WHITEPAPER

The Hidden Cost of Fiber Consolidation

For Infrastructure and Network Engineering Leaders

Consolidation does not simply change the nameplate on your circuit. It potentially changes the failure domain underneath it.

By Doug Turtz, Chief Revenue Officer at Lightpath

About This Paper

This paper is for VPs of Infrastructure and Network Engineering responsible for enterprise network resilience across multiple sites, data centers, applications or regions.

While the changing nature of underlying infrastructure should be under review consistently by network operations, this focuses on a specific event taking place in the telecommunications industry as the backdrop for diving deeper into fiber consolidation and network diversity risk. Zayo's acquisition of Crown Castle's fiber solutions is a structural change to the network environment of every enterprise that sources fiber networking services from either provider. These events may introduce vendor consolidation at the physical, operational and ownership layers affecting enterprise resilience.

This paper is a diagnostic framework for the enterprise leaders — the ones who need to confirm that their diversity assumptions, as originally designed, hold true after vendor consolidation events.

The goal is to make the case that diversity assumptions formed previously require formal review — and that now, while conditions are stable, is the lowest-risk time to do this analysis. And should those assumptions turn out to be challenged, now is the time to enact change.

Executive Summary: The Case in Plain Terms

The five shifts introduced by consolidation — **physical convergence, operational coupling, centralized remediation, reduced ownership independence and knowledge degradation** — reshape enterprise risk whether or not it shows up in uptime metrics, SLAs or contracts. These changes don't happen all at once. They build quietly over time and often remain invisible at the logical or contractual level.

Risk can increase even when nothing has gone wrong. Favorable conditions aren't the same as proven resilience. Consolidation makes certain types of correlated failures more likely. They're rare, but when they happen, the impact is outsized — especially in environments where more workloads rely on fewer aggregation points to support mission-critical operations.

The right response is formal validation. Consolidation creates a clear, time-bound reason to reassess. Governance now expects evidence, not assumption. And proactive validation is almost always less costly than reacting after the fact. Just as important, validation doesn't commit you to change — it commits you to clarity.

