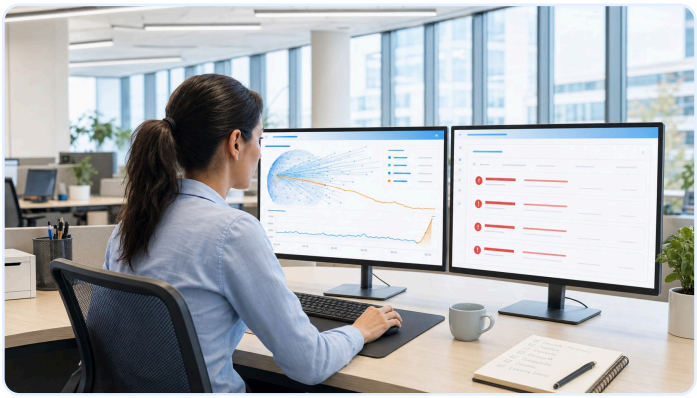
LanGuard

PRODUCT PAIRING

The signal nobody could read

GFI LanGuard + GFI ClearView AI + GFI AppManager AI



It started with a complaint about slow internet.

Not an alarm. Not a security alert. Just a message from the sales floor on a Monday morning: video calls are choppy, the CRM is lagging, could someone take a look? The kind of thing usually explained by a software update running in the background or someone streaming something they should not be.

The network administrator opened GFI ClearView AI. Thirty seconds later she had her answer. Or at least the beginning of one.

What GFI ClearView AI saw

GFI ClearView AI was reading the wire.

Without decrypting HTTPS traffic, GFI ClearView AI had been watching the traffic of every application and every conversation on the network with up to 1-second granularity. In the real-time host monitor, something was immediately visible: one device consuming a disproportionate share of outbound bandwidth. Steady, persistent, consistent. Not a spike. A slow, continuous stream to an external destination that matched no known business application.

GFI ClearView AI had found the signal. What it could not tell her was what was generating it.

Without GFI LanGuard: the signal with no name

She checked the DHCP logs. The IP had been assigned three weeks ago. The lease had been reassigned twice since. Records were incomplete. She walked the floor. Nobody recognized it.

Eventually she found it. In a storeroom adjoining the main office, plugged into a wall socket nobody had considered in months: a workstation from a previous employee's desk. Decommissioned in theory. Still powered on. Still connected. Still doing something.

She unplugged the machine. Filed an incident report. Wrote "*cause: unknown*" in the summary field.

The honest answer to "*what happened?*" was: she did not know.

With GFI LanGuard: the signal with an explanation

Same Monday. Same complaint. Same GFI ClearView AI alert for the same IP.

This time, cross-referencing the IP in GFI LanGuard returned an immediate result. The device was in scope. Three weeks ago it had appeared on the network, been picked up by GFI LanGuard's automatic discovery, and scanned within the next scheduled cycle. What GFI LanGuard found: four critical unpatched vulnerabilities, including one publicly associated with remote access toolkits designed for persistent low-volume data exfiltration. She looked at the CVE. Remote access toolkit. Persistent low-volume exfiltration.

The signal had a name now. GFI ClearView AI had seen the behaviour. GFI LanGuard explained it.

With GFI AppManager AI: the connection made before Monday

Running GFI ClearView AI and GFI LanGuard separately still leaves the gap that mattered in this story: **they cannot see each other.**

Without GFI AppManager AI, the GFI ClearView AI traffic alert and the GFI LanGuard High-severity alert for the same device exist in two disconnected systems. The connection between an unusual IP in one console and a critical CVE in another requires the administrator to make the link manually. If she thinks to look, and if she knows where.

In GFI AppManager AI, both are in the same session. GFI ClearView AI's top traffic consumers sit alongside GFI LanGuard's High-severity device alerts, same view, same network. The device with the unusual outbound stream and the device with four critical CVEs are the same entry. The connection is not a deduction. It is visible.

By Thursday of the previous week, before the Monday complaint, that device's GFI LanGuard alert was already in GFI AppManager AI, in the same session as GFI ClearView AI's bandwidth dashboard. An administrator who saw both would have had a question worth asking four days earlier. And when the device needs containing, the response runs from the same session: restrict the device, deploy the patches, and document the remediation, with no second login and no system switch.

See the signal. Name the device. Understand the risk. Act. One session.



GFI Clearview AI

Every application, every conversation, every device on the network visible in real time without decrypting a packet. The signal is there the moment it exists.



GFI LanGuard

Every managed device scanned, assessed, and patched. ~70,000 CVEs, automated remediation across Windows, Linux, macOS and 60+ third-party applications. The device is known. Its vulnerabilities are documented.



GFI AppManager AI

One login, one view. Traffic behavior and device vulnerability in the same session. The signal and the explanation, visible together.

Ready to Get Started?

Request a demo at gfi.ai | Contact sales: sales@gfi.com

Copyright © GFI USA, LLC, All rights reserved.