Arelion

Network trust, tested.

A practical guide before you commit to a network provider

The trust gap enterprises can no longer afford to ignore

✳ The trust gap enterprises can no longer afford to ignore

93% of enterprise leaders say they largely or completely trust their current network provider.

But their trust is often built on a number of expectations: security against threats, reliability and uptime, performance and latency, data sovereignty, network ownership and operational control. Trust tends to accumulate through familiarity and the absence of a crisis rather than active proof, and most enterprises have never had reason to distinguish between the two. This creates a significant risk when business continuity is increasingly network-dependent.

The trust gap enterprises can no longer afford to ignore

And with AI and digital transformation evolving at break-neck speed, this gap matters more than ever. Cisco and Foundry's 2026 research found AI has already created network challenges for 97% of enterprises surveyed, with AI-driven traffic expected to triple within three years[1]. Additionally, Gartner's research into third-party risk found 62% of organizations still overly trust vendor due diligence questionnaires, which are increasingly AI-generated, to inform their risk decisions[2] – leaving them exposed to risks that only surface after contracts are signed.

62% of organizations still overly trust vendor due diligence questionnaires

✳ The trust gap enterprises can no longer afford to ignore

That urgency is already showing up in our recent report: 85% of leaders expect provider trust to become more important over the next three years.

“If your provider has never had to prove trust under pressure, you may not know whether that trust is real until the cost of finding out is already way too high.”

Why trust without proof puts your business at risk

SLAs do not prove readiness

1.

Only 15% of leaders have complete confidence in their provider's ability to detect a serious incident quickly. Verizon's 2026 Data Breach Investigations Report found that AI is shrinking the vulnerability exploitation window from months to hours.[3]

Third parties create hidden exposure

2.

Verizon’s 2026 report also found breaches involving a third party jumped 60% year over year and now account for 48% of all breaches. Fewer third-party hops mean fewer places for risk to enter.[4]

AI is raising the stakes

3.

Deloitte’s 2026 State of AI in the Enterprise survey found 74% of organizations hope AI will drive revenue growth, yet only 20% say it is doing so today. A network that cannot deliver predictably can become an invisible blocker to AI scale.

The trust gap enterprises can no longer afford to ignore

Trust failures rarely stay abstract. They tend to hit the initiatives enterprises can least afford to delay: AI and data-driven projects, security and compliance programmes, digital transformation and market expansion. If one of those projects stalls for a quarter because of a provider issue the business could not see, the cost is no longer just network-related.

That is why ownership and operational control matter more than buyers often realize. Network ownership may not always appear at the top of procurement scorecards, but it is often what makes security, resilience and data sovereignty possible in practice.

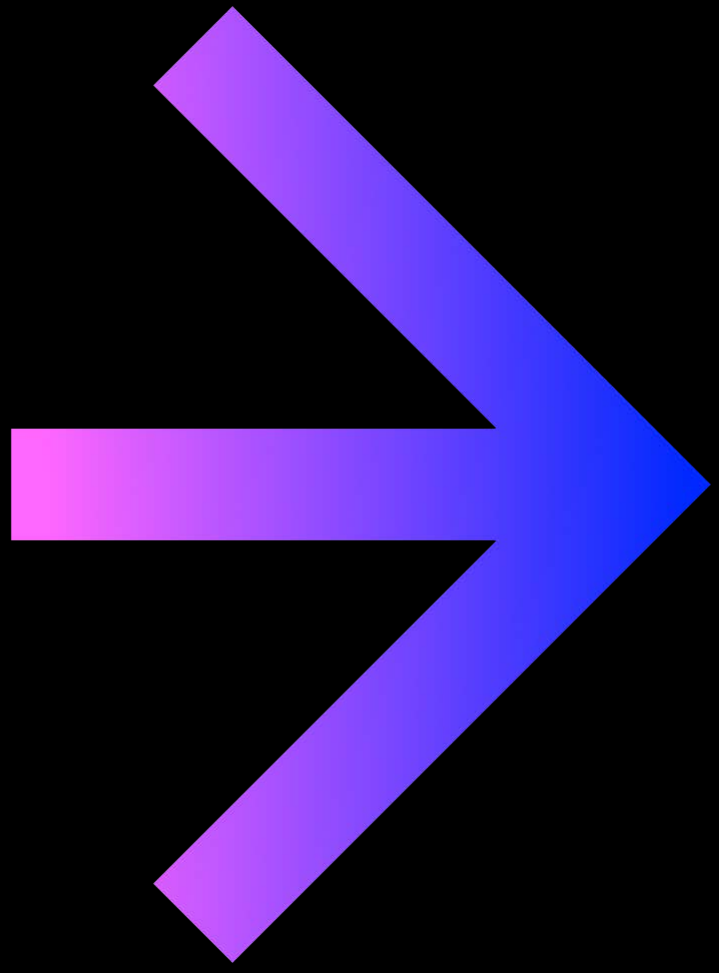
The trust gap enterprises can no longer afford to ignore

