Pelion

The Connected Fleet 2026

Market Trends and Buyer Insights from Enterprise IoT Leaders

An industry insights report from Pelion, in partnership with ABI Research, drawing on a 2026 survey of 675 cellular IoT decision-makers and ten in-depth interviews with enterprise IoT leaders.

Pelion

THE CONNECTED FLEET

Contents

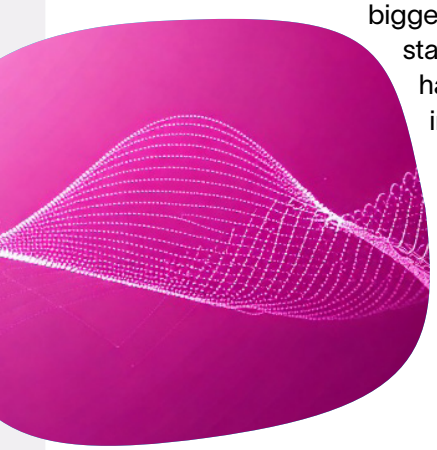
FOREWORD

Dave Weidner CEO, Pelion

Connectivity is the easy part of IoT, until it isn't.

That paradox sits at the centre of nearly every conversation Pelion has with people running large connected estates. The pattern is consistent: by the time the device has been built, the application is working, and the first thousand units are in the field, it becomes clear that the operating model wrapped around connectivity has not kept pace with the rest of the deployment. The fleet has crossed a border, scaled in volume, or simply aged into territory the original procurement decision was never designed for, and the assumptions that shaped that decision are quietly costing money.

We commissioned a survey, run with our research partner ABI Research, to test that observation against the wider market. We polled 675 cellular IoT decision-makers across the UK, US, Canada and Europe, covering energy, healthcare, logistics and transport, manufacturing, and smart buildings. The findings confirmed something we had already begun to see in our own customer base. The buyer's centre of gravity is shifting. International connections will nearly double inside five years, from 29% of fleets today to 49% by 2030. More than three-quarters of cellular IoT decision-makers not currently using an MVNO would consider one for their next deployment. Six in ten cite a shortage of expertise, internal or external, as the single biggest reason their projects stall. One in four respondents had an IoT-related security incident in the past twelve months.



This isn't a story about cellular getting faster or cheaper. It's a story about the rising demands of operating IoT at scale.

Three forces are reshaping the choices our customers face. The first is eSIM. The eUICC capability that defines eSIM, the ability to hold and switch between multiple operator profiles over the air, is now available across the full range of SIM form factors, from the familiar removable SIM card to embedded MFF2 chips and integrated iSIM. The SGP.32 standard, the first eSIM specification designed for IoT rather than adapted from consumer mobile, lands later this year. Together they let MVNOs offer enterprises the breadth of carrier choice that fixed-SIM models never could. The second is the maturing role of satellite. It is no longer an exotic line item. For remote sites, gas pipelines and energy assets where cellular thins out, LEO and GEO services are now priced close enough to cellular that the trade-off is real and being made. The third is the steady pull of complexity towards a managed model. As estates grow past their second or third generation of devices, the gap between *we own a cellular contract* and *we run a global IoT operation* becomes very expensive to close in-house.

Pelion

Pelion's view is straightforward. The future of enterprise IoT connectivity is borderless, eSIM-led, and managed. Not because those words sound modern, but because the buyer pain in this report points there. We are also seeing eUICC-enabled SIMs spill out of their traditional industrial home into use cases that were previously the preserve of single-carrier, fixed-profile devices: consumer-class wearables, retail terminals, and micromobility. The commercial benefits of being able to provision and reprovision a device's network identity without a truck roll are becoming harder to ignore.

What we hope you take from the rest of this document isn't a vendor pitch. It's an honest picture of where deployments are stalling, where security is biting, where money is leaking, and where the next two years of estate decisions are likely to be won or lost. We've added our perspective in two places, once here and once towards the end, and stayed out of the analyst's way in between.

Connectivity is the easy part of IoT, until it isn't, and the part that isn't is the work Pelion exists to do.

Pelion

1

49%

of cellular IoT connections will be international by 2030, up from 29% today

2

65%

cite *managing deployments outside core coverage area* as their biggest scaling pain

3

45.3%

share of profile downloads expected to be SGP.32-compliant **by 2030**, rising from 7.6%

4

62%

report unstable connectivity or capacity concerns

5

47%

struggle with using multiple Connectivity Management Platforms (CMPs)

6

60%

name lack of expertise, internal or external, as the top blocker of cellular IoT projects, ahead of budget and connectivity itself

7

77%

of respondents not currently using an MVNO would consider one for their next deployment

8

24.6%

experienced an IoT security incident in the past twelve months. 30% of those incidents cost more than $100K in lost revenue, and 8% more than $1M

9

64%

view data breach and privacy exposure as a significant security risk when scaling IoT; **57%** flag insufficient threat detection

10

80%+

of respondents in every vertical found at least one capability of their current connectivity provider not sufficient

Source: Outside the Core: The State of Enterprise IoT Connectivity 2026 survey, conducted by Pelion in partnership with ABI Research, fieldwork Q4 2025 to Q1 2026. Full sample of 675 respondents in the UK, US, Canada and Europe across energy, healthcare, logistics and transport, manufacturing, and smart buildings/smart city.

