
- Network slicing for strict SLAs: Slicing allows enterprises to secure guaranteed sub-20ms latency for critical OT traffic over shared networks.

Obstacles

- **Unclear ROI against alternatives:** Cautious enterprises struggle to justify 5G investments, perceiving that mature 4G, Wi-Fi or low-power alternatives sufficiently service most of their current industrial use cases with lower risk.
- **3GPP Release 16 maturity:** Buyers perceive that the true value of 5G relies on advanced Release 16 capabilities (such as dynamic network slicing), whose commercial maturity and broad availability are still a work in progress.
- **Deployment and integration complexity:** Global multisite scaling is hindered by highly fragmented regional spectrum regulations and the technical friction of unifying private 5G with legacy enterprise Wi-Fi and existing OT frameworks.
- **Device availability and hardware costs:** There remains a limited ecosystem and high cost for ruggedized industrial devices natively designed to operate on the dedicated radio bands available for private network use.

User Recommendations

- Mitigate deployment complexity and internal engineering skill gaps by adopting private 5G through OPEX-based network-as-a-service (NaaS) offerings, thereby transferring operational responsibilities to managed service providers that leverage zero-touch provisioning and unified management dashboards to streamline IT operations.
- Address specialized use cases in conjunction with Wi-Fi by deploying private 5G networks specifically for operational scenarios that demand extensive coverage and stringent, deterministic application performance, rather than positioning private 5G as a wholesale replacement for enterprisewide wireless LAN.
- Enable advanced industrial AI and edge computing applications by aligning critical requirements, such as low inference latency, high-capacity uplink throughput, and data sovereignty mandates, with the unique capabilities of 5G technology prior to finalizing network architecture decisions.

Sample Vendors

AT&T; Celona; China Mobile; Ericsson; Hewlett Packard Enterprise; Huawei; Nokia; T-Mobile; Verizon; Vodafone

Gartner Recommended Reading

How to Prepare for 5G Private Mobile Network Adoption

How to Craft Comprehensive Private Mobile Network Offerings for Enterprises

Market Trend: Top 5 PMN Industries Offer Revenue Gains for TSPs

8 Critical Functionalities for Enterprise 5G Private Mobile Network Management and Orchestration

CSP Industry Vertical Solutions

Analysis By: Pablo Arriandiaga, Khurram Shahzad

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Communications service provider industry vertical solutions combine enterprise communications and digital services built and targeted for specific industry verticals. These solutions can span basic tailored communications services and CSP digital services like AI, IoT, security, and cloud, or combine with third-party industry vertical solutions through industry ecosystems. They can address adjacent industries like banking, healthcare, or physical security where CSPs become an industry player.

Why This Is Important

To achieve sustainable growth, communications service providers (CSPs) must move beyond commoditized connectivity offerings. Targeting verticals allows CSPs to reach underserved segments such as small and midsize businesses (SMBs) and drive adoption of advanced technologies — such as 5G, edge computing, AI, and the Internet of Things (IoT) — among large enterprises. By developing tailored solutions for specific industry verticals, CSPs can engage earlier in the B2B decision-making process, shifting the conversation from cost to quantifiable business outcomes.

Business Impact

- Transitions B2B buyer engagement from technology-focused conversations to high-value, outcome-driven partnerships.
- Unlocks new revenue streams by addressing underserved segments, such as SMBs, with customized solutions.
- Expands the CSP footprint into lucrative adjacent industries, including banking, healthcare, and physical security.
- Drives high-value implementations by combining private 5G and industrial AI into industrial edge offerings for IT/OT convergence and autonomy.

Drivers

- The commoditization of basic connectivity compels CSPs to differentiate by expanding into digital services and industry-specific ecosystems.
- Enterprise buyers now prioritize vendors with deep industry expertise who deliver measurable ROI, not just stand-alone technology.
- Composable business architectures and packaged business capabilities (PBCs) enable CSPs to orchestrate modular, scalable, and vertical-specific solutions.
- Seamless integration of digital services — such as cloud, security, and communications — is essential for operational outcomes and compliance, especially in regulated sectors.
- The evolution of digital channel strategies toward highly targeted, industry outcome-driven value propositions is enabling CSPs to deliver greater relevance and value to their customers.
- Adjacent sectors across consumer and B2B markets enable CSPs to create opportunities to diversify through their extensive customer bases.
    - Growing demand in consumer markets is fueling CSP expansion into banking, healthcare, telehealth, and physical security.
    - Increasing complexity in B2B environments is driving CSPs to deliver specialized solutions for heavy-asset industries.
- Emerging technologies — such as 5G, AI/machine learning (ML), communications platform as a service (CPaaS), edge computing, IoT, and private 5G — are transforming industries like automotive, healthcare, logistics, manufacturing, media, energy, retail, and utilities. CSPs' last-mile ownership gives them a latency edge for real-time applications over cloud providers. However, aligning solutions with each sector's needs is essential.
- Enterprise demand is shifting toward advanced, industry-specific AI solutions that blend vertical and industrial AI, increasing the importance of CSP assets such as private 5G, managed edge infrastructure, and strict SLAs for delivering differentiated, ready-to-deploy offerings tailored to targeted verticals.
- The rise of industry ecosystems is driving CSPs to collaborate with partners, accelerating innovation and enabling delivery of integrated, vertical-specific solutions.

Obstacles

- Legacy, siloed CSP product catalogs and inflexible fulfillment systems severely restrict the agility needed to orchestrate customized, multiservice vertical propositions.
- In large enterprises, CSPs often lack deep, credible domain expertise across multiple industries, and scaling this knowledge through organic development or costly acquisitions is highly challenging.
- The inability to accurately quantify the bottom-line business value and ROI of integrated solutions stalls enterprise adoption and prevents projects from scaling beyond pilots.
- Poorly managed indirect sales channels and complex partner ecosystems often lead to misaligned value propositions, hindering effective market penetration.
- Integrating modern AI with enterprise IT and legacy OT systems poses significant challenges, including real-time latency demands, safety requirements, and a shortage of talent skilled in AI, OT, and industrial engineering.

User Recommendations

- Adopt a phased approach to build composable capabilities, starting within individual service lines and orchestrating them via open APIs to create robust vertical solutions.
- Accelerate vertical credibility by partnering with or acquiring system integrators and software vendors that already possess deep, proven expertise in target industries.
- Overhaul go-to-market messaging to focus on quantifiable enterprise business outcomes and ROI rather than highlighting raw technological features.
- Systematically develop integrated indirect channel programs with prepackaged modules and flexible pricing to simplify the value chain for partners and customers.
- Shift from AI consumer to solution creator by developing differentiated industrial and vertical AI solutions and packaging unique CSP assets — such as private 5G, edge inference, data sovereignty, and strict SLAs— into integrated offerings for targeted verticals.

Sample Vendors

Airtel; AT&T; Deutsche Telekom; NTT DATA; Orange Business; Telefónica; Telenor Group; Telstra; Verizon; Vodafone Group

Gartner Recommended Reading

Innovation Insight: Industry Edge Enhances Manufacturing Excellence

Innovation Insight: Industry Edge Enhances Government Transformation

Innovation Insight: Industry Edge in Transportation and Automotive

Innovation Insight: Industry Edge Enhances Power and Utilities Performance

Innovation Insight: Cross-Industry Edge Computing Solutions Unveiled

Innovation Insight: Industry Edge Computing Enhances Retail Transformation

Innovation Insight: Edge Computing Enhances Healthcare Provider Efficiency

Forecast: Enterprise IT Spending by Vertical Industry Market, Worldwide, 2023-2029, 4Q25

AI in Industries: Next Trillion-Dollar Opportunity Lies in Industry-Transforming Synergy and Orchestration

Define Your AI Identity With Horizontal, Vertical and Industrial AI for Industry Product Leadership

LEO D2D Services

Analysis By: Khurram Shahzad

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Low Earth orbit (LEO) satellite direct-to-device (D2D) connectivity uses LEO constellations to deliver basic to full broadband services directly to unmodified, standard smartphones and IoT devices. This creates a hybrid connectivity infrastructure that provides seamless, ubiquitous coverage, even in environments where traditional cellular networks are uneconomical or impossible to deploy, also referred to as supplementary coverage from space (SCS) and space-based infrastructure (SBI).

Why This Is Important

While 95% of the world's population is covered by mobile broadband, only about 15% of the Earth's surface has terrestrial coverage, leaving a critical need for coverage in remote and underserved areas. This is addressed by LEO D2D services that are rapidly moving from niche emergency-only services toward a mass-market broadband offering that promises to eliminate coverage gaps, provide robust backup for enterprises, open doors for innovative business models and enhance service offerings.

Business Impact

- Expands market reach to remote and underserved regions
- Unlocks new revenue streams with premium D2D services
- Enhances service resilience and reduces churn
- Increases ARPU through value-added satellite offerings
- Drives competitive differentiation in saturated markets
- Introduces partnership and integration complexities with LEO providers
- Requires significant network upgrades and higher operational costs
- Faces regulatory hurdles in spectrum, cross-border and data compliance

Drivers

- LEO D2D services enable CSPs to provide connectivity in regions where terrestrial infrastructure is economically unfeasible or technically challenging, thus broadening their addressable market and supporting digital inclusion initiatives.
- Many regulators require CSPs to extend coverage to all citizens. LEO D2D provides a cost-effective means to achieve compliance without massive terrestrial investments.
- Enterprises and public-sector clients increasingly require seamless, reliable connectivity for mission-critical operations, and LEO D2D can fulfill these stringent requirements.
- The inherent resilience of satellite-based D2D communications ensures service continuity when terrestrial networks are compromised during natural disasters or network outages, enhancing CSPs' disaster recovery capabilities and public safety offerings.
- By integrating LEO D2D, CSPs can stand out in saturated markets with innovative services, attracting new customer segments and reducing churn among existing customers.
- The promise of ubiquitous, reliable service, regardless of location, drives higher customer satisfaction and loyalty, directly impacting CSPs' brand reputation and Net Promoter Score.
- LEO D2D enables value-added services such as direct satellite messaging, asset tracking and IoT connectivity, allowing CSPs to monetize new use cases and verticals.
- Advances in satellite technology and increased competition among LEO providers are driving down costs and improving service quality, making LEO D2D integration financially attractive and operationally viable for CSPs.

Obstacles

- Deploying full LEO D2D services demands significant capital investment, including upgrades to core networks, edge infrastructure and OSS/BSS for seamless satellite-terrestrial integration.
- Few services work indoors, as smaller satellite antennas only support higher frequencies with very poor building penetration.
- Device upgrades or replacements may be needed for LEO compatibility, raising customer costs, slowing uptake and impacting ROI, potentially requiring CSP subsidies.
- LEO networks still face limited capacity, higher latency and variable reliability versus terrestrial, challenging consistent user experience.
- CSPs must manage complex new partner ecosystems with revenue sharing, SLAs and joint GTM.
- Satellite communications introduce unique security risks and data sovereignty issues, requiring robust security and regulatory compliance.
- The evolving business case, uncertain pricing and competition complicate revenue forecasts and investment decisions, increasing financial risk.

User Recommendations

- CSP product leaders should rapidly define their D2D strategy — partner, build or buy — and embed it in product and network roadmaps.
- Build a robust business case by analyzing target segments, geographies and verticals as well as quantifying revenue, costs and ROI.
- Prioritize partnerships with 3GPP-NTN-compliant LEO providers for 5G compatibility and seamless handover, avoiding proprietary lock-in.
- Implement a zero-trust architecture with multilayer encryption and mutual authentication to mitigate the increased surface area of nonterrestrial signal interception and cross-border data sovereignty risks.
- Start with messaging-first, tiered rollouts, scaling to voice/data as LEO networks mature.
- Optimize capex for high-throughput density, leveraging D2D to reduce uneconomical spend in remote areas.
- Target enterprise SLAs and industrial IoT for high-margin, ubiquitous coverage opportunities.

Sample Vendors

Amazon Leo; AST SpaceMobile; BeiDou; Lynk Global; Skylo; Starlink; TianTong

Gartner Recommended Reading

Market Trend: Emerging Use Cases for LEO Satellite Communication Services

Integrate LEO Satellite Connectivity to Enhance Network Resiliency

Market Guide for Low Earth Orbit (LEO) Satellite Communication Services

Top Technology Trends in Enterprise Communication Services for 2026

Network Monetization APIs

Analysis By: Gaspar Valdivia, Ajit Patankar, Enrique Hernandez-Valencia

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Emerging

Definition:

Network monetization APIs refer to application programming interfaces that software developers can use for programmatic access to directly retrieve data, request services, or modify service capabilities from telecommunications networks. These APIs are designed for ease of integration, enabling the monetization of network assets and supporting a variety of business models, ranging from transactional charges to subscriptions and revenue sharing across the value chain.

Why This Is Important

Network monetization APIs enable telecom providers to generate returns on network investments in new ways by giving developers access to advanced network functions and services. The GSM Association (GSMA) is sponsoring the Open Gateway initiative in partnership with the Linux Foundation CAMARA project to develop a programmatic approach that drives cross-network interoperability, accelerates innovation, and enables global monetization in collaboration with the software industry.

Business Impact

Network monetization APIs can create a new API economy by enabling the use of network capabilities and data retrieved from the network in new ways. They support new use cases for businesses and public agencies or facilitate consumption and improve user experience in others. Most use cases today focus on fraud detection and prevention, while others, such as roaming cost optimization, carrier billing, and network quality on demand, are evolving at varying speed depending on geographies.

Drivers

- The CAMARA Project provides a framework for network operators and partners to design, implement, and manage a common set of consistent and interoperable northbound service APIs to expose network capabilities. Examples of such APIs include number verification, know your customer/MATCH, device location, SIM swap, and carrier billing.
- Since the launch of Open Gateway in February 2023, the initiative has scaled notably. As of March 2026, 85 operator groups representing over 300 mobile networks and around 80% of global mobile connections are part of the Open Gateway community. New operators continue to join to monetize their networks.
- National coalitions are driving nationwide use cases. For example, New Zealand telcos (Spark, One NZ, and 2degrees) recently signed an MoU to deliver standardized “Number Verification” and “SIM Swap” APIs to combat fraud and identity theft. Similar collaborations exist in Brazil, the U.K, the U.S., and other territories.
- Network equipment providers, such as Ericsson (via their Aduna venture) and Nokia (through their Network as Code approach), actively support the ecosystem by offering Open Gateway API aggregation platforms, commercial frameworks, and distribution channels. They also provide tools to help CSPs launch network APIs, and assist developers in using them.
- Cloud hyperscalers such as Google (enabling APIs in their Firebase software development kit [SDK]) serve as a powerful channel for developers to discover and use telco network APIs.
- Communications platform as a service (CPaaS) vendors like Infobip and Sinch are also involved. Initially focused on enabling basic telecom services like SMS and SIP trunks through APIs, they proved a market opportunity that can now be extended to the broader 5G community with more use cases and applications.
- The ability to expose consistent APIs for enterprises and developers to use in private mobile network requirements further drives innovation.

