Research Note

Author: Mohit Agrawal

March 26, 2026

# Simetric's Enterprise-first Approach is Unifying IoT Connectivity's Fragmented Ecosystem

## Introduction

The dream of seamless global IoT has always hit the same wall which is a fragmented mess of operators, platforms, and rigid tech. Enterprises have essentially been forced to play by the rules of mobile operators and vendors who built the stack for network control instead of focusing on the companies actually trying to deploy devices at scale. This "operator-first" legacy approach has created a nightmare for companies trying to scale. They are stuck with "black box" deployments, rigid contracts, and no real way to switch networks when performance dips or costs spike.

Simetric is tackling this head-on by flipping the script. Instead of adding more noise to the ecosystem, they are building a horizontal orchestration layer to hide the underlying complexity. They are not trying to replace the operators or the platform providers. Instead, they are positioning themselves as a neutral control plane. This gives enterprises a single interface to manage multiple vendors and networks, bringing the benefits of software-defined infrastructure to the IoT world.

This strategy is clearly gaining traction across the entire value chain. Major carriers like **AT&T** and **Vodafone** are already working with Simetric to offer their customers more flexibility. At the same time, hardware and solution leaders like **Digi International** and **Itron** are using the platform to gain the operational oversight they have been missing.

Simetric's deeper technical ties with **Kigen** and **Thales** are also vital. These partnerships bridge the security and provisioning gaps that still plague the **SGP.32** ecosystem. By remaining vendor-neutral at the device level, Simetric ensures that enterprises are not just trading one form of lock-in for another.

This note breaks down why this enterprise-first shift is a way forward for a fragmented market. We will explore how Simetric's architecture solves these historical pain points and why so many industry heavyweights are finally aligning around a unified vision for connectivity.

## Need for Enterprise-first Approach for CMP

The CMP works well when all the devices are connected to the same carrier in the same geography. However, for a global implementation managing connectivity across carriers presents the following challenges for enterprise customers:

1. **The Multiple Portal Problem:** Large enterprises rarely use just one carrier. They might use AT&T in the US, Vodafone in Europe, and a local provider in Brazil. Enterprise teams have to log into 5-10 different CMPs from Cisco Control Center to Vodafone GDSP or Telefonica's Kite platform to check data usage or troubleshoot a device.
2. **Data and Reporting Inconsistency:** Every carrier formats their data differently. One might report usage in kilobytes every hour while another in megabytes every day. This makes it difficult to get accurate global view of costs or performance because the "math" does not match.
3. **Bill Shock from Unmanaged Usage:** In a fragmented environment, it is hard to see which devices are over-consuming data until the bill arrives at the end of the month. Manual rate-plan changes across hundreds and thousands of devices are impossible, leading to massive overage fees.
4. **Hardware and SIM Variety (eSIM/iSIM/Physical):** Companies often have a mix of old physical SIM cards and new eSIMs or iSIMs from different manufacturers (Thales, Kigen, and more). Managing the SIM lifecycle (activating, switching profiles, or decommissioning) of these different hardware types usually requires different technical stacks.
5. **The IT vs OT Gap:** Network teams (OT) usually see the carrier data, while Help Desk teams (IT) use tools like ServiceNow. When a device fails, the Help Desk has no visibility into the cellular network status, leading to long "finger-pointing" delays.

Counterpoint Research has been tracking the Connectivity Management Platforms (CMP) for Internet of Things (IoT) connectivity. Unsurprisingly, in our recent survey of connectivity management platforms, ***Single Pane of Glass (SPoG)*** emerged as top requirement from the enterprise customers, even ahead of AI tools.

A traditional CMP like Cisco Control Center was built for Carriers to manage their own subscribers. An enterprise-first approach is necessary because modern companies no longer buy connectivity from just one source and their need for analytics is different from that for carriers. Additionally, in the future, enterprises would need an aggregated and normalized platform in the agentic AI era to make the connectivity management autonomous. As a result, the enterprise-first approach is no longer optional even for connectivity providers.

Many CMP providers have part of SPoG capabilities or have the feature on their roadmaps for 2026 as connectivity providers and enterprises ask for it but the level of integration other CMPs varies leading to a sub-optimal fragmented experience.