Pelion

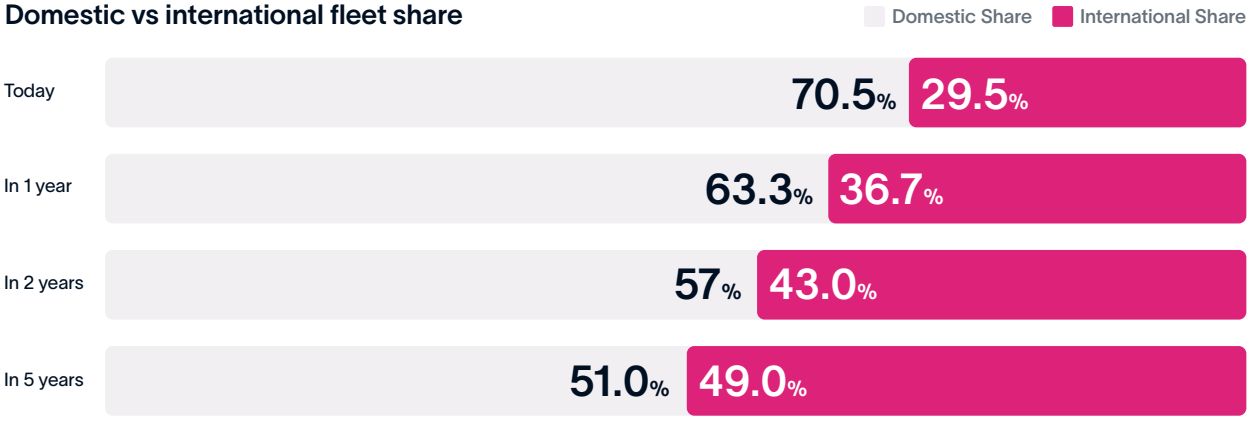
SECTION 01

The Estate Is Going International

Cellular IoT decision-makers expect their international footprint to nearly double inside five years. The full survey shows the average respondent's fleet split shifting from 70% domestic / 30% international today to roughly 51% / 49% by 2030. The trajectory accelerates: international share rises by seven points in the first year, by another six in the second, and continues to climb after that.

Two cuts of the data are worth pausing on. UK Energy respondents already report 35% international today and expect to reach 54% by 2030. For many of these firms, the centre of gravity will literally cross the channel within the planning horizon. US Manufacturing respondents expect to move from 31% international today to 48% by 2030. These are not edge cases. They reflect a steady, broad-based reorientation of where connected devices live.

Domestic vs international fleet share



Source: Q6, full survey base n=675. Averages of respondent self-reports.

The operational implications are not subtle. A connectivity model designed when 70% of devices were on home networks tends to assume one carrier relationship, one billing cycle, one CMP, one regulatory regime, and one set of support hours. Each of those assumptions becomes load-bearing in a way the original procurement decision never anticipated.

Roaming agreements that were a footnote at year zero become the dominant cost line by year five. Regulatory exposure that was domestic becomes multi-jurisdictional. The escalation path that worked for a single account team starts to fray when the device is in another country and the local SIM provider has different SLAs.

Pelion

Enbridge's IIoT lead walked through the trade-off explicitly when describing the company's most recent connectivity decision. The pipeline operator runs gas infrastructure across both the United States and Canada. The logical thing to do, given that two perfectly good Mobile Network Operators (MNOs) sit on either side of the border, would have been to sign one contract per country and run them in parallel. Instead, Enbridge chose a single global IoT SIM with private APNs, accepting some pricing concession from the rejected Canadian MNO in exchange for centralised SIM lifecycle management and one dashboard for both sides of the border. *"Can't get central SIM lifecycle management from an MNO in fragmented cellular network connectivity,"* the IIoT lead observed. The Canadian MNO had favourable pricing, but a patchwork of regional contracts wasn't a price worth paying.

Autoliv, the Swedish-headquartered automotive safety supplier, has lived through the same tension from the other end. Its Vice President & Head of IT for Autoliv Americas described renegotiating a managed network services contract because plant locations had changed and the original provider was contractually unable to switch the underlying carrier without unwinding a third-party agreement. With 15 plants across the US, Mexico, Canada and Brazil, Autoliv now runs most of its cellular IoT through a network managed services model on a single bill, with an MVNO underneath. The lower TCO Autoliv cites, around 20% versus direct vendor procurement, is real. But it is downstream of a more basic decision: at this fleet shape, multi-network is a coverage and operations question first, a price question second.

Key takeaway

The takeaway for IoT leaders planning their next two procurement cycles is uncomfortable but useful. The connectivity model that fits today's fleet probably will not fit the fleet you will run in 2030. The gap becomes harder to close the longer it is left.