Obstacles

- Developers expect consistent network APIs across CSPs for cross-operator use cases. Lack of cross-network functionality support undermines value.
- Business and commercial models, including settlement mechanisms, must satisfy all stakeholders, including network providers, API aggregators, hyperscalers, potentially system integrators, software developers, enterprises, and end users.
- Tailoring business and commercial models, as well as price points, to use cases and geographies can delay time to market. Aggregators and channel partners help accelerate integration and time-to-value.
- Some APIs, like “Quality on Demand,” require more complex technologies and business models, additional network investments, and regulatory changes in some markets, so availability varies by operator and region.
- Some APIs, like those related to location, face stricter compliance, privacy and security standards, which also vary by market. Many of these requirements still need to be defined and operationalized.

User Recommendations

- Collaborate with other CSPs via GSMA Open Gateway and CAMARA to ensure consistent, interoperable, cross-network APIs, maximize market reach, and drive adoption.
- Engage API aggregators, marketplaces, and hyperscalers to leverage their platforms for API distribution and marketing to a wider developer community.
- Co-develop direct-to-enterprise use cases where unique network capabilities offer a competitive edge (for example, edge discovery APIs).
- Support developers with documentation and curated code samples, SDKs, sandboxes for testing and experimentation, and dedicated support channels.
- Architect your API exposure platforms to facilitate seamless consumption by agentic AI and machine customers. Implement frameworks such as Agent-to-Agent (A2A) protocols and the Model Context Protocol (MCP) to empower autonomous software agents to dynamically discover network APIs, automatically negotiate network capabilities, and orchestrate goal-driven workflows.

Sample Vendors

Aduna Global; AT&T; Deutsche Telekom; Ericsson; Nokia; Orange Business; Telefónica; TIM; Verizon; Vodafone

Gartner Recommended Reading

Market Guide for CSP Network API Providers

Industry Insight: Revenue Opportunity Projection of the Network API Market

AI Vendor Race: Prepare Enterprise Network Services for Machine Customers, or Lose to Competitors Who Have

How MCP and the A2A Protocols Impact API Management

Sovereign Cloud

Analysis By: Rene Buest, Gregor Petri

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Sovereign cloud is the provision of services by a cloud provider to ensure that data, operational and technological sovereignty meet the sovereignty requirements of its intended customer base. Sovereign cloud ensures that data, applications, infrastructure and operations are immune from control by external jurisdictions and are fully protected from foreign government interference and access.

Why This Is Important

Public sector and commercial organizations depend on cloud services, leading to greater demand for control and operational autonomy and thus offerings that provide a high degree of sovereignty. In many jurisdictions, data residency, data protection requirements and privacy laws are increasing. Increasing geopolitical tensions, different economic ideologies and proliferating cybersecurity risks from a variety of directions, including state actors, are steadily elevating interest in sovereignty.

Business Impact

Concerns about data, operations and technology being controlled by foreign-owned cloud providers are increasing the demand for true sovereign clouds. Regulators are introducing requirements to restrict organizations from using services provided by vendors outside their own country. These regulations impact choices organizations make when using cloud services. Consequently, end users may face difficulties in accessing resources and innovation to support their digital business initiatives.

Drivers

- Ongoing geopolitical turmoil and uncertainty accelerate sovereignty concerns, particularly among governments, regulated industries and critical infrastructure, especially in Europe, the Middle East, Latin America and Asia/Pacific. Organizations in these regions are increasingly concerned about their dependence on foreign cloud infrastructure providers and the sovereignty of data, applications, infrastructure and operations hosted in foreign-owned cloud service offerings.
- Concerns over digital sovereignty lead countries and confederations of states to pursue their own sovereign digital strategies. Many commercial organizations are increasingly impacted by digital geopolitical issues, such as trade disputes, legislation coming from one country that impacts global operations, and government-imposed restrictions on the acquisition and use of digital technology.
- Given the critical role that digital technology plays in the economic, cultural, social and government institutions of a country, great power competition sharpens the focus on digital sovereignty. Particularly in a world of public clouds, every organization needs to be in control to be able to address its own risk management, compliance policies, culture or business strategy and to address multiple regulatory requirements.
- Organizations are increasingly concerned that cloud and digital infrastructure will be used as a tool to exercise pressure, coerce, and enforce political influence. This has led to a rethinking of cloud strategies and the acceleration of geopatriation. The call for a higher degree of digital sovereignty aims to preserve autonomy by developing and maintaining one’s own capabilities and avoiding dependencies.

Obstacles

- Domestic cloud providers are currently not able to fully compete with hyperscale cloud offerings, as the hyperscaler capabilities still exceed most domestic cloud offerings. Considerable technical obstacles exist if domestic clouds are expected to deliver the maturity and level of the scalability and functionality of hyperscale offerings.
- The growing influx of sovereign cloud options from global cloud providers, all based on various approaches and delivery models, is making it hard for end users to understand the actual value of each offering and how they differ.
- Individual governments defining their own requirements for sovereign cloud offerings may lead to compliance regimes that impede public cloud scale and innovation and lead to conflicting regulations.

User Recommendations

- Define the sovereignty requirements and agree on the sovereignty level required by your organization by country, vertical industry and workload type by working with your legal counsel and risk departments.
- Differentiate between different sovereign cloud approaches by the type of workload, data and infrastructure when making cloud deployment decisions. Classify various delivery models between the cloud provider approaches. Establish a consistent, repeatable and defensible process when assessing sovereign offerings.
- Evaluate cloud services for offerings that can be provided locally and leverage third-party solutions to protect data at rest and in transit.
- Evaluate the different cloud provider approaches to meet your defined sovereignty requirements by quantifying their technological limitations that might limit the delivery of your mission-critical solutions.
- Consider sovereignty as only one of several critical dimensions that must be considered when evaluating a cloud service provider.

Gartner Recommended Reading

Build a Sovereign Cloud Strategy

Prioritize on Sovereign Capabilities When Choosing Your Cloud Provider

Threat Intelligence in ECS

Analysis By: Jon Dressel

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Threat intelligence for enterprise communication services (ECS) involves the automated collection and analysis of diverse data sources to detect and mitigate cyberthreats — including phishing, malware, ransomware, APTs and insider threats. Leveraging AI, it informs proactive defense, incident response and compliance with evolving regulations, such as SEC Cybersecurity Disclosure Rules and NIS2, enhancing both CSPs and enterprises' overall security posture.

Why This Is Important

ECS threat intelligence is crucial for timely mitigation of evolving cyber risks, identifying vulnerabilities in communication channels and preventing data breaches and unauthorized access. By leveraging AI-driven analysis of attacker behavior, CSPs enhance security, safeguard sensitive information, ensure business continuity, support regulatory compliance and foster a proactive, collaborative security culture.

Business Impact

ECS threat intelligence minimizes cyberattack risks, safeguards data, protects brand reputation and reduces breach financial losses. It provides actionable insights for improved decision making, ensures regulatory compliance and upholds customer trust. It enhances operational efficiency and business continuity, boosting the firm's reputation and competitive advantage. ECS threat intelligence complements traditional cyber threat intelligence, including dark and deep web monitoring.

Drivers

- AI and automation risks: The integration of AI and automation in communication services introduces new threats, necessitating advanced threat intelligence to predict and mitigate AI-driven and automated attacks, along with attacks on AI.
- Evolving regulation compliance: Adhering to data protection laws and industry standards (e.g., NIS2, CRA, HIPAA) requires threat intelligence to ensure data privacy and regulatory compliance.
- Proactive TDIR capabilities: Mandated threat detection, investigation and response (TDIR) are essential for meeting legal and industry requirements.
- Cost efficiency: Minimizing financial losses from breaches and optimizing security investments through AI-driven, informed decision making supports organizational cost efficiency.
- Customer trust and brand reputation: Demonstrating strong threat intelligence practices enhances reputation management and maintains customer trust.
- Digital transformation: Adoption of new technologies and digital transformation initiatives requires updated threat intelligence to secure modern communication platforms.
- Expansion of attack surface: The proliferation of 5G, PMNs, IoT and edge computing increases vulnerabilities, demanding enhanced threat intelligence for interconnected networks.
- Cloud migration: The shift of communication services to the cloud drives the need for specialized threat intelligence solutions, including fraud detection and cloud-native security tools.
- Remote and hybrid work: The prevalence of remote and hybrid work environments require adaptive threat intelligence to secure communication tools against targeted attacks.
- Supply chain security: The security of CSPs and their supply chains is critical, necessitating comprehensive threat intelligence strategies aligned with regulations.
- Virtualization and containerization: As network functions become virtualized and containerized, understanding and mitigating threats in these environments is a key driver for ECS threat intelligence innovation.

Obstacles

- The volume and complexity of modern communication networks' data can overwhelm threat intelligence systems, complicating accurate threat detection.
- Rapidly evolving attack tactics, including AI-driven and automated threats, require continuous updates and agile adaptation of threat intelligence strategies.
- A shortage of skilled cybersecurity professionals with expertise in advanced threat intelligence for CSPs and their clients impedes effective implementation and analysis.
- Finite financial resources may restrict investments in next-generation threat intelligence technologies and automation due to competing investment priorities.
- Balancing threat intelligence activities with stringent privacy regulations and compliance requirements remains a significant challenge.
- High false positive rates can lead to alert fatigue, causing critical threats to be overlooked.
- Integration challenges with legacy systems and cloud-native or virtualized environments hinder seamless threat intelligence deployment.

User Recommendations

CSPs should:

- **Invest in advanced tools:** Deploy AI/ML-driven threat intelligence to process large data volumes, adapt to evolving threats, and reduce alert fatigue.
- **Enhance skills:** Prioritize training and hiring cybersecurity professionals skilled in advanced threat intelligence, telecom-specific vulnerabilities, and automation.
- **Integrate seamlessly:** Ensure solutions work with existing and emerging security architectures.
- **Prioritize privacy:** Maintain compliance with evolving regulations (e.g.,, NIS2, SEC) through strong data protection measures.
- **Focus on accuracy:** Reduce false positives by refining detection algorithms and using contextual analytics.

- **Define PIRs:** Establish and update priority intelligence requirements to optimize resource use.
- **Allocate resources:** Align budgets with security objectives for sustainable investment in threat intelligence.
- **Promote Industry sharing and collaboration:** Provide threat intelligence sharing and collaborate with industry peers.

Sample Vendors

AT&T; BT Group; Deutsche Telekom; Lumen; NTT; Orange Business; Verizon

Gartner Recommended Reading

AI-Driven Network Threat Intelligence Allows CSPs to Build Superior Security Offerings

How to Evaluate Your Threat Intelligence Program's Effectiveness

Improve Cyber Resilience With Threat Intelligence

The Evolution of Threat Intelligence Is Unified Cyber Risk Intelligence

Alternative WAN Backbone Services (XBaaS)

Analysis By: Karen Brown

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Alternative WAN backbone services (XBaaS) is an option offered by colocation, cloud or security providers that allows enterprise customer WAN traffic to flow across their private backbones. This can improve network security and performance for users, devices and locations, but it also requires customers to procure access circuits to and from the provider.

Why This Is Important

Enterprises continue to look beyond traditional WAN providers to alternative backbone as a service (XBaaS) WAN offerings to support network traffic between their corporate locations. Not only does XBaaS provide a competitive alternative, but it typically offers better application performance because there are fewer router hops on the provider's private backbone. As a private backbone, it also offers better security compared to public internet transport.

Business Impact

Compared to traditional WAN services, XBaaS offers better application performance and security for transport, which is the largest segment of a WAN. Available from SASE and colocation vendors, these services don't support end-to-end connectivity. Clients must still buy access circuits from a traditional network provider to link their sites to the XBaaS provider's node. This can add to cost as well as vendor and network management complexity. XBaaS service geographic reach and SLAs also vary.

Drivers

- Public colocation, cloud and security providers use aggressive marketing and sales techniques to convince enterprise clients to use their backbone services and discard legacy WANs.
- XBaaS is attractive to enterprise customers relying on the provider's colocation, cloud and security service edge (SSE) services.
- Enterprises often see XBaaS private backbones as a means to improve network security by limiting exposure to the public internet infrastructure.
- As an architecture, XBaaS is compelling for organizations that lack data center investment and instead rely heavily on one public cloud or colocation provider.
- XBaaS provides additional route diversity for clients seeking to improve their WAN business continuity architectures.
- SASE providers' XBaaS offerings make their solutions more compelling as a single-vendor underlay and overlay vendor option.
- Enterprise dissatisfaction with traditional WAN carriers is high, and many clients seek to limit reliance on these providers. Enterprises often believe that the carriers have ignored their complaints about lack of support and network performance issues, further accelerating their efforts to seek better alternatives.
- Organizations deploying AI and agentic AI are increasingly relying on multiple cloud and neoclouds for support. This increases the importance of WAN performance, which increases the appeal for XBaaS options.

Obstacles

- XBaaS can be more expensive than traditional WAN services.
- Since XBaaS providers support only their own customer traffic, they are less useful to clients relying on multiple colocation, cloud or security providers.
- While XBaaS offers improved security across the provider's private backbone, this protection does not extend to the access link from the customer's locations to the provider's nodes. Access connection security depends on the traditional telco supplier.
- The number of XBaaS nodes is typically small compared to traditional telcos. This can limit resilience options if a node fails and add end-to-end latency depending on an end user's location relative to the serving node.
- Limited colocation and cloud monitoring data impairs XBaaS value to network operations personnel.
- SLAs cover availability only, lacking circuit performance guarantees such as latency, jitter and packet loss.
- XBaaS providers may not support cloud onramp connectivity to other IaaS or SaaS application providers.

User Recommendations

- Use XBaaS opportunistically, given its higher costs. For example, use XBaaS if there is a specific need to lower latency for high-capacity interregional or intraregional links between data centers or for connectivity to a particular colocation, cloud or security provider.
- Verify that the provider's backbone aligns with your organization's corporate location footprint. If the provider's nodes are a significant distance from any subset of corporate locations, a long access connection will be necessary, which will add cost and introduce latency for performance-sensitive applications.
- Ensure enterprise traffic is secure end-to-end, including security across the access connection. Mitigate the security vulnerability when traffic moves between the access provider and XBaaS providers' access circuits by adding VPN or ZTNA security to internet access connections or use private access connections such as MPLS.

