expereo

Insight report

Network as a Service: **Beyond Connectivity**



From network complexity to performance, resilience and control

A practical guide to dependable applications, proven resilience and greater control across global networks.

Explore the report





Evidence and methodology

This report offers enterprise technology and network leaders practical criteria for assessing Network as a Service (NaaS): application performance, global service delivery, resilience and intelligent operations.

The research used AI-assisted audience profiling to analyze public online opinions likely to reflect the perspectives of senior technology, infrastructure and network decision-makers in distributed organizations.

It examined 77,876 online opinions across X, Quora, Reddit, Bluesky, TikTok and Threads in the 12 months through October 11, 2026. The underlying analysis reports a 95% confidence interval and a 5% margin of error. Independent industry research and technical standards provide context.

Because these are AI-modeled opinions rather than responses from a representative survey of verified individuals, the percentages indicate patterns in the discussions analyzed, not verified enterprise adoption, performance or investment rates.

Executive summary

A network can be available while the business it supports is struggling. That gap matters when people rely on cloud applications, global connectivity and a chain of suppliers that few enterprises can see end to end.

NaaS can help manage that complexity, but adopting a different buying model is not the result. Nor is a wholesale migration always necessary. The real test is whether a change delivers dependable applications, faster deployment, proven recovery and less effort for the teams operating the network.

This report sets out five tests for enterprise buyers

1. **Maturity over migration.** Measure service outcomes, not the share of links bought as a service.
2. **Application experience over uptime.** An available connection is not enough if the business application is slow.
3. **Coordination over carrier consolidation.** Keep useful local choices; remove fragmented support and visibility.
4. **Recovery over reassurance.** Test critical applications through real failures, not just SLA targets.
5. **Results over automation volume.** AI has value when it improves diagnosis, decisions and restoration.

Together, these tests shift the conversation from how connectivity is bought to what employees and operations can depend on.



Expereo perspective:

Matthew Lea
Product Development Director, Expereo

Certainty is the outcome that matters.

You need a network you can plan around, in every country and on every application. A new way to buy connectivity is only the start. The real shift is one system, designed around your business and run by one accountable partner. That's what we design, deploy and manage for global businesses, through local partners in more than 190 countries. You get the clarity to see it working and the resilience to perform at your peak. We call it relentless predictability. This report shows why it now sets the standard.



Theme 1:

Adoption is not the same as maturity

Why the transition to service-based networking must be measured by what it delivers, not simply how much infrastructure has been migrated

NaaS adoption is easy to count: migrated sites, managed links and services billed monthly. Operational maturity is harder. Can you launch a site on time, diagnose incidents across suppliers and sustain the application experience your business needs?

For distributed enterprises, the value of Network-as-a-Service depends on more than the delivery model. It depends on whether organizations gain the flexibility to respond to changing business requirements, the visibility to manage performance across complex environments, and the operational control to maintain reliable connectivity at scale.

Before comparing offers, select three critical business services and ask how the proposed NaaS model will affect each one. Set a baseline for site readiness, application response, incident ownership and time to restore. That creates an acceptance test for the buying decision, not just a migration dashboard.

Judge the operating model, not the contract

The MEF NaaS Customer Experience White Paper, 2025 identifies seven attributes of NaaS: on-demand, observable, manageable, programmable, secure, flexible and modular.

These attributes extend the conversation beyond how connectivity is purchased or provisioned. They describe the capabilities enterprises should expect from a modern service-based network, including greater visibility, more responsive management and the ability to integrate networking into wider operational processes.

Ask who owns ordering, configuration changes, monitoring and fault management when a service crosses more than one carrier. A single portal may simplify reporting, but a buyer also needs one clear escalation route and decisions that can be acted on.

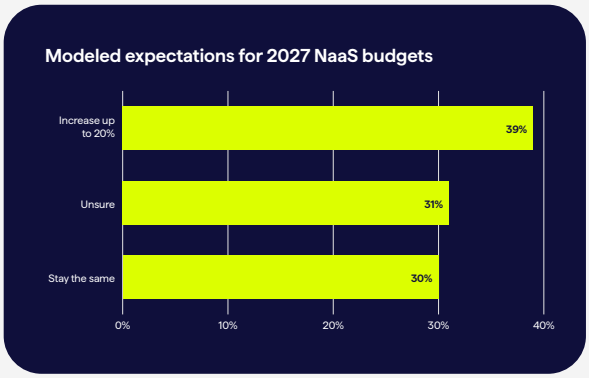
Ask how an incident moves from detection to diagnosis across provider boundaries, how changes are approved and how service quality is reported. If the answer still depends on separate tickets and dashboards, the complexity remains.

Investment needs an outcome test

In the modeled discussions, 39% were associated with expectations of NaaS budgets increasing by up to 20% in 2027, 30% with unchanged budgets and 31% with uncertainty about future spend.

The distribution suggests mixed investment sentiment. Whatever the budget, justify NaaS against a service and operational baseline.

Before committing more spend, measure site deployment times, repeat incidents, application performance and hours spent coordinating providers. Recheck those measures after the operating model changes.



Modeled 2027 NaaS budget sentiment: 39% expect an increase, 30% no change and 31% remain uncertain.



Five outcomes to test before you buy

For technology leaders, a more useful evaluation starts with the services the network must support. Key questions include whether new locations can be connected predictably, whether critical applications perform consistently and whether service teams can diagnose issues across provider boundaries without lengthy hand-offs.

1. **Simpler operations:** Fewer hand-offs and a named owner for cross-provider incidents.
2. **Application assurance:** Visibility into user experience and the path between people and services.
3. **Resilience:** Tested dependencies, failover and recovery for critical workflows.
4. **Control:** Accessible service data and practical rights to manage change.
5. **Agility:** Predictable lead times for new sites, upgrades and service changes.

Set baselines and ask for evidence. A capability list is not proof of an improved operating model.

They also suggest that NaaS maturity is not an all-or-nothing destination. Different organizations will require different combinations of managed services, automation, visibility and operational support, depending on their existing infrastructure, geographic footprint and business priorities.

Strategic insight

Maturity is the difference between a service that has moved and a business outcome that has improved.

