IoT Now: ISSN 2397-2793

2026 • VOLUME 16 • ISSUE 2

IOTNOW

CONNECTX FOR THE ENTERPRISE

COVER INTERVIEW

Simetric and Thales detail strategic partnership for eSIM simplicity and SPoG orchestration

IoT SECURITY
Why enterprises need IoT security-as-a-service. Read the IoT Now Report at www.iot-now.com

TRANSPORT
Expanded use cases and new connectivity needs. Read the IoT Now Report at www.iot-now.com

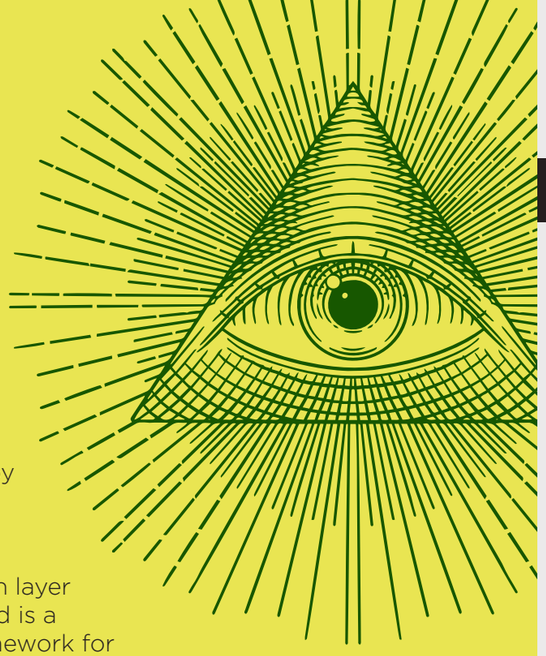
UTILITIES
Learn how to deliver smart metering for a changing world Read the IoT Now Report at www.iot-now.com

CONNECTIVITY
How eSIM is shifting the battleground from connectivity to orchestration

IoT GLOBAL NETWORK
Log on at www.iotglobalnetwork.com to discover our portal for products, services and insight

PLUS: **PELION CEO INTRODUCES THE ERA OF IOT CONNECTIVITY ADAPTABILITY** • Why IoT is embracing the need for an all-seeing eye • Is commercialised SGP.32 making connectivity for IoT easier? • Aeris and Verizon Business simplify IoT expansion with unified connectivity and orchestration • Globalstar explains satellite's expansion from coverage to capability • floLIVE and KORE detail Kigen collaborations • How Thales and Simetric are enabling a unified approach to scalable IoT connectivity • Why not all single panes of glass are created equal • Will IoT maximise the benefits of SGP.32? • Transforma Insights on the six 'S's of IoT connectivity • Does SGP.32 rewrite the rules of IoT connectivity ask Kigen and KORE? – News, Features and Interviews online at www.iot-now.com

IN THIS ISSUE



IoT embraces the need for an all-seeing eye

We're on the edge of a new era for IoT where the minutiae of connectivity are being addressed by a new breed of increasingly unified systems that bring together connectivity management with enterprise systems. This abstraction layer is actually much more than that and is a foundational element in a new framework for orchestrating IoT devices that encompasses all relevant inputs and actions. The scope here is dizzying and it won't all happen at once, but the complex islands of fragmented functions that make up effective management of an IoT asset are being linked.

George Malim, managing editor

This is completely essential for efficient IoT operations at massive scale. Increased automation demands data that can be integrated across all the platforms and systems of IoT and many business cases – and use cases – simply won't work without this unifying all-seeing eye. Of course, it's not just about being able to see what's going on in a holistic way, it's also about then being able to act on what is visible and that is set to streamline capabilities and truly deliver on optimised IoT.

As Counterpoint Research points out in this issue, this emerging era is transforming approaches to IoT connectivity for good. The firm says value is moving from the SIM and the network towards intelligence that governs how connectivity is deployed and managed. That's not the end goal, though. Companies like Simetric and Thales are targeting enablement of a more closely converged set of capabilities that bring together the systems and foundations of IoT.

Connectivity remains complex but it's getting simpler to provision, manage and refine. For connectivity providers, this is, as Aeris' Marcus Lindblom Törnqvist confirms on p16, a pivotal moment. That doesn't mean they're excluded and their value will be inevitably diminished, it means that they can add value if they embrace eSIM and modernise their platforms. They can be the providers of IoT services that extend far beyond basic connectivity and reap the rewards. However, if they don't engage they risk being cut out of the loop in a marketplace where enterprises won't wait for software-defined, automated and service-led capabilities.

This change has been on the tip of peoples' tongues but the arrival of eSIM for IoT and the SGP.32 specification have proved the catalyst for articulating the new vision for IoT operations. This goes beyond managing connectivity and takes us into complete, single-screen management of IoT assets. That won't happen overnight or in a single leap but systems that integrate with others across the value chain and help to eliminate fragmentation and open up siloes are now on everyone's shopping list.

It's about time.

Enjoy the magazine!

George Malim

MANAGING EDITOR
George Malim
Tel: +44 (0)7930 301 841
g.malim@wkm-global.com

DIGITAL SERVICES DIRECTOR
Nathalie Millar
Tel: +44 (0) 1732 808690
n.millar@wkm-global.com

SALES CONSULTANT
Cherisse Jameson
Tel: +44 (0) 1732 807410
c.jameson@wkm-global.com

DESIGN
Jason Appleby
The Ark Design Agency
Tel: +44 (0) 7801 817 139

PUBLISHED BY
WeKnow Media Ltd. Suite 138,
80 Churchill Square, Kings Hill,
West Malling, Kent ME19 4YU, UK
Tel: +44 (0) 1732 807410

Aeris and Verizon Business simplify global IoT expansion with unified connectivity and orchestration

Aeris has announced an inbound IoT connectivity management relationship with **Verizon Business** to transform how multinational enterprises manage and scale international IoT deployments. The collaboration introduces Aeris IoTA Inbound Services, a solution that integrates the IoTA Connectivity Management Platform directly with the Verizon ThingSpace platform to simplify multi-region operations. The collaboration has already enabled US-based enterprises with outbound connectivity for international IoT deployments using Aeris IoTA, and this extension is set to broaden those capabilities by opening up the US market for global device fleets.

The new collaboration directly addresses the primary challenge for global IoT carriers attempting to localise in the US, the friction caused by fragmented platforms and complex domestic connectivity stacks. By combining Verizon's US network and the ThingSpace platform with the Aeris IoTA platform, enterprises can now manage US and global deployments through a single pane of glass, ensuring consistent commercial terms and unified SIM management.

"Global enterprises require a strategic shift away from the inefficiency of juggling numerous connectivity contracts and disparate platforms," said Mark

Mark Cratsenburg, Aeris

Cratsenburg, the chief commercial officer of the IoT Business unit at Aeris. "Through this integration with Verizon, Aeris is delivering a unified solution that allows our tier one global partners to expand their IoT customer solutions into the US market with speed and simplicity while continuing to enable a seamless experience for Verizon customers deploying devices outside of the US."

Shamik Basu, the vice president of Strategic Connectivity and IoT at Verizon Business, added: "Our collaboration with Aeris allows us to enrich the IoT experience for global customers by providing them access to our top-class connectivity and platforms in the critical US market. As IoT becomes increasingly mobile and global, collaborations like this one provide customers with unprecedented reach and seamlessness without compromising on reliability and value, which is critical for meaningful international expansion."

Telenor IoT expands global connectivity with launch of global APN

Telenor IoT has announced an enhancement to its global connectivity offering with the launch of its new Global APN service to strengthen performance, resilience and regional routing capabilities for customers worldwide. An access point name (APN) is the configuration that allows a device to access mobile data services. The new Global APN service has been introduced to help customers achieve optimal global network access by enabling devices to dynamically connect to Telenor IoT's local points of presence (PoP).

The new Global APN service simplifies global IoT deployments by enabling companies to use a single APN across Europe, Asia-Pacific and the Americas. Devices automatically connect to the geographically closest PoP, ensuring optimised performance without reconfiguration. In addition to the existing local break-out possibilities in partner networks with local access, with multiple regional PoPs also available, customers gain a faster, more resilient data path for regional IoT traffic. They also gain improved performance for latency-sensitive use cases such as payments, real-time analytics and industrial automation.

Telenor IoT also works closely with local operator and peering partners to continuously optimise routing paths, ensuring that device traffic takes the shortest, most efficient route through the network. Combined with the Global APN, this regional access footprint provides a powerful foundation for enterprises whose IoT solutions require lower latency, strong resilience and global scalability.

News in Brief

Wiliot partners with Databricks to power physical AI

Wiliot has announced a partnership with **Databricks** to run Wiliot's Physical AI platform and supply chain automation solutions on the Databricks platform. As a Databricks Built-On partner, the collaboration enables enterprises to ingest, manage and analyse volumes of real-time data generated by Wiliot's IoT Pixels, transforming everyday products and assets into intelligent, connected data sources.

Wiliot's Physical AI technology – built around battery-free, postage stamp-sized IoT Pixels – creates a continuous stream of granular, item-level data across supply chains and retail environments. By integrating the Wiliot Physical AI platform with Databricks' scalable lakehouse architecture, Wiliot customers can unify physical-world data and enterprise data sources with new levels of speed and precision. From there, they can apply Wiliot's advanced AI analytics tools to unlock new operational insights.

PTC completes divestiture of Kepware and ThingWorx

PTC has completed the previously announced sale of the company's Kepware industrial connectivity and ThingWorx Internet of Things (IoT) businesses to **TPG**, a global alternative asset management firm. PTC received cash proceeds of US$523 million upon closing and net after-tax transaction proceeds will be approximately US$375 million. PTC will use the proceeds for share repurchases.

"We are pleased to complete the divestiture of our Kepware and ThingWorx businesses as we increase our focus on our intelligent product lifecycle vision," said Neil Barua, the president and CEO of PTC. "We want to thank the teams moving over for their years of service, and we wish them well moving forward."

floLIVE and KORE collaborate with Kigen on SGP.32 connectivity

floLIVE has announced that it has launched operational support for GSMA SGP.32 across its global IoT infrastructure through its relationship with **Kigen**. As a result, floLIVE can support customer requirements that range from full SGP.32 compliant operations to a broad range of hybrid deployment models that combine elements of SGP.32 with proven multi-IMSI connectivity using eSIM and other SIM formats.

"Delivering immediate access to SGP.32 capabilities, as well as hybrid connectivity, allows us to support a broad range of deployment demands from enterprises, IoT service providers and mobile network operators," said Nadav Doron, the vice president of product management at floLIVE. "These models allow businesses to take advantage of critical operational benefits such as remote zero-profile provisioning that places connectivity decisions in the hands of the enterprise. Our partnership and deep technology integration with Kigen provides us with a strong framework for delivering secured connectivity options that can be customised to satisfy the specific needs of customers around the world." Through this collaboration, floLIVE uses Kigen's SGP.32-compliant eSIM IoT remote manager (eIM) and secure eSIM OS to deliver a seamless 'factory-to-field' experience. By integrating Kigen's in-factory profile provisioning (IFPP) capabilities, floLIVE can now ship embedded universal integrated circuit cards (eUICCs) that are pre-configured at the factory with an initial connectivity profile based on the floLIVE multi-IMSI SIM. This allows devices to connect immediately upon activation, anywhere in the world, and download local profiles via SGP.32 standards without complex setup – effectively realising the promise of a single global SKU for massive IoT deployments.

"SGP.32 provides the missing operations layer for connectivity state, so market expansions and fleet transitions can be delivered at scale with confidence," said Jean-Louis Carrara, the global head of sales at Kigen. "Combined with Kigen's In-Factory Profile Provisioning within floLIVE's connectivity offering, this makes first-connect behaviour deterministic and removes the most error-prone moments – so enterprises can go live faster with operational readiness built in."

KORE has separately announced a new portfolio of SGP.32-compliant connectivity solutions in partnership with Kigen, with commercial availability planned for later in 2026. Purpose-built for IoT and based on the GSMA's next-generation eSIM standard, KORE's SGP.32 solutions support a wide range of devices, from high-power gateways to battery-powered sensors, and include a range of connectivity profiles tailored to different operational needs. These include streamlined roaming, resilient multi-network approaches and local connectivity with intelligent failover and recovery – enabling organisations to deploy and manage connected devices globally, while adapting connectivity over time.

"Enterprise customers don't just need standards – they need a proven way to operationalise them at scale," said Ron Totton, the president and CEO of KORE. "With SGP.32, success depends on deep carrier relationships, global infrastructure and the ability to manage complexity across the full device lifecycle. That's where KORE delivers – helping customers turn new standards into real-world, scalable deployments."

Kigen is contributing its secure, GSMA-certified SGP.32 eSIM and eIM technology to the solution to underpin its enterprise-grade architecture.

News in Brief

Simetric partners with Thales to orchestrate eSIM

Simetric has announced a partnership with **Thales** to deliver a next-generation, best-of-breed eSIM orchestration for OEMs and enterprises operating large scale IoT and edge efforts, providing global execution continuity. Led by Simetric's single-pane-of-glass (SPoG) network orchestration platform, the joint solution integrates Thales' GSMA-certified eSIM provisioning, Advanced eSIM Orchestration (eSO) and trusted security capabilities. Together, the companies deliver an end-to-end solution that simplifies eSIM adoption while providing enterprises with centralised visibility, policy control and enterprise-grade security.

"eSIM is no longer just a provisioning function – it has become the operational and security control plane for the network edge," said Allen Boone, the chief executive of Simetric. "By integrating Thales' trusted eSIM and remote SIM provisioning (RSP) foundation directly into Simetric's single-pane-of-glass orchestration platform, we are giving OEMs and enterprises the ability to manage connectivity, security and policy."

G+D and AWS collaborate on new cloud-based remote eSIM provisioning

Giesecke+Devrient (G+D), a provider of eSIM technology, has launched a new cloud-based eSIM solution powered by **Amazon Web Services** (AWS). This new collaboration combines digital security from G+D with cloud agility and scale from AWS, enabling customers to deploy and manage devices with eSIM connectivity worldwide.

Under the collaboration, G+D will transition eSIM workloads to the AWS cloud environment. This newly launched solution combines G+D's focus on GSMA compliance and foundational security with AWS' secure, high availability cloud infrastructure to deliver global provisioning and low-latency connectivity solutions across multiple geographies.

"As the pioneers in SIM and eSIM, and the undisputed leader in security for more than 170 years, we are delighted to be achieving another industry first today through our collaboration with AWS," added Philipp Schulte, the chief executive of G+D Mobile Security. "By bringing eSIM to the cloud and increasing agility and scalability, we will accelerate eSIM adoption in both consumer and IoT applications, providing a secure, future-proof and cost-effective solution for our customers. Together with AWS's innovative solutions, customers benefit from an unparalleled offering that adapts quickly to their evolving requirements."

Philipp Schulte, Giesecke+Devrient

Gordon Mansfield, the vice president of global technology planning at **AT&T**, commented, "We have been successfully using G+D eSIM services for more than a decade. eSIM has passed the tipping point to become the primary means of connecting to our network. The means to distribute services across multiple GSMA certified cloud locations represents a significant opportunity for us to expand our offering globally across a broad range of verticals. The fact that we will also be able to source now G+D's technology directly from the AWS marketplace means a breakthrough in terms of time to market on a global scale."

Semtech LoRa Plus platform enables multi-protocol smart home and security development

Semtech has announced an agreement with **Trident IoT** that positions Semtech's LoRa Plus platform as the connectivity foundation for next-generation multi-protocol smart home and security solutions. With this agreement, customers who purchase Semtech's LoRa Plus transceivers will have royalty-free access to Trident IoT's software development kit (SDK) and development tools, positioning Semtech as a one-stop provider for Z-Wave connectivity, with development plans to support Zigbee and Thread/Matter.

The collaboration addresses the growing complexity developers face in supporting multiple smart home connectivity standards by integrating Trident IoT's award-winning ELCap development platform and SDK with Semtech's LoRa Plus family, including the LR2021 multi-PHY transceiver. This turnkey approach eliminates traditional development fragmentation, accelerating time-to-market for manufacturers of smart home, security and IoT devices.