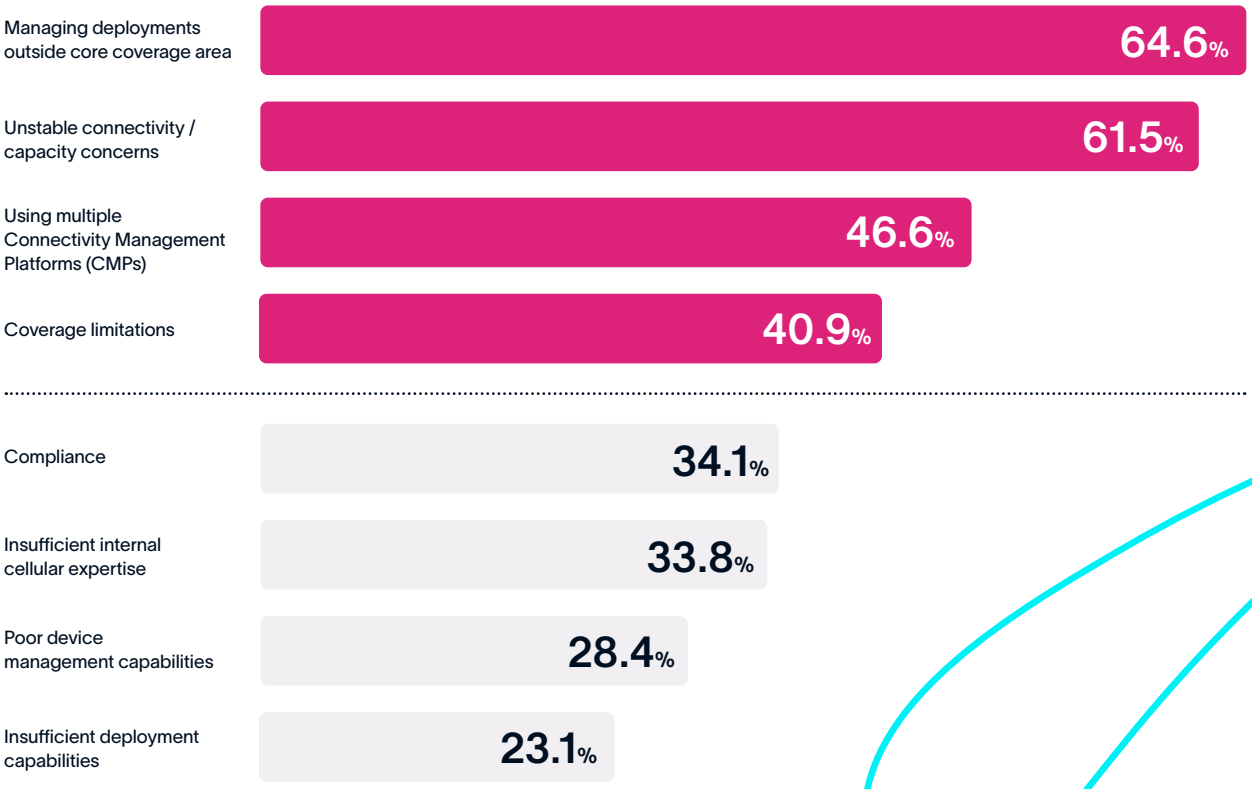
Pelion

SECTION 02

Coverage Is No Longer the Hard Part. Operating Outside the Core Is.

The single biggest scaling pain reported in the survey is not coverage as such, but the operational reality of managing deployments beyond the core coverage area. The distinction is sharper than it might first appear: coverage limitations register as a scaling problem for 41% of respondents, *while managing deployments outside the core coverage area* registers for 65%. That 24-point gap is the story.

Problems encountered or anticipated when scaling cellular IoT deployments



Source: Q22, full survey base n=675. Multi-select.

Pelion

What this distinction captures is operational reach, not radio reach. Most enterprises have figured out how to commission a SIM where their main estate sits; what they struggle with is the long tail of new regions, rural pockets, cross-border deployments, and the sites at the end of a fibre run that the cell tower itself depends on. In those places, the absence of local feet on the ground, local provisioning, local roaming agreements and local support starts to matter more than spectrum availability.

Three of the ten interviewees independently raised Scotland as a coverage problem zone, for very different IoT use cases. Rural and remote coverage emerged as a consistent operational concern across interviewees, with Scotland the most frequently cited geography - raised independently by three participants spanning very different IoT use cases. Equans, the facilities management firm whose Strategy and Growth Director oversees its IoT product portfolio, switched its primary cellular provider after coverage in remote locations failed to recover from agreed remediation, including a partner's commitment to add masts and form an agreement with another operator. Royal Mail's IoT and AI program management team flagged patchy rural coverage as a contributing factor to delayed parcel-tracking data during the 2025 peak season, a year in which the operator handled more than one million misplaced parcels. Drax's IoT and connectivity lead, who oversees connected assets across the energy generator's distributed estate, captured the broader challenge: in remote UK areas - whether in Scotland, rural Wales, or parts of Northern Ireland - where cellular falters, the failure mode is rarely resolved by switching MNOs, because *"if cellular coverage is bad in an area, another carrier does not necessarily have better coverage."*

Enbridge made the point in a different register. Last year, the pipeline operator attempted to deploy 5,000 Cathodic Protection Remote Monitoring Units (RMUs), devices that protect steel pipeline infrastructure from corrosion, across its North American footprint. The deployment ran into pockets of poor Cat-M coverage that required external antennas, slowing the rollout. Worse, the procurement cycle ran longer than anticipated, and the seasonal installation window, set by weather, closed before all the RMUs went in. Devices that should have been protecting the asset were sitting in a warehouse waiting

drax

"In the UK, if cellular coverage is bad in an area, another carrier does not necessarily have better coverage. The bigger issue is whether you have someone close enough to put feet on the ground when something fails." Drax IoT lead

This pattern shows up in the survey's wider numbers. Reliability is the second-most-common scaling concern (62%), and the most-cited specific reliability complaint among dissatisfied respondents is outage frequency of once a month or more. Once-a-month outages are tolerable for a smartphone fleet. They are corrosive for IoT applications where the value proposition rests on continuous data, in patient monitoring, pipeline integrity, fleet telemetry, and EV charging session integrity.

Two practical consequences follow. First, coverage validation needs to happen before the contract is signed, not after. Several interviewees described it as the long pole in the project tent. Second, the question to ask a provider is not *"do you cover X"* but *"how do you behave at the edge of coverage X"*. What fallback options exist, how fault domains are bounded, how quickly the provider can put either a remote fix or a person on the ground when something breaks.

Pelion

SECTION 03

The CMP Sprawl Problem

A Connectivity Management Platform (CMP) is the operational dashboard that lets a customer activate, suspend, monitor, troubleshoot and bill SIMs. Each network operator typically supplies its own. For an enterprise running multiple operator relationships across multiple regions, the result is exactly what you would expect: multiple CMPs.

The survey shows 47% of respondents flagging *using multiple CMPs* as a scaling problem. This problem is downstream of the previous section. As fleets go international, the typical response is to sign a regional carrier in each region, which multiplies CMPs in lockstep. The result is a connectivity operations team that lives in three or four browser tabs, reconciles billing across formats, and discovers anomalies a beat slower than they should because the data lives in different systems.

Honeywell

Even though all the cellular connectivity is on a single bill, the contract with cellular operator for a single router will fall on a different date due to when router installed. Managing the staggered contract end-dates means knowing when to renew contracts for sometimes hundreds of routers.

Senior Product Manager
Honeywell

A subtler version of the same problem surfaced in Pelion's interview with a Senior Product Manager at Honeywell. Honeywell's Building Management Systems are designed to last 15 years; cellular routers come and go on a far shorter cadence. As Honeywell sells BMS into customers with hundreds of buildings, those routers end up being installed and switched on whenever each building goes live, sometimes over months or years. Each router carries its own contract, with its own start and end date.

"Even though all the cellular connectivity is on a single bill," the Honeywell product manager explained, *"the contract with cellular operator for a single router will fall on a different date due to when the router was installed. Managing the staggered contract end-dates means knowing when to renew contracts for sometimes hundreds of routers."* Multiply that by 100 customers with hundreds of buildings each, and the renewal calendar becomes its own operating cost.

