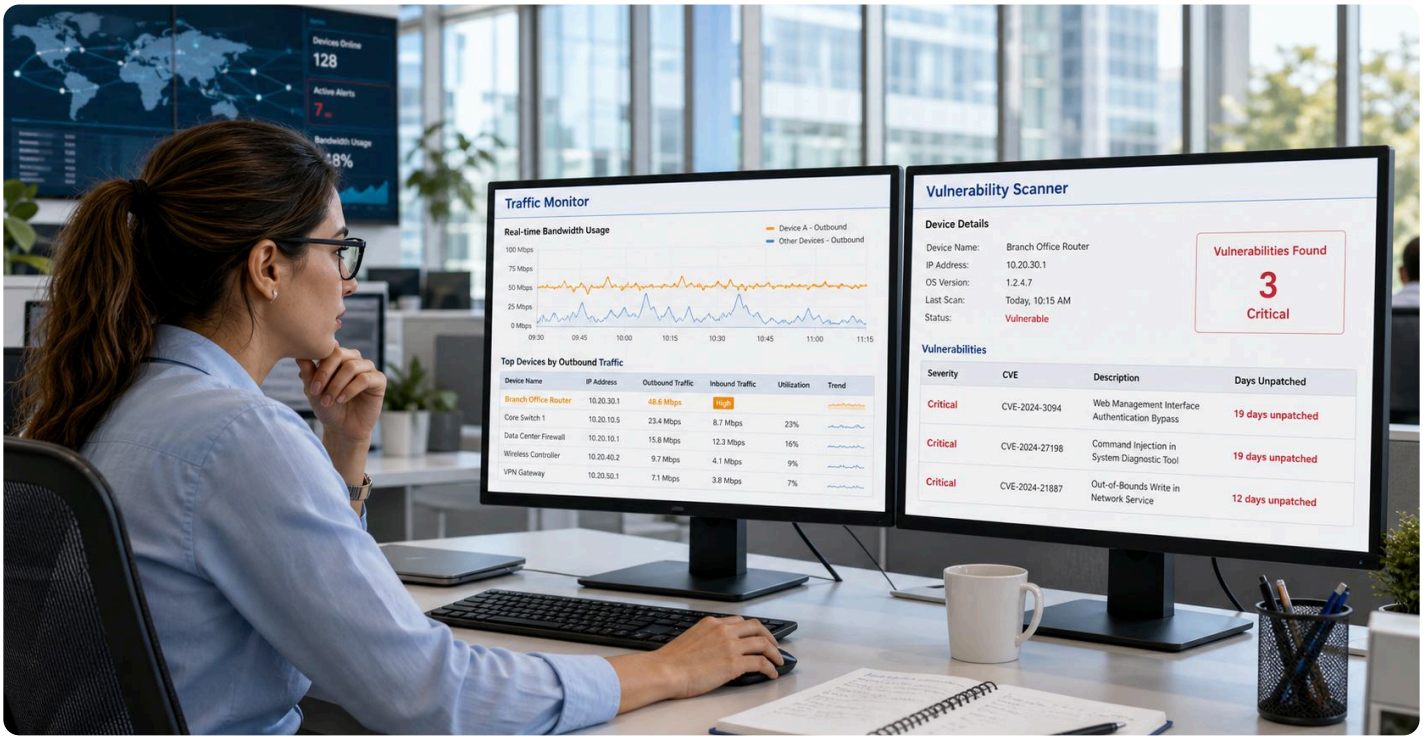
USE CASE

GFI LanGuard + GFI Exinda AI + GFI AppManager AI: The slow drain



Nothing tripped an alarm. No connection got blocked, no helpdesk ticket came in. What gave it away was a pattern in the traffic itself.

GFI Exinda AI had been doing what it always does, classifying and measuring every application on the network in real time. On a Tuesday morning, among the cloud traffic and video calls, one workstation was sending small amounts of data outbound, hour after hour, to a destination that matched no business application GFI Exinda AI recognized. The traffic had started cleanly and kept going. GFI Exinda AI caught it immediately. What it couldn't say was why.

What GFI Exinda AI sees, and what it can do about it

GFI Exinda AI was watching and managing the network, classifying and measuring every application in real time.

It orchestrates network traffic through shaping policies that prioritize critical business applications.