Fig 1: The Window Between Consolidation and Correlated Failure

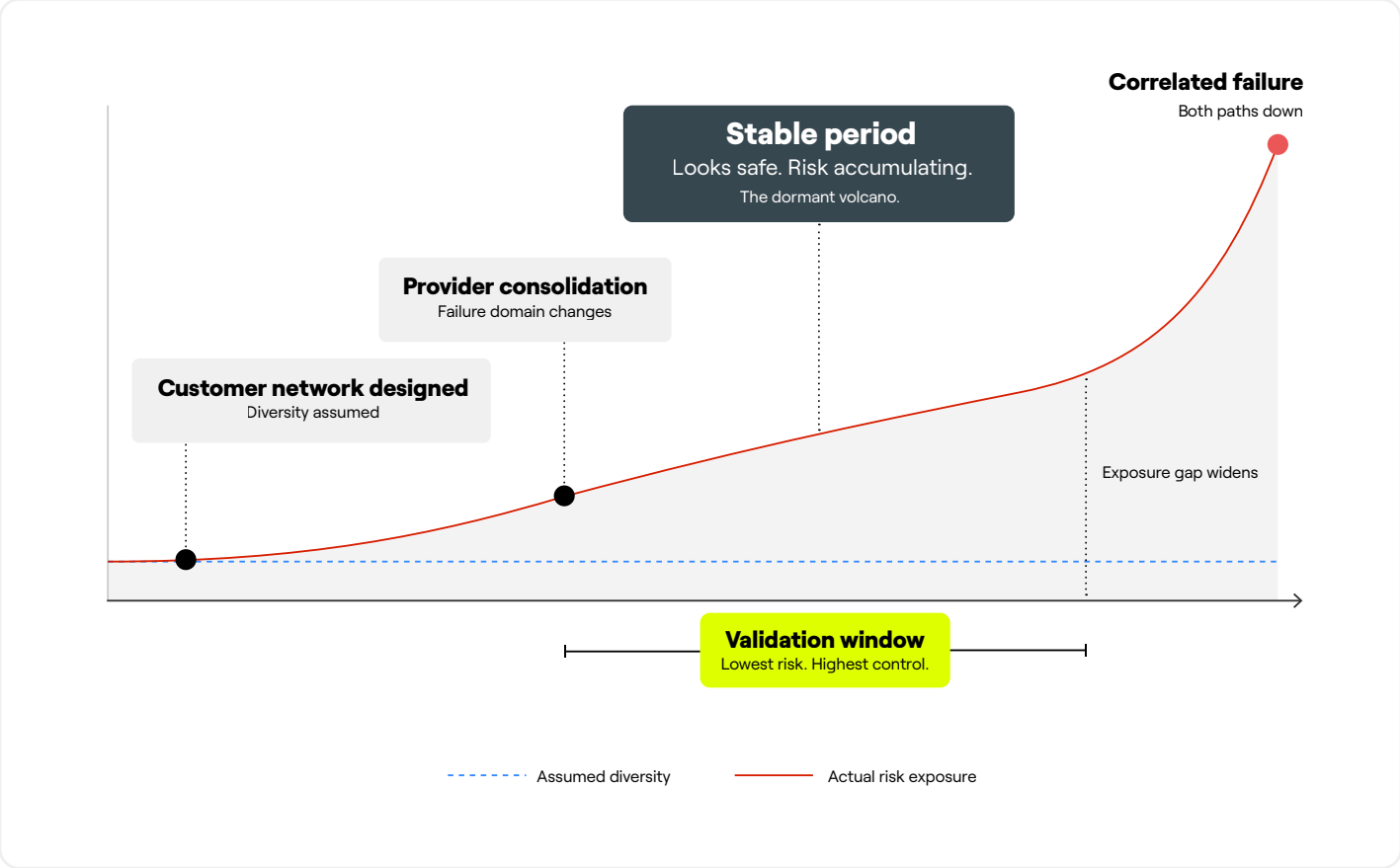

Fig 1: The validation window is open now, before a correlated failure closes it. Formal validation now costs less — in every dimension — than reactive remediation after an incident.

The organizations most exposed are often the ones that completed a diversity review during initial design and haven't revisited it since. What was sound three years ago may no longer be — not because of a single visible change, but because these structural shifts have accumulated beneath the surface.

Validating now, while systems are stable, creates the space to answer the right questions on your terms — before a correlated failure forces the issue.

The real question isn't whether an outage happened. It's whether your architecture can survive in a post-consolidation environment — and whether you can defend it if something goes wrong.

Why Risk Increases Even Without Outages

The Most Dangerous Phase

The most dangerous phase following consolidation is often the one that looks the safest: the period before the first major correlated failure. Stability is not the same as resilience. The two feel identical — until they aren't.

During this period, systems function normally. Uptime holds. No incidents have intersected the newly shared failure domain. Nothing in day-to-day network operation signals that anything has changed.

But there is a counter narrative worth exploring. Enterprise customers receiving communications from account teams preceding and immediately following a vendor consolidation event, are hearing a consistent message: the acquisition is a positive development, service will be uninterrupted and the combined network will be stronger. That message addresses service continuity. It does not address structural independence.

Historical Uptime Is Not a Resilience Indicator

Networks continue to operate normally after consolidation for a straightforward reason: nothing has gone wrong yet. No construction crew has cut the shared conduit that now carries both of your diverse circuits. No regional facility has experienced simultaneous power loss affecting multiple paths. No operational error has propagated across previously isolated networks. No grooming of POPs has caused an outage on what was believed to be diverse POP infrastructure.

This is not resilience. It is favorable conditions, like a dormant volcano.

The distinction matters because most internal conversations about network risk default to historical uptime as the primary evidence. “We’ve had no major outages in three years” is treated as a proxy for “our architecture is sound.” Post-consolidation, those are different claims. One describes what has happened. The other describes what the architecture can withstand — and that requires different evidence.

The Core Problem

Absence of outages means nothing has gone wrong yet. It does not mean nothing can go wrong. Post-consolidation, the failure domain has changed. The architecture has not been reassessed. The gap between them is the risk.

