WanAware

THE 2025 TELECOM OBSERVABILITY BENCHMARK REPORT.

www.wanaware.com

Executive Summary

Telecommunications is the backbone of modern economies, powering everything from remote work and telemedicine to smart cities and global commerce. Yet despite more than $300 billion in infrastructure investments since 2018, the industry faces a growing paradox: capital expenditures (CapEx) are rising, while returns on invested capital (ROIC) have dropped 10–15% (North America and Europe).

Our new survey of 180 telecom leaders reveals a core reason for this disconnect: network observability has not kept pace with infrastructure growth. While the industry pours billions into AI, 5G, and edge innovation, much of that investment is at risk due to persistent visibility gaps, especially in rural expansions, shared infrastructure, and next-gen deployments.

Intelligent observability is no longer a “nice to have.” It is the invisible foundation of the telecom AI revolution. Without it, the industry's most critical initiatives—from automation and sustainability to XaaS models and real-time security—will fail to deliver their promised returns. This report explores why solving the visibility gap is the only path forward.

The Investment vs. Visibility Disconnect

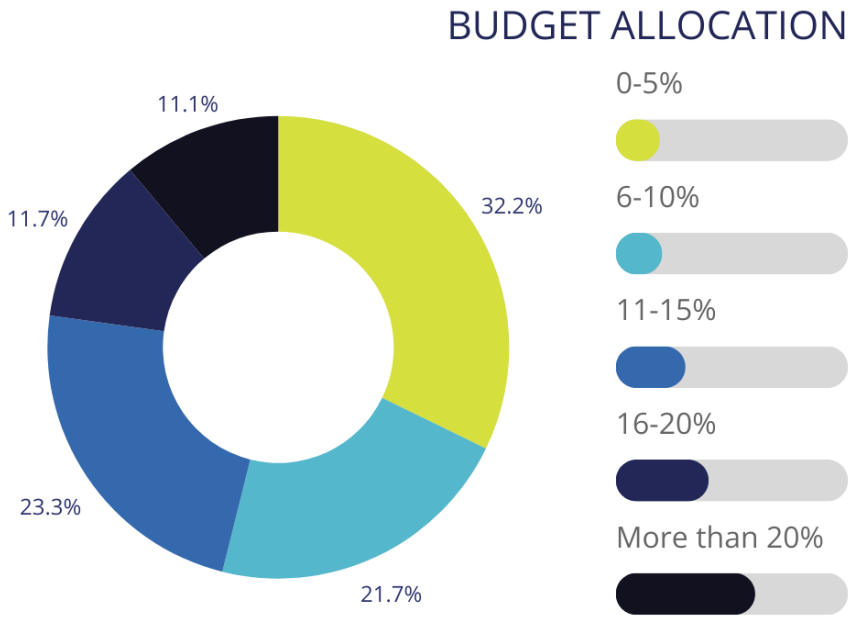
As telecom operators double down on building the networks of the future, many are doing so without a clear view of what’s happening under the hood. Despite steady or rising infrastructure investments, the tools designed to monitor and manage these assets aren’t receiving the same level of attention—or funding.

More than half of telecom leaders—54%—allocate 10% or less of their infrastructure budget to observability tools. At the same time, 56% report that their capital expenditures have either remained flat or increased over the past two years. This disconnect between spending and visibility is creating blind spots that can hinder performance, slow innovation, and open the door to security risks.

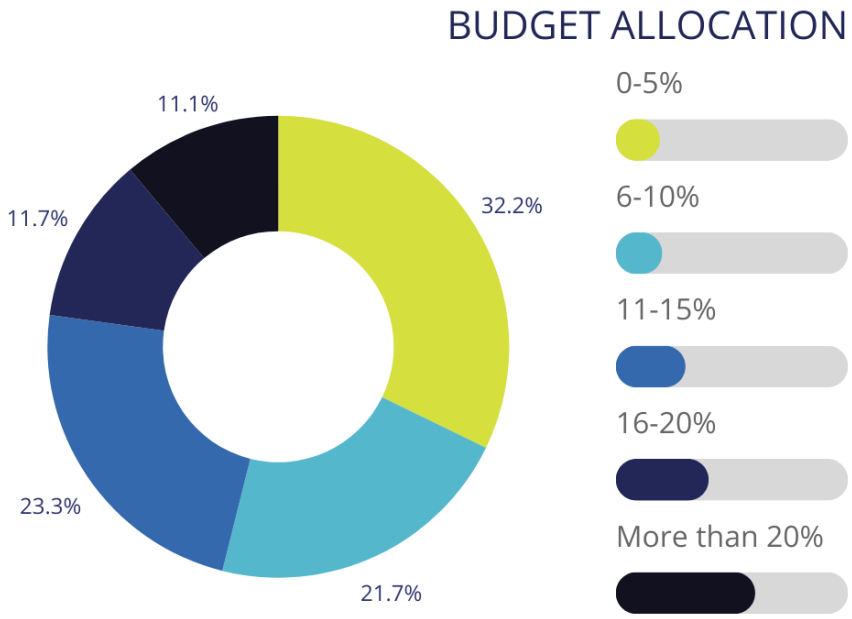
However, only a small fraction, just 7%, say they have full visibility (91–100%) into their current infrastructure. In fact, over 62% of respondents admit they can see less than half of their own assets through their existing monitoring tools, highlighting a significant visibility gap.