Sometimes migration is not the first move

If existing connections are reliable but faults take too long to diagnose, shared monitoring and better incident coordination may deliver more immediate value than replacing circuits. If only a few applications or sites are struggling, targeted path changes or access upgrades may be the right response. NaaS deserves investment where it demonstrably removes a constraint the business cares about, not simply because more services can be purchased on a subscription.

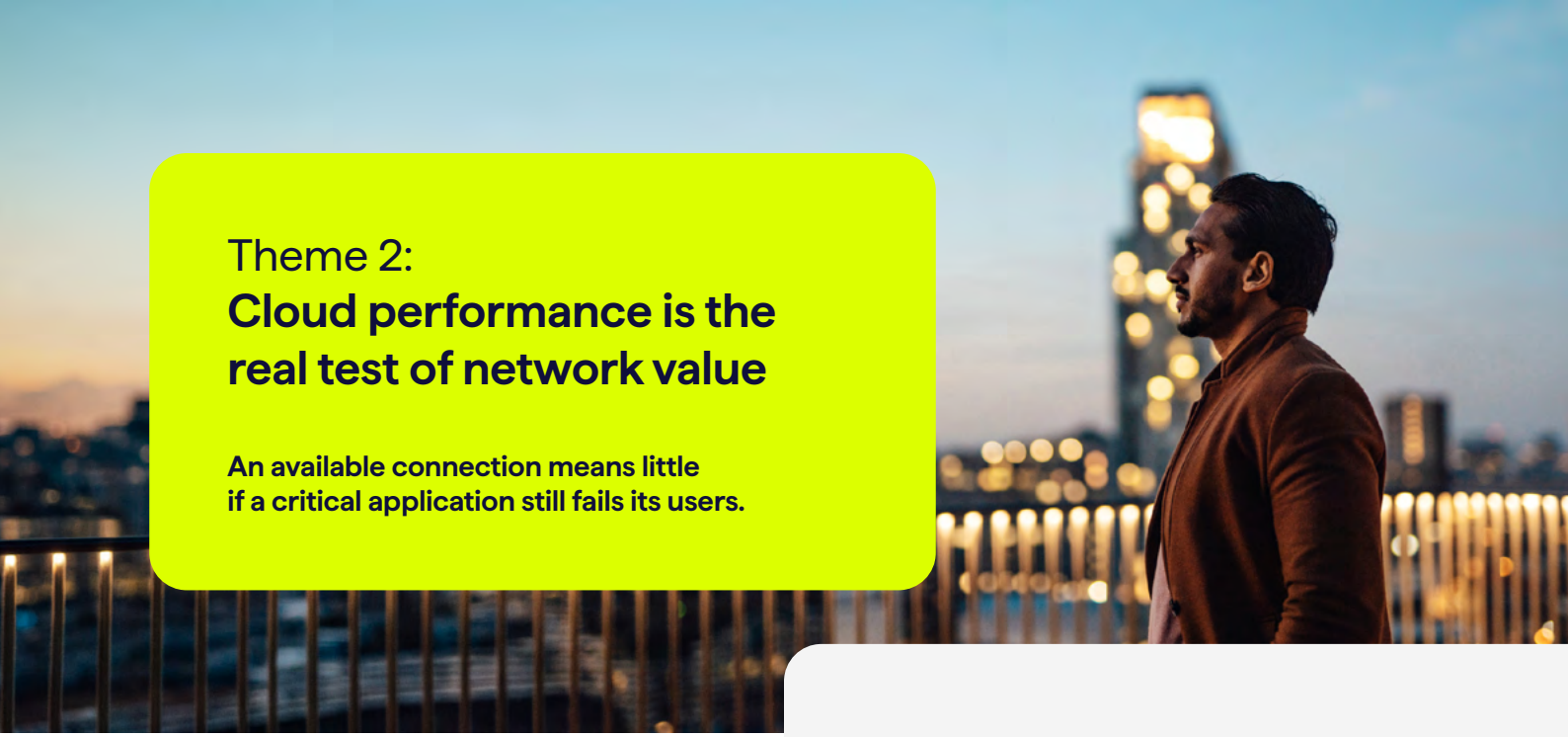
A useful procurement question is: what can we improve without replacing what already works? Ask any prospective partner to explain which services should change, which should remain and what evidence would justify expanding the model.

Expereo perspective:

Start with the estate you have and the outcomes you need.

Expereo designs managed connectivity around individual sites, applications and operating requirements, rather than treating migration volume as the goal. For a buyer, the important commitment is a measurable plan: which services will change, who will own delivery and how the result will be assessed before the model is expanded.

Matthew Lea
Product Development Director, Expereo



Theme 2:

Cloud performance is the real test of network value

An available connection means little if a critical application still fails its users.

A user can be connected to a cloud application and still struggle to work. Slow transactions, intermittent degradation and inconsistent performance across locations can disrupt customer service, collaboration and critical workflows even while a link is technically available.

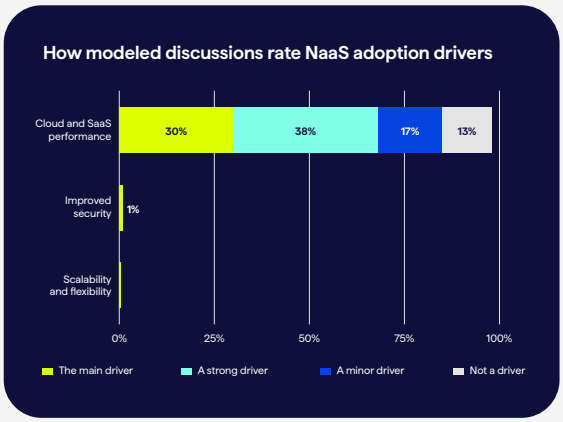
This distinction matters more as enterprise applications are delivered through different cloud platforms and accessed from offices, remote facilities and home environments. The network is judged increasingly by the services it enables, not simply by whether an access link is active.

This difference is easy to overlook in a distributed business. A logistics site may have an active access connection but still struggle to complete transactions in a cloud-hosted warehouse application. An office may meet its network availability target while collaboration tools remain unreliable at peak times. These are illustrative situations, but they show why enterprise buyers need to look beyond the status of a connection to the quality of the application journey.



