

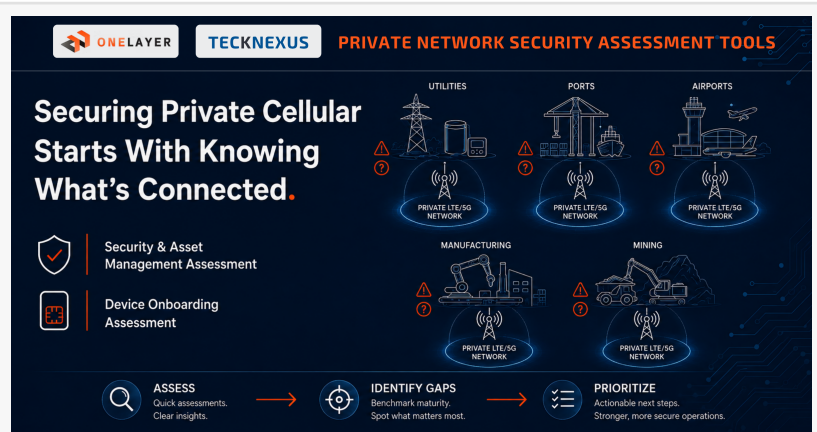
TeckNexus and OneLayer Launch Cellular Security Assessments Amid Emerging Private APN Threats to Critical Infrastructure

New interactive tools help critical infrastructure operators assess security, visibility & device-management maturity as threats target connected infrastructure

PHOENIX, AZ, UNITED STATES, August 27, 2026 /EINPresswire.com/ -- In a follow-up report published this month, CERT Polska disclosed that attackers had pivoted through a shared private APN to reach a Polish combined heat and power plant serving roughly 50,000 residents, executing an attack in December 2025 that forced critical PLCs to shut down. TeckNexus and [OneLayer](#) are giving critical infrastructure operators a way to check their own exposure before it becomes a headline.

TeckNexus, the vendor-neutral intelligence platform for private 5G/LTE networks and enterprise connectivity, today announced two new interactive assessment tools built in partnership with OneLayer, the leader in private LTE/5G OT management and Zero Trust security. Both tools are live now on the TeckNexus Intelligence Platform.

The launch comes as the security assumptions around cellular-connected infrastructure are being tested by real-world attacks. The August 8 disclosure covers the second of two CHP plant



TeckNexus and OneLayer launched two interactive assessment tools helping utilities, ports, airports, manufacturing, and mining operators benchmark private cellular security and device onboarding maturity.

The Device Onboarding Assessment benchmarks how efficiently organizations provision, track, and retire cellular-connected devices as fleets scale.

compromises Polish officials confirmed this year, both traced to attackers who used a shared APN as a lateral path from an unrelated wind farm into the power plant's OT environment.

As organizations connect more operational assets through private LTE/5G and carrier private APNs, security and operations teams need to understand what is connected, how devices communicate, whether unexpected lateral movement can be detected, and how quickly policy can be enforced when risk appears. Cellular connectivity is often adopted specifically because it scales faster than fiber or fixed wireless: devices can go live within days rather than months, with no trenching or site survey delays. But the visibility, governance, and provisioning processes behind that connectivity frequently haven't scaled at the same pace, leaving gaps that most organizations only discover during an audit, an incident, or the moment a device turns up that no one can account for.

