ONELAYER

You Run Thousands of Devices Across Carrier APNs. You Deserve to See Every One of Them.

Your carrier APN estate has grown for decades: devices deployed by teams that have since turned over, SIMs scattered across disconnected portals, and no reliable link between what's on the network and what's in your records. That gap is where operational and security risk lives. OneLayer closes it.

WHAT'S STANDING IN YOUR WAY

You Can't See What's on Your Network

- Your SIMs live in disconnected carrier portals, with no unified view across carriers and APNs
- You have no reliable link between a SIM, the device it powers, and where it sits in the field
- Devices behind cellular routers are invisible to your carriers, and to you

Every Deployment Gets Slower

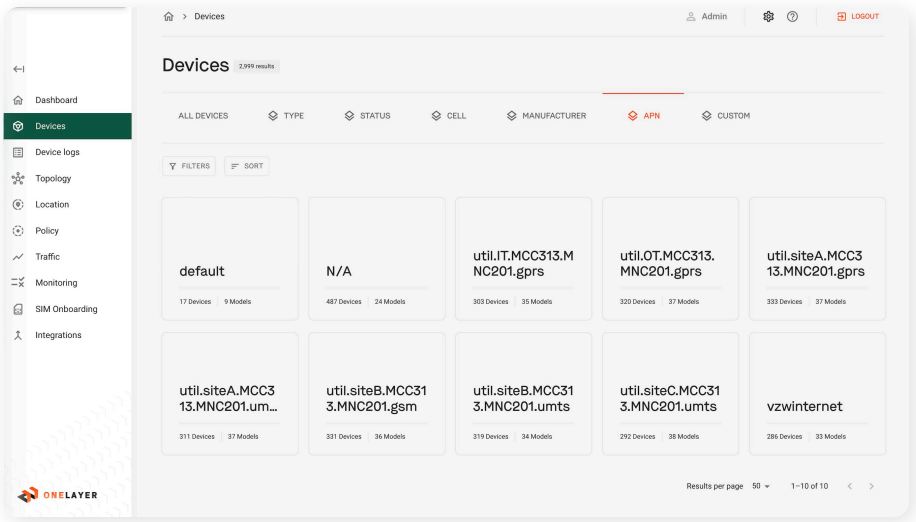
- Portal access is restricted to a handful of people. Your team hits a bottleneck every time you scale
- Onboarding is a manual maze: approvals, package tiers, IP allocation, security policy binding
- Decommissioned devices leave SIMs running in the background, and you have no way to know

Your Security Stops at the SIM

- Carrier APNs authenticate the SIM, not the device. Any hardware with a valid SIM gets full access to your APN
- The carrier network is part of your attack surface, not a trusted boundary
- Your firewalls, NAC, and SIEM operate independently, with no shared device identity to enforce policy consistently

The Cost of Waiting

- Carrier network changes are forcing large-scale device updates, and your current tools weren't built for it
- IT/OT convergence and Zero Trust mandates demand control you don't have today
- Device growth is outpacing your team's ability to manage SIMs manually
- Your carrier APN estate won't disappear overnight. Hybrid environments will persist for years



Single Pane of Glass Across Carrier APNs

"What used to take 15 steps now takes just 1 or 2 before we can act."

- Steve Liegl, Director of Infrastructure and Operations at WEC Energy Group

Here's How You Get There

ONELAYER

1 Single Pane of Glass Across Every Carrier, APN, and Device

Stop reconciling carrier portals. OneLayer gives you one inventory: every device, every APN, every carrier, accurate and current from day one.

- Pulls SIM and device data via carrier API; actively queries your routers and gateways to surface devices your carrier can't see
- Where a SPAN is deployed, OneLayer analyzes decrypted traffic flows to detect anomalous communications and identify tethering activity across the network
- Continuously validates every device is on its intended APN, and alerts you immediately when it isn't
- The network on paper finally reflects the network in the field

2 Automated Device Onboarding and Lifecycle Management

Your team shouldn't need carrier portal access to deploy a device. OneLayer builds a full device fingerprint and automates the workflow, from package tier to security policy.

- Starts with what your carrier already knows (SIM identity, IMEI, APN, subscription tier), pulled automatically via carrier API
- Adds the context your carrier never has: device make/model, firmware version, GPS location, downstream devices behind routers
- Executes against predefined onboarding templates; syncs device context directly into your CMDB and ITSM platforms
- Tracks every device from activation through decommission, flagging SIMs that have gone dark or never reached a device

3 Device Identity and Zero Trust Enforcement Across the Cellular Layer

A valid SIM pulled from a protection relay and inserted into a laptop gives that laptop full access to your APN. OneLayer closes that gap with persistent device identity at the cellular layer, independent of the SIM.

- Every device is fingerprinted, assigned a role-based profile, and continuously validated against that baseline
- Hardware changes (SIM swaps, unauthorized substitutions) are detected and isolated automatically, reducing your dwell time
- Zero Trust Network Access ensures only approved devices connect; context-based segmentation controls what each device can reach
- When a vulnerability is identified in a specific modem or device type, every affected device is found and access restricted in hours, not weeks

Start Every Monday Knowing Exactly What's on Your Network

Book a discovery session. We'll map your carrier APN environment: inventory, onboarding gaps, and security blind spots, in a single view.

Book a Discovery Session