Sample Vendors

Alkira; Amazon; Cato Networks; Cloudflare; Digital Realty; Equinix; Google; Megaport; Microsoft; Netskope

Gartner Recommended Reading

Optimize WAN Architectures for Workloads That Span the Hybrid Cloud and the Multicloud

Market Guide for Specialty Cloud Providers

Look to XBaaS to Address Long-Standing WAN Challenges

Securing CSP AI/ML Models in Communications

Analysis By: Jon Dressel

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Securing artificial intelligence (AI) and machine learning (ML) in communications is the process of safeguarding the development, deployment and operation of AI and ML models within communication systems against evolving threats, including adversarial attacks and data poisoning. It enables communications service providers (CSPs) to leverage secure AI/ML technologies while ensuring compliance, cybersecurity resilience and trust in AI/ML environments.

Why This Is Important

Securing AI/ML models in communications is critical to protect sensitive data, minimize breach risks and prevent misuse. Advanced defenses detect and mitigate evolving threats, ensuring model integrity and privacy across all stages. Compliance with updated regulations, reliability and resilience are prioritized. Addressing bias and explainability supports ethical, transparent and equitable AI, building trust and accountability for CSPs and their enterprise customers.

Business Impact

Securing AI/ML models in communications delivers significant business value by protecting intellectual property, enhancing customer trust, ensuring regulatory compliance and minimizing financial, and reputational losses. It maximizes AI/ML potential while mitigating risks. Leading solution providers, such as Nokia and Ericsson, now integrate MLSecOps and continuous monitoring into the software development life cycle (SDLC) to address emerging threats and foster innovation.

Drivers

- **Data protection and privacy regulations:** Heightened global regulatory focus, including the EU AI Act, China's cybersecurity laws, and emerging U.S. frameworks, mandates robust security for AI/ML models to ensure compliance and protect sensitive data.
- **Rising cyberthreats:** The proliferation of sophisticated AI-driven attacks — such as deepfakes, prompt injection/extraction, training data poisoning, adversarial manipulation, and AI-powered phishing — requires advanced detection and mitigation strategies.
- **Growing reliance on AI/ML technologies:** Communications service providers (CSPs) increasingly leverage AI/ML for network optimization, customer service automation, predictive maintenance and fraud detection, amplifying the need for secure and resilient models.
- **Trust, reputation and explainability:** Explainable AI (XAI) and transparency are critical for building and maintaining trust with customers, regulators and stakeholders, as well as for addressing ethical and fairness concerns.
- **Intellectual property protection:** AI/ML models represent valuable proprietary assets. Securing these models safeguards algorithms, data and research against unauthorized access, theft and reverse engineering, preserving organizational competitive advantage.
- **Evolving industry standards and best practices:** Adoption of MLSecOps, continuous monitoring, and secure AI life cycle management is increasingly required to address emerging threats and maintain industry leadership.
- **Cross-border data governance:** As CSPs operate globally, secure AI/ML model deployment must address sovereignty, cross-border data transfer, localization requirements and multijurisdictional compliance.

Obstacles

- Limited awareness of AI/ML risks among CSPs requires ongoing education and upskilling to address emerging threats.
- The complexity of securing AI/ML models demands specialized expertise in both cybersecurity and AI/ML, complicating integration into DevSecOps and MLSecOps teams.
- Evolving cyberthreats necessitate continuous monitoring, adaptive defenses, threat hunting and rapid incident response.
- Balancing data privacy, regulatory compliance and AI/ML model performance remains a significant implementation challenge.
- The evolving landscape of AI security standards hinders the establishment of consistent best practices.
- The opaque, "black-box" nature of advanced AI models complicates vulnerability identification, attack detection and security verification.
- Limited availability of automated tools for AI/ML security further impedes effective risk mitigation.

User Recommendations

- Implement AI-based security tools, such as advanced anomaly and fraud detection, to protect AI/ML systems.
- Use secure data handling practices, including homomorphic encryption and differential privacy, to safeguard model data.
- Employ continuous, AI-driven monitoring and automated model updates to address vulnerabilities and attacks in real time.
- Conduct dynamic, AI-powered threat modeling and risk assessments specific to communications environments.
- Integrate explainable AI (XAI) to enhance transparency, accountability and regulatory compliance.
- Provide ongoing employee training on AI/ML security best practices.
- Develop and regularly update incident response plans for AI/ML-related breaches.
- Stay current with evolving data protection laws, industry standards and best practices by engaging in AI/ML security forums and consortiums.

Gartner Recommended Reading

Emerging Tech: Explainable AI Is Essential for Customers to Trust Autonomous AI Solutions

AI Vendor Race: GMs: Win the AI Security Battle With an AI Security Platform

Start Your AI Application Security Journey Using Existing Security Platforms

Emerging Tech: AI in CPS Security

VNFaaS

Analysis By: Khurram Shahzad, Enrique Hernandez-Valencia

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Virtual network function as a service (VNFaaS) is a cloud-native model where network functions, such as routing, firewalling and WAN optimization are deployed and managed in virtualized and cloud environments. Offered on a consumption-based, pay-as-you-go service model, VNFaaS lets enterprises dynamically scale and orchestrate services without major hardware investment, deploying software functions on shared or dedicated infrastructure at service provider PoPs or in public/private clouds.

Why This Is Important

VNFaaS changes network delivery by decoupling network functions from dedicated hardware, offering a dynamic operating expenditure model with elastic scalability. By using x86 devices or cloud nodes instead of vendor-specific hardware, organizations gain agility and faster time to market. This “as-a-service” approach replaces monolithic infrastructure with automated provisioning, significantly reducing capital expenditure (capex) while simplifying scaling and enhancing operational flexibility.

Business Impact

VNFaaS enables service providers to expand their service offerings, increase infrastructure utilization and monetization, and attract new customers by reducing entry barriers or long-term commitments. For organizations, it provides greater flexibility to deploy networking capabilities on-demand without the need to swap networking appliances. This results in reduced deployment costs, faster time to market for new services, improved commercial flexibility and lower ongoing network management costs.

Drivers

- Organizations want to simplify the deployment of networking and wide-area connectivity solutions. VNFaaS reduces enterprise networking appliance sprawl, truck rolls, and the costs and risks associated with ownership of enterprise communication infrastructure while simplifying network operations.
- As enterprises increasingly adopt cloud-based applications and services, the demand for agile and scalable network infrastructure intensifies. VNFaaS enables on-demand scaling of network functions, offering the agility to support evolving business requirements.
- VNFaaS platforms often integrate network as a service (NaaS) capabilities providing programmatic control, automation, self-service and self-monitoring capabilities. VNFaaS allows service providers to build and offer unique service packages with preintegrated network functions, creating differentiation in a competitive market.
- VNFaaS leverages the trend in disaggregated networking equipment, providing flexibility in solution deployment and enabling the centralization of network function management for service providers and enterprises, improving operational control, resource utilization and efficiency.
- Maturity of VNFs enable service providers to offer them as a service with business-grade SLAs. VNFs are attractive as they enable software-driven modernization and innovation without a forklift upgrade replacement of deployed infrastructure. Additionally, they can offer cost-effective alternatives to custom-made, custom-built hardware solutions.

Obstacles

- Limited VNF interoperability hinders seamless integration between third-party VNFs and VNFaaS platforms. This creates complex integration requirements for cloud hosting and OSS/BSS, ultimately slowing customer adoption.
- VNFs may suffer from performance degradation on suboptimal hardware compared to dedicated appliances. High-performance scaling requires specialized hardware (DSPs, GPUs) and software acceleration (DPDK, SR-IOV).
- Moving to VNFaaS introduces new security vulnerabilities through open APIs, and risks associated with customer-managed configurations.
- Integrating multivendor VNFs with existing network infrastructure can be complex and resource intensive.
- Adoption is slowed by lack of VNF expertise. Providers must offer enablement programs to overcome the preference for physical assets associated with a capex mindset.

User Recommendations

- Invest in open standards and interoperable APIs to facilitate VNF deployment, integration, orchestration and life cycle management enabling end-to-end to achieve a high degree of automation in service design, creation and delivery across hybrid/virtual networks.
- Customize VNFaaS offerings for targeted customer use cases (e.g., WAN optimization, security, network slicing for IoT) and flexible, consumption-based pricing models.
- Develop a broad ecosystem of VNF vendors to ensure a comprehensive VNFaaS portfolio. For example, several service providers are offering firewall, router, SD-WAN gateways and WAN optimization features through VNFaaS.
- Prioritize security and compliance by implementing proactive threat detection and mitigation strategies.
- Improve customer experience through intuitive onboarding, real-time VNF performance monitoring, self-service tools and support to help with adoption and effective utilization of VNFs.

Sample Vendors

Broadcom; Cisco Systems; Fortinet; Hewlett Packard Enterprise (HPE); Huawei Cloud; Nokia; Palo Alto Networks; Versa Networks

Gartner Recommended Reading

Hype Cycle for Telco Cloud Services, 2025

Top Technology Trends for CSP CIOs in 2026

Top Strategic Trends for CSP CIOs in 2026

Market Guide: CSP NaaS Providers

2025 Top Trend: Rise of CSP Digital Marketplaces

Sliding into the Trough

CSP Superapps

Analysis By: Susan Welsh, Lacy Lei

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

A superapp provides a unified mobile app experience to end users through a mobile platform with core features that fosters an ecosystem of miniapps. This ecosystem eradicates the requirement of a separate application marketplace and enables users to have a consistent and personalized app experience by offering the ability to discover, install and activate/deactivate miniapps inside the superapp.

Why This Is Important

Users demand powerful and easy-to-use mobile-first experiences. Communications service providers (CSPs) can offer superapps for external use by customers for consolidating self-service across product lines or as a business model for delivering composable application and lifestyle service bundles with partners to enterprises or consumers. CSPs can also provide internal superapps to organize multiple solutions for their own employee base, e.g., for frontline workers to enhance their ability to provide good customer experience.

Business Impact

CSPs are exploring and offering superapps with aims to drive revenue and expand relevance to customers to increase retention. Superapps reduce user experience (UX) friction (such as context switching) and development effort by consolidating multiple mobile apps or related services. Superapps provide a more engaging and streamlined experience for customers, partners or employees. They improve UX and personalization by enabling users to activate their own toolboxes of miniapps and services.

Drivers

- **Range of use cases for CSPs for superapps:** CSPs can use superapps to consolidate customer self-service across multiple service lines, promote customer discovery and use of products and services, and for internal use by employees as workforce superapps.
- **Expanded composable service offerings and partner ecosystem to differentiate:** Superapps offer one app where digital transactions, services and subscriptions can be organized, personalized and managed. CSPs use superapps to expand to adjacent services (such as fintech, insurance, utilities bill pay and wellness solutions) and to attract a wide range of partners (including smaller and local partners). Examples include EE's EE APP with EE ID, Jio Platforms' MyJio, Orange Middle-East Africa's Max it, Proximus's superapp Proximus+ (Belgium), Safaricom's M-PESA, SK Telecom's A. with AI assistants and LLM-based agents, the Tata group's Tata Neu, and Telkomsel's MyTelkomsel.
- **Wide range of KPIs focused on revenue growth and increased customer satisfaction:** CSPs aim to drive frequent customer digital engagement, and enhance discovery and promotion of adjacent services for more upsell and user satisfaction while minimizing churn. They also want to target a broader set of customer segments, gain more customer insights through telemetry, enhance brand awareness and drive internal efficiencies by using a superapp. This can consolidate self-service apps across different product lines for converged service bundles.
- **Enterprise use cases:** As the superapp concept can be applied to enterprise SaaS applications and tools, such as workflow, collaboration and messaging platforms, CSPs are seeing the potential for offering superapps as a product to B2B customers. One example is Safaricom's M-PESA for Business. CSP teams and product managers can also use superapps internally for different employee use cases and workflows by region.
- **Simplified development:** The availability of platforms that offer GenAI-powered low-code/no-code significantly simplifies the development of miniapps, making it accessible beyond IT teams, so that business teams can create and deploy miniapps.

Obstacles

- Superapps require a platform for miniapp development, strict standards around integration with the platform and a high level of software development life cycle governance, which some CSPs lack.

- Creating the business ecosystem and compelling, lasting user engagement (with consistent UX design between superapp and miniapp) can be more challenging than technology implementation.
- Converting multiple existing applications (such as self-service apps and loyalty apps across different CSP product lines) with different UI and purposes under a single superapp can cause poor UX.
- Data sharing is complex — including financial information, location data and user preferences — and reinforced by simple user authentication, such as single sign-on (SSO), while tracking user preferences or app usage history. This raises concerns about data privacy, security and governance for the miniapp-superapp relationship.
- CSPs may focus on different digital ecosystem platforms, such as integrating multiagent AI solutions for customers, rather than a superapp.
- Obtaining publishing approval for the superapp from leading mobile device manufacturers is associated with several challenges, such as the ongoing legal battle between the U.S. Department of Justice and Apple over the restriction of superapps. (See Justice Department Sues Apple for Monopolizing Smartphone Markets on the U.S. Department of Justice's website.)

User Recommendations

- Identify whether a superapp is the right fit for your case.
- Address who leads superapp projects, such as a business team for external superapps and a fusion team driven by IT for internal workforce superapps.
- Build on the existing base of users and functionality in the current customer mobile app to add miniapp capabilities. Focus on core features in your superapp (such as commerce, payments, communications or collaboration) that will drive a greater mass of adopters and create developer interest.
- Choose a superapp technology platform that supports real-time updates and extensibility without requiring a complete rebuild of the application.
- Offer an AI-enabled developer experience (such as APIs, AI coding assistant, software development kits and frameworks) for partners to build, test, register and submit miniapps into miniapp stores for potential monetization.
- Define security and data protection needs by establishing governance reinforced with common platform implementation.

- Prepare for an AI-first superapp strategy such as using the multimodal conversational interaction model to replace traditional mobile app experience. Integrate agentic AI for automation and likely win use cases such as customer service.

Sample Vendors

Alibaba Cloud; Emeldi Group; Globant (GeneXus); KOBIL; Microsoft; OutSystems (Ionic); Paytm; Tencent; Whale Cloud Technology

Gartner Recommended Reading

Top Strategic Technology Trends for 2023: Superapps

Quick Answer: What Is a Superapp?

Quick Answer: How Does a Superapp Benefit the Digital Employee Experience?

The Three Pillars of an Effective Workforce Superapp Strategy

CSP Digital Marketplaces

Analysis By: Will Rice, Susan Welsh

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

CSP digital marketplaces are digital commerce channels through which CSPs enable self-service or guided selling of composable offerings from their own products and partner ecosystems. Marketplaces interact with other capabilities such as product and service catalogs, inventory, billing, charging, and fulfillment. They can be broad platforms or have a specific purpose, such as selling Internet of Things (IoT) devices, consumer subscriptions, small-business essentials, or APIs for developers.