"This definitive agreement establishes Semtech as a performance leader and comprehensive solution provider for multi-protocol IoT connectivity," said Madhu Rayabhari, the senior vice president and general manager of Semtech's analogue, mixed-signal and wireless products group. "By integrating Trident IoT's production-ready development tools with our multi-award-winning 4th generation transceiver, LR2021, we're becoming one of the industry's most complete solutions for smart home and security applications. Our customers benefit from a single-source platform that combines proven silicon with robust software tools, significantly reducing their development complexity and accelerating their path to market."

Madhu Rayabhari, Semtech

The agreement builds on Semtech's established position in low-power connectivity, extending the company's LoRa Plus platform strategy to address complementary smart home protocols alongside its existing LoRaWAN and **Amazon** Sidewalk offerings.

"This partnership represents an evolution in our collaboration with Semtech," said Mariusz Malkowski, the chief technology officer of Trident IoT. "By combining our ELCap platform and SDK with Semtech's LoRa Plus transceivers, we're removing the barriers that have traditionally complicated multi-protocol IoT development. The integration delivers a truly turnkey solution that enables our mutual customers to focus on product innovation rather than connectivity implementation."

GCT Semiconductor partners with Skylo to accelerate global satellite connectivity

GCT Semiconductor Holding, a designer and supplier of advanced 5G and 4G semiconductor solutions, and **Skylo Technologies**, a global non-terrestrial network (NTN) provider spanning 36 countries across 70 million square kilometres of coverage, have announced a partnership to advance next-generation satellite connectivity. As part of this collaboration, the companies will jointly pursue chip and module certification to enable a new class of multi-use devices. These devices will allow customers to have ubiquitous connectivity by connecting to Skylo's network when terrestrial connectivity is out of reach.

"This partnership marks another significant step in GCT's commitment to powering the rapidly expanding 5G-to-space ecosystem," said John Schlaefer, the CEO of GCT. "We're excited to deepen our collaboration with Skylo and to help accelerate the next generation of global satellite connectivity for customers and device-makers worldwide."

"Our collaboration with GCT is a critical milestone in making global connectivity truly seamless," said Vijay Krishnan, the vice president of strategy partnerships of Skylo. "By integrating GCT's 3GPP-compliant silicon with Skylo's satellite network, we are eliminating the traditional boundaries of cellular coverage. This isn't just a technical proof of concept; it's a demonstration of a ready-to-scale ecosystem that brings reliable, standards-based IoT connectivity to the most remote corners of the globe. We are proving that 'always-on' isn't a luxury – it's the new standard for global industry."

Vijay Krishnan, Skylo

News in Brief

Deutsche Telekom launches multi-orbit IoT roaming

Deutsche Telekom has introduced multi-orbit roaming for IoT with a new offering to ensure that IoT devices can transmit their data worldwide – either via terrestrial mobile networks or via satellite, depending on the situation. Multi-orbit roaming has now been demonstrated using a commercial NB-IoT device that operates across geostationary (GEO) and low earth orbit (LEO) satellites as well as terrestrial networks.

The solution connects Deutsche Telekom's global IoT network, composed of NB-IoT and LTE-M cellular networks, with satellite services from several partners including **Skylo**, DT's first satellite service provider which provides coverage in geostationary orbit, while **Sateliot** and **OQ Technology** handle radio connectivity to LEO satellites.

"This establishes Deutsche Telekom as the leading global network operator offering IoT connectivity across multiple satellite orbits, both technically and commercially," said Jens Olejak, the head of satellite IoT at Deutsche Telekom IoT.

1NCE and Netmore combine cellular and LoRaWAN access

1NCE has opened access for its customers to LoRaWAN services provided by **Netmore**, a low power wide area network operator for massive IoT. With growing demand for low power long range connectivity, the Netmore LoRaWAN Network Server (LNS) Plugin provides 1NCE customers with access to cellular and LoRaWAN IoT coverage options through one platform.

The launch of the Netmore Plugin marks the beginning of a collaboration to expand the combined offering of 1NCE and Netmore. Working together to support their respective customer bases with both cellular and LoRaWAN technology delivers a powerful layer of redundancy to cover the hardest to reach spots with reliable connectivity and IoT services. Through a unified visibility, ingestion and routing software tool, it's now possible to seamlessly manage both technologies in one place.

Converged orchestration via a single-pane-of-glass makes eSIM simplicity a mass-scale reality for enterprises

Uptake of embedded SIM (eSIM) in IoT has been significantly simplified and is set to accelerate thanks to the introduction of the 'made-for-IoT' SGP.32 eSIM specification from GSMA. SGP.32 brings a highly scalable framework for efficient management of eSIM profiles but the fragmented ecosystem of mobile network operators, connectivity management platforms and enterprise systems is still complex and inefficient. The ultimate goal of frictionless automation of cellular IoT connectivity depends on global execution continuity and demands simple network orchestration alongside eSIM provisioning and orchestration, as well as trusted security capabilities.

To close the loop on SGP.32's potential and ease the adoption and execution for IoT operations, Thales and Simetric announced a new partnership in the run up to MWC26 Barcelona.

This is not a typical marketing wrap and is instead something based on real deployments, bringing together Simetric's single-pane-of-glass (SPoG) network orchestration platform and Thales' GSMA-certified eSIM provisioning, Advanced eSIM Orchestration (eSO) and security expertise. The two companies have a shared drive to combine their capabilities and pursue a truly strategic partnership in which success is delivered, not sold. To achieve this, the partners have created an end-to-end, unified process that simplifies eSIM adoption while simultaneously supporting centralised visibility, policy control and enterprise grade security across multi-carrier, multi-region IoT deployments.

To understand how this approach is transformative in enterprises' journeys to fully automated cellular IoT connectivity, George Malim, the managing editor of IoT Now, interviewed Jean-Francois Gros, the head of IoT Services Product Lines at Thales Digital Identity and Security, and Allen Boone, the chief executive officer of Simetric ▶

Allen Boone
Simetric

Jean-Francois Gros
Thales

George Malim: How do you see the need for unified and centralised visibility into entire device fleets crystallising? What do enterprises and other IoT device fleet operators really want?

Allen Boone: IoT has long operated without a control plane to afford users with a source of truth. If connectivity dependencies are fragmented, data and device level security certainly are fragmented and vulnerable. Fragmentation drives unnecessary complexity and prevents scalability. With this partnership, we are bringing everything into one framework regardless of where it sits in the SIM management framework.

If you consider a global logistics operator with 500,000 assets, a percentage of those will go dark during provisioning and a further percentage will experience roaming failure but no one will know until the truck stops reporting and the customer calls in to complain. With a unified control plane, you can visualise different profiles and see what's happening on an asset level.

From an operating budget standpoint this enables a shift from reactive SIM management to proactive eSIM-based connectivity management. Proactive connectivity management at the device level with tailored performance rules reduces costs and field service expenses such as truck rolls for addressing stranded profiles, as just one example.

The control plane becomes the single place where decisions are made and policies are enforced.

Jean-Francois Gros: From our perspective, we started with a pre-standard vision – aligned with SGP.31/SGP.32 – for achieving simplicity for end users like OEMs and ODMs as well as service providers. What they really need is simplicity and having a single pane of glass is essential for that. Our initial customers were mobile operators but we had the big ambition to address enterprises because our solution could address their needs. Our SGP.32 standardised server was good for mobile network operators and, while mobile operators know a lot about SIMs and eSIMs and connectivity management platforms (CMPs), talking to enterprise systems is very, very difficult for them – there was no expertise and no orchestration.

For us to make the vision happen, we needed an events orchestrator that was eSIM-centric and enabled everything to be automated, which we developed. When we realised that moving from SIM to eSIM would see enterprises move from single to multi mobile operator relationships, we needed another layer to orchestrate with the MNOs and the enterprise system. This is where Simetric comes in, with APIs to MNOs and to all enterprise systems. ▶

IoT has long operated without a control plane to afford users with a source of truth

We have the shared conviction that this new eSIM era demands a fundamentally different operating model

Think of it as Thales bringing our certified eSIM Management solutions including our eSIM orchestrator and Simetric providing APIs through enterprise systems and into the mobile operators, as well as its SPoG capabilities. The combination of both companies' strengths creates a fully-automated solution that gives the customer financial benefits as a result of full visibility, simpler operations and better capabilities. This is just the first step to achieving simplified IoT connectivity at massive scale, we have a programme in place called 'Better Together' that aims at bringing further innovations and capabilities in the future.

GM: Can you outline the value of bringing the entire device fleet into one control plane and its implications for eSIM adoption?

AB: We have the shared conviction that this new eSIM era demands a fundamentally different operating model. The really important thing is not just technical alignment but philosophical alignment around how we get into market and help the enterprises scale. What's happened with the SGP.32 specification is there has been a disaggregation of the technology stack which has created enormous flexibility and that allows enterprises to think about this in a different way.

That disaggregation does create complexity so what we're doing is creating a platform to simplify adoption and mitigate operational risks for customers.

J-FG: The landscape has changed and it's now device makers and service providers who are mandating or purchasing eSIMs. What we provide is a solution to deliver them the full control and ownership of the usage of their devices for various needs. This isn't about providing a black box that manages connections for them, instead they have full control and that's important because some markets are focused on cost or regulatory compliance, others on resilience or security which means enterprises need to be able to control device connections accordingly.

We want to give them all the management and automation capabilities so they can achieve their goals in a scalable manner. For instance, an electricity meter being able to connect is mission critical because its data is essential for balancing the grid therefore ensuring uninterrupted connectivity is essential. Functions such as track-and-trace or permanent roaming can be fully automated with our platform, addressing the business priorities of our customers in real-time.

GM: Why have you chosen to work with each other here? What strengths does each company bring to the partnership?

J-FG: This isn't just another technology partnership in which 2+2=4, this is an alignment on strategy that combines Simetric's APIs to CMPs and enterprise systems with our portfolio of eSIM orchestration and management solutions.

AB: At Simetric, we do not take the word partnership lightly. Satisfying customer successes requires leading technologies from both sides, but it also requires a strong commitment to invest in unifying technical innovations to achieve a far greater outcome for customers and an investment in all go-to-market motions. Thales brought all that to the table to collaborate. It was customer and market first from the outset. Lastly, we shared a deeply common customer success criteria – device level security.

GM: What verticals are you targeting and what needs are you seeing in the market that amplify the need for this partnership?

JF-G: We have customers in segments including track-and-trace, metering, mPoS, security and automotive and some are moving fast to adopt eSIMs because they recognise the benefits and the increased operational flexibility. This will increase the diversity of connectivity providers they will use to support their business. All are fully committed to rolling out eSIM-enabled devices but the go-to-market cycle can be long because their structure, policies and regulations are different. Automotive customers are all-in but it takes few ▶

years before a product comes onto the market. This is why we have designed a solution they are able to seamlessly integrate into their devices and that works out of the box.

AB: Simetric, like Thales, has deep existing relationships in every industry. We see the largest eSIM migrations, referencing installed devices moving to be eSIM-enabled, in major industries like utilities, oil and gas, fleet and logistics, manufacturing, such as in HVAC, and security devices. Demand is growing across every industry, but critical infrastructure and device-led industries want adoption with controlled migration.

GM: How does this new approach the two companies are putting forward differ from traditional connectivity management platforms?

AB: I think the current CMPs from an enterprise point of view are more focused on the MNO connectivity problem set rather than the enterprise set of problems. We do not displace CMPs but enrich essential functionality that enterprise and public sector users require. Regarding eSIM, legacy CMPs were not made to support their adoption. Additionally, the word 'orchestration' is thrown around too loosely and risks confusing users.

Thales and Simetric are focused on eliminating that buyer side confusion. Orchestration requires CMP. RSP, device level data and, routinely, internal data sources from a customer to truly execute the right device level protocols. Our collaboration satisfies all that in a seamless workflow.

J-FG: Imagine a system that is connected to CMPs and to external systems such as device management but also ticketing, ERP and others. A system that is connected to all eSIMs and all devices. It is a very centralised system from which you can get a lot of context and orchestrate activities from all directions. We provide the ability to fully automate and integrate with customer systems – traditional CMPs don't do that.

GM: What should we expect next from the Thales and Simetric partnership?

J-FG: As we target enterprises, we see a need to go further than only managing connectivity. We see a need to provide the capability to offer a view of all the devices and elements and also to manage the full lifecycle of the devices from connectivity to security to onboarding of devices. Enterprises now have connectivity, security and device management platforms and what we want to build is a SPoG that will show them all the key elements they need to operate and make decisions.

AB: We see this partnership as a platform to accelerate eSIM adoption across the industry and we are showing the way forward. When the market gets to a place with the transition to eSIM is low risk and easily orchestrated in a secure manner, it stops being an aspirational roadmap and becomes an operational reality. Thales and Simetric are making that operational reality a true reality at global scale. ■

Simetric, like Thales, has deep existing relationships in every industry

www.simetric.com
www.thalesgroup.com

Thales and Simetric – A unified approach to scalable IoT connectivity

A global IoT service provider operating large-scale device fleets for the utilities sector was looking to scale its connectivity operations while maintaining security, resilience and operational efficiency. With deployments spanning multiple regions and network partners, the IoT service provider needed a unified way to manage connectivity across its growing IoT estate without increasing operational complexity.

While SGP.32 provides the essential baseline for large-scale eSIM, it is a foundation, not the complete solution

As enterprises and IoT service providers scale global device deployments, connectivity becomes a foundational operational dependency. Supporting thousands, if not millions of devices across multiple regions, operators and regulatory environments introduces complexity that traditional models simply cannot resolve. Achieving consistent, secure and uninterrupted data flow across these varying network lifecycles requires absolute excellence in both connectivity and security.

The evolution to eSIM

eSIM technology and the GSMA SGP.32 specification represent a tremendously positive revolution for the global IoT landscape. Historically, organisations were locked into single network providers, which stifled global expansion. However, eSIM provides a new level of flexibility and choice. It enables scalable, remote over-the-air provisioning, allowing enterprises to dynamically select the best connectivity service providers based on region, cost and signal strength without ever needing to physically swap a SIM card.

This flexibility future-proofs IoT fleets, empowering original equipment manufacturers (OEMs) and IoT service providers to innovate faster, enter new geographic markets seamlessly and design products with a truly global footprint from day one. eSIM is the positive catalyst that makes agile, boundless IoT a reality.

While SGP.32 provides the essential baseline for large-scale eSIM, it is a foundation, not the complete solution. True IoT scale requires more than just meeting a standard, it demands operational control, automated orchestration and end-to-end security. Simetric and Thales partnered together to build on top of SGP.32 to turn these standards into scalable business outcomes.

Turn eSIM flexibility into operational simplicity

Embracing the remarkable power of eSIM, this enterprise customer engaged with multiple mobile network operators (MNOs) and mobile virtual network operators (MVNOs) to guarantee localised coverage and optimised connectivity rates around the world.

However, capitalising on this flexibility introduced a practical operational hurdle: managing a complex, multi-operator ecosystem. Without a unified system, the enterprise customer's operational teams found themselves logging into multiple distinct connectivity management platforms (CMPs). Each platform had its own unique interfaces, distinct application programme interfaces (APIs), operational workflows and billing structures. Suddenly, subscription management, troubleshooting and service level agreement (SLA) monitoring became highly fragmented.

Why traditional connectivity models no longer scale

As the deployment expanded across regions and network partners, several operational limitations became clear:

- Reliance on multiple operator portals' fragmented visibility and control and decentralised operational workflows.
- Manual, ticket-based processes slowed response times during network issues. Subscription management, diagnostics and SLAs varied drastically across platforms.
- Scaling operations increased overhead rather than driving efficiency.

At scale, IoT is fundamentally about device control. While dynamic connectivity is critical, true resilience requires commanding device behaviour, executing mass actions across global fleets and maintaining deep, real-time visibility into device health. If you cannot see and command the device alongside the network, proactive troubleshooting fails. Ultimately, you can't scale what you can't control.

Our customer recognised that the flexibility enabled by multi-operator eSIM environments required a centralised and automated orchestration model to remain operationally sustainable at scale.

Thales and Simetric unified architecture for real-time device control

To address these challenges, the customer adopted a unified connectivity orchestration model combining secure remote SIM provision (RSP), advanced orchestration and a single pane of glass (SPoG) approach.

