Hype Cycle for Private Networks for Industry, 2026

9 June 2026 - ID G00846630 - 110 min read

By: Sylvain Fabre, Peter Liu

Initiatives: Technologies and Markets; Delivery of Functional Responsibilities

Private networks for industry leverage commercial technologies to provide reliable, secure, low latency connectivity in vertical settings for devices, networks, compute and AI at the edge to support secure, real time operations. CIOs can use this Hype Cycle to identify and prioritize key technologies and innovations that will enable their private networks for industry strategy.

Analysis

What You Need to Know

Private networks for industry provide dedicated connectivity for the people and assets of an enterprise industrial setting. To maximize long-term value from these private networks for industry, communications service providers (CSPs) must now integrate advanced technologies such as generative AI (GenAI) in manufacturing operations, agentic AI, physical AI, multimodal AI, and industry edge integrated solutions. These innovations are driving rapid transformation across industrial verticals, enabling enhanced automation, predictive analytics, and real-time decision making at the edge. The adoption of solutions like edge AI, network security microsegmentation, and CPS wireless airspace defense is further strengthening operational resilience and security, critical for modern industrial environments in the current geopolitical context.

Beyond foundational connectivity and 5G, CSPs must broaden their offerings to include industrial digitization, comprehensive security frameworks, and ecosystem platforms. The emergence of CSP open APIs and eSIM technologies is facilitating seamless integration and onboarding of devices, while network slicing and private LTE are enabling tailored connectivity for diverse industrial applications. By collaborating with partners and leveraging open APIs, CSPs can unlock new value streams and support more sophisticated use cases.

The competitive landscape is intensifying as CSPs, equipment vendors, system integrators, and resellers increasingly deliver end-to-end solutions, positioning themselves as primary contractors for private networks for industry deployments. To remain competitive, these private networks for industry service providers must therefore prioritize innovation and differentiation in their portfolios, incorporating technologies such as neutral host network for 5G, time-sensitive networking, and CPS network cloaking and segmentation to remain relevant to industrial clients.

This Hype Cycle addresses the evolving requirements of end-to-end private networks for industry, and the most impactful innovations — including generative and multimodal AI, advanced edge architectures, and next-generation security solutions — to accelerate market adoption and deliver transformational value to industry.

The Hype Cycle

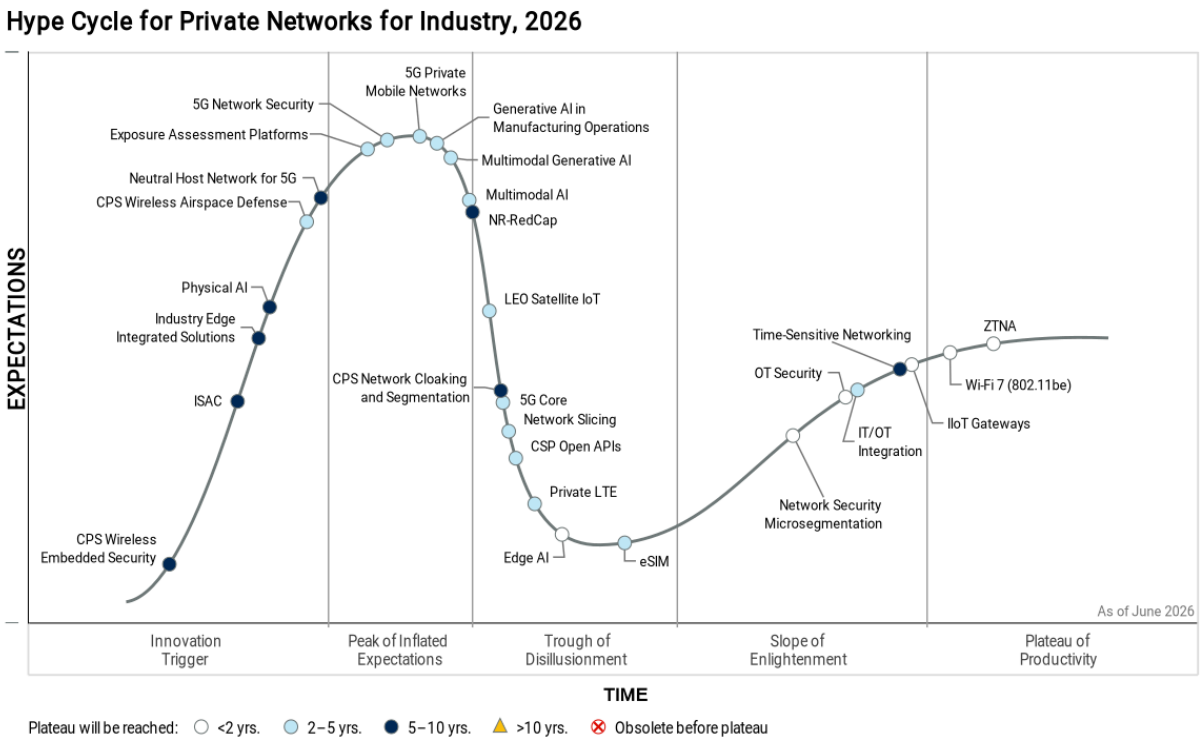
Disruptive changes are presenting both opportunities and challenges to private networks for industry service providers, particularly as enterprises seek solutions that deliver tangible business outcomes and clear return on investment. As a result, the innovations featured in this Hype Cycle reflect a blend of advancements in intelligent automation, edge computing, enhanced network security, and flexible connectivity models.

To remain competitive, private networks for industry service providers must foster innovation across multiple dimensions — including network architecture, security strategies, and service delivery approaches — often achieved through strategic collaboration with ecosystem partners and integration of emerging digital capabilities.

CIOs should use this Hype Cycle to:

- Identify the required technologies and capabilities to enable their private networks for industry service vision and support transformation strategies for enterprise customers.
- Evaluate current technology investments, identify opportunities for differentiation, and inform strategic provider selection to support business goals.
- Develop consensus with business leaders, product teams and service teams on which technologies, features and capabilities to support — and when to introduce them.
- Plan investments in necessary technology- and service-related capabilities, including workforce skills development and ecosystem management.

Figure 1: Hype Cycle for Private Networks for Industry, 2026



The Priority Matrix

The Priority Matrix maps the benefit rating of each innovation against the expected time to mainstream adoption. It underscores the need for strategic, coordinated, and sustained investments by CSPs to enhance their industry private network capabilities. The innovations highlighted in this Hype Cycle will have different expected benefits and will reach maturity at different rates — ranging from less than two years to more than 10 years.

For many emerging capabilities — such as industrial AI platforms, advanced edge architectures, and integrated security frameworks — CSPs must adopt a holistic approach that goes beyond traditional network-centric strategies to capture the full potential from these capabilities. This includes prioritizing areas like adaptive security, intelligent automation, and flexible connectivity models that address the specific demands of industrial environments. Edge intelligence, cloud-native operations, and open network programmability are becoming increasingly important for supporting diverse industrial applications and unlocking new value streams, to enable AI and serve AI-driven outcomes.

Security remains a critical focus and a continuously evolving area, with particular emphasis on proactive threat mitigation, network segmentation, and resilient architectures to safeguard industrial assets. CSPs should collaborate with ecosystem partners to address evolving risks, leveraging best practices in operational technology (OT) security and advanced network defense mechanisms.

Industry-specific solutions, such as AI-driven manufacturing, real-time asset tracking, physical AI and time-sensitive networking, are enhancing the relevance and impact of private networks for Industry in enterprise settings. The adoption of integrated Internet of Things (IoT) platforms and edge solutions is enabling real-time data processing, improved operational efficiency, and seamless device management across complex industrial environments. Other innovations — such as managed connectivity, network orchestration, and advanced analytics — are becoming essential for optimizing and securing industrial networks.

Developing these capabilities, especially those outside traditional CSP domains, will require targeted investments in talent, technology, and strategic partnerships. CSPs must prioritize continuous innovation and collaboration to deliver differentiated industry private network offerings that meet the evolving needs of industrial clients.

Table 1: Priority Matrix for Private Networks for Industry, 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		CSP Open APIs eSIM Generative AI in Manufacturing Operations Multimodal AI Multimodal Generative AI	Industry Edge Integrated Solutions Physical AI	
High	Edge AI Network Security Microsegmentation	5G Core 5G Private Mobile Networks CPS Wireless Airspace Defense Exposure Assessment Platforms IT/OT Integration Network Slicing Private LTE	CPS Network Cloaking and Segmentation CPS Wireless Embedded Security ISAC Neutral Host Network for 5G Time-Sensitive Networking	
Moderate	IIoT Gateways OT Security Wi-Fi 7 (802.11be) ZTNA	5G Network Security LEO Satellite IoT	NR-RedCap	
Low				

Source: Gartner (June 2026)

Off the Hype Cycle

The following changes have been made to this Hype Cycle:

- The name changed from Hype Cycle for Private Mobile Network Services to Hype Cycle for Private Networks for Industry. This is to reflect how end users perceive and procure these solutions — i.e., as enablers to achieve specific outcomes in their industry — rather than how vendors see private networks for industry (i.e., as a mobile technology).

Profiles removed (due to refocusing of the Hype Cycle along connectivity, security and industry-specific context):

- 5G in manufacturing operations
- Cloud-native telco operations
- Network digital twin
- Smart care venues
- Indoor location for assets
- Managed IoT connectivity
- Microservices
- Network microsegmentation (replaced by network security microsegmentation)
- Connected factory worker
- Industrial operational intelligence
- Innovation ecosystems
- IoT platform
- Bidirectional brain-machine interface
- Digital twins of factories
- IT/OT/ET alignment
- Multiaccess edge computing for CSPs
- Partner ecosystem management platforms for CSPs
- Extended detection and response (XDR)
- vRAN
- Network as a service (NaaS)

On the Rise

CPS Wireless Embedded Security

Analysis By: Mohini Dukes, Wam Voster

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Many CPS' use wireless communication, making these technologies critical to business operations. Technologies such as Bluetooth, Wi-Fi, cellular and LoRa are used based on the communication range, use case and infrastructure availability. Irrespective of range and frequency, all are prone to security risks. Organizations need CPS security that is natively integrated, such as cryptographic hardware, network protection, protocol-level protection, tamper detection and secure boot loader security.

Why This Is Important

Cyber-physical systems (CPS) and diverse use-case scenarios drive organizations to adopt wireless communications in operational technology (OT) environments. This approach expands the threat surface due to the connections between formerly airgapped OT environments and public or IT networks. Wireless is prone to cyberattacks, data breaches and system manipulation that are hard to detect due to the variety of wireless protocols. When compared to wired systems, wireless CPS assets need native secure communications in addition to any external or third-party wireless security mechanisms.

Business Impact

CPS are the foundation of business operations. While wireless communication binds CPS into functional networks, CPS becomes the target rather than conduit for attacks. Therefore, any threat to CPS poses a significant risk to:

- Continuous business operations — Financial, regulatory and reputational damage due to a break in production or service delivery.
- Proprietary data — Malicious or state-sponsored actors accessing proprietary, confidential and sensitive data.

- Mission-critical safety — Compromised CPS resulting in safety hazards and threat to life in mission-critical environments.

CPS become attack vectors when networks are compromised, resulting in risks like data interception — device hijacking, network intrusion, and operational or mission critical system service disruption.

Drivers

- CPS' assets range widely from sensors to robots and automated heavy machinery. The variety of wireless technologies depend on the CPS' assets, use case, vertical or manufacturer, making it difficult to secure all these communications links with a single method.
- Securing CPS using wireless technologies requires organizations to identify and inventory the assets along with discovering the communications protocols the assets are using. Most existing security solutions support either one of these requirements and are external to the CPS assets.
- Organizations may not be aware of all of the wireless technologies manufacturers embed into their CPS. Identifying the various protocols requires additional solutions to perform RF detection, usage and analysis.
- Organizations will have to track and manage a plethora of security techniques specific to each wireless technology or vendor and there can be multiple vendor deployments, which increases complexity.

Obstacles

- Embedded cryptographic capability has to be specific to securing communications protocols at a physical wireless link level (PHY). This needs to be a capability in addition to Trusted Platform Module (TPM) or other intrinsic cryptography.
- Although there are cryptographic capabilities to intrinsically secure the hardware modules, the functionality does not extend to securing the wireless communications initiated from the module. Any such capabilities that may exist are at a nascent stage.
- CPS' assets will need natively embedded security on a chip (SeconC) for cryptographic communications, which could drive up the costs of the assets.

- The embedded cryptographic capability has to be specific to securing communications protocols at a physical wireless link level (PHY). This needs to be a capability in addition to TPM or other intrinsic cryptography.
- Some CPS manufacturers may not be security specialists and will need to rely on technology partnerships to embed or integrate the security modules. Other manufacturers may be security specialists but may choose not to implement the SeconC because of cost pressures.
- Organizations need to thoroughly vet technology partnerships as part of supply chain compliance of trusted hardware adding more steps in the procurement process.

User Recommendations

- Create a device policy that addresses hardware and software bills of materials to identity supply chain risks.
- Focus on native cryptographic support to secure communications from the assets, in addition to external solutions for RF detection, asset discovery and encryption.
- Evaluate any interrelations that exist between security policy controls or security management with the native cryptographic support.
- Make the requirement for CPS manufacturers to provide a list of all supported wireless protocols supported by the asset, irrespective of whether it is used for operational data or system/telemetry data communication.
- Prioritize identifying the integration of CPS asset discovery solutions overlaid on the wireless network solutions if there is no embedded cryptographic support on the CPS.
- Disable unused wireless interfaces. If a device includes multiple wireless radios (e.g., Wi-Fi and Bluetooth), disable the unused ones to reduce attack surfaces. Reconfirm that these settings are not reenabled following firmware updates.
- Educate stakeholders, engineers and operators on secure wireless practices. Humans are a major vector for configuration weaknesses.