Why This Is Important

Digital marketplaces are an increasingly important part of communications service providers' (CSPs') go-to-market strategy for connectivity and digital services to consumer segments as well as enterprises, including small and midsize businesses (SMBs), or B2C, B2B and B2B2X (enabling enterprise customers to resell). CSPs can enrich their offerings with partner solutions, drive data insights on buyer behavior, and implement automation for faster cycles and improved digital engagement. CSPs can use marketplaces to differentiate from competitors by expanding their portfolio with partner offerings, ease of use, automation, composable bundles, verticalization, and locally tailored offerings.

Business Impact

A digital marketplace accelerates time to market, extends outreach to target segments, expands partner ecosystems and speeds up the sales cycle. For CSPs, marketplaces target increased self-service and digital engagement, revenue growth, tailored solutions that can be composed based on the needs of each buyer, and actionable data insights on purchase behavior that can inform product developers and enrich the support of ecosystem partners.

Drivers

- CSP B2B digital marketplaces can support a platform business model and composable commerce, with offerings built by combining products and services from the CSP and ecosystem partners.
- Key portfolio expansion areas driving interest in marketplaces are SaaS applications and value-added services such as hardware and apps to provide value on top of connectivity (for example, IoT marketplaces) and network API monetization.
- CSPs seek to enhance customer experience (CX) and drive revenue through richer sets of data for AI/machine-learning-driven recommendations and next best actions.
- Providing buyer journey data to partners can help to attract and retain more partners.
- CSP ecosystem interest in digital marketplaces is increasing. Examples of CSP digital marketplaces include A1 Digital, BT SME marketplace, Comcast Business Marketplace, Docomo Business Online Shop, KDDI Australia, STC Marketplace, Telefónica Tech SME marketplace, TELUS Business Marketplace, TIM Digital Store and Vodafone Business Marketplace.
- Business buyers benefit from reduced procurement costs in obtaining multiple different products in different categories from a single marketplace, creating an improved CX. The primary applications used to create enterprise marketplaces — i.e., marketplace operation applications — have grown in prevalence and functionality during the past year. Several digital commerce platform vendors are adding marketplace functionality to their offerings. Some of these vendors are also adding a network of preintegrated suppliers to CSP marketplace operators, in order to more rapidly and easily scale their marketplace and have ready-to-go offerings with preonboarded partners. Examples include Amdocs Subscription Marketplace and AppDirect's AppMarket.
- Digital marketplaces can cater to machine customers that purchase based on data-driven decisions and allow them to more quickly and comprehensively comparison shop by providing a richer set of product data and parameters.

Obstacles

- Success depends on integration with existing capabilities, including the digital commerce platform, partner ecosystem management, and other operations support system (OSS)/business support system (BSS) capabilities, such as catalog, inventory, fulfillment, and automation. These capabilities may need to be changed to support digital marketplaces.
- Even when built and launched, customers may still prefer human-interaction channels and underutilize the marketplace until buyer behaviors, sentiment, and procurement processes change.
- Data privacy and security processes, as well as regulatory compliance among partners and in the marketplace, need to be properly developed and managed.
- Challenges may arise with the need to define and manage processes related to customer service, loyalty, returns, and logistics across the range of offerings and partners. Sales transformation may also be required, including changes in commercial models and targets.
- CSP digital marketplaces are often siloed initiatives for one CSP service line or segment, but not structured and funded across the whole organization.

User Recommendations

- Evaluate the priority of a marketplace by sizing the market opportunity, assessing your target buyers' preference and complexity of the buying process.
- Incorporate buyer journey analysis and good UX to create a marketplace that will be more widely adopted and utilized, both by more technical users and nontechnical purchasers.
- Blend digital engagement and commerce with human-centric guidance and support to provide curated offerings and increase traction for customers who do not want a fully digital experience by offering a human-augmented digital experience.
- Assess which components of OSS/BSS need to be changed to integrate with a digital marketplace, particularly to support increasing automation, use of AI, and end-to-end digital processes across the buyer journey.
- Integrate with a partner ecosystem platform, which may need to be developed in tandem.
- Educate customers, partners, and CSP salespeople on the role of the marketplace in the buying process.

Sample Vendors

Amazon Web Services; Amdocs; AppDirect; Beyond Now; CloudBlue; Comviva; Marketplacer; Tecnotree

Gartner Recommended Reading

Market Guide for CSP B2B Digital Marketplace Solutions

Competitive Landscape: CSP Customer Management and Experience Solutions

Market Overview for CSP AI-Enabled Marketing and Sales Solutions

B2B Self-Service Capabilities

Analysis By: Khurram Shahzad, Amresh Nandan, Susan Welsh

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

B2B self-service capabilities offered by communications service providers (CSPs) refer to the utilization of digital and online portals, applications and API integrations that enable B2B customers to fully or partially manage their services. These include activities like service selection, design, service management, order tracking, billing, transactions, performance monitoring and observability, support and troubleshooting.

Why This Is Important

B2B self-service enables CSPs to enhance customer experience (CX) and operational efficiency by offering flexibility, agility, autonomy and convenience. It allows CSPs to scale service delivery with limited resources, maximize the impact of human interactions to deliver high-value use cases and leverage customer insights to personalize offerings and optimize go-to-market (GTM) strategies, driving revenue growth and competitive differentiation.

Business Impact

B2B self-service enhances CX through digital convenience, flexibility and transparency. It boosts efficiency by automating routine tasks, lowering operational costs and scaling service delivery — especially for SMBs. Additionally, it leverages usage data to personalize offers and predict churn. By integrating performance insights into enterprise systems, CSPs foster loyalty and differentiation while mitigating churn.

Drivers

- B2B customers increasingly expect digital self-service options across all touchpoints, mirroring consumer experiences in other industries.
- CSPs strive to reduce operational costs by shifting from resource-intensive customer support channels to automated, scalable self-service platforms.
- Businesses of all sizes adopting cloud-based solutions and everything as a service (XaaS) models require near-real-time management capabilities, driving demand for advanced self-service tools.
- With adoption of technologies like SD-WAN, advanced 5G and IoT, network configurations become more complex. Enterprise customers want self-service capabilities to manage, customize, and troubleshoot critical business services.
- Some B2B customers want integration of their communication services with existing enterprise systems to enable seamless service journeys and single platforms for management and data analytics.
- CSPs are looking for scalable solutions to efficiently address increasingly complex requirements of large numbers of SMBs while delivering a good CX.
- CSP ecosystem partners want the ability to co-create, configure and add their specialized services on top of CSP products. B2B self-service capabilities enable partners to develop and deliver integrated complex solutions.

Obstacles

- Integrating self-service platforms with older back-end billing (BSS) and provisioning (OSS) systems can lead to high costs, longer timelines and disruptions to existing operations.
- Exposure of sensitive data through the portal/APIs imposes higher security requirements for data privacy/protection and compliance.
- Building an intuitive self-service experience for non-technical users can be complex because of nuances of complex technology options and parameters.
- Driving engagement of self-service requires targeted training, incentives and initiatives, while presenting the right level of information for diverse customer intents and use cases.
- Human interactions are still needed and self-service needs to provide seamless and integrated CX for a range of customer needs.
- Siloed development of product-level self-service capabilities result in a fragmented experience for customers, who are not able to resolve end-to-end requests in a consistent manner.

User Recommendations

- Develop intuitive interfaces tailored to specific B2B user personas.
- Use Gartner's total experience (TX) framework to unify CX, EX, MX and UX to drive greater customer and employee satisfaction, loyalty and advocacy.
- Deploy composable platforms that allow customization of diverse and complex use cases across various customer roles, segments, and industry verticals. Integrate summarization tools, visualization tools, fault detection and natural language (NL) interfaces via AI.
- Implement robust security protocols and role-based access controls to ensure customer data privacy and platform integrity.
- Launch a comprehensive enablement program with training and incentives. Incorporate GenAI into knowledge management to summarize data and optimize content delivery based on customer context.
- Design customer journeys that blend digital and human touchpoints. Monitor interactions to identify friction, allowing users to switch to human support for complex or high-value issues.

Sample Vendors

Amdocs; Ericsson; Huawei; NEC (Netcracker), Nokia, Oracle; ServiceNow; Salesforce

Gartner Recommended Reading

2025 Top Trend: Rise of CSP B2B Self-Service Capabilities

Market Trend: CSPs Increase Sales to SMBs With Human-Augmented Digital Customer Journeys

CSP CIO Benchmarks for Platform Prioritization in 2025

B2B Customers Choose Self-Service but Need More Guidance to Resolution

How CSPs Can Achieve Maximum Growth From SMBs in 2025

AI Security in ECS

Analysis By: Jon Dressel

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

AI-powered security in enterprise communication services (ECS) leverages advanced AI, machine learning (ML), generative AI and agentic AI to automate real-time threat detection, investigation and response across diverse security data sources. This empowers communications service providers (CSPs) to proactively identify and mitigate sophisticated cyberattacks, enhancing zero-trust security posture and optimizing security operations with adaptive automation.

Why This Is Important

AI-powered security is critical in today's communication landscape due to ever-evolving cyberthreats. Traditional security solutions cannot match the speed and scale of modern attacks. AI-powered security provides these advantages by shifting from a reactive posture to a proactive, intelligence-driven defense:

- Automates threat detection and response
- Proactively identifies attacks
- Offers continuous monitoring and threat hunting
- Reduces false positives
- Enhanced security visibility and decision making

Business Impact

AI-powered security can enhance the security posture of CSPs through improved business continuity and reduced security costs via increased efficiencies while reducing operational risk. AI-powered threat detection and response offerings provide proactive threat identification and mitigation, minimizing the risk of successful cyberattacks, leading to a more secure communication environment. This reduces the potential for data breaches and financial loss and protects the organization's reputation.

Drivers

- **Expanded threat landscape with generative and agentic AI:** Threat actors are increasingly leveraging GenAI and agentic AI tools for automated phishing campaigns, deepfake social engineering and crafting zero-day exploits. This evolution necessitates advanced AI-driven detection mechanisms capable of identifying known attack patterns and proactively recognizing novel, AI-generated and agent driven threats.
- **The explosion of data:** The volume of data generated through communication channels is growing exponentially. This data deluge presents both challenges and opportunities. While it can be overwhelming for traditional security tools, AI excels at processing and analyzing these vast datasets.
- **Advancements in AI and ML:** AI is undergoing rapid advancements, with breakthroughs in areas like agentic AI, deep learning and natural language processing. These advancements translate into more sophisticated AI-powered security solutions with improved capabilities for threat detection, anomaly identification and automated response.
- **Advanced explainability and transparency:** Continuous advancements in explainable AI (XAI) are addressing the historical "black box" issue. Organizations are expected to adopt new standards for transparency, leveraging models that provide real-time insights and post-incident audits on decision-making processes. This not only builds trust but also ensures compliance with increasingly stringent regulatory requirements.
- **Growing regulatory landscape:** AI regulations like the EU Artificial Intelligence Act (EU AI Act) and Japan's Basic Act on the Advancement of Responsible AI are placing stricter requirements on how organizations collect, store and use user data. AI-powered security solutions can play a crucial role in ensuring compliance with these regulations by providing organizations with better visibility into data flows and enabling them to detect and prevent unauthorized access or misuse of sensitive information.

Obstacles

- **Limited practical implementations:** While the potential of AI in security is widely recognized, many organizations hesitate to deploy these solutions due to integration challenges with legacy systems, operational complexity, and a lack of in-house expertise to manage and maintain AI-driven security tools. This slows real-world adoption, regardless of the technology's theoretical benefits.
- **Overpromising and underdelivering:** Some vendors exaggerate the capabilities of their AI security solutions, creating unrealistic expectations for buyers. However, many vendors have recently begun to set more realistic expectations by accurately describing their progress.
- **The "black box" problem:** The inner workings of some AI models are often unclear, complicating understanding of their decision-making processes. Recent advancements in next generation XAI address these issues, shifting focus toward new best practices and technologies that promote trust through transparency and ethical decision-making.

User Recommendations

CSP product leaders should:

- Collaborate with vendors and other CSPs to develop standards and best practices for AI-powered security solutions. This will ensure consistent performance, improve transparency and facilitate seamless integration with existing infrastructure.
- Invest in the development of XAI techniques. XAI provides insights into how AI arrives at decisions, fostering trust and enabling human oversight.
- Encourage collaboration and AI security information sharing among organizations, including other CSPs, researchers and developers.
- Invest in ongoing R&D to improve the capabilities of AI-powered security solutions by allocating dedicated resources to research teams focused on emerging threats and new detection techniques.
- Bridge the skills gap needed for successful AI security implementation by providing targeted training programs and hands-on workshops for internal security teams.
- Establish rigorous security benchmarking and testing procedures for AI-powered security solutions.

Sample Vendors

Cisco; CrowdStrike; Darktrace; Deepwatch; Ericsson; McAfee; Nokia; OneLayer; Palo Alto Networks; SentinelOne

Gartner Recommended Reading

Generative AI Adoption: Top Security Threats, Risks and Mitigations

Emerging Tech: AI Vendor Race: The Rise of AI-Based Predictive Threat Intelligence

AI Vendor Race: GMs: Win the AI Security Battle With an AI Security Platform

Implement AI Security in the Generative AI Workflow

NaaS

Analysis By: Jonathan Forest, Andrew Lerner

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Network as a service (NaaS) is a standardized and automated delivery model for network products and services. NaaS providers own and operate the offering, with the primary objective of simplifying full life cycle network operations, inclusive of equipment refreshes and capacity scaling. While not a market, it combines hardware, software and management into a consumption- or subscription-based opex pricing model. Many vendors promote offerings as NaaS, with few meeting the definition.

Why This Is Important

NaaS is overhyped, as vendors are positioning a wide range of network products and services as NaaS, but rarely meet the formal definition. The main objective of enterprises interested in NaaS is to simplify full life cycle network operations and, to a lesser extent, deliver a more flexible consumption model. It also offers organizations an asset-light-model option for those who don't want to own infrastructure.

Business Impact

Customers seeking NaaS are looking to simplify their network operations with a flexible consumption model. NaaS provides enterprises with agility, defined service delivery quality, automation, and end-to-end full life cycle management — with up/down scalability and adaptive billing. NaaS providers' goal is to offer alternative network sourcing options with a managed opex model, where customers don't own the equipment.

Drivers

- Enterprises are interested in a service offering where simplified life cycle network operations are delivered via an opex-friendly pricing model. The rise of NaaS could potentially disrupt campus networking, data center switching and WAN markets, for both on-premises or cloud-based network functions.
- Enterprises primarily see NaaS as an option for more opex-based pricing, with a "pay-for-what-is-used" model. In short, customers who have more available opex budget and less capex budget.
- Some enterprises see NaaS as a more flexible option to supply equipment and connection services for temporary locations.
- Enterprise buyers seek a focus on their end users and applications for improved service delivery quality and automation, and a more predictable customer experience.
- NaaS provides a simpler, turnkey network consumption model for smaller organizations.
- NaaS is seen as an asset-light model where the customer doesn't own the equipment.
- Built in network refreshes and software updates ensure functionality is up to date.
- This type of offering is attractive to customers who are familiar with and open to the cloud consumption model.
- Customers who require dynamic shifts in networking resources may favor NaaS.
- NaaS may be helpful to organizations that lack network operations resources and specific skill sets.