When the slow drain appeared, GFI Exinda AI could not automatically act. The admin had to deliberately create a policy to contain the outbound traffic by assigning it a minimal bandwidth allocation.

Shaping unknown traffic is containment, not a cure. To act confidently, the administrator needed to know the device's software, vulnerabilities, and changes.

That question belongs to GFI LanGuard.

Without GFI LanGuard

Shaping a Symptom

The admin saw the pattern and built the shaping policy. Outbound traffic dropped to the floor, and the network stopped feeling the effect.

The traffic itself didn't stop, though, and she still had no idea why it was happening. Checking the machine by hand turned up nothing obvious. It had been running unattended for weeks on a service account nobody was watching, with one process she didn't recognize.

She logged a ticket: unidentified outbound traffic, source unknown, shaped via GFI Exinda AI, investigation ongoing.

Three days on, the traffic was still there within its minimal allocation, the process was still running, and the vulnerability behind it remained a mystery. GFI Exinda AI had kept the damage in check without ever closing the hole.

With GFI LanGuard

The policy and the fix

Same workstation, same Tuesday, except this time GFI LanGuard is in the picture.

When the pattern appeared, the admin pulled up GFI LanGuard. The machine had been scanned two weeks earlier and flagged with three critical, unpatched vulnerabilities, one of them a publicly documented remote-access CVE that appears in data exfiltration toolkits. A patch had existed for 19 days.

GFI Exinda AI's traffic behavior and GFI LanGuard's vulnerability report were the same event seen from two sides. GFI Exinda AI went first, dropping the drain to almost nothing with a minimal-bandwidth policy, so the device stayed on the network but couldn't move anything worth stealing. GFI LanGuard then pushed an emergency patch for all three CVEs. By the next morning, GFI Exinda AI showed no anomalous traffic, GFI LanGuard confirmed the fix, and the shaping policy was removed.

GFI Exinda AI handled the immediate risk. GFI LanGuard removed the cause.

With GFI AppManager AI: both signals, one session

Run GFI Exinda AI and GFI LanGuard separately, and you have two data streams that somebody has to connect by hand. The line between "odd outbound traffic" and "critical remote-access CVE" only gets drawn if an admin thinks to draw it.

GFI AppManager AI puts both signals in front of you at once. GFI Exinda AI's traffic and GFI LanGuard's alerts sit in the same view, so the decision to shape gets made with the full picture: a deliberate response to a vulnerability that already has a name.

The timing is the real point here. GFI LanGuard's High-severity alert had landed in GFI AppManager AI four days before the Tuesday pattern. An admin watching that view would have patched the machine before the drain ever started.

It works the other way round too. When GFI LanGuard runs a big patch deployment, GFI Exinda AI registers the bandwidth hit in real time as application performance dips and video calls start to stutter. From GFI AppManager AI, the admin writes a GFI Exinda AI policy that pushes patch traffic down the priority list and hands bandwidth back to the applications that need it, no rescheduling required. The patches go out safely, and the network keeps performing.

See the traffic, shape it on purpose, understand the device, patch it, all from one place.

The network usually knows something is off before anyone does, and GFI Exinda AI catches the anomaly the moment it appears and gives you the tools to respond. The device knows more than the network can show, and GFI LanGuard finds the CVE, documents it, and closes it. Put both in GFI AppManager AI, and that quiet Tuesday morning oddity becomes something you can actually close: the traffic has an explanation, and the vulnerability has a name, both in the same view, with the patch a click away.

GFI Exinda AI

Network visibility and active orchestration. Traffic shaping, QoS enforcement, TCP acceleration, edge caching, and real-time bandwidth management. It tells you what's moving across the network and lets you shape it by policy.

GFI LanGuard

Patch management and vulnerability assessment. ~70,000 CVEs, automated patching across Windows, Linux, macOS, and 60+ third-party applications. It tells you what's on the device and gets it remediated.

GFI AppManager AI

One login, one view. GFI Exinda AI's network performance and GFI LanGuard's device security in a single session, so the traffic signal and the device explanation are actionable side by side.

See it, explain it, fix it, from one screen.

Start a free trial and put GFI Exinda AI, GFI LanGuard, and GFI AppManager AI to work on your network today.

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

Copyright © GFI USA, LLC, All rights reserved.