Correlated Failures: Low Frequency, High Impact

Consolidation doesn’t make single-circuit outages more likely. It increases the risk of correlated failure — a single event that disrupts multiple circuits or paths that were designed and assumed to operate independently.

These failures often stem from shared exposure: a single excavation cutting through conduit that carries multiple “diverse” circuits; a regional power or facility issue affecting infrastructure that now overlaps; an operational error that propagates across networks that were once isolated; or a major weather event that reveals hidden physical co-location.

They’re rare. But their impact is anything but.

A correlated failure doesn’t scale linearly. Losing three circuits at once doesn’t create three times the disruption — it creates exponentially more. Failover paths don’t perform as expected. Redundancies collapse. Multiple critical systems can go down at the same time.

And the organizations most at risk are often the ones that have never experienced this kind of event. Their assumptions about resilience were shaped under different conditions — before consolidation changed the nature of failure itself.

Legacy Design Assumptions Persist After Environment Changes

Enterprise network architectures are designed at a point in time, based on conditions that existed at that time. The diversity assessment done three years ago was valid for the environment three years ago: two providers, two ownership structures, two operational organizations, two independent physical plants.

Consolidation changes that environment — but it does not automatically trigger review of the architecture built on it. This creates a gap between the assumptions embedded in the current design and the actual structure of the network today. The gap does not manifest as an alert or a notification. It accumulates quietly, and the architecture that was sound at design time becomes progressively less sound as post-consolidation integration proceeds.

Fig 2: What Consolidation Changes About Your Assumptions

Legacy assumption	Post-consolidation reality
Different providers = different fiber	Different providers may share common ownership and physical plant
Two POPs = two independent network entry points	POPs consolidate post-merger — both circuits may share one facility
Separate contracts = separate operations	Unified operations regardless of contract structure
Diversity assessed once at design is sufficient	Diversity requires ongoing validation as infrastructure changes
Historical uptime = architectural soundness	Uptime reflects conditions, not validated resilience
Two NOCs = two independent escalation paths	One consolidated NOC may handle both circuits

Fig 2: Every assumption in the left column was valid when it was formed. Consolidation invalidates them without triggering a review. In all instances, this is no longer a two-provider solution.

Risk Accumulates Quietly

As enterprise environments become more centralized and workload-dense, the business impact of network failures grows. More applications depend on fewer aggregation points. Failover paths carry greater revenue and operational criticality. The window between “network degraded” and “business operations interrupted” compresses.

Consolidation risk does not accumulate in isolation — it accumulates against a backdrop of increasing dependency. The same correlated failure that would have been a manageable incident two years ago, today could shut down business operations, because the architecture assumed diversity that no longer exists and the workloads that depend on it have grown.

Risk compounds incrementally and often invisibly. It does not announce itself. It surfaces under outage conditions, when remediation options are constrained and leverage with providers is minimal.

What Consolidation Actually Changes

The risk created by consolidation rarely shows up first in contracts, circuit inventories or billing records. It shows up deeper in the structure of the network itself.

When two fiber providers merge, most enterprise teams start with the visible checks: Do the SLAs still hold? Are the circuit IDs unchanged? Is billing still stable? In many cases, the answer is yes. And for many organizations, that is where the review stops.

That reaction is understandable. But it misses the real issue.

Consolidation changes the operating reality beneath the contract layer. It can reshape how infrastructure is shared, how failures propagate, how remediation is prioritized, how control is exercised, and how institutional knowledge is retained. None of that may be obvious in the moment. All of it can materially change enterprise risk.

The five structural changes that follow are the mechanisms that matter most. Each one operates below the level most customers are used to monitoring. And each one can alter resilience, even when no service term has changed and no outage has yet occurred.