Cloud performance influences NaaS decisions

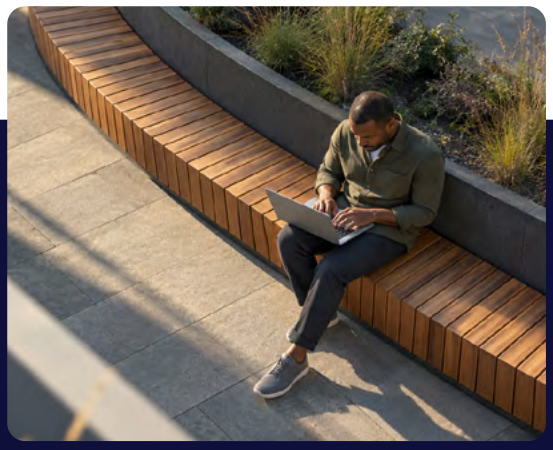
In the modeled audience findings, 30% rated cloud and SaaS performance the main driver of NaaS consideration and 38% a strong driver. Another 17% rated it a minor influence and 13% not a driver.



In Modeled discussions, 30% rate cloud and SaaS performance the main NaaS driver; 38% rate it a strong driver.

Flexera's 2026 State of the Cloud Report found that 73% of 753 respondents operated hybrid cloud environments. For network buyers, an application journey may now involve several technologies and suppliers.

Hybrid cloud also complicates accountability. An employee's request may traverse local access, one or more Internet networks, security controls and a cloud provider before reaching the application. Different parties can each report healthy infrastructure while the transaction remains slow. Network teams therefore need sufficient cross-domain information to separate faults in transport and routing from problems in the application or cloud environment itself.



Availability and experience are different measures

Capacity is only one possible cause of poor application experience. Routing, DNS, packet loss, cloud-platform performance or an application fault may matter more.

The diagnostic question is where the experience starts to deteriorate. That may require visibility into path changes, latency and packet loss, DNS resolution, local access behavior and application response. No single measurement explains every failure. Used together, these signals can shorten investigations and avoid the common response of purchasing more capacity before confirming whether capacity is the constraint.

Cisco ThousandEyes' 2025 analysis of Internet and application outages highlights incidents in which core infrastructure appeared healthy while important application functions were impaired. It offers a useful reminder that reporting only link availability can conceal the service problems users experience.

This is where performance-aware operations become valuable. Application and path telemetry, combined with suitable routing controls, can help teams detect deteriorating conditions, compare available paths and investigate whether an alternative route would improve performance. Such interventions are only useful when their effect on the end user can be measured.

Application-aware traffic management can help when suitable alternative paths exist, but a faster route is not necessarily a better user experience. It must preserve security policy, have enough capacity and avoid instability. Ask providers to demonstrate the measured application impact of a routing change rather than merely showing that the feature exists.

Put the critical application journey first

The MEF NaaS Industry Blueprint positions application assurance alongside on-demand connectivity, cybersecurity and multi-cloud networking as part of the evolving NaaS model.

For a customer, application assurance is a prompt to ask what happens beyond the access link: how the managed network observes application paths, which faults it can act on and how problems outside its own infrastructure are escalated.

Rank the applications that cannot afford poor performance. Map their main user paths, sites and cloud dependencies, then set monitoring and response targets for those journeys.

Application outages, cloud platform failures and endpoint problems may remain outside the direct control of a network provider. The value of an intelligent operating model is therefore not simply its ability to optimize connectivity, but its capacity to distinguish network-related issues from wider service problems and support a faster, more coordinated response.



What to measure

Keep availability and bandwidth measures, but pair them with evidence of application experience and recovery:

- **Application experience:** Are critical applications responsive across priority locations?
- **Network quality:** How do latency, loss, jitter and routing changes affect those applications?
- **Operational response:** How quickly do teams detect, isolate and resolve degradation?
- **Business impact:** Are interruptions to critical workflows becoming less frequent or shorter?

Review these measures by application and location. Trend them before and after changes so improvement can be demonstrated.

For investment decisions, compare the cost of the intervention with the service impact. The aim is not the fastest possible connection at every site; it is an appropriate level of application performance, maintained without unnecessary expense or repeated troubleshooting.



Strategic insight

If applications are slow while the link is healthy, the network has not met the business need.

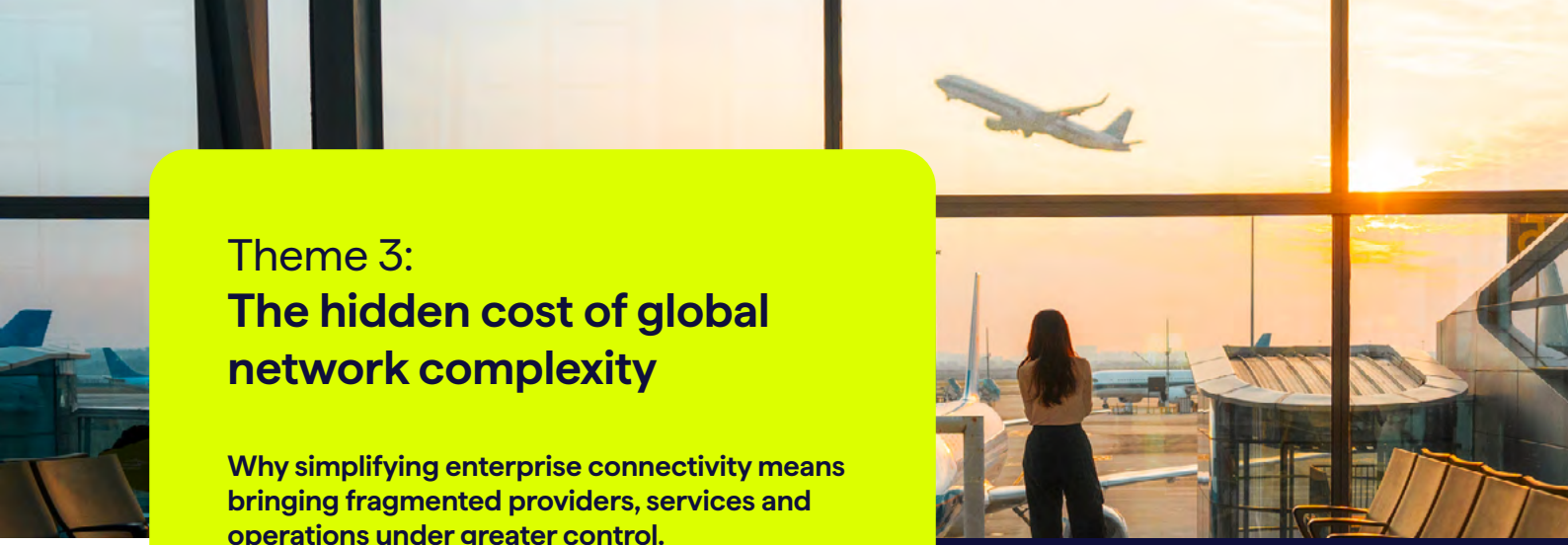
But delivering that experience consistently across a distributed enterprise presents a further challenge. Different locations depend on different Internet service providers, connectivity architectures, supplier relationships and operational processes. Even when individual services perform effectively, managing them collectively can introduce significant complexity.