Gartner Recommended Reading

Transform Network Connectivity for the Edge

Enhance CPS Security With Network Segmentation Techniques

Emerging Tech: Top-funded Startups for Cyber Electronic Defense (CED)

ISAC

Analysis By: Peter Liu

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Embryonic

Definition:

Integrated sensing and communications (ISAC) refers to cellular network architectures sharing spectrum, hardware, and signal processing to combine wireless communication with environmental sensing (object detection, mapping, and positioning). Distinct from Wi-Fi capabilities (IEEE 802.11bf), ISAC focuses on cellular systems, noted as a 3GPP Release 19 study item and a 6G core capability in ITU-R IMT-2030.

Why This Is Important

CSPs can monetize existing RAN infrastructure as a sensing platform — delivering positioning, object detection, and environmental mapping without dedicated radar equipment. This unlocks sensing-as-a-service revenue streams while reducing spectrum fragmentation. ISAC is vital for 6G Physical AI, enabling real-time environmental perception. As sensing and communication share RAN resources, dynamic spectrum scheduling is required to balance these functions.

Business Impact

ISAC offers major benefits for both communications service providers (CSPs) and enterprises. CSPs can launch new sensing services alongside connectivity, creating new revenue streams in areas like logistics, smart cities, autonomous mobility, and the vertical economy (such as airborne drones and taxis). This enables early adopters to secure vertical market positions before hyperscaler entry. Enterprises also benefit from lower capital expenditure (capex), as ISAC removes the need for stand-alone deployments.

Drivers

- **6G standardization momentum:** ITU-R IMT-2030 and 3GPP Release 19 formally elevated ISAC from research concept to standardized network capability, accelerating vendor and CSP investment
- **Spectrum scarcity:** The shared-sensing communication spectrum eliminates the need for dedicated radar bands, making ISAC economically compelling as spectrum costs rise.
- **Physical AI proliferation:** Physical AI devices such as autonomous delivery robots, vehicles, and drones require real-time environmental awareness that ISAC-enabled networks can provide natively at scale.
- **Enterprise vertical demand:** Logistics, manufacturing, and smart city clients increasingly require sensing and connectivity from a single infrastructure provider.
- **CSP revenue diversification:** Declining ARPU from traditional connectivity services forces CSPs to monetize existing RAN assets through new sensing-based service layers.
- **RAN hardware convergence:** AI-accelerated baseband processing enables RAN hardware convergence by allowing joint sensing-communication on shared silicon, lowering deployment cost and complexity.
- **Smart city and government mandates:** Regulatory requirements for real-time urban monitoring and public-safety sensing create guaranteed demand for network-native sensing infrastructure.

Obstacles

- **Standardization immaturity:** 3GPP Release 19 scoped ISAC as a study item only; full normative standardization and interoperability specifications are years away.
- **Interference complexity:** Simultaneous sensing and communication on shared waveforms create self-interference and signal-processing challenges not yet resolved at scale. Sensing also competes directly with communication for RAN time-frequency resources, creating a hard capacity trade-off in congested cells.
- **Privacy and regulation:** Passive city-scale sensing triggers surveillance concerns; regulatory rules for data monetization remain undefined.
- **Spectrum coordination:** Sharing spectrum between communication and sensing functions requires coordination with aviation, meteorological, and defense radar incumbents who hold priority rights in key bands.
- **Ecosystem fragmentation:** No dominant ISAC platform or API standard exists; vertical market integrations require custom-made development, slowing go-to-market.

User Recommendations

- Pilot before standardization. Launch controlled ISAC trials in private 5G settings (ports, factories, campuses) using prestandard implementations to gain operational expertise and avoid late-mover disadvantages before the 3GPP normative release.
- Integrate ISAC into private network propositions. Bundle sensing capability into existing private mobile network offers rather than launching stand-alone or with a public network.
- Align RAN roadmaps with ISAC by ensuring next procurement cycles specify ISAC-ready hardware; retrofitting existing deployments will be costly and technically difficult.
- Engage regulators early to secure the ISAC-compatible spectrum. Influencing policy provides first-mover advantages in viable bands and avoids future refarming costs.
- Deploy technical teams to 3GPP ISAC and ITU-R IMT-2030 groups to shape normative specs, interface designs, and interoperability standards.

Sample Vendors

Ericsson; Huawei; InterDigital; Nokia; NVIDIA; Qualcomm; Samsung; ZTE

Gartner Recommended Reading

Top Strategic Trends for CSP CIOs in 2026

Top Technology Trends for CSP CIOs in 2026

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

Physical AI

Analysis By: Sushovan Mukhopadhyay, Chirag Dekate

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Physical AI refers to AI systems embodied in physical form factors, such as robots, drones, autonomous vehicles and smart devices, that use AI to sense, interact with the real world. By combining sensors, actuators and AI models, these systems connect digital intelligence to physical action, enabling them to manipulate objects, move through space and autonomously respond to dynamic environments.

Why This Is Important

Physical AI-powered systems interact with and take action in the physical world, enabling automation, precision, adaptability in a dynamic environment. This integration unlocks new efficiencies by facilitating real-time interactions with devices like robotics, IoT, edge devices, autonomous vehicles, allowing them to operate in unstructured environments. It harnesses insights from sensors to perceive the environment in which it is operating to dynamically interact with the physical objects around it, delivering practical, real-world solutions across domains like manufacturing, logistics, retail, healthcare.

Business Impact

Physical AI can perceive its environment, enabling machines, devices and vehicles to deliver advanced automation. This leads to cost reductions, improved operational efficiency, intelligent decision making, improved safety, and minimized human error and risks, while addressing persistent labor shortages by automating repetitive, hazardous or hard-to-staff tasks. Businesses can benefit from enhanced productivity, streamlined supply chains and innovative service offerings, spurring competitive advantage and opening new revenue streams.

Drivers

Business drivers:

- **Real-world impact with real-time AI processing:** Physical AI systems, when mature, could be integrated into environments requiring complex, unstructured, unpredictable decisions. There is an increasing demand for intelligent, adaptive physical systems in domains like robotics, logistics, healthcare, transportation.
- **Increasing demand for automation:** Physical AI can streamline operations, reduce human error and lower long-term costs by automating repetitive or dangerous tasks. Sectors like warehousing, security and transportation benefit from AI systems that can perform repetitive tasks with accuracy and operate continuously without fatigue.

Technical drivers:

- **Advancements in sensor, actuator, connectivity technologies:** Improvements in hardware (sensors and actuators) enable AI systems to sense, adapt and interact more accurately and efficiently with the physical world. Sensor fusion combines data from complementary modalities (vision, lidar, radar and tactile sensing) to increase precision, robustness and situational awareness.

- **Edge AI advancements:** The rise of edge computing allows AI systems to process data locally, reducing latency and improving responsiveness. This is crucial for applications requiring real-time decision making, like autonomous vehicles and smart manufacturing. More compute capacity per node at the similar power envelope enables new use cases for battery-powered physical AI solutions.
- **Innovations in world models:** These models serve as the cognitive backbone for physical AI, interpreting sensory data and predicting outcomes. By integrating intuitive physics-based simulations and AI-generated synthetic data, they create hyperrealistic digital twins and synthetic environments for training these AI models.
- **GenAI perception models:** Innovations in vision language and vision language action models connect images, language and actions for scene understanding and control. Selective state space models improve temporal reasoning with fast, memory efficient inference on edge devices.

Obstacles

- **Perception and interaction challenges:** The physical world is unpredictable, requiring AI to handle edge scenarios in real time. Operating safely around humans and in unstructured environments requires near-perfect perception and control, which are still developing and models trained in simulation often fail to fully generalize to real-world conditions (the sim-to-real gap).
- **Hardware limitations:** It requires advanced sensors and precise actuators, which are expensive and fragile. Battery limits reduce runtime and performance for untethered systems. Telemetry is constrained by power, bandwidth and terrain, reducing command-center visibility into device status, location, interoperability.
- **Commercial viability challenges:** High initial investments with uncertain long-term ROI slow adoption in commercial settings. Expensive hardware, specialized manufacturing and maintenance raise entry barriers.
- **Ethical, legal, social issues:** Ambiguity around responsibility for physical AI errors hinders adoption. Concerns over job displacement, surveillance, and varying regional regulations complicate deployment.

User Recommendations

- Start with pilot projects in controlled environments to test and refine physical AI systems, focusing on repetitive or low-risk use cases that require both adaptivity and efficiency. Use feedback from these implementations to enhance system design, functionality, and infrastructure readiness before full-scale deployment.
- Build strategic partnerships to collaborate with technology providers, research institutions and industry experts to stay informed about the latest advancements and best practices.
- Develop clear guidelines and accountability frameworks for AI errors and decision-making processes while engaging with regulatory bodies to ensure compliance with regional laws and standards.
- Provision greenfield environments for physical AI by designing the physical space to support adoption. This includes adequate gangway width, access paths, mounting points, power and network availability, and integration interfaces for future automation.

Sample Vendors

ABB; AGIBOT; Agility Robotics; AMD; Boston Dynamics; Diligent Robotics; Fourier; Google DeepMind; Intel; KUKA; Liquid AI; NVIDIA; UBTECH Robotics; Unitree Robotics

Gartner Recommended Reading

Emerging Tech Impact Radar: Physical AI

Adopting Physical AI for Real-World Use Cases

Emerging Tech: Top-Funded Startups in Physical AI

Emerging Tech: AI Vendor Race: Startups to Watch in Physical AI

CPS Wireless Airspace Defense

Analysis By: Sylvain Fabre, Mohini Dukes

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cyber-physical systems (CPS) wireless airspace defense is the practice of detecting, identifying, tracking and neutralizing unauthorized or malicious use of RF spectrum within a protected zone — primarily rogue drones, jammers and spoofing devices. It is increasingly relevant to private 5G network security for critical infrastructure to prevent wireless interference, data exfiltration and unauthorized control of assets.

Why This Is Important

Traditional IT security is blind to the RF attack surface, leaving cyber-physical systems exposed. Wireless airspace defense is critical to stop attackers from using unmonitored protocols to bypass firewalls and subvert zero-trust architectures, or from RF jamming to render private 5G networks or GPS unusable. Furthermore, fake signals from GPS spoofing can manipulate location information, creating severe operational and safety risks.

Business Impact

Wireless vulnerabilities drive severe financial, operational and reputational damage. Over half of organizations suffer financial losses from wireless incidents, many exceeding $1 million annually. Unmitigated RF threats lead to prolonged production downtime, regulatory compliance violations, and civil or criminal liabilities. Securing this airspace ensures business continuity, protects brand trust and prevents costly operational halts.

Drivers

- **AI-powered and democratized threats:** Adversaries increasingly use AI to automate reconnaissance, mimic legitimate users and evade detection; Claude Mythos and open-source models add urgency. Low-cost SDR radios and turnkey hacking tools lowered the barriers to entry for sophisticated RF attacks.
- **Explosion of IoT and connected devices:** Modern enterprises' cyber-physical domains are saturated with IoT and operational technology (OT) devices communicating over cellular protocols. These unmanaged endpoints drastically expand the attack surface, creating invisible pathways for data exfiltration that easily bypass traditional wired firewalls.
- **Convergence of IT and OT networks without regard to security:** As industrial environments modernize, previously air-gapped OT systems are increasingly integrated with IT networks, exposing vulnerable, legacy infrastructure to wireless threats.
- **Proliferation of commercial drones:** The widespread accessibility of inexpensive unmanned aerial systems (UAS) introduces severe physical and electronic risks to corporate airspace, with increasing use for hostile surveillance, payload delivery and malicious reconnaissance.
- **RF spectrum congestion and 5G complexity:** The rapid expansion of wireless services, including the transition to 5G and dynamic spectrum sharing, has created highly congested electromagnetic environments. This density elevates the risk of both accidental signal overlap and intentional RF jamming or spoofing attacks.
- **Stringent regulatory mandates:** Stricter government regulations surrounding critical infrastructure protection, data privacy and spectrum management require robust RF monitoring, increasingly mandating interference-free operations through active airspace surveillance.
- **Cybersecurity talent shortages:** A severe lack of skilled wireless security professionals limits the ability of organizations to manually monitor complex RF environments, driving adoption of automated, AI-driven airspace defense platforms.
- **Geopolitical tensions:** Conflicts in Ukraine and the Middle East have shown the increased use and lethality of kinetic use of drones against civilian critical infrastructure, accelerating government mandates.

Obstacles

- **Regulatory limits and fragmentation:** Strict laws (e.g., Wiretap Act and FCC regulations, ITU Article 45, U.K. RIPA 2000) often prohibit signal decoding and active mitigation tactics such as jamming. This significantly restricts organizations from actively neutralizing detected airspace threats.
- **Encryption and spoofing:** Adversaries increasingly encrypt communications, rendering traditional radio frequency (RF) decoding obsolete. Furthermore, spoofing techniques can generate fake signals or mask true origins, severely complicating accurate threat tracking.
- **Environmental interference:** Dynamic physical environments with dense infrastructure, weather variations and moving objects cause signal scattering and overlap. This congestion makes isolating malicious anomalies from benign background noise technically difficult.
- **Computational and data demands:** Training AI detection models requires massive, hard-to-acquire datasets of labeled malicious signals. Deploying these resource-heavy AI models for real-time analysis on constrained edge devices remains a significant hurdle.
- **Legacy system integration:** Many enterprises rely on outdated communication infrastructures that were not designed for advanced, AI-driven RF monitoring. Retrofitting these legacy systems is costly and highly complex, and requires specialized engineering.

User Recommendations

- **Deploy** continuous wireless intrusion detection systems by actively scanning the RF spectrum in order to identify rogue access points before they compromise the network.
- **Enforce** strict zero-trust principles by utilizing microsegmentation and continuous device validation in order to limit lateral movement and secure unmanaged IoT endpoints.
- **Modernize** existing wireless security frameworks, by adopting WPA3 and eliminating outdated legacy protocols, in order to drastically reduce credential-based vulnerabilities.
- **Restrict** access to OT systems by implementing layered physical barriers and logical firewalls in order to prevent unauthorized manipulation of critical infrastructure.
- **Maintain** layered multisensor drone detection by combining RF triangulation, radar and optical tracking in order to locate malicious drones before they breach protected airspace.