Fig 3: What Your Records Show vs. What Consolidation Changes

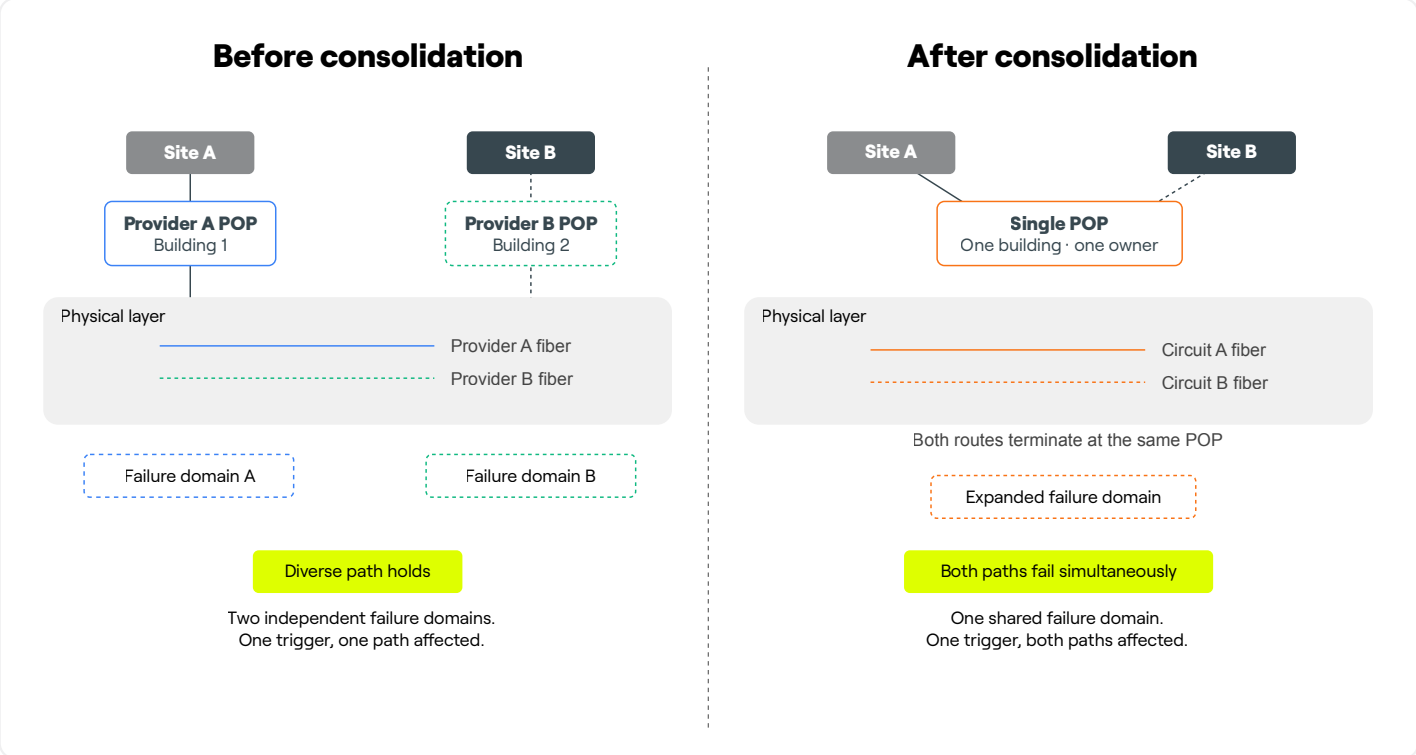

Fig 3: Separate circuits and separate conduit in the ground are not sufficient. If both routes terminate at the same POP, diversity does not exist at the ownership layer. There is no longer a two-provider solution.

1. Operational Coupling

The first change consolidation introduces is rarely visible — and often not immediate.

In the early stages, systems may still appear separate. Different circuit IDs. Different portals. Different escalation paths. On paper, the architecture looks unchanged.

But over time operations begin to unify. Shared field crews. Shared network operations centers. Shared dispatch workflows and repair queues.

This shift is driven by efficiency. But it changes how the network behaves under stress.

At 2 a.m., when multiple circuits require attention at the same time, there aren't independent teams responding. There's one crew. One dispatch queue. One set of prioritization decisions.

The architecture may still look redundant. The operational reality is not.

Key Risk Pattern

During an incident, a single staffing constraint, procedural error or repair prioritization decision can affect multiple services at once — regardless of how independently they were designed to operate.

