5

Five visibility mistakes organisations keep making

and how to avoid them...

Network visibility has become foundational to modern security and operations. Yet even with best-in-class platforms like Gigamon, many organisations struggle to realise sustained value.

The issue is rarely the technology. It is how visibility is approached, owned and evolved over time.

Based on real-world experience in both enterprise and service provider sectors at Vizst Technology, here are five common mistakes we see - and what mature teams do differently.

1 Treating visibility as a short-term fix

Visibility initiatives are often introduced to address an immediate gap - a new security requirement, a compliance deadline or a specific incident. When the focus is short term, visibility becomes reactive and tactical rather than strategic.

What works better

Approach visibility as a long-term capability. Define what it needs to support over the next 12 to 36 months, including growth, resilience, and evolving security priorities - not just the problem in front of you today.

2 Designing for today's network only

Networks change faster than most visibility architectures. Cloud connectivity, East-West traffic, remote users and new security controls quickly expose design limitations.

What works better

Architect visibility with change in mind. Designs should assume growth, architectural evolution and new data consumers rather than optimise only for the current state.

3 Letting visibility become siloed

Visibility often ends up owned by a single team - typically security or networking. This limits value and creates duplicated effort elsewhere.

What works better
Design visibility as shared infrastructure. When security, networking and operations teams consume the same trusted data, outcomes improve without additional tooling.

4 Treating AI as a switch, not a journey

Advanced analytics and AI-driven insights are often expected to deliver immediate value. In reality, poor data quality and inconsistent visibility limit their effectiveness.

What works better
Stabilise and govern visibility first. AI capabilities deliver meaningful insight only when data is complete, consistent and trusted.

5 Failing to wrap visibility in a service model

Even well-designed visibility architectures struggle without a delivery and governance framework. Tools alone cannot adapt to organisational and technical change.

What works better
This is where Vizion by Vizst comes in - providing an operating model around Gigamon that includes ownership, continuous improvement and accountability. Vizion ensures visibility remains aligned to business priorities rather than becoming another unmanaged platform.

Strong visibility is not about collecting more data. It is about having confidence in what your network is doing, how it supports security and resilience, and how it will scale over time.
If you are using Gigamon today or considering it as part of your security and observability strategy, we can help you avoid these common pitfalls.
Talk to Vizst about Gigamon delivered through Vizion by Vizst - and make network visibility work the way it should.

Speak to our experts today