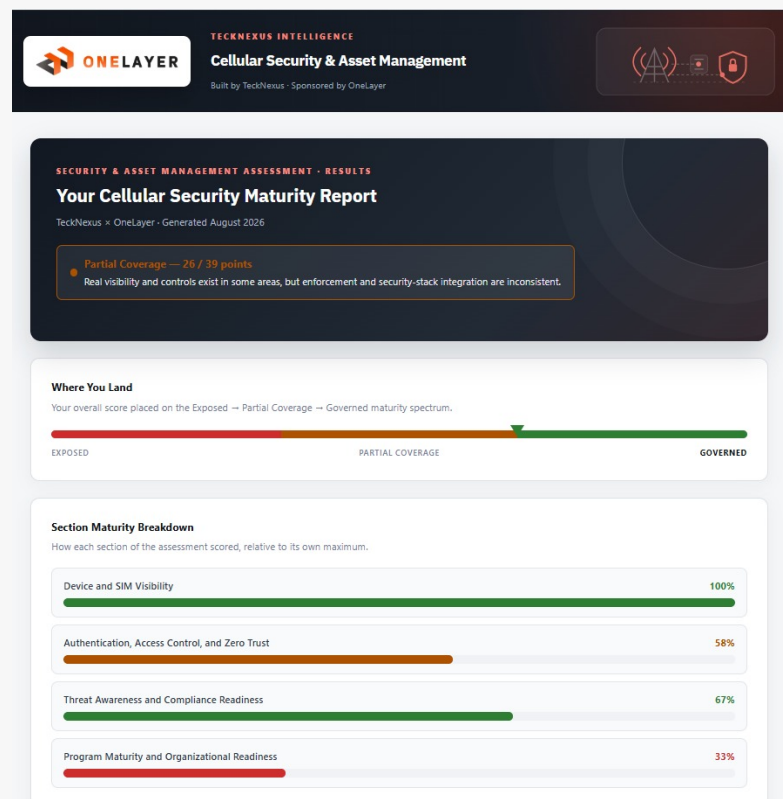
The two new tools give network, security, and operations leaders a structured way to benchmark exactly where those gaps sit, benchmarked against a scored maturity model built around the specific failure points OneLayer and TeckNexus see most often in the field, not a generic industry survey.

[DEVICE ONBOARDING ASSESSMENT](#): WHAT IT MEASURES

The Device Onboarding Assessment is a five-section, sixteen-question benchmark that takes five to seven minutes to complete and places an organization on a maturity spectrum from Reactive

The screenshot shows the landing page for the 'Cellular Security & Asset Management' assessment. At the top, it features the OneLayer logo and the TeckNexus Intelligence branding. The main heading is 'How Governed Are Your Cellular OT Devices, Really?'. Below this, a brief description states: 'A 5-section assessment for security leaders responsible for cellular-connected OT device risk. Answer questions about your current visibility and controls — we'll benchmark your maturity and flag your most urgent security gap. Select the option that most accurately describes your current state, not your aspirational state.' A table lists the assessment details: 5 sections - 17 questions, ~5-7 minutes, Personalized maturity report, and PDF summary included. A 'BEGIN ASSESSMENT' button is at the bottom right.

The Security and Asset Management Assessment benchmarks visibility, authentication, and compliance readiness for cellular-connected OT devices in under seven minutes.



The Device Onboarding Assessment benchmarks how efficiently organizations provision, track, and retire cellular-connected devices as fleets scale.

to Structured to Automated. Reported onboarding times across those tiers range from under 30 minutes where provisioning is automated to half a day or more where it runs through multiple manual handoffs. It covers:

- SIM and device provisioning today: how many teams and approvals are typically involved before a new device goes live, and how long onboarding actually takes from SIM activation to a fully configured device on the network.

- SIM lifecycle and inventory accuracy: whether every SIM an organization pays for is confirmed to be attached to an active device in the field. "Ghost SIMs," SIMs still active and billing but no longer tied to any operational device, are one of the most common and highest-risk gaps the assessment surfaces, typically originating from decommissioning processes that rely on a team remembering to notify rather than an automated deactivation workflow.