Stephen Palomba, Senior Network Engineer at St. John's Episcopal Hospital, put it plainly after experiencing repeated connectivity failures with a prior provider:

"When it comes down to it, I don't pedal the bike. I must rely on someone else to pedal; if they are not delivering, it looks bad for the hospital and me."

Post-consolidation, the number of organizations you depend on shrinks to one — but the consequences of that dependency don't.

2. Escalation and Remediation Centralization

As operations converge, so does decision making.

During major events — fiber cuts, facility outages, cascading failures — escalation and repair are no longer managed independently. They are coordinated once, at the organizational level.

In practice, circuits designed as independent recovery paths may compete with each other during an outage. The same approval chain governs both. When one is prioritized, the other waits.

This isn't a failure of intent. It's a structural outcome of consolidation.

And it further reduces the practical independence of recovery — even when redundancy still exists on paper.

3. Localized Knowledge Degradation

As operations and decision making centralize, something less visible begins to erode: localized knowledge.

Before consolidation, engineering and field teams build deep familiarity with specific routes and regions. They know which conduit floods in the spring, which splice point was a temporary fix, which segment carries marginal signal but hasn't yet failed.

That kind of knowledge doesn't transfer cleanly in a merger.

Teams are reorganized. Coverage areas expand. Individuals take on broader scope. Over time, the route-level awareness that helps teams anticipate and prevent issues begins to fade.

Unlike operational coupling or centralized escalation, which affect how incidents are handled, knowledge degradation affects whether issues are caught early at all.

The impact shows up in slower diagnosis, longer repair times and missed early warning signs. Small issues escalate. Repeat failures occur because the historical context is gone.

> ***And critically, this loss of context amplifies every other risk in the system —*** making operational conflicts harder to resolve, remediation slower to execute and structural issues harder to detect before they fail.

4. Loss of Ownership Independence

Beneath operations, remediation and knowledge sits a more fundamental shift: ownership.

Before consolidation, two providers make independent decisions about capital investment, route hardening, maintenance timing and risk tolerance. Different incentives create natural diversification.

After consolidation, those decisions are made by one organization — one capital plan, one set of priorities, one definition of acceptable risk.

Circuits that appear independent at the contract level now share the same strategic and financial decision making. The question is no longer how two providers will respond differently — it's how one provider will allocate resources across competing needs.

This doesn't always create immediate risk. But it shapes how the network evolves — and where resilience is strengthened or allowed to degrade over time.

5. Physical Infrastructure Convergence

Over time, those strategic decisions translate into physical change.

What begins as separate infrastructure under common ownership is gradually rationalized. Through maintenance, optimization and cost pressure, networks are reconfigured: shared conduit, shared laterals, consolidated splice points, fewer POP and hub locations.

This process is incremental and largely invisible to customers. It happens through internal work orders, not contract updates.

Months or years after consolidation, routes that were designed to be physically independent may share the same pathway at critical points.

At that stage, the shift is no longer operational or organizational. It is structural.

> ***Contractual or provider diversity does not guarantee physical diversity once assets fall under common ownership. Logical separation can persist even as physical separation erodes.***

If your redundancy strategy assumes two providers equal two independent paths, that assumption requires ongoing validation — because over time, it may no longer be true.

Why Formal Validation Is the Right Response Now

Consolidation is one of the few moments when infrastructure changes in a way that's visible, documented and tied to a specific point in time. Most risk accumulates quietly. This doesn't.

That makes consolidation a clear trigger for action — a chance to reassess while conditions are still stable, not after something breaks.

There are four conditions that make formal validation the right move now — while you still have the advantage of time.

Consolidation Is a Recognized Trigger Event

One of the practical challenges of proactive network review is justifying it internally. In a stable environment, the question "why now?" can be difficult to answer without sounding alarmist. Resources are constrained. Competing priorities are real.

Consolidation provides the precipitating event. It is an external, documented change to the network environment — and it gives infrastructure leaders a straightforward, defensible rationale for scheduling a formal review.

From a governance standpoint, this is one of the few moments where reassessment is expected rather than questioned. The window is finite. As post-consolidation integration proceeds and the changes become normalized, the trigger loses its weight, and the review becomes harder to justify.

Fig 4: What a Network Diversity Validation Examines

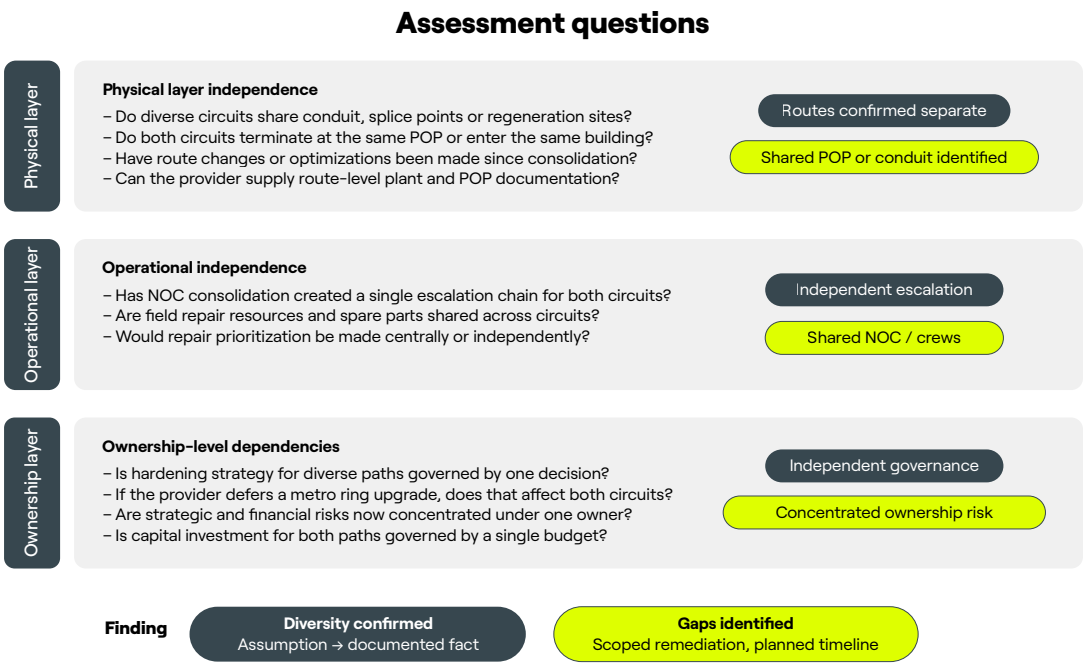

Fig 4: Either finding has value. Confirmed diversity is a documented fact. Identified gaps are a scoped, actionable remediation.

Governance and Accountability Expectations Have Shifted

Boards, regulators, auditors and insurers increasingly require organizations to demonstrate resilience through evidence, not assumption.

"We believed our circuits were diverse" is no longer a satisfactory answer to audit questions or incident post-mortems — particularly when the consolidation event that invalidated that belief was publicly documented and the organization took no formal action in response.

Formal validation produces documented evidence of due diligence. If the assessment finds that diversity remains intact, that finding is defensible to any auditor or insurer who asks. If it finds gaps, those gaps can be addressed on a planned timeline rather than under incident pressure — which is both cheaper and more defensible than the alternative.

Proactive Validation Costs Less Than Reactive Remediation

The cost comparison is not close. Proactive validation requires time and coordination. Reactive remediation requires all of that, plus the business disruption of a major outage, the reputational damage of a failure that could have been anticipated and the negotiating disadvantage of needing emergency solutions from the same provider whose consolidation created the exposure.