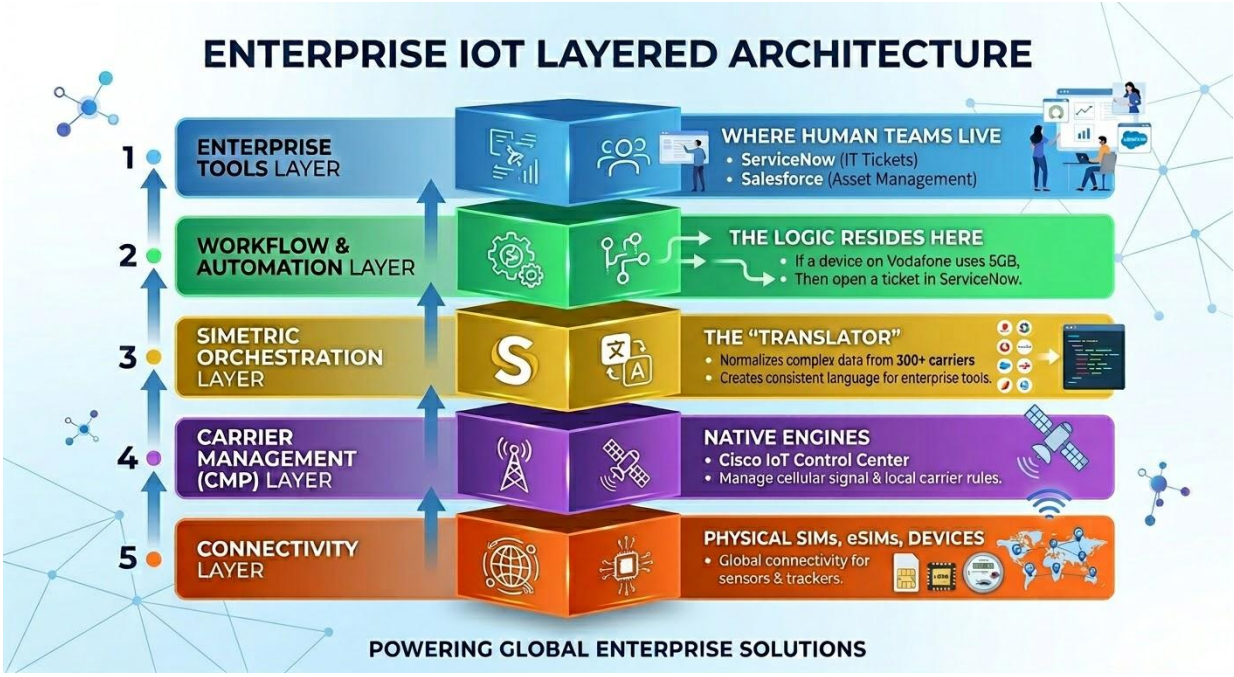
## How are the Connectivity Providers Reacting to Enterprise Needs?

While the connectivity providers have been waiting for the traditional CMPs to come up with ways to fulfil enterprise needs, a new trend has emerged where the IoT connectivity providers are looking to add a new layer on top of the CMP.  It helps not only to integrate multiple CMPs but also ease the workflow with enterprise tools.

This aggregation layer is provided by players like Simetric and IOTM. These companies focus on a single pane of glass, ensuring consistent analytics and managing workflows. Simetric, in particular, has been aggressive in forging partnerships with IoT connectivity and service providers such as AT&T, Vodafone, Digi, Itron, Soracom and Tata Communications. Additionally, it has also partnered with Kigen and Thales to integrate eSIM provisioning and orchestration on its platform. The partnerships are helping Simetric create an ecosystem around IoT connectivity that focuses on enterprises rather than connectivity providers. This enterprise-first approach helps focus on the unmet enterprise and operational requirements missed by M(V)NOs, networking OEMs, and device manufacturers.

## What Exactly is a Simetric Orchestration Layer?

Simetric is an orchestration and management platform designed to simplify the complexity of large-scale IoT deployments. Acting as a ***single* pane of glass**, it unifies data from 40+ CMPs and 300+ global carriers into one streamlined interface. By normalizing fragmented data and automating workflows, Simetric allows businesses to manage thousands of devices, optimize data costs in real-time, and detect security anomalies without having to juggle multiple carrier portals. Essentially, it serves as the central operating system that bridges the gap between raw cellular connectivity and enterprise IT tools like ServiceNow.




