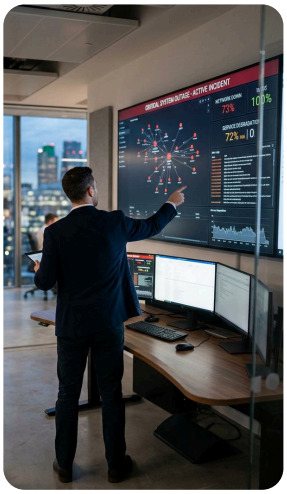
ClearView AI

USE CASE

Proof, not finger-pointing:

Using network evidence to resolve cross-team IT disputes



When a critical application slows down, the problem is rarely just technical. It quickly becomes operational.

The application team says the network is the issue.
The network team says the WAN is healthy.
The ISP says the circuit is fine.
Users keep complaining, leadership wants answers, and the resolution drags on.

This is a common failure point in IT operations: too many teams, too many tools, and no shared source of truth.

GFI ClearView AI helps stop the blame game. It provides IT teams with neutral, timestamped, application-aware evidence of what was happening on the network at the moment users experienced the issue. Instead of chasing opinions, teams can work from facts.

The business problem

In many organizations, application performance issues create friction across internal teams and external providers.

Without clear evidence:

- Root cause analysis takes too long
- Escalations become subjective and difficult to defend
- Internal teams lose time proving innocence instead of solving the issue
- Providers can delay action because the issue has not been clearly demonstrated
- Business users lose confidence in IT

For IT leaders, this means longer outages, higher operational costs, and more tension between teams that should be working together.

What IT leaders need instead

Decision-makers do not need more finger-pointing. They need faster answers.

They need a way to:

- See what happened during the incident window
- Understand if the problem was network-related or not
- Validate provider performance with evidence
- Give teams a common operational view
- Reduce mean-time-to-resolution across shared ownership environments

That is where **GFI ClearView AI** fits.

How GFI ClearView AI helps

GFI ClearView AI provides visibility into network and application behavior, enabling IT teams to investigate incidents using shared, objective data.

With GFI ClearView AI, teams can review:



Timestamped traffic behavior
during the exact period of degradation



WAN and link conditions
to identify congestion, latency, or packet loss



Historical evidence
to support escalation and post-incident review



Application-aware visibility
to see which apps were active and affected



Bandwidth consumption patterns
to see what else was competing for resources

This allows teams to answer the question that matters most: **Where is the problem actually happening?**

From assumptions to evidence

When an ERP, CRM, VoIP platform, or cloud application slows down, GFI ClearView AI helps separate perception from fact.

Instead of asking:	Teams can see:
✗ "Was it the network?"	✓ If the WAN link was healthy
✗ "Was it the ISP?"	✓ If a specific application experienced abnormal behavior
✗ "Was it the application?"	✓ If bandwidth contention was present
✗ "Was someone saturating the link?"	✓ If the issue aligns with provider-side conditions
	✓ If the network was normal, pointing the investigation elsewhere

That changes the tone of the entire incident. It turns a defensive conversation into a fact-based one.

GFI ClearView AI as a single source of truth

In multi-team environments, the real challenge is often not a lack of data. It is a lack of trusted data that everyone accepts.

GFI ClearView AI becomes the common reference point because it is:

- **Neutral** across teams and vendors
- **Time-based,** so investigations focus on the real incident window
- **Application-aware,** so business impact is easier to understand
- **Historical,** so that issues can be validated after the fact
- **Practical** for both internal troubleshooting and provider escalation

That shared view reduces friction and helps teams align faster.

Example scenario

A company's ERP becomes slow during peak hours.

- The application team believes the WAN is unstable.
- The network team sees no obvious outage.
- The ISP reports the circuit is operating normally.

Using GFI ClearView AI, IT reviews the incident timeframe and finds that a large backup-related transfer was consuming bandwidth at the branch edge during the same period that users reported poor ERP performance. WAN health was stable. The ISP was not the problem. The ERP itself was not failing. The issue was localized bandwidth contention.

Instead of spending hours in back-and-forth across teams and vendors, the organization identifies the source quickly and takes corrective action.

That is the difference between troubleshooting with opinions and troubleshooting with proof.

The outcome

With GFI ClearView AI, organizations can:

- Reduce mean-time-to-resolution
- Cut the operational cost of cross-team disputes
- Improve the quality of provider escalations
- Give leadership clearer answers
- Create a more disciplined, evidence-based troubleshooting process

GFI ClearView AI provides IT teams with neutral, application-aware network evidence that helps them identify where performance problems actually reside, resolve incidents faster, and stop the blame game between teams and vendors.

Ready to get started?

Request your free trial

Contact: sales@gfi.com gfi.ai/clearview

Copyright © GFI USA, LLC, All rights reserved.