Memfault

RESEARCH REPORT

The IoT Visibility Gap

New data shows the cost of scaling in the dark

Executive Summary

Based on a 2025 survey of 200 U.S.-based IoT decision-makers, this report reveals that device observability gaps are driving up support costs, delaying product launches, and putting customer trust at risk. Despite widespread adoption of observability solutions, most teams still lack the visibility needed to manage devices effectively at scale. The cost of these gaps is high:

Finding 01: Lack of visibility is a hidden tax on IoT teams. Limited device insight forces teams to spend more on field fixes than on new product R&D, with 3 in 4 mid-sized companies seeing support costs surge and innovation stall.

Finding 02: Customers are the de facto QA team. 1 in 3 companies learn about issues from complaints or returns, hurting satisfaction and brand perception.

Finding 03: Visibility gaps are a barrier to scaling. 77% say poor observability limits their ability to scale; 57% of mid-sized companies report launch delays.

To compete in today's market, IoT teams need end-to-end visibility across their fleets to reduce risk, accelerate delivery, and build more resilient products.

This admission highlights urgent questions for product leaders. As devices become more connected, do IoT teams have the visibility to manage them effectively at scale? Or are their customers beating them to device issue discovery?

By 2030, connected devices worldwide are expected to grow to over 40 billion — more than tripling from 2020 levels.[1] But is device observability keeping pace with this growth?

In Q2 2025, Memfault surveyed 200 U.S.-based IoT decision-makers to better understand the current state of device observability and the business impact of visibility gaps. While all 200 respondents reported some form of observability solution, critical gaps persist.

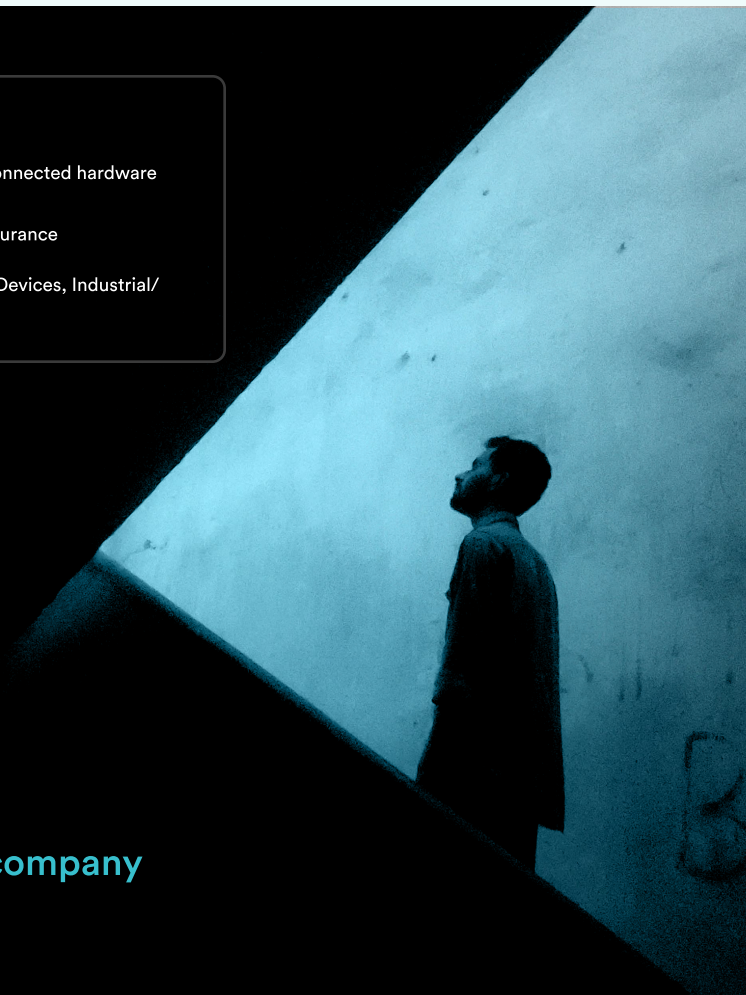
[1] https://iot-analytics.com/wp-content/uploads/2024/09/INSIGHTS-RELEASE-Number-of-connected-IoT-devices-vf.pdf

Respondent Profile

Qualifier 200 U.S.-based IoT leaders at companies with 100+ employees that develop connected hardware

Departments Engineering, Firmware Development, Product Management, Quality Assurance

Industries Consumer Electronics, Automotive, Communications/Networking, Medical Devices, Industrial/Manufacturing, Agriculture/Environmental Sensors



"A significant amount of our support center activity stems from issues we could have proactively prevented."

– VP at an agriculture/environmental sensors company

Finding 01

Lack of visibility is a hidden tax on IoT teams

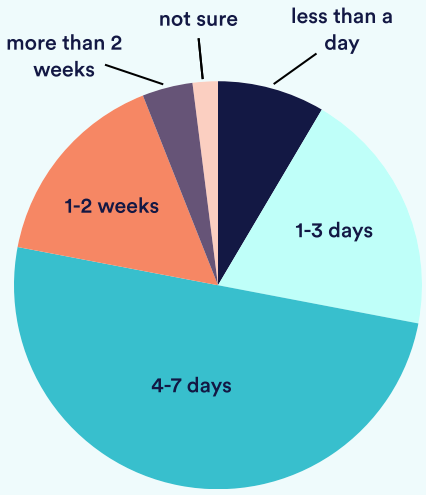
When engineering teams can't see what's happening on deployed devices, **they pay in time and effort.** Recurring operational burdens quietly accumulate after launch, turning maintenance into an ongoing cost center. In effect, lack of visibility continuously drains resources that could have powered the next innovation.

Many IoT leaders describe this as an unseen drag on productivity. One VP in automotive put it bluntly: **"We've spent more on field engineer travel this year than on new product R&D."** In other words, time lost to chasing down issues is time (and money) diverted from roadmap progress.

Our research shows that this hidden tax hits mid-sized companies the hardest. In fact, **roughly three-quarters of mid-market respondents said that limited visibility significantly increased their support and field operation expenses**, a higher share than any other segment. This makes sense: mid-sized IoT organizations often have large enough fleets to generate constant issues, but lack the deep bench of specialized engineering resources that large enterprises can rely on to absorb the workload. The result is a disproportionate impact on their engineering efficiency and support budgets.

Post-deployment debugging costs are a predictable symptom of poor device visibility. Teams that use third-party IoT monitoring and observability tools experience dramatically less downstream spend. Surveyed **companies with dedicated device observability platforms reported far lower support costs and fewer firefighting hours** than those relying on ad-hoc monitoring.

On average, how long does it take your team to identify the root cause of a field-reported issue?



"We burn more time debugging in the field than we do developing new features."

— VP, Consumer Electronics

Finding 02

Customers are the de facto QA team

One-third of IoT leaders rely on customer complaints as the first point of discovery for in-field problems, while **35% learn about device issues through physical device returns**. As one director of a mid-size consumer electronics company put it, “We’ve faced a high level of customer complaints because we weren’t able to detect issues in the field.”

Worse, **15% of enterprises discover device issues only after they surface on public review platforms** like Amazon. “We’re losing customer trust due to unresolved device issues,” a C-Suite leader at a mid-size automotive enterprise told Memfault.

When device issues are first detected by your customers instead of your tools, the damage quickly compounds. Customer trust erodes. Upsell opportunities vanish. Brand reputation suffers. Still, many IoT enterprises continue operating in this reactive mode, exposing that their observability tools aren’t delivering the visibility needed to get ahead of problems.

Top 5 ways device issues are discovered[2]

52%
Internal QA/field testing

50%
Automated fleet monitoring

40%
Remote logs or telemetry

35%
Physical device returns

33%
Customer complaints/ support tickets

[2] Answers are based on a “Select All That Apply” question.

Finding 03

Visibility gaps are a barrier to scaling

77% of IoT companies say insufficient device observability is a barrier to overall business growth. The consequences directly impact operations: Of the enterprises that report visibility gaps as a challenge to scaling, **48% have experienced a delayed product launch within the last year** directly due to device issues, while **38% report a product recall** in the same timeframe.

Mid-sized companies (501-1,000 employees) are hit hardest, with **57% reporting launch delays** tied to visibility gaps. For organizations like these, which are often centered around a single product line, visibility gaps can be existential. A missed launch window, for instance, could mean jeopardizing a funding milestone or missing critical seasonal demand — consequences that could threaten the business' long-term viability.

Fleet blind spots are costing IoT teams time, trust, and traction. If your observability tooling can't help your team see and solve device issues in real time, it's putting your roadmap, revenue, and reputation at risk.

77%

of IoT companies say insufficient device observability is a barrier to overall business growth.

38%

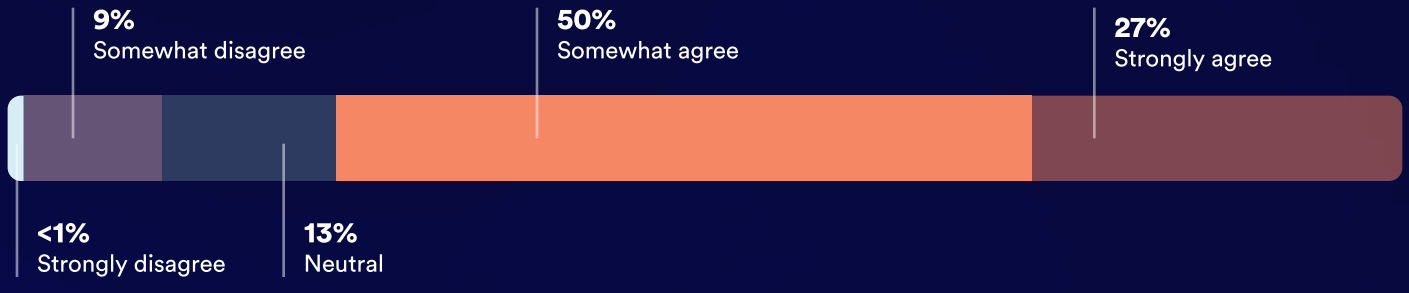
report a product recall within the last year.

57%

of mid-sized companies report launch delays tied to visibility gaps.

"A lack of real-time visibility is a barrier to our company scaling."

Response Breakdown



Memfault

Toward a more observable future

IoT organizations face critical visibility gaps impacting scaling, customer trust, and operational efficiency. And while all 200 survey respondents report having some type of observability solution in place, our findings suggest that **current tooling is falling short.**

The type of observability solution in use — whether built in-house, open source, or third party — appears to play some role in the extent of these visibility gaps. **Companies using in-house observability solutions, for instance, are over twice as likely as those using third-party tools to attribute business scaling challenges to a lack of real-time device visibility (43% vs. 20%).** Similarly, those using in-house tools are much less likely to characterize their products as "extremely reliable" (11% vs. 29%).

However, our results point to insufficient observability largely transcending solution type — revealing an overall observability infrastructure that isn't keeping pace with today's product development lifecycles. When IoT teams manage devices reactively, the consequences are clear: Customers report device issues first. Updates introduce unnecessary risk. Product launches get delayed, and device recalls occur.

As complexity rises and tolerance for device issues shrinks, better observability will become essential — and just collecting device data won't be enough. **To proactively address issues, teams need complete, real-world visibility into system behavior across all device states and in every deployed unit.** With this level of observability, teams can build more resilient products — and a brand reputation that endures.

Ready to close the visibility gap? Visit memfault.com to see how leading embedded teams scale smarter with full-stack device observability.