Expereo perspective:

Application experience should shape network design, not simply follow it.

Expereo combines performance visibility and application-aware network capabilities to identify where a path or routing change may help. Where the cause sits in a cloud application, endpoint or third-party dependency, the first job is to isolate it accurately and coordinate the response. Ask for evidence that users experienced an improvement, not just that the network route changed.

Matthew Lea
Product Development Director, Expereo



Theme 3:

The hidden cost of global network complexity

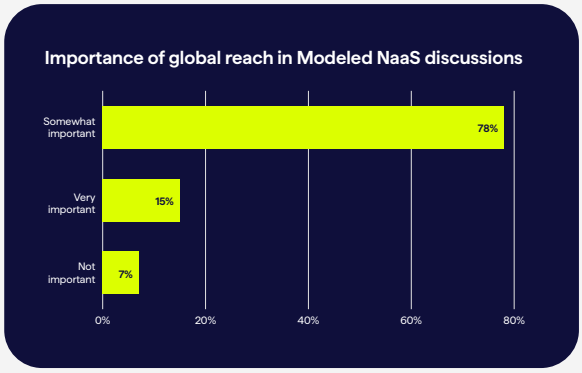
Why simplifying enterprise connectivity means bringing fragmented providers, services and operations under greater control.

A global network can span dozens of local carriers, access technologies, support models and contracts. The commercial footprint may be global; day-to-day operations are often local and fragmented.

The problem is not the number of suppliers. It is the number of unresolved hand-offs when something goes wrong.

Global coverage is a starting point, not a service guarantee

In the modeled discussions, 15% classified global reach as very important to their NaaS choice, 78% as somewhat important and 7% as not important.



In Modeled discussions, 15% rate global reach very important and 78% somewhat important.

For enterprise buyers, coverage must be assessed alongside consistent ordering, monitoring, fault escalation and service reporting.



Supplier choice is not supplier sprawl

Different providers may offer advantages in particular regions, access to infrastructure unavailable elsewhere, or alternative routes that support network resilience.

You may need different carriers for local quality, access or genuinely diverse routes. Keep those choices where they serve the business; simplify the way they are managed.

The 2025 ISG Provider Lens Enterprise Managed Network Services report for the United States, published in January 2026, identifies growing demand for coordinated management across underlying connectivity, cloud environments, software-defined networks and security functions.

For buyers, the critical test is the operational layer joining connectivity, cloud and security, not just the size of a provider's footprint.

The hidden cost is coordination

The network bill rarely captures the full cost of running it. Separate contracts, service desks, incident records and reporting tools consume time that could be spent supporting expansion or improving application experience.

Operational fragmentation can also hide in ordinary tasks. A new site may require different order forms, carrier contacts and installation updates. A change request may need local approvals and multiple support queues. The buyer should ask what those processes look like in practice and whether their internal team will still be orchestrating each step.

In EMA's 2025 study of 351 IT decision-makers, 90% operated multi-vendor network infrastructure and fewer than 17% used one observability tool. This concerns equipment and tools rather than ISP counts, but shows why a joined-up view can be hard to achieve.

Nearly 27% in that sample used four or more equipment vendors. The operational implication is to connect monitoring data and incident records across systems, not to assume that changing ISP contracts will solve observability gaps.

Complexity becomes costly when it slows action

Consider the steps involved when a critical site experiences intermittent packet loss. The enterprise may first check its own equipment, then engage the local access provider, then seek routing evidence from an upstream carrier. If no one owns the end-to-end investigation, each organization can complete its assigned check while the underlying problem remains unresolved. A coordinated model does not remove every dependency, but it can establish one incident record, a clear escalation path and a shared understanding of progress.

The same test applies to site delivery: who coordinates local access, third-party changes and dependencies so launches do not stall between suppliers?

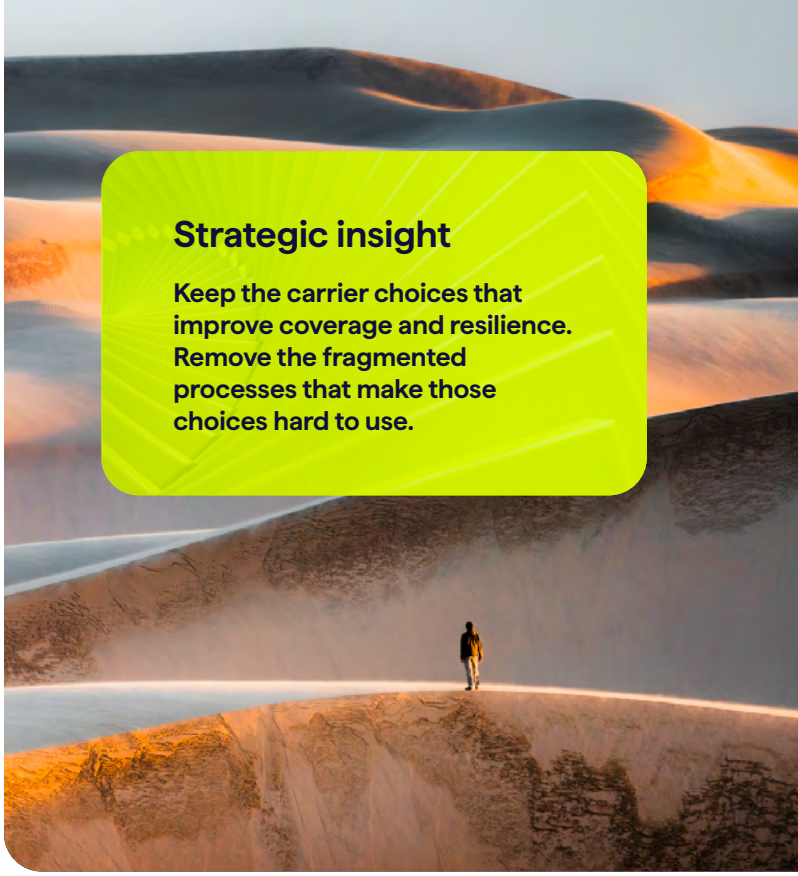
The MEF 2025 NaaS Industry Blueprint identifies common service standards and Lifecycle Service Orchestration APIs as foundations for automated interactions between network ecosystem participants. It reinforces a practical principle: standardization and coordination are what allow diverse services to operate more effectively together.



