MailEssentials AI

USE CASE

Intelligent DLP Rule Generation

Closing the “execution gap”: from compliance intent to enforcement in minutes

1. Executive summary: the execution gap problem

Most organizations don’t struggle with what to protect; the policies are clearly written by Legal and Risk teams. The breakdown happens at the point of technical implementation.

- **The traditional reality:** A mandate to “Block Social Security Numbers” requires an IT specialist to research formats, write complex Regex (Regular Expressions), and test for false positives. This process typically takes 40+ hours and sits in an IT backlog for weeks.
- **The AI reality:** GFI MailEssentials AI translates plain-English business requirements into technically precise, deployable XML rule sets in under 5 minutes.
- **Core Value Proposition:** Move from policy intent to active