Obstacles

- Many provider offerings are limited to pricing/licensing changes, which isn't true NaaS.
- Some organizations view leasing as a form of NaaS, which has been around for decades.
- Many enterprises view NaaS primarily as consumption-based pricing and overlook the operational benefits.
- Most enterprises prefer flat-rate predictable pricing.
- NaaS is often more expensive than more traditional capex-based pricing models.
- Enterprises entering into NaaS agreements relinquish control and face complete replacement of product components upon contract exit.
- Large, established vendors have been reluctant to prioritize NaaS offerings due to the risk of impacting the revenue of their existing installed base.
- NaaS is often confused with network on demand delivered by carriers.
- NaaS is not a market, but often is referred to as such. The NaaS term is often misused to the point of it becoming nondescriptive.
- NaaS is not attractive for customers who have more capex budget and less opex budget.

User Recommendations

- Exercise caution with NaaS due to confusion created by the provider community. Expect that most offerings marketed as NaaS don't actually align with true NaaS principles.
- Prioritize network operations benefits of NaaS, rather than pricing flexibility, when evaluating vendors.
- Choose NaaS offerings when you have limited resources and are looking for a turnkey SLA-backed network solution priced as opex with no asset ownership.
- Choose NaaS offerings when you require a high SLA and/or have limited internal resources to meet the desired SLA.
- Where there is a concern of vendor lock-in, retain network design control by separately procuring equipment as an operating lease and adding managed network services.
- Calculate before-and-after-NaaS ROI by capturing all in-scope costs and uniformly comparing proposals to identify the differences.
- Avoid NaaS if you sweat network assets beyond a typical life cycle. This will effectively increase the price when compared to traditional capex models.

Sample Vendors

Alkira; Join Digital; Megaport; Meter; Nile; Verizon

Gartner Recommended Reading

What Is NaaS, and Should I Adopt It?

Early NaaS Pricing Lessons to Drive Adoption

Magic Quadrant for Managed Network Services

I&O Platforms Primer for 2025

Market Guide for Platform-Native Consumption Services

Market Trend: CSP NaaS Offerings for Enterprise Networking

eSIM

Analysis By: Pablo Arriandiaga

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

The embedded SIM (also called eSIM or eUICC) is a programmable subscriber identity module (SIM) that is physically embedded into a mobile or IoT device. If embedded into an SoC, it becomes an iSIM. It is designed to remotely manage multiple CSPs' profiles and be compliant with GSMA specifications. An eSIM is provisioned over the air (OTA) with operator credentials, giving users the ability to change providers. Dominant applications include international roaming and IoT connectivity.

Why This Is Important

eSIM standardizes global mobile and IoT connectivity, enabling organizations to scale efficiently while reducing operational costs. As leading smartphone and wearable OEMs expand eSIM support, consumer adoption is accelerating. In the IoT domain, eSIM eliminates the need for physical SIM logistics, facilitates remote provisioning, and ensures devices are ready for use out of the box — a process now significantly accelerated and simplified by the transition to the new GSMA SGP.31/32 IoT standard.

Business Impact

- **Consumer devices:** Enables users to seamlessly switch operators over the air, allowing wearables to function as independent, connected devices.
- **Enterprise and travel:** Facilitates local-rate global connectivity, reduces roaming costs by up to 90%, and centralizes cellular expense management.
- **IoT:** Streamlines global deployments with a single SKU, simplifying logistics, remote activation, and supply chain management.
- **Security and compliance:** Reduces SIM theft, cloning risks and supports compliance with local KYC and data rules.

Drivers

- The eSIM shipments in 2025 were 605 million reflecting an 18% year over year (YoY) increase according to the Trusted Connectivity Alliance (TCA), maintaining the double-digit growth seen in the previous year. Consumer adoption grew 43% YoY.
- Leading device manufacturers — including Apple and Samsung — now offer eSIM support across their latest smartphones and wearables. Over the past year, Chinese brands such as Xiaomi, Vivo, Huawei, HONOR, and Oppo have continued to expand their portfolios of eSIM-compatible devices. Notably, U.S. versions of Apple's iPhone 14 and later, as well as the Google Pixel 10 series, have eliminated the physical SIM slot and rely exclusively on eSIM technology, positioning North America as the region with the strongest eSIM adoption.
- Travel and roaming: Enterprises and consumers use eSIMs based on the SGP.22 standard to easily access local connectivity abroad, avoiding high roaming fees and permanent roaming restrictions. Vendors are launching enterprise-grade eSIM solutions that include integration with unified endpoint management (UEM) platforms, enhancing control and security for corporate travelers.
- New B2B2C Channels: Industries like banking, retail, and travel are embedding eSIM connectivity via APIs to enhance loyalty and offer branded digital services.
- In IoT, the estimated adoption of eSIM among vendors participating in the Magic Quadrant for Managed IoT Connectivity Services, Worldwide is approximately 22% of their installed base. Automotive leads eSIM adoption, while uptake in utilities and logistics has lagged. SGP.32 launch in 2026 is expected to drive broader adoption across more industry verticals. The SGP.32 eSIM standard for IoT streamlines remote provisioning, giving enterprises greater control and paving the way for large-scale IoT deployments.
- Government mandates (EU, India) and regulatory pressure to lower roaming costs and enforce local connectivity laws are accelerating eSIM adoption for greater choice, security, and interoperability.

Obstacles

- **Standardization confusion:** The shift from legacy M2M standards (SGP.02) to SGP.32 is creating uncertainty around interoperability, security, and hardware compatibility. Delays in the standard's launch, originally expected last year, have also created uncertainty among organizations.
- **Integration complexity:** Integration complexity in eSIM and IoT orchestration creates major challenges for MNOs, MVNOs, and consumers, with device OS changes, multivendor management, and secure remote profile updates adding supply-chain risks and operational overhead.
- **Security concerns:** The shift to eSIM expands the attack surface, exposing organizations to risks such as foreign hardware, cloud-based threats, firmware vulnerabilities, and supply-chain compromises.
- **Market awareness:** Many consumers and enterprises lack awareness of eSIM benefits outside of travel, as most MNOs are not actively promoting the technology in these segments.
- **Regulatory changes:** Regulatory changes may delay operator rollouts or require costly eSIM solution adjustments.

User Recommendations

- **Enterprises:** Assess CSP and MVNO offerings based on global coverage, supported standards (such as SGP.32 readiness), NB-IoT compatibility, and interoperability with unified endpoint management and connectivity platforms.
- **OEMs:** Integrate eSIM into devices that benefit from frequent carrier switching or remote provisioning, and collaborate with GSMA and CSPs to ensure seamless out-of-the-box connectivity.
- **CSPs:** Leverage eSIM flexibility to develop innovative service bundles — such as combining mobile plans with wearables or travel connectivity — to attract frequent travelers and improve customer retention.
- **MVNEs:** Use API-driven eSIM platforms to deliver "MVNO-in-a-box" solutions, enabling non-telco brands like Fintech and travel to embed mobile connectivity and generate new revenue.
- **IoT providers:** Accelerate SGP.32 testing to enable simplified remote provisioning, and integrate eSIM orchestration into unified platforms to ensure resilient global coverage and prevent vendor lock-in.

Sample Vendors

1GLOBAL; Aeris Communications; Amdocs; Eseye; eSIM Go; Gigs; IDEMIA; Kigen; Thales; Wireless Logic

Gartner Recommended Reading

Magic Quadrant for Managed IoT Connectivity Services, Worldwide

Critical Capabilities for Managed IoT Connectivity Services, Worldwide

Market Guide for IoT Mobile Virtual Network Enablers

Market Share: PCs, Tablets and Mobile Phones, Worldwide, 3Q25

LEO Satellite Communication Services

Analysis By: Peter Kjeldsen, Mohini Dukes

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Low Earth orbit (LEO) satellites operate at altitudes under 2,000 km, less than 4% of the distance of traditional communication satellites. Connections to LEO satellites use less power, support low latency and deliver data faster. However, coverage requires a multitude of satellites, most of which will have limited lifespans. Some providers have launched LEO satellites for broadband services, and others target direct-to-device (D2D) and low-speed/low-power Internet of Things (IoT) connectivity.

Why This Is Important

LEO satellite services have reached commercial scale, with Starlink surpassing 10 million subscribers, Eutelsat OneWeb serving enterprises globally, and Amazon Leo and SatNet offering previews testing with wider rollout planned during 2026. Falling launch costs, ubiquitous availability, low latency, and high throughput make LEO a credible complement to terrestrial networks — closing coverage gaps in maritime, aviation, remote, and rural markets and offering resilience via backup connectivity.

Business Impact

LEO satellite communication services:

- Offer ubiquitous connectivity and D2D services reaching enterprises, airplanes, ships, sea platforms, ground transportation and consumers in remote areas.
- Offer nonterrestrial redundancy paths that can increase network resiliency for enterprises.
- Allow CSPs to extend coverage without terrestrial infrastructure investment.
- Represent a disintermediation risk for CSPs from constellation operators pursuing direct enterprise relationships for connectivity and D2D services.

Drivers

- The LEO satellite communication market is seeing rising demand for services, with extensive ongoing and newly announced investments. Starlink and Eutelsat both are offering commercial broadband services today, Amazon Leo is at the enterprise preview stage and plans to add D2D capabilities via the announced acquisition of Globalstar and Telesat and at least two Chinese constellations will likely launch new broadband services in the coming years.
- LEO satellite communication services target various use cases, including broadband access, IoT access, D2D, supplementary coverage from space (SCS) aka space-based infrastructure (SBI) and wireless infrastructure backhaul. They also apply to more vertically specific services, including maritime, aviation, military and government use cases (see Market Trend: Emerging Use Cases for LEO Satellite Communication Services).
- The current geopolitical environment has increased the focus on network resilience, and here LEO broadband services offer nonterrestrial backup for terrestrial services.
- Wireless backhaul via LEO satellite can extend cellular coverage into remote areas that previously were economically unviable because of a lack of backhaul options.
- The 3rd Generation Partnership Project (3GPP) is defining the regulatory framework to allow nonterrestrial networks to be an integral part of 5G and 6G infrastructure. This includes SCS that enables LEO satellite providers and mobile operators to partner around delivering satellite connectivity directly to handsets. SCS initially targets narrowband (IoT and messaging) but will evolve to also offer voice and data (see Emerging Tech Impact Radar: NewSpace Technologies).
- Narrowband LEO satellites serve distinct IoT requirements for bandwidth, latency and throughput, focusing on low cost and low power to enable global asset monitoring and tracking.
- Cloud service providers will incorporate LEO services into new bundles and services, for example, offering connectivity for remote sites or as part of network resilience. Many have already made announcements that range from developing strategic partnerships with LEO satellite operators to reselling LEO services.

Obstacles

- Cost and performance, compared with alternative technologies, will limit adoption, except in areas with few or no competitive alternatives.
- Shortage of heavy-lift launch vehicles is a primary short-term limiting factor for new entrants.
- The need to continually refresh constellations implies ongoing operating costs for LEO constellation owners.
- Some buyers prefer not to use constellations they perceive to be under certain political controls.
- Country-level regulations (e.g., spectrum control) limit services in some areas and complicate maritime and aviation use cases.
- Satellite capacity and performance limitations result in capacity shortage in certain areas.
- Visibility of a significant proportion of the sky is required to track satellites, which impacts opportunities in some urban areas and in dense forests.
- Satellites and ground stations are cyber-physical systems with large attack surfaces. Cybersecurity frameworks and standards are only emerging.
- Medium Earth orbit satellite services can offer alternatives to LEO services.

User Recommendations

- Consider LEO satellite services as a nonterrestrial backup for terrestrial services, and consider how agile provision of LEO satellite services can augment existing plans for emergency response scenarios.
- Evaluate potential geopolitical implications of procuring LEO services from any given provider.
- Exploit the rapid development of LEO services by adding satellite connectivity to strategic workforce and business planning.
- Protect investments by validating your provider’s technical and financial ability to launch and maintain its constellation.
- Assess compatibility of on-premises provider equipment and be ready to replace proprietary equipment when changing providers.

Sample Vendors

Amazon; China Satellite Network Group; E-Space; Eutelsat OneWeb; Shanghai Spacesail Technologies; SpaceX; Telesat

Gartner Recommended Reading

Market Guide for Low Earth Orbit (LEO) Satellite Communication Services

Market Trend: Emerging Use Cases for LEO Satellite Communication Services

Forecast: LEO Satellite Communications Services, Worldwide, 2024-2029, 2025

Forecast Analysis: LEO Satellite Communications Services, Worldwide

Integrate LEO Satellite Connectivity to Enhance Network Resiliency

Rich Communication Services

Analysis By: Lisa Unden-Farboud, Ajit Patankar

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Rich Communication Services (RCS) is the GSMA messaging protocol used as a more feature-rich alternative to SMS/Multimedia Messaging Service (MMS) for person-to-person (P2P) and application-to-person (A2P) mobile device messaging. It supports rich, interactive messaging capabilities, like custom branding, video calling, multimedia sharing, group chat, delivery/read receipts and service discovery. The intent is for RCS to be carrier-supported and available on any network and any device.

Why This Is Important

RCS offers a richer and more affordable messaging alternative to SMS. Enterprises looking for an effective customer experience find RCS to be a great fit due to competitive pricing when compared with WhatsApp and a richer feature set than SMS. Moreover, Apple's support for RCS since 2024, with the iOS 18 release, has made RCS messaging between Android and iOS devices a reality and made its reach global for the entire smartphone userbase.

Business Impact

RCS offers a rich messaging experience, letting enterprises engage users with interactive features such as emojis, media, buttons, maps and carousels. RCS Business Messaging also supports branding and verified business communication, boosting trust, security and click rates compared to SMS, especially for marketing and transactional messages. Its primary use for now is as an SMS upgrade for OTPs and notifications, due to increased brand trust, security and competitive pricing.