Price the work of running the network

A NaaS business case should count the operational workload as well as the monthly service cost:

- **Site delivery:** Time from approved request to usable connectivity.
- **Supplier overhead:** Contracts, bills, service desks and staff hours spent coordinating them.
- **Incident response:** Time to isolate faults and restore the affected application.
- **Visibility:** Consistency of service information and reporting across sites.
- **Operating cost:** Internal effort and provider charges measured against service outcomes.



Strategic insight

Keep the carrier choices that improve coverage and resilience. Remove the fragmented processes that make those choices hard to use.

Customer example:

HERAS

In a published customer case study, Expereo describes delivering managed internet connectivity across 12 Heras locations in five European countries.

A remote facility without suitable fixed-line access received a managed low-Earth-orbit satellite connection, allowing staff to use business applications that had previously been affected by poor connectivity.

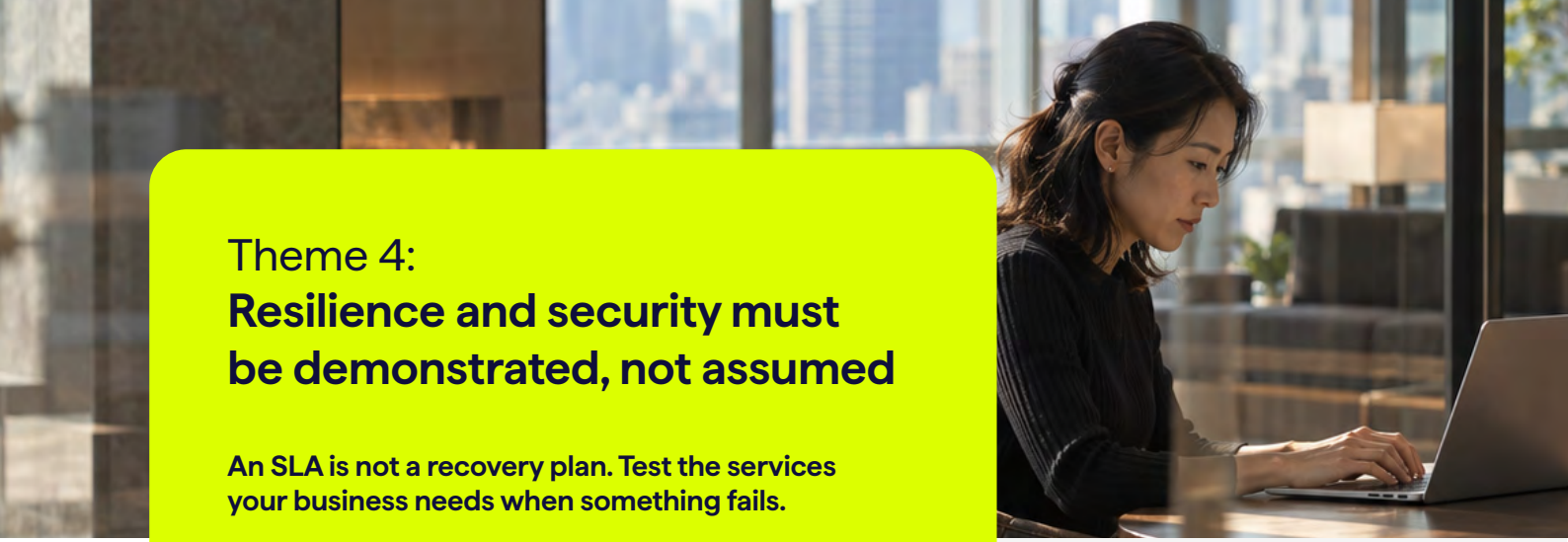
The solution also gave Heras site-level performance visibility and a single service contact. For buyers, the evidence to request is equally concrete: where coverage improved, whether applications became usable and how the network is supported after launch.

Expereo perspective:

Global coverage is useful only when an enterprise can operate it as one service.

Expereo keeps access choices local where that makes technical or commercial sense, while bringing monitoring, service records and escalation into a coordinated model. The point of carrier neutrality is not unlimited supplier choice; it is being able to choose what works at each site without asking the enterprise to manage every carrier relationship separately.

Matthew Lea
Product Development Director, Expereo



Theme 4:

Resilience and security must be demonstrated, not assumed

An SLA is not a recovery plan. Test the services your business needs when something fails.

For distributed businesses, a network failure can quickly become an operational incident.

Employees lose access to systems, production or logistics workflows may stop and customer-facing services can be interrupted. Because modern network estates depend on external carriers, cloud platforms and other shared infrastructure, some of the most important risks sit outside an organization's direct control.

Start with the workflows that matter most. A factory floor, contact center and regional office will not need identical recovery targets. Set priorities by business impact, acceptable downtime and feasible alternatives.

Measure disruption in business terms

In the Uptime Institute Annual Outage Analysis 2026, 57% of respondents said their most recent major outage cost over $100,000; one in five reported more than $1 million. These figures cover major IT and data center outages broadly and show why recovery should be planned around business impact.