Sample Vendors

Airbus (Airbus Defence and Space); AirEye; Axon (Dedrone); Bastille Networks; Cisco Systems; HawkEye 360; Keysight Technologies; LOCH Technologies; Netline; Rohde & Schwarz

Neutral Host Network for 5G

Analysis By: Kosei Takiishi

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Embryonic

Definition:

A neutral host network (NHN) for 5G is a shared wireless infrastructure model in which an independent third-party provider owns and operates a multitenant 5G RAN to support both public and private networks. As of 2026, NHNs are increasingly positioned as venue- and campus-level connectivity platforms that enable the coexistence of mobile CSP services and enterprise private 5G over a single physical network.

Why This Is Important

- NHNs minimize redundant infrastructure by sharing resources across stakeholders, reducing capital and operational costs.
- NHNs address coverage and capacity gaps, improving user experience for public and private 5G deployments.
- The NHN model enables new revenue opportunities for integrators managing multistakeholder environments.
- Neutral hosts make coverage viable in rural, indoor and dense urban areas where deployment constraints exist.

Business Impact

- **Cost and asset efficiency:** Shared infrastructure lowers deployment and life cycle costs while improving use of assets.
- **Accelerated deployment:** NHNs speed up 5G rollout by avoiding parallel infrastructure builds across stakeholders.
- **Operational simplification:** A single NHN integrator simplifies operations, maintenance and upgrades across public and private 5G.
- **Service-level differentiation:** CSPs and enterprises can focus on service innovation instead of competing on duplicated infrastructure.

Drivers

- **Growth of private 5G deployments:** Enterprises increasingly deploy private 5G for operational control, security and performance, creating demand for infrastructure that can coexist with public networks in shared spaces.
- **Cost and space constraints in venues and campuses:** Indoor venues, transport hubs, campuses and dense urban areas face physical, regulatory and economic constraints that limit parallel deployments by multiple CSPs.
- **Regulatory and policy encouragement:** Many regulators encourage infrastructure sharing to reduce environmental impact, improve spectrum efficiency and expand coverage, reinforcing neutral host adoption.
- **Maturity of multitenant technologies:** Advances in virtualization, Open RAN and network management platforms make multioperator, multitenant 5G deployments more practical and scalable than earlier generations.

Obstacles

- **Stakeholder alignment:** Coordinating commercial, operational and technical interests across CSPs, enterprises, venue owners and integrators remains complex.
- **Business model uncertainty:** Revenue sharing, investment responsibility and long-term return models continue to vary by region and use case.
- **Governance and control concerns:** Responsibility for service quality, security and fault resolution can be unclear in multitenant environments.
- **Strategic resistance:** Some CSPs remain reluctant to rely on shared infrastructure due to concerns over loss of control and differentiation.

User Recommendations

- Evaluate neutral host networks as a default option for complex venues, campuses and shared spaces where public and private 5G must coexist.
- Engage all stakeholders early to define governance, service-level responsibilities and commercial models.
- Prioritize interoperability by ensuring that the NHN supports multitenancy access with robust security and performance.
- Adopt flexible business models by exploring various revenue-sharing, leasing and investment options tailored to local market conditions and use cases.

Sample Vendors

Celona; CommScope; Ericsson; Freshwave; NEC

Gartner Recommended Reading

5G Infrastructure Sharing: How Vendors Incorporate It Into Their Products

At the Peak

Exposure Assessment Platforms

Analysis By: Mitchell Schneider, Dhivya Poole, Jonathan Nunez

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Exposure assessment platforms (EAPs) continuously identify and prioritize exposures, such as vulnerabilities, misconfigurations and control gaps, across diverse asset classes. They visualize attack paths to business-critical assets and enable remediation through integration with ticketing systems, patching workflows and compensating controls. EAPs aggregate exposure data from external discovery tools or perform native discovery to centralize and contextualize exposures for unified visibility.

Why This Is Important

Without a comprehensive focus on continuous threat exposure management (CTEM), cybersecurity leaders risk reputational damage, regulatory fines, data loss and security breaches. EAPs are an essential technology element supporting CTEM programs by providing a comprehensive and prioritized view of exposures across a broad range of asset classes, streamlining remediation and addressing business risk.

Business Impact

EAPs enable organizations to proactively identify exposures most likely to be exploited and speed decisions on remediation or mitigation, helping prevent attackers from leveraging known exposures. EAPs improve operational efficiency, support business-driven prioritization and streamline remediation by consolidating results, automating identification of critical assets, assigning ownership and coordinating workflows. They also provide reporting and exposure-trend insights.

Drivers

- Organizations need a more advanced approach than just CVSS scores or basic external data for vulnerability prioritization. EAPs use richer internal context — asset and business criticality, environment details, control effectiveness and cybersecurity validation — to deliver actionable insights. Some vendors add predictive models for likely future exploits, but these also need internal context for meaningful prioritization.
- EAPs highlight the most significant exposures, deduplicate findings, and help prioritize remediation or compensating controls to prevent compromise. Attack path analysis adds insight by showing how exposures can chain together, refining which issues pose real risks.
- EAPs reduce operational overhead from misprioritized findings with a consolidated view, helping organizations retain talent and improve efficiency by focusing on higher-value activities. Automation features further cut manual triage and speed remediation.
- EAPs enhance SOC efforts like TDIR by providing contextual asset enrichment and multiple views (e.g., attack paths) to accelerate investigations. Deeper integration with SIEM and ITSM platforms enables more coordinated workflows.
- Organizations are broadening their scope to include not just traditional vulnerabilities but also exposures without CVEs, like misconfigurations, identity hygiene issues, SaaS risks and control gaps, driving demand for EAPs that unify discovery across the attack surface.
- Automated, closed-loop remediation is increasingly required. EAPs meet this need by integrating with ITSM, SOAR, EDR, CNAPP and patching tools, enabling faster, more consistent exposure treatment and reducing reliance on manual processes.
- Continuous, defensible insight into control effectiveness and exposure trends is essential for cyber GRC. EAPs provide telemetry-based reporting, ongoing validation and auditable remediation tracking, supporting continuous, data-driven compliance over checklist approaches.

Obstacles

- EAPs offer limited value when applied to broken, undefined or immature processes in vulnerability management. Without clear ownership, strong data hygiene and operational workflows, even advanced capabilities yield minimal improvement.

- Organizations that restrict EAP use to compliance mandates or static CVSS scoring will not realize full value, as this overlooks business context and criticality, exploitability, active threat behavior and cybersecurity control effectiveness.
- EAPs can produce attack path analysis, but it is also available through AEV tools that focus on attack simulation and cybersecurity validation. Organizations with existing AEV investments may not view passive attack-path visualization features as providing meaningful added value.
- Organizations operating multiple overlapping platforms may face fragmented inventories, inconsistent data models and competing prioritization engines, reducing overall clarity and operational impact.

User Recommendations

- Implement an outcome-driven approach that:
  - Identifies available context (e.g., stakeholder needs, compliance requirements) for prioritization and ensures data quality and ownership are sufficient to prevent negative impact.
  - Correlates asset business context, threat intelligence, cybersecurity controls, security configurations and proprietary algorithms to calculate a dynamic, evidence-based risk rating.
- Shift from siloed tools to EAPs to centralize asset, attack surface and vulnerability management using AI-supported prioritization, automated remediation and attack path insights.
- Select vendors with strong bidirectional integrations to broaden attack surface visibility, refine prioritization and support coordinated, cross-team remediation.
- Deploy EAPs that evaluate exposure telemetry, starting with control configurations and expanding to cloud, identity and SaaS posture for a more actionable threat landscape.

Sample Vendors

Axonius; CrowdStrike; Microsoft; Nucleus Security; Qualys; Rapid7; ServiceNow; Tenable; Wiz; XM Cyber

Gartner Recommended Reading

Use Continuous Threat Exposure Management to Reduce Cyberattacks

Strategic Roadmap for Continuous Threat Exposure Management

How to Grow Vulnerability Management Into Exposure Management

We're Not Patching Our Way Out of Vulnerability Exposure

Innovation Insight: Attack Surface Management

5G Network Security

Analysis By: Sylvain Fabre, Nat Smith, Peter Liu

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

The 5G network offers security enhancements over 4G like mutual authentication and enhanced subscriber privacy. However, 5G's cloud-native architecture, edge processing, increased network capacity and low latency can amplify risks, given the proliferation of vulnerable IoT devices. Although 3GPP strengthens the air interface security, the distributed nature of 5G, with network function security left to various international forums, can lead to inconsistencies and a wider attack surface.

Why This Is Important

Securing 5G networks is a priority for CSPs' public networks. The increasing adoption of private mobile networks (PMNs) deployments, vertical applications, cloud architecture, and massive Internet of Things (IoT) connections is creating new vulnerabilities and challenges, such as distributed denial of service (DDoS) attacks. 5G network security offers a single, unified framework to manage how users and devices are authenticated when connecting to the network, regardless of their cellular 3rd Generation Partnership Project (3GPP) or other (non-3GPP) access methods.

Business Impact

5G security:

- Enhances subscriber privacy with unified authentication and Subscription Concealed Identifier (SUCI) encryption, mitigating international mobile subscriber identity (IMSI) catchers.
- Adds user plane integrity protection and a security edge protection proxy (SEPP) for roaming.
- Secures network access of external entities via network exposure function (NEF) and verifies users and devices across different access types through Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA).
- Enables application layer security via service-based architecture (SBA).
- Verifies device location using home network public key (HNPK) authentication when in a visited network, preventing spoofing attacks.
- Mitigates bidding-down attacks and neutralizes fake base stations (aka IMSI catchers).

Drivers

- The wider industrial 5G ecosystem demands security tools with varying capabilities to deliver SLAs and end-to-end security for diverse use cases. This includes an application-focused approach at the edge, ensuring security is tailored to specific industry needs.
- Liability exposure in enterprises deploying private 5G necessitates robust network security.
- Increasing regulations around user data privacy are a key driver, further amplified by legislation like the EU's Cyber Resilience Act (CRA) and Network and Information Systems (NIS2) directive, which mandate stronger cybersecurity measures and reporting obligations.
- Heightened scrutiny on 5G infrastructure vendors and competition based on perceived security levels continue to drive security enhancements.
- Interconnection with legacy networks, satellites and less secure IoT devices requires robust mechanisms to handle such connections safely. The proliferation of poorly secured IoT devices significantly expands the attack surface.
- Delivering cloud-based 5G infrastructure and services (core, slicing, edge) necessitates comprehensive cross-domain security. Network virtualization and cloudification, while offering flexibility, introduce inherent security challenges.
- Demand for edge enterprise solutions will accelerate 5G security adoption, particularly with the need to secure application workloads closer to the data source.
- 5G SBA infrastructure virtualization, automation, orchestration and multivendor solutions increase risk exposure for CSPs and enterprises.
- CSPs can offer differentiated security options, such as using slicing, as a value-added service.
- Growing reliance on 5G for critical infrastructure (smart grids, transportation, healthcare) and the current geopolitical climate make robust security paramount to protect essential services and public safety.

Obstacles

- 5G end-to-end security presents new challenges for operators (e.g., hacks on misconfigured containers) but an IT-centric approach to network functions and back-end/core can improve security posture.
- Some security settings are optional, so implementation security levels may vary.
- Chief information security officers (CISOs) may not realize the need to secure their on-premises 5G PMNs or understand additional threats in 3GPP-based infrastructures. They rely on their vendors, who tend to focus on performance and project delivery rather than security.
- Supply chain security concerns remain for 5G as open-source approaches add complexity. Not all network components are (yet) known and defense models may have to broaden as implementation progresses.
- Backward compatibility with 4G/LTE means some legacy security issues affect 5G; for example, general packet radio service (GPRS) Tunneling Protocol [GTP] attacks.
- 5G runs on commodity hardware and containerization, which creates a larger attack surface compared to 4G.
- Deployment scenarios for private 5G have different risk profiles and security needs.
- The increased network complexity of 5G, coupled with lack of integration with legacy infrastructure and standardization, poses further obstacles.

User Recommendations

- Avoid overreliance on 3GPP 5G security. Solve all 4G issues and continue ongoing security initiatives, since many 5G security features are designed to protect the network rather than secure user data.
- Assess and anticipate increased risk of attacks such as DDoS by improving 5G network design infrastructure, endpoints, and recovery procedures.
- Implement layered DDoS defense by using best-of-breed scrubbing, a cloud-web-application firewall, bot mitigation, DNS protection, ISP and on-premises DDoS appliances.
- Initiate effective mitigation by correlating network traffic, application availability, server performance, and other relevant data.
- Complement 5G infrastructure security with distributed AI/ML anomaly detection algorithms for zero days, covering newer domains such as core slicing.
- Implement edge protection concepts used in application security for elasticity, focusing on app-layer protection.
- Implement 5G end-to-end security by managing algorithm strength, secret keys negotiation, confidentiality protection, cross-domain slice orchestration, and heterogeneous network layers.
- Use a clear model of shared responsibility between operators, vendor partners, and end-user organizations.

Sample Vendors

A10 Networks; Fortinet; Microsoft; Nokia; OneLayer; Palo Alto Networks; SentinelOne; Trend Micro; VIAVI Solutions; Zscaler

Gartner Recommended Reading

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

Navigating the Complexities of 5G Private Network Security

Market Trend: CSPs Need Tailored Security for 5G Networks

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

Generative AI in Manufacturing Operations

Analysis By: Chris Campbell

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Generative AI refers to AI techniques that learn a representation of artifacts from data and use it to generate brand-new, unique artifacts that resemble, but don't repeat, the original data. Generative AI can produce novel content (including text, images, video, audio and structures), computer code, synthetic data, workflows and models of physical objects. Generative AI can be used in tasks such as drug discovery or material design.