Drivers

- Many telecom operators and device OEMs globally have adopted the GSMA's Universal Profile for RCS, enabling cross-operator messaging. Universal Profile support is mandated for 5G, so as 5G rolls out, global RCS interoperability is becoming reality.
- Google's Jibe platform is the dominant RCS enablement used by carriers globally. Jibe simplifies RCS deployment by supporting Universal Profile and offering cloud-hosted infrastructure, allowing operators to quickly launch and scale RCS services. Jibe Hub provides interoperator connectivity, allowing operators to connect easily to the global RCS network.
- Vendors such as Mavenir and Openmind Networks also offer RCS and Universal Profile as an alternative to Jibe. They provide infrastructure software for mobile carriers to deploy in their own networks, as part of messaging or 5G core strategy, giving the carriers more control over data, traffic and revenue compared to third-party platforms like Google Jibe.
- RCS adoption for A2P messaging is surging in markets such as India, U.S., China and Brazil. Vendors including those that provide CPaaS have launched RCS hubs, enabling enterprises to easily use RCS for messaging campaigns, with SMS fallback for unsupported devices or carriers. This lets enterprises upgrade from SMS and use RCS's rich, conversational features at the same time.
- Adoption is expanding rapidly in Brazil, Mexico, parts of Europe, South Africa, South Asia (notably India) and the U.S., driven by increasing smartphone use and 5G deployment which enhances carrier-driven rich messaging as an alternative to WhatsApp/OTT messaging.
- Apple began supporting RCS interoperability for Business Messaging with the October 2024 release of iOS 18.1, allowing enterprises to reach users on supported Apple devices where enabled by operators.
- RCS Business Messaging lets enterprises add logos and rich features to communications, creating a branded, personalized experience that builds trust and can increase customer engagement.

Obstacles

- Substitutes with higher user adoption than RCS (e.g., WhatsApp is widely adopted [over 3 billion global users and over 95% adoption in markets like Brazil, India and Europe]).
- SMS is a more reliable solution for simple messages (OTP, notifications and reminders) considering that RCS primarily requires active internet connection for the users to receive messages. For critical use cases, enterprises still want to rely upon SMS or are looking at fallback options with RCS. The value of RCS may prove greater for the branding verification that organizations don't get on SMS.
- Current trends suggest that RCS for A2P messaging is priced at or slightly above SMS for basic messages and higher than SMS for rich/interactive content. For rich interactive messages, RCS can be priced higher compared to WhatsApp, depending on country and carrier fees. The higher price may hinder enterprise and user adoption.
- Carrier support for A2P RCS, while growing, still lags behind the universal support for SMS.

User Recommendations

- Collaborate with device OEMs and OS vendors such as Google and Apple to ensure RCS support across your user base.
- Experiment with RCS pricing to attract enterprises compared to SMS and OTT channels, ensuring ROI through use cases like marketing and customer engagement.
- Engage with RCS ecosystem stakeholders, including CPaaS vendors, to boost enterprise adoption through co-marketing, co-selling, customer education and promotional pricing.
- Enhance value by offering tools like bots, agent interfaces and AI on RCS for improved customer experience and functionality, surpassing SMS and WhatsApp, for example, in sales conversion rate.

Sample Vendors

Airtel; AT&T; Claro; Ericsson (Vonage); Google; Infobip; MTN; Orange, Sinch; Telefónica; T-Mobile; Twilio; Verizon; Vivo; Vodafone

Gartner Recommended Reading

Magic Quadrant for Communications Platform as a Service

Critical Capabilities for Communications Platform as a Service

Climbing the Slope

Communications Platform as a Service

Analysis By: Lisa Unden-Farboud, Ajit Patankar

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Communications platform as a service (CPaaS) is a cloud-based platform enabling businesses to embed communications capabilities (like voice, SMS, email, messaging apps and video) into their workflows. CPaaS also provides conversational capabilities, security, authentication and automation. CPaaS delivers omnichannel programmable experiences for digital customer engagement. From 2026, it aims to offer deeper capabilities such as CJA, personalization and omnichannel engagement driven by AI and 5G.

Why This Is Important

CPaaS lets organizations integrate communication channels into workflows by APIs or low-code/no-code tools, enabling those with modest IT skills to deploy SMS, voice, email, rich messaging and chat securely and compliantly for use cases from transactional notifications to customer service and marketing. Digital natives and enterprise developer teams can build complex workflows too, adding features like video, payments, web chat, marketing campaigns, RCS, and advanced channels such as WhatsApp.

Business Impact

CPaaS transforms enterprise IT by enabling developers to build communications capabilities into enterprise systems. An ecosystem of APIs, SDKs and documentation gives low-cost tools for improving operational efficiency and customer experience. Vendors now offer visual builders so business analysts with little to no coding skills can build simple workflows and integrate AI. Most organizations start by deploying CPaaS for a single business unit use case, from which it is quickly adopted elsewhere.

Drivers

- Organizations continue to operationalize their customer experience (CX) using no-code/low-code communications capabilities from CPaaS vendors that offer composable capabilities and templated vertical-specific solutions.
- Visual builders and low-code application platform (LCAP) tools in general continue to be rolled out in the market to allow the participation of noncoding business analysts. This expands the total available market (TAM) to users building simple workflows or making modifications to existing workflows.
- Customer service leaders increasingly look beyond SMS and voice as basic forms of communications with customers and continue to expand adoption of email, WhatsApp, RCS, and video. Meanwhile, they are also making use of advanced capabilities such as security, authentication, conversational capabilities with AI, and payments. This, in turn, enables organizations to build more complex workflows, yielding a better, more secure and personalized customer experience.
- The market is witnessing the increasing need for bots — mainly AI/generative AI (GenAI)-based and agentic AI customer assistant capabilities, incorporating data from customer data platforms (CDPs) and driven by advanced campaign management — to be incorporated in their workflows. CPaaS provides these technologies and enables their integration with enterprise IT systems.
- CPaaS vendors are doubling down on building systems integrator (SI) partnerships focused on complex vertical use cases. This provides a scaling opportunity as the SIs have strong CIO relationships for building advanced IT workflows.

Obstacles

- The CPaaS landscape is complicated with new vendors and others repositioning their product offerings. In such a crowded field, many CPaaS vendors struggle with brand awareness. Many IT decision makers are not sure which CPaaS providers are best suited to align with.
- Some CPaaS providers' CDP and contact center as a service (CCaaS) capabilities are still basic and evolving.
- The broader ecosystem of customer service providers, such as CCaaS, CRM customer engagement center (CEC), conversational AI platforms, digital customer services (DCS) and hyperscalers, is expanding their digital capabilities and competing in this space.

- Market adoption of several mature CPaaS offerings like SMS, 2FA and number anonymization is strong, but they have poor margins. CPaaS vendors need greater adoption into the newer capabilities — WhatsApp, RCS and conversational capabilities with AI — to evolve and grow further.

User Recommendations

- Implement first with simple solutions based on SMS, 2FA, number anonymization and voice if you have modest IT skills or a bundled solution with seamless integration into workflows.
- Explore advanced communications such as messaging apps (e.g., WhatsApp, RCS), payments and e-commerce, if you have strong IT skills. CPaaS is viable for all business sizes given the shift toward horizontal- and vertical-specific/templated solutions available to operationalize customer experience.
- Explore opportunities to adopt CPaaS across the entire business, starting with a single BU then expanding to others — like HR and operations for maximum benefits.
- Expose the organization's developer workforce to CPaaS, and use AI-augmented development where required to fully leverage CPaaS for competitive edge. IT core competency is not a luxury but a necessity for survival.
- Hire SIs or boutique CPaaS development firms for initial projects. Have your IT team learn from them, so you can build your own core competency.

Sample Vendors

Bandwidth; Infobip; Mitto; Proximus Global; Sinch; Tanla; Twilio; Vonage

Gartner Recommended Reading

Magic Quadrant for Communications Platform as a Service

Critical Capabilities for Communications Platform as a Service

Forecast Analysis: Communications Platform as a Service, Worldwide

Seize Key Trends in CPaaS to Improve the Customer Experience

Product Leader Strategies to Boost CPaaS Selection

Managed SD-WAN Services

Analysis By: Gaspar Valdivia

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Managed software-defined WAN (SD-WAN) services refer to the outsourced operational management of enterprise networks that use SD-WAN technology. Typically delivered by communication service providers (CSPs), system integrators or specialized managed service providers, they include the design, deployment, and 24/7 monitoring of edge devices and WAN links, usually backed by SLAs. Features include maintenance, troubleshooting, real-time analytics, dynamic traffic routing, and integrated security.

Why This Is Important

Managed SD-WAN has become central to many enterprise networks as businesses shift to cloud-centric operations and remote work. Providers deploy these services for enterprises migrating, entirely or partially, from legacy Multiprotocol Label Switching (MPLS). Beyond enabling agility, performance, cost reduction, and operational simplification, managed SD-WAN offerings are now adding AI capabilities for smarter network management.

Business Impact

Managed SD-WAN delivers major benefits for enterprises requiring secure, high-performance connectivity at multiple sites. Enterprises can streamline network operations using third-party-provided runtime management of the SD-WAN network, so internal IT teams can focus on other strategic initiatives. Often, organizations using third-party-provided managed SD-WAN gain enhanced performance and cost-efficiencies compared with hiring and training specialized in-house staff to manage the network.

Drivers

- Outsourcing network runtime management to third-party providers enables internal IT personnel to pivot toward high-value strategic initiatives rather than daily operational maintenance.
- Managed service providers mitigate technical complexity during architectural design and rollout — particularly for MPLS-to-SD-WAN migrations — minimizing configuration errors and accelerating time to market with flexible co-management or fully managed models.
- Proactive 24/7 monitoring and incident remediation, increasingly enhanced by AIOps, ensure sustained network performance and reliability governed by comprehensive service-level agreements (SLAs).
- Advanced service portals and centralized orchestration provide deep visibility into application health and traffic patterns, facilitating data-driven decision making and rapid resolution of network anomalies.
- Managed offerings streamline the integration of heterogeneous transport types — including broadband, 5G, and low Earth orbit (LEO) satellites — leveraging dynamic path optimization to ensure high availability and resilient connectivity.
- Often, service providers offer optimized cloud on-ramps to IaaS and SaaS environments, delivering high-performance, scalable connectivity without requiring significant upfront capital expenditure.
- Third-party-provided life cycle management of software updates and security patches can help keep enterprise networks future-ready while mitigating the risks of technical obsolescence.
- Leveraging provider expertise helps organizations navigate complex data sovereignty requirements and industry-specific regulatory frameworks (e.g., the Payment Card Industry Data Security Standard [PCI-DSS], or the Health Insurance Portability and Accountability Act [HIPAA]), reducing overall compliance risk.

Obstacles

- Upfront implementation costs, license overages, and recurring fees may reduce ROI, making DIY models more economical for organizations with internal expertise.
- Ambiguous SLAs or insufficient service credits can expose enterprises to inconsistent performance, lowering outsourcing value.
- Rigid portfolios and limited interoperability between vendor functions or carriers restrict flexibility and architectural choices.
- Underdeveloped broadband infrastructure or limited transport options negate performance benefits of SD-WAN.
- The rapid industry transition toward integrated secure access service edge (SASE) frameworks risks making stand-alone managed SD-WAN offerings less competitive.
- The emergence of “coffee-shop networking” shows a shift toward prioritizing universal, secure internet access over traditional site-centric WAN architectures for hybrid work.
- Advances in AI-driven autonomous management by OEMs are making DIY SD-WAN more accessible for smaller teams, disrupting the traditional managed services value proposition.

User Recommendations

- Provide a diverse portfolio of SD-WAN technology options, complemented by co-management capabilities accessible via robust service portals and APIs.
- Leverage AIOps and agentic AI to systematically automate Day 0, Day 1, and Day 2 operations, prioritizing predictive maintenance and autonomous incident remediation.
- Deliver high-value service bundles that integrate managed SD-WAN with complementary solutions such as WAN transport or optimized cloud connectivity.
- Transition from stand-alone managed SD-WAN architectures toward comprehensive managed SASE frameworks.
- Implement flexible and transparent pricing models, ranging from traditional fixed monthly rates to scalable, consumption-based network-as-a-service (NaaS) models, to suit varying enterprise preferences.
- Establish full accountability through end-to-end SLAs.
- Mitigate enterprise concerns regarding integration complexity and ROI by providing evidence-based case studies and clearly articulated business benefits.

Sample Vendors

Accenture; AT&T; Colt; Deutsche Telekom; HCLTech; MetTel; Microland; Tata Communications; Wipro Enterprises; XTIUM

Gartner Recommended Reading

Magic Quadrant for Global WAN Services

Market Trend: Dedicated Internet Access, Worldwide, 2025

Market Trend: CSP NaaS Offerings for Enterprise Networking

MDR Services

Analysis By: Andrew Davies

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Managed detection and response (MDR) services provide customers with remotely delivered, human-led, modern security operations center (SOC) functions. These allow organizations to rapidly detect, analyze, investigate and actively respond through threat disruption and containment. MDR providers offer a turnkey experience using a technology stack that covers endpoint, network, logs and cloud. This telemetry is analyzed by the provider's experts, skilled in threat hunting and incident management.

Why This Is Important

The cyberthreat landscape is in a constant state of change, and the complexity of attacks against organizations is escalating faster than ever before with the use of AI-driven attacks. Given the changes in the threat landscape, scaling your security operations practice is vital. MDR services provide an effective means of scaling your workforce for security operations. Most organizations lack the resources, budget or appetite to build and run their own 24/7 SOC function, required to help them protect and defend against attacks that increasingly impact and cause more damage to operations. MDR services enable organizations to mature their threat detection and response coverage.

Business Impact

MDR services combine people, process and technology, translating security issues into business-focused risks, impacts and outcomes, reducing complexity and allowing increased security maturity through turnkey adoption. Organizations that have not invested in threat detection and response capabilities are at greater risk from the impact of cyberincidents. The challenge of finding, acquiring and retaining the necessary expertise and threat detection, investigation, and response products makes building an adequate internal capability onerous.

Drivers

- Buyers require fast adoption of mature capabilities that take a long time to build or buy, or are prohibitively expensive to operate. MDR delivers a turnkey solution for those wishing to quickly build and maintain threat detection investigation and response (TDIR) capability.
- MDR services enable organizations to focus on outcome-driven responses as they provide the expertise to interpret and deliver against a set of requirements. Ultimately, this delivers relevant and actionable business outcomes.
- MDR providers can help you extend your TDIR capabilities quickly to a broader range of new environments than is typically possible with smaller internal-only teams.
- MDR providers allow for remotely delivered mitigative response actions, enabling buyers to respond and alleviate issues faster and with less impact to their business, although the level of autonomy granted to vendors varies according to the trust level. With the improved access to MDR service providers' portals, clients can validate the response for some scenarios, and possibly execute it.
- Many MDR providers are expanding their offering beyond TDIR to include exposure management. This is a driver for MDR when buyers seek to better harmonize their TDIR practice with their exposure management practice.

