LanGuard

PRODUCT PAIRING

The email that got through

GFI LanGuard + GFI KerioConnect® + GFI AppManager AI



The invoice arrived on a Wednesday. Familiar supplier, correct amount, a link to a shared document on a cloud storage platform, the kind suppliers and partners send dozens of times a day.

GFI KerioConnect® checked everything. Sender domain verified, SPF valid. Cryptographic signature confirmed, DKIM present. Dual anti-spam engines cleared it. The URL resolved to a legitimate cloud storage service, no blocklist match. The email was clean. *A genuine message from a recently compromised supplier account.* **Real sender. Real domain. Real signing history. Nothing false about it.**

GFI KerioConnect® delivered it correctly. The system worked exactly as designed.

The employee clicked the link, downloaded the document, and opened it. What happened next had nothing to do with the email. Or the link.

The threat was never in the email

The document the employee downloaded contained code that only becomes active on the device that opens it. It was not in the email. It was not in the URL. It was sitting on a cloud storage server, unreachable for scanning until the moment the employee chose to download it.

Once opened, it looked for one thing: device-layer vulnerabilities. An unpatched operating system. An outdated document reader. A known CVE in a document handler. The threat never existed inside the email or the link that delivered it. That is precisely why it arrived in the inbox. There was nothing in either for a mail server to act on.

If those device-layer vulnerabilities existed, the code would exploit them. If they had been patched, it would find nothing and fail.

GFI KerioConnect®'s job was the mail stream. It did that completely. **The outcome rested on one separate question: what was the security posture of the device that opened the document?**

That question belongs to GFI LanGuard.

Without GFI LanGuard

The device nobody hardened

Daniel is the head of business development: senior, well-connected, constantly travelling. His laptop had not been on the network in six weeks, missing the last two patch cycles. Four unpatched critical vulnerabilities. One in Outlook itself. Without GFI LanGuard, nobody knew.

When the PDF executed, it found exactly what it needed. Multiple exploitable CVEs, all patchable for weeks. The malware established persistence within minutes and harvested Daniel's cached credentials. Within hours, it was sending email from his authenticated account, his address, his domain, his DKIM signature, indistinguishable from anything he had ever sent. Three days later, the CEO received a message from Daniel requesting urgent approval for a supplier payment. Correct tone. Familiar name. No reason to doubt it. The finance team received one too. So did four external clients. None of them knew Daniel's laptop had not been on the corporate network in six weeks. Unopposed. Largely invisible until replies and complaints started coming back.

The device was the gateway. That was the only failure in this story.

With GFI LanGuard

The vulnerability that never became an incident

Same Wednesday. Same email.
GFI LanGuard present.

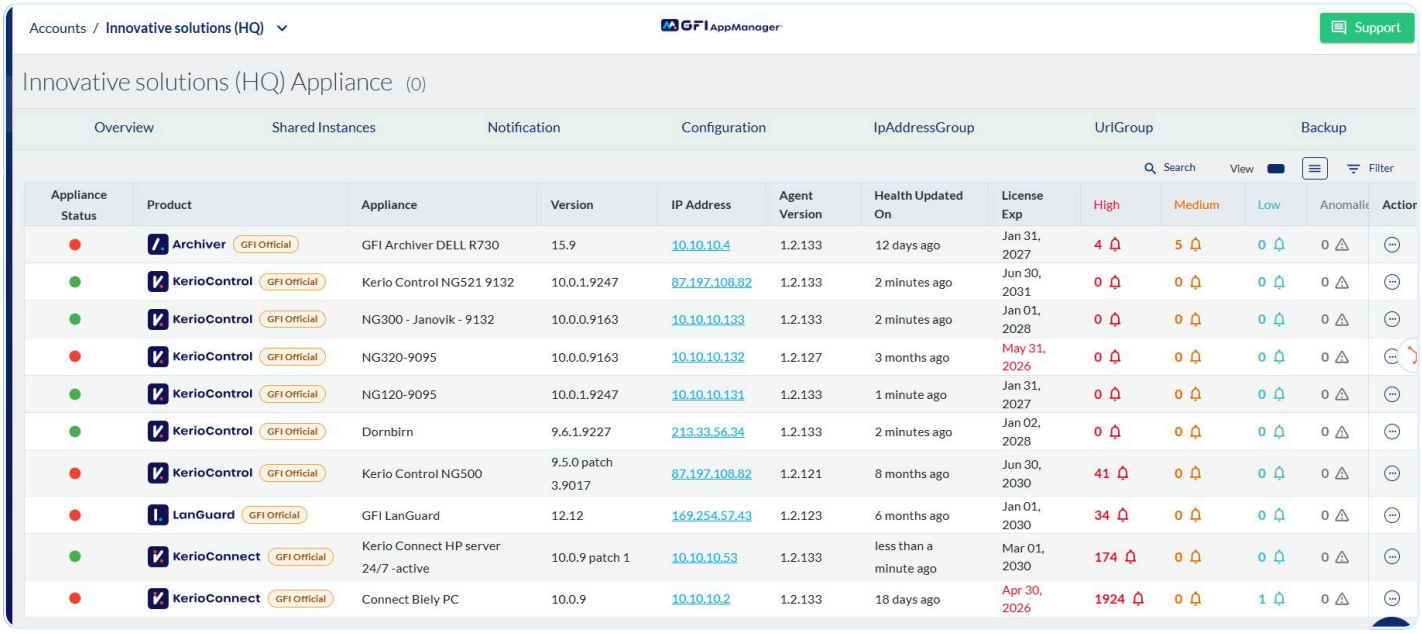
Four days earlier, GFI LanGuard had scanned Daniel's laptop remotely during a VPN session. Four critical CVEs identified, high-severity alert raised, patches deployed automatically overnight. By Wednesday morning, the device was fully current.

