

The device nobody questioned

GFI LanGuard + GFI KerioControl + GFI AppManager AI

Perimeter Secured

Internal Device Vulnerable



The contractor arrived on a Tuesday. Legitimate engagement, signed agreement, visitor badge issued at reception. Friendly enough. Knew his way around a network.

He was given credentials for the shared project folder, standard practice for a short engagement. His laptop connected to the network for that access, and the work began.

Three days later he packed up, shook hands, and left.

His laptop left with him. What it had moved onto the shared folder did not.

Where the perimeter ends

GFI KerioControl was doing exactly what it was built to do. It was watching the boundary.

Every packet crossing the perimeter was inspected. Inbound threats were filtered through IPS, gateway antivirus, and Shield Matrix AI. VPN connections were authenticated. Firewall rules were current. Nothing unauthorized crossed the edge.

GFI KerioControl secures what crosses the perimeter. It does not assess the security posture of devices already inside. That is not its job.

The device was temporary; it came in and went away with the contractor.

Without GFI LanGuard: 60 hours nobody noticed

Friday evening. Most staff had already gone for the weekend. The payload, seeded by the contractor's device onto an internal machine, was activated.

It did not go outward. GFI KerioControl was watching outward. It went sideways. Laterally across the trusted internal network, device to device, using a known vulnerability in the Windows file-sharing protocol. A CVE with a patch that had been available for weeks. On every unpatched machine it reached, it found what it needed. Each one became the next stepping stone.

By Saturday morning it had reached the file server. By Saturday afternoon, the backup server. By Sunday, the site-to-site VPN carried it quietly to three branch offices: all trusted connections, all internal traffic, all completely normal to everything watching the boundary.

Internal devices talking to internal devices. Permitted traffic. No threat. That is what it looked like. Because from the perimeter's perspective, that is exactly what it was.

The IT team found out Monday morning when staff called in to say they could not open anything. Folders encrypted. Backups gone. The phones rang for two hours before anyone started to understand the scale.

Sixty hours. Three sites. One question nobody could answer: *which devices were unpatched, and how long had they been that way?*

Nobody knew. There was no record. There had never been one.

With GFI LanGuard: the vulnerability that had nowhere to go

Same contractor. Same Tuesday. GFI LanGuard present.

GFI LanGuard had already done its work. Every managed device on every network segment was scanned, assessed, and catalogued. The Windows file-sharing vulnerability the payload was built to exploit had been identified the week before: high severity, flagged, patched automatically overnight across every managed endpoint and every server. By the time the contractor arrived, the door the payload needed had already been closed.

Friday evening. The payload activated. It moved laterally, exactly as before. It reached the first internal device and scanned for the vulnerability.

It was not there.

The next device. The next. Every managed machine was clean. The lateral movement ran out of surface. It spread as far as the contractor's device had seeded it, found nothing to grip, and stopped.

No encryption. No lost files. No Monday morning phone calls.

With GFI AppManager AI: the view that connected both

Running GFI KerioControl and GFI LanGuard separately still leaves one gap: they cannot see each other.

Without GFI AppManager AI, the GFI LanGuard vulnerability data and GFI KerioControl's perimeter status live in separate consoles. The administrator watching the firewall is not looking at the same screen as the one checking patch compliance. The connection between "this device is unpatched" and "this device sits on a segment GFI KerioControl trusts" has to be made manually, if anyone thinks to make it at all.

By Thursday of that week, the day before the payload activated, an administrator doing a morning check in GFI AppManager AI would have seen it: a high-severity GFI LanGuard alert for unpatched devices on that internal segment, right there in the same session as GFI KerioControl's perimeter status. One view. The gap named, visible, and actionable before it had a chance to open.

GFI AppManager AI puts both in the same place. When a vulnerability is found, the response is immediate: GFI KerioControl restricts the device from the network while GFI LanGuard deploys the patch, all from the same GFI AppManager AI session. Once clean, access is restored.

Identify. Restrict. Patch. Restore. One session.

The contractor's device was never going to be in GFI LanGuard's inventory. It was never a managed asset. But every device the payload tried to move through? Known. Current. Patched. And visible in GFI AppManager AI, right alongside the perimeter that had been watching the boundary.



GFI KerioControl

Secures the network boundary. Stateful firewall, IPS/IDS, Shield Matrix AI, gateway antivirus, VPN, brute force protection. Watching the edge, every minute.



GFI LanGuard

Secures what GFI KerioControl is protecting. ~70,000 CVEs, automated patching across Windows, Linux, macOS and 60+ third-party applications. Every managed device. Known. Current. Hardened.



GFI AppManager AI

One login, one view. Perimeter status and endpoint vulnerability in the same session. The gap between them visible before it becomes an incident.

Ready to Get Started?

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