Why This Is Important

GenAI will impact a broad spectrum of production activities, deliver new insights and drive a new level of efficiency in operations to increase supply reliability. GenAI can:

- Improve the worker experience with more intuitive guidance and recommendations in natural language.
- Provide additional synthetic data for model training — and then generate and model novel scenarios and workflows for solving complex problems — to improve flow and manage change.

Generative code development lessens the cost and time for automation programming or developing completely new manufacturing applications, where the codebase is not built on proprietary low-code/no-code platforms. Most manufacturers are experimenting with the technology

Business Impact

GenAI will disrupt manufacturing operations by:

- Recalibrating the relationship between human and machine by transforming the human-machine interface (HMI) through virtual advisors, chatbots and the ability to communicate with systems more naturally.
- Introducing insights with different content creation, classification and presentation, resulting in greater efficiencies in identifying losses and/or shift handovers.
- Enhancing productivity through generative code development or suggesting enhancements to existing code, so operations can autonomously adapt to changing conditions.

Yet, intellectual property (IP) protection will be needed. Responsible AI, trust and security will be necessary for safe exploitation of GenAI.

Drivers

- GenAI simplifies interfaces and increases transparency into more complex models, analytics and decision support fulfilled by machine learning and other forms of AI.
- Rapidly emerging proofs of concept (POCs) and value stories are forcing manufacturing organizations to accelerate their exploration of the potential applications of AI on a broad scale to boost overall productivity and optimize costs.
- Synthetic data draws the attention of enterprises by helping to augment scarce data, mitigate bias or preserve data privacy. These capabilities can be well-utilized to predict demand and supply patterns in complex supply networks.
- Elimination of redundant or time-consuming tasks such as coding, documentation and forms of analysis allows for resource synergies, hedging labor availability risks.

Obstacles

- Data access remains elusive, which impacts adoption at scale. There are many ongoing pilots in manufacturing. Yet, generating accuracy and trust in GenAI applications is difficult because it means connecting critical data and information representing different bills of materials (BOMs), bills of process (BOPs), work instructions and time series data sources. Scaling across multiple sites exposes deep technical debt, systems upgrades and integration. Data quality concerns and low analytics maturity can limit adoption.
- Compared to conventional manufacturing systems (manufacturing execution system, quality management system), a suitable deployment model for GenAI is unclear. Publicly available models are not a substitute for internal IP and the content needed. These models are evolving faster than manufacturers can keep pace. Building their own models is a huge risk for manufacturers from the financial and capability perspectives.
- There is a tendency to overlook the need to converge and align IT, operational technology (OT) and engineering technology (ET). Shared infrastructure, knowledge transfer and security are needed.
- Depending on the model chosen for fine-tuning, the compute resources for training foundation models are heavy and not affordable for most enterprises. Impact and sustainability concerns about high-energy consumption for training generative models are rising.

User Recommendations

- Quantify GenAI's requirements and limitations against any quantifiable financial and productivity improvements, as well as harder-to-track, intangible metrics such as decision speed or time to competency, to determine the advantage.
- Determine and communicate expected ROI and intangible benefits of GenAI pilots, ranging from better understanding of the potential and challenges of deploying the technology to quantifiable financial and productivity improvements.
- Ensure the success and viability of initial use cases by doubling down on data management. New investments are needed to develop, curate, validate and continually fine-tune large language models and foundation models. Also, prepare to allocate funding to ingest, cleanse and contextualize data from untapped or legacy data sources. In other instances, removing paper or manual ways of working will be needed. Do not overlook that the number, size and level of fine-tuning, as well as investments in infrastructure and integration, need scoping.
- Mitigate GenAI risks by working with legal, security and fraud experts. Technical, institutional and political interventions will be necessary to fight AI's adversarial impacts. Start with data security and different geographic guidelines.
- Optimize the cost and efficiency of GenAI solutions by combining GenAI with other AI techniques such as Agentic AI and technologies (e.g., 5G, IoT) and existing manufacturing systems.

Sample Vendors

Amazon Web Services; Google; IBM; Microsoft; Rockwell Automation; Siemens

Gartner Recommended Reading

Innovation Insight: What Generative AI Means to Manufacturing Strategy Leaders

Determine Generative AI Use Cases for Manufacturing Operations

GenAI's Great Expectations Shape Supply Chains' Adoption Plans

Industrial Manufacturing Case Examples to Build Your Generative AI Strategy

Multimodal Generative AI

Analysis By: Danielle Casey, Roberta Cozza

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Emerging

Definition:

Multimodal generative AI is the ability to use multiple types of data inputs and outputs in generative models, such as images, videos, audio, text, numerical data, maps and biometric information. Multimodality refers to both data input and output, in which multiple data formats can be used or consumed during an interaction. Multimodality augments the usability of AI by allowing models to interact with and create outputs across various modalities.

Why This Is Important

Multimodal GenAI is important because real-world data is multimodal. Multimodality helps capture the relationships between different data streams and scales the generation and automation benefits of GenAI across applications and workflows. Multimodal functionality will increasingly be present in tech offerings as foundation models lower the technical barrier to multimodal functionality, and as users demand associated performance.

Business Impact

Multimodal GenAI is increasingly having a transformational impact on enterprise applications by enabling the addition of new features and functionality otherwise unachievable. The impact of multimodality is not limited to specific industries or use cases and can be applied at any touchpoint between AI and humans. Today, text, voice and image are common modalities. Over the next few years, models will evolve to support additional modalities that are more complex and domain-specific. As multimodal GenAI matures, multimodal understanding will evolve into multimodal actioning, where agents automate tasks from multimodal data inputs.

Drivers

Multimodal GenAI is being driven by:

- **Model innovation:** GenAI models are lowering the technology barrier for providers to offer multimodal functionality in their offerings. The emergence of domain-specialized models will also drive multimodal innovation. Models trained on industry-, role- or use-case-specific data will be increasingly multimodal (e.g., legal, finance, healthcare, marketing and multimedia). World models will also create new multimodal opportunities in physical AI.
- **Improved user experience (UX):** Multimodality improves UX by enabling richer experiences as it meets users with the data that is available. The ability to interact with both unstructured and structured data is supporting additional use cases within the organization.
- **Extensibility of automation:** Multimodality supports new tasks, such as data extraction, data manipulation (converting one data type to another) and creating new data outcomes. Multimodal applications will have a higher automation potential, and the use of multimodality with agentic automation will create new use case opportunities. By 2030, multimodality will increase AI automation potential by 50% with new functionality and use cases.

Obstacles

Multimodal GenAI models are primarily inhibited by:

- **Training challenges:** Multimodal data has varying degrees of quality and formats compared to unimodal data, amplifying challenges with training costs and time, as well as potential inaccuracies and biases in output from multimodal data sources.
- **Lack of data:** Data availability may be limited in some modalities (e.g., large-scale audio datasets or healthcare imagery), which impacts model training and accuracy.
- **Data governance:** Multimodal GenAI increases the exposure to a wider range of sensitive data. Examples of particularly sensitive data types include maps or geolocation data, biometric data or health data. Enterprise governance standards and the lack of regulations and standards are also inhibiting capability advancement.
- **Lack of application experience:** Best practices, testing methods, software libraries and supporting tools have not been fully developed to enable multimodal applications.

User Recommendations

- Identify two or three modalities that are most important to your organization when choosing which GenAI model to use for which use case.
- Evaluate and explore use cases where multimodal capabilities may offer differentiating capabilities or new opportunities that are out of reach of unimodal offerings.
- Assess the technical complexities of processing and integrating data inputs and outputs from diverse multimodal sources, and the potential risks and controls required for using agents to automate tasks based on multimodal inputs.
- Create specific cross-modal data policies and tools aimed at protecting privacy, detecting bias and ensuring compliance with emerging AI regulations.

Sample Vendors

Alibaba Cloud; Anthropic; Archetype AI; DeepSeek; Google; Microsoft; Mistral AI; OpenAI; Stability AI; TwelveLabs

Gartner Recommended Reading

Emerging Tech: Multimodal Generative AI Interfaces Transform User Experiences

Emerging Tech Impact Radar: Generative AI

Emerging Tech: Data Fabrics With Multimodal Data Focus for Generative AI-Enabled Applications

Emerging Tech: Unlock Multimodal GenAI's Potential to Drive Differentiation

Multimodal AI

Analysis By: Nick Ingelbrecht, Sushovan Mukhopadhyay, Yogesh Bhatt

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Multimodal AI models are trained with multiple types of data (also known as modalities) simultaneously, such as images, video, audio and text. This enables them to create a shared data representation to improve performance in different tasks. At runtime, they can handle more than one modality, either in their inputs, their outputs or both.

Why This Is Important

Multimodal AI adds significant new technology capability and insight, and spurs new specialized applications. New use cases such as visual question answering of image frames, manufacturing optimization, and fraud detection in banking and finance deliver significant business value outcomes. The physical world and the data it generates are inherently multimodal. By integrating and analyzing diverse data sources, a more comprehensive evaluation of complex environments and tasks can be achieved.

Business Impact

Gartner forecasts that:

- Over the next five years, multimodal AI will become increasingly integral to capability advancement in every application and software product across all industries.
- By 2030, 80% of generative AI (GenAI) solutions will be multimodal (text, images, audio and video), up from 10% in 2025.

Drivers

Multimodal AI adoption will generate cross-sector transformational opportunities. Key drivers:

- A paradigm shift will occur from traditional, linear processes to dynamic, AI-driven systems where humans and machines collaborate seamlessly. Further evolution of agentic AI will involve increasing integration with multimodal AI techniques to handle the complexity and richness of real-world data and tasks.
- Recent AI advances, particularly in the realm of large language models (LLMs) and vision language models (VLMs), are driving multimodal AI development. These advancements have catalyzed a renaissance in natural language processing and computer vision.

- Intelligent applications, by their nature, are context-rich and designed to adapt to constantly changing scenarios. This makes multimodal AI a crucial component for intelligent applications' development and evolution.
- World models are a significant driver for multimodal AI because they inherently require the ability to process and understand information from various modalities to accurately represent and simulate the complexity of the real world.
- Broader availability of AI/GenAI multimodal models, both proprietary and open-source, lowers the barriers to entry and adoption via AI marketplaces.
- There is a demand for multimodal domain-specialized models in areas such as healthcare, where multimodality extends or enriches use cases.

Obstacles

Multimodal AI is powerful in understanding and processing various modalities, but faces several primary obstacles to adoption:

- Integrating diverse data types is challenging due to differences in format and time stamps, risking inaccurate interpretations. Multimodal AI models are complex, combining various modality-specific subnetworks, which can obscure transparency and explainability.
- Architectural complexity, increased data volume and the need for data fusion lead to inference latency, hindering reliable operation where immediate decision making is crucial.
- Dataset bias originates from leveraging training datasets, which may inadvertently reflect societal or cultural biases. This can result in making unfair or inaccurate predictions/decisions.
- Handling sensitive data across modalities increases breach risks and privacy violations. This complicates compliance with privacy regulations as multimodal AI exposes new attack surfaces and heightens privacy risks with diverse data types.

User Recommendations

Organizations looking to implement multimodal AI should:

- Identify AI use cases where multimodal AI can enhance business value beyond unimodal AI foundation models.

- Run pilots with off-the-shelf multimodal models to demonstrate not only technical feasibility but the business value.
- Build a strong model evaluation by assessing the quality of relationships between modalities, such as comparing generated captions from images to ground-truth labels/descriptions.
- Prioritize building or accessing robust data infrastructure supporting the collection, storage and processing of diverse data types.
- Build or acquire expertise to handle the technical complexities of processing and integrating multimodal data with legacy and existing workflows.
- Create or extend AI governance strategies and policies to address challenges with multimodal datasets.
- Incorporate multimodality into technology roadmaps and create migration paths for multimodal AI in systems procurement.

Sample Vendors

Aimesoft; Google; Hugging Face; Jina AI; Meta; Midjourney; NVIDIA; OpenAI; Stability AI; TwelveLabs

Gartner Recommended Reading

Emerging Tech: Generative AI's Path to Revolutionary Computer Vision Products

Emerging Tech: Multimodal Generative AI Interfaces Transform User Experiences

Innovation Insight: Multimodal AI Explained

Emerging Tech: AI Vendor Race: Agentic Vision AI Revolutionizes Security, Health and Safety Monitoring

NR-RedCap

Analysis By: Kosei Takiishi

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

New Radio Reduced Capability (NR-RedCap) is a 5G specification introduced in 3GPP Release 17 that defines a class of devices with reduced complexity, bandwidth and power consumption compared with full 5G NR. It targets midtier IoT and connected devices by balancing performance and efficiency. As of 2026, NR-RedCap is emerging as a complementary option between LTE-based IoT and full 5G, with evolving deployment scenarios.

Why This Is Important

Existing cellular IoT technologies either focus on low-power, low-data applications (e.g., NB-IoT, LTE-M) or high-performance use cases (e.g., 5G eMBB), leaving a gap in intermediate requirements. NR-RedCap addresses this gap by supporting devices that require moderate throughput and latency with lower complexity than full 5G. However, its near-term importance depends on the emergence of clear use cases where LTE-based IoT or full 5G are not sufficient.

Business Impact

- **Midtier IoT enablement:** Supports new device categories such as advanced wearables, industrial sensors and video-enabled IoT.
- **Network consolidation opportunity:** Provides a potential pathway to reduce reliance on legacy IoT technologies over time.
- **Flexible device ecosystems:** Expands device options between low-power IoT and high-performance 5G devices.
- **Uncertain commercial value:** Business impact depends on identifying use cases that justify its performance and cost positioning.

