THE NETWORK WORKS.

UNTIL IT DOESN'T.

What utilities need to know about operational certainty on Carrier APNs

ONELAYER

When the Phones Start Ringing

Something drops during a storm and within minutes you're being asked questions you should be able to answer. Which devices are affected. Whether it's a network problem or something in the field. Whether your team has it under control.

Most of the time you don't have a clean answer. You have a partial picture assembled from carrier portals, router logs and whatever your field crews can tell you from memory. You're not blind. But you're not seeing the full picture and on the night it matters most, that's the part that will cost you.

Carrier APNs provide broad, reliable connectivity across substations, field assets and remote infrastructure. They can't tell you what's actually on that network, whether a failure is in the device or the network, or whether what's running today matches what was approved yesterday. That's operational certainty, and it's a different problem.

Connectivity and operational certainty are not the same.

What is Actually on My Network Now?

The carrier portal shows you SIMs. The firewall shows you IP addresses. Neither one shows you the devices sitting behind the router at Substation 7.

That knowledge lives in people, not systems. When those people are unavailable, or when the question comes in at 2am during a winter storm, there is no system to fall back on.

You don't know which devices are offline, how many are affected or how long it will take to fix it. You don’t even know exactly where the problem is.

Risk accumulates quietly in that gap. Every time a device gets swapped, a router replaced or a contractor provisions something and the spreadsheet doesn't get updated.

The Visibility Gap

The carrier portal shows the router. It doesn't show the RTU, the PLC or the sensor sitting behind it. Those devices are on your network, consuming connectivity and generating traffic. They're invisible to every system you have.

The Gap Carrier APNs Leave Behind

What you can see	What you can't
Network is up Signal confirmed, SIMs active	**What is actually connected** Every device, not just every SIM
Traffic Outage! Carrier portal shows there is an issue	**What failed, and where** Device vs. network, in real time
Router is reachable Gateway pings, dashboard is green	**What changed overnight** New, moved or unauthorized devices
APN is provisioned Configured at deployment	**What the auditor will ask** Answered before the review begins
What the carrier delivers By design. Works as intended.	**What the operator needs** Not built in. Must be added.

Carrier APNs solve connectivity. They do not provide operational certainty.

ONELAYER

Is this a Device or Network Problem?

The difference between a failed device at a substation and a degraded carrier signal covering that same area looks identical from the operations center until someone dives into the details.

But it's slow manual work because your systems are not connected. You pull the carrier portal. You check the router. You look at the internal monitoring for that part of the network. Each system speaks its own language and holds a different piece of the puzzle. None of them were designed to talk to each other. You need to solve this under pressure when the people with the most context are hardest to reach.

Every minute spent correlating disparate systems is another minute of downtime. Inevitably, a truck is dispatched because putting someone on site is the fastest way to find a definitive answer.

> *"If we don't have to roll a truck because we've identified the problem, absolutely the ratepayers benefit from that."*
>
> *-Steve Liegl*
> *Director, WEC Energy Group*

This is the diagnostic gap. The information needed to resolve the problem remotely exists somewhere across those systems. An active outage just doesn't wait for you to find it.

The Typhoon Attacks by the Numbers.

Two Chinese state-sponsored campaigns targeted US critical infrastructure and telecom networks. Different operations. Same playbook: find what nobody is watching.

VOLT

200

US critical infrastructure entities breached, per FBI briefing to Littleton Electric

VOLT

4

Critical sectors targeted: energy, water & wastewater, transport, comms

VOLT

5 years

Maximum confirmed undetected dwell time inside US critical infrastructure

VOLT

?

Compromised US critical infrastructure sites we will **never** find

SALT

1M+

Users metadata accessed from telecom networks

SALT

9

Major US carriers breached

SALT

$10M

FBI bounty posted for Salt Typhoon operatives

ONELAYER

Are We Exposed?

This is the question that makes most security teams pause when asked directly. The honest answer, for most utilities running Carrier APNs, is that they don’t really know.

Carrier APNs are widely regarded as secure by design. Traffic is logically separated from public internet traffic and access requires a SIM provisioned by the carrier.

SIM ≠ Device

Cellular networks identify devices by SIM, not hardware. A SIM can be moved, swapped or cloned. The device your policy covers and the device on your network aren't always the same.

IP ≠ Identity

Firewalls enforce policy on IP addresses. On a cellular network with NAT, those addresses shift and don't reliably map to devices. The policy looks intact. The assumption underneath it isn't.

Then ≠ Now

Most utilities have never fully audited their Carrier APN. Devices get swapped, routers replaced, contractors cycle in and out. Each change leaves a small gap and those gaps accumulate.

Your security tools see a SIM. Not a device.

From Connectivity to Operational Certainty

None of the problems in this ebook are new. Utilities have been managing them with spreadsheets, tribal knowledge and truck rolls for years. They worked when the network was smaller and change was slower. Neither is true anymore.

The structural reason is straightforward. Carrier APNs were designed to manage subscribers and deliver connectivity. That is what they do well. Giving operations and security teams device-level context was never part of the brief.

Closing that gap means treating the network as something to be continuously verified, not checked periodically. Most utilities are still doing neither.

> *Carrier APNs were designed to manage subscribers and deliver connectivity. That is what they do well. Giving operations and security teams device-level context was never part of the brief.*

Meet OneLayer

Carrier APNs were built to deliver connectivity, not device-level context needed to run a grid. OneLayer closes that gap.

ONELAYER

Isolate Issues Faster

Know whether a failure is in the field device or the network before you dispatch a truck.

Trust your Security Posture

Know what's connected and if it's supposed to be there. Enforce policy based on device identity.

See what's on your Network

A single pane of glass showing every device on your network from RTUs to PLCs and everything behind your field routers.

PROUD MEMBER OF

UBBA Utility Broadband Alliance

Utilities Technology Council™

450 alliance

Electricity Canada Our energy future

Électricité Canada Notre avenir énergétique