OF NOTE: While only 11% of respondents are allocating a substantial portion (>20%) of their budget to observability, this small but focused group may gain competitive advantages in uptime, security detection, and infrastructure management.

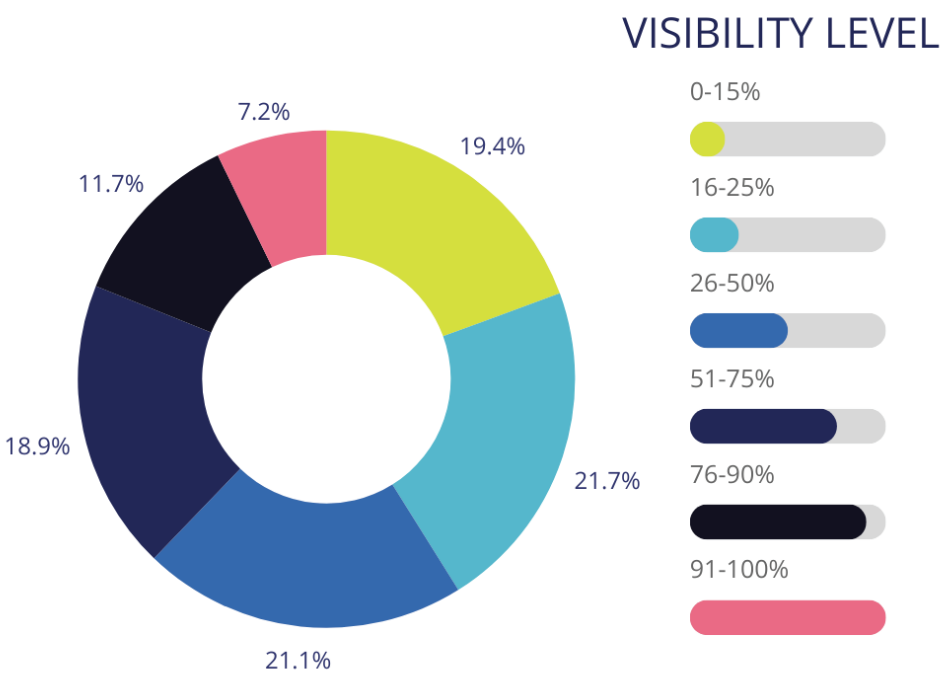
What percentage of your telecom infrastructure budget was allocated to network monitoring and observability tools in the past 12 months?



How has your capital expenditure on network infrastructure changed in the past 24 months?



Based on your existing network monitoring and observability stack, what percentage of your overall infrastructure assets do you believe you have visibility into today?



Insight: Despite the urgency to modernize, network observability has yet to become a strategic priority for many telecom leaders—often overshadowed by other pressing investments due to unclear ROI, budget constraints, or lack of executive buy-in.. This creates a risky imbalance: while observability is essential to enabling AI, automation, and next-gen deployments, the pace of network expansion has clearly outstripped its implementation. The result is a growing "visibility debt"—a blind spot in performance and security that threatens providers' ability to deliver on quality of service, ensure security, and realize long-term ROI as AI-driven initiatives scale.

> *"There's a clear disconnect between where telecom dollars are going and where they're most urgently needed. While spending on infrastructure remains strong, observability is being left behind. You can't manage what you can't see—and with over 60% of leaders admitting they have visibility into less than half of their assets, we're looking at a growing blind spot that puts performance, security, and reliability at risk."*
>
> — Jeff Collins, CEO of WanAware