The PDF opened. The code scanned for the CVEs it needed.

They were not there.

No foothold. No persistence. Endpoint antivirus quarantined the file in seconds. One low-severity alert the next morning. A short investigation, then close. Two lines in the incident log. Nothing more.

With GFI AppManager AI: both layers, one story



Appliance Status	Product	Appliance	Version	IP Address	Agent Version	Health Updated On	License Exp	High	Medium	Low	Anomalie	Actior
	Archiver GFI Official	GFI Archiver DELL R730	15.9	10.10.10.4	1.2.133	12 days ago	Jan 31, 2027	4	5	0	0	
	KerioControl GFI Official	Kerio Control NG521 9132	10.0.1.9247	87.197.108.82	1.2.133	2 minutes ago	Jun 30, 2031	0	0	0	0	
	KerioControl GFI Official	NG300 - Janovik - 9132	10.0.0.9163	10.10.10.133	1.2.133	2 minutes ago	Jan 01, 2028	0	0	0	0	
	KerioControl GFI Official	NG320-9095	10.0.0.9163	10.10.10.132	1.2.127	3 months ago	May 31, 2026	0	0	0	0	
	KerioControl GFI Official	NG120-9095	10.0.1.9247	10.10.10.131	1.2.133	1 minute ago	Jan 31, 2027	0	0	0	0	
	KerioControl GFI Official	Dornbirn	9.6.1.9227	213.33.56.34	1.2.133	2 minutes ago	Jan 02, 2028	0	0	0	0	
	KerioControl GFI Official	Kerio Control NG500	9.5.0 patch 3.9017	87.197.108.82	1.2.121	8 months ago	Jun 30, 2030	41	0	0	0	
	LanGuard GFI Official	GFI LanGuard	12.12	169.254.57.43	1.2.123	6 months ago	Jan 01, 2030	34	0	0	0	
	KerioConnect GFI Official	Kerio Connect HP server 24/7 -active	10.0.9 patch 1	10.10.10.53	1.2.133	less than a minute ago	Mar 01, 2030	174	0	0	0	
	KerioConnect GFI Official	Connect Biely PC	10.0.9	10.10.10.2	1.2.133	18 days ago	Apr 30, 2026	1924	0	1	0	

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

GFI AppManager AI closes it. GFI KerioConnect® mail events and GFI LanGuard device alerts appear together in a single view, for the same organisation, the same user, the same device. On the day Daniel's laptop first drifted out of compliance, GFI LanGuard's High-severity alert for his machine would have appeared in GFI AppManager AI. In the same session, the administrator would have seen his active GFI KerioConnect® mail account tied to that vulnerable device.

When the Wednesday invoice eventually came in, it would still have passed GFI KerioConnect® correctly. The difference is that GFI LanGuard would already have closed the door it was designed to exploit, and GFI AppManager AI would have made that fact visible.

The preparation that determines the outcome happens before Wednesday morning. Not after.



GFI KerioConnect®

Secures the mail stream. Dual-engine anti-spam, antivirus, SPF/DKIM, greylisting, 2FA. Working correctly, every day.



GFI LanGuard

Secures the device layer no mail server can see. ~70,000 CVEs, automated patching across Windows, Linux, macOS and 60+ third-party apps.



GFI AppManager AI

Where GFI MailEssentials AI lives. Both layers are visible together, before the gap between them becomes an incident.

Ready to Get Started?

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

Copyright © GFI USA, LLC, All rights reserved.