Cloudflare's review of 2025 Internet disruptions documented more than 180 observed disruptions, with causes including cable damage, power failure, extreme weather and technical problems. Your recovery design must account for dependencies outside the primary provider.

Contracts cannot replace recovery capability

Service-level agreements provide an important contractual baseline, but a high availability commitment is not a guarantee of uninterrupted operations. Coverage, exclusions and service boundaries matter. An access circuit may meet its contracted target while an application remains unavailable because another provider, cloud environment or route has failed.

Similarly, a backup circuit does not automatically provide resilient service. Alternate connections can share ducts, power or upstream dependencies. During an incident, they may also lack sufficient capacity for the applications they are expected to protect. Recovery arrangements need to be tested under realistic conditions, not assumed from a topology diagram.



For example, two circuits may terminate at separate provider hand-offs while still relying on the same physical route into a building. A successful failover test also needs to confirm that critical applications work on the secondary path, that authentication and security policies remain effective, and that the reduced capacity can handle priority traffic. Paper redundancy offers limited assurance until its behavior has been tested under realistic operating conditions.

Security and continuity must work together

NIST Zero Trust Architecture guidance calls for access decisions grounded in identity, device and policy rather than network location. For a distributed enterprise, those controls must still work during failover and alternative-access scenarios.

Zero trust and network resilience address different risks. Identity-led access controls may limit unauthorized use of resources, but they cannot repair a damaged access route. Equally, a redundant connection does not compensate for weak identity controls or misconfigured access policies. Senior leaders should assess how these protections interact, including which provider owns each control and how security decisions are maintained during failover or recovery.

Strategic insight

Resilience is measured by how quickly critical work can resume, not by the SLA percentage alone.

When assessing a managed NaaS arrangement, request evidence of cross-provider incident ownership, tested alternative paths and recovery reporting for priority applications. A supplier may manage the network, but the enterprise still sets business recovery priorities and decides what level of disruption is acceptable.

Know who takes charge in an incident

The enterprise owns recovery priorities; managed partners may monitor, triage and restore services. Define escalation and change authority before an incident. The NIST Cybersecurity Framework 2.0 offers a useful structure for detection, response and recovery.

Those responsibilities need to be agreed before a major incident. A useful operating playbook defines who declares an incident, who coordinates third-party carriers, who authorizes service changes, how business-critical teams receive updates and who confirms successful recovery. These decisions are often more consequential than the wording of an availability guarantee. They also provide a practical test of whether a managed service relationship will reduce the enterprise's operational burden during disruption.

Measure time to detect, time to isolate and time to restore each critical workflow, not just link uptime.

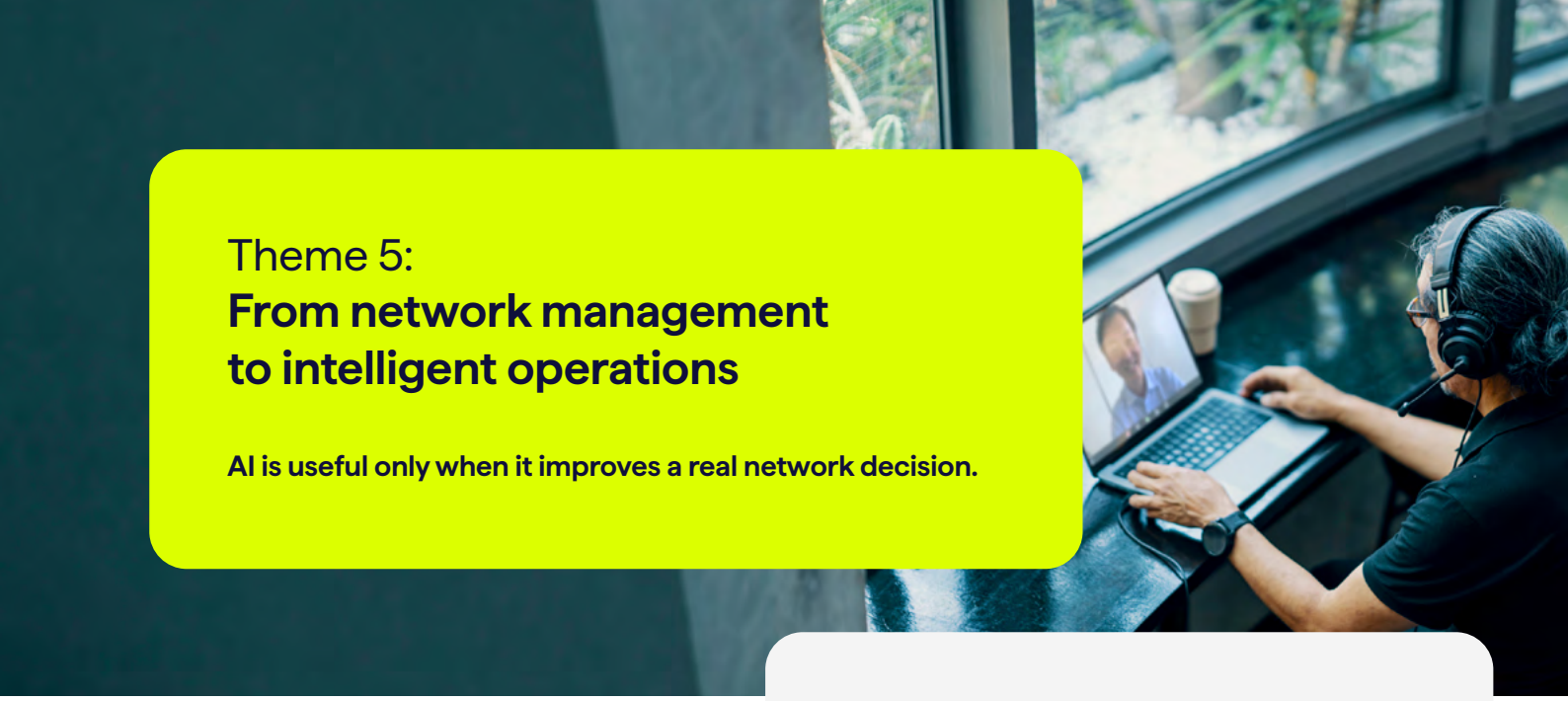
Recovery testing should record both technical and business results. Switching to an alternate link is one result; restoring a usable application experience is another. Measures such as time to detect, time to isolate and time to restore priority workflows allow the organization to identify weaknesses and track improvement. As sites, applications and suppliers change, the recovery plan needs to be revisited rather than treated as a one-off exercise.