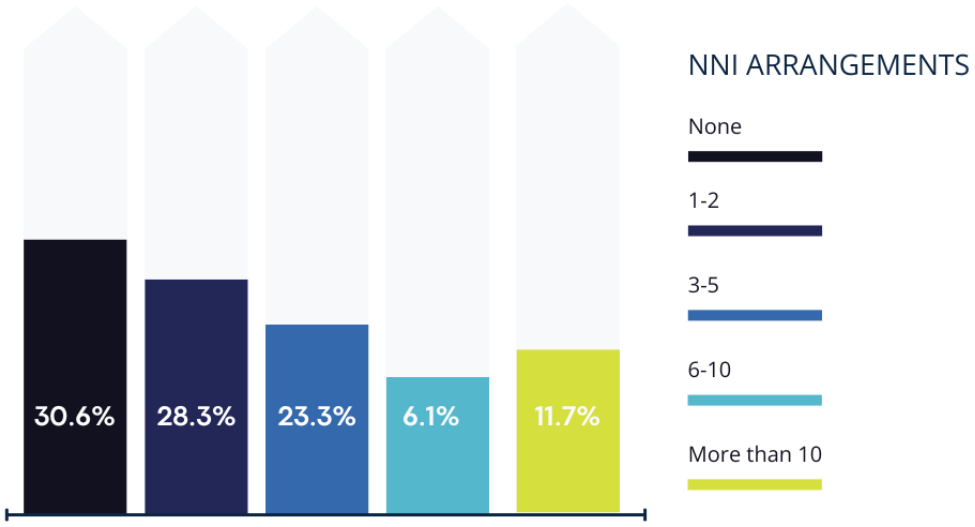
Shared Infrastructure, Shared Risk

As telecom networks become increasingly interconnected, shared infrastructure agreements like network-to-network interfaces (NNIs) are now the norm rather than the exception. These partnerships promise greater coverage, efficiency, and flexibility—but they also introduce new layers of complexity and risk. While NNIs offer strategic benefits, they often come at the cost of reduced visibility and control.

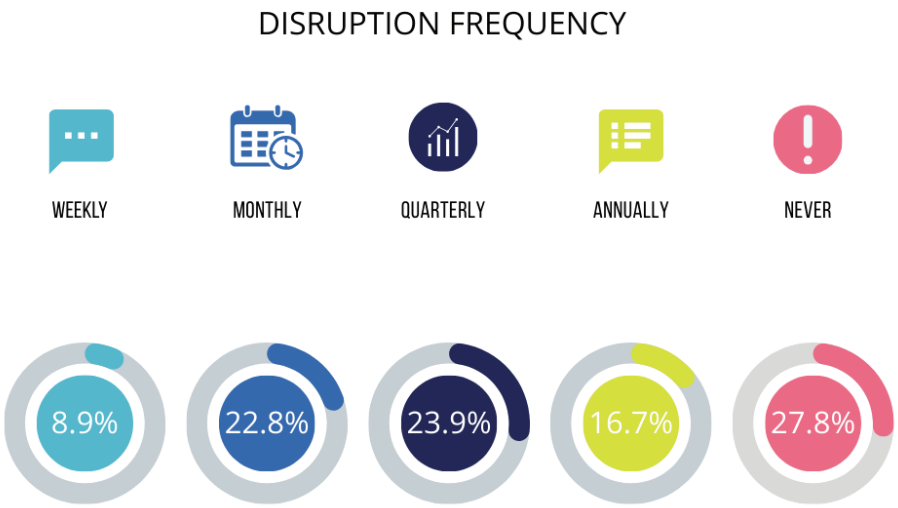
While NNIs offer strategic benefits, they often come at the cost of reduced visibility and control. Nearly 70% of respondents participate in at least one NNI arrangement, with 11% engaged in more than 10 such partnerships. Yet when something goes wrong, pinpointing the issue becomes exponentially harder. In fact, 55% of operators report experiencing service disruptions that could have been prevented with better visibility—nearly 9% say these disruptions happen as often as once a week.

Security is also a concern. For 36% of respondents, fewer than 20% of security incidents are detected by their own monitoring systems, suggesting that shared infrastructure isn't just a technical challenge—it's a security blind spot as well.