Obstacles

- The vastly different approaches by providers to offer MDR services often cause buyers to question how to strategically engage a provider.
- Technology vendors with threat detection, investigation and response-capable solutions offer similarly named, but often more light-touch, overlay services, such as managed endpoint detection and response (EDR) and co-managed security information and event management (SIEM). This increases buyers' confusion.
- Misaligned expectations and a lack of effective internal processes to consume MDR outputs lead to performance issues with MDR service providers and failed engagements.
- Not assigning staff as the point of contact to the service can cause challenges. If not defined effectively, segmentation of operational responsibilities and building effective response processes usually leads to dissatisfaction with services.
- New AI-driven solutions promising to initiate measures for active containment or disruption of a threat or an exposure are in direct competition with MDR providers

User Recommendations

- Focus on outcomes, not technologies. Organizations underinvested in technologies capable of TDIR, such as EDR, should favor contract vendors that provide the tools and deliver the desired outcomes.
- Ensure that your MDR provider supports additional security services as your security maturity improves and business-driven risks change, so you don't need to add additional vendors at a later time. These services include exposure management and continuous threat exposure management (CTEM).
- Assess if the MDR service deliverables focus on completeness, actionability and options for service provider follow-up incident response and threat hunting activity.
- Examine co-managed security monitoring service offerings when adjacent capabilities are required to support the management and expansion of your own TDIR investments, such as EDR and SIEM.
- Buy MDR services that offer a migration path to more self-service in the future. Looking for vendors that have open communication channels with analysts and delivery teams can support that goal.
- Less mature organizations with lower security maturity can find quicker time to value with technology-driven MDR services.

Sample Vendors

Accenture; Arctic Wolf Networks; Critical Start; CrowdStrike; eSentire; Expel; Rapid7; ReliaQuest; Sophos

Gartner Recommended Reading

Peer Lessons Learned for Managed Detection and Response Service Implementation

Market Guide for Co-Managed Security Monitoring Services

Market Guide for Managed Detection and Response

Voice of the Customer for Managed Detection and Response

SASE

Analysis By: Andrew Lerner, Jonathan Forest, Neil MacDonald

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Secure access service edge (SASE) delivers converged network and security capabilities, including SD-WAN, secure internet access, secure SaaS access, firewall and zero-trust network access capabilities. SASE supports branch office, remote worker and on-premises secure access use cases. Primarily delivered as a service, SASE enables zero-trust access based on the identity of the device or entity, combined with real-time context, and security and compliance policies.

Why This Is Important

SASE enables modern digital business transformation, including work from anywhere, branch office transformation and the adoption of edge computing and cloud-delivered applications. It also dramatically simplifies the delivery and operation of critical network and security services via a cloud-centric management and delivery model. SASE reduces the number of vendors for secure access to one or two explicitly partnered vendors.

Business Impact

- SASE enables digital business use cases (such as branch office transformation and hybrid workforce enablement) with increased ease of use while reducing complexity.
- It allows I&O and cybersecurity teams to deliver consistent and integrated networking and network security services, supporting the needs of digital business transformation, edge computing and work from anywhere.

Drivers

- Digital workforce and branch transformation projects driven by the adoption of cloud-based services and an increasingly mobile workforce require secure access anywhere, anytime.
- Organizations desire to move toward a zero-trust security architecture while managing complexity.
- There are dozens of vendors who offer competitive SASE platform offerings that are prominently promoting and positioning their offerings to customers.
- SASE can reduce the deployment time for new users, locations, applications and devices.
- SASE enables a single way to set consistent policy enforcement across internet, web application and private application access, which reduces the attack surface and shortens remediation times.
- Enterprises want to simplify network and network security deployments via the reduction of policy engines and management consoles.

Obstacles

- Organizations that have not embraced cloud/SaaS are much less likely to benefit from a SASE architecture.
- SASE requires a coordinated approach across security, networking and digital workplace teams, which is challenging given refresh and renewal cycles, silos and staff expertise.
- A vendor's cloud footprint may prevent SASE deployments in certain geographies such as China, Africa, South America and the Middle East, which may be related to sovereign requirements.
- Concentration risk: Organizations cite both commercial and technological concerns over consolidating multiple technologies from a single vendor.
- It is challenging to justify SASE deployment solely from a financial/cost perspective.
- Agentic AI adoption shifts enterprise needs and may bypass decryption and inspection by SASE deployments, requiring new products to be deployed.

User Recommendations

- Involve both cybersecurity and network teams when evaluating offerings and roadmaps from incumbent and emerging vendors to ensure an integrated approach.
- Leverage renewals and refresh of SD-WAN, Firewall and VPN to update network and network security architectures.
- Avoid enabling SASE outcomes with more than two product vendors to avoid complexity and suboptimal performance.
- When implementing a dual-vendor SASE solution, use only vendor combinations with explicit integration including turnkey automation, visibility and, ideally, management and data plane integration.
- Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the number of vendors required.

Sample Vendors

Cato Networks; Check Point Software Technologies; Cisco; Cloudflare; Fortinet; Hewlett Packard Enterprise; Netskope; Palo Alto Networks; Versa Networks; Zscaler

Gartner Recommended Reading

How to Pick the Right SASE Platform

Magic Quadrant for SASE Platforms

Critical Capabilities for SASE Platforms

Managed IoT Connectivity

Analysis By: Pablo Arriandiaga

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Managed Internet of Things (IoT) connectivity services enable device and connectivity, data collection and analysis services necessary for connected solutions. For large organizations, managed IoT connectivity services are normally delivered fully managed, including dedicated help desk, and project and service management capabilities. For midsize and small organizations, they are frequently delivered as a self-service provided through a management portal, including Level-2 and Level-3 support.

Why This Is Important

The IoT market has shifted from basic connectivity to advanced, AI-driven life cycle management. Enterprises deploying millions of devices globally face rising cyberthreats, complex data regulations and roaming bans. Managed IoT connectivity services are essential, embedding proactive security, seamless IoT orchestration (cellular, satellite, low-power wide-area networks [LPWAN]), autonomous operations, and integration of eSIM SGP.32, 5G RedCap and private 5G.

Business Impact

From SMBs to large enterprises, organizations leverage managed IoT connectivity services to offload network complexity to a single accountable provider. While IoT platforms offer tools like orchestration and AI copilots for API integration, managed services deliver guaranteed SLAs, global hardware logistics and continuous life cycle support. This shifts operational risk, reduces total cost of ownership and ensures regulatory compliance, empowering enterprises to focus on their core business.

Drivers

- **Exploding Fleet Scale and Complexity:** IoT has become mission-critical for enterprises, fueling double-digit market growth year over year. The average year-over-year growth of connections among all participants in the Magic Quadrant for Managed IoT Connectivity Services is over 16%. To manage this scale, enterprises rely on managed services to handle operational complexity, global logistics and 24/7 monitoring of large device fleets.
- **Demand for Flexible and Hybrid Management Models:** Enterprises are moving away from rigid outsourcing toward hybrid models tailored to internal IT capabilities. Providers offer options from self-service portals to co-managed and fully managed operations, enabling enterprises to control SIM life cycle management while outsourcing global logistics and 24/7 fault resolution.
- **AI-Driven Life Cycle and Workflow Automation:** Managed service providers use agentic AI, generative AI (GenAI) copilots and no-code tools to increasingly automate life cycle management. This shifts the administrative burden from the enterprise, enabling proactive anomaly resolution and stricter SLA adherence with minimal enterprise IT involvement.
- **Outsourced Global Logistics and IoT Orchestration:** The eSIM SGP.32 standard enables a "single global SKU" logistics model. With API-driven bring your own connectivity (BYOC), providers serve as a single point of accountability — navigating permanent roaming bans, protecting enterprises from excessive tariffs and ensuring regulatory compliance worldwide.
- **Security by Design and Regulatory Compliance:** Mandates like the EU Cyber Resilience Act (CRA) and NIS2 Directive force enterprises to outsource risk. Providers offer managed zero trust network access (ZTNA), agentless firewalls and IoT SAFE to assume these compliance and monitoring burdens.
- **Single-Provider Hybrid Network Federation:** Demand for resilient coverage drives convergence of cellular, LPWAN, private 5G and satellite networks that are managed via unified contracts and support.

Obstacles

- **Inconsistent Global Service Delivery and Support:** While providers market unified global services, many providers still rely on local partner networks outside their core footprint. This leads to persistent disparities for IoT technologies, sourcing and logistics. Multinational enterprises often encounter inconsistent availability, fragmented management tools and variable technical support across regions.
- **Technology Fragmentation and Uneven Availability:** Despite efforts for unified global connectivity, commercial rollout of next-gen capabilities — like 5G SA, 5G RedCap and LEO satellites — remains fragmented. Enterprises encounter disparities in feature sets, regulatory compliance and governance, as access varies by geography, carrier maturity and provider integration.
- **Security Standardization Gaps:** The heterogeneity of IoT edge devices, hardware protocols and multibearer connections makes adoption of standardized, end-to-end security frameworks highly challenging across the ecosystem.

User Recommendations

- Mitigate inconsistent global delivery by requiring providers to demonstrate uniform service capabilities across all target regions. Request evidence of feature parity, equivalent local support and SLAs to prevent operational fragmentation when providers rely on local partners outside their core footprint.
- Prioritize vendors embedding agentic AI, machine learning, GenAI for predictive analytics, zero-touch provisioning and self-healing networks to reduce operational overhead.
- Evaluate vendors based on their IoT orchestration roadmap and readiness for global deployments and dynamic profile localization.
- Ensure security by demanding network-layer protections like ZTNA and device-level cryptography such as IoT SAFE and meeting evolving regulatory standards like CRA,NIS2 and sector-specific mandates.
- Consolidate hybrid network complexity by choosing providers that unify cellular, LPWAN, private 5G and satellite (NTN) under a single managed contract with centralized IT/OT support.

Sample Vendors

AT&T; Deutsche Telekom; KORE; NTT DATA Group; Orange Business; Soracom; Telefónica; Verizon; Vodafone; Wireless Logic

Gartner Recommended Reading

Magic Quadrant for Managed IoT Connectivity Services, Worldwide

Critical Capabilities for Managed IoT Connectivity Services, Worldwide

Market Guide for IoT Mobile Virtual Network Enablers

Peer Insights: Enterprises' Preferences for Managed IoT Connectivity Services

Market Guide for Embedded Security for IoT Connectivity

Market Guide for Satellite IoT Services

Entering the Plateau

Dedicated Internet Access

Analysis By: Gaspar Valdivia

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Dedicated Internet Access (DIA) is a high-speed internet access service that provides a direct, uncontended link to the internet, ensuring constant bandwidth and symmetrical upload and download speeds. This connection offers robust performance SLAs, reduced latency and enhanced security compared with contended broadband internet. Organizations typically rely on DIA for mission-critical operations requiring dependable high-speed internet connectivity.

Why This Is Important

Bandwidth needs are surging due to increased use of data-heavy applications, and traffic patterns are changing due to broad cloud adoption and AI workloads. Traditional private multiprotocol label switching (MPLS) services are often more expensive. As a replacement, DIA provides a dedicated, unshared connection with guaranteed symmetrical speeds and consistent performance. It outperforms shared broadband by offering financially backed SLAs for uptime and latency.

Business Impact

Enterprises leverage DIA to handle data-intensive workflows, cloud applications, and emerging AI workloads, ensuring mission-critical operations run uninterrupted. It delivers guaranteed symmetrical speeds and performance SLAs essential for real-time apps like VoIP and videoconferencing. Organizations across finance, healthcare, and other industry verticals rely on DIA for consistent, high-performance connectivity at a more affordable price point than equivalent MPLS connections, while remaining backed by SLAs.

Drivers

- DIA offers guaranteed, symmetrical bandwidth to support critical applications' performance, often at a lower price than comparable MPLS circuits.

- As data traffic increases, organizations require DIA's highly scalable, high-throughput, and low-latency backbone to support distributed AI inferencing and direct integration with multicloud environments.
- Because it provides a dedicated path, DIA reduces exposure to shared-network vulnerabilities. It acts as a deterministic underlay for SASE and zero-trust architectures, ensuring compliance and data protection.
- SD-WAN enables enterprises to use DIA as the premium underlay connectivity layer for mission-critical traffic. It is increasingly paired with 5G, LTE, or broadband failover to effectively manage overall network resilience, performance, and cost.
- Typically, DIA offers latency performance that enables better user experiences for real-time services, including VoIP and videoconferencing.
- Most CSPs' DIA offerings support API-driven provisioning, scalable capacity, and bandwidth bursting options to accommodate rapid growth and data-heavy traffic spikes.
- Compared with broadband internet, DIA's long-term ROI is realized through strict SLAs that guarantee greater uptime (typically ranging from 99.95% to 99.999%) and rapid repair times, reducing costly operational disruptions and preserving productivity.
- CSPs are pivoting investments from MPLS toward advanced internet backbones, internet access services, and development of ISP aggregation capabilities.

Obstacles

- Upfront provisioning and activation charges, fiber construction and inflexible multiyear contracts can deter smaller organizations, which must carefully evaluate budget constraints.
- DIA relies heavily on physical fiber. In underserved regions, limited infrastructure and right-of-way permits can delay installations by months, often requiring hybrid alternatives.
- Organizational buy-in can be difficult to secure in enterprises that operate in highly regulated markets or with very high security and data privacy requirements. These companies may show preference for an end-to-end private access and backbone service such as MPLS.

- Geopolitical considerations can influence decision making for connectivity services in favor of MPLS versus internet-based connections.
- For some organizations, the cost advantage in shifting from MPLS to DIA services may not give enough ROI to justify the risk of migration.

User Recommendations

Recommendations for CSPs and internet service providers:

- Highlight guaranteed bandwidth and symmetrical speeds as core value propositions, emphasizing how uncontended DIA supports heavy AI workloads, data gravity needs, and real-time services.
- Showcase DIA's reliability. Prove its dependability for mission-critical applications over broadband internet, with low latency and zero peak-hour congestion.
- Position DIA as an MPLS alternative. Articulate DIA's superior ROI and cost predictability compared to legacy MPLS networks.
- Enable NaaS and API scalability. Offer automated bandwidth bursting to seamlessly adapt to dynamic traffic spikes without complex overhauls.
- Provide transparent, detailed SLAs to ensure buyer trust in performance and uptime commitments.
- Bundle with SASE and hybrid underlay. Combine DIA with SASE, SD-WAN, and 5G or LEO satellite failover to deliver unified, highly resilient solutions that justify premium pricing.

Sample Vendors

AT&T; BT; Colt Technology Services; Deutsche Telekom; GTT Communications; NTT; Orange Business; Tata Communications; Verizon; Vodafone

Gartner Recommended Reading

Market Trend: Dedicated Internet Access, Worldwide, 2025

Market Trend: SaaS Adoption Growth Spurs CSPs to Deliver on Enhanced Connectivity

Market Opportunity Map: Enterprise Network Services, Worldwide

ZTNA

Analysis By: John Watts

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Zero-trust network access (ZTNA) provides secure network access. ZTNA creates an access boundary based on identity and dynamic device context that encompasses an enterprise user and privately hosted application or set of applications. The applications are hidden from discovery and access is restricted via a trust broker to a collection of named entities, which limits lateral movement within a network.