*Source: AI-generated image based on Counterpoint Research's information*

As seen in the diagram above, Simetric is an orchestration layer on top of the CMP layer but below the enterprise layer. Simetric platform is essentially two key offerings:

1. **CMP Aggregation:** Simetric's SPoG unifies multiple CMPs into one interface allowing businesses to manage SIM and eSIM lifecycles across different providers without switching between various portals. Simetric focuses more on ***abstraction*** and ***normalization***. It excels at taking data from hundreds of different CMPs and ***normalizing*** it so a business sees consistent reports and triggers regardless of the source network.
2. **Workflow Management:** Simetric has deep integration with IT service tools such as ServiceNow. As a result, Simetric is often chosen for its Business Process Automation (BPA). It includes deep ***if-this-then-that*** workflows designed to optimize costs by automatically switching rate plans based on real-time usage data across different carriers. Its BPA enables more stringent SLA establishment and satisfies a common request for greater device productivity.

One of the outcomes of abstraction and normalization is the ability to ***support agentic AI***. In the future, since Simetric is an abstraction layer, it can allow the AI agents to interact with the physical cellular networks. Simetric provides a unified API layer across 300+ carriers and AI agents can use Simetric to execute commands without needing custom code for every carrier. For an AI agent to make smart decisions, it needs high-fidelity data. As Simetric feeds the agent real-time telemetry, an agent can detect a sleepy device (one that is on but not sending data) and automatically trigger a reboot command via the Simetric workflow.

## How Does the Partnership With Kigen and Thales Fit?

eSIM are becoming increasingly important for IoT and the new eSIM standards for IoT, SGP.32 are providing fresh impetus to eSIM penetration by including the constraint devices under its ambit and providing real carrier mobility. However for successful SGP.32 implementation and life cycle orchestration, its integration with CMP is critical. eSIM IoT (SGP.32) requires three tightly coupled layers:

- eSIM OS/eIM
- Provisioning + security infrastructure
- Cross-carrier orchestration/workflow layer

Simetric offers the last layer which is orchestration and workflow. However, it needs to partner to provide the other two layers and this is where Kigen and Thales comes in with them filling the first and the second layers. By partnering with eSIM players, Simetric will be able to provide cross-carrier orchestration across physical SIMs and eSIMs.

It is important to note that there is significant overlaps between Kigen and Thales offerings and hence in most projects Simetric will either partner with Kigen or Thales.

## Is AT&T and Vodafone's Partnership with Simetric Pointing to Market Disruption or Evolution?

Simetric might be positioned as a disruptor to traditional CMPs, but this framing is incomplete. Simetric is not disrupting CMPs in the classic sense. It is abstracting them into a higher-order orchestration layer. Orchestration layer is fundamentally reshaping how connectivity is consumed and controlled by enterprises.

CMPs will still be responsible for handling provisioning, managing the SIM lifecycle, and more, and Simetric will depend on the CMPs for data and execution end points. At its core, Simetric is introducing a ***horizontal control plane*** that sits above operator-led CMPs, normalizing fragmented systems into a unified interface. This shifts CMPs from being enterprise-facing platforms to ***backend execution layers***, reducing their visibility while preserving their functional importance.

**Key implications:**

- **CMPs are becoming commoditized infrastructure**
  As enterprises increasingly interact through a unified orchestration layer, differentiation across individual CMPs diminishes. Platforms operated by players such as Cisco Control Center or Telefonica's Kite risk being reduced to standardized connectivity pipes and APIs.
- **Control is shifting from operators to enterprises**
  Simetric enables enterprises to define connectivity policies, automate network selection, and manage lifecycle operations across multiple operators. This

represents a structural shift in decision-making authority away from operator-controlled environments toward enterprise-driven architectures.

- **A new category is emerging – Connectivity Management Orchestration (CMO)**
  Simetric is among the early players defining a new layer that orchestrates multiple CMPs rather than replacing them. This layer becomes the ***system of control***, while CMPs remain systems of record and execution.
- **Operators are adapting, not resisting**
  Partnerships with operators and solution providers, including AT&T, Vodafone, and Digi International, signal recognition that future enterprise IoT deployments will be inherently multi-network and multi-platform. Participation in orchestration-led ecosystems is becoming critical to maintaining relevance.

Simetric is not eliminating CMPs but it is making them ***invisible to the enterprise***. In doing so, it is accelerating the evolution of the IoT connectivity stack toward a ***software-defined, enterprise-controlled model*** where value shifts from network ownership to orchestration and intelligence. Security is a very important focus now. The unified visibility Simetric is creating, for M(V)NOs and enterprises alike, is elevating the buying center of connectivity to CIOs and CISOs. This shift is driven under security and underpinned by a need for robust data access, measured device performance, unified ecosystems (SIM+eSIM) and real-time execution governance. The point is not a lesser focus on IoT connectivity, just the fact that the parameters of managing secure operations require greater control in total and at the device. The more robust the security governance, the greater the use of IoT is put into operational execution.