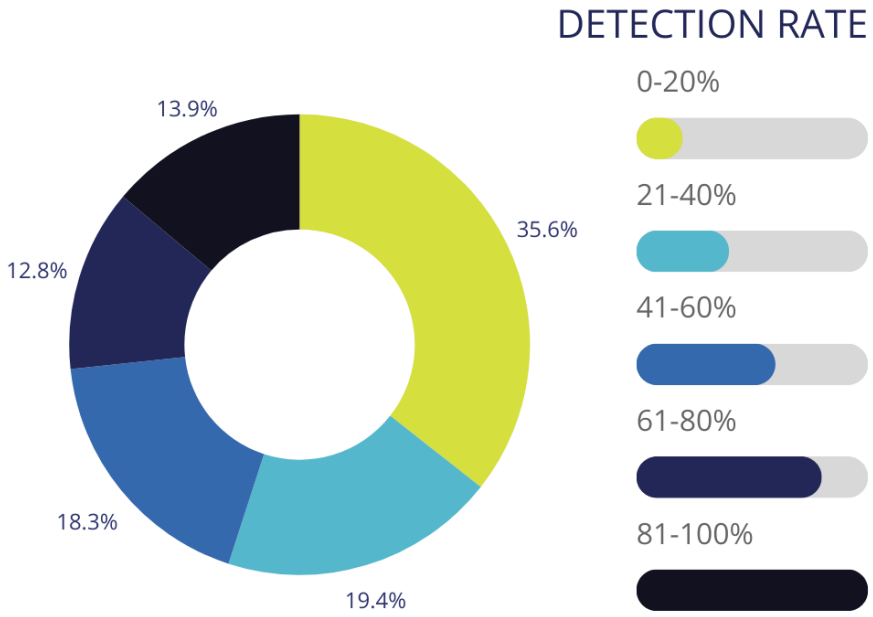
How many network-sharing (NNI) arrangements does your organization currently participate in?



How frequently does your organization experience service disruptions that could have been prevented with better network visibility?



What percentage of security incidents in the past 12 months were first detected by your network monitoring systems (versus customer reports or other means)?



Insight: In multi-operator environments, a lack of unified visibility introduces critical risk. Operators are effectively flying blind across shared infrastructure—jeopardizing uptime, security, and customer experience.

> *"As Data Center networks scale to meet global demand—extending deeper into edge locations and emerging markets—the importance of comprehensive network visibility is rising sharply. Growth should enhance operational control, not diminish it. In an increasingly complex environment, relying on fragmented tools and isolated systems creates unnecessary risks. Building resilient infrastructure today means unifying observability across the entire Data Center footprint—from core to edge—to ensure performance, security, and customer trust keep pace with expansion."*
>
> — Chris Sharp, CTO of Digital Realty

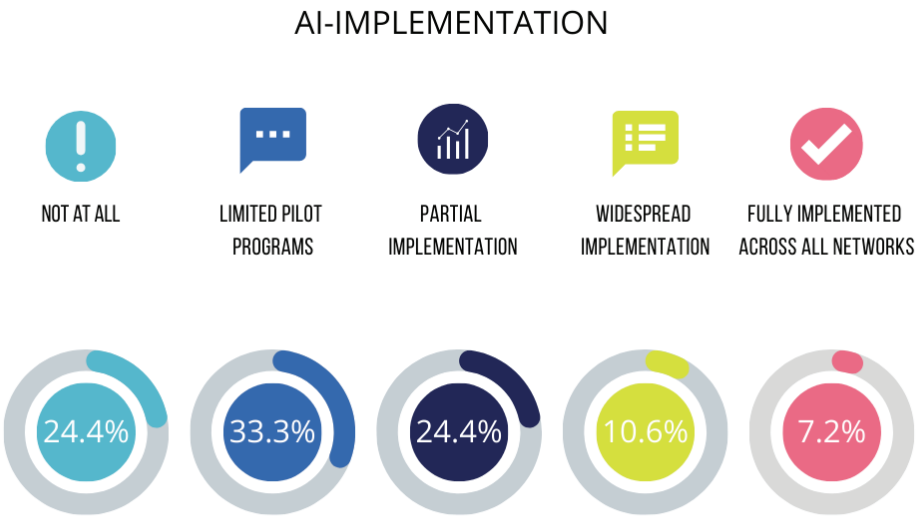
AI Can't Thrive Without Observability

AI promises to transform telecom operations—streamlining processes, detecting anomalies faster, and improving overall network performance. But there's a catch: without foundational visibility into infrastructure, AI can't deliver on its full potential.

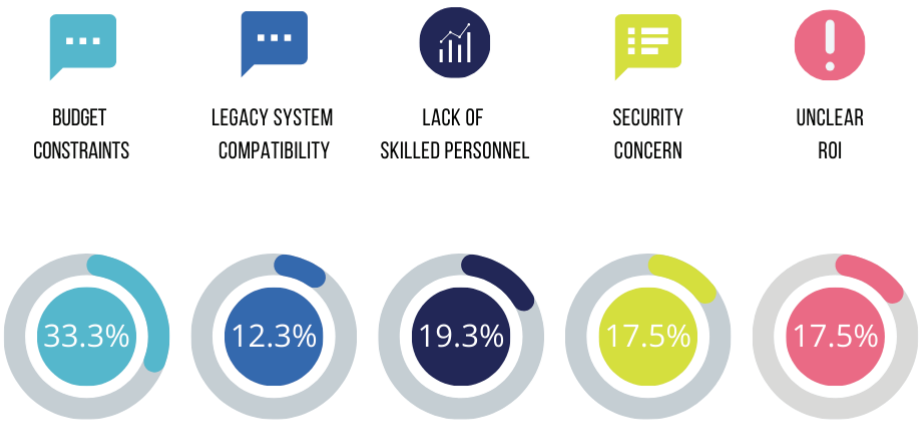
While enthusiasm is high, actual deployment remains limited. Only 7% of respondents have fully implemented AI-powered observability across their networks, while 57% are still in pilot mode or early adoption. Many are struggling to get past proof-of-concept due to budget constraints (29%), legacy system compatibility (22%), and a lack of skilled personnel (23%).