Why This Is Important

ZTNA enables adaptive user-to-resource segmentation based on least logical privileged access through a trust broker. It allows organizations to hide private resources from discovery and attack. It reduces the surface area for attack by obfuscating an organization's infrastructure and creating individualized "virtual perimeters" that encompass only the user, the device, and the resource.

Business Impact

ZTNA reduces the attack surface for the organization by logically separating the source user and device from the destination resources to mitigate full network access. This approach improves some user experience (UX) issues with static, network-based VPN routing and enables remote access flexibility with dynamic, granular, user-to-resource segmentation through adaptive access controls defined as zero-trust policies. Cloud-based ZTNA offerings improve scalability and ease of adoption for secure remote access.

Drivers

- When pursuing a zero-trust strategy, organizations seek a more precise and adaptive access and session control to private resources hosted in infrastructure as a service (IaaS).
- Organizations seek protection against attacks against vulnerable, exposed legacy VPN infrastructure.
- The rise of IaaS adoption and hybrid infrastructure requires more flexible secure remote connectivity to enable access directly to resources as opposed to static connections that are then routed to multiple destinations.
- Organizations have a need to connect third parties, such as suppliers, vendors, and contractors, to resources directly, without using a full-tunnel VPN to their networks or exposing resources directly to the internet in a DMZ.
- Organizations that undergo mergers and acquisitions need to be able to extend access to resources to acquired companies without deploying endpoints or interconnecting their corporate networks.

Obstacles

- ZTNA cost is roughly twice or three times that of traditional VPNs and is typically licensed per named user on a per-user/per-year basis.
- Cloud-based trust brokers may not extend policy enforcement points on-premises, limiting use cases compared to universal ZTNA offerings that offer distributed enforcement points.
- When implemented properly, ZTNA requires well-established user-to-application mapping, which is complex and difficult at scale. Organizations must map resource access for users and balance risk mitigation with complexity. Organizations may end up granting all users access to all applications or access that is too granular, which adds significant overhead to managing the product over the long term.
- Mature zero-trust implementations must continuously assess access based on context of user accounts and devices. Many organizations find this difficult to adopt at scale due to complicated troubleshooting and inconsistency of access controls based on fluctuating risk scores.

User Recommendations

- Enable resource-specific access with clientless ZTNA rather than full-tunnel network access for unmanaged devices.
- Based on the risk posture of the organization, start small with narrow, risk-based and dynamic access controls or wider access to fewer end users and refine over time.
- Align agent-based ZTNA vendor choice with security service edge (SSE) or SASE vendor choice to support the organization's zero-trust strategy.
- Unify access control policies when providers offer both on- and off-premises enforcement points with added IoT support to replace legacy technologies, such as network access control.
- Mitigate the risk of operational downtime with hot or cold standby options when the vendor has a single point of failure for connecting end-user devices to applications.
- Assess the need for separate products to address adjacent functionality, such as remote privileged access management, and to support nonuser devices, such as IoT and desktop-as-a-service alternatives. ZTNA does not solve all use cases.

Sample Vendors

Absolute Security; Appgate; Cisco; Cloudbrink; Cloudflare; Microsoft; Netskope; Palo Alto Networks; Zentera Systems; Zscaler

Gartner Recommended Reading

Implement Zero-Trust Network Access Through a Life Cycle Approach

Strategic Roadmap for Zero Trust Security Program Implementation

Quick Answer: How to Select a ZTNA Vendor Based on Use Case

Contact Center as a Service

Analysis By: Megan Fernandez

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Contact center as a service (CCaaS) is a cloud-based application service platform that enables organizations to manage multichannel customer interactions holistically with prepackaged applications that support the customer and employee experience. CCaaS solutions are used by organizations that need to manage front-office operations such as customer service, sales, support centers and employee help desks.

Why This Is Important

The CCaaS market is rapidly transforming, fueled by the infusion of generative and agentic AI. As customer expectations for effortless, real-time engagement continue to rise, CCaaS platforms are central to delivering self-serve and assisted service and support experiences through both digital and voice touchpoints. Application leaders can access integrated CCaaS solutions that combine omnichannel engagement, workforce management, AI powered chatbots, agent assist tools, and advanced analytics.

Business Impact

The business impact of CCaaS is broad and deep:

- **Smart automation:** GenAI and agentic AI drive intelligent self-service, agent-assist and automated operations for greater efficiency and scalability.
- **Superior CX:** CCaaS enhancements enable frictionless, proactive, and personalized interactions to boost customer satisfaction and retention.
- **Lower costs and agility:** CCaaS reduces capital expenses and frees resources for customer experience transformation.

Drivers

- Accelerated GenAI and agentic AI innovation within CCaaS platforms combined with reduced innovation in legacy contact center solutions encourages migration to cloud-based contact center solutions.
- Customer communications preferences, including expectations for rapid, low effort, personalized customer support across self-serve and assisted paths, and growth of digital engagement for product and service acquisition are evolving and will pressure organizations to modernize their contact center solutions.
- Growing interest among customer service leaders in delivering more proactive and frictionless support — enabled by advanced platforms that understand customer intent and maintain conversation context across channels — is expected to drive CCaaS transformation projects.
- CCaaS platforms are well-placed to manage both voice and digital channels (e.g., chatbots/virtual assistants, email, SMS/messaging, social media) and are becoming the preferred option when a single skills engine is required to support customer service representatives trained in multiple modalities.
- Economic and budget pressures are driving investment in CCaaS to enhance self-serve options and introduce innovative agent-assist features, aiming to reduce operational costs and achieve financial benefits such as increased retention, loyalty, and improved brand reputation through better service delivery.

Obstacles

- The emergence of GenAI is simultaneously introducing opportunities for differentiation and creating disruption, as users determine the cost and value trade-off of GenAI-infused use cases.
- Insufficient data readiness, siloed systems of record and interoperability continues to constrain the adoption of customer-facing GenAI.
- The ongoing transformation of the CCaaS provider landscape creates challenges for customers, who must navigate frequent updates to customer-facing GenAI, AI-infused analytics, agent-assist solutions, and WFM tools to ensure systems remain aligned with evolving end-user requirements.
- Rising concerns about sovereign cloud and data security in Europe could encourage interest in hybrid and private cloud contact center provisioning models in the region.
- Organizations with 10,000+ users struggle to justify migration costs due to existing premises-based investments, operating shifts, concerns about resiliency and uptime, and uncertainty over CCaaS feature parity.

User Recommendations

- Identify high-impact customer touchpoints where automation or AI can meaningfully enhance the customer experience.
- Prioritize data hygiene initiatives to ensure AI automation delivers accurate and reliable customer service.
- Accelerate investment in intelligent, AI-infused self-service CCaaS capabilities that enable seamless transitions to assisted channels.
- Evaluate back-office GenAI capabilities that empower agents to deliver more personalized and efficient customer support.
- Select CCaaS providers with demonstrated success in your industry (e.g., healthcare, finance, retail) to ensure compliance and alignment with best practices.
- Minimize disruption during migrations by selecting providers with proven transition frameworks.
- Update customer service metrics to measure CCaaS success, shifting focus from average handle time to real-time sentiment, loyalty, and customer effort.

Sample Vendors

Amazon Web Services; Cisco; Content Guru; Ericsson (Vonage); Five9; Genesys; NiCE; Odigo; Talkdesk; Zoom

Gartner Recommended Reading

Magic Quadrant for Contact Center as a Service

Forecast Analysis: Contact Center & GenAI Customer Support, Worldwide

Critical Capabilities for Contact Center as a Service

Overcome the Challenges of On-Premises to CCaaS Migration

Competitive Landscape: Contact Center as a Service

Market Opportunity Map: Contact Center, Worldwide

UCaaS

Analysis By: Rafael Benitez

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Unified communications as a service (UCaaS) is a cloud-based multitenant offering that integrates enterprise telephony, personal and team messaging, SMS, meeting solutions (web/video conferencing, whiteboarding and content sharing), contact center, mobile apps, and communications-focused AI assistants. Organizations typically buy multiyear agreements and pay a monthly (or yearly) flat rate per user.

Why This Is Important

Unified communications (UC) is a foundational I&O technology for organizations of all sizes, industries and geographies. In developed regions with reliable and inexpensive data networking services, UCaaS is preferred over on-premises UC due to its more modern feature set, maturity of AI capabilities, subscription-based model and user experience. In markets with poor data network connectivity, cloud regulatory restrictions or skepticism of cloud, migration from UC systems to UCaaS will be slower.

Business Impact

UCaaS's scalable licensing provides buyers with procurement agility as they grow, retrench, acquire or merge with other organizations. UCaaS inherently supports disaster recovery as providers have global networks of UCaaS service nodes. Support for hybrid workers is native, has a superior user experience vs. premise UC, and does not require additional infrastructure to deploy, unlike UC does. UCaaS reduces management costs compared to premise UC as platform updates are performed by the provider.

Drivers

- **Modernization:** In collaboration and mobile apps UCaaS offers a superior feature set when compared to on-premises UC solutions. Over the past 2-3 years UCaaS vendors have infused their offerings — telephony, meetings, messaging, administration and contact center — with AI to make end users and administrators more productive, provide automation and insights, and improve business outcomes. AI enhancements include messaging (message composition), meetings (meeting summaries), calling (pop-up notifications) and contact center services (realtime agent assistance, self-service chatbots and voicebots, sentiment analysis). Most leading UC vendors are limiting R&D innovation and investments in on-premises UC solutions, so modernization is often not an option with UC.

- **On-premises system's end-of-life milestone:** Most organizations facing a UC end-of-life event, or a costly major upgrade with hardware refresh (rack mount servers, desk phones) will use this event to justify migrating to UCaaS. Currently the installed base of on-premises systems is 1/3 the size of the UCaaS base. However, the most widely deployed on-premises systems are expected to be supported for 3 to 5 years.

- **Staff/skill loss:** On-premises UC solutions require engineering skill to manage (patching, upgrades) while UCaaS requires less technical skill and effort. If the current system on-premises UC platform administrator is no longer available, and given that this role is difficult to fill, many organizations will turn to UCaaS as the solution.

- **Cost optimization:** The total cost of UCaaS is expected to be lower than UC by buyers. However, whether or not savings can be realized not only depends on the market price of UCaaS but also the current costs of the UC system being replaced. In some cases, organizations may have very low costs with their UC system and, therefore, may have higher costs with UCaaS. Typically, organizations can realize savings or keep costs at a similar level when transitioning to UCaaS.

Obstacles

- **Regional availability:** MNOs find it challenging to find providers that can deliver local calling in less-developed countries. Organizations that are not multinational but operate solely in less developed regions may find UCaaS less desirable than UC because their region may have expensive or unreliable data networking services to support cloud.
- **Telephony feature gaps:** UCaaS is mature and can satisfy the telephony feature requirements of most organizations. Some organizations still require advanced telephony features that may not be available from UCaaS providers. This is increasingly rare but can still limit the ability to adopt UCaaS for such organizations.
- **Unusually stringent SLA targets:** Some organizations have exceedingly stringent mean time to repair service level targets (for example, financial services firms with stockbrokers or public safety organizations often require a recovery target of less than one hour), which may not be commercially available from most UCaaS providers.

User Recommendations

- Select UCaaS if your organization has less than 1,000 users. UCaaS has matured and meets the telephony and resiliency requirements of small and midsize businesses. SMBs can build a compelling business case for UCaaS by weighing their limited IT resources and skill set, the complexity of supporting remote sites, and the benefits of the high pace of innovation UCaaS vendors provide.
- Adopt UCaaS if your organization is large (more than 1,000 users) and has locations concentrated in a single developed region. Many public-sector organizations fall into this category and are adopting UCaaS frequently.
- Opt for hybrid UCaaS/UC if your organization is multinational and operates in regions where reliable data networking services may be unavailable or prohibitively expensive. While multinational organizations should explore UCaaS, less developed countries are also often challenged by restrictive local telecommunication regulations, sometimes making premises-based UC in such countries necessary.

Sample Vendors

8x8; Cisco; Dialpad; Ericsson (Vonage); Francisco Partners (GoTo); Microsoft; Nextiva; RingCentral; Vonage; Zoom

Gartner Recommended Reading

Magic Quadrant for Unified Communications as a Service

Forecast Analysis: Unified Communications, Worldwide

Appendixes

See the previous Hype Cycle: Hype Cycle for Enterprise Communication Services, 2025

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner

Table 3: Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	Status	Products/Vendors
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner

Evidence

[1] This projection is an integral baseline for Gartner's Forecast: Enterprise IT Spending by Vertical Industry Market, Worldwide, 2024-2030, 1Q26.

Document Revision History

Hype Cycle for Enterprise Communication Services, 2025 - 24 June 2025

Hype Cycle for Enterprise Communication Services, 2024 - 16 July 2024

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Top Technology Trends in Enterprise Communication Services for 2026

Predicts 2026: Enterprise Communication Services

Forecast: Communications Services, Worldwide, 2024-2030, 1Q26

2030 CSP Scenarios in the AI-Era: Strategic Priorities for CSP Product Leaders

Table 1: Priority Matrix for Enterprise Communication Services, 2026

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	*2 to 5 Years* ↓	*5 to 10 Years* ↓	*More Than 10 Years* ↓
Transformational	SASE Sovereign Cloud	Communications Platform as a Service eSIM	Agentic SMB Service Bundles Industry Edge Integrated Solutions Network Monetization APIs	
High	Managed IoT Connectivity UCaaS	5G Private Mobile Networks AI Security in ECS B2B Self-Service Capabilities LEO Satellite Communication Services MDR Services Rich Communication Services Securing CSP AI/ML Models in Communications Sovereign AI Threat Intelligence in ECS	CSP Edge Cloud Platform CSP Industry Vertical Solutions Machine Customers in Telecom VNFaaS	6G
Moderate	Contact Center as a Service CSP Data Monetization CSP Digital Marketplaces Dedicated Internet Access	Alternative WAN Backbone Services (XBaaS) Cross-Cloud Networking LEO D2D Services	CSP Superapps CSP XLAs Digital Twins of Telecom Networks	

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	*2 to 5 Years* ↓	*5 to 10 Years* ↓	*More Than 10 Years* ↓
	Graphics Processing Unit as a Service Managed SD-WAN Services ZTNA			
Low		NaaS		

Source: Gartner (July 2026)

Table 2: Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner

Table 3: Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner

Table 4: Maturity Levels

Maturity Levels	Status	Products/Vendors
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner