



2026 State of IoT Report.

Growth, Boardroom Risk and the Rise of Connectivity Orchestration

Go beyond

@Eseye Limited • Sept 2026
Ref no: 9141

Contents

Foreword	3		
Key trends and market dynamics	5		
5 key market trends	7		
The value of IoT today	10		
- <i>The non-negotiables</i>	12		
Barriers to IoT success	13		
- <i>The satisfaction paradox</i>	15		
How IoT Adoption Varies by Industry	16		
- <i>EV Charging & Smart Grid</i>	17		
- <i>Healthcare & Medical Devices</i>	18		
- <i>Manufacturing</i>	19		
- <i>Retail, Catering and Leisure</i>	20		
- <i>Smart Vending</i>	21		
- <i>Supply Chain & Logistics</i>	22		
Regional Insights: UK vs. US IoT adoption trends	23		
- <i>Deployment scale</i>	23		
- <i>Growth intentions</i>	23		
		- <i>Different Stages of Scale</i>	23
		- <i>Growth Expectations Remain Strong</i>	24
		- <i>The Connectivity Gap Challenge</i>	24
		- <i>Different Measures of IoT Value</i>	24
		Our recommendations	26
		- <i>Build a business case around industry-specific value and operational outcomes.</i>	26
		- <i>Address reliability before deployment</i>	27
		- <i>Retain strategic control, outsource operational complexity</i>	28
		- <i>Design for multi-network resilience</i>	29
		- <i>Make security and network migration strategic priorities</i>	30
		- <i>Prepare for network sunset now</i>	31
		Conclusion	32
		About Eseye	33
		- <i>Methodology</i>	33

Foreword



There comes a point in the evolution of every major technology when the question shifts from whether it will be adopted to how it can be scaled effectively and trusted completely.

For the Internet of Things, that moment has arrived.

IoT is no longer an emerging technology. It is now a core component of how organisations operate, innovate and compete. Across industries, connected devices are transforming customer experiences, enabling new business models, optimising operations and delivering the real-time intelligence that drives better decisions.

The findings in this year's State of IoT Adoption Report show that enterprise ambition continues to accelerate. Nearly eight in ten organisations expect their connected device estates to expand over the next 18 months, while two-thirds plan to increase investment over the next two years. The strategic importance of IoT has never been clearer.

However, the research also highlights a critical reality: scaling IoT successfully is becoming as much an operational challenge as a technology one.

As deployments grow in scale and business importance, organisations face increasing complexity. Connectivity resilience, security, device management and the challenge of managing

multiple providers remain significant obstacles.

More than half of enterprises still report average connectivity performance of 90% or below, despite near-continuous connectivity now being essential for many applications.

“This matters because IoT has evolved beyond a technology initiative into business-critical infrastructure.”

This matters because IoT has evolved beyond a technology initiative into business-critical infrastructure. Connected devices increasingly support revenue generation, customer service, operational efficiency and, in many cases, essential services. When connectivity fails, the impact extends far beyond the technology team.

Encouragingly, enterprises are becoming more sophisticated in how they approach connectivity. While cost remains important, organisations are placing greater emphasis on resilience, flexibility, global reach and operational simplicity. Increasingly, they recognise that delivering these outcomes requires more than access to networks. It requires the ability to manage connectivity intelligently and consistently at scale.

This is particularly evident in the growing interest around SGP.32 and next-generation eSIM technologies.

The promise of greater flexibility and control is compelling, but this year's findings suggest enterprises also understand that flexibility alone is not enough.

Realising the full value of these technologies requires orchestration, automation and expertise.

For me, that is the defining insight from this year's research. The appetite to scale IoT has never been greater, but operational maturity must now keep pace. The organisations that succeed in the next phase of IoT adoption will be those that make connected infrastructure effectively invisible: resilient, intelligently managed and trusted to perform whenever and wherever it is needed.

I hope you find this year's research insightful and valuable as you plan the next stage of your IoT journey.

Tony Byrne
Chief Executive Officer

Takeaways for time hungry readers

- 1 Enterprise IoT is scaling rapidly.** Most organisations now operate between 1,000 and 10,000 devices, 78% expect their estates to grow within 18 months, and 66.5% plan to increase IoT budgets over the next two years.
- 2 IoT connectivity has reached the boardroom.** More than three quarters (75.6%) of enterprises now regard IoT connectivity as board-level priority as connected technology becomes more deeply embedded in customer-facing products and business-critical operations.
- 3 Operational performance is not keeping pace with ambition.** More than half of enterprises achieve 90% or below average uptime, while only around 1% achieve higher than 98%, even though near-total connectivity is considered critical.
- 4 Enterprises want managed complexity, not surrendered control.** Businesses want visibility, flexibility and governance, but increasingly expect providers to handle orchestration, network switching and day-to-day operations.
- 5 Resilience is becoming a non-negotiable.** Multi-connectivity, network choice and managed connectivity are rising up the futureproofing agenda as enterprises look beyond basic network coverage.

What's changed since 2025?

-  **SGP.32 moves from specification to deployment.** Enterprises want the flexibility SGP.32 promises, but are increasingly recognising that orchestration is needed to manage the complexity.
-  **Device growth intentions.** Growth is back on the agenda. After a more cautious 2025, enterprises are once again planning to scale their connected estates.
-  **Budget growth intentions.** Investment is following ambition, with significantly more enterprises now preparing to increase IoT spending.

 **Multi-connectivity as the top futureproofing priority.** The biggest shift in futureproofing priorities. Enterprises are increasingly looking to network choice and resilience as they scale.

 **Managed network connectivity as the top futureproofing priority.** More businesses are recognising that greater connectivity choice also brings complexity, strengthening the case for managed orchestration.

“Enterprises are increasingly looking to network choice and resilience as they scale.”

“Enterprises want the flexibility SGP.32 promises.”

Key trends and market dynamics

After a more cautious 2025, enterprise IoT appears to have regained its momentum.

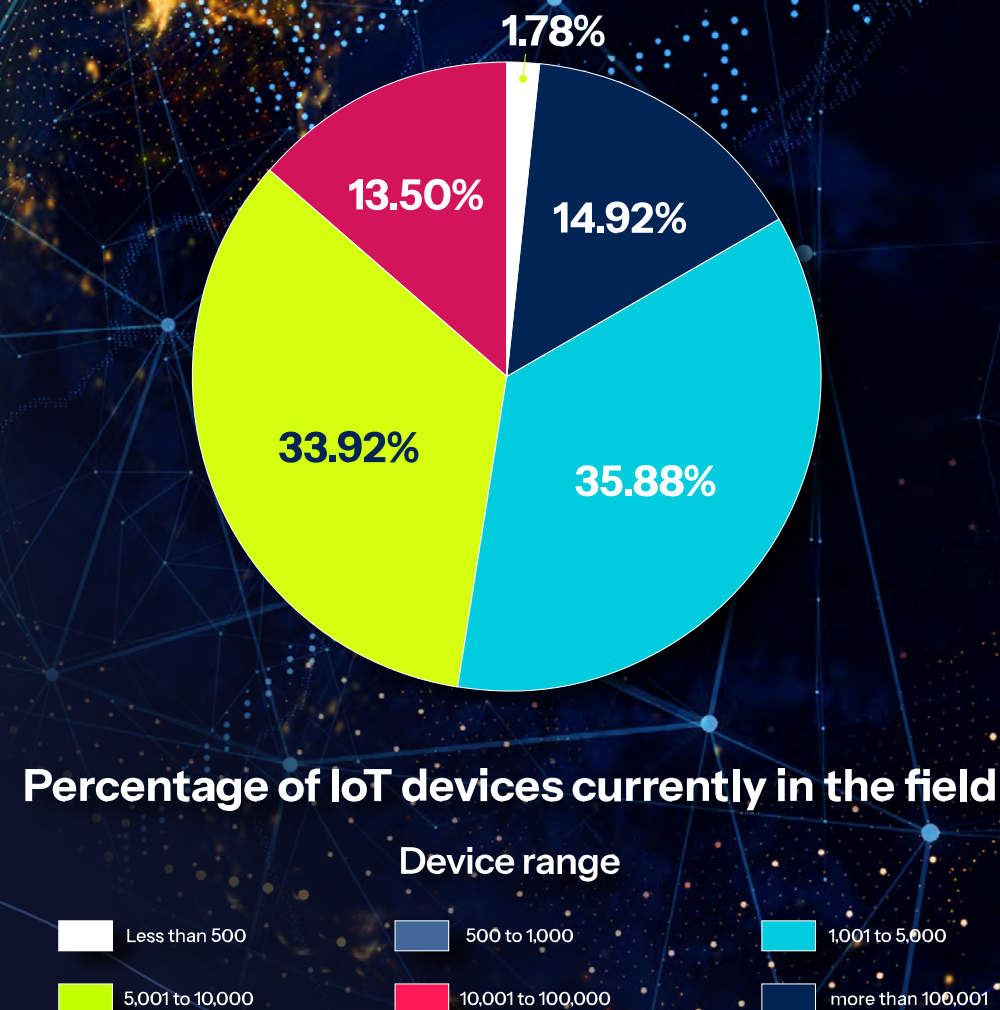
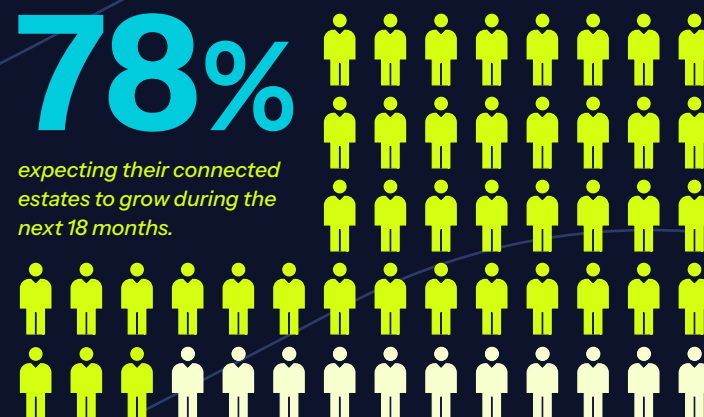
Deployment ambitions are accelerating again, with 78% of organisations expecting their connected estates to grow over the next 18 months, while 66.5% plan to increase IoT budgets over the next two years. This marks a notable change from 2025, when expansion intentions had fallen to 66% and just 47% planned to increase investment. The picture in 2026 is therefore not simply one of IoT reaching maturity, but of enterprises returning to growth with greater confidence and with a much clearer understanding of what successful scale requires.

But this renewed confidence has not removed the challenges that come with scale. Many of the issues identified in our previous State of IoT Adoption reports remain unresolved, from inconsistent connectivity and device-level failures to technical complexity and the burden of managing multiple providers.

The difference in 2026 is that enterprises are increasingly looking towards multi-network resilience, managed connectivity and orchestration as the way to address them.

Most surveyed organisations now manage between 1,000 and 10,000 devices, with 78% expecting their connected estates to grow during the next 18 months. Investment is following the same trajectory; two-thirds plan to increase budgets, generally by meaningful amounts rather than marginal increments.

However, operational capability continues to not keep pace with expansion. Enterprises continue to struggle with multiple SIM and connectivity suppliers, access to specialist support, multi-region coverage, device-level performance and security. More than half report average uptime at 90% or lower, exposing a significant gap between the resilience businesses say they require and what they currently achieve.



The role of managed connectivity is becoming more sophisticated as enterprises prepare for SGP.32. Overall preference for working with a managed IoT provider remains consistently high, at 75.5%, but the 2026 findings provide a clearer picture of what enterprises now expect that provider to manage.



Managed SGP.32 orchestration is seen as beneficial by 78.1% of enterprises and is the highest-rated provider capability tested this year. Enterprises still want greater control, but increasingly appear to define that as visibility, policy ownership, network choice and supplier flexibility, rather than responsibility for every operational task.

“Overall preference for working with a managed IoT provider remains consistently high...”

The most valued provider capabilities were consistently identified as managed SGP.32 orchestration, end-to-end services, multi-operator access and rapid failover.

“Managed SGP.32 orchestration, end-to-end services, multi operator access and rapid failover rank among the most valued provider capabilities.”

As SGP.32 moves from specification towards operation, the opportunity for providers is therefore shifting from simply managing connectivity to orchestrating it across networks, profiles and the wider device lifecycle.

Over the next few years, competitive differentiation will increasingly come from resilience, automation, device intelligence, security and the ability to simplify global IoT operations.

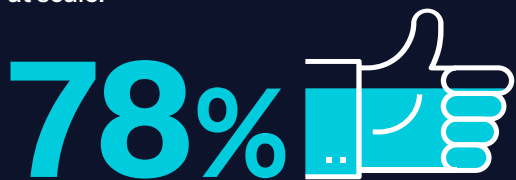


5 key market trends



1. Managed eSIM orchestration will become central to enterprise IoT.

With SGP.32 solutions only becoming ready for deployment this year, the conversation is naturally shifting from what the standard promises to how it will work in practice. In 2025, 74.3% of enterprises said they understood SGP.32 and its implications, while 75.1% wanted greater control over switching between networks. The 2026 findings provide an early indication of what enterprises expect as they begin considering the operational realities of SGP.32 at scale.



see managed SGP.32 orchestration as beneficial

While businesses still value the flexibility and control SGP.32 promises, 75.4% now believe self-managing it would be complex and resource-intensive, while 78.1% see managed SGP.32 orchestration as beneficial – the highest-rated provider capability tested this year.

These are not directly comparable measures, but together they point to an important evolution in enterprise thinking, where businesses still want control but are recognising they don't necessarily want the operational burden that comes with it.

This indicates the need for a role for a hybrid model in which enterprises retain governance, visibility and network choice, while providers manage the underlying orchestration through automation and specialist expertise.



2. Growth intentions have rebounded as enterprises plan their next phase of scale.

Enterprise IoT is already operating at significant scale, with nearly 70% of respondents managing between 1,000 and 10,000 connected devices and fewer than 2% operating estates below 500. Healthcare and Supply Chain & Logistics tend to report some of the largest fleets in this year's sample. However, rather than reading changes in estate size as a year-on-year market trend (the respondent samples differ between surveys) the more significant 2026 signal is renewed appetite for growth.



of respondents are managing between 1,000 and 10,000 connected devices

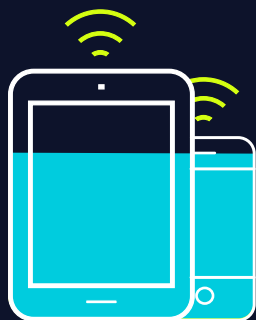
Some 78% of enterprises expect their device estates to increase over the next 18 months, up from 65.8% in 2025. This suggests that, following last year's more cautious outlook, expansion is firmly back on the agenda. Investment intentions have strengthened alongside this, with 66.5% expecting IoT budgets to increase over the next two years, compared with 46.8% in 2025. Together, these findings suggest that, following last year's more cautious outlook, both expansion and the investment to support it are firmly back on the agenda.

The challenge for enterprises and their providers will be ensuring that renewed growth does not bring a corresponding increase in connectivity complexity, management overhead and operational risk.

“This indicates genuine confidence rather than growth”

3. Investment in IoT connectivity is accelerating alongside growth.

Following on from above, 78% of enterprises expect device numbers to increase over the next 18 months, with doubling a common expectation (25% of respondents) and the largest organisations commonly anticipating more than twofold growth. At the same time, 66.5% expect budgets to rise over two years, with increases of between 25% and 50% particularly common.



78%

of enterprises expect device numbers to increase over the next 18 months,

This indicates genuine confidence rather than growth based solely on doing more with existing resources. Manufacturing, EV Charging, Smart Vending and Logistics are particularly expansionary.

“At the same time, 66.5% expect budgets to rise...”



4. Operational complexity intensifies as growth returns.

The challenge is increasingly not whether devices can be connected, but how effectively growing, geographically distributed estates can be managed. As deployment ambitions rebound in 2026, some of the operational pressures associated with scale are becoming more pronounced. Reliable multi-region connectivity has risen from 16.7% in 2025 to 20.8% as the main challenge while managing multiple connectivity or SIM vendors has increased from 19.8% to 21.6%.

Access to technical IoT support is also among the leading challenges this year, with one fifth (21.5%) reporting it as their main issue, while device-level issues continue to be widely recognised as a cause of project failure.



21%

report managing multiple SIM vendors as a challenge

As estates grow, every manual process can become more costly and difficult to manage, from supplier coordination and profile management to troubleshooting, billing reconciliation and lifecycle intervention.

“The greatest challenges are not whether devices can be connected, but whether increasingly distributed estates can be managed...”

With growth returning, the challenge for enterprises is therefore not simply how to connect more devices, but how to scale without multiplying the operational burden around them. This strengthens the case for platforms, orchestration and specialist services that reduce the effort required to manage connectivity across increasingly complex global estates. As IoT becomes more embedded in customer-facing and business-critical services, that operational burden increasingly becomes a business-risk issue rather than simply a connectivity-management challenge.



5. Multi-connectivity has become a top priority for future-proof resilience.

As we've reported in previous years, there remains a persistent gap between the connectivity enterprises say they need and the performance they achieve. More than three-quarters of enterprises believe cheap connectivity is not a good long-term investment, with a similar proportion regarding near-100% global connectivity as crucial to the business case. Multi-network choice, the ability to change operators, global coverage from a single SIM and fixed-line failover all attract strong support. Yet only around 1% currently achieve higher than 98% average uptime.

“This persistent expectation-performance gap will place growing pressure on providers to prove resilience through measurable service performance...”



75%

of enterprises expect believe cheap connectivity is not a good long-term investment.

75%



100%

regard near-100% global connectivity as crucial to the business case.

This continues a long-running trend: in 2024, fewer than 0.5% achieved connectivity of more than 98%, rising to just 2% in 2025. This persistent expectation-performance gap will place growing pressure on providers to prove resilience through measurable service performance, proactive optimisation and business-continuity capabilities instead of simple claims around network coverage.

The value of IoT today

The value of IoT has expanded beyond its traditional association with operational efficiency.

Enterprises now see connected technology as a broad business-transformation tool capable of supporting growth, sustainability, social impact, product innovation and competitive differentiation.

Sustainability and positive social or human impact were the joint-leading benefits in the survey, each selected by 37.1% of respondents. Increased revenue followed closely at 36.2%, with delivering a competitive advantage at 33.9%, operational cost reduction at 33.6%, and the development of smart connected products at 32.9%. The relatively narrow spread between these results shows that IoT does not deliver one universal benefit, but rather that its value depends on the organisation's strategy and industry.

The priorities differ meaningfully between segments. Smaller enterprises are most likely to associate IoT with revenue generation, while the largest organisations place greater emphasis on social impact.

EV Charging, Smart Grid and Healthcare enterprises prioritise sustainability, Smart Vending enterprises focus more strongly on reducing operating costs,

“IoT is delivering value across a wider range of business priorities...”

and Logistics companies see value in diversifying into connected products.

This suggests that the value of IoT is increasingly broad and multidimensional. Enterprises are looking to connected technologies to support revenue growth, competitive advantage and operational cost reduction, alongside sustainability and positive social impact. Rather than being defined by a single outcome, IoT is delivering value across a wider range of business priorities.

37.1%

Sustainability + Positive social or human impact



36.2%

Increased revenue



33.6%

Delivering a competitive advantage



32.9%

Development of smart connected products



Top benefits	2021	2022	2023	2025	2025	2026
1	Enter new markets (35%)	Create operational efficiencies (30%)	Increase revenue (55%)	Increase revenue (63%)	Contribute to sustainability goals (44%)	Joint lead: Contribute to sustainability goals & play a positive social or human impact (37.1%)
2	Increase profits (34%)	Three-way tie: enter new markets; reduce costs, increase revenue and profit; deliver a new line of business/new products (28%)	Create operational efficiencies (53%)	Contribute to sustainability goals (57%)	Play a positive social or human impact (38%)	Increased revenue (36.0%)
3	Deliver new lines of business (32%)	Deliver competitive advantage (24%)	Deliver competitive advantage (51%)	Deliver competitive advantage (57%)	Create operational efficiencies (36%)	Deliver a competitive advantage (33.9%)

“This suggests that the value of IoT is increasingly broad and multidimensional. Enterprises are looking to connected technologies to support revenue growth...”

The non-negotiables

As the value enterprises expect from IoT becomes more diverse, the connectivity requirements underpinning it are becoming broader too. In 2025, sustainability was the clear leading IoT benefit at 44.2%. In 2026, it stands at 37.1%, level with positive social or human impact, while revenue remains broadly stable at 36.2%, compared with 35.6% last year. Rather than one outcome dominating the business case, IoT is increasingly expected to deliver across a more balanced mix of commercial, operational, environmental and social priorities.

Enterprises increasingly expect IoT connectivity to provide resilient global coverage, rather than basic network access. Near-100% availability, multi-network choice, the ability to switch operators and continuity across regions are becoming baseline requirements. Businesses also want end-to-end support, specialist technical expertise and managed orchestration that removes day-to-day complexity.

However, enterprises also clearly indicate that flexibility cannot come at the expense of control. Enterprises want visibility into performance, costs and policies, together with the ability to govern how their estates operate, but they do not necessarily want to execute every network or eSIM management task internally. Security, regulatory compliance, data sovereignty and migration away from legacy 2G and 3G networks must also be designed into the service.

The implication for providers is that there is no longer a single measure of successful IoT connectivity. It must be resilient enough to protect revenue and operations, flexible enough to support changing business requirements, and manageable enough to scale without adding unnecessary complexity. Ultimately, a simple low-cost roaming SIM is no longer enough. Providers are expected to deliver reliability, transparency and operational simplicity across the complete device lifecycle

“Enterprises want visibility into performance, costs and policies, together with the ability to govern how their estates operate, but they do not necessarily want to execute every network or eSIM management task internally...”



Barriers to IoT success

The biggest obstacles to successful IoT connectivity are increasingly operational rather than conceptual.

Enterprises generally understand the value of IoT and are investing in larger estates, but many lack the processes, resources and service models required to manage that growth efficiently.

The most frequently identified challenges are managing multiple connectivity or SIM providers, accessing specialist technical IoT support and achieving reliable multi-region connectivity. Each was selected by roughly one in five enterprises as its main device-related challenge. These issues become more difficult as deployments cross borders, use different technologies and depend on several network or platform suppliers. Fragmentation creates duplicated processes, inconsistent visibility, complex billing and slower fault resolution.

Top benefits	2021	2022	2023	2025	2025	2026
1	Security (39%)	Three-way tie: Managing multiple carrier or provider contracts, Mitigating permanent roaming issues, Security of the devices (30%)	Achieving reliable device connectivity across multiple countries/regions/locations (18%)	Security of the devices (26%)	Three-way tie: Navigating technical device challenges, Accessing technical IoT support, Reliable multi-region connectivity (20%)	Managing multiple connectivity / SIM vendors (21.6%)
2	Device onboarding (35%)	Device onboarding (21%)	Security (17%)	Accessing technical IoT support (25%)	Security of the devices (17%)	Accessing technical IoT support (21.0%)
3	Cellular connectivity (35%)	Deliver deployment (20%)	Ongoing management of the device estate and professional services support (15%)	Reliable multi-region connectivity (22%)	N/A	Reliable multi-region connectivity (20.8%)

“Enterprises generally understand the value of IoT and are investing in larger estates...”

Device-level problems are another major barrier. More than three-quarters of enterprises agree that most IoT project failures originate at the device level. Poor antenna design, modem behaviour, firmware development, power consumption, installation conditions or inadequate testing can all affect connectivity failures once devices enter the field. This means successful connectivity cannot be separated from device engineering, validation and lifecycle management.

Actual connectivity performance also continues to fall short of enterprise expectations, with little evidence of meaningful improvement year-on-year. More than half (56.9%) of organisations report average uptime at 90% or below, compared with 54.8% in 2025, while only 1.2% achieve more than 98%, down from 2.1% last year. Healthcare and Logistics generally perform more strongly, while Manufacturing, EV Charging and Smart Vending remain concentrated around 81-90% uptime. This persistent performance gap is particularly significant because nearly three-quarters say near-total global connectivity is crucial to their business case.

Almost a third (29.3%) of enterprises identify an inability to operationalise AI effectively because of a lack of reliable IoT data among the consequences



or risks associated with limitations in achieving reliable, secure and globally accessible IoT connectivity. Looking ahead, 31.4% believe widespread and effective IoT deployment could improve business decision-making and process automation through better access to that data.

For organisations looking to bring AI into physical operations, IoT is the infrastructure working in the background. Connected devices generate the real-world data that AI models, agents and automated systems depend on to make informed decisions. If that data foundation is unreliable, the intelligence built on top of it will be limited too. Poor or intermittent connectivity therefore can create gaps in the data feeding AI and automation, undermining its completeness, timeliness and reliability.

“Actual connectivity performance also continues to fall short of enterprise expectations...”



As AI adoption accelerates, enterprises that fail to build a resilient IoT and connectivity foundation risk being unable to operationalise AI as effectively as those that do.

Security is an additional concern, with 73.3% reporting experience of an IoT security breach during the previous 12 months. Legacy-network migration also presents risk, with roughly three-quarters anticipating disruption from 2G and 3G shutdowns.

Finally, new capabilities can introduce their own complexity. Although SGP.32 offers greater flexibility, 75.4% believe self-management would be complex and resource-intensive. The barrier to using SGP.32 is therefore not access to technology alone, but the ability to operationalise at scale. To overcome this enterprises need managed eSIM orchestration, unified visibility, proactive support and stronger integration between devices, connectivity and business operations.



73%

of companies reporting experience of an IoT security breach during the previous 12 months.

The satisfaction paradox

92% say they are satisfied with their IoT connectivity provider. But should they be?

Overall provider satisfaction has risen sharply, from 78.6% in 2025 to 92.2% in 2026. Yet underlying connectivity performance has not improved alongside it. 56.9% of enterprises still report average uptime at 90% or under, while only 1.2% achieve higher than 98% uptime.



56%

enterprises still report average uptime at 90% or under.

The survey cannot tell us why satisfaction and technical performance appear so disconnected, but it raises an important question for the industry: are enterprises judging their providers against what good IoT connectivity could deliver, or simply what they have come to expect?

“92% say they are satisfied with their IoT connectivity provider. But should they be?”



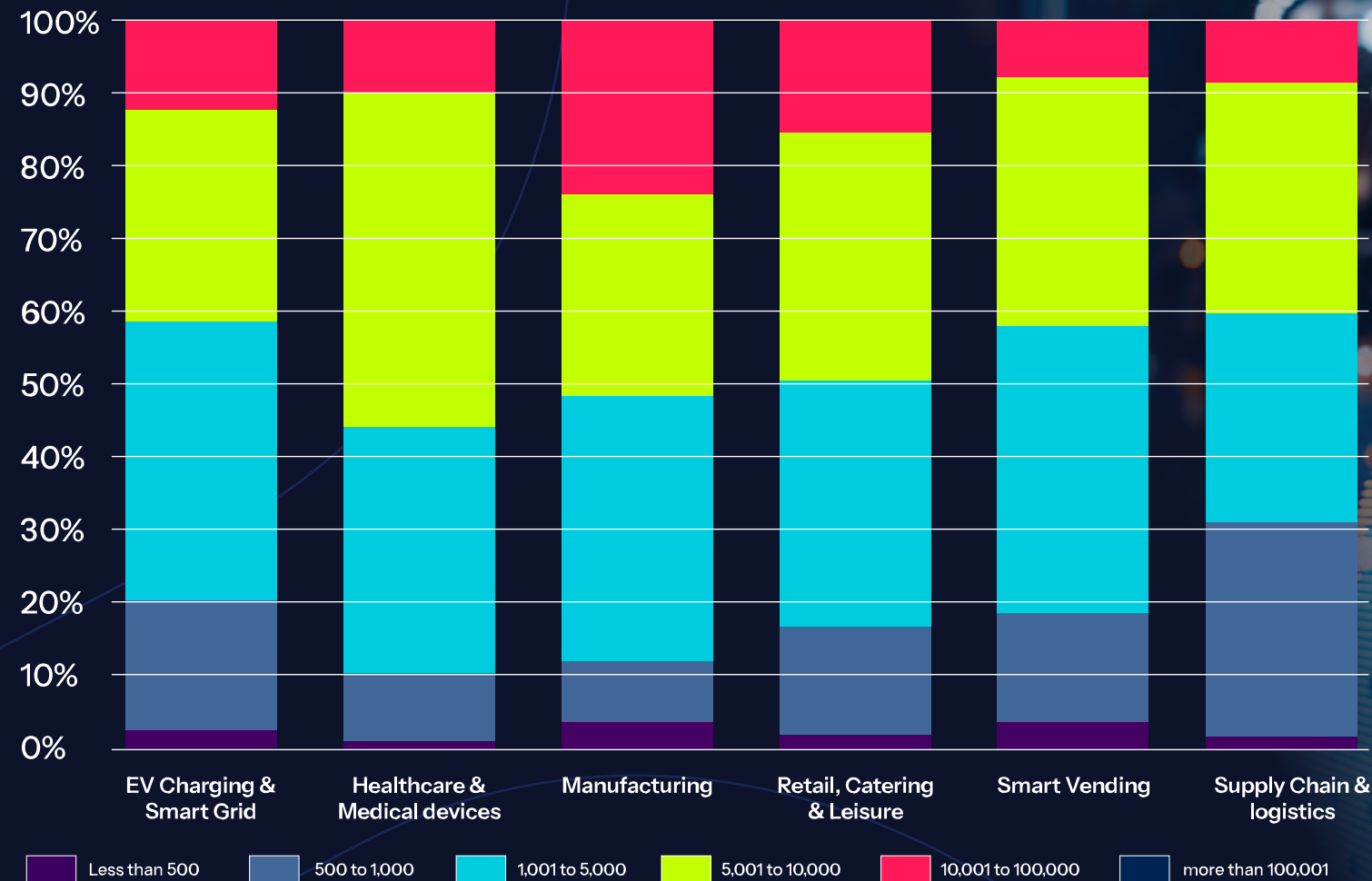
How IoT adoption varies by industry

IoT maturity varies significantly by sector.

Healthcare and Logistics enterprises operate relatively large, reliable estates. Manufacturing enterprises are expanding quickly but face vendor and performance complexity. EV Charging enterprises remain in an infrastructure scale-up phase. Smart Vending enterprises combine aggressive growth with strong demand for control. Retail, Catering & Leisure enterprises report very high provider satisfaction while increasingly prioritising edge intelligence and support.

“Smart Vending enterprises combine aggressive growth with strong demand for control..”

Adoption variety by industry



EV charging & smart grid

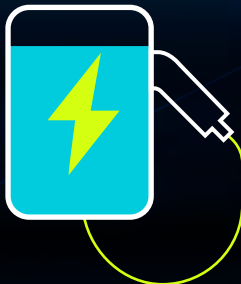
Growth remains strong, while budget confidence appears to have recovered materially from the more cautious 2025 picture.

EV Charging and Smart Grid organisations remain in an active infrastructure expansion phase. Most operate between 1,000 and 5,000 devices, but more than one-fifth still have fewer than a thousand in active deployment, indicating a less mature profile than an industry like Healthcare & Medical Devices or Logistics. Nevertheless, growth expectations are strong: 81.6% expect their device estates to increase over the next 18 months, and 77.4% plan to raise IoT investment over the next two years.

Sustainability is the IoT benefit most prominently selected, reflecting the role of connected infrastructure in supporting energy transition, load optimisation and the monitoring of distributed assets. The operational priority is resilient scale.

82%

expect their device estates to increase over the next 18 months.



Managing multiple SIM or connectivity vendors is the most commonly reported main challenge, while most organisations believe multi-network connectivity, managed services and near-total coverage are critical for business growth.

Average uptime most commonly sits between 81% and 90%, leaving a considerable gap between current performance and the reliability expected of public or business-critical infrastructure. Although clear majorities value managed connectivity and SGP.32 support, the sector is somewhat less emphatic than others across several measures. This may reflect its relative youth, differing deployment architectures or confidence that existing systems can support continued growth.

Over the next few years, EV Charging and Smart Grid adoption will be shaped by the ability to deploy internationally without creating fragmented supplier relationships.

Providers will need to offer resilient multi-network coverage, scalable orchestration, regulatory support and proactive management. The opportunity is substantial, but reliability and operational simplicity must improve as estates grow.

“Average uptime most commonly sits between 81% and 90%, leaving a considerable gap between current performance and the reliability expected...”

77%

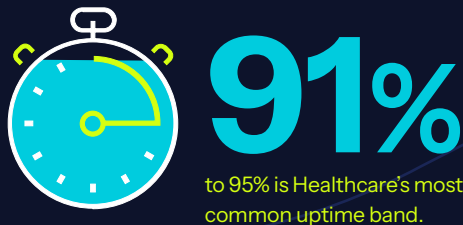
plan to raise IoT investment over the next two years.



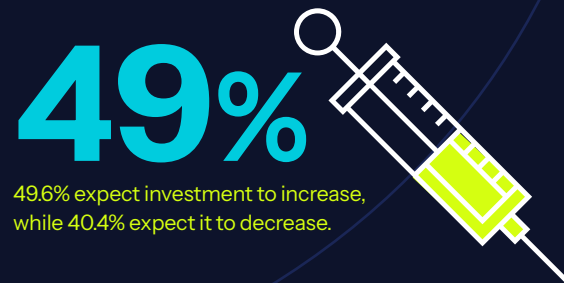
Healthcare & Medical Devices

Healthcare & Medical Device enterprises are among the most mature IoT adopters in the survey. Nearly half operate between 5,000 and 10,000 devices, while fewer than 1% have fewer than 500. Their most common uptime band is 91-95%, putting the sector ahead of many others, although none of the surveyed healthcare organisations reported average uptime at more than 98%.

Reliable multi-region connectivity is the leading operational challenge. Given that connected medical devices may travel between markets, operate in regulated environments or support clinically or operationally important functions, this does not come as a surprise. Near-100% connectivity, resilience, security and continuity during network changes are consequently treated as central business requirements.



Growth is positive but more measured than elsewhere. Healthcare organisations most commonly expect device numbers to rise by slightly less than double. Budget sentiment is notably cautious - 49.6% expect investment to increase, while 40.4% expect it to decrease. This makes Healthcare & Medical Devices the most divided industry in the survey in terms of future spending.



Sustainability is the sector's leading perceived IoT benefit, but some of the structural challenges surrounding IoT remain stubbornly persistent. Reported security breaches are broadly unchanged year-on-year, moving only slightly from 74.7% in 2025 to 73.3% in 2026, while the proportion expecting 2G and 3G shutdowns to affect their business has remained almost identical, at 74.3% compared with 74.7% last year.

Rather than emerging threats, these are established challenges that enterprises have yet to fully resolve.

For Healthcare & Medical Devices, where connected assets may remain in service for years and support critical applications, that makes security and lifecycle planning particularly important. Providers serving this market must therefore compete on demonstrable reliability, regulatory and roaming expertise, device-level support, security and long-term network migration. Healthcare may grow less aggressively than other industries, but the value and criticality of each connected device make service quality especially important.

“This makes Healthcare & Medical Devices the most divided industry in the survey in terms of future spending.”



Manufacturing

Growth intent has remained remarkably consistent at roughly 85–86%, suggesting sustained confidence rather than a sudden 2026 acceleration.

Manufacturing demonstrates some of the strongest momentum of adoption. Most surveyed manufacturers operate between 1,000 and 5,000 devices, 85.1% expect their estates to grow within 18 months (the highest proportion of any surveyed industry) and 70.6% plan to increase IoT spending over the next two years.

The sector views IoT as contributing to positive social and human impact as well as operational and commercial outcomes. Connected machines, sensors and production systems can improve safety, visibility, maintenance and resource use, but manufacturing also displays significant operational strain. Managing multiple connectivity or SIM suppliers is its leading challenge, and average uptime most commonly sits between 81% and 90%.

“The sector views IoT as contributing to positive social and human impact...”

Manufacturers strongly reject low-cost connectivity as a sustainable long-term strategy with more than four-fifths preferring a managed IoT provider.

This reflects the potentially high cost of downtime. Intermittent connectivity can disrupt production data, remote maintenance, asset monitoring and automated workflows.

Device-level reliability is particularly important. Hardware, modem and environmental issues can be magnified in factories, where equipment must operate for years under difficult conditions. The sector also shows strong demand for edge processing and Fixed Wireless Access, suggesting future architectures will use, and potentially combine, local intelligence with resilient cellular connectivity.

Manufacturing’s adoption outlook is highly positive, but growth could be constrained by fragmentation and performance inconsistency. Providers that combine device expertise, multi-network connectivity, unified management, responsive technical support and predictive service optimisation will be best placed to support the sector’s next phase.



“This reflects the potentially high cost of downtime. Intermittent connectivity can disrupt production data...”

Retail, Catering and Leisure

Retail, Catering & Leisure enterprises generally operate between 1,000 and 5,000 devices, with only 1.8% reporting fewer than 500. Eighty per cent expect their estates to grow over the next 18 months, although budget intentions are more restrained. 60.59% plan to increase spending, while 28.8% expect reductions.

The sector has the highest provider satisfaction in the survey, with 97.7% reporting that they are satisfied and no respondents reporting overall dissatisfaction. This industry also reports the strongest unaided provider awareness, suggesting a relatively informed and active market. Awareness, however, does not mean the sector has solved every operational problem. Access to technical IoT support is its most common main challenge, and more than four-fifths agree that device-level issues are a leading cause of failure.



“The sector views IoT as contributing to positive social and human impact as well as operational and commercial outcomes.”

Retail organisations place particularly strong emphasis on edge intelligence, sustainability and direct connectivity control.

This reflects environments containing payment terminals, kiosks, digital signage, refrigeration systems, ‘smart kitchens’ and customer-facing devices that may need rapid local processing and high availability. 5G Fixed Wireless Access solutions have also proven to be attractive where sites need fast deployment, backup connectivity or alternatives to delayed fixed-line installations.

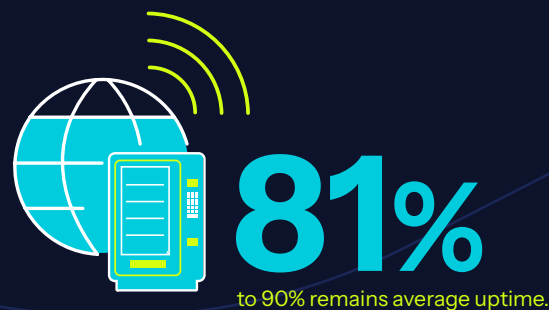
Future adoption will be driven by the need to operate large numbers of distributed, customer-facing devices with minimal on-site intervention. Providers must therefore combine high availability with strong support, remote diagnostics, rapid deployment and commercial stability. Retail customers appear broadly satisfied, but they will increasingly expect providers to contribute to device intelligence, resilience and business continuity.

Smart vending

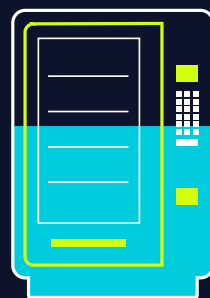
The 2025 report described consolidation/cooling; the 2026 data shows 79.3% expecting estate growth and 72.4% increasing budgets.

Smart Vending is one of the most active and operationally distinctive industries in the survey. Most enterprises operate between 1,000 and 5,000 devices, fewer than 1% have fewer than 500, and 79.3% expect deployment growth within 18 months. More than a quarter anticipate their estates will grow by more than double and up to triple. Investment intentions are similarly strong, with 72.4% expecting budgets to rise.

The sector's leading benefit is operational cost reduction, reflecting the value of remote stock monitoring, predictive maintenance, cashless payments and fewer unnecessary field visits.



However, reliable multi-region connectivity is its most commonly cited primary challenge. Average uptime remains concentrated between 81% and 90%, which is potentially problematic for geographically dispersed, unattended machines that depend on connectivity for revenue and serviceability.



65%
would choose greater control
even if it introduced complexity.

Smart Vending shows the strongest preference for direct control. 65.5% would choose greater control even if it introduced complexity. At the same time, nearly three-quarters say they would prefer a managed service provider and regard multi-provider management as time-consuming. This indicates a desire for strategic control (visibility, policies, commercial options, the ability to change networks) without assuming the full operational burden.

“The sector is also highly receptive to Fixed Wireless Access and increasingly views connectivity as supporting business-critical AI infrastructure.”

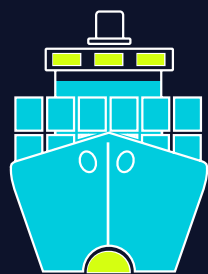
The sector is also highly receptive to Fixed Wireless Access solutions and increasingly views connectivity as supporting business-critical AI infrastructure. Future growth will depend on multi-network resilience, remote diagnostics, automation and edge intelligence. Providers that give vending operators granular control through a managed platform are likely to align particularly well with this market.

Supply chain & Logistics

Supply Chain & Logistics priorities continue to evolve as one of the most mature IoT sectors.

In 2024, the sector was strongly focused on competitive advantage and revenue, while sustainability became the leading benefit in 2025. In 2026, smart-product diversification comes to the fore, suggesting a shift towards embedding connected capabilities more directly into products and services. Growth appetite also remains strong, with more than three-quarters expecting device estates to increase and 70.8% planning higher investment.

Most organisations operate between 5,000 and 10,000 devices, and fewer than 1.5% have fewer than 500. More than three-quarters expect device growth within 18 months, while 70.8% plan to increase spending over two years, typically by more than 25%.



70%

plan to increase spending over two years, typically by more than 25%.

The sector sees smart-product diversification as its leading IoT benefit, reflecting the ability to add tracking, condition monitoring and connected services to assets and shipments. Access to technical IoT support is its most commonly identified challenge, although its most frequent uptime band of 91-95% is stronger than most industries.

Supply Chain & Logistics also differs from other sectors in its attitude towards control. A narrow majority prefers simpler managed connectivity even where that means less direct control. This potentially reflects the difficulty of coordinating devices, routes, carriers, warehouses and jurisdictions, where operational simplicity can be more valuable than managing each connectivity decision internally.

Provider satisfaction is particularly high, with 95.6% satisfied and more than half extremely satisfied. Yet the sector still values access to many operators, managed SGP.32 orchestration and rapid connectivity where fixed lines are unavailable. Its future requirements will centre on seamless international coverage, asset mobility, reliable handovers, simplified management and specialist support capable of resolving problems across complex distributed operations.

“Supply Chain & Logistics also differs from other sectors in its attitude towards control.”

95%

satisfied and more than half extremely satisfied with their connectivity.



Regional insights: UK vs. US five-year IoT adoption trends (2021–2026)

The UK and US provide a useful comparison because the two markets are broadly aligned. UK enterprises operate slightly larger estates, report somewhat stronger uptime and express greater urgency around resilience, sustainability, managed services and network sunsets. US organisations show marginally stronger growth intentions and better unaided provider awareness, while investment expectations are almost identical across the two regions.

Deployment scale

UK deployments are generally larger, with 38.2% of UK organisations operating between 5,000 and 10,000 devices. In the US, the average estate is smaller, with 36.2% operating between 1,000 and 5,000 devices. Very few organisations in either region have fewer than 500 connected devices, indicating mature production adoption in both markets.



Growth intentions

Growth expectations are strong in both markets, although the US is marginally more optimistic. Some 27.8% of US enterprises expect to double their estates, compared with 24.7% in the UK. Only 8.3% of US organisations anticipate reductions, versus 12.8% in the UK. Budget-growth intentions, however, are almost identical.



Different Stages of Scale

UK enterprises most commonly manage between 5,000 and 10,000 devices, whereas US organisations are most frequently in the 1,000–5,000 range. UK respondents also report somewhat stronger average uptime and are marginally more likely to reach the highest reliability bands. This suggests that the average UK estate may be further along its scaling

journey, although neither market is consistently achieving genuinely mission-critical availability.

Only 1.3% of UK respondents and 1.0% of US respondents report uptime of more than 98%. Across an estate of thousands of connected devices, even relatively small gaps in availability can therefore translate into significant periods of lost connectivity, reinforcing why every percentage point of uptime matters as IoT becomes more deeply embedded in business-critical operations.

UK organisations also show greater concern across many of the operational statements tested. They are more likely to regard near-total global connectivity as critical, identify device issues as the cause of project failure, prefer managed providers and expect disruption from 2G and 3G shutdowns.

These differences may reflect greater experience of the operational problems that emerge as estates mature.

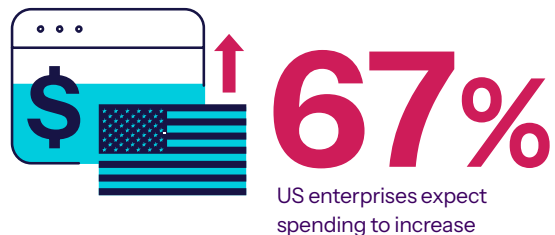
For providers, the UK opportunity may therefore be centred on improving established deployments, raising uptime, simplifying fragmented estates, migrating legacy devices and introducing orchestration. The US opportunity may combine optimisation with a greater proportion of first-wave scaling. In both markets, however, the central need is similar, translating growing device numbers into dependable operational performance.

Growth Expectations Remain Strong

US businesses are marginally more optimistic about device growth. Approximately 27.8% expect to double their estates during the next 18 months, compared with 24.7% in the UK. The proportion expecting contraction is also lower in the US with 8.3% against 12.8% in the UK.

This does not indicate a dramatic divergence (the majority in both countries expect growth) but it suggests the US market may contain a somewhat larger pool of organisations entering an accelerated scaling phase. The UK's slightly greater incidence of planned reductions could reflect consolidation, estate rationalisation or the retirement of older deployments rather than declining confidence in IoT itself.

Budget intentions reinforce the overall similarity. Some 65.8% of UK enterprises and 67.2% of US enterprises expect spending to increase. This near alignment means that regional strategies should not treat one market as fundamentally expansionary and the other as cautious. Instead, propositions should recognise subtle differences in maturity.



US messaging may place more emphasis on enabling rapid growth and international expansion; UK messaging may resonate more strongly when focused on optimisation, resilience and lifecycle management. Across both, the data supports a positive investment outlook.

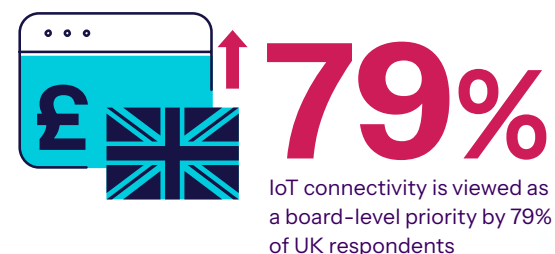
The Connectivity Gap Challenge

UK respondents consistently register stronger agreement across connectivity and lifecycle issues. Seventy-eight per cent say near-100% global connectivity is crucial, compared with 71.2% in the US. Similarly, 80.5% of UK organisations attribute most IoT failures to device-level issues, versus 72% of US organisations.

“80.5% of UK organisations attribute most IoT failures to device-level issues...”

UK respondents are also more likely to prefer managed connectivity, see multi-provider management as time-consuming, expect an impact from 2G and 3G shutdowns and recognise significant potential value from Fixed Wireless Access. IoT connectivity is viewed as a board-level priority by 79% of UK respondents, against 72.2% in the US.

The pattern suggests UK enterprises may feel operational pressures more intensely, perhaps due to their average deployments being larger or due to international connectivity and roaming complexity being more prominent. It does not mean US enterprises consider these issues unimportant. Agreement remains above 70% in most cases.



“The pattern suggests UK enterprises may feel operational pressures more intensely, perhaps due to their average deployments being larger...”

Different Measures of IoT Value

UK organisations most commonly identify positive social or human impact as a benefit of IoT, selected by 40.0%. US organisations most commonly highlight contribution to sustainability goals, at 35.2%. The differences are not absolute. Both outcomes matter in both countries, but they indicate distinct ways in which IoT value may be framed internally.

In the UK, connected technology may be more readily positioned in terms of service quality, safety, accessibility, societal outcomes or employee and customer experience. In the US, environmental efficiency, energy optimisation and progress towards sustainability targets may provide a stronger lead narrative.

“they indicate distinct ways in which IoT value may be framed internally.”

These distinctions matter for how providers and enterprise teams construct business cases. A generic message focused only on cost reduction may miss the broader strategic motivations driving adoption.



UK organisations most commonly identify positive social or human impact as a benefit of IoT.

IoT investment now spans commercial, operational, environmental and social goals.



US organisations most commonly highlight contribution to sustainability goals, at 35.2%.

Providers should therefore demonstrate how the same connectivity foundation can support multiple types of value. Improved reliability and operational efficiency, but also reduced environmental impact, better customer or end-user outcomes and more sustainable product design. Regionally adapted proof points may be more persuasive than a uniform global proposition.

“Providers should therefore demonstrate how the same connectivity foundation can support multiple types of value.”

Our recommendations

1 Build a business case around industry-specific value and operational outcomes

Getting the fundamentals right matters more as IoT estates grow. That makes clarity around the outcome of every project essential, and there is no single definition of IoT value.

In 2026, EV Charging and Healthcare & Medical Devices place particular emphasis on sustainability, Smart Vending prioritises cost reduction, and Supply Chain & Logistics focuses on connected-product diversification.

Every deployment should be linked to a limited number of measurable outcomes. Connectivity metrics should then be connected directly to those outcomes.

“EV Charging and Healthcare & Medical Devices place particular emphasis on sustainability...”

A healthcare deployment may prioritise regulatory expertise and reliability, while logistics may value roaming flexibility and managed simplicity.

Clear commercial and operational goals make it easier to justify investment, measure success and avoid scaling deployments that generate activity without sufficient business value.

“Clear commercial and operational goals make it easier to justify investment, measure success...”

As IoT moves deeper into business-critical operations, enterprises need to be clearer than ever about what value they expect, how they will measure it and what level of performance is required to deliver it.



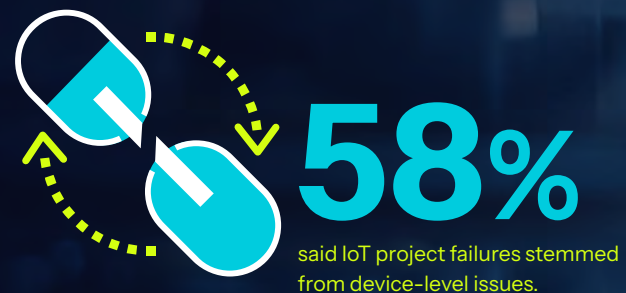
2 Address device reliability before deployment.

Reliability has been one of the most consistent themes across our State of IoT Adoption research. In 2024, fewer than 0.5% of organisations achieved connectivity uptime of higher than 98%; that rose to only 2% in 2025, and stands at just 1.2% in 2026.

The device itself remains a major factor. In 2024, 58% said IoT project failures stemmed from device-level issues, rising to 76% in 2025 and 76.3% in 2026. Enterprises should therefore design for resilient connectivity from the outset, considering modem firmware, power management, network behaviour, enclosure design and deployment environment.

“Enterprises should therefore design for resilient connectivity from the outset...”

Connectivity providers, device engineers and application teams should collaborate early, testing devices across intended countries, operators and network technologies.



Remote diagnostics, firmware management and recovery mechanisms should also be built in to reduce field interventions and support costs throughout the device lifecycle.

“Connectivity providers, device engineers and application teams should collaborate early...”

Six years of research point to the same conclusion: connectivity performance cannot be fixed by connectivity alone. Reliable IoT starts with getting the device, network architecture and testing strategy right before deployment.

3 Retain strategic control, outsource operational complexity

The apparent tension between connectivity control and managed services is best resolved by separating governance from execution. Enterprises want authority over policy, suppliers, costs, data and network decisions, without necessarily managing profiles, platforms and troubleshooting themselves.

Organisations should determine which responsibilities are strategically important to retain.

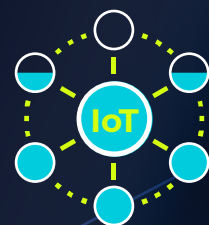
Internal teams might own device architecture, risk, commercial governance and performance targets, while specialists manage provisioning, profile orchestration, network optimisation and operational intervention.

“Organisations should determine which responsibilities are strategically important to retain.”

More than three-quarters believe self-management would be resource-intensive, making managed orchestration an attractive way to access greater connectivity flexibility without building a permanent internal operations capability.

“making managed orchestration an attractive way to access greater connectivity flexibility...”

However, contracts and platforms should retain transparency, policy controls and exit flexibility to avoid supplier lock-in.



75%

believe self-management would be resource-intensive.

4 Design for multi-network resilience

Network choice, fallback and switching should be architectural requirements from the outset. Multi-network connectivity is now the leading future-proofing priority, while more than half of organisations still report average uptime of 90% or lower. Coverage alone does not protect against congestion, roaming restrictions or changes in network availability.

Enterprises should understand how devices respond when their preferred network becomes unavailable, how quickly alternatives can be selected and whether connectivity can be optimised remotely.

“Coverage alone does not protect against congestion, roaming restrictions or changes in network availability...”

The business case should account for the cost of downtime, field visits, lost transactions and unavailable data, with resilience governed through meaningful SLAs.

“The business case should account for the cost of downtime, field visits, lost transactions and unavailable data...”

Multi-network connectivity cannot eliminate every failure, but it can reduce dependence on individual operators and provide greater flexibility as conditions change.



5 Make security and network migration strategic priorities

Nearly three-quarters of enterprises report experiencing an IoT security breach in the previous year (2025). Similar numbers were reported in 2025 (75%) for security breaches in 2024, compared with 50% reported in 2024 for security breaches in 2023. Security is therefore an established business risk, not simply a technical concern.

Protection should extend across device identity, encryption, access control, network segmentation, patching, anomaly detection and incident response, with clear responsibility across enterprises, manufacturers, connectivity providers and application platforms.

Eseye's AnyNet+ eSIM supports secure device identity and connectivity through GSMA-compliant eUICC technology, secure over-the-air profile management, multi-IMSI resilience and localised network access.

“Security is therefore an established business risk, not simply a technical concern.”



75%

of enterprises report experiencing an IoT security breach.

Infinity CMP extends these controls through private networking, VPNs, Private APNs, IMEI locking, firewalling, policy-based orchestration and monitoring.

“Protection should extend across device identity, encryption, access control, network segmentation, patching, anomaly detection and incident response.”

Security and network longevity should therefore have clear ownership, investment and governance at business level.

6 Prepare for network sunset now

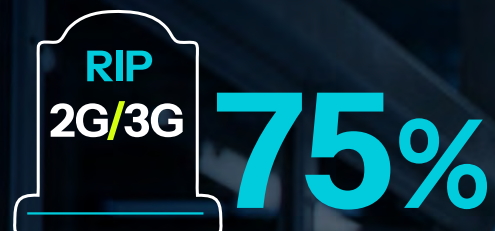
2G and 3G retirement is already a business-continuity issue for IoT. Almost three-quarters (74.3%) of enterprises expect network shutdowns to affect their business, while many connected devices are designed to remain operational for years.

Enterprises should identify devices dependent on legacy networks and establish migration plans covering hardware compatibility, replacement cycles, testing, costs, market-specific sunset dates and continuity arrangements. Waiting until retirement deadlines approach risks turning a planned migration into an operational problem.

“Enterprises should identify devices dependent on legacy networks and establish migration plans...”

Network flexibility should also be designed into future deployments, giving devices a clear path to alternative connectivity and ensuring services can remain operational as networks change.

“...giving devices a clear path to alternative connectivity and ensuring services can remain operational.”



of enterprises expect network shutdowns to affect their business.

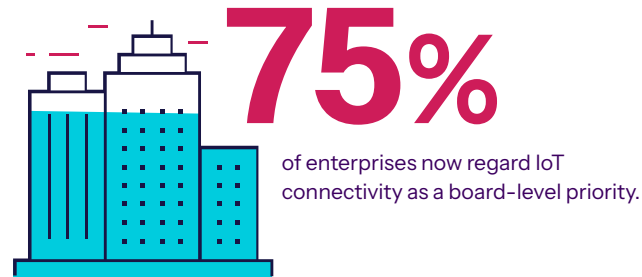
Conclusion

Six years of State of IoT Adoption research show that the fundamentals of successful IoT have remained remarkably consistent. Devices must work. Connectivity must be resilient. Security must be designed in. And businesses need access to the expertise required to manage increasing complexity.

What has changed is the scale. Therefore, so has the consequence of getting those fundamentals wrong. It is telling that more than three quarters (75.6%) of enterprises now regard IoT connectivity as a board-level priority. As connected technology moves deeper into customer-facing products and business-critical services, connectivity decisions increasingly carry consequences for the wider organisation.

“What has changed is the scale. Therefore, so has the consequence of getting those fundamentals wrong.”

Today's enterprises are deploying thousands of devices, increasing investment and embedding IoT into business-critical operations.



At that scale, a small gap in uptime becomes significant downtime, fragmented connectivity becomes an operational burden, and a firmware or network-lifecycle decision made during design can create problems years later.

The opportunity for enterprises is therefore not simply to deploy more IoT, but to deploy it better.

That means designing for resilience from day one, building in security and network flexibility, using multi-network connectivity to reduce dependency, retaining strategic control while outsourcing unnecessary operational complexity, and measuring success against clear business outcomes. The technology to achieve this already exists.

The next phase of IoT will be defined by how effectively enterprises decide to operationalise it

“The opportunity for enterprises is therefore not simply to deploy more IoT, but to deploy it better.”

About Eseye

As a global leader in IoT Connectivity, eSIM Orchestration, and Fixed Wireless Access (FWA), Eseye empowers Enterprises and MNOs to deliver high-performing, resilient global connectivity.

We provide the expertise to integrate, manage, and orchestrate IoT and wireless connectivity for any scale or complexity, intelligently optimising connections to millions of devices and locations across 190 countries, leveraging over 800 networks with near-100% uptime.

Our innovative eSIM Orchestration technology enables advanced federated localisation, allowing Enterprises and MNOs to seamlessly manage eSIM profiles and FWA deployments across regions and platforms, ensuring global scalability with localised precision.

Methodology

The research was conducted by Censuswide, among a sample of 1,200 Respondents in companies employing 500+ people (600 based in the UK, 600 based in the US).

The data was collected between 09.06.2026 - 15.06.2026.

With decades of delivery experience for companies including TELUS, AT&T, MTN, Amazon, and Shell, Eseye provides fully managed, secure, and future-proofed IoT and FWA connectivity solutions that support mission-critical applications and long-term success.

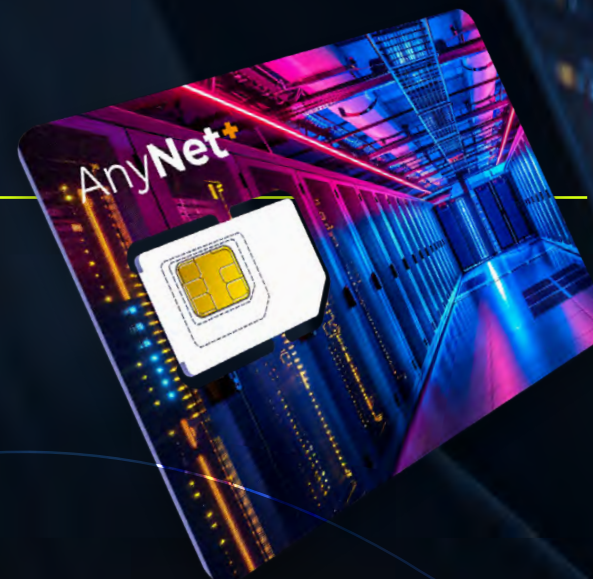


Nobody does IoT connectivity better.

[Learn more](#)

Censuswide is a member of the Market Research Society (MRS) and the British Polling Council (BPC), and a signatory of the Global Data Quality Pledge. We adhere to the MRS Code of Conduct and ESOMAR principles.

“...across 190 countries, leveraging over 800 networks with near-100% uptime.”





Go beyond

Talk to Eseye about
your **IoT journey** today.

Contact Us