Drivers

- **Gap between LTE-based IoT and 5G performance tiers:** Existing technologies such as NB-IoT and LTE-M address low-power, low-throughput use cases, while 5G NR targets high-performance IoT applications, leaving unmet intermediate requirements.
- **Demand from vertical industries:** Industries such as manufacturing, automotive and healthcare require devices with moderate bandwidth, lower latency and longer battery life than traditional IoT technologies.
- **Transition from legacy networks:** CSPs are phasing out 2G/3G and optimizing 4G/5G networks, creating demand for new IoT solutions that can operate within modern 5G architectures.
- **Ecosystem and standardization maturity:** 3GPP standardization in Release 17 and beyond is enabling device and network support, although ecosystem maturity remains early.
- **Device innovation opportunities:** NR-RedCap enables new device form factors and capabilities, particularly where full 5G is unnecessary and LTE-based IoT is insufficient.

Obstacles

- **Unclear use case definition:** It remains uncertain which applications specifically require NR-RedCap instead of LTE-M, NB-IoT or full 5G.
- **Limited monetization models:** The business value for CSPs and enterprises is not yet well established.
- **Technology positioning complexity:** NR-RedCap adds another option to an already fragmented IoT connectivity landscape.
- **Ecosystem immaturity:** Device availability, chipset support and large-scale deployments are still developing.

User Recommendations

- Identify specific use cases where moderate performance, latency and power requirements cannot be efficiently met by LTE-based IoT or full 5G before committing to NR-RedCap.
- Avoid positioning NR-RedCap as a universal IoT solution and instead treat it as a targeted option within a broader multitechnology strategy.
- Align NR-RedCap adoption with long-term network evolution plans, including legacy network retirement and 5G expansion.
- Engage with device vendors and ecosystem partners early to validate availability, performance and interoperability.

Sample Vendors

Ericsson; Huawei; Nokia; Qualcomm; ZTE

Gartner Recommended Reading

Magic Quadrant for CSP 5G RAN Infrastructure Solutions

Critical Capabilities for CSP 5G RAN Infrastructure Solutions

Sliding into the Trough

LEO Satellite IoT

Analysis By: Peter Kjeldsen

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Low Earth orbit (LEO) satellites offer low-power communications with a global footprint to collect data from Internet of Things (IoT) endpoints for tracking or sensing. Data is generally in the form of short messages made available through a cloud service. Low power consumption may allow battery life of five or more years.

Why This Is Important

Global IoT connectivity using cellular services typically involves complex roaming arrangements and cannot provide coverage everywhere. IoT communication using LEO satellites can provide affordable global coverage for low-bandwidth, message-oriented communications used in applications such as tracking and sensing.

Business Impact

Being able to track and communicate with IoT devices anywhere creates a wide range of opportunities. This eliminates blind spots in global supply chains, reducing insurance premiums and operational losses. Data from remote sites allows for predictive maintenance, preventing costly equipment failures. Applications include supply chain management and visibility, monitoring sensors in remote locations, global connectivity to vehicles, and smart agriculture.

Drivers

- Enterprises need global visibility into supply chains and operations, and suitable communications often aren't available from terrestrial cellular networks or require backup and/or redundancy options.
- The industrialization and privatization of space have reduced the cost of satellite development, deployment and operations.

- Reduced technical and commercial entry barriers have encouraged new providers and business models.
- Hardware developers can create a single product version that can operate globally without the complexity of supporting many cellular frequency bands.
- 3GPP has standardized some 5G communications with nonterrestrial networks (NTN) and will add further standards in the future to benefit organizations that prefer to avoid proprietary solutions.
- Terrestrial LPWA protocols such as LoRa and Bluetooth have been repurposed for satellite operations, reducing cost, complexity and risk.
- Modern LEO satellites can now process data in orbit with edge computing rather than just sending everything back to Earth. This allows for immediate filtering of IoT data, sending only critical alerts to the ground, saving time, bandwidth and cost.

Obstacles

- The technology is typically limited to outdoor use cases as satellite services usually require line of sight and struggle to penetrate buildings.
- Communications may be one-way only — collecting data from IoT endpoints but with no ability to update firmware or make changes remotely.
- In-building use cases sometimes require an external antenna that may not be practical in all locations.
- There are many new vendors entering this domain; not all will survive.
- Competitive pressure is driving down the cost of terrestrial IoT connectivity, making satellite service comparatively more expensive (if still affordable).
- Not all services are truly global, with regulatory licensing of radio spectrum access still proving a barrier to some services.
- LEO satellite services typically support short messages with high latency (e.g., from trackers and sensors) and are unsuitable for large messages or high data rates (e.g., for video or firmware updates).
- Many systems use nonstandard protocols and don’t support Internet Protocol (IP) connectivity.

User Recommendations

- Complement IoT connectivity services by including satellite communication as a global network option in IoT deployments where terrestrial communication options are limited or unavailable.
- Consider hybrid solutions where standards such as LoRa and/or NB-IoT may enable roaming between satellites and terrestrial communication services.
- Identify projects where gateway solutions may provide an additional option using a satellite-connected hub to backhaul local endpoints equipped with LPWA network technologies.

Sample Vendors

Astrocast; Lacuna Space; Myriota; ORBCOMM; SAT4M2M

Gartner Recommended Reading

Market Guide for Satellite IoT Services

Market Trend: Emerging Use Cases for LEO Satellite Communication Services

5G Core

Analysis By: Peter Liu

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

The 5G core is the foundational hardware, software, and services layer through which CSPs deliver reliable and secure mobile connectivity in 5G stand-alone (SA) deployments. Built on a cloud-native, service-based architecture, it underpins access and mobility management, authentication, subscriber data management, policy control, and session routing. Unlike non-stand-alone alternatives, SA enables network slicing, ultra-low latency, and granular QoS control.

Why This Is Important

- 5G SA unlocks network slicing, ultra-low latency, and massive IoT — forming the substrate for edge AI inference, autonomous systems, and mission-critical enterprise applications.
- The shift to cloud-native, service-based architecture enables CSPs to deploy and scale network services with software-like agility, reducing time-to-market and operational costs.
- Open APIs enable CSPs to embed programmable network intelligence into enterprise workflows and AI-driven service chains.

Business Impact

The cloud-native 5G Core, with open APIs and Service-Based Architecture (SBA), speeds up service deployment and revenue agility. It enables new B2B income through network slicing for SLA-backed enterprise services and acts as a platform to accelerate AI-native application development. This programmable foundation is essential for the physical-digital economy, supporting edge AI, Industrial IoT, and AR/VR, and centralizing CSPs' role.

Drivers

- **Mobile infra monetization:** CSPs accelerating 5G stand-alone deployments require the 5G core as the mandatory technical foundation for advanced capabilities for service creation unavailable in non-stand-alone architectures.
- **Operational transformation:** Cloud-native, service-based architecture with open APIs enables more agile, automated, and resilient operating models — reducing dependency on monolithic vendor stacks.
- **AI-driven network intelligence:** NWDAF embeds real-time analytics and machine learning directly into the 5G core, enabling autonomous network management such as proactive service assurance, and data-monetization opportunities.
- **Open ecosystem economics:** Service-based architecture lowers barriers to entry, enabling best-of-breed and fit-for-purpose vendor assembly without end-to-end solution mandates — accelerating innovation and price competition.
- **Private network expansion:** The increasing enterprise demand for reliable and secure private wireless infrastructure, primarily utilizing 5G stand-alone (SA) architecture, is driving significant expansion in core network deployments.

Obstacles

- **Migration complexity:** Transitioning from legacy EPC to cloud-native 5G core involves a substantial increase in service enablement capabilities that demand significant technical expertise, organizational change management, and phased architectural transformation — raising execution risk for most CSPs.
- **Capital and ROI constraints:** Lack of GTM strategy and substantial infrastructure, equipment, and licensing investment — without mature monetization paths for advanced capabilities beyond eMBB — leads many CSPs to defer SA adoption in favor of extended NSA deployments.
- **Expanded attack surface:** Disaggregated, distributed architecture introduces new security exposure, requiring zero-trust frameworks, API security governance, and continuous threat monitoring across a broader perimeter.
- **Cloud-native skills shortage:** Insufficient internal expertise in cloud-native development, DevOps/AIOps, and automated operations constrains deployment velocity and long-term operational efficiency.

User Recommendations

- Focus your 5G stand-alone strategy and roadmap on the 5G core. The chosen core must enable smooth migration from NSA or interoperability with LTE, ensuring a clear path to ROI.
- Adopt an open, disaggregated 5G core with microservices and multivendor capabilities. Work closely with vendors across the network stack to overcome cloud environment challenges for efficient deployment and operations.
- Select vendors offering production-ready 5G Core Network Data Analytics Function (NWDAF) for AI-driven operations. This enables real-time closed-loop automation, intelligent traffic steering, and easy integration with external AI/ML platforms. Analytics are critical.
- Test 5G cores from nonincumbent vendors in a limited environment, like a PMN. PMN use cases are typically more advanced than public networks but require less capacity and are easier to deploy.
- Engage in continuous real-time testing, assurance and CI/CD pipeline management across vendors to increase the probability of success.

Sample Vendors

Ericsson; Huawei; Mavenir; Microsoft; NEC; Nokia; Oracle; Reliance Industries (Jio Platforms); Samsung Electronics; ZTE

Gartner Recommended Reading

Magic Quadrant for CSP 5G Core Network Infrastructure Solutions

Critical Capabilities for CSP 5G Core Network Infrastructure Solutions

Top Technology Trends for CSP CIOs in 2025

Market Trend: The Mobile AI Era Will Revolutionize 5G Adoption and Monetization

5G Network Slicing: Unlock New Revenue With Near-Term Use Cases

CPS Network Cloaking and Segmentation

Analysis By: Katell Thielemann, Thomas Lintemuth

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Cyber-physical systems (CPS) cloaking and segmentation includes solutions that discover existing network topologies, manage firewalls, create enclaves that cloak networks, or optimize zones and conduits to prevent the spread of malware or sensitive-data exfiltration.

Why This Is Important

CPS network cloaking and segmentation is essential for securing critical cyber-physical systems (CPS) environments. By mapping networks, managing firewalls and creating cloaked security zones (segmentation), it prevents unauthorized lateral movement, north-south cyber attacks from IT to production systems, and insider threats. This radically reduces the risk of cyber attacks that might exfiltrate intellectual property or impact visibility into physical process control.

Business Impact

CPS network cloaking and segmentation deliver significant business impact by improving operational resilience through logical separation of sites and process control systems from business networks. This reduces the attack's blast radius via optimized access control and partitioning of production lines. Optimized access control within and between zones ensures only authorized individuals or systems can access assets or perform tasks, thereby reducing the blast radius in case of an attack.

Drivers

- **Evolving threat landscape:** An increase in attacks, notably ransomware-related, has led companies to proactively shut down operations out of concern for potential malware spread to CPS environments.
- **Containment:** Enterprises are more aware that having very large trust zones at a facility increases risks. Dividing a network into smaller segments or zones makes it harder for attackers to move laterally.
- **Best practices and security frameworks recommendations:** Zoning and segmentation is a core recommendation in industry-recognized frameworks such as NIST SP 800-82 Rev. 3 and ISA/IEC 62443.
- **Compliance:** Several industry regulations and standards, such as NERC-CIP, require organizations to implement network segmentation as part of their security measures. Compliance with these regulations is essential for avoiding penalties, maintaining customer trust and protecting sensitive data.
- **Improved performance:** Segmentation can improve network performance by reducing congestion and optimizing traffic flow.
- **Scalability:** Zoning and segmentation allow for new devices or systems to be added to specific segments without impacting the entire network.

Obstacles

- **Lack of visibility and complexity:** Lack of visibility into the network and its components as well as potentially unknown interdependencies, where different components or processes rely on each other to function properly, pose a hurdle.
- **Operational impact:** Zoning and segmentation may introduce additional network complexity and constrain bandwidth, potentially affecting operational performance.
- **Limited resources and expertise:** Many organizations full of CPS lack budgets and skilled personnel with the required security and engineering know-how.
- **Operational constraints:** In certain critical infrastructure sectors, such as energy or manufacturing, downtime or disruptions can have significant financial and safety implications.
- **Fear of the unknown:** Production or plant owners may be wary that cybersecurity efforts will introduce production risks.
- **Security portfolio complexity:** They provide yet another tool for security teams to deploy and manage.

User Recommendations

- Deploy CPS protection platforms to discover all CPS assets and gain visibility over existing network topologies.
- Work with engineering teams to architect security zones around physical process loops based on criticality, safety, risk profiles and operational constraints. Each zone should have a specific purpose and level of security controls.
- Use network segmentation technologies to create isolated network segments and control traffic flow between zones.
- Deploy cloaking or obfuscation solutions to hide the CPS assets and networks from direct access.
- Apply the principle of least privilege to limit user access rights and privileges to only what is necessary for specific roles, enforcing policies through gateways around users, assets, application and controllers.
- Monitor and log network traffic within each security zone. This enables the detection of suspicious activities and helps in incident response.

Sample Vendors

BlastWave; Blue Ridge Networks; ColorTokens; Elisity; Seclab; Xage Security; Zero Networks; ZeroTier

Gartner Recommended Reading

Pros and Cons of Using Corporate Active Directory for Your CPS

Network Slicing

Analysis By: Susan Welsh, Peter Liu

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Network slicing refers to a set of capabilities that allow communications service providers (CSPs) to create isolated end-to-end logical networks in the form of network slices on top of a common shared physical network infrastructure. Each slice can be customized to provide a specific performance profile based on the requirements for distinct end-user needs, driving revenue opportunities.

Why This Is Important

Network slicing enables 5G monetization and cost-efficiencies for the CSP. Slices can be tailored to meet specific needs of applications, services, devices, customers or operators delivered as a value-added service. Slicing can also optimize the allocation and management of network resources to meet specific performance requirements (e.g., required bandwidth, speeds, latency and reliability) for different use cases.

Business Impact

Network slicing is an essential capability to fully extract value from infrastructure investments in mobile and fixed networks through new revenue opportunities. In the case of dynamic slicing, it can increase infrastructure utilization and economic efficiency. CSPs can offer business customers access to highly customized network slices tailored to specific requirements in a cost-effective, timely and efficient way that can be backed by an SLA.

Drivers

- Slicing enables composable services creation across network domains and elements, increasing service creation agility. It uses standardized processes, driven by slice templates or well-defined APIs, to deliver desired service parameters over 5G networks that can be quantified in an SLA.
- Slicing enables CSPs to deliver industry-tailored SLAs to vertical industries in their digital transformation efforts and integrate connectivity, cloud services and sensor data into mission-critical operations. For example, AI on edge computing applications that need secure and reliable low-latency/high-bandwidth connectivity. Slicing is also being deployed inside private mobile networks for a range of use cases and service needs.
- Broader commercial deployments of stand-alone (SA) 5G core will serve as a catalyst for more rapid growth of network slicing in commercial service offerings.
- Advancements in commercial deployments are targeting a range of use cases. They include support for fixed wireless access, architecture options for private and hybrid mobile networks, public safety priority access and premium connectivity, and video broadcasting and point-of-sales terminals support for live events. These are providing lessons to support further commercial slicing use cases and deployments.
- More slicing use cases are enabled by increased incorporation of network slicing capabilities in end-user devices. For example, UE Route Selection Policy (URSP) and support from mobile device management or more comprehensive unified endpoint management (UEM) solutions for slice management.
- The use of open APIs to expose network quality on demand is expanding the ecosystem, thus raising awareness for slicing capabilities in developer and end-user communities.
- Network slicing helps improve security and customer data traffic management to minimize potential interference with data and control information from other slices by isolating each slice in operations. This enables slices on the public network to more cost-effectively deliver private networking services, bringing benefits downstream to smaller businesses through affordable offers.

Obstacles

- Some CSPs lack capabilities to support 5G network slicing at scale, including comprehensive network inventory, automated data-driven operations, dynamic orchestration for low-touch operations to manage subdomains/subnets, test and assurance of SLAs, and 5G charging.
- Widespread commercial deployment of 5G SA is limited, delaying broader slicing implementation.
- Lack of reports of strong revenue generation at scale from commercially deployed use cases for 5G network slicing hampers investment decisions by other CSPs.
- The lack of consistent slicing capabilities across CSPs to encourage developer communities to incorporate slicing into B2B, B2C and B2B2X applications increases the time to generate demand and revenue from network slices.
- A siloed approach to network infrastructure requires new capabilities to coordinate security policy among different domain infrastructures. For app-based requests to connect to a slice, identity verification and other security concerns must be addressed.

User Recommendations

- Evaluate technologies and use cases by working with vendors and customers to co-develop solutions, identify operational gaps and measure business impact.
- Drive customer centricity by focusing on business outcomes. Work with product teams to translate how technology features can help solve problems or create opportunities for end customers.
- Determine how network capabilities will be exposed to application developers to facilitate those outcomes.
- Implement key enablers; for example, a software-defined network, cloud virtualized radio access networks, edge computing, cloudification, real-time inventory, 5G core and 5G charging, and increased automation capabilities.
- Identify ways to deliver cost optimization while supporting revenue growth. Work with vendors to get the right out-of-box functionality, low-code solutions to support use by business units, flexible procurement for pay-as-you-grow and business models that fit the targeted use cases.

Sample Vendors

Amdocs; Ciena (Blue Planet); Cisco; Ericsson; Google; Huawei; Nokia; ZTE

Gartner Recommended Reading

Market Guide for CSP Service Design and Orchestration Solutions

Market Guide for CSP Service and Network Assurance Solutions

5G Network Slicing: Unlock New Revenue With Near-Term Use Cases

Critical Capabilities for CSP 5G Core Network Infrastructure Solutions

CSP Open APIs

Analysis By: Amresh Nandan, Ajit Patankar

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Communications service provider (CSP) open APIs refer to publicly available APIs that allow developers programmatic access to CSP IT and operational technology (OT) applications. Such APIs, often developed by a commercial entity, industry body, or industry standardization/specification organization, are designed for ease of integration, utilization of data and functionalities, and monetization of network assets/capabilities.

Why This Is Important

CSPs are increasingly adopting open APIs for better modularity, faster integration and reduced vendor lock-in, and to foster innovation. Integration and monetization requirements have forced detailed specification and standardization by industry bodies, such as the 3rd Generation Partnership Project (3GPP), European Telecommunications Standards Institute (ETSI), TM Forum, Mplify Alliance, CAMARA project, and GSMA.

Business Impact

With increase in modularity of applications and microservices architecture, adopting open APIs for faster, easier, and cost-effective integration is crucial. Open APIs can have a big business impact, but their success depends on their adoption level, which has improved significantly across CSPs and vendors in recent years. Vendors' implementation of open APIs has increased due to CSPs' compliance requirements in their RFPs, leading to improved and faster integration of typical business support system (BSS) and operations support system (OSS) applications.

Drivers

- There are over 100 TM Forum Open APIs available, with more than 1,700 API certifications, downloaded extensively by thousands of companies. On the network exposure side, the CAMARA 2025 meta release brings the total to 60 APIs, including several new APIs, backed by more than 1,000 contributors from more than 400 organizations. GSMA Open Gateway is supported by more than 75 mobile CSPs groups, representing close to 300 networks.
- Majority of CSPs have adopted TM Forum Open APIs. There are some key reasons for end-user adoption of open APIs:
  - The desire to achieve greater freedom in sourcing, seamless integration and lower operational costs.
  - The ability to expose certain standard APIs for utilization by enterprises and developers (such as for private mobile network requirements).
  - To drive innovation via developers.
  - Network APIs will become a necessity for CSPs in the next 12 to 15 months.
- In addition, such APIs by industry bodies are often specified or developed in a collaborative manner, leading to early identification of nuanced requirements and integration challenges.
- CSPs sourcing technologies from multiple vendors is the most appropriate way for faster and cost-effective interoperability.
- As CSPs look toward developing and participating in ecosystems (such as GSMA Open Gateway), open APIs are a necessity to expose data and functionalities, while enabling simultaneous secure integrations with industry verticals and other partners.
- CSPs are increasingly tracking the level of TM Forum open API adoption and certification by vendors through their RFIs and RFPs.
- The 5G network data analytics function (NWDAF) and network exposure function (NEF) have further boosted the idea of standard/open APIs for better management and monetization of the network.

- Overall, the industry is in a steady adoption and early monetization phase. Internal APIs are maturing, partner APIs are growing, and external monetization APIs are emerging.

Obstacles

- Security and privacy are the industry's top concerns regarding network APIs, with authentication issues and shadow APIs posing risks.
- Inadequate security and lack of user-friendliness impact some developers and affect the pace of adoption.
- The continuation of old solutions and architectures in many CSPs is an obstacle for open API implementation, though some CSPs have been working on overlay mechanisms.
- Even though vendors' adoption of open APIs has increased, some continue to exhibit reluctance in implementing open APIs, unless forced by their key customers.
- Some vendors have developed their own set of APIs and project them as analogous to open APIs. Such an approach adds complexities and fragmentation to open API adoption.

User Recommendations

- Develop your integration strategy as a standard guideline for using standard and open APIs, and alternate mechanisms (such as your own or vendor-supplied) where such APIs are unavailable.
- Update your procurement process to assess the adoption of open APIs by vendors as a critical evaluation criterion during the vendor evaluation process.
- Negotiate the implementation of open APIs by vendors in their implementation, as and when they are available, through contract terms and conditions.
- Dedicate resources for participation in API development initiatives, trials, and pilot programs, as the effectiveness of such APIs takes time and investment.
- Ensure access to development resources and support the efficient use of open APIs to enable partners. Examples of such initiatives include TM Forum's Open API Catalyst programs, where many CSPs and vendors participate to address specific challenges.
- Participate in industry open API programs that offer CSPs ways to monetize network assets with ecosystem-based or platform-based business models.

Gartner Recommended Reading

Objectives and Principles for OSS Architecture Evolution in CSPs

Market Guide for CSP Service Design and Orchestration Solutions

Market Guide for CSP Customer Management and Experience Solutions

Market Guide for CSP Revenue Management and Monetization Solutions

Private LTE

Analysis By: Sylvain Fabre

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Private LTE is a private wireless network based on 4G/LTE technology infrastructure, which interconnects people/things in an enterprise setting. It can borrow licensed spectrum owned by a communications service provider (CSP) or dedicated spectrum allocated by local regulations independent of CSPs' networks. 4G/LTE can support voice, video, messaging, broadband data and IoT, with increased security and predictable connectivity performance because the infrastructure is not shared publicly.

Why This Is Important

Enterprises can customize their own private Long Term Evolution (LTE) performance with specific service-level agreements, enabling networks for mission-critical, latency-sensitive applications. This can be implemented either leveraging a licensed communications service provider (CSPs') spectrum, or with a dedicated spectrum. Private LTE also enables wireless coverage in areas where CSPs do not provide adequate coverage from public cellular infrastructure.

Business Impact

Industry verticals require private LTE connectivity to ensure reliable, secure wireless operations for specialized applications within controlled environments. Private LTE enhances productivity and reduces costs by providing predictable, low-latency connectivity for AGVs, remote-controlled machinery, and real-time asset tracking in complex settings — like underground mines and metallic manufacturing floors — where public cellular or Wi-Fi is insufficient.

Drivers

- **Wi-Fi and low-power wide-area (LPWA) limitations:** Many industries have deployed wireless network technologies such as Wi-Fi and non-3rd Generation Partnership Project (3GPP) LPWA networks, but these cannot assure high data throughput, mobility and reliable communication assured by private LTE.
- **Expanded enterprise procurement options:** Technology vendors and system integrators now offer Private LTE solutions directly to enterprise customers, reducing traditional reliance on communications service providers (CSPs). This increased competition enables enterprises to select highly flexible OpEx pricing models, such as Network-as-a-Service, and choose partners best suited to their specific factory or operational requirements.
- **Global democratization of spectrum:** The growing availability of dedicated industrial and shared spectrum frameworks — such as localized enterprise licensing in Europe and the Americas — enables organizations to independently secure network frequencies. This regulatory shift breaks traditional carrier monopolies and significantly expands the pool of potential private LTE providers for enterprise buyers.
- **Proven maturity and device ecosystem:** While 5G attracts significant attention, consistent GSA data shows that about half of all PMN deployments currently use private LTE (see GSA: The Industry Voice Of The Global Mobile Ecosystem. This widespread adoption is driven by LTE's mature, cost-effective device ecosystem and its proven ability to deliver immediate ROI, especially as the broader rollout of 5G IoT devices is still underway.
- **Data privacy and network isolation:** Enterprises increasingly require enhanced data privacy, strict isolation from public cellular networks, and stronger authentication than legacy Wi-Fi can provide. Private LTE enables organizations to process and retain sensitive OT data entirely on-premises, minimizing attack surfaces and meeting stringent data sovereignty mandates.

Obstacles

- **Geographic spectrum limitations:** Private spectrum availability remains fragmented and limited in certain regions, creating regulatory hurdles for enterprises seeking to deploy homogeneous blueprints.
- **Niche ROI justification:** Lack of clear ROI for private LTE deployment, except in cases where reliable wireless coverage across large facilities is the only cost-effective connectivity solution for enterprise operations.
- **Mission-critical redundancy costs:** Achieving high uptime SLAs for critical industrial environments requires redundant architectures — like dual on-site servers, geo-redundant cores, and overlapping backhaul. This level of resilience adds significant technical complexity and raises total cost of ownership.
- **The "5G Shadow" and technology coexistence:** Enterprises hesitate to invest in private LTE as private 5G expands. Concerns include migration paths, coexistence on industrial campuses, and whether to deploy private LTE over shared bands (e.g., CBRS) while 5G matures.

User Recommendations

- Enhance competitiveness by bundling private LTE with advanced network capabilities — unified SIM management, closed-loop automation (self-healing), and seamless national roaming. Differentiate your offering further by integrating rich communication services (VoLTE, video, messaging) for comprehensive on-site operations.
- Accelerate enterprise adoption by developing vertical-specific blueprints through partnerships with industrial ecosystem players. Deliver preintegrated, repeatable private LTE configurations tailored to the compliance, security, and operational needs of each vertical (e.g., manufacturing, mining), reducing deployment complexity.
- Alleviate enterprise hesitancy by articulating a clear 4G-to-5G migration path. Provide transparent technology roadmaps detailing coexistence of private LTE and private 5G on industrial campuses, and design networks to minimize interference and operational disruption for clients transitioning to 5G stand-alone architectures.

Sample Vendors

AT&T; China Mobile; DRUID; Ericsson; Hewlett Packard Enterprise; Huawei; Nokia; Vodafone; ZTE

Gartner Recommended Reading

Tool: Attractiveness Index for Private Mobile Networks Technologies

Critical Capabilities for 4G and 5G Private Mobile Network Services

Magic Quadrant for 4G and 5G Private Mobile Network Services

How to Craft Comprehensive Private Mobile Network Offerings for Enterprises

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

Edge AI

Analysis By: Akhil Singh, Walker Black

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Edge AI is the use of AI techniques embedded in non-IT products (consumer, industrial) and distributed devices for autonomous operations in manufacturing, energy utilities, defense, and aerospace. It enables local processing of distributed AI workloads, syncing with cloud environments. Devices include servers, IoT gateways, robotics, autonomous vehicles, and mobile devices. While predominantly focused on inference, it includes local training, streaming analytics, and swarm or federated learning.

Why This Is Important

Edge AI applies AI techniques for latency-sensitive, data-intensive applications requiring local autonomy — both data sovereignty and operational control. It ensures safe operations and compliance for resource-constrained assets in hazardous, mission-critical settings. This improves reliability via closed-loop feedback to execute automated machine tasks. Specialized on-device models boost privacy and cost efficiency, providing high-fidelity, real-time decision support for regulated applications.

Business Impact

- Real-time data analysis and decision intelligence
- Improved operational efficiency and throughput via automated visual inspection and adjustments
- Enhanced customer experience via embedded AI feedback
- Reduced latency and telemetry bandwidth costs through local inferencing
- Persistent functionality, independent of cloud connectivity
- Optimized storage through localized data filtering and prioritization
- Enhanced data control and privacy at the endpoint, via federated learning and without moving raw data

Drivers

Edge AI has benefited from improvements in AI capabilities, including:

- Maturation of MLOps and ModelOps that simplify use of a broader set of features, moving beyond initial narrow focus on model compression.
- Improved performance of combined ML techniques like optimizing TinyML on resource-constrained microcontrollers and increased data availability (e.g., time-series data from industrial assets).

Business demand driving the use of AI at the edge includes:

- Reduction of full-time equivalents using vision-based solutions for surveillance or inspections.
- Improvement of manufacturing production quality through process automation.
- Optimization of operational processes across industries.
- Use of new approaches to customer experience (CX), such as personalization on mobile devices or edge-based smart check-out points of sale in retail.
- Use of privacy-preserving edges

Additional drivers include:

- More organizations are modernizing legacy environments. MLOps platforms allow AI software to be hosted in edge computers, gateways, or embedded within products.
- Manufacturers are embedding AI in IoT endpoints for product servitization (e.g., automobiles in battery management systems and smart home infrastructure like CCTVs) to run models that interpret captured data and drive endpoint functions.
- Decentralized training for adaptive AI (dynamic autonomy and reasoning) is seeing rising R&D demand, leading to decentralized models at the edge and driven by needs such as data regulations and compliance, or the requirement for machines and processes to run in disconnected scenarios.
- Shifts to advanced architectures that are accelerated by linear-complexity and vision-language-action (VLA) models overcome latency limits to enable autonomous operation across domains.

Obstacles

- High initial installation cost and limitations of deployed equipment (form factor, power budget, data volume, decision latency, security).
- Edge AI systems can be nondeterministic, limiting use cases where safety and security are primary requirements.
- Autonomy of edge AI solutions, built on ML and deep learning, raises trust issues, especially when inferences are not easily explainable. This is amplified as adaptive AI solutions grow, potentially leading to diverging behaviors or data drift across identical models deployed to equivalent endpoints.
- Lack of quality and sufficient industry-specific training data, and high barriers to generating synthetic data.
- Deep learning in neural networks is compute-intensive, requiring high-performance chips with corresponding high-power budgets, restricting deployment in locations needing small-form factors and low power.
- Memory optimization in models through quantization and pruning is a hurdle for microcontroller scaling.

User Recommendations

- Determine whether edge AI use provides suitable cost-benefit improvements or whether traditional centralized data analytics and AI methodologies are adequate and scalable.
- Evaluate when to consider AI at the edge versus a centralized solution. Good candidates for edge AI are applications that have high communications costs, are sensitive to latency, require real-time responses or ingest high volumes of data at the edge.
- Repurpose existing customer infrastructure and focus on improving integration capabilities to speed up time to market for edge AI solutions, prioritizing interoperability and deployment over requiring customers to replace current hardware.
- Use edge gateways and servers as the aggregation and filtering points to perform most of the edge AI and analytics functions. Make an exception for compute-intensive endpoints, where AI-based analytics can be performed on the devices themselves.

Sample Vendors

Arm; Barbara; IFS.ai; Johnson Controls; NVIDIA; Pratexo; Qualcomm; Siemens; SiMa.ai; Synadia

Gartner Recommended Reading

Emerging Tech Impact Radar: Edge Artificial Intelligence

Innovation Insight for Edge AI

Emerging Tech: Differentiate With an Edge AI Benchmarking Strategy

Market Guide for Edge Computing

Emerging Tech: Empower Outcome-Centric IoT With AI

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

Climbing the Slope

Network Security Microsegmentation

Analysis By: Adam Hils, Rajpreet Kaur

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Network security microsegmentation is the creation of more granular and dynamic access policies than is possible in traditional network segmentation. It is deployed by the insertion of a security control between workloads, applications, or nodes in the same segment. Microsegmentation tools support the implementation of finer-grained zoning across public, private and hybrid cloud infrastructures. The local enforcement points are orchestrated by management consoles.

Why This Is Important

Once a system is breached, attackers often attempt to move laterally (including in ransomware attacks), which can cause serious damage. Microsegmentation seeks to limit the propagation and spread of such attacks. It can greatly reduce the initial attack surface as well. In addition to security enforcement, microsegmentation products also provide enhanced visibility into network traffic as well.

Business Impact

Microsegmentation reduces attack surface and enables breach containment of cyberattacks. It is a component of zero-trust architecture that controls the access between workloads and is used to limit lateral movement, if and when an attacker breaches the enterprise network. Microsegmentation also enables enterprises to enforce consistent segmentation policies across on-premise and cloud-based workloads, including those hosting containers.

Drivers

- As servers are being virtualized, containerized or moved to infrastructure as a service (IaaS), existing safeguards such as traditional firewalls, intrusion prevention solutions and antivirus software struggle to follow the fast pace of deployment for new assets. This leaves the enterprise vulnerable to attackers gaining a foothold and then moving laterally within enterprise networks. This has created increased interest in visibility and granular segmentation for east-west traffic between applications, servers and services in modern data centers.
- Zero-trust approaches are expanding and are now a requirement in modern data center design. Microsegmentation is cited by zero-trust frameworks as a practical way to build a secure policy-driven infrastructure.
- The increasingly dynamic nature of data center workloads makes traditional network-centric segmentation strategies difficult to manage at scale, if not impossible to apply.
- Microsegmentation products provide rich application communication mapping and visualization, allowing data center teams to identify which communication paths are valid and secure.
- The shift to application microservices has increased the amount of east-west traffic and further restricted the ability of network-centric firewalls to provide segmentation.
- The extension of data centers into IaaS has placed a focus on software-based approaches for segmentation — in many cases, using the built-in segmentation capabilities from cloud-based vendors.
- The emerging need to secure CPS environments is driving an interest in microsegmentation for non-IT environments.
- Growing interest in zero-trust networking approaches has also increased interest in using application and service identities as the foundation for adaptive application segmentation policies. This is critical to enforcing segmentation policies in the dynamic networking environments used within container-based environments.

Obstacles

- **Complexity** — If not planned and scoped correctly, microsegmentation projects can lose organizational support before completion.

- **Lack of application dependency knowledge** — Cybersecurity leaders don't know which applications should be communicating with others, sowing doubt in automatically generated protection rules.
- **Legacy network firewalls** — Traditional firewalls can present operational challenges to some microsegmentation solutions when policies overlap or conflict.
- **Organizational dynamics** — Cloud-centric organizations employing DevOps may value agility more than security, believing that any additional security controls will introduce operational friction.
- **Expense** — Full microsegmentation can come at a high price. Many organizations consider microsegmentation to be a net-new budget item.

User Recommendations

- Select zones to microsegment based on the highest risk. Oversegmentation is the leading cause of failure and excessive costs.
- Seek a solution that maps application communication paths and makes policy recommendations, using AI-based policy recommendations.
- Do not use IP addresses or network location as the foundation for east-west segmentation policies. Use logical tags, labels, fingerprints or stronger identity mechanisms to identify workloads.
- Use the microsegmentation style (such as network overlay, host-based, cloud-native and API-based) that best works with your environment, factoring in location (such as on-premises, hybrid and IaaS) and environment (such as containers and virtual machines).
- Focus on automating microsegmentation deployment and changes integrated with the DevOps continuous integration/continuous delivery pipeline to maintain agility.
- Plan for coexistence of traditional firewalls and microsegmentation approaches and seek microsegmentation products that support integrations with firewalls.

Sample Vendors

Akamai; Broadcom; Cisco; ColorTokens; Elisity; Fortinet; Illumio; Palo Alto Networks; Zero Networks; Zscaler

Gartner Recommended Reading

Implementing Segmentation for Zero Trust Networking

Quick Answer: What Is Zero-Trust Networking?

Quick Answer: Where Do I Start With Zero-Trust Initiatives?

Market Guide for Network Security Microsegmentation

IT/OT Integration

Analysis By: Kristian Steenstrup, Jo-Ann Clynch

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

IT/OT integration is the data and process integration of IT and OT systems in an organization. IT/OT integration unlocks the ability to share data across IT systems and OT systems. When IT and OT are integrated, data can be shared more readily and processes linked seamlessly. This requires both technical data integration and organizational integration to deliver a complete solution.

Why This Is Important

IT/OT integration is pivotal for unifying support systems and resources to achieve strategic business objectives. IT/OT integration is crucial not only for accessing OT data more reliably and effectively but also to help manage the OT environment. This can provide benefits by reducing overall support costs and mitigating risks, including cybersecurity, thereby aligning with overarching organizational goals and driving sustainable competitive advantage.

Business Impact

As IT and OT platforms and tools converge, successful digital businesses learn to manage IT and OT together. Responsibility for the systems is shared, even though direct reporting lines of employees managing the systems may not shift. This often exposes flaws in the operating model. It has a potentially significant impact on the organizational structure as fusion teams become the norm and are formalized. IT/OT integration also has the potential to reduce costs and technical debt, which are high priorities for CIOs and heads of I&O.

Drivers

- OT technical integration gives better, more consistent access to OT data. This data is essential for operational decisions, such as adjusting and responding to production events, managing energy consumption, ensuring environmental sustainability, measuring material consumption, and elevating product quality, safety and reliability.
- IT/OT integration is part of a broader modernization and digitization strategy to improve data management and contextualization. This enhanced capability results in operational cost reduction, increased capacity and competitive improvement.
- The most common data-oriented IT/OT drivers are managing physical equipment (e.g., predictive maintenance using OT data) and reducing manual processes and production downtime.
- Integrated operational intelligence enables better production management, quality control and responses to events in the supply chain, as well as more efficient production processes. The result is a more agile and responsive organization.
- Internet of Things (IoT) and OT data collection needs, integration of IT and OT systems to support initiatives such as digital twins, digital threads, product as a service and equipment as a service.
- IoT and edge computing require IT/OT data unification and governance to achieve an overall data fabric. Aiming for clear end-to-end accountability for data leads to unified data governance.

Obstacles

- Common governance structures are lacking due to the historically siloed approach to managing technology and deeply rooted traditions in many businesses.
- Lack of cross-functional skills and incentives across IT and OT, combined with separate organizational reporting structures, creates challenges.
- Regulatory and budgetary constraints may restrict OT integration. Organizations must remain compliant and adhere to role-based, restricted access requirements.
- Many companies have disparate standards of technology in IT and OT and even different standards for documenting the technologies.
- A common data model spanning IT and OT rarely exists.
- External professional services are available for data integration but rarely for organizational integration, requiring a hybrid in-house/outsourced approach.
- Cyberattacks on OT are perceived to have origins in IT. Thus, most stakeholders in OT will be cautious about “opening the door to ransomware” when integrating IT and OT.
- Old architecture and OT vendor lock-in create challenges.

User Recommendations

- Evaluate the IT/OT integration challenges and benefits specific to your organization.
- Implement common standards across disaster recovery, and use software management to minimize risks such as zero-trust architecture.
- Seek consensus across groups and management. Create an alignment activity first to manage security, governance and standards. Sustainable integration needs IT/OT alignment or points of view will diverge.
- Adopt a progressive approach to integration using fusion teams or a center of excellence (COE) extending to data exchange and platform maintenance, communications, cybersecurity and enterprise architecture.
- Develop a combination of edge+cloud strategy aligned with business outcomes and data integration risks to govern IT and OT data as IT cloud adoption continues to increase, but real-time processing at the edge remains important.

Sample Vendors

Accenture; AVEVA; Cisco; Eurotech; NTT DATA; PTC; Rockwell Automation

Gartner Recommended Reading

How CIOs Are Approaching IT/OT Alignment and Integration

Emerging Tech: Tech Innovators for Digital Twins — ET/OT Providers

Strategic Roadmap for IT/OT Alignment

2025 Strategic Roadmap for Edge Computing

Quick Answer: What Are IT/OT Alignment and IT/OT Integration?

Alternative Organizational Models for IT/OT Alignment

How CIOs Are Approaching IT/OT Alignment

Bridging IT and OT for the Factory of the Future

How CIOs Are Approaching IT/OT Integration

Why Does a CIO Need to Be Involved in OT?

OT Security

Analysis By: Katell Thielemann

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Operational technology (OT) includes hardware and software that detect or cause a change through the direct monitoring and/or control of industrial equipment, assets, processes, and events. OT security focuses on protecting them. The once-generic OT security market category has been replaced by discrete cyber-physical system (CPS) security markets serving a growing list of use cases.

Why This Is Important

Technology used in production and operational environments started becoming known as operational technology to differentiate from information technology systems two decades ago. Over time, OT assets started connecting to each other and IT systems. This situation created cybersecurity, safety, and operational resilience risks that were largely supported by a network-centric view of security, with a focus on segmentation and firewalls.

Business Impact

The number of cyber events in OT environments has increased year over year, whether caused by internal errors, nation-states targeting critical infrastructure and intellectual property (e.g., manufacturing for cyberespionage or cyberwarfare), or financially motivated hackers deploying ransomware. The impact of operational disruption can range from mere annoyance to hundreds of millions of dollars in lost revenue, along with reliability, life, and safety impacts.

Drivers

- Due to a rapidly changing threat landscape including the geopolitical environment, asset-centric organizations are increasingly focusing their attention on the security risks they face outside of enterprise IT.
- One of the initial focus areas was network-based security, anchored by the Purdue model, which has underpinned most OT security efforts for the last three decades.
- International standards and regulations, such as IEC 62443, NIS2, and the NIST 800-82 series, are emerging to provide guidance. In some industry verticals, security mandates such as NERC CIP or TSA directives are already in place. Given the close relationship between critical infrastructure and national security, and the growing concerns of targeted attacks, government-led efforts are on the rise, adding to the growing list of existing national legislations.
- Digital transformation initiatives are multiplying in asset-intensive organizations, creating new generations of systems that go beyond traditional OT/ICS/SCADA systems. These Internet of Things (IoT), industrial IoT, Industrie 4.0, building management systems (BMS), engineering technology (ET), polyfunctional robots, and now edge computing devices are creating an “Old Tech” connotation for OT. This connotation is creating challenges for cybersecurity teams struggling to attract skilled security resources.

- One thing all of the systems mentioned above have in common is that they are cyber-physical systems (CPS) — they might be managed digitally, but they interact with the physical world. The approach to securing them has also evolved from an amorphous OT security market to distinct categories such as:
  - CPS protection platforms
  - CPS secure remote access
  - CPS backup and recovery
  - CPS security training/ranges
  - CPS risk management
  - CPS network cloaking and segmentation
  - CPS security services
  - CPS removable media security
  - CPS unidirectional gateways
  - CPS threat intelligence
  - CPS wireless security

Obstacles

- Heterogeneous industrial protocols and custom logic programmed to support production create complexities for cybersecurity teams that do not understand production environments.
- Organizations face cultural, governance and security controls challenges that prevent a one-size-fits-all approach to cybersecurity in production environments, which often run 24/7 and cannot be stopped at will.
- Assets that can last over 30 years lack security updates as manufacturers focus on deploying more robotics and next-generation automation systems.
- OT security is evolving into CPS security, enabled by solutions that support not only OT but also IoT, industrial IoT, robotics or smart building assets. This is changing OT security from focusing on segmentation, firewalls and data diodes to placing the assets at the center of security and layering defense-in-depth approaches around them. As a result, OT security becomes CPS security and is supported by distinct market categories supporting a growing list of use cases.

User Recommendations

- Establish appropriate governance and ownership for the security of OT assets.
- Initiate risk discussions between cybersecurity and production/engineering teams and determine the current extent of OT security efforts.
- Deploy CPS protection platforms to conduct asset discovery, inventory, and network mapping, and evaluate what other security use cases are critical, such as CPS secure remote access.
- Determine immediate gaps, such as flat networks and missing or misconfigured firewalls.
- Accelerate security awareness and skills training.
- Focus on organizational and cultural trust challenges between IT and OT personnel.
- Prepare for the new reality of CPS security as a centralizing discipline across old and new production and mission-critical asset types, supported by new categories of security tools.

Gartner Recommended Reading

Magic Quadrant for CPS Protection Platforms

Critical Capabilities for CPS Protection Platforms

Market Guide for CPS Secure Remote Access

IIoT Gateways

Analysis By: Tim Zimmerman, Mike Leibovitz

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

An industrial Internet of Things (IIoT) gateway is an architectural tool that bridges a field network or IoT platform to the IT network. IIoT gateways provide translation capabilities as well as data aggregation or preprocessing points for field devices or wireless networks. They provide local storage and compute capabilities, as well as user interfaces for data processing and system management.

Why This Is Important

IIoT gateways provide protocol transmission, translation and optimization, as well as data normalization, which is critical for brownfield projects and IT/OT convergence. These gateways enable efficient transmission of industrial data from endpoints, or translation to standard protocols, which significantly reduces bandwidth costs by normalizing and filtering most data at the edge.

Business Impact

IIoT gateways are a critical component of any IIoT project that aggregate, translate, filter and forward data that can provide faster integration, near-real-time insights and improved visibility. Manufacturing, automotive and utility sectors are increasingly deploying IIoT gateways as part of initiatives to migrate OT architectures into IT, since they help translate industrial protocols to enterprise IP. IIoT gateways also play a critical role in building management and smart city initiatives.

Drivers

- The growth of IoT devices and data production at the edge requires gateways for connectivity and data processing — especially where low latency is a requirement.
- The various data formats and connectivity methods require normalization and protocol translation and conversion.
- While more general-purpose edge servers will take on deeper analysis and inference roles, the larger demand for light data processing and local aggregation of IoT interactions is best handled by gateways.

Obstacles

- Most industrial gateway vendors offer in-house-developed gateway management applications, with limited integration to Tier 1 IoT platforms, thus complicating deployment, change management and scalability.
- A myriad of edge network protocols and rapidly evolving cellular network technology warrants a modular gateway architecture. However, most IIoT gateways do not offer this, demanding frequent reinvestment and system redesign.
- Gateways in industrial settings are deployed in physically challenging and mission-critical environments and need to meet stringent safety and security requirements.
- Users face challenges when technically integrating with existing programmable logic controllers and other legacy equipment, as well as organizational, cultural and process challenges working across the traditional IT/OT/ET divide.

User Recommendations

- Create a roadmap for the current and future role of gateways in the IoT architecture and invest in a combination of low-end IIoT gateways and intelligent IoT gateways to address various use cases.
- Standardize on gateways that can be managed and programmed by preferred IoT platforms and can provide software development kits for custom integration and management.
- Extend the usable life of IIoT gateways and reduce the need for new investments by choosing gateways that are modular and can accommodate new peripherals.
- Select IIoT gateways that are certified for international, as well as country- and industry-specific safety standards, and provide an adequate level of overall system security.

Sample Vendors

Advantech; Aspen Technology; Cisco; ClearBlade; Dell Technologies; Eurotech; Hewlett Packard Enterprise; Lantronix

Gartner Recommended Reading

Magic Quadrant for Global Industrial IoT Platforms

2026 Strategic Roadmap for Edge Networking

Time-Sensitive Networking

Analysis By: Tim Zimmerman

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Time-sensitive networking (TSN) is a set of networking standards that guarantees data delivery times. Working across both wired and wireless connections, TSN supports critical, real-time data — like data used in industrial control systems — with extreme reliability and consistent delivery. Crucially, this reliable, time-sensitive traffic can run on the same network alongside normal internet traffic.

Why This Is Important

Historically, wireless network traffic (Wi-Fi) was sent as "best effort," meaning there was no guarantee that data would arrive on time. Even modern standards like Wi-Fi 6 could still see delays because any data, regardless of importance, could be put on hold by a technical delay mechanism. TSN solves this by taking the time-guaranteed delivery already available on wired networks and extending it to wireless networks.

Business Impact

Companies can now use Wi-Fi for business-critical services, such as time-sensitive manufacturing controls, without the risk of material loss or employee injury caused by network delays (latency). This guaranteed timing also benefits professional audio applications by preventing inconsistent delays, or "jitter." Furthermore, TSN creates a single, open standard, which eliminates the need for unique, proprietary vendor protocols that often lead to vendor lock-in.

Drivers

- **Need for reliable performance:** Many business and industrial applications require extremely reliable, low-latency performance.
- **Convergence of IT and OT networks:** As OT converges with IT technologies, latency requirements must be addressed with technologies such as Wi-Fi.
- **Cost reduction and open standards:** Deploying equipment based on open standards eliminates proprietary or functionally limited solutions, reduces costs for new network installations ("greenfield" projects), and helps reduce maintenance costs and vendor lock-in throughout the enterprise.

Obstacles

- **New requirements:** All network devices (both endpoints and network components) must be registered to use the service.
- **Infrastructure overhaul:** Implementing new, standards-based TSN solutions often requires replacing existing proprietary solutions used to solve the same problem.
- **Interoperability:** Multivendor implementations must be tested to assure interoperability.

User Recommendations

- Identify usage scenarios — such as in precision manufacturing — that require predictable, low-latency, and highly reliable data delivery to achieve specific business outcomes with TSN.
- Verify vendor integration of TSN, as current availability of these services is limited.
- Confirm that TSN functionality will be available during your next infrastructure refresh cycle.

Gartner Recommended Reading

Magic Quadrant for Enterprise Wired and Wireless LAN

Critical Capabilities for Enterprise Wired and Wireless LAN

Innovation Insight: Wi-Fi 7 (802.11be) Helps Address Specific Connectivity Use Cases

Entering the Plateau

Wi-Fi 7 (802.11be)

Analysis By: Tim Zimmerman, Christian Canales, Mike Leibovitz

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Wi-Fi 7 (IEEE 802.11be) is the latest wireless LAN (WLAN) standard, designed to improve throughput, latency and spectrum efficiency compared with previous generations. The standard expands channel bandwidth, increases the number of spatial streams, and improves operation across 5 GHz and 6 GHz spectrum. Wi-Fi 7 also introduces mechanisms intended to support more deterministic and lower-latency traffic, although adoption and practical value vary by deployment and endpoint maturity.

Why This Is Important

New high-performance applications, such as AR/VR and high-resolution video, are increasing performance and latency expectations for enterprise WLANs. Wi-Fi 7 leverages expanded spectrum availability in many geographies and introduces enhancements intended to improve capacity and latency characteristics. While peak performance claims are largely theoretical today, the standard establishes a foundation for future enterprise and industrial wireless use cases as ecosystems mature.

Business Impact

For most enterprises, the immediate business impact of Wi-Fi 7 is incremental rather than transformational. Organizations are primarily adopting Wi-Fi 7 as part of normal campus WLAN refresh cycles, driven by vendor roadmaps, hardware availability and access to 6 GHz spectrum. While advanced low-latency and high-throughput use cases remain niche, Wi-Fi 7 provides improved capacity, spectrum efficiency and long-term platform viability for environments with growing device density.

Drivers

- **Refresh-driven adoption:** Wi-Fi 7 is increasingly selected during routine campus WLAN refresh cycles as vendors prioritize new designs around the latest standard and reduce focus on earlier generations.

- **Ecosystem availability:** Broad availability of Wi-Fi 7 access points and supporting infrastructure, along with expanding 6 GHz regulatory adoption, is accelerating uptake regardless of immediate performance need.
- **Incremental capacity and efficiency gains:** Improvements in spectrum usage and channel flexibility offer benefits in high-density environments, even if peak throughput advantages are rarely realized in practice.
- **Future-proofing infrastructure:** Organizations favor Wi-Fi 7 to extend platform lifespan and avoid deploying infrastructure that may age quickly as endpoint and application requirements evolve.

Obstacles

- **Surplus performance for many enterprises:** Wi-Fi 7 will typically provide speed up to 46 Gbps in a single coverage area, which is more than three times greater than 802.11ax.
- **Marginal near-term value for most enterprises:** While Wi-Fi 7 offers significant theoretical performance gains, most enterprise use cases do not yet require these capabilities or have 6 GHz devices, limiting immediate business justification beyond refresh alignment.
- **Upstream infrastructure requirements:** Realizing the benefits of Wi-Fi 7 may require upgrades to campus switching (multigig Ethernet and higher PoE), increasing overall project cost and complexity.
- **Endpoint and ecosystem maturity:** Although Wi-Fi 7 access points are broadly available, many client devices do not yet fully support the standard, delaying realization of benefits in typical enterprise environments.

User Recommendations

- Adopt Wi-Fi 7 primarily as part of planned campus WLAN refresh cycles rather than as a standalone upgrade driven by performance requirements.
- Plan for associated wired infrastructure upgrades, including multigig Ethernet and higher PoE, and align WLAN refreshes with access-layer switching updates to manage cost and disruption.
- Test Wi-Fi 7 in a pilot project to evaluate performance improvements, while considering the support of 6GHz in your environment’s end-user devices before deciding to scale it out enterprisewide.

- Be prepared to update LAN switching to address higher Power over Ethernet (PoE) requirements for access points and accommodate the higher-performance wireless connectivity. Use campus WLAN refreshes as an opportunity to also upgrade access switches.

Sample Vendors

Arista Networks; Cisco; Extreme Networks; Fortinet; Hewlett Packard Enterprise; Huawei

Gartner Recommended Reading

Magic Quadrant for Enterprise Wired and Wireless LAN

Critical Capabilities for Enterprise Wired and Wireless LAN

Define End-User Experience When Deploying Campus Networks or Fail

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

Appendixes

See the previous Hype Cycle: Hype Cycle for Private Mobile Network 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 (June 2026)

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 (June 2026)

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 (June 2026)

Acronym Key and Glossary Terms

5G	fifth generation
AI	artificial intelligence
API	application programming interface
CIO	chief information officer
CSP	communications service provider
eSIM	embedded subscriber identity module
ET	engineering technology
IoT	Internet of Things
LTE	Long Term Evolution
ML	machine learning
NaaS	network as a service
NR-RedCap	New Radio Reduced Capability
OT	operational technology
PMN	private mobile network
vRAN	virtualized radio access network
Wi-Fi	Wireless Fidelity
XDR	extended detection and response

Document Revision History

Hype Cycle for Private Mobile Network Services, 2025 - 17 July 2025

Hype Cycle for Private Mobile Network Services, 2024 - 22 July 2024

Recommended by the Authors

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

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner’s Hype Cycle Builder

How to Craft Comprehensive Private Mobile Network Offerings for Enterprises

Target 4 Key Buyer Roles to Accelerate Private 5G Success in Industrial Manufacturing

Magic Quadrant for 4G and 5G Private Mobile Network Services

Critical Capabilities for 4G and 5G Private Mobile Network Services

---

Table 1: Priority Matrix for Private Networks for Industry, 2026

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	*2 to 5 Years* ↓	*5 to 10 Years* ↓	*More Than 10 Years* ↓
Transformational		CSP Open APIs eSIM Generative AI in Manufacturing Operations Multimodal AI Multimodal Generative AI	Industry Edge Integrated Solutions Physical AI	
High	Edge AI Network Security Microsegmentation	5G Core 5G Private Mobile Networks CPS Wireless Airspace Defense Exposure Assessment Platforms IT/OT Integration Network Slicing Private LTE	CPS Network Cloaking and Segmentation CPS Wireless Embedded Security ISAC Neutral Host Network for 5G Time-Sensitive Networking	
Moderate	IIoT Gateways OT Security Wi-Fi 7 (802.11be) ZTNA	5G Network Security LEO Satellite IoT	NR-RedCap	

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 to 5 Years* ↓	*5 to 10 Years* ↓	*More Than 10 Years* ↓
Low				

Source: Gartner (June 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.

Phase	Definition

Source: Gartner (June 2026)

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 (June 2026)

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 (June 2026)