Even among those who've begun integrating AI, the payoff has been mixed. A third of respondents (32%) reported no reduction in downtime from AI-based observability tools, and just 6% have seen improvements of more than 50%. Without comprehensive, real-time visibility, AI can't operate effectively—let alone optimize performance at scale.

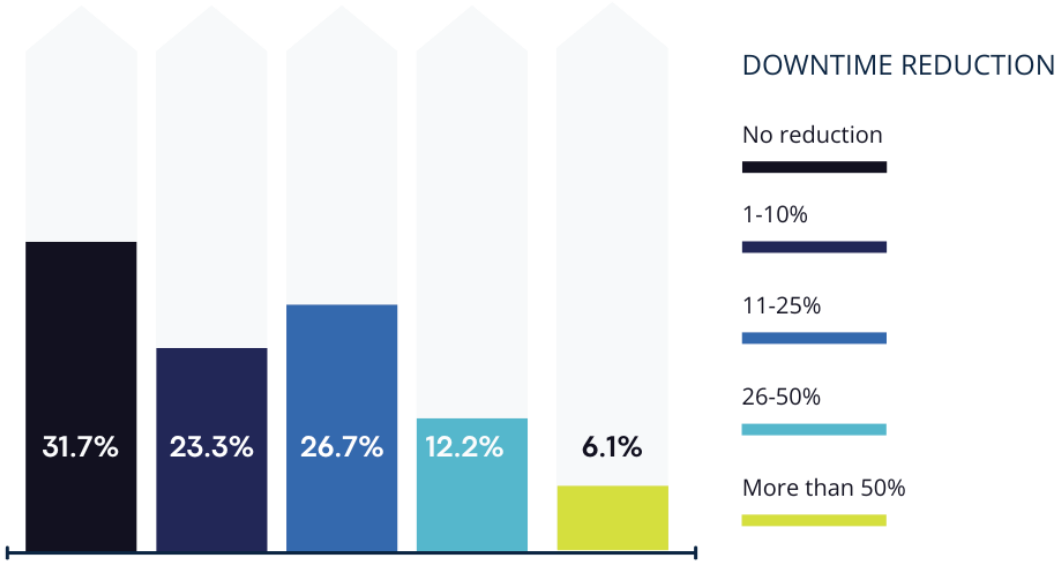
To what extent has your organization implemented AI-powered tools for network monitoring and observability?



What is your biggest barrier to implementing advanced network observability solutions?



What percentage reduction in network downtime have you achieved from implementing intelligent observability solutions?



Insight: AI's benefits depend on data. Without complete, real-time observability, AI-powered tools deliver suboptimal returns—or fail outright. Organizations must address these visibility gaps before scaling AI.

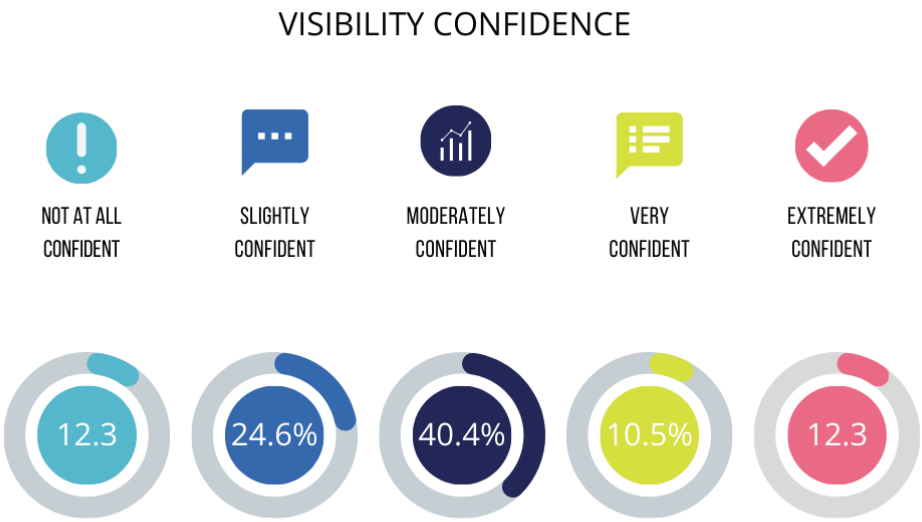
Expansion = Exposure

As telecom providers push to close the digital divide and bring connectivity to rural and underserved areas, they're also confronting a new wave of operational complexity. Every mile of new fiber, every added tower, and every edge deployment increases the surface area that needs to be monitored—and protected.