Our vision is simple: connectivity should drive global growth, not create operational hurdles. IoT success relies on an entire ecosystem rather than just a single piece of technology. By taking an ecosystem-first approach, we bridge technology, operations and business workflows across device makers, connectivity providers, platform operators and service providers. From devices to operations, we orchestrate the ecosystem. To realize this, Thales and Simetric have forged a strategic partnership. Together, we move the market away from fragmentation and toward normalised, unified control. At the core of our joint offering are tightly integrated building blocks designed to harmonise the global IoT lifecycle:

- **Thales: The foundation of trust and agility**

Thales brings its recognised global leadership in eSIM, SGP.32-certified remote provisioning and embedded security. We deploy our eSIM IoT Manager (eIM) and eSIM Advanced Subscription Orchestrator (eSO) to provide secure, GSMA-compliant lifecycle management. This is further strengthened by an intelligent eSIM agent that detects events directly from the device and makes its own autonomous local decisions. Together this enables automated profile downloads, network switching, fallback and rollback across multiple operators seamlessly.

- **Simetric: The single pane of glass**

Simetric perfectly complements Thales by delivering advanced orchestration and workflow normalisation across hundreds of IoT connectivity providers worldwide. Through the SPoG, Simetric's platform delivers a unified operational interface that aggregates data and actions across various CMPs, operator APIs and enterprise systems — importantly, without requiring the enterprise to rip-and-replace their existing platforms. Furthermore, because the journey to eSIM is incremental, the platform fully supports legacy SIM alongside eSIM. Customers can migrate at their own pace with no disruption.

How the unified architecture addressed operational challenges

By deploying the combined Thales-Simetric solution, the enterprise customer overcame its operational bottlenecks through the following practical capabilities:

- **Eradicating silos through workflow normalisation:** Instead of navigating half a dozen different operator portals to manage global fleets, operational teams use one single, unified interface. The SPoG successfully abstracts the complexity of the underlying networks, creating a single, normalised source of truth for the entire IoT ecosystem.
- **Automating the IoT lifecycle at scale:** Manual provisioning is eliminated. Automation and AI are built in, not bolted on. Intelligent rules and AI-driven decisions replace manual intervention, allowing enterprises to scale operations efficiently. Simetric's advanced orchestration engine uses comprehensive device context to execute mass actions automatically.
- **Unlocking true real-time control:** The combination of the Simetric platform and the Thales eSIM unlocks true real-time control, a first in the market. Real-time events trigger real-time decisions. If network performance drops, the platform proactively triggers Thales' eSO to download a new profile and switch networks across impacted devices instantly and in bulk mode.
- **Anchoring security at the edge:** Security is not an add-on; it is designed into every layer from device to cloud. Thales natively embeds security-by-design, using its eSIM as a highly secure hardware root of trust. The joint solution enables cryptographic device-to-eSIM binding, secure device-to-cloud communications and rigorous firmware integrity checks. This compliance-ready approach protects not only data but also service continuity and brand reputation.
- **True network convergence:** The Simetric and Thales partnership extends normalised control across both terrestrial cellular and satellite networks. This convergence allows remote devices to transition smoothly between connectivity types in dead zones, maintaining seamless visibility throughout the journey.

Key outcomes

By deploying the combined Thales–Simetric architecture, the organisation achieved:

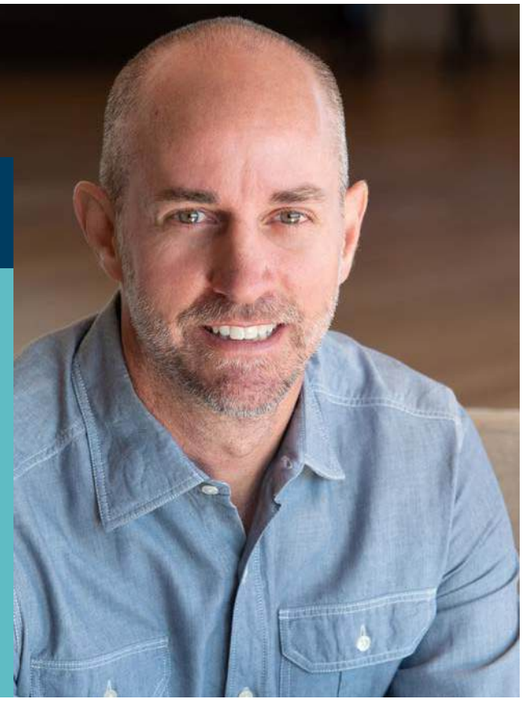
- Centralised visibility and control across multiple operators through a single interface.
- Faster response to connectivity degradation through automated profile switching.
- Reduced operational overhead by eliminating manual provisioning workflows, through eSIM event-based automation.
- Improved consistency of security and compliance across regions and networks.
- Greater resilience for globally distributed IoT deployments.
- Validated adoption workflows.
- Access to combined innovation roadmap of the partnership to better improve the customer operations.

By adopting a unified orchestration approach, the enterprise transformed connectivity from an operational constraint into a scalable foundation for growth. By harmonising Thales' secure, flexible eSIM foundations with Simetric's advanced automation and SPoG workflow normalisation, we deliver unparalleled value to the market.

Together, we empower enterprises to effortlessly embrace the flexibility of multi-operator eSIM environments, simplify global operations, enhance fleet resilience and ultimately unlock the limitless potential of connected IoT. By combining standards like SGP.32 with ecosystem orchestration, real-time control, automation and security, we enable IoT at industrial scale – today and tomorrow. ■

SPONSORED CASE STUDY

Not all single panes of glass are created equal



Coming away from MWC Barcelona, one phrase appeared in every conversation: 'single pane of glass (SPoG)'. Every connectivity provider, legacy connectivity management platform (CMP) provider and device OEM has adopted it as their new positioning anchor. There is a legitimate reason for the narrative shift – enterprises are demanding unified visibility and control over their IoT estates. But CIOs, CISOs and finance executives should be asking a harder question: single pane of glass over what, exactly, writes Kevin Bandy, the president and chief strategy officer of Simetric.

eSIM adoption is having a material impact on the need for a true SPoG

Because in most cases, what is called a SPoG is nothing more than a cellular connectivity dashboard – something far short of an enterprise control plane. The distinction matters enormously: for operational outcomes, security posture and enterprise resilience.

The market has a definition problem

The IoT industry has a long history of vendors selling what they have rather than what enterprises need. Even the largest tech and connectivity players cannot offer an end-to-end IoT architecture, leaving enterprises to heavily customise their own efforts. Classifying everything as SPoG risks compounding that problem further.

Many connectivity management platforms are adding a unified interface and calling it a 'control plane' to sound more IT-centric. But those platforms are optimised to manage the provider's business – subscriber relationships, data consumption, billing – not the enterprise's operational requirements.

Analysts at Transforma Insights are now formally distinguishing between connectivity-centric offerings and the device-centric platforms that can genuinely participate in enterprise workflow management. That distinction is exactly where buying decisions will be won or lost.

The forcing function enterprises can no longer ignore

eSIM adoption is having a material impact on the need for a true SPoG. It has surfaced a competency gap that was always present but easy to defer. Enterprises are discovering that existing tools were built to manage connectivity spend, not device productivity. Connectivity spend is a line item. Device productivity is an operational outcome.

eSIM adoption also migrates operational responsibility for device productivity squarely to the enterprise – not the MNOs and their platforms. And it should be viewed as a device migration strategy: the greater control you have over deployed assets, the greater your insight ▶

into deploying eSIM-enabled devices with tailored performance rules. The question every enterprise must now answer: is their SPoG anchored to the device, or to the rate plan? That architectural choice determines almost everything that follows.

The architectural divide that buyers must recognise

In a connection-centric SPoG, the rate plan or usage is the primary identifier – the device is an attribute of that connection. When a device changes carrier or undergoes an eSIM update, continuity of device history, security posture and operational context can be lost. No unified dashboard resolves that operational limitation.
In a device-centric architecture, the device carries its own persistent identity. Connectivity becomes an attribute of the device – enabling continuous asset visibility, SIM/eSIM orchestration, tailored anomaly detection, infinite estate hierarchy planning and cost attribution by business unit or customer. It also enables platform-to-platform value realisation through genuine integration with enterprise systems like ServiceNow or SAP. Without that foundation, a platform can observe enterprise workflows. It cannot govern them.

Where Simetric sits – and where customers are driving SPoG value realisation

As enterprises take control of their IoT efforts, accountability is rising to the CIO and CISO level – making cybersecurity, revenue assurance and data continuity board-level priorities. With that shift, a category is emerging: Intelligent IoT Operations – a governed, device-centric discipline spanning connectivity, device lifecycle, security and workflow integration.

Simetric was not born of telecommunications. We come from Cisco, Microsoft, Palo Alto, Accenture and beyond – and we built an 'enterprise-first, device-centric platform' to unify the entire IoT ecosystem. Customers own their digital transformations. Our platform is built to serve that ambition in full. The maturity framework, set out in the table opposite, maps the market and shows where Simetric operates today – and where adoption is headed.

Many claiming a SPoG position operate at Stage 2. Simetric enters at Stage 3 and its full platform delivers Stage 4 – Distributed Device Orchestration – the point at which IoT transitions from connectivity management into governed enterprise discipline. Stage 5, Autonomous IoT Intelligence, is the frontier Simetric is actively building with customers and partners including ServiceNow. With Intelligent IoT Operations, customers want to enrich, and close gaps in, existing IT investments like Cisco, ServiceNow and others.

Stage	Label	What It Means	Who Lives Here
1	Siloed Connectivity	Carrier-by-carrier portals, no unified view, manual processes	Legacy telco portals, single-carrier tools
2	Unified Visibility	Single Pane of Glass – a unified dashboard across connectivity positions	M(V)NOs and OEMs with enriched connectivity dashboards on top of CMPs
3	Intelligent Monitoring	Anomaly detection, cost intelligence, usage analytics, federated data lake	Simetric – entry point
4	Distributed Device Orchestration (DDO)	Bi-modal network automation, SIM/eSIM unified orchestration, device BPA, policy control, real-time interrogation, APN execution	Simetric – full platform
5	Autonomous IoT Intelligence	Agentic AI, self-healing network orchestration, predictive optimisation, zero-touch operations	Tailored Simetric DDO + ServiceNow ITSM agentic exposure

The security imperative can no longer be ignored

The threat environment has made IoT device management a security decision. Iran-linked actors are actively targeting internet-facing OT devices in live exploitation campaigns. Across Europe, the EU Cyber Resilience Act adds binding lifecycle obligations extending well beyond the network perimeter. A connectivity-centric SPoG cannot meet either challenge – it lacks the device-layer visibility, persistent identity and policy enforcement every CISO requires.

The security dimensions of device-centric IoT governance – Zero Trust enforcement, CRA compliance posture, anomaly detection at scale – warrant dedicated treatment. We will address them in a follow-on article at ***www.iot-now.com*** ■

In a connection-centric SPoG, the rate plan or usage is the primary identifier – the device is an attribute of that connection

How will IoT maximise the benefits of SGP.32 for eSIM provisioning through unified, automated orchestration?

There's significant potential in the adoption of the SGP.32 specification and simplified eSIM provisioning which are poised to transform how enterprises select and utilise IoT connectivity. The ecosystem is now engaging beyond the specification to reduce fragmentation and unify processes but could many of the advantages be missed if the specification isn't adopted alongside systems and processes that aid automation and improve visibility into connectivity at the asset level, asks George Malim?

Simplified provisioning of connectivity profiles is the goal but an ecosystem around the specification is needed to deliver the benefits

SGP.32 ushers in a made-for-IoT specification that promises to radically simplify the provisioning and management of IoT connectivity. "The latest eSIM SGP.32 standard is a major step forward for the IoT industry because it removes many of the barriers that previously made global eSIM deployments more complex than they needed to be," says Marcus Lindblom Törnqvist, the head of IoT Platform Services at Aeris. "The new standard lowers the barrier to entry for sectors that were historically held back by differing form factors, bespoke integrations and rigid provisioning models. It also enables zero-touch connectivity management at a scale that was previously difficult to achieve."

"But standards alone do not transform markets – execution does," he adds. "To fully realise the benefits of SGP.32, organisations now need the operational capabilities around the specification – including automated provisioning, policy-driven orchestration, remote lifecycle management and real-time visibility across devices, networks and regions. The real opportunity is to make connectivity dynamic. Businesses should be able to localise connectivity by geography, switch profiles remotely, optimise performance and scale globally without friction."

Simplified provisioning of connectivity profiles is the goal but an ecosystem around the specification is needed to deliver the benefits. "SGP.32 IoT eSIM, based on SGP.22 Consumer eSIM, simplifies operator profile provisioning for IoT, but most deployments are still at an early stage, with around 40% of operators having launched or testing services," confirms Yolanda Sanz, the head of technical working groups at GSMA. "The next step is scaling these deployments and embedding the specification into day-to-day operations from the operator and device perspective."

Dynamic connectivity management

"This means integrating SGP.32 into automation, orchestration and lifecycle management across large device fleets," she adds. "As IoT deployments increasingly span multiple networks and geographies, organisations need the ability to manage connectivity dynamically, with resilience and continuity built-in. The real value will come from treating connectivity as an ongoing, managed capability across the lifetime of an asset, rather than a one-off provisioning step."

Others are also looking to move on from the standardisation process and make routine operations a reality. "IoT organisations now need to move SGP.32 out of a pure standards discussion and firmly into day to day operating models," says Philipp Schulte, the chief executive of Gisecke+Devrient (G+D) Mobile Security. "That means evolving existing infrastructure so devices, embedded universal integrated circuit cards (eUICCs) and provisioning platforms can support IP based, remote lifecycle management at scale, while still accommodating legacy SGP.02 deployments during the transition. SGP.32 delivers the most value when combined with in factory profile provisioning (IFPP), allowing devices to leave production already prepared for secure remote management throughout their lifetime, even across large, globally distributed fleets."

"The real payoff comes when SGP.32 is embedded end to end into lifecycle processes – from manufacturing and deployment to operation and retirement – rather than being treated as a standalone connectivity upgrade," he adds. "In practice, this shifts connectivity from a technical component to a security critical foundation for trusted, resilient IoT operations at scale."

Operator opportunities

For Lindblom Törnqvist that changed value will also have significant impacts on mobile network operators. "For the mobile operators, this is also a pivotal moment," he says. "Those that embrace eSIM and modernise their platforms can deepen enterprise relationships and unlock new service revenues. Crucially, it will enable them to offer more specialised services, creating new upsell and cross sell opportunities on their local networks – or via local partners. If they don't move with the times, they could find themselves being cut out of the loop altogether – as enterprises turn to other ▶

Marcus Lindblom Törnqvist
Aeris

Yolanda Sanz
GSMA

Philipp Schulte
Giesecke+Devrient Mobile Security

Romain Durand
Transatel

connectivity partners in a market that is becoming increasingly software-defined, automated and service-led."

Operationalising the specification provides a shared and common foundation for massive IoT. "SGP.32 gives the industry a shared architectural language for the first time, built specifically for IoT realities: screenless devices, constrained networks and long device lifecycles," says Romain Durand, the co-founder and director of innovation at Transatel. "The first certified solutions are now emerging, but broad adoption will depend less on the standard itself and more on how effectively the ecosystem executes around it. Technical readiness is advancing faster than organisational readiness. The standard is here but the next challenge is helping enterprises operationalise it successfully."

There's a substantial bit in the middle between celebrating the specification and the arrival of eSIM in IoT and reaping the rewards and that has been neglected. Has eSIM orchestration attracted enough attention?

"Put simply, no," says Schulte. "The industry has focused heavily on the technical benefits of SGP.32, but much less on the operating model required to manage it effectively at scale. Organisations now need to define how eSIM orchestration works in practice: who governs profile changes, how regional and regulatory policies are applied, and how connectivity decisions are automated and coordinated across suppliers, cloud platforms and internal systems. Without this orchestration layer, a significant part of the efficiency and flexibility that SGP.32 promises risks being left unrealised." ▶

"The real payoff comes when SGP.32 is embedded end to end into lifecycle processes – from manufacturing and deployment to operation and retirement – rather than being treated as a standalone connectivity upgrade

“That level of flexibility is powerful, but it also increases the importance of orchestration”

Insufficient focus

Durand agrees: “Not yet, and this is where the next phase of market maturity will be decided,” he predicts. “The industry has done a good job explaining the architecture: eSIM IoT manager (eIM), IoT profile assistant (IPA), subscriber manager data preparation plus (SM-DP+), and the simplification brought by removing the need for traditional device-side local profile assistant (LPA) models. But there is still insufficient focus on what it takes to operate SGP.32 successfully in real-world deployments. Switching a profile in a controlled demo environment is one thing. Managing hundreds of thousands of devices across multiple countries, with strict uptime requirements, regulatory obligations, automated fallback processes and integration into billing or field operations systems, is something very different.”

“That is where orchestration becomes critical,” he explains. “It is not simply a technical function; it is an operational capability. Enterprises need platforms that can automate decisions, maintain compliance and provide clear governance across the full device lifecycle. As adoption grows, the real differentiator will not just be who supports SGP.32, but who can make it work reliably at scale.”

It’s now time to move beyond necessary foundational steps. “Early efforts have focused on enabling compatible services, which is a necessary first step,” says Sanz. “The bigger challenge is how those services are coordinated at scale. Without effective orchestration, organisations can still face fragmentation across platforms and processes, even with a common specification in place. To unlock the full benefits, SGP.32 needs to be supported by tools that provide visibility and control across connectivity, device status and performance, allowing enterprises to manage their deployments in a consistent and scalable way.”

The orchestration challenge

Lindblom Törnqvist also doesn’t think sufficient attention has been given to how organisations will orchestrate eSIMs in the SGP.32 era. “Much of the industry conversation has understandably focused on the specification itself, but orchestration is where the next challenge and opportunity now sits,” he says. “SGP.32 has introduced a fundamentally new model for IoT connectivity – one that is far more dynamic, localised and service-driven than legacy approaches. Enterprises are no longer simply provisioning a SIM once and leaving it untouched for years. They now can remotely manage devices, localise connectivity, change providers based on geography or use case, and adapt connectivity strategies as operational needs evolve.”

“That level of flexibility is powerful, but it also increases the importance of orchestration,” he explains. “Provisioning an eSIM remotely is only one part of the equation. Too many organisations still equate profile downloads or activation with orchestration. True orchestration means automating actions across thousands of eSIMs based on location, usage, performance or policy, without manual intervention. Organisations also need to maintain security, push updates, manage lifecycle and monitor fleet performance across multiple operators and markets. In the SGP.32 era, strong orchestration is what turns flexibility into scale.”

Integration of eSIM orchestration with traditional connectivity management platforms (CMPs), enterprise systems and legacy processes to then create a unified vision of an asset’s performance is the destination but most recognise this won’t happen in one move or as a single upgrade. “eSIM management systems will increasingly act as the bridge between established SIM environments and newer SGP.32 enabled fleets,” says Schulte. “Rather than forcing organisations to replace legacy processes overnight, connectivity management platforms need to support both SGP.02 and SGP.32, giving teams a single point of control across mixed deployments.”

“SGP.32’s IP based approach also makes lifecycle events more reliable and timelier, which simplifies integration with IoT platforms and enterprise systems,” he adds. “In manufacturing, IFPP allows connectivity credentials to be linked with production data before devices ever enter the field, while remote provisioning enables operator switching and updates throughout the asset’s operational life. When these capabilities are brought together within cloud based platforms, organisations can move beyond isolated data silos towards a more unified, near real time view of each asset - combining connectivity status, behaviour and performance across its full lifecycle.”

Silo-breaking for scalability

“The market is moving away from siloed tools,” says Lindblom Törnqvist. “Historically, SIM management, connectivity oversight and operational systems often sat separately, creating blind spots and slowing decision-making. That model becomes harder to sustain as IoT estates scale globally.”

“eSIM management needs to sit inside broader connectivity management environments and integrate into enterprise systems through APIs and automated workflows,” he says. “That means linking connectivity data with logistics platforms, field operations tools, customer systems and analytics environments so organisations can understand not only whether a device is connected, but whether it is performing commercially and operationally. The most advanced organisations will move towards a closed-loop model where data is captured from the asset, analysed in real-time and converted into automated action. eSIM management should no longer be treated as an isolated telecoms function – it should be embedded into the wider operating model of the business.”

Sanz also foresees a staged process of replacing and upgrading tools and systems. “Integration will be gradual and built around existing systems,” she predicts. “eSIM IoT manager is becoming part of a broader connectivity and device management stack, linking with connectivity management platforms and enterprise IT systems through APIs and automation layers. This allows organisations to build on current processes while improving how connectivity is provisioned and managed.”

“Standardisation plays an important role here by ensuring interoperability across devices, networks and platforms,” she adds. “In practice, SGP.32 can support a unified connectivity layer across different network and device types, helping enterprises improve resilience and maintain service continuity. Over time, this will support a clearer and more consistent view of asset performance without requiring a full system overhaul.”

Unified onto a single-pane-of-glass

There is significant talk about managing and orchestrating IoT assets via a single-pane-of-glass or SPoG but fragmentation remains and the full vision of one system to manage all aspects of an asset is only just being considered. “The direction of travel is clearly towards greater unification,” acknowledges Lindblom Törnqvist. “Enterprises are increasingly frustrated by fragmented portals, multiple carrier dashboards and disconnected data sources. That fragmentation creates cost, slows response times and limits visibility. A single-pane-of-glass model is therefore an attractive long-term goal particularly if it combines connectivity status, lifecycle management, device performance, security posture and commercial insights in one place.”

“That said, the near-term reality for many organisations will be more nuanced,” he says. “Complex estates, legacy systems and regional partnerships mean some businesses will operate with a connected ecosystem of platforms rather than one perfect interface. What matters most is not whether there is literally one screen, but whether the experience feels unified and enables fast, informed decisions across the fleet. Ultimately, the market will reward simplicity, automation and visibility, however they are delivered.”

Sanz sees an appetite for simplicity driving decisions. “The trend is towards simplification, but IoT environments remain complex and diverse,” she explains. “Different device types, networks and operational requirements make it difficult to manage everything through a single interface. A more practical approach is to ensure interoperability between systems so that data can be shared and used effectively.”

“SGP.32 improves that interoperability between the connectivity access and the device, which reduces the fragmentation,” she adds. “The broader objective is to improve how systems work together, giving enterprises a consistent and actionable view of their assets across multiple platforms.”

The universal screen

Schulte doesn’t believe the nirvana of a universal screen that fits every IoT application is realistic. “IoT is clearly moving towards more unified and coordinated management, but the near term reality is unlikely to be one universal screen that fits every user and every use case,” he says. “A more pragmatic and scalable approach is a connected ecosystem of specialist tools, built on shared, consistent data, with tailored views for different teams and roles. SGP.32 supports this direction by standardising and strengthening connectivity lifecycle management, while cloud infrastructure provides the scale, security and resilience needed to extend visibility across operations. The goal should not be a single interface at all costs, but unified insight across the organisation – ensuring that everyone works from the same trusted data, even if they access it through different tools.”

Yet streamlining the complexity of different tools for different functions is an enabler of massive scale IoT and the inherent need for effective automation. “As enterprises deploy devices across multiple countries and operators, the need for an abstraction layer above multiple CMPs is becoming critical,” says Durand. “Managing multiple local operators, eSIM profiles, device alerts, usage data and service workflows through separate tools is becoming unsustainable. That demand is no longer theoretical. It is showing up in every enterprise RFP we see across automotive, utilities and industrial IoT.”

“A true single-pane-of-glass platform should go far beyond dashboards,” he adds. “It should allow enterprises to view, control and automate key events in one place: profile changes, network quality alerts, billing anomalies and device health signals, all with auditability and policy-based automation. For a logistics company managing tens of thousands of mobile assets, or a utility operating smart meters under strict reporting obligations, that unified operational layer becomes essential. The long-term direction is clear: the leaders will be those who can simplify complexity and give enterprises unified control without forcing them to rebuild everything underneath.” ■

“The trend is towards simplification, but IoT environments remain complex and diverse”

OPTIMISED IoT

eSIM shifts the IoT battleground from connectivity to orchestration

The cellular IoT industry is entering a phase where connectivity is no longer the primary challenge, writes Counterpoint Research. Over the past decade, advances in cellular technologies, wider global coverage and declining module costs have made it possible to connect devices at scale across industries and geographies. However, as deployments mature, a more complex issue is coming into focus – how to manage connectivity dynamically, at scale, and for a longer duration. This shift can be particularly seen in large, distributed IoT deployments where devices are no longer restricted to single markets or static environments. They move across borders, operate over long lifecycles and are expected to perform reliably under ever changing network conditions, in varied regulatory conditions and commercial constraints. In such scenarios, it becomes important that connectivity is not treated as a one-time setup that remains fixed or rigid but instead adapts continuously to meet changing needs, conditions and enterprise requirements.

19 companies were ranked based on their response to a detailed survey followed by in-depth discussions and demonstrations of their products

This is where IoT eSIM orchestration begins to take shape. In the context of the GSMA's SGP.32 specification, orchestration refers to the intelligent coordination of connectivity across the entire device lifecycle. While SGP.32 enables remote provisioning and management of SIM profiles, it does not define how these capabilities should be applied. Orchestration builds on this foundation, allowing connectivity to be governed through policies, automated workflows and real-time decision-making. eSIM orchestration lets connectivity become a programmable resource, enabling enterprises to dynamically control how devices connect based on several factors such as location, performance, cost and regulations replacing manual, fragmented processes with centralised, software-driven systems. As this shift accelerates, orchestration is emerging as a key point of consideration within the IoT space, especially at a time when the market looks towards more simplification and seamless solutions.

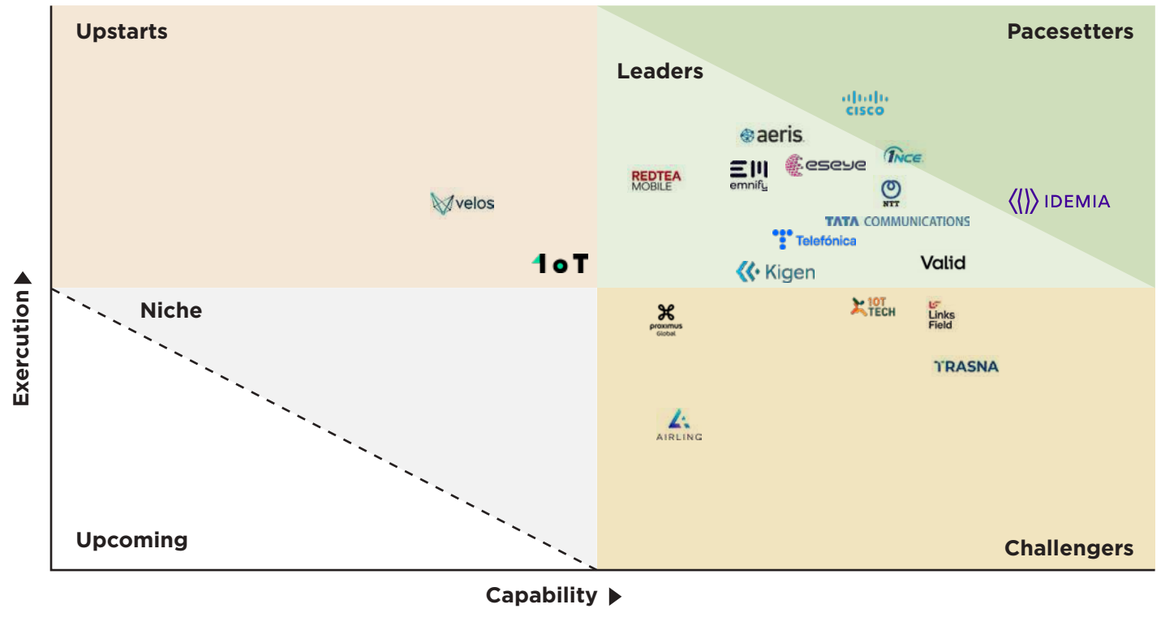
Counterpoint's IoT eSIM Orchestration Core Rankings 2026

Counterpoint's latest IoT eSIM Orchestration Ranking highlights the evolving ecosystem and the roles of vendors as eSIM penetration in IoT devices continues to grow, pushing the market towards adopting more automated, orchestration-led platforms designed to manage connectivity at scale. Going beyond eSIM provisioning capabilities, eSIM orchestration focuses on the players' ability to automate connectivity decisions, integrate with enterprise systems, manage profiles dynamically and support the operational and regulatory requirements of large-scale IoT deployments.

The evaluation highlights Pacesetters, such as **Cisco** and **Idemia Secure Transactions**, which have established strong SGP.32 readiness, advanced automation and deep enterprise integration, alongside a growing number of eSIM-enabled devices driving progress in the IoT space. Leaders follow with well-rounded orchestration capabilities and strong market presence, while continuing to deepen their offerings. Challengers are comparable to Leaders in terms of core capabilities and are expected to focus on execution and scale as the market expands. Meanwhile, Upstarts are likely to deepen their orchestration solution to complement their well-defined execution capabilities.

In total, 19 companies were ranked based on their response to a detailed survey followed by in-depth discussions and demonstrations of their products. The research evaluates vendors across a range of parameters, including lifecycle management, eIM capabilities, security strengths, go-to-market strategies, and geographic reach. It also helps bridge critical layers such as eSIM enablement, provisioning and IoT connectivity management platforms. Many vendors have integrated orchestration capabilities within their connectivity management platform (CMP) offerings, and are turning their focus to expanding automation, enhanced analytics, AI-driven monitoring and support for emerging standards. Overall, the roadmap across players remains highly extensive, with a clear focus on capitalising on the growing demand for eSIM in IoT. This framing also explains why different players across the ecosystem are approaching orchestration from distinct starting points. Some emphasise lifecycle automation, others focus on API-driven control, while some embed orchestration within simplified service ▶

Figure 1: Counterpoint CORE: IoT eSIM Orchestration, 2026



models. Yet across these approaches, a common pattern is noticed which is the value moving away from the SIM and the network, towards the intelligence that governs how connectivity is deployed and managed.

Why does it matter now?

Counterpoint projects that eSIM penetration in cellular IoT modules will increase nearly fourfold by the end of the decade. This shift is already visible today, as enterprises push for greater flexibility and tighter control over how their devices connect, operate and scale across different environments. However, the anticipated growth and capitalisation of this opportunity continue to face a range of ecosystem challenges, such as permanent roaming restrictions in markets like India, Turkey, Egypt, Brazil and Indonesia, originating either from a regulatory standpoint or mobile network operator (MNO) framework, making static connectivity models difficult to sustain, particularly for global deployments. At the same time, devices are becoming more distributed, mobile, with longer lifecycles, and are increasingly business-critical, further driving the need for dynamic, adaptable connectivity.

With SGP.32 establishing the foundation for remote and scalable SIM lifecycle management, the focus is beginning to shift towards tangible outcomes. The specification enables remote profile downloads, activations and switching, but it does not define the logic that guides those actions. Hence, orchestration becomes essential, providing the framework to turn technical features into meaningful, coordinated connectivity management.

Orchestration introduces a programmable, software-defined layer that transforms connectivity into a continuous, policy-driven system. Instead of manually managing profiles or reacting to issues, enterprises can define rules based on geography, network performance, cost or regulatory requirements and have those decisions executed automatically across device fleets. By doing this, orchestration makes it possible for enterprises to remain compliant with local regulations in a dynamic manner to optimise network selection as conditions change in real-time, and to maintain service continuity through automated failover mechanisms that step in seamlessly whenever disruptions occur.

This capability is crucial for large-scale, long-life IoT deployments, where devices must adapt to changing environments over many years. Without orchestration, each change in network conditions, regulation or commercial terms introduces friction and operational complexity. Orchestration enables these variables to become inputs into an automated decision engine that can respond intelligently and at scale. It also makes connectivity easier to manage by hiding the complexity of working with operators, platforms and enterprise systems, and presenting it all through one clear interface, making eSIM more practical for global IoT deployments. As SGP.32 adoption grows, connectivity is shifting from something fixed into something programmable, and orchestration is the layer that makes it usable, scalable and aligned with the modern day requirements of enterprises.

Counterpoint's latest assessment of the IoT eSIM orchestration landscape arrives at a moment when both technology readiness and enterprise ▶

With SGP.32 establishing the foundation for remote and scalable SIM lifecycle management, the focus is beginning to shift towards tangible outcomes

One dimension that is beginning to separate more advanced platforms from the rest is the integration of AI and machine learning into the orchestration layer

expectations are rising in parallel. The market has moved beyond trials and is now preparing for large-scale, production deployments built on automation, control and long-term reliability.