Ownership alone is not the full answer, though. What matters is network cohesion: whether a provider has genuine familiarity with the full operational stack, from fiber through to network management systems.

A provider that owns and understands that stack can give clearer answers about where risk sits and who is accountable when something goes wrong.

Fewer hops.
Less risk.

Trust isn’t written
into your SLA



Trust isn’t written into your SLA

An SLA tells you what your provider has promised. It doesn’t really tell you what happens the moment something breaks, and that gap is where trust really gets tested. Detection speed, escalation quality, transparency and operational familiarity are often the things that matter most in a serious incident, yet they are rarely captured properly in standard service terms.

Only 15% of leaders have complete confidence in their provider’s ability to detect a serious incident quickly

Trust isn’t written into your SLA

Our report highlights the problem sharply: only 15% of leaders have complete confidence in their provider’s ability to detect a serious incident quickly. Leaders are more confident in their own organisation’s ability to respond once an incident is identified than in their provider’s ability to spot it early. That may sound reassuring, but it points to the real risk: by the time response begins, the walls may already have been crossed.

Most SLAs were built for a slower threat environment. AI is changing that by accelerating traffic growth, increasing operational complexity and shortening the time available to detect and contain threats. Buyers therefore need to look beneath the SLA and ask whether the provider can prove readiness under modern conditions, not simply promise availability on paper.

Five questions to ask before you sign

1. What is the price not telling you?

98% of leaders say they would pay more for a provider that could consistently demonstrate trust-worthiness. Evaluate risk as well as cost. The market already values trust over cost — it's just that procurement processes don't always reflect it.

2. What sits underneath the SLA?

Ask who owns the topology, how many networks are involved and whether the provider understands the full stack from fiber to management systems.

3. Where is the evidence?

Look for independent satisfaction data, incident response history, detection metrics and clear examples of what changed after a serious event. Ask how past incidents were handled; what changed afterwards is often the strongest signal.

4. Is security built-in or bolted-on?

No provider can protect you from everything: even the best network cannot save you from a compromised password or successful phishing email.

Ask whether the network and its management systems operate in a separate, tightly controlled domain, with protections such as DDoS mitigation built-in rather than added later.

5. Where does your data actually go?

Storage location proof is not enough. A provider that owns its network can show the full route; one leasing capacity usually cannot. Ask where your data is stored, which jurisdictions it transits and how compliance is evidenced.



Why Arelion

Arelion helps enterprises close the trust gap by making trust easier to prove. We own and operate our own global backbone, ranked the world's number one IP network, rather than relying on a patchwork of leased capacity. That means fewer third-party dependencies, clearer accountability and greater transparency into how data moves.

For enterprises scaling AI, strengthening security, managing compliance or expanding into new markets, network trust can no longer stay assumed. It needs to be tested, evidenced and designed into the infrastructure behind the SLA.



Before your next important network decision, ask us to help you test what your current provider can really prove — and where hidden risk may be hiding under the surface.

1 https://foundryco.com/research/research-ai-priorities/

2 https://www.riskrecon.com/predicts-2026-third-party-cybersecurity-risk-management-evolves-for-the-ai-era-march-2026

3 https://www.verizon.com/about/news/breach-industry-wide-dbir-finds

4 https://www.verizon.com/about/news/breach-industry-wide-dbir-finds

Arelion

Learn more insights and
read the full report here