Pelion

This is the unglamorous reality of IoT connectivity at scale. The decisions that look small at procurement time, including the assumption *"we'll add this site's SIM whenever the site goes live,"* accumulate into operational debt that nobody owns. The CMP question is rarely framed as *"can your platform replace the four I currently have?"* It is framed as *"can your platform absorb the next round of new sites without forcing me to add a fifth?"*

When asked why they would consider an MVNO for their next deployment, 58% of survey respondents named *more connectivity management functionality* as a reason. It is the second-most-cited driver after cost flexibility. That ranking is not because MVNOs are universally better at building dashboards. It is because the MVNO commercial model implies a single CMP across whatever underlying carriers are stitched together for the customer. The dashboard is the unification point.

But not every MVNO actually delivers on this promise, and the survey is candid about it. Among manufacturing respondents who flagged *connectivity management* as not sufficient at their current provider, 38% were already on an MVNO, and all of them were looking to switch.

Key takeaway

The lesson is that *"single CMP"* is a feature claim that needs to be probed, not assumed.

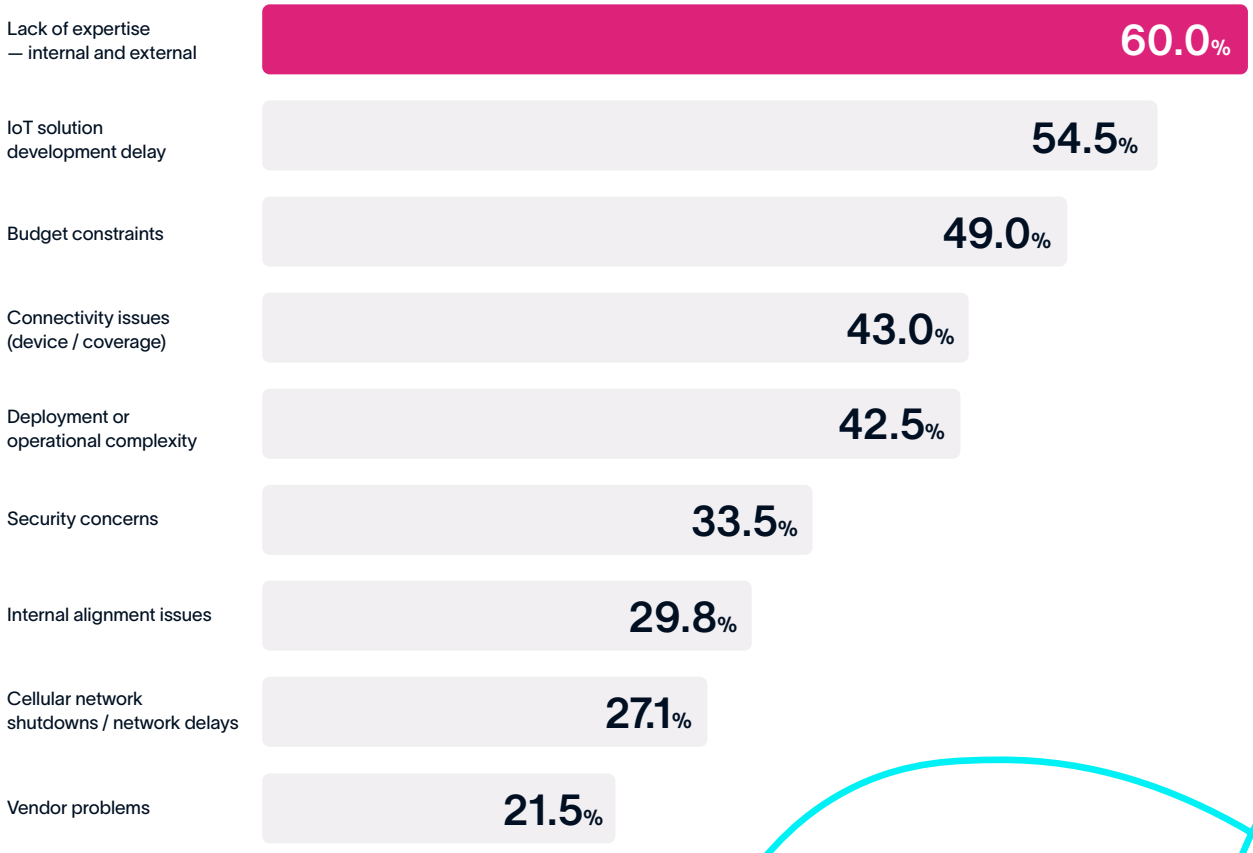
Pelion

SECTION 04

Why "Lack of Expertise" Tops the Block List

The single most-cited reason cellular IoT projects get delayed or blocked is not coverage, not security, not the network, not even budget. It is lack of expertise, internal and external, named by 60% of respondents. Budget constraints come second at 49%. Connectivity issues, the failure mode the network is most often blamed for, comes fourth at 43%.

Factors that have delayed or blocked cellular IoT projects



Source: Q14, full survey base n=675. Multi-select.

This is a striking finding for an industry that has spent the past decade getting cheaper, faster, and more standardised at the radio layer. The bottleneck has moved up the stack, and the most telling symptom is that customers can buy a SIM in seconds but cannot buy the advisory help they need in anything close to the same timeframe.

The interviews put faces to the data. Drax's IoT lead was direct about the pattern from a buyer's seat: *"From the vendors, the lack of understanding of their customer needs is generally appalling. You know that they're constantly trying to sell something that I don't want or I don't need."* CVS Health's connectivity lead described a related symptom: the slowness of carriers to approve testing of new cellular medical devices, which during the COVID period meant a prototype could not be cleared in time for the use case that motivated it. Enbridge's IIoT lead described pulling out of an RMU procurement after the vendor would not meet SIM-level security and lifecycle management requirements. The vendor's commercial team did not understand what the operator was asking for, and a truck roll became necessary as a result.

Where customer dissatisfaction with current providers concentrates

UK respondents:	US respondents:
1. IoT Expertise (27% rated not sufficient)	**1.** Pricing/Offers (24%)
2. Deployment Services (23%)	**2.** IoT Expertise (23%)
3. Connectivity Management (20%)	**3.** Deployment Services (22%)
4. Security (20%)	**4.** Security (20%)

The expertise gap divides cleanly into two failure modes when you read the data. The first is advisory. The buyer wants help thinking through the right architecture, the right network technology (Cat-M vs Cat-1 vs NB-IoT), the right SIM choice, the right roaming model. The provider does not have anyone qualified or available to give it. *Limited or poor advisory services* is the most-cited specific complaint among respondents dissatisfied with their provider's IoT expertise. The second failure mode is responsiveness. The buyer needs help during deployment, and the provider's resources are slow to engage. Lack of resources, slow to respond is the most-cited complaint about deployment services. Pre-deployment device testing and validation runs second.

This is the pattern of providers who treat IoT connectivity like a wholesale SIM business. The volume model assumes the customer will figure out the operational details on their own; the customer cannot, because the operational details are precisely the part that does not scale with experience-elsewhere. A customer who has run hundreds of fleet vehicles knows almost nothing useful about deploying medical-grade Cat-M devices. A customer who has run patient monitors knows almost nothing useful about RMUs. The expertise gap is not laziness; it is structural.

The implication is that the buyer should treat *advisory bandwidth* as a procurement criterion in its own right.

Key takeaway

Ask, in the RFP, what specific pre-deployment activities the provider performs as part of the contract: coverage validation in target regions, device certification testing, network technology recommendations against the use case, integration support against the customer's CMP and security architecture. If the answer is *"we'll connect you to support after go-live,"* that is the wrong answer.

Pelion

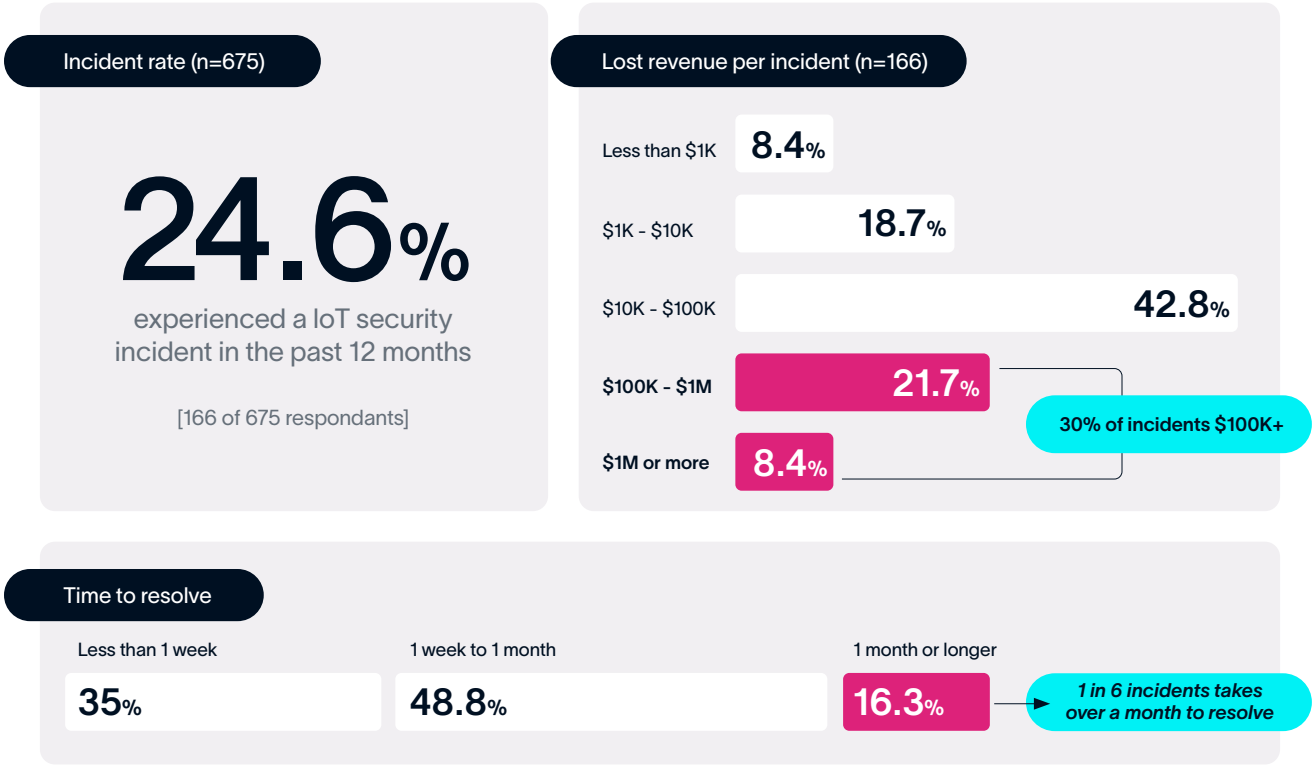
SECTION 05

Security Has Crossed the Operational Threshold

Two years ago, security in IoT was mostly a question for the design phase. Today, it is an operational reality on the budget line.

The data is unsparing. Just under one in four respondents (24.6%) experienced a security incident involving an IoT device in the last twelve months. Among those incidents, nearly a third (30%) cost the business more than $100,000 in lost revenue, and 8% cost more than $1 million. Sixteen percent of incidents took longer than a month to resolve once detected.

IoT security incidents in the past 12 months and their financial impact



Source: Q26 base n-675; Q27a/c base n=166 (respondants who experience an incident).

Yet 82% of survey respondents rate security as critical or important when selecting an IoT connectivity solution. The mismatch between *we know it's important and one in four of us has been hit* is the gap this section is about.

When asked which security risks they consider significant when deploying IoT at scale, respondents converged on three answers. Data breach and privacy exposure is the most-cited risk (64%) and the most likely to be ranked the top risk (42% rank it #1). Insufficient threat detection comes second (57% / 41% rank #1). Regulatory non-compliance and the financial and reputational costs that follow comes third (52% / 38% rank #1). Connectivity loss and network attacks, the threat most directly the connectivity provider's problem, registers for 37%, with about a third of those ranking it as their top concern.

> ***Since the Ukraine war, the number of attempted hacks has gone from a few per month to tens per day.*** — Drax IoT lead

The interviews colour in why these numbers are what they are. Two operators in this survey's interview pool had already experienced the kind of supply-chain or SIM-level incident that the survey asks about in the abstract. Equans had a SIM tampering incident severe enough that the firm engaged a consulting partner to design an intrusion detection system based on data pattern recognition. Enbridge experienced malicious profile switching in supply chain tampering, a category of attack that becomes possible specifically because eSIM enables remote profile management, and that requires GSMA-compliant Remote SIM Provisioning with strict profile governance to defend against. "*SIM identity theft is a growing issue as device fleets scale,*" the company's IIoT lead observed. "*Attackers steal the SIM, take the IMSI and clone the SIM profile. You lose a lot of telemetry data.*"

The regulatory dimension is becoming a budget item in its own right. Drax estimates fines under the EU's NIS2 directive can exceed $30 million for non-compliance. In the United States, Pipeline and Hazardous Materials Safety Administration (PHMSA) civil penalties accrue at $250,000 per day; FERC penalties run at $100,000 per day per violation. Methane leak detection regulations add another $50,000 per day. Energy respondents in the survey ranked regulatory non-compliance and data breach as joint top security risks, which is the rational read of the exposure.

What this means for the buyer of cellular IoT specifically is that the boundaries between *device security, network security, application security* and *regulatory evidence* have effectively dissolved. A connectivity provider that ships a SIM and bills for data is not a partner in this environment. The buyer needs private APNs, deterministic routing, IPSec or VPN options, monitored profile changes, audit trails, integration with the customer's existing SIEM and intrusion detection, and the ability to respond fast when an indicator turns up. Roughly 90% of respondents now place primary responsibility for IoT security inside an IT function: IT-Operations (35%), IT-Information Security (27%), IT-DevOps (19%), Network Engineering (9%). This is the most centralised the buying function has been at any point in IoT's commercial history.

The structural shift to watch is the one Saputo described from the inside. The dairy producer's senior manager of operational technology has spent five years pulling factory connectivity out of an open-internet model into something defensible. That work includes immutable offsite backups, endpoint protection on every device, secure remote access (Saputo uses ClaritySRA and BeyondTrust for vendor support), VLAN segmentation, and a rule that anything on the periphery of the plant sits on a different network from anything core to the manufacturing process. *"Want only one front door, no side doors,"* he put it. Cellular is one of the side doors that has to be closed properly, and the IT-OT unification most survey respondents are now in the middle of is the project that closes it.

Pelion

SECTION 06

eSIM: Real, Useful, Uneven

eSIM is one of the few topics in this report where the survey data and the interview data point in genuinely different directions. The data shows clear forward momentum: multi-network eUICC SIMs are already in use by a non-trivial share of UK respondents, healthcare leads adoption, and satellite (which depends operationally on the same profile-management capability) is identified by more than half of respondents as a serious consideration in the next two to five years. Industry forecasts now put the SGP.32 share of new standards-compliant IoT profile downloads rising from 7.6% in 2026 to 45.3% in 2030, which would mark the fastest profile-format transition the industry has seen.

A clarifying note before going further. eSIM in the IoT context refers to the eUICC capability that lets a SIM hold and switch between multiple operator profiles over the air. That capability is available across all the SIM form factors a customer is likely to deploy: the familiar removable SIM card (still a "physical SIM" but with eUICC inside), the embedded MFF2 chip soldered onto a board, and the newer integrated iSIM that lives inside the cellular modem itself. Choosing a removable form factor does not preclude OTA profile management, and choosing an embedded form factor does not require the operator to give up control. The form factor is an industrial-design decision; the eUICC capability is the connectivity decision. Most of the buyer disagreement that follows is really about operating preference, not technology.

The interviews show something more nuanced. Adoption is real, but it is not even, and the disagreement among sophisticated buyers is genuine.

UPS is actively using eSIM to keep the option of switching cellular providers open. Enbridge is enthusiastic about eSIM. Its IIoT lead described eUICC as solving *"one of the biggest operational challenges"* by enabling remote profile provisioning, multiple profile support, and a meaningful reduction in truck rolls. The migration itself, however, will take several years given the device replacement cycle. Honeywell's product manager noted no operational obstacle to eSIM but observed that the customer typically picks the gateway and the carrier, so eSIM adoption is customer-led rather than vendor-pushed.

At the other end of the spectrum, Drax's IoT lead was emphatic that eSIM is not the right fit for distributed energy critical infrastructure: *"eSIM does not change the propensity to switch because we use physical SIMs. We're never going to do that swap over without someone on site anyway. eSIM is much more of a consumer thing than an industrial thing. If you decided to do a remote swap and then it didn't work, then yeah, things would not go well. If the swap doesn't work, put in the old SIM. We don't want to be down in comms for half a day."* Autoliv's Vice President of IT for the Americas sees the value of eSIM for switching connectivity providers but is unconvinced it solves contractual obligations between the providerand downstream carriers, which was the actual blocker on his previous contract.

Pelion

Both views capture something real, even if the underlying technology applies equally to both. For high-volume, geographically distributed fleets such as wearables, asset trackers, smart meters, and EV chargers, the operational and commercial case for using eUICC profile management to its full extent (provisioning at the point of activation, switching profiles remotely, retiring devices without truck rolls) is straightforward, and the economics demand it. For lower-volume, higher-stakes installations where someone is going to be on site anyway, the buyer often prefers a more conservative operating model with physical access to the device and tighter governance over when profiles change. That preference is reasonable, and it is best understood as a choice about operations rather than about the technology itself. The same eUICC SIM can run either way, and a buyer who insists on on-site replacement today retains the option to enable OTA profile management later.

Key takeaway

Two practical points follow. First, the arrival of SGP.32 matters because it is the first eSIM standard built specifically for IoT, solving the device-side complexity that previous specifications, designed around consumer phones, never properly addressed. The eSIM offered today is a meaningfully different proposition from the eSIM that will be offered in 2027. Second, eSIM is not a free upgrade on the threat model. The Enbridge incident is a real-world example of an attack vector that eSIM creates: malicious profile switching in the supply chain. The mitigation, GSMA-compliant Remote SIM Provisioning with strict governance over which profiles a SIM is allowed to accept and from where, should be specified in the contract, not assumed.

Pelion

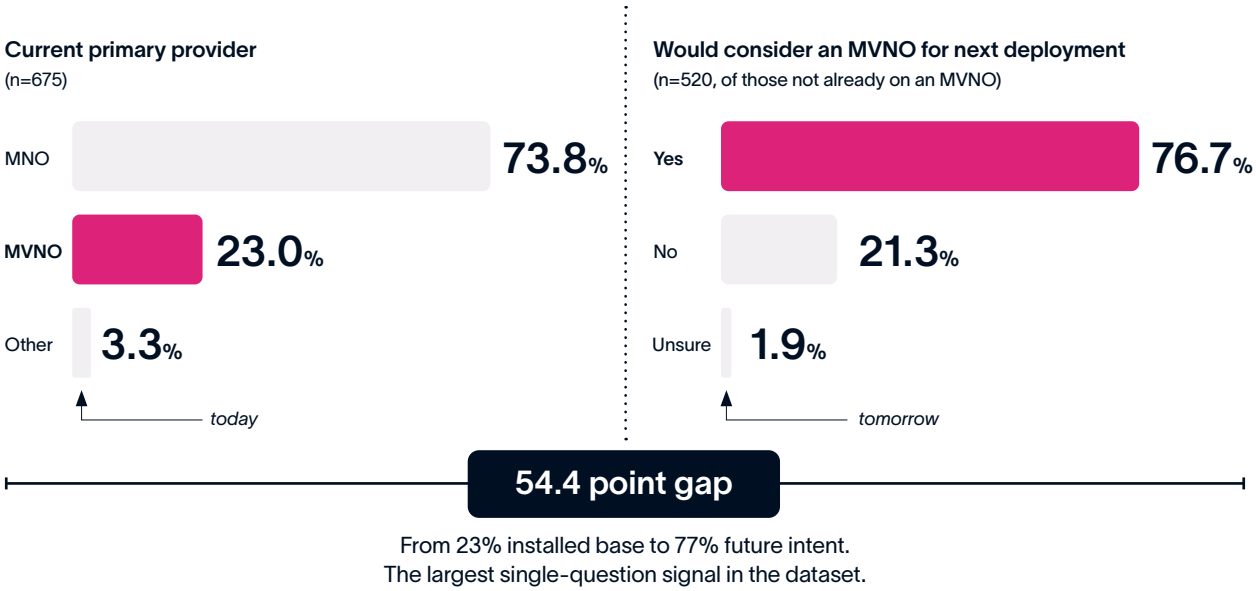
SECTION 07

The MVNO Question

The most striking single number in this report is what enterprises say about their next deployment: 77% of respondents not currently using an MVNO would consider one for their next deployment.

The current installed base tells a different story. Just 23% of respondents named an MVNO as their primary provider; 74% named an MNO. The gap between would consider and currently use is roughly 54 percentage points, and that gap is what every MVNO sales team in cellular IoT is staring at this year.

Current cellular IoT primary provider versus future intent



From 23% installed base to 77% future intent.
The largest single-question signal in the dataset.

Source: Q15 base n=675; Q17 base n=520 (respondents not currently on an MVNO).

Why the gap exists, and why it is closing, is worth taking seriously. The reasons respondents gave for being open to switching are operational. Cost and commercial flexibility led at 66%. *More connectivity management functionality* came second at 58%, the single-CMP argument from Section 3. Global multi-network carrier access, the ability to sit on top of multiple operators with one SIM, came third at 48%. These are problems an enterprise running an international, scaling fleet recognises immediately.

The reasons given for not considering an MVNO are different in character. The leading objection, cited by 61%, concerns reliability and network offerings; limited global coverage came second at 50%, and support and services concerns followed at 36%. Reliability and coverage, it should be noted, are perceptions about the underlying network, and an MVNO's underlying network is, by definition, an MNO's. The honest read of these reasons is that the buyer is comparing the MVNO to a hypothetical version of the MNO that doesn't exist in their actual experience.

The interviews reflect both sides of the trade-off, intelligently argued. United Health Group's CTO prefers MNOs for patient-monitoring connectivity on the basis that MNOs *"control the infrastructure directly, they can offer strong coverage guarantees and direct support for troubleshooting."* His concern about MVNOs as an additional layer between him and the network is a reasonable one in healthcare specifically, where patient safety raises the bar for incident response time. Equans prefers MNOs partly for security certification reasons. At least one UK government ministry contract excluded MVNOs over information security management standards. Drax's preference for MNOs is grounded in critical-infrastructure cybersecurity: the MNOs Drax buys from explicitly avoid Chinese components in their network equipment.

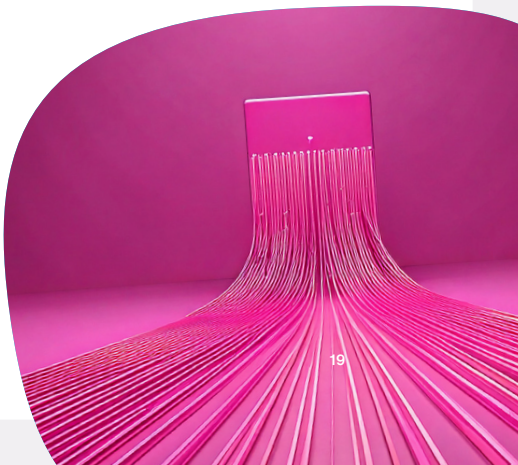
On the other side, Enbridge, which also operates critical infrastructure and is also rigorous about security, chose an MVNO precisely because the unified SIM lifecycle management, single APN architecture, and cross-border consistency mattered more than direct MNO ownership of the spectrum. Autoliv's choice of a managed multi-network model is fundamentally an MVNO bet. The dispersion in these choices is real, and tracks the kind of estate the buyer is running: estates that are geographically concentrated and reliability-critical lean MNO, while estates that are geographically distributed and operationally complex lean MVNO.