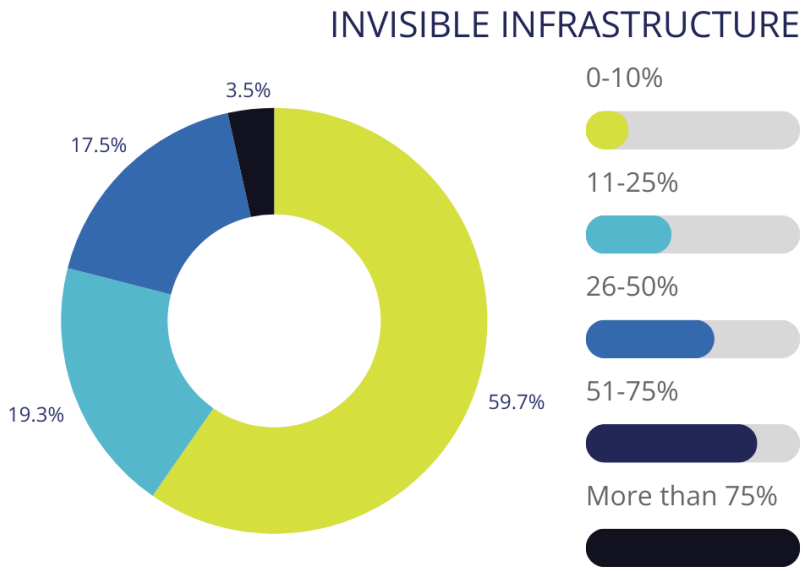
But with expansion comes exposure. Twenty-five percent of telecom leaders say they are slightly or not at all confident in their visibility into new or expanded infrastructure. Nearly 40% report that over a quarter of their network infrastructure is insufficiently monitored, revealing a growing disconnect between physical buildout and operational oversight.

Making matters worse, tool sprawl is compounding the issue. Thirty percent of respondents rely on seven or more monitoring tools, which adds integration headaches and hinders unified visibility—just as networks become more distributed and harder to manage.

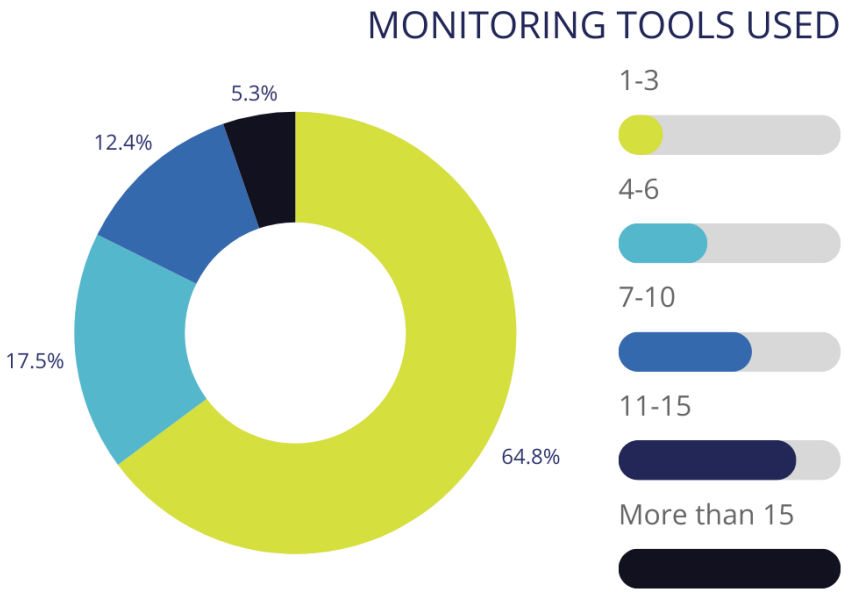
How confident are you in your visibility into new or expanded network infrastructure?



What percentage of your network infrastructure is currently "invisible" or insufficiently monitored?



How many different monitoring tools does your organization currently use to maintain network visibility?



Insight: Rural expansion creates a visibility gap that compounds technical debt. Without integrated, intelligent observability, providers risk outages, increased operational costs, and missed KPIs in new regions.

Readiness for Future Networks

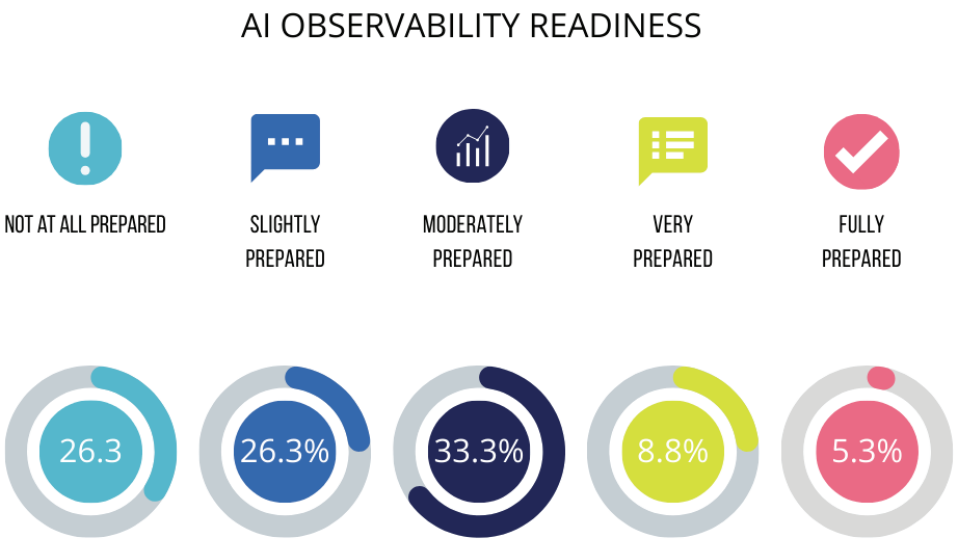
Telecom networks are entering a new era—defined by AI-driven applications, dynamic service models, and decentralized architectures like 5G, edge computing, and XaaS. But success in this next chapter depends on whether observability can evolve alongside the infrastructure it's meant to support.

Right now, many operators aren't confident in their readiness. Only 27% of respondents feel very or fully prepared to support AI-intensive applications with their current visibility tools. Even more telling: 80% report that less than 60% of their network monitoring is automated, signaling heavy reliance on manual oversight at a time when agility and scale are critical.

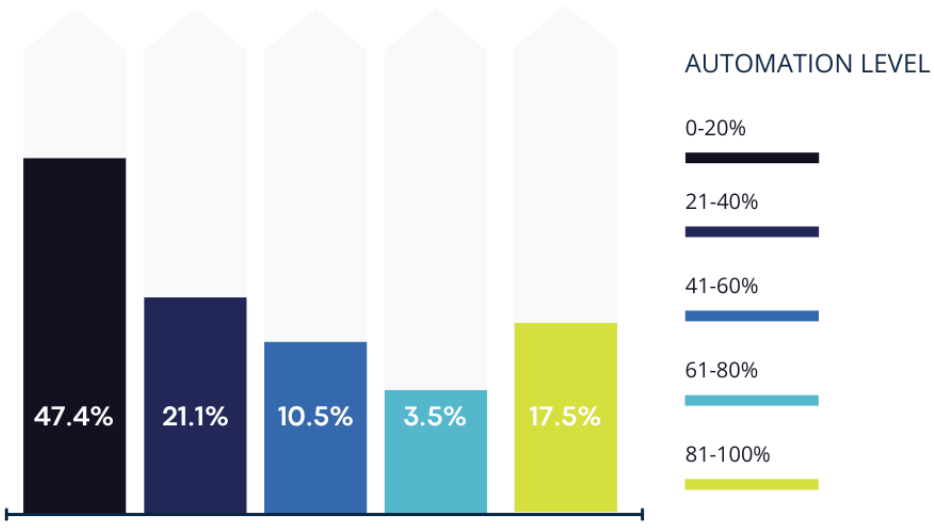
As telecom infrastructure becomes more complex and distributed, 55% of leaders express moderate to extreme concern about visibility gaps during these rollouts. Without modern observability to match modern networks, future-proofing efforts risk stalling before they even begin.

> *"Network-sharing agreements may help telecom operators scale faster, but : they also introduce new layers of complexity and risk. When visibility is fragmented across shared infrastructure, no one has the full picture. The fact that over half of operators are experiencing preventable service disruptions-and many are missing critical security incidents- should be a? wake-up call. Shared infrastructure must come with shared accountability and unified observability."*
>
> — Patrick Shutt, CEO of Resolute CS

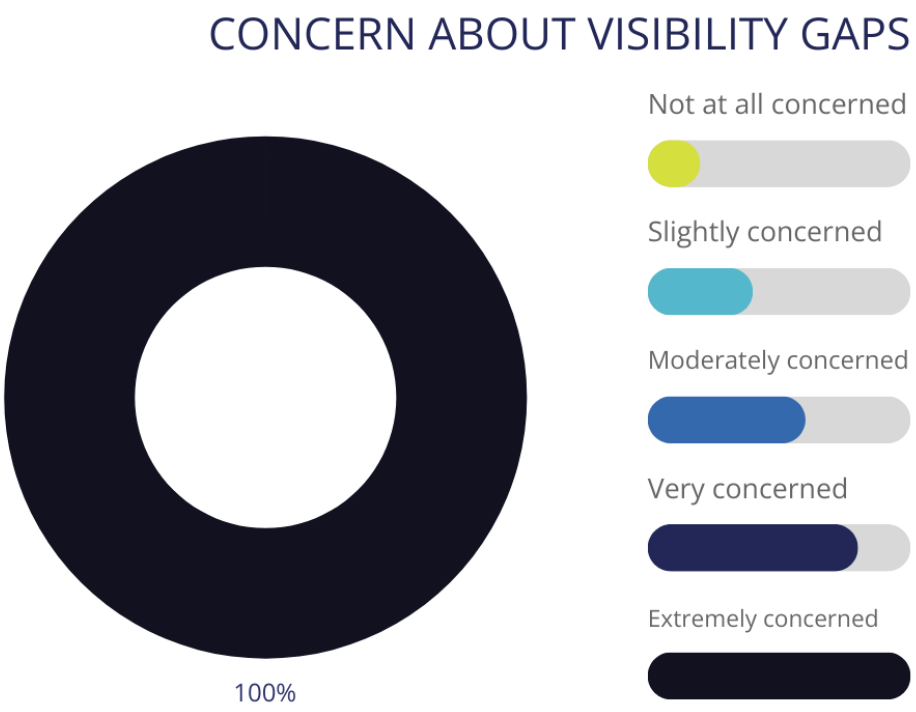
How prepared is your organization to provide observability for AI-intensive applications?



What percentage of your network monitoring is currently automated?



How concerned are you about visibility gaps as your network adopts new technologies (5G, edge computing, etc.)?



Insight: Network delayering, virtualization, and edge compute all demand greater visibility across physical and virtual assets. The current tools and strategies are not enough—without change, "Future Networks" will be built on unstable ground.

> *"Next-generation networks demand next-generation visibility. You can't scale AI, 5G, or edge services on a foundation that's still largely manual and fragmented. These findings make it clear: if we don't redefine observability now, we risk building the future of telecom on blind spots. True readiness means moving from reactive monitoring to intelligent, automated observability at every layer."*
>
> — Wes Jensen, COO of WanAware

Closing the Visibility Gap

The data is clear. Telecom's transformation hinges on closing the visibility gap. AI, sustainability, automation—none of these innovations can succeed without a strong observability backbone.

WanAware's core belief is validated by this survey: Massive investments in telecom infrastructure are at risk unless observability is prioritized. Visibility isn't just a support function. It's a strategic imperative.

Closing this gap means more than adding new tools. It requires a shift toward unified, intelligent observability that delivers real-time insights across the entire network footprint. By moving from fragmented monitoring to AI-driven observability, providers can reduce downtime, prevent costly incidents, accelerate digital transformation, and maximize ROI on every other initiative—from next-gen connectivity to operational efficiency and customer experience.

In an industry defined by speed, scale, and resilience, the winners will be those who can truly see what's coming—and act on it.

Telecom leaders can't afford to wait. If you're serious about unlocking the full potential of your network investments, now is the time to connect with WanAware. Our platform was built to eliminate blind spots and give you the end-to-end visibility required to compete—and win—in the AI-powered future of telecom.

> *"As infrastructure gets more abstract and dependencies stretch across clouds, carriers, and platforms, observability isn't just about uptime—it's about trust, accountability, and control in a world built on shared responsibility."*
>
> — Vincent English, Former CEO of PacketFabric and Megaport

Report Fast Facts:

32% of leaders allocate just **0–5%** of their budget to observability
62% have less than **50%** visibility into their infrastructure
55% report preventable service disruptions
36% detect less than **20%** of security threats via network tools
Only **7%** have fully implemented AI observability
80% say monitoring is still mostly manual
55% are concerned about visibility gaps with 5G, edge tech, and XaaS

www.wanaware.com