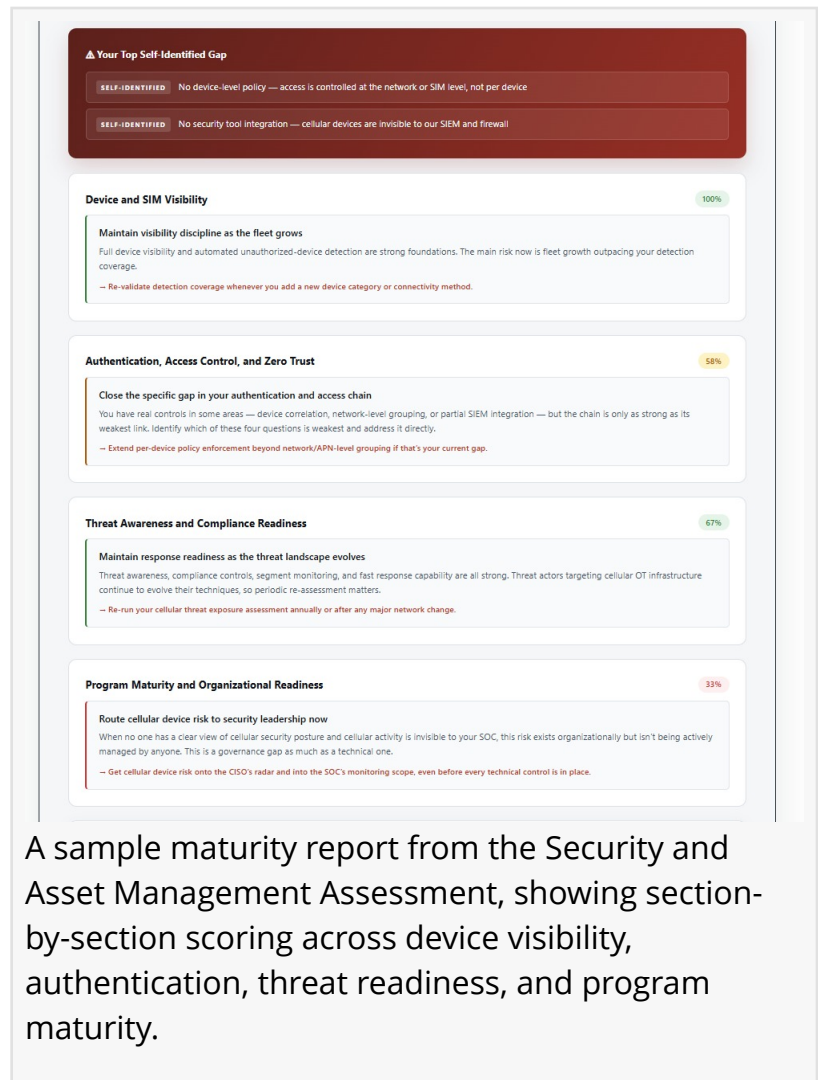
- Team burden and troubleshooting: how many people hold direct SIM provisioning access, and what happens when a device in the field stops communicating, from automated device-level alerts down to dispatching a field technician to investigate in person.

- Coverage and future readiness: whether the fleet operates across multiple carriers or network cores, whether SIMs support over-the-air profile migration without physical replacement, and how prepared the current onboarding process is to support a 25-50% increase in device deployments over the next 18 months.

Results include a maturity tier, a section-by-section breakdown, and a prioritized action plan showing which gaps to close first and which manual handoffs are stretching onboarding time.

[SECURITY AND ASSET MANAGEMENT ASSESSMENT](#): WHAT IT MEASURES

The Security and Asset Management Assessment is a five-section, seventeen-question



A sample maturity report from the Security and Asset Management Assessment, showing section-by-section scoring across device visibility, authentication, threat readiness, and program maturity.

benchmark, also five to seven minutes, that places an organization on a maturity spectrum from Exposed to Partial Coverage to Governed. It covers:

- Device and SIM visibility: whether an organization can identify the make, model, manufacturer, and firmware of every device on its cellular network, including devices sitting behind routers or gateways it didn't directly provision, and whether it can detect unauthorized devices connecting outside its standard procurement process.
- Authentication, access control, and Zero Trust: how devices are authenticated before being granted network access, whether SIM-to-device correlation is continuously validated (catching, for example, a SIM removed from an authorized device and placed into unauthorized hardware), and whether per-device access policy is enforced at the cellular layer rather than only at the broader IT/OT boundary.
- Threat awareness and compliance readiness: organizational familiarity with state-sponsored campaigns such as Salt Typhoon and Volt Typhoon, which have specifically targeted telecom and cellular infrastructure, and how cellular-connected devices are addressed under frameworks including NERC CIP, IEC 62443, and TSA cybersecurity directives, areas where cellular assets often sit just outside documented compliance scope.
- Program maturity and organizational readiness: which stakeholders currently have visibility into the cellular fleet's security posture, how integrated that posture is with SOC monitoring and incident response, and how quickly the organization could locate and restrict every device of a specific type or manufacturer if it were confirmed compromised.

Results include a maturity tier, section-level scoring, a flagged top gap, and a recommended action sequence.

Each assessment ends with the option of a no-cost architecture walkthrough with the OneLayer team, built around the individual results, along with a downloadable PDF summary.

"As private cellular deployments scale across utilities, airports, ports, and manufacturing, most organizations do not have a clear picture of their onboarding or security maturity until something breaks," said Hema Kadia, Founder and CEO of TeckNexus. "These tools give operators and security teams a benchmark they can act on, built from real deployment patterns rather than a generic survey."

"Cellular devices are proliferating across OT environments faster than most security and operations teams can govern them. The recent attack on Polish energy infrastructure shows why that visibility matters now, with attackers using a private APN as a path into critical OT. We built these assessments with TeckNexus so organizations get a quick, honest read on where they stand before they try to close the gap," said Dave Mor, CEO and Co-Founder of OneLayer.

WHY THIS MATTERS ACROSS VERTICALS

The assessments are built to apply across the industries where private cellular deployment is accelerating fastest. In utilities, cellular-connected grid control and monitoring devices, the same category of asset compromised in the Poland incident, often span both carrier APNs and private LTE, making unified visibility across both environments a recurring gap. In ports and airports, device fleets spanning cranes, containers, baggage systems, and ground equipment tend to grow through multiple procurement channels and vendors over time, which is precisely the pattern that produces untracked or unauthorized devices. In manufacturing and mining, remote and distributed sites frequently rely on cellular precisely because trenching fiber isn't practical, which means the provisioning and lifecycle gaps the Device Onboarding Assessment surfaces tend to compound fastest in exactly these environments.

Both assessments are available now on the TeckNexus Intelligence Platform (<https://tecknexus.com/intelligence/>). For more on the TeckNexus and OneLayer partnership, visit the OneLayer coverage hub (<https://tecknexus.com/keyword/onelayer/>) on TeckNexus.

Media and analysts interested in a briefing with TeckNexus and OneLayer can reach out via the contact below.

ABOUT TECKNEXUS

TeckNexus is a vendor-neutral B2B intelligence and media platform covering private 5G/LTE networks, AI infrastructure, and enterprise connectivity across manufacturing, mining, ports, airports, utilities, and other verticals. The platform combines proprietary deployment tracking, interactive intelligence tools, and editorial coverage for vendors, systems integrators, enterprises deploying private networks, and telecom network operators. For more information, visit <https://tecknexus.com/>

ABOUT ONELAYER

OneLayer, headquartered in Boston, Massachusetts, provides advanced asset management, operational intelligence, and Zero Trust security for private LTE/5G and private APN networks. Its technology empowers enterprises to manage and secure cellular-connected devices across both private and carrier environments, without the need for cellular expertise. For more information, visit <https://www.onelayer.com>

MEDIA CONTACT

Hema Kadia, Founder and CEO, TeckNexus
tecknexus.com

Hema Kadia
TeckNexus
[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[X](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/936812623>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.