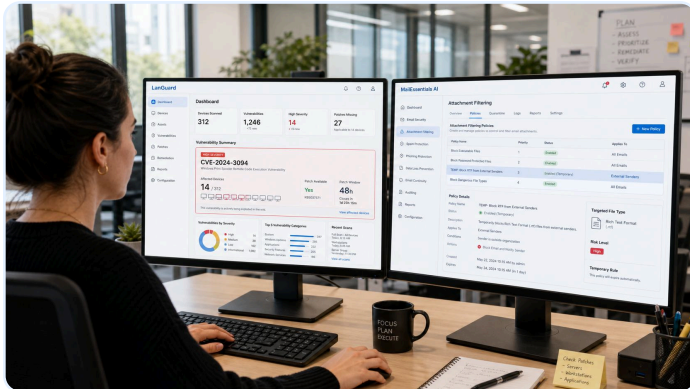


The 48 hours

GFI LanGuard + GFI MailEssentials AI + GFI AppManager AI



Sara had been the IT administrator for three years. She knew Thursday mornings: open the dashboard, see what GFI LanGuard had found overnight, act on it.

Most Thursdays it was routine. That Thursday it was not. Fourteen devices. One CVE. High severity. A vulnerability in a widely used document handler that attackers had been actively exploiting for three weeks, delivered via a macro-enabled file type that arrived in inboxes every day. The patch existed. The deployment window was the weekend. Forty-eight hours away.

GFI LanGuard had told her everything she needed to know. What happened next depended on what GFI MailEssentials AI was ready to do with it.

What GFI MailEssentials AI was already doing

GFI MailEssentials AI was doing exactly what it was built to do. It was filtering every email, correctly, against the rule framework it had been given.

That framework had not been built by hand. When the organisation had first registered GFI MailEssentials AI in GFI AppManager AI and accessed GFI MailEssentials AI, the setup had taken forty minutes: the administrator had described the organisation, its sector, its compliance obligations, the data categories it handled. The AI had generated a complete rule set: regex patterns, policy scopes, quarantine actions, content controls mapped to the organisation's actual profile. Exported as XML. Imported into GFI MailEssentials AI. Running ever since.

The baseline was right. Every rule was calibrated to what this organization actually needed to protect.

What GFI MailEssentials AI needed on that Thursday morning was one additional targeted rule, and a framework already intelligent enough to make writing it fast.

Without the AI baseline: starting from zero

Before GFI MailEssentials AI, Sara's Thursday looked like this.

She saw the GFI LanGuard alert. Identified the file type. Opened GFI MailEssentials AI in a separate session. Attempted to write the blocking rule manually: file extension scope, sender conditions, quarantine action, regex for the attachment pattern. Checked the syntax. Was not certain. Looked it up. Revised it. Tested it in staging.

Twenty-five minutes. From scan result to rule going live: twenty-five minutes of manual process during which that file type could still reach any of the fourteen vulnerable users.

Three of them received emails carrying it during that window. One opened the attachment at 08:54, eleven minutes before the rule was active.

Her device was one of the fourteen. The CVE was still present. The patch was 46 hours away.

With GFI MailEssentials AI: the framework that was already ready

Same Thursday. Same scan result. GFI MailEssentials AI already configured through GFI AppManager AI.

Sara saw the GFI LanGuard High-severity alert. She knew the file type. She opened GFI MailEssentials AI. The rule framework the AI had built at setup already had the right attachment policy structure, the right scope definitions, the right quarantine routing for her organization. She was not starting from a blank form. She was adding one targeted rule to a framework that already understood the organization's profile.

Four minutes. One rule. External senders. The specific file extension. Quarantine action. Duration: 72 hours.

Over the next 48 hours, four emails arrived carrying that file type. All four quarantined before reaching any inbox. None of the fourteen vulnerable users saw them.

Saturday night, GFI LanGuard deployed the patches. Fourteen devices. CVE closed. Sunday morning Sara removed the temporary rule. Normal mail flow restored.

No incident. Not because the rule was clever. Because the foundation it was built on already was.

What GFI AppManager AI made possible

She knew Thursday mornings: open the dashboard, see what GFI LanGuard had found overnight, act on it. The GFI MailEssentials AI instance must be registered there before the AI can generate rules for it. That registration is also what makes the rule framework intelligent from day one: the AI takes the organization's context (sector, compliance obligations, data categories, registered country) and builds a baseline that reflects what that organization actually handles.

When GFI LanGuard's Thursday morning alert appeared, Sara was already working in the same portal where GFI MailEssentials AI lived. The intelligence from one product and the policy controls of the other were reachable in the same session: without switching systems, without a second login, without re-establishing context in a separate tab.

Without GFI AppManager AI, there's no GFI MailEssentials AI. Without GFI MailEssentials AI, the baseline is generic, the temporary rule takes twenty-five minutes to write, and the window that costs eleven minutes is the window that matters.

Scan. Assess. Build. Block. Patch. Restore.



GFI MailEssentials AI

Multi-engine antivirus, anti-spam, anti-phishing, and attachment filtering with an AI-built rule framework calibrated to the organization's actual profile. The filter that is already intelligent when the patch window opens.



GFI LanGuard

Vulnerability assessment across ~70,000 CVEs, automated patching across Windows, Linux, macOS and 60+ third-party applications. Every vulnerability is named. Every exposure window known.



GFI AppManager AI

Where GFI MailEssentials AI lives. The portal through which the AI rule framework is built, and the session where GFI LanGuard's device intelligence and GFI MailEssentials ai policy controls are reachable together. The intelligence and the action, connected from the start.

Ready to Get Started?

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