Expereo perspective:

Resilience needs to reflect business impact.

Expereo can combine diverse access options, site-specific policies and managed incident coordination, but even a well-designed network cannot prevent every cloud, carrier or site failure. The right customer test is a rehearsed one: can priority applications continue over the alternate path, who takes charge across suppliers and how quickly can the business recover? Our role is to help design and operate that response, with responsibilities agreed before disruption.

Matthew Lea
Product Development Director, Expereo



Theme 5:
From network management to intelligent operations

AI is useful only when it improves a real network decision.

Network teams collect telemetry from access, routing, applications and cloud services. The hard part is joining it into evidence that guides intervention before service suffers.

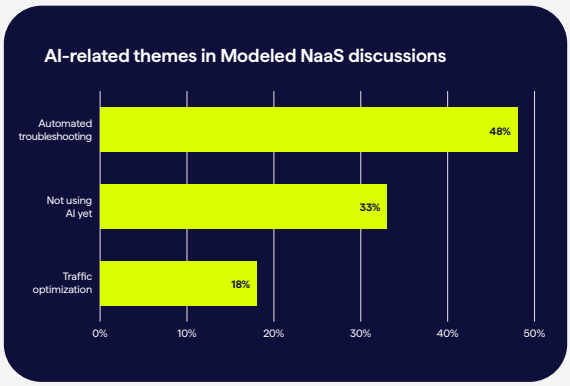
An AI tool does not make a network dependable on its own. Trustworthy data, a tested response process and clear decision rights matter more than the volume of automated actions.

For network teams, the first challenge is often signal quality. Multiple systems may generate alerts about the same event, while incomplete asset records make it difficult to understand which sites or applications are affected. AI can assist with correlation and diagnosis, but a convincing operational model must still maintain a reliable service inventory, meaningful telemetry and a clear history of changes and incidents.



Interest in AI is ahead of proven results

In the modeled discussions, 48% referenced automated troubleshooting, while 33% indicated that AI was not yet in use.



AI-related themes in Modeled discussions: 48% refer to automated troubleshooting; 33% indicate no AI use.

Interest in automated troubleshooting is a useful signal, but the business case rests on whether it makes fault resolution faster and more accurate.

EMA's January 2026 NetOps study of 458 IT professionals found that 35% considered their AI-driven network management initiatives completely successful, while 44% had full confidence in the network data behind them. For buyers, data quality is part of the capability being evaluated.

These findings support a measured approach to investment. A tool that produces plausible incident summaries may save time, but only if its conclusions can be checked against the network's actual state. Where provider and enterprise datasets disagree, the priority is to resolve that gap rather than allow an automated recommendation to appear more certain than the evidence warrants.



Start with evidence, not algorithms

Join path telemetry, application signals and change records across relevant providers. Use that view to spot degrading routes, identify likely causes and choose the right intervention.

An illustrative example is a gradual deterioration in performance between several offices and a cloud application. Correlating path telemetry with user-experience signals may reveal that only traffic using one upstream route is affected. The next action could be to investigate that route, ask a provider to intervene or test an available alternative. The valuable capability is not a model merely identifying an anomaly; it is a workflow that leads from evidence to an appropriate and verifiable response.

The TM Forum Autonomous Networks framework describes progression toward closed-loop operations, primarily for communications providers. For enterprises, the practical sequence is straightforward: observe, diagnose, act, verify and record the result.

Verification is essential. After a route or policy change, teams should confirm that the original degradation has improved, that security controls remain intact and that no new issue has appeared elsewhere. If the outcome is poor, the operating model needs an escalation or rollback path. This feedback loop helps distinguish intelligent operations from a collection of isolated automated tasks.

Govern automation by risk

Automated routing or policy changes can affect many sites at once. Set thresholds for what may proceed automatically and what needs human approval.

NIST AI Risk Management Framework provides principles for assessing risk, assigning oversight and measuring outcomes. Apply lighter controls to low-impact diagnostics and stronger approvals to changes affecting critical systems.

Governance should be proportionate to operational risk. Low-impact diagnostic activity may be automated with limited intervention, while changes affecting essential applications or a large number of sites may require human approval. Change logs, rollback procedures and agreed decision rights are particularly important when a managed service partner operates parts of the network on the enterprise's behalf.

Those controls should enable progress, not stall it. Automate routine diagnosis where the evidence is strong, but keep experienced people responsible for material changes and complex incidents. The test for the customer is whether the operating model makes safe action quicker.

Do not reward automation volume. Judge it by earlier detection, shorter incidents and fewer repeat faults.



What to measure

A sensible implementation sequence starts with reliable visibility, then introduces AI assistance into clearly defined tasks such as alert correlation or initial fault classification.

Automation can be extended where its accuracy, operational benefit and safeguards are evidenced. This makes it easier to compare before-and-after performance, build confidence among network teams and avoid scaling an approach that has not yet demonstrated value.

- **Detection and diagnosis:** Are emerging performance problems identified earlier, and can teams establish their likely causes more efficiently?
- **Service restoration:** Are network incidents resolved more quickly, with fewer repeated escalations and less disruption to business-critical applications?
- **Application experience:** Are improvements in network management translating into more consistent performance for employees, customers and operational systems?
- **Automation effectiveness:** Are automated recommendations and actions accurate, appropriately governed and demonstrably successful, with safeguards and rollback procedures where required?
- **Operational efficiency:** Are teams spending less time on repetitive troubleshooting and coordination, allowing greater attention to service improvement and strategic priorities?



Expereo perspective:

Matthew Lea
Product Development Director, Expereo

Operational intelligence should make incidents easier to understand and resolve.

Expereo Predictive Intelligence is designed to bring service signals and operational knowledge together, while engineers remain responsible for interventions that affect critical services. Customers should ask to see how an alert becomes a diagnosis, who approves changes and how the result is verified. An automated action is not the success measure; shorter disruption and more dependable applications are.