The 77% figure reflects the full survey base across the UK, US, Canada and Europe. Looking only at the UK and US, MVNO consideration sits at approximately 60%. The wider number is shaped by Canada and Europe, both regions where MVNO presence in cellular IoT is more established. It is the more accurate read of the wider Western European and North American market. The deeper provider-rating data also shows that in the United States, MNOs scored worse than MVNOs on most criteria (including IoT expertise, deployment services and security) among dissatisfied respondents. The takeaway is not that MVNOs are universally better. It is that the concerns around reliability holding many enterprises back are not borne out in the operational satisfaction data of buyers who have actually moved.

For a buyer planning their next two years of estate decisions, the practical question is more useful than the abstract debate. *Does the carrier I am buying from have enough operational ownership of the elements I most need (global SIM lifecycle management, a single CMP, deterministic roaming, security architecture, advisory bandwidth) to actually solve my problem? Or am I buying a wholesale SIM with a logo on it?* That question cuts across the MNO/MVNO label and points at what the buyer actually needs.

Key takeaway

The takeaway is not that MVNOs are universally better. It is that the concerns around reliability holding many enterprises back are not borne out in the operational satisfaction data of buyers who have actually moved.



Pelion

SECTION 08

What Good Looks Like

Pelion's view

This is the second of two sections where Pelion steps in front of the analyst and offers a point of view. Five characteristics, in our experience, separate connectivity providers who solve the problems described in this report from those who quietly become part of them.

Borderless network access on a single SIM.

A multi-network eUICC SIM that connects across 600+ networks in 150+ countries removes the operational tax of regional carrier patchworks. It also keeps the option of changing carrier open after deployment, without a SIM swap. This is the foundation; everything else assumes it.

One CMP that survives carrier changes.

The Pelion Portal exists because the *staggered renewals across hundreds of routers* problem Honeywell described is not Honeywell's fault. It is the fault of an industry that built its tooling around carrier billing cycles rather than around customer estates. A single management portal, with over-the-air SIM updates, real-time visibility, policy enforcement, and API integrations, should absorb new carriers, new regions, and new device classes without forcing the customer to add a fifth dashboard.

Pre-deployment advisory, not just reactive support.

The 60% of survey respondents who say lack of expertise is blocking their projects are not asking for a longer support phone tree. They are asking for help thinking. Pelion's IoT experts function, including a named pre-deployment testing service, exists for one reason: a connectivity decision made well at the start saves more money than any support escalation can recover. We learned this the hard way over 25 years, and we structure the customer engagement around it.

Security built into the connectivity layer, not bolted on.

Private APNs, IPSec VPN options, eUICC profile governance, and operational monitoring belong with the SIM, not in a separate product the customer has to buy and integrate. The buyer who is being asked by their regulator (under NIS2, CRA, RED, or HIPAA) for evidence that their connectivity is secure should be able to get that evidence from one place.

Commercial model that flexes with fleet growth.

Flexible pooled data plans, transparent overage controls, and the operational resilience of 99.995% uptime exist to make scaling a non-event. The right commercial model lets the customer's IoT estate grow without forcing a re-procurement every time the fleet shape changes.

These are also the characteristics this report's data points to. Pelion has built towards them, and we are not the only people who can. The work for the buyer is to make sure whoever they choose is doing the same, and to recognise the warning signs when they are not. We made ***Connectivity Made Effortless*** our strapline because it is also the brief: connectivity is the easy part of IoT, until it isn't, and the rest of the work is what separates a deployment that scales from one that quietly consumes margin.

Pelion was ranked #1 for IoT Connectivity Management on G2 in Summer 2026. Further detail on the products and services referenced above is at pelion.com.

Pelion

SECTION 09

Practical Takeaways for IoT Leaders

For decision-makers planning the next two procurement cycles, six questions are worth putting to any cellular IoT connectivity provider, incumbent or new, before signing.

1

What does your operating model look like when half my fleet is outside my home market?

The fleet shape of 2030 is not the fleet shape of 2025. The contract should be sized for the destination, not the starting point.

2

How do you handle staggered SIM and contract end-dates across an estate built over years?

This is the question Honeywell's experience makes concrete. If the answer is *"each contract runs independently,"* the buyer is taking on the operational debt.

3

What specific pre-deployment activities are part of the contract?

Coverage validation in target regions, device certification testing, network-technology recommendations against the use case, integration support. These belong before go-live, not after.

4

What evidence will you provide when my regulator asks about supply-chain integrity, SIM-level security, or incident response?

Compliance evidence has become an operational requirement in its own right, and a buyer who has to assemble it from disparate vendors is effectively paying for it twice.

5

How is your security architecture integrated rather than add-on?

Private APNs, eUICC profile governance, monitored routing, audit trails. If these are products the buyer has to combine themselves, the seam is the vulnerability.

6

If I want to leave you in two years, what does that exit look like?

The right answer involves eUICC SIMs, portable profiles, and a clean handover. The wrong answer involves replacing single-profile SIMs in 50,000 devices.

The connectivity decision made at the start of an IoT programme determines whether the next five years cost more or less than expected. The data in this report suggests most enterprise buyers know this. It also suggests the gap between knowing and doing is currently wider than it should be.

About this report

Outside the Core: The State of Enterprise IoT Connectivity in 2026 **is published by Pelion in partnership with ABI Research, who facilitated the survey design, fieldwork and qualitative interview programme.**

The primary survey was conducted between Q4 2025 and Q1 2026 across 675 cellular IoT decision-makers, budget holders and influencers in the UK (255), US (195), Canada (78) and Europe (147), spread across energy, healthcare, logistics and transport, manufacturing, and smart buildings/smart city. The qualitative interview programme was conducted between November 2025 and January 2026 with senior IoT decision-makers at Autoliv, CVS Health, Drax, Enbridge, Equans, Honeywell, Royal Mail, Saputo, United Health Group and UPS. Interview attribution in this report is by company and role; individual interviewees are not named. The narrative, analysis and recommendations in this report are Pelion's.

Further information: **pelion.com** | **Talk to us**

Pelion

Global IoT Connectivity Made Effortless

Contact us today or visit our website

hello@pelion.com | Pelion.com