The IoT eSIM Orchestration rankings highlight growing confidence in eSIM as a core enabler for IoT, especially as SGP.32 gains traction. At the same time, enterprise requirements are evolving from basic provisioning to more granular control, automation and integration with enterprise systems, indicating that eSIM as a connectivity technology will require a strong orchestration layer to fully realise its value.

To make sense of what constitutes effective orchestration, Counterpoint frames the market through four foundational pillars. These pillars reflect how orchestration is evolving from a conceptual layer into a set of measurable capabilities.

1. The first is **policy-driven orchestration**, which defines how connectivity decisions are automated based on predefined rules. This includes logic tied to geography, cost, performance or regulatory requirements, allowing connectivity behaviour to adapt dynamically without manual intervention.

2. The second pillar is **network-aware profile management**. Here, the focus shifts to how intelligently platforms can manage and switch profiles based on real-time network conditions, availability and performance thresholds. This is where the promise of SGP.32 becomes operationally meaningful, enabling responsive and context-aware connectivity decisions.

3. The third is **zero-touch provisioning and secure bootstrap**. As deployments scale, the ability to onboard devices without physical interaction becomes essential. Secure, automated provisioning ensures that devices can be activated, authenticated and connected seamlessly, even in remote or constrained environments.

4. The fourth pillar is **compliance-ready monitoring and governance**. With increasing regulatory scrutiny and localisation requirements, orchestration platforms must provide visibility, auditability and control mechanisms that align with regional policies. This extends orchestration beyond technical execution into risk management and compliance assurance.

Together, these pillars show that orchestration is not just one feature but a broad capability that covers automation, intelligence, security and governance.

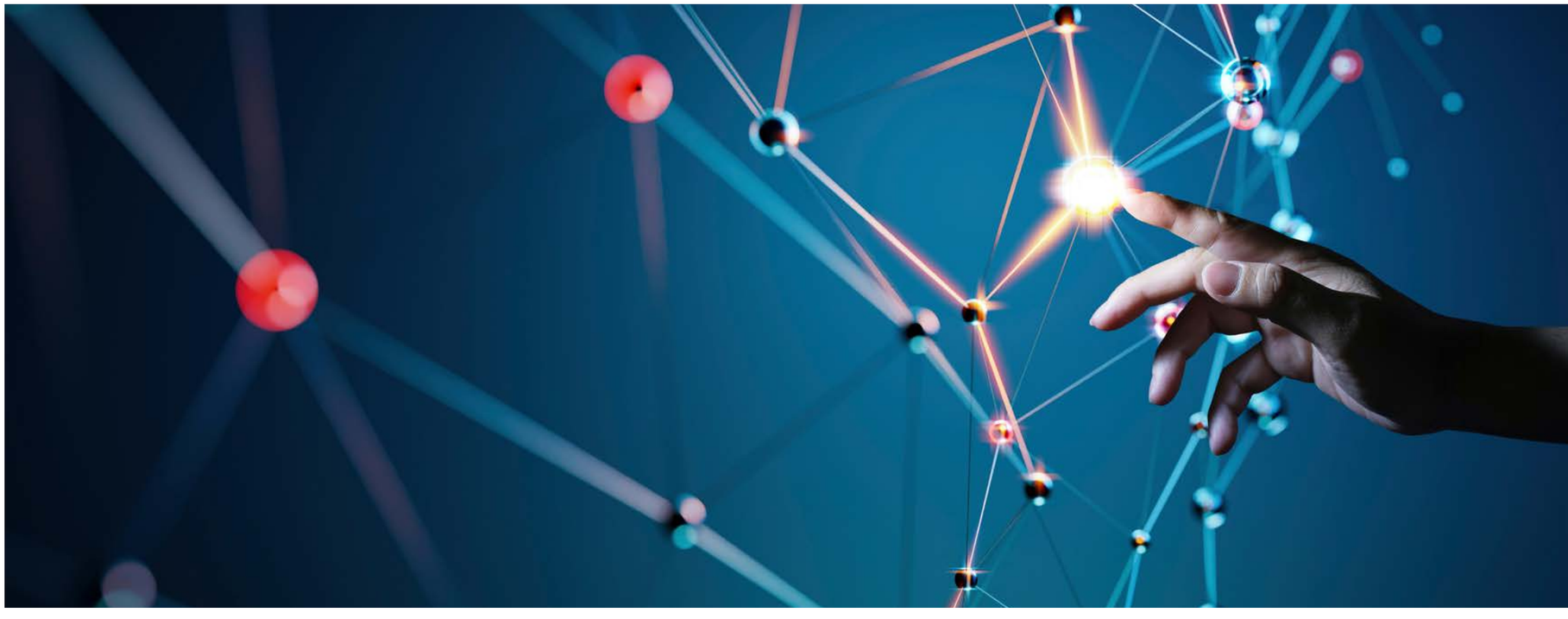
The rankings also highlight the heterogeneous nature of the competitive landscape, which remains far from consolidated. Rather than a single dominant model, three distinct archetypes are emerging, each contributing different strengths to the orchestration stack.

- **eSIM specialists** bring deep technical expertise, particularly around remote SIM provisioning and emerging components such as the eIM. Their strength lies in standards alignment and the ability to implement SGP.32 capabilities at a granular level.

- **Connectivity management platform** providers focus on enterprise integration and operational control. They extend orchestration into business workflows, enabling automation, visibility and large-scale device management across complex deployments.

- **Connectivity-led platform** players, including global mobile virtual network operators (MVNOs) and network providers, contribute scale, resilience and commercial intelligence. Their strength lies in managing multi-operator relationships, optimising network access and ensuring service continuity across geographies.

What becomes clear is that no single archetype ▶



fully addresses the orchestration challenge on its own. As a result, partnerships and ecosystem collaboration are emerging as critical success factors, enabling players to combine strengths across infrastructure, platform and connectivity layers.

Alongside these established archetypes, a new set of players is emerging that seeks to unify these capabilities into a more cohesive orchestration layer. Companies such as **Simetric** are positioning themselves at the intersection of connectivity abstraction, automation and enterprise integration. Rather than focusing on a single layer of the stack, they aim to combine policy control, multi-operator management and API-driven workflows into a unified platform. This reflects a broader shift in the market towards converged orchestration models, where the boundaries between connectivity, platform and enterprise systems begin to blur.

One dimension that is beginning to separate more advanced platforms from the rest is the integration of AI and machine learning into the orchestration layer. Instead of relying only on static policy rules, AI-enabled platforms can analyse patterns across device fleets in real-time, predict network degradation before it impacts performance, rank available profiles based on historical data and detect anomalies that may signal security or connectivity issues. This shifts orchestration from a reactive model to a more predictive and adaptive system. For large-scale deployments where manual monitoring is not practical, this transition towards intelligence-driven orchestration is becoming an important differentiator. While most platforms are still at an early stage, the direction is clear. AI will increasingly play a central role in how connectivity decisions are made.

Looking forward

Looking ahead, Counterpoint's outlook suggests that the market is entering a new phase. Over the next five years, IoT eSIM orchestration is expected to move from early-stage standard adoption to operational maturity. This transition will be shaped by increasing reliance on policy intelligence, growing regulatory complexity shaping decisions and strategies and deeper integration with enterprise systems.

Importantly, the market is unlikely to consolidate around a single type of provider. Instead, success stories will emerge from platforms that can effectively combine standards expertise, automation maturity and enterprise integration resilience. In this sense, the competitive battleground is not defined by who offers eSIM capabilities, but by who can operationalise them most effectively through orchestration. ■

Importantly, the market is unlikely to consolidate around a single type of provider

www.counterpointresearch.com

Easier IoT management through commercial SGP.32 solutions

Market developments around new standards are now making it easier for industries to deploy and manage their IoT systems, reports Antony Savvas.

Enterprise customers don't just need standards, they need a proven way to operationalise them at scale

At the recent MWC26 in Barcelona, Tele2 IoT, Idemia and Cisco jointly unveiled an IoT solution based on eSIM SGP.32. And Giesecke+Devrient (G+D) and AT&T announced a collaboration bringing SGP.32 and 5G connectivity to Rivian's upcoming R2 vehicles. Meanwhile, Evergy, a US utility firm, has selected Kigen's eSIM OS and eIM solution, based on the latest GSMA SGP.32 eSIM specification, in a deployment that unifies private LTE and public networks in a single connectivity layer.

Christina Patsioura, lead analyst for IoT and enterprise at GSMA Intelligence, says: "Enhancements to the SGP.32 eSIM specification are driving renewed interest in eSIM for IoT, with growing commercial activity. Major eSIM vendors such as G+D, Thales and Idemia are highlighting their product announcements and partnerships. Kigen, Soracom, Onomondo, Tele2, KPN and Transatel are among the companies to recently launch SGP.32-compatible solutions."

Changing priorities

Patsioura says: "Operators and IoT connectivity providers should consider prioritising launches. Only a few operators have launched initial SGP.32 IoT services, though this grows to around 40% if testing is included. As momentum builds - and early market response is positive - connectivity providers that do not offer SGP.32-compatible solutions may be left behind. Those that have launched services may enjoy an early-mover advantage."

She adds that providers should emphasise connectivity resilience. For SGP.32 solution providers whose core value proposition is connectivity resilience, positioning should focus on enterprises that operate connected assets across multiple locations and networks. This includes mobile assets, such as vehicles that move across countries, and static deployments, particularly in remote or poorly covered areas. "Providers should emphasise the guaranteed uptime, defined redundancy tiers and managed failover capabilities, and price their solutions at a premium accordingly," she says.

Evidence from mission-critical deployments, such as Evergy's grid infrastructure work with Kigen, shows some enterprises are willing to pay higher prices for assured resilience, adds Patsioura.

Going commercial

KORE, the provider of IoT connectivity, solutions and analytics, will soon release a new portfolio of SGP.32-compliant connectivity solutions in partnership with Kigen, with commercial availability planned for "later in 2026", say the partners.

KORE's SGP.32 solutions support a wide range of devices, from high-power gateways to battery-powered sensors, and include a range of connectivity profiles tailored to different operational needs, such as streamlined roaming, resilient multi-network approaches and local connectivity with intelligent failover and recovery. This enables organisations to deploy and manage connected devices globally, while adapting connectivity over time. Kigen is contributing its secure GSMA-certified SGP.32 eSIM technology to the solutions to underpin the enterprise-grade architecture.

Whether devices are stationary or on the move, KORE's solutions give customers the ability to remotely provision, switch and optimise connectivity without costly truck rolls. The offer is said to ensure interoperability, carrier-grade integrations and the intelligence needed to manage device fleets at scale.

Operationalise at scale

"Enterprise customers don't just need standards, they need a proven way to operationalise them at scale," says Ron Totton, president and CEO of KORE. "With SGP.32, success depends on deep carrier relationships, global infrastructure and the ability to manage complexity across the full device lifecycle. That's where KORE delivers, helping customers turn new standards into real-world, scalable deployments."

Vincent Korstanje, the chief executive of Kigen, adds: "SGP.32 is a defining milestone for the industry because it removes the complexity that has long held back scale for enterprise IoT, making connectivity truly flexible, resilient and secure by design. By building on Kigen's GSMA-certified eSIM, KORE is establishing a trusted foundation that enables enterprises to deploy, manage and scale next-generation connectivity with confidence." ▶

Christina Patsioura,
GSMA Intelligence

Vincent Korstanje,
Kigen

Philipp Schulte,
Giesecke+Devrient

In another launch, Digi International recently introduced its Digi IX25, a next-generation industrial cellular router platform designed to deliver secure, scalable connectivity for critical networking infrastructure. Industrial and enterprise IT and operational technology teams face persistent challenges when deploying cellular connectivity at scale. Field cabinets and kiosks often lack space for multiple networking devices. And industrial environments require hardware that can withstand extreme temperatures and hazardous conditions. At the same time, organisations must meet evolving compliance requirements and prepare for private LTE and 5G networks.

"Digi IX25 is our answer to what industrial customers have been asking for: one rugged solution that delivers 5G connectivity, integrated edge computing, eSIM with live (bootstrap) connectivity out of the box for true zero-touch provisioning, and a lifecycle designed for long-term industrial deployments," says Tony Puopolo, president for Digi Managed Solutions.

Pre-loaded SGP.32-compliant bootstrap

Operational flexibility is enhanced through GSMA SGP.32-compliant eSIM support with live bootstrap pre-loaded, enabling zero-touch provisioning, remote carrier provisioning and multi-carrier management without physical SIM swaps.

In another development, Giesecke+Devrient has launched a new cloud-based SGP.32-compliant eSIM offering that is powered by Amazon Web Services. The collaboration combines digital security from G+D with the necessary cloud agility and scale from AWS. The solution promises to deliver global provisioning and low-latency connectivity solutions across multiple geographies through IoT and other networks.

"As pioneers in SIM and eSIM, we are achieving another industry first through our collaboration with AWS," says Philipp Schulte, the chief executive of G+D Mobile Security. "By bringing eSIM to the cloud and increasing agility and scalability, we will accelerate eSIM adoption in both consumer and IoT applications, providing a secure, future-proof and cost-effective solution for our customers."

SPoG

An emerging trend in the eSIM market is SPoG - single pane of glass - to control your deployments even more easily. SIMPL Wireless' EverSIM supports 5GSA with backwards compatibility to NB-IoT and "everything between", says SIMPL. As IoT architectures evolve toward higher bandwidth, lower latency and always-on connectivity, enterprises need infrastructure that can scale seamlessly. EverSIM addresses this shift by combining advanced eSIM capabilities with centralised bring-your-own-carrier (BYOC) connectivity management, allowing organisations to manage, localise and control devices worldwide without operational fragmentation.

Built on the SIMPL orchestration platform powered by Thales eSIM and eSIM IoT Remote Manager (eIM) technology, EverSIM enables connectivity solution providers and OEMs to "deploy globally in days", while managing complex, multi-operator environments "through a true single pane of glass", SIMPL says.

EverSIM allows customers of every size to test eSIM capabilities, including SGP.32 standards, via proof of concepts (POCs), and "easily scale to mass production".

EverSIM ships pre-loaded with T-Mobile and an additional tier one operator profile, which customers can activate with SIMPL or under their own agreements. Additional carrier profiles can be downloaded and localised globally, with centralised management of up to 100 mobile network operators.

"Connected deployments don't fit a single commercial model. EverSIM lets customers use our amazing carrier relationships, bring their own carrier relationships, or blend both, while managing everything through a single pane of glass," says Ryan Keefe, chief operating officer of SIMPL Wireless. ■

In another development, Giesecke+Devrient has launched a new cloud-based SGP.32-compliant eSIM offering that is powered by Amazon Web Services

IoT connectivity is entering its adaptability era

EV chargers, smart meters, fleet trackers, connected medical devices, industrial sensors. They fail in different ways, but they tend to break for the same reasons. Each was designed for one set of conditions and now has to keep working in another. The asset stays put, the world around it does not and the cycle of change is getting shorter, writes Dave Weidner, the chief executive of Pelion.

Operators are now using remote SIM provisioning (RSP) to make real commercial decisions

This is not a generic point about uncertainty. It is a specific operational reality. Carrier pricing models shift on shorter notice than they used to. Regional regulations are being rewritten. 2G and 3G sunsets are still rolling through a number of markets including the United Kingdom. Data residency rules keep tightening. Cross-border connectivity is increasingly subject to politics that did not exist eighteen months ago. Connectivity pricing for IoT that was stable for a decade is not stable now.

None of these things is unusual on its own. What is unusual now is how these stack on top of each other. A connectivity model that has to absorb one of them is a normal procurement question. A model that has to absorb several of them, across a deployment running anywhere from eighteen months to eight years, is something else.

That is why adaptability is no longer optional in IoT connectivity. Whether your deployment is short-term or long-term, the conditions around it will move. The decisions that hold up are the ones that built in room for that to happen.

What most IoT deployments are still getting wrong

Most deployments are still procured as if change is the exception. Physical SIMs that cannot be repurposed without a site visit are still deployed. Coverage maps that match today's footprint, not next year's, are relied on. A carrier choice that made sense at signing but offers no practical way to switch when commercial terms drift continues to be accepted.

Truck rolls to swap SIMs, cost surprises when roaming rules change without warning, devices stranded in regions where the original carrier is no longer commercially viable and months of delay for re-certifying hardware to support a new operator profile are where businesses are losing money in IoT. None of it shows up in the original business case while all of it shows up in the operating one.

This is also, almost exactly, the problem that embedded SIM (eSIM) was designed to solve.

eSIM is not new - adoption at scale is

eSIM has been around in some form for the better part of a decade. For most of that time, it sat in datasheets as a future capability rather than something operators used in volume. What has changed is the surrounding ecosystem. Module support is broad, carrier provisioning APIs are mature and bootstrap profiles work reliably across regions.

Operators are now using remote SIM provisioning (RSP) to make real commercial decisions. These include testing a carrier in a new market without recommitting hardware, swapping profiles when a network's coverage degrades, isolating a misbehaving fleet from production traffic and rotating profiles after a known compromise. None of these were practical with physical SIMs at any sensible scale.

The point is not that eSIM is exciting. What matters is that it solves a practical problem: how you keep a deployment commercially viable when the conditions around it keep moving.

eSIM is evolving at pace, adoption is following demand

eSIM adoption is picking up across IoT for a simple reason. Deployments are demanding more flexibility than they used to. The toolkit available to meet that demand has expanded to match. ▶

Pelion

SPONSORED ARTICLE

Pelion has been working in this space for years. We have helped businesses put remote provisioning to real use, choosing carriers across markets, switching between them as conditions change, and turning that flexibility into measurable outcomes. These include faster route to revenue in a new region, lower cost-to-serve at scale, the digitisation and sustainability gains that come from running fewer truck rolls and getting a longer working life out of every asset deployed.

The tools to meet that demand have caught up. Most IoT estates were built on embedded universal integrated circuit card (eUICC) SIMs using the GSMA's SGP.02 standard for M2M. Pelion now offers SGP.22 capability (Consumer eSIM) on top of that, extending managed connectivity beyond the device categories the original M2M spec was designed for such as tablets, wearables, point-of-sale units or anything in a consumer form factor finding its way into commercial IoT use. Consumer eSIM adoption has done the heavy lifting of driving down module and firmware costs, and IoT deployments are now picking up the benefit.

And SGP.32, the next step in that evolution, shows no sign of slowing the pace down.

SGP.32 points to where this is heading

SGP.32 is the next chapter in eSIM standards, building on what SGP.02 brought to M2M and what SGP.22 brought to consumer form factor devices. The aim is to combine the operational discipline IoT estates need with the kind of remote profile management that keeps devices flexible long after they leave the factory.

If the spec delivers on what it sets out to do, the result is connectivity that is genuinely borderless, with zero-touch network switching as deployments cross regions, regulations and commercial conditions. That is the right destination. It is also still some distance off in practice.

We are early. Devices in the field need to catch up. Network operators need to adopt the standard. Connectivity providers need to make the use cases concrete enough for buyers to act on, not just admire from a distance. None of those are blockers. But they are real and the projects that pretend otherwise will find that out the hard way from the challenges it will introduce.

The question worth asking is not 'should we wait for SGP.32?' It is 'what does our connectivity model need to do over the next several years, and how do we start moving towards that without freezing the project we are trying to ship?'

Where capability stops and operations begin

Putting eSIM in the device is one thing. Running two million of them is another.

In practice, this is unglamorous and very specific and involves live visibility into which device is on which network and policy controls that flag a device suddenly transmitting ten times its expected volume before the bill arrives, not after. A way to test, stage and roll out a new operator profile without taking the estate offline is needed along with support that picks up at 3am when something out of contract has gone wrong. The device in the field does not care what the office hours are.

Pelion's approach is built on three layers that have to work as one: IoT connectivity, in the form of multi-network SIM and eSIM coverage across 600 networks in more than 150 countries; a platform that gives operators the visibility, policy and orchestration to run an estate sensibly rather than reactively; and a service layer of expertise and support, from carrier negotiation through outage triage, that handles the parts buyers do not want to staff in-house. The result is connectivity that adapts as your business does, with the commercial control and operational insight to keep cost-to-serve from running away from you at scale.

Being voted #1 for IoT Connectivity Management on G2 is peer-reviewed evidence that the approach holds up day to day. The numbers behind it are 1.5 million-plus connections live, 99.9995% uptime, and someone primed for the 0.0005% when things go wrong. The point is not that any one of those layers is novel on its own. It is that buyers who try to assemble them separately tend to discover, eighteen months in, that the seams are exactly where the failures sit.

What to take away

If you are planning a deployment in 2026, four questions are worth pressure-testing with whoever is providing your connectivity.

- What happens if our primary network changes its commercial terms?
- How do we move a million devices to a new profile without sending a truck to each one?
- Who picks up the phone at 3am on a public holiday?
- What does our cost per connected device look like in year five, not year one?

The winners over the next decade will not be the organisations that connect the most devices. They will be the ones that can keep those devices connected, controlled and commercially sustainable as the conditions around them change. That is what the adaptability era looks like in practice.

We sometimes tell people at parties that we connect things to stuff. The serious version is that we keep things connected for the long haul, even when the world around them does not stay still. ■

Two follow-ups, if you want to continue the conversation:

IoT Expo North America. I will be at IoT Expo in North America, showing how our eSIM proposition keeps large-scale IoT fleets reliably connected. One multi-network offering, coverage for any device, in any state. If you want to compare notes on your own deployment, find me there.

An invitation: London, 2 July. We are co-hosting a private evening with IoT Now and Transforma Insights for IoT leaders and the people running deployments into the next era of connectivity. Honest conversation about eSIM today and where SGP.32 takes us next. The room will be small. If that sounds useful, get in touch and we will see about a seat.

*Global IoT Connectivity Made Effortless. More at **pelion.com**.*

How to differentiate an IoT connectivity offering – the six ‘S’s

One of Transforma Insights’ key focus areas is cellular-based IoT connectivity, tracking key trends in best practice and the evolution of technology, regulation and commercial models in the space. One perennial concern for IoT connectivity providers, whether MNOs or MVNOs, is price erosion. As a result, writes Matt Hatton, the founding partner of Transforma Insights, one overriding key theme of their evolving strategies is the pursuit of mechanisms to mitigate continuing declines in average revenue per connection.

In this article we explore the six key approaches to differentiation that we identified in our recent Communications Service Provider IoT Peer Benchmarking Report

As a side note, we should emphasise that this challenge can be somewhat overstated as much of it stems from increasing support for low revenue use cases rather than necessarily precipitous declines on a like-for-like basis. Nevertheless, there is a perpetual requirement to continue to support growing numbers of connections at a lower cost-per-unit.

The overall impact is that communications service providers (CSPs) continue to look for ways to reduce costs, differentiate propositions and diversify revenue. Differentiation of the service offering and securing additional revenue streams are two sides of the same coin. Effective differentiation tends to mean higher revenue per connection for the core connectivity proposition.

In this article we explore the six key approaches to differentiation that we identified in our recent Communications Service Provider IoT Peer Benchmarking Report: Software, Supply, Scale, Services, Solutions and Systems.

Supply

Supply relates to the core connectivity proposition delivered by CSPs, particularly in the form of wholesale and roaming data access. This remains the foundational layer of any IoT connectivity offering. Historically, the most successful mobile virtual network operators (MVNOs) have differentiated themselves by securing direct access agreements with mobile network operators (MNOs). These arrangements provide greater control, improved pricing structures and enhanced service quality compared to more commoditised models based on sponsored roaming or mobile virtual network enabler (MVNE) platforms.

Such differentiation has been critical in a market where many providers otherwise offer largely indistinguishable connectivity services. However, the emergence of eSIM localisation is beginning to disrupt established dynamics. By enabling more flexible provisioning and network switching, eSIM technology reduces reliance on traditional roaming ▶

constructs. This shift introduces both opportunities and risks, requiring CSPs and MVNOs alike to establish new forms of trusted partnerships. In this evolving landscape, the ability to maintain privileged access arrangements while adapting to more dynamic connectivity models will be a key determinant of competitive positioning.

Scale

Scale is a fundamental driver of competitiveness in IoT connectivity. Although pricing models are typically structured as cost-plus, where CSPs apply a margin to a largely externally determined per-gigabyte data cost, scale introduces several indirect advantages. Larger players benefit from stronger negotiating leverage when forming direct access agreements, enabling them to secure more favourable commercial terms.

In addition, scale often translates into broader network access across multiple geographies. This is increasingly important in a fragmented technological environment where enterprises require multi-network resilience and coverage diversity. Another significant benefit lies in cost distribution. Fixed investments, such as internally developed middleware platforms, compliance frameworks and security capabilities, can be amortised across a larger revenue base. This improves overall margin profiles and allows scaled providers to reinvest in innovation more effectively than smaller competitors.

Software

Software capabilities, particularly middleware platforms, are central to enabling and differentiating IoT connectivity offerings. At a baseline level, most CSPs provide similar functionalities, including SIM lifecycle management, billing and reporting. However, meaningful differentiation increasingly arises from advanced features layered on top of this core. These include eSIM orchestration, cloud platform integration and enhanced security modules, delivered either through in-house development or third-party partnerships.

Despite the availability of such features, monetisation has historically been challenging. Enterprises have often resisted paying premiums for add-ons, viewing connectivity as a commodity. Nevertheless, there is growing evidence that enterprise buyers are selecting providers based on the depth and sophistication of their software capabilities. This trend is reinforced by the emergence of artificial intelligence applications, such as anomaly detection, predictive maintenance and automated optimisation. While still relatively nascent, AI-enhanced value-added services have the potential to materially strengthen propositions and create new revenue streams, particularly if positioned effectively within broader solution offerings.

Services

Services encompass the range of professional and support offerings that complement core connectivity. These extend from enhanced customer support and technical account management to pre-sales consulting, post-sales optimisation and full-scale systems integration. Many CSPs also provide access to development labs and hardware support capabilities, helping enterprises design, test and deploy IoT solutions more efficiently.

Not all services are directly monetised; some function as strategic enablers designed to increase customer retention and lifetime value. In addition, services play an important role in shaping brand perception. In a market where technical differentiation is often limited, positioning as a trusted, reliable and compliant partner can be a decisive factor. Established telecoms brands, in particular, benefit from longstanding reputations that signal stability and reduced counterparty risk. This ‘trust premium’ can influence enterprise purchasing decisions, especially in regulated or mission-critical environments.

Solutions

The question of whether CSPs should move ‘up the stack’ to deliver end-to-end solutions has been debated for many years. In practice, relatively few have achieved sustained success in this area. Delivering complete solutions requires not only technical capability but also a credible ‘right to play’ within specific vertical markets, many of which are already highly competitive and fragmented. For most CSPs, this limits viable opportunities to a small number of sectors where they possess domain expertise or strategic partnerships.

That said, recent innovation has been more promising in horizontal capabilities that can be applied across multiple industries. Examples include video analytics platforms, managed gateway services and enterprise branch connectivity solutions. These offerings avoid the need for deep vertical specialisation while still enabling value creation beyond basic connectivity. A critical success factor is contextualisation: adapting and presenting horizontal capabilities in ways that resonate with specific industry use cases. This approach allows CSPs to balance scalability with relevance, improving their ability to capture value in diverse markets.

Matt Hatton,
Transforma Insights

Systems

Underlying systems and operational processes are increasingly central to the economics of IoT connectivity. Reducing the cost to serve large volumes of connections requires significant optimisation of internal platforms and workflows. Over the past year, many CSPs have intensified their focus on automation and digitalisation initiatives aimed at improving efficiency and scalability.

Key areas of development include self-service portals that enable customers to manage connectivity independently, cost optimisation tools that provide greater transparency and control, and proactive incident management systems that minimise downtime. Additionally, there is a strong emphasis on automating order management and fulfilment processes to reduce manual intervention and accelerate time to market.

Infrastructure strategy is also evolving, with a growing shift towards globally distributed, cloud-based architectures. These approaches favour operating expenditure models over traditional capital-intensive deployments, providing greater flexibility and scalability. Collectively, these system-level improvements are essential for sustaining margins and supporting growth in an increasingly competitive and price-sensitive market. ■

TRANSFORMA INSIGHTS

Global Advisors on IoT, AI and Digital Transformation

Every year Transforma Insights publishes its list of IoT 'Transition Topics' highlighting where we expect to see seismic change occurring during the year. This year the list focuses on the intersection of AI and IoT, the persistent challenge of regulation, greater localisation, and the impact of a shifting connectivity technology landscape.

IoT Transition Topics 2026

- AI-enabled IoT video analytics poised for explosive growth
- IoT vendors use AI to optimise and differentiate their offerings
- A shake-out is on the cards for cellular network technologies
- The rise of the Single Pane of Glass platform
- Continued geopolitical challenges and polarisation of markets
- The increasing requirement for localisation
- The rubber hits the road for SGP.32
- How to sell more IoT?
- Hardware innovations driving growth
- The implications of the evolution to software-defined vehicles

To learn more about the Transition Topics, you can find more details in our press release: transformainsights.com/news/iot-transition-topics-2026

The Transition Topics will form the basis of a significant part of the research agenda for the Transforma Insights Advisory Service in 2026, as well as sponsored Position Papers and Virtual Briefings. To learn more about our 2026 Research Agenda, or to discuss sponsorship opportunities, please contact us at enquiries@transformainsights.com

Rewriting the rules of IoT connectivity: inside the shift to SGP.32

The next phase of IoT is not being defined by devices alone – it is being shaped by how seamlessly those devices connect, adapt and scale across borders, networks and evolving business needs. For enterprises deploying connected solutions globally, the challenge has never simply been connectivity; it has been complexity.

The partnership between KORE and Kigen around the GSMA SGP.32 eSIM standard represents an important shift in how that complexity is addressed. Rather than introducing entirely new technology paradigms, SGP.32 refines and simplifies existing eSIM capabilities – making them more accessible, interoperable and aligned with real-world customer needs.

This evolution is less about technology disruption and more about removing friction. It is about enabling enterprises to focus on outcomes – operational efficiency, resilience and global reach – while the underlying connectivity infrastructure becomes more adaptive and easier to manage.

The customer challenge: Complexity at scale

For enterprises operating across multiple geographies, connectivity has historically been a balancing act. Traditional SIM-based deployments required upfront decisions about carriers, regions and network strategies – often locking organisations into rigid models that struggled to keep pace with changing business conditions.

Even earlier eSIM standards, while transformative, introduced their own operational hurdles. Deploying and managing profiles could require significant technical dependency and orchestration, specialised infrastructure and coordination across multiple ecosystem partners.

As highlighted in industry discussions, previous standards often placed the burden of deployment and management on the customer, requiring them to navigate fragmented systems and workflows.

At the same time, the global landscape has become more dynamic. Regulatory shifts, regional requirements and geopolitical changes increasingly demand that enterprises adapt connectivity strategies in near real-time or expediently based on business logic. A static approach is no longer sufficient.

SPONSORED ARTICLE

In this context, the true customer need is clear: simpler, more flexible connectivity that can scale globally without increasing operational overhead.

Simplifying what already works with SGP.32

The GSMA SGP.32 standard builds on the foundation of earlier eSIM specifications but introduces meaningful simplifications that directly address customer pain points.

One of the most significant changes is the removal of legacy architectural components – such as the subscription manager secure routing (SM-SR). Doing away with this reduces the complexity involved in provisioning and managing connectivity profiles. This streamlining makes profile delivery more efficient and lowers the technical barriers to adoption.

Equally important, SGP.32 introduces a more flexible and interoperable framework. Instead of operating within closed ecosystems tied to specific providers, enterprises can now work across multiple eSIM management platforms and service providers. This openness enables greater choice and adaptability, but it also requires stronger coordination across the ecosystem.

From a customer perspective, the value is not just technical - it is operational.

- Faster and simpler deployment of connectivity
- Greater flexibility in choosing and switching network providers
- Reduced dependency on complex backend infrastructure

In short, SGP.32 transforms eSIM from a powerful but sometimes complex capability

Equally important, SGP.32 introduces a more flexible and interoperable framework. Instead of operating within closed ecosystems tied to specific providers, enterprises can now work across multiple eSIM management platforms and service providers

into a more accessible and scalable tool for global IoT.

The role of partnership: Why KORE and Kigen matter

Technology standards alone do not solve customer challenges; they clear the barriers that make solutions possible. Their success depends on how effectively they are implemented, integrated and supported across the ecosystem.

This is where the collaboration between KORE and Kigen becomes significant.

KORE, with its extensive experience in global IoT connectivity and orchestration, provides the operational layer that translates these technical capabilities into real-world outcomes. With a heritage rooted in direct carrier integrations and global connectivity management, KORE is positioned to help enterprises navigate the complexity of multi-network deployments.

Kigen, as a leader in secure eSIM and iSIM technology, brings deep expertise in enabling GSMA eSA certified eSIMs and GSMA SAS-certified remote SIM provisioning, and ensuring interoperability across devices and networks. Their role in advancing SGP.32 standard's architecture aligned with the broader industry push towards simplifying connectivity suited for IoT while maintaining robust security and scalability.

Together, the partnership reflects a shared focus: making advanced connectivity capabilities usable, manageable and valuable for customers through shared expertise.

Interoperability as a customer imperative

One of the defining characteristics of SGP.32 is its emphasis on interoperability. Unlike earlier models that often operated within closed loops, the new standard enables multiple eSIM management providers to coexist and interact.

While this introduces new opportunities, it also underscores the importance of coordination. Enterprises must ensure that devices, modules, networks and management platforms work together seamlessly.

As industry experts note, the success of SGP.32 depends not just on the technology itself, but on how well ecosystem partners collaborate to provide clear documentation, testing frameworks and integration support.

For customers, this translates into a critical requirement: confidence that their entire IoT stack – from hardware to connectivity management – will operate cohesively.

This is where experienced partners play a crucial role. By guiding customers through testing, validation and deployment, they help ensure that the promise of interoperability becomes a practical reality.

From fragmentation to visibility: The single pane of glass

As IoT deployments scale, another challenge emerges: visibility.

Enterprises often manage devices and connectivity across multiple regions, carriers and platforms. Without a unified view, operational efficiency suffers, and decision-making becomes more complex.

SGP.32, combined with orchestration capabilities from providers like KORE, enables a shift toward centralised management

The global nature of IoT is both an opportunity and a challenge. Enterprises operating across dozens of countries must navigate varying regulatory environments, network requirements and market conditions.

across the enterprise device estate. The concept of a single pane of glass becomes increasingly important – allowing customers to monitor, manage and optimise their entire connectivity estate from one interface.

This approach addresses a fundamental customer need: simplicity in management, even as complexity grows underneath.

Rather than logging into multiple systems or coordinating across disparate providers, enterprises gain a consolidated view of their operations. This not only improves efficiency but also enhances control and strategic insight.

Globalisation, localisation and resilience

The global nature of IoT is both an opportunity and a challenge. Enterprises operating across dozens of countries must navigate varying regulatory environments, network requirements and market conditions.

In this context, SGP.32 enables a critical capability: dynamic localisation. Instead of relying solely on roaming agreements, enterprises can provision local connectivity profiles as needed - often instantly. This allows devices to operate more efficiently within specific regions while maintaining global consistency.

The importance of this capability is growing. As geopolitical and regulatory dynamics evolve, the ability to adapt connectivity strategies quickly becomes essential. Enterprises can no longer rely on static models; they need solutions that can respond to change in real-time. ▶

For multinational organisations, this is no longer optional. As noted in industry discussions, ability to utilise advanced eSIM capabilities is becoming table stakes for global operations.

Technology as an enabler, not the endpoint

A key theme in the evolution of SGP.32 – and in the KORE and Kigen partnership – is the idea that technology should serve the customer, not the other way around.

The goal is not to introduce complexity in the name of innovation, but to remove barriers that prevent customers from achieving their objectives.

This perspective reframes the role of connectivity in IoT:

- It is not just about connecting devices
- It is about enabling business outcomes
- It is about supporting agility, resilience and growth

By simplifying profile management, enhancing interoperability and enabling centralised control, SGP.32 allows enterprises to focus on what matters most: delivering value through their connected solutions.

The path forward: Collaboration across the ecosystem

The success of SGP.32 and the broader evolution of IoT connectivity – depends on collaboration. Device manufacturers, module providers, network operators and eSIM solution providers must work together to ensure compatibility, standardisation and ease of use. Clear documentation, robust testing and shared best practices will be essential.

Encouragingly, the industry is already moving in this direction. Module manufacturers are developing solutions that better support profile transactions and ecosystem partners are aligning around common standards and frameworks.

By simplifying profile management, enhancing interoperability and enabling centralised control, SGP.32 allows enterprises to focus on what matters most: delivering value through their connected solutions.

For customers, this collaborative approach reduces risk and accelerates adoption. It creates an environment where innovation can flourish without being hindered by fragmentation or uncertainty.

A customer-centric evolution

The partnership between KORE and Kigen around SGP.32 is not just about advancing eSIM technology – it is about redefining how connectivity supports the modern enterprise.

By focusing on simplification, interoperability and scalability, this collaboration addresses the real challenges faced by global IoT deployments. It enables organisations to move beyond the constraints of traditional connectivity models and embrace a more flexible, resilient approach.

Ultimately, the value of SGP.32 lies in what it enables:

- Seamless global operations
- Adaptive connectivity strategies
- Simplified management at scale

In a world where change is constant and complexity is inevitable, the ability to simplify and adapt becomes a competitive advantage. And that is where the true impact of this partnership is felt – not in the technology itself, but in the outcomes it makes possible for customers. ■

www.korewireless.com
www.kigen.com

From coverage to capability - why satellite is becoming a core layer of IoT connectivity

For much of its history, satellite connectivity has occupied a narrow, specialised role within the broader IoT ecosystem. It has been viewed as a solution for edge cases, a fallback when terrestrial networks fail, or a tool reserved for industries operating in the most remote parts of the world. This perception shaped how systems were designed, how investments were prioritised, and how connectivity strategies were evaluated, but now it is beginning to shift in a meaningful way, writes Martin Jefferson, global solutions architect at Globalstar.

Across industries, expectations around connectivity have evolved. Organisations are no longer satisfied with technology that functions most of the time or in most locations. They are being asked to operate with consistency, visibility and responsiveness across increasingly distributed environments. These demands are not theoretical. They are being driven by operational realities, regulatory pressures and the growing reliance on connected systems to manage critical infrastructure, assets and personnel.

On top of that, properly designed communications infrastructure must include any and all technologies from day one in order to satisfy the variable connectivity requirements of their users.

In this context, satellite connectivity is taking on a new role. It is no longer confined to the margins of IoT architecture. It is becoming an intentional, integrated layer that supports how modern operations function and one that needs to be built into the connectivity infrastructure from the start.

Rethink the boundaries of connectivity

Traditional connectivity strategies have largely been built around the strengths of terrestrial networks. Cellular and Wi-Fi infrastructure have enabled large-scale deployments and supported the rapid growth of IoT over the past decade. These networks are efficient, widely available and well understood. However, they are also inherently limited by geography, infrastructure and environmental conditions. They are also subject to financial caveats such as being able to support infrastructure with sufficient subscriptions. ▶

SATELLITE IoT

As deployments expand, those limitations become more visible.

A logistics company may track vehicles seamlessly across urban corridors but lose visibility as soon as those assets move into rural or cross-border regions. A utility provider may monitor infrastructure effectively under normal conditions but struggle to maintain communication during storms or outages. A remote industrial site may rely on intermittent connectivity that introduces delays and uncertainty into operations.

These gaps are often treated as exceptions. In reality, they are becoming a defining characteristic of modern IoT deployments.

The scale and distribution of connected systems are increasing faster than the reach of terrestrial infrastructure. This creates a mismatch between where operations occur and where connectivity is available. Addressing that mismatch requires a different approach. It requires thinking about connectivity not as a single network, but as a layered capability that can adapt to different environments.

Satellite plays a critical role in that layered model. It extends connectivity beyond the boundaries of terrestrial infrastructure and provides a level of continuity that cannot be achieved through ground-based networks alone.

Design for reliability instead of coverage

One of the most important shifts taking place in IoT architecture is the move from maximising coverage to ensuring reliability.

Coverage, in its traditional sense, implies that a device can connect when it is within range of a network. Reliability, on the other hand, focuses on whether a system can consistently perform its intended function regardless of external conditions. This distinction matters because many IoT applications do not require constant high-bandwidth connectivity. They require dependable communication at critical moments.

A sensor monitoring pipeline pressure does not need to transmit large volumes of data continuously. It needs to send an alert when conditions change. A tracking device attached to a shipping container does not need to stream information at all times. It needs to provide accurate location updates when the asset moves or reaches a checkpoint. A safety device carried by a field worker does not need to maintain an open channel. It needs to be able to send a distress signal immediately when required.

In each of these scenarios, the value of connectivity is tied to reliability rather than throughput. ▶

The scale and distribution of connected systems are increasing faster than the reach of terrestrial infrastructure

The combination of edge processing and satellite connectivity creates a more resilient architecture

Satellite connectivity aligns naturally with this requirement. It provides a consistent communication pathway that is not dependent on local infrastructure. When integrated into a broader connectivity strategy, it ensures that critical signals can be transmitted even when other networks are unavailable or unreliable.

This approach supports what many organisations are now describing as a 'connected enough' model. Systems are designed to function autonomously where possible and to communicate selectively when necessary. Satellite serves as the mechanism that guarantees those communications can occur.

The growing role of intelligence at the edge

At the same time that connectivity strategies are evolving, so too is the way data is processed within IoT systems. The traditional model of sending all data to centralised cloud platforms for analysis is becoming less practical as deployments scale. It introduces latency, consumes bandwidth and creates dependencies on continuous connectivity that are difficult to maintain in many environments.

In response, organisations are moving toward a more distributed model of intelligence.

Devices are becoming capable of filtering, analysing and acting on data locally. This reduces the amount of information that needs to be transmitted and allows systems to respond more quickly to changing conditions. It also enables operations to continue even when connectivity is intermittent.

This shift places new demands on connectivity. Instead of supporting constant data transfer, networks must support targeted, high-value communication. They must ensure that when a device determines that information needs to be shared, there is a reliable pathway available.

Satellite connectivity is particularly well-suited to this model. Its strength lies in its ability to provide dependable communication across wide geographic areas with relatively low power requirements. It complements edge intelligence by ensuring that local decisions can be locally actioned as well as be communicated to centralised systems as necessary.

The combination of edge processing and satellite connectivity creates a more resilient architecture. It allows organisations to have low power requirements and cost savings by only transmitting actionable data, while allowing local decision-making with near-zero latency.

Extend visibility in the real world

The impact of this approach can be seen in practical deployments across industries.

Lonestar Tracking provides a clear example. The company supports customers who need to track assets across environments where connectivity is inconsistent or nonexistent. These assets may include vehicles, equipment or high-value shipments that move across large geographic areas.

In many cases, traditional tracking solutions perform well within established network coverage. The challenge arises when assets move beyond those boundaries. At that point, visibility is lost. Organisations are left without accurate information about location, status or movement until the asset returns to a covered area.

This gap introduces a range of operational issues. It can lead to delays in locating assets, reduced utilisation and increased risk of loss or theft. It also limits the ability to respond to unexpected events.

By integrating satellite connectivity into its solutions, Lonestar Tracking has been able to address these challenges. Assets can be monitored continuously, regardless of their location. Critical updates can be transmitted even when cellular networks are unavailable. This creates a consistent flow of information that supports more effective decision-making.

The broader lesson is not specific to a single company or use case. It reflects a general pattern. As soon as visibility extends beyond the limits of terrestrial networks, satellite becomes an essential component of the solution.

A key insight from Lonestar Tracking's deployment reinforces a broader shift happening across IoT architectures. As Lonestar Tracking's CEO Thomas Remmert noted, the goal was never to create a continuous stream of data. What mattered was receiving the right data at the right moment. This distinction is important. Not every use case benefits from constant connectivity and, in many cases, it introduces unnecessary cost and complexity. Instead, systems are being designed to surface actionable data – critical events, change in status or key location updates when they occur. Satellite connectivity supports this model by ensuring those high-value transmissions can always get through, regardless of where the asset is. It algins directly with the move towards more intelligent, efficient data strategies, where relevance and timing take precedence over volume.

Operational resilience and the cost of uncertainty

As organisations become more dependent on connected systems, the consequences of connectivity gaps become more significant. In many cases, the cost of lost connectivity is not immediately visible. It appears as delays, inefficiencies or missed opportunities. Over time, these impacts accumulate. They affect productivity, increase operational costs and introduce risk.

In other cases, the impact is more direct. A failure to receive an alert can lead to equipment damage. A lack of visibility into asset location can result in loss or theft. An inability to communicate during an emergency can compromise safety. ▶

These outcomes are driving a reassessment of how connectivity is valued.

Rather than focusing solely on the cost of implementing connectivity solutions, organisations are increasingly considering the cost of not having them. This shift changes the conversation. It moves connectivity from a discretionary investment to a core component of operational resilience.

Satellite connectivity plays a central role in this context. It provides a level of assurance that critical communication pathways will remain available. This reduces uncertainty and allows organisations to operate with greater confidence.

Supporting the next generation of connected systems

Looking ahead, the importance of reliable connectivity will continue to grow as new technologies emerge.

One of the most significant developments is the rise of physical AI. This refers to the integration of artificial intelligence into physical systems such as robots, drones and autonomous vehicles. These systems rely on continuous data exchange to function effectively. They must be able to receive inputs, process information and respond to their environment in real-time.

Many of these applications are being deployed in environments where connectivity is limited. This creates a challenge. The systems that depend most on reliable communication are often operating in areas where traditional networks are least effective.

Addressing this challenge requires a connectivity strategy that is both flexible and robust. Satellite provides a foundation for that strategy. It ensures that communication can be maintained across diverse environments and supports the deployment of intelligent systems at scale.

This is not a distant future scenario. Early implementations are already underway in industries such as logistics, energy and agriculture. As these systems become more common, the demand for integrated connectivity solutions will increase.

Connectivity as a core element of infrastructure

The evolution of IoT is leading to a broader redefinition of connectivity.

It is no longer sufficient to treat connectivity as a feature that can be added to a system. It must be considered as part of the underlying infrastructure that supports operations. This perspective aligns connectivity with other foundational elements such as power, transportation and physical facilities.

When viewed in this way, the importance of resilience, scalability and reach becomes clear.

Satellite connectivity addresses these requirements in a way that complements terrestrial networks. It provides a global layer of communication that is independent of local conditions. This makes it a valuable component of any comprehensive connectivity strategy. Organisations that adopt this perspective are better positioned to design systems that can adapt to changing conditions. They can deploy solutions with greater confidence and operate more effectively across diverse environments.

A new standard for connected operations

The role of satellite in IoT is changing because the requirements of IoT are changing.

What was once considered sufficient is no longer adequate. Systems must be more reliable, more flexible and more capable of operating across a wide range of conditions. Meeting these requirements requires a shift in how connectivity is approached.

Satellite connectivity provides a way to meet that challenge. It extends the reach of connected systems, supports new operational models and enables the dynamic deployment of advanced technologies on an ongoing basis.

The transition from optional to essential is already underway. Organisations that recognise this shift are beginning to integrate satellite into their connectivity strategies as a standard component rather than a specialised tool.

This integration will shape the next phase of IoT development. It will influence how systems are designed, how operations are managed and how value is created.

Connectivity, in this sense, has evolved beyond simply moving data to enabling capability and driving business outcomes. ■

One of the most significant developments is the rise of physical AI. This refers to the integration of artificial intelligence into physical systems such as robots, drones and autonomous vehicles

www.globalstar.com

IoT Tech Expo North America 2026 promises intelligence at the edge and action in the real world

Taking place 18-19 May 2026 in San Jose, California, USA, IoT Tech Expo North America 2026 arrives at a pivotal moment - when the industry's focus shifts from connecting devices to making them consequential.

The IoT industry has moved on. Connectivity is no longer the headline. What matters now is what connected systems actually do - the decisions they make, the processes they drive and the value they deliver at operational scale. IoT Tech Expo North America 2026 reflects that shift directly, with a programme built around execution rather than aspiration.

The agenda features senior figures from Google, Qualcomm, IBM, NVIDIA, Siemens, Schneider Electric, Ericsson, Airbus, Bosch, Boston Dynamics, Mastercard and PepsiCo, among others. What is notable is not just the calibre of speakers, but the specificity of what they are addressing: not IoT's potential, but its delivery. ▶

Digital twins are evolving rapidly - from operational models into active decision-support systems capable of simulation, prediction and autonomous action

The operationalisation challenge of edge AI

Edge AI sits at the centre of this year's programme - and the conversation has moved well beyond architecture. Shilen Jhaveri of Google, Trilok Agrawal of Qualcomm and Abraham Jun Zou of Mastercard focus on how organisations are embedding intelligence into production environments where latency, reliability and cost must all be managed simultaneously.

Joseph Glover of Akamai and Saad Malik of Spectro Cloud address what happens when edge deployments scale from dozens of locations to thousands. At that point, the challenges are no longer primarily technical - they are operational. Orchestration, immutability and failure management at scale are the realities that determine whether an edge AI strategy holds together under production conditions.

Beyond industrial IoT pilots

Manufacturing remains the proving ground for IoT - and the place where ambition most frequently meets resistance. Sessions from Kevin Clark of Siemens, Helenio Gilabert of Schneider Electric and Ninad Kulkarni of PepsiCo take on the 'pilot purgatory' problem directly: many organisations have demonstrated IIoT value in controlled environments but are struggling to scale those systems across complex, legacy-laden operations. The focus is on system-level thinking - data architectures built for industrial volumes, integration strategies for environments not designed to be connected, and the organisational alignment needed to make digital transformation stick. Will Foss of Boston Dynamics adds another dimension, exploring the convergence of IoT and robotics as connected systems move from monitoring physical processes to actively intervening in them.

Digital twins move from reflection to reasoning

Digital twins are evolving rapidly - from operational models into active decision-support systems capable of simulation, prediction and autonomous action. Dan Isaacs, the chief technology officer of the Digital Twin Consortium, and Sri Kodali of NVIDIA are both contributing to this track, reflecting the degree to which advances in AI and compute are reshaping what twins can do.

One of the most practically valuable sessions of the event takes place in the on-site Learning ▶

Hub on Day 1 (18 May, 09:30–10:30). Isaacs joins Pieter Van Schalkwyk, the chief executive and founder of XMPro, for a hands-on workshop: *Developing Digital Twins with Generative AI*. The session bridges two established frameworks - the Digital Twin Capabilities Periodic Table (DT CPT) and the AI Agent Capabilities Periodic Table (AIA CPT) - to show how Intelligent digital twins can be built that don't simply mirror assets, but reason, predict and take autonomous actions using generative AI. Attendees will learn how to apply both frameworks to guide their own technology selection. For anyone currently evaluating or expanding a digital twin strategy, this is a directly actionable session.

Later that afternoon, the Digital Twin Consortium hosts an Internet of Things Community Meetup (14:00–14:40, Day 1) - a structured opportunity for practitioners to continue those conversations with peers facing the same implementation challenges. Connectivity evolves from access to orchestration Connectivity is being reframed. Where it was once treated as a provisioning question, it is now a management discipline. As enterprises combine terrestrial, private 5G and satellite networks across multiple geographies and regulatory environments, the challenge is orchestration - keeping a heterogeneous, dynamic connectivity layer working reliably at scale.

Olof Liberg of Ericsson outlines the path from current 5G deployments to 5G Advanced and beyond. Martin Whitlock of Telenor IoT, a top sponsor of the event, addresses the immediate operational complexity of managing multi-network environments - a challenge that is becoming more pressing as IoT deployments grow in scope and geographic spread.

Security is an ongoing discipline, not a fixed state

Security runs through every track at the event - but the framing has changed. Perimeter defence is giving way to continuous risk management across the full device and system lifecycle. Sessions from Dr. Chase Cunningham and Maximilian Kleemann of ONEKEY address firmware security, zero-trust architectures and automated compliance, with the Cyber Resilience Act providing an increasingly urgent regulatory backdrop.

The message is consistent: organisations still approaching IoT security as a compliance exercise are accumulating risk that compounds with every new deployment.

Embedded intelligence and autonomous systems

At the device level, Paul Smith of Airbus and Vivek Jain of Bosch explore the challenge of running machine learning models on constrained hardware - where power, memory and reliability are hard constraints rather than optimisation

targets. Emnify, also a top sponsor, addresses the operational side: how devices are configured, updated and managed after deployment, as the industry moves towards software-defined devices that continue to evolve in the field.

At the furthest edge of the programme, NVIDIA, Airbus and Boston Dynamics explore physical AI and autonomous systems - IoT at the point where it begins to act rather than report. The integration of perception, decision-making and physical control into cohesive autonomous systems is not yet mainstream, but it is clearly the direction the most advanced deployments are heading. The infrastructure decisions being made today will determine whether organisations are positioned to absorb that shift or caught flat-footed by it.

Organisations still approaching IoT security as a compliance exercise are accumulating risk that compounds with every new deployment

The ecosystem in San Jose

The sponsor and exhibitor line-up reflects where IoT investment is currently concentrated. Top sponsors include IBM, Akamai, Telenor IoT, Lenovo, LG CNS, Rhino Federated Computing, Pelion and emnify. On the exhibition floor, Toyota Tsusho Systems, SAP, SUSE, OpenText, AtomBeam and SpectroCloud are among those represented - spanning connectivity, edge infrastructure, device management and enterprise integration.

For IoT Now readers tracking vendor strategy alongside technology trends, the combination of conference programme and exhibition floor offers a practical calibration of where the market is genuinely investing.

The questions defining IoT's next phase

What this programme ultimately reflects is an industry that has internalised the hard lessons of early deployment and is now asking more precise questions. How do you design for scale from day one? How do you maintain control across distributed environments? How do you ensure security without compromising performance - and deliver measurable operational outcomes rather than proof-of-concept results?

These are the conversations happening at San Jose McEnery Convention Center on 18-19 May 2026. The event offers both free and paid pass options, making it accessible whether you are attending for a focused afternoon of sessions or committing to the full two-day programme. Full details, the complete agenda and registration are at **https://www.iottechexpo.com/northamerica/**. ■

Max your hardware opportunities at pioneering show

Hardware Pioneers Max 2026 will be held at Excel London on 10-11 June 2026, bringing together 6,000 engineers and technology leaders with more than 250 exhibitors from across the global electronics industry

This year marks a major milestone for the event. Hardware Pioneers Max has doubled in size compared with the previous edition and has now become the largest event of its kind in the UK and Northern Europe. The move to Excel London reflects the rapid growth of the community around the show and positions the event in the most prestigious venue in the country.

The exhibition floor will feature companies from every corner of the electronics ecosystem and from all parts of the world, including China, Australia, Germany, Spain, Sweden and Poland. Major exhibitors include Microchip, Infineon, Raspberry Pi, Innodisk, Murata, ST, Renesas and many more companies showcasing the technologies shaping the next generation of electronic products.

Alongside the exhibition, the conference agenda will host leading voices from across the industry. Speakers from organisations such as Jaguar Land Rover, Leonardo Helicopters, NXP, Microchip, Nordic Semiconductor and Synaptics will share insights on topics like edge AI, embedded vision, power management, field-programmable gate array (FPGA) technology, and much more.

IoT Now readers can register for the event at **hardwarepioneers.com** and use the dedicated VIP discount code **INVIP20** to receive 20% off VIP tickets.

What did Mobile World Congress and Embedded World tells us about the state of IoT connectivity?

The twin industry gatherings of Mobile World Congress and Embedded World in consecutive weeks in March offered a revealing snapshot of the evolving IoT connectivity market. Unlike previous years, when a single technology narrative dominated the discussion, the overarching message in 2026 was one of gradual evolution and maturity. The industry continues to discuss artificial intelligence, but the real developments lie in infrastructure, positioning and market maturity rather than breakthrough technologies. In this article, Matt Hatton, the founding partner at Transforma Insights shares some of the key trends he noted during the two events.

Every year the technology industry arrives at its major trade shows expecting to discover the next defining narrative. For the mobile and IoT ecosystem, those narratives have historically arrived in rapid succession: low-power wide-area networks, 5G, satellite connectivity, eSIM, edge computing and now artificial intelligence.

Yet one of the most striking takeaways from Mobile World Congress 2026 in Barcelona and Embedded World 2026 in Nuremberg is that no such breakthrough technology narrative really emerged. There were many conversations about all of the relevant technologies, but each was really about incremental change rather than something that would trigger any kind of substantial shift.

That absence, however, may actually be the most important signal about where the IoT connectivity market now stands. Rather than chasing the next headline technology, the sector increasingly appears to be settling into a phase of maturity. Conversations across both events suggested that the industry's priorities are shifting away from hype cycles and toward infrastructure, operational resilience and long-term deployment realities.

AI is everywhere, but not yet transformative

Artificial intelligence unsurprisingly dominated messaging across both shows. Few stands lacked references to AI, and vendors across the connectivity, platform and device ecosystems were keen to position themselves within the broader AI narrative. Yet behind the branding, the practical impact of AI on cellular IoT remains somewhat elusive.

Many discussions revolved around the idea that IoT devices generate the real-world data required to fuel AI models. Some industry players have begun referring to this relationship as 'physical AI', emphasising the role of connected devices in linking digital intelligence to the physical world. The concept has some merit. Real-time video analytics, predictive maintenance and intelligent fleet optimisation are all examples of applications where AI and connected devices intersect. Indeed, Transforma Insights has examined one aspect of this in the work we have done on AIoT.

The real story: infrastructure

Instead, a more substantive shift appears to be occurring in the underlying infrastructure that supports IoT deployments, and the growing demands of AI.

As connected devices generate increasing volumes of data and support more latency-sensitive applications, the traditional model of routing traffic through centralised network hubs is becoming less viable. Enterprises increasingly require data processing closer to the device, both for performance reasons and to address regulatory requirements around data localisation. I explored many of these topics in a recent blog post 'What does greater 'localisation' mean for IoT delivery?'

This trend is accelerating interest in distributed network architectures built around local packet gateways, local breakout capabilities and edge processing environments. A recent Transforma Insights report 'Evolving approaches to traffic management for international roaming' (February, 2026) focused on several aspects of this trend. For connectivity providers, this shift has significant implications. The role of the IoT connectivity provider is gradually evolving from that of a SIM and data plan supplier toward something closer to a global infrastructure operator.

In other words, connectivity providers are beginning to look less like telecom operators and more like infrastructure platforms. The best analogy is perhaps to that of the content delivery network. Just as CDNs distribute content closer to users to improve performance, distributed IoT connectivity infrastructure allows device data to be processed closer to where it is generated. That shift may ultimately reshape how the industry thinks about connectivity itself. Rather than being the core product, connectivity becomes one component within a broader managed infrastructure service.

A market finding its differentiation

Another theme evident across meetings and discussions at both events was the growing importance of differentiation. For much of the last decade, the IoT connectivity market has been characterised by intense competition around basic ▶

Artificial intelligence unsurprisingly dominated messaging across both shows

Mobile network operators, in particular, are attempting to utilise their broader enterprise relationships and infrastructure assets

connectivity pricing and global coverage claims. But as deployments scale and enterprises demand greater reliability, the basis of competition is changing.

Connectivity providers are increasingly emphasising their unique capabilities. For some, that means global infrastructure and distributed network architectures, as discussed above. For others, it involves vertical industry expertise or deeper integration with enterprise systems.

Mobile network operators, in particular, are attempting to utilise their broader enterprise relationships and infrastructure assets. By bundling connectivity with managed gateways, analytics platforms and vertical solutions, they are trying to move up the value chain beyond basic connectivity provision. Meanwhile, newer players in the IoT connectivity ecosystem continue to differentiate through specialised capabilities, whether in global connectivity orchestration, resilience features or advanced device management tools.

The result is an increasingly diverse ecosystem in which the underlying connectivity provision, in terms of SIM cards and data plans, is a subsidiary consideration.

Resilience becomes a central requirement

Another potential differentiator for IoT connectivity is resilience. With enterprises relying on connectivity for critical processes, and the connectivity market itself showing evidence of maturing, there is increasing focus on security and resilience as enhanced value-added features. We note continued growing interest in features such as multi-network access, advanced fallback mechanisms and network observability tools.

Regulation, particularly CRA, should be front of mind

While infrastructure and resilience dominated many discussions, another issue is quietly moving up the industry agenda: regulation. The European Union's Cyber Resilience Act will introduce extensive cybersecurity requirements for connected products. The regulation places significant obligations on manufacturers to ensure their products are secure by design, free of known vulnerabilities and supported by appropriate incident reporting and remediation processes. The first compliance deadlines are approaching within the next year, yet awareness of the regulation still appears inconsistent across parts of the IoT ecosystem. For those not familiar, more details can be found in the CRA entry in the Transforma Insights Regulatory Database.

Interestingly, the topic seemed to receive much more attention at Embedded World than at Mobile World Congress. That may reflect the more hardware-focused nature of the embedded systems community, where device security considerations are often more visible. However, the regulation applies broadly across the connected product ecosystem. Companies involved in device manufacturing, connectivity services and platform development will all need to consider how their offerings align with the new requirements. In that sense, regulatory readiness may become one of the defining challenges for the IoT industry over the next several years.

The end of the hype cycle?

Taken together, the signals from Mobile World Congress and Embedded World suggest that IoT connectivity may be moving beyond its most hype-driven phase. That does not mean innovation has stopped. Technologies such as 5G standalone networks, satellite connectivity and advanced eSIM standards continue to evolve and will undoubtedly play important roles in future deployments. But the industry conversation appears to be shifting. Rather than searching for the next buzzword, companies are increasingly focused on building the infrastructure, security frameworks and operational capabilities required to support large-scale, long-term IoT deployments. For an industry that has spent much of the last decade promoting future possibilities, that shift toward practical implementation may be the most significant development of all. ■

www.transformainsights.com

Our pick of the IoT industry's upcoming events

Intelligent Manufacturing
Kuala Lumpur
13-15 May 2026
Kuala Lumpur, Malaysia
https://iot-now.com/event/intelligent-manufacturing-kuala-lumpur-imkl-2026/

Edge Computing Expo North America
18-19 May 2026
San Jose McEnery Convention Centre, California, USA
https://edgecomputing-expo.com/northamerica/

Intelligent Automation North America
18-19 May 2026
San Jose McEnery Convention Centre, California, USA
https://intelligentautomation-conference.com/northamerica/

AI Everything x GITEX Kenya
19-21 May 2026
Nairobi, Kenya
https://www.aieverythingkenya.com/

MVNOs World
1-3 June 2026
Amsterdam, Netherlands
https://tmt.knect365.com/mvnos-world/

London Tech Week
8-12 June 2026
Olympia, London, UK
https://www.iot-now.com/event/london-tech-week/

The Battery Show Europe
9-11 June 2026
Messe Stuttgart, Germany
https://iot-now.com/event/the-battery-show-europe-2/

IoT Days Summer: Thick Edge Applications
10-11 June 2026
https://iotm2mcouncil.org/iot-library/event/imc-events/iot-days-summer-thick-edge-applications/

Hardware Pioneers Max 2026
10-11 June 2026
London, UK
https://iot-now.com/event/hardware-pioneers/

MWC Kigali
16-18 June 2026
Kigali, Rwanda
https://www.mwckigali.com/

Critical Communications World
16-18 June 2026
London, UK
https://www.critical-communications-world.com/

DTW Ignite
23-25 June 2026
Bella Center, Copenhagen, Denmark
https://iot-now.com/event/dtw-ignite-2026/

MWC Shanghai
24-25 June 2026
SNIEC, Shanghai, China
https://www.mwcshanghai.com/

GITEX Europe
30 June - 1 July 2026
Berlin, Germany
https://iot-now.com/event/gitex-ai-europe/

One control plane: enterprises stay in control

Make SGP.32 eSIM simplicity a reality at mass scale, with unified orchestration and security

If your IoT is scaling, are you scaling control?

If «orchestration» feels like a black box, do you still own your policies?

If mission-critical devices can't fail, can your connectivity adapt in real-time?

It's not just about the financial upside of IoT operations.
It's also about the vulnerability exposed when visibility and control are fragmented.

To learn more → **Read the Interview**
More on Simetric and Thales partnership
More on Thales solutions






THALES
Building a future we can all trust

simetric.