Strategic insight

Intelligence earns its place when it restores service faster and protects application experience.

Network Value and NaaS Maturity Scorecard

A practical six-dimension assessment for enterprise network leaders

Use this scorecard to identify where your network is dependable today and where the next improvement would have the greatest impact.

Rate each dimension Developing, Established or Advanced using evidence from your sites, applications, suppliers and incident records. There is no universal target score.

Dimension	Developing	Established	Advanced
1. Application performance	Performance is primarily assessed through connectivity availability and bandwidth, with limited visibility into application experience.	Critical application performance is monitored across priority locations, with defined thresholds and processes for investigating degradation.	End-to-end application experience is measured across distributed environments, with proactive identification and optimization of network-related performance issues.
2. Global connectivity and supplier coordination	Connectivity providers, contracts and support processes are managed separately across locations, creating fragmented visibility and accountability.	Service information, supplier coordination and operational processes are increasingly standardized across the network estate.	Diverse connectivity providers operate within a coordinated management model, with consistent visibility, streamlined service delivery and clear accountability.
3. Resilience and business continuity	Resilience relies primarily on availability commitments and backup infrastructure, with limited testing of business-critical dependencies.	Critical dependencies are identified, recovery responsibilities are defined and resilience arrangements are tested for priority services.	Resilience is regularly validated through realistic failure scenarios, with recovery performance measured against business continuity requirements.
4. Security and governance	Security controls and operational responsibilities vary across environments, with inconsistent policies or limited visibility into risk.	Common security policies, access controls and incident responsibilities are established across core network environments.	Risk-based security and zero-trust principles are embedded into network operations, with controls continuously assessed and responsibilities clearly governed.
5. Visibility and intelligent operations	Monitoring relies on fragmented tools and reactive troubleshooting, with limited correlation between network and application information.	Consolidated monitoring, consistent incident processes and selected automation capabilities support more efficient operations.	Reliable operational intelligence supports proactive detection, coordinated responses and appropriately governed automation, with outcomes regularly evaluated.
6. Commercial value and business agility	Success is assessed mainly through connectivity costs, service availability and infrastructure deployment.	Operational performance, deployment speed and network-related costs are measured against defined objectives.	Network investment is evaluated through demonstrable improvements in service quality, operational efficiency, responsiveness and business outcomes.

How to use the scorecard

Advanced is not the goal in every dimension. The right level depends on business risk, critical applications, geographic footprint and the cost of disruption.

Use the scorecard in three steps

1. **Identify gaps by business impact.** Start with the applications, locations and dependencies where failure matters most.
2. **Set measurable targets.** Record the performance, restoration, site-delivery and management-effort baselines you want to improve.
3. **Assign ownership.** Agree on which changes belong to internal teams, managed partners or both, and review progress regularly.

For example, poor supplier coordination may call for shared incident records and reporting before any network replacement. Capture the evidence behind each rating, agree on an owner and revisit the assessment quarterly or twice a year.

expereo

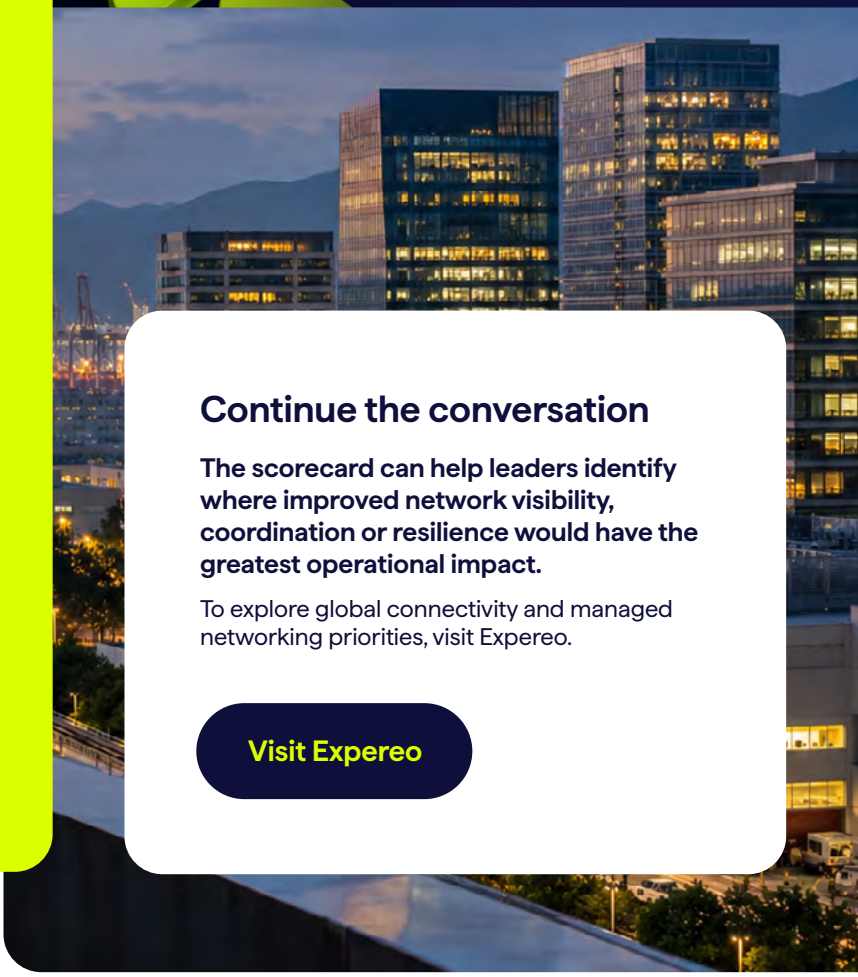
Final perspective from Expereo:

“

The network that serves your business best may combine several carriers, technologies and management models.

What matters is whether people can work, performance can be explained and recovery has an owner. Expereo brings local connectivity and managed operations together to make those outcomes easier to deliver and measure. Use the scorecard to set your priorities, then ask every potential partner, including Expereo, to show how improvement will be evidenced. That is what relentless predictability should mean in practice.

”



Continue the conversation

The scorecard can help leaders identify where improved network visibility, coordination or resilience would have the greatest operational impact.

To explore global connectivity and managed networking priorities, visit Expereo.

Visit Expereo