Fig 5: Proactive Validation vs. Reactive Remediation

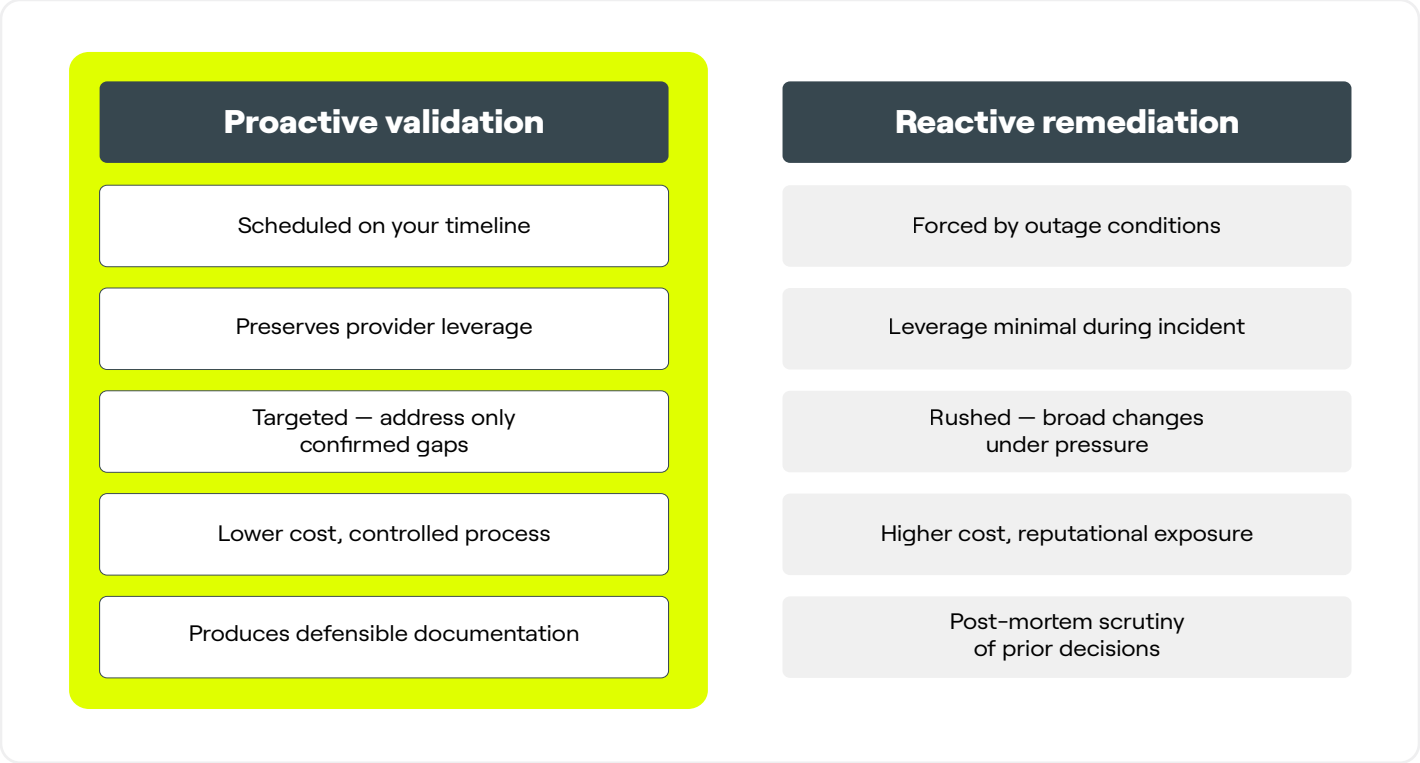

Fig 5: Proactive validation preserves leverage, controls cost and produces documentation that holds up. Reactive remediation does none of those things on your terms.

Validation Does Not Presume Change

A formal network diversity validation is not a commitment to architectural change. It is an assessment. The outcome may be a clean finding — a confirmation that your current architecture maintains genuine physical and operational independence. That is a valuable result. It converts an assumption into a documented fact.

If the assessment does find gaps, it identifies specific, bounded risks — not a mandate to rebuild. Targeted remediation addresses confirmed exposure, not theoretical vulnerability. The work is scoped, justified and defensible.

The objective is confidence and defensibility. A well-structured validation process does not produce unnecessary disruption.

A Framework for Network Diversity Validation

For infrastructure leaders who have decided that formal validation is warranted, the following framework covers how to scope and execute the assessment.

1. Define the Scope

Not every circuit in your portfolio carries equal risk. Scoping the validation means identifying which circuits and paths are designated as primary/secondary failover pairs for latency-sensitive or revenue-critical applications; sourced from providers involved in a recent consolidation event; last formally assessed for physical diversity more than 18 months ago; or crossing geographic areas where the consolidating providers had overlapping infrastructure.

> ***Start with the circuits that combine high business criticality and post-consolidation provider overlap. That is where the exposure is most likely to be real.***

2. Validate Physical Layer Independence

The harder problem is not knowing what to ask for — it is getting a consolidated provider to produce it.

Verification at the physical layer means confirming — not assuming — that circuits designated as diverse do not share conduit, manholes, splice points, regeneration sites or colocated facilities. This requires route-level documentation from the provider, not circuit-level confirmation from an account team.

Account teams can confirm that two circuit IDs exist and that contracts describe them as diverse. In most cases, providers can share street-level route maps on request. What account teams typically cannot provide, and what requires escalation to network operations or engineering, is POP-level detail: where your circuits terminate, which building they enter and where the lateral entrances are. Getting it requires asking for it explicitly, escalating past the account team when necessary, and framing the request in terms of your contractual diversity commitments rather than as a general inquiry.

If your provider cannot or will not confirm physical layer independence at the route level, that is itself a finding. Document the request, the response and the date. That record has value in any future governance review or incident post-mortem.

Questions to put in writing for your provider

1. Please provide a street-level as-built map of the network routes serving our designated diverse circuits.
2. Please share the POP locations on our network and identify the lateral entrances to each building or data center we connect into.
3. At which points, if any, do our designated diverse circuits share conduit, splice enclosures, regeneration sites or colocated facilities?
4. Have any route changes, maintenance reroutes or network optimizations been made since the consolidation closed?
5. Are the diverse paths served by separate NOC escalation chains and separate field repair crews?
6. Are spare parts and repair resources independently stocked for each path, or drawn from a shared pool?

3. Map Operational Independence

Physical independence is necessary but not sufficient. Operational independence, such as having separate crews with their own repair authority and unique escalation paths, determines how quickly each path can be restored independently if both fail simultaneously.

This assessment looks at whether NOC consolidation has created a single escalation chain for both circuits; whether field repair resources are shared across circuits that are supposed to be independent; whether the same change management windows govern maintenance on both paths; and whether repair prioritization decisions would be made independently or centrally.

4. Assess Ownership-Level Dependencies

This is the assessment most enterprise teams skip entirely because it does not fit neatly into a circuit review. It requires a different kind of question: Is the capital investment, hardening strategy and route protection for your diverse paths governed by a single ownership decision? If the post-consolidation organization decides to defer hardening on a particular metro ring, does that decision affect both of your "diverse" circuits?

If the answer is yes, you have ownership-level concentration risk. That does not necessarily require immediate action, but it should be documented, disclosed to appropriate stakeholders and incorporated into your resilience planning.

5. Document the Findings

The outcome of a validation only has organizational value if it is documented. A finding that lives in someone's memory, or in notes from a single meeting, does not satisfy governance requirements, cannot anchor a budget request and provides no defense in a post-mortem.

If diversity is confirmed: that documentation supports governance requirements, provides a baseline for future reassessment and converts a working assumption into a verified fact. If gaps are identified: documentation scopes the remediation, justifies the budget request and demonstrates due diligence.

In either case, the documentation should be dated, attributed and retained — because the relevant question in any future incident or audit is not just what the architecture is, but what steps the organization took to understand and manage its risk.

Request a Route Mapping Session

In 60 minutes, you'll know exactly where your current provider's routes overlap with ours — and where genuine physical separation exists for your critical paths.

The session covers:

- Your current provider's fiber routes mapped against Lightpath's network at the geographic and route level
- Where your designated diversity paths share common corridors with your current provider's infrastructure
- Where Lightpath's routes offer genuine physical separation for your critical applications
- A clear picture of what an independent alternative path looks like for your specific environment

lightpathfiber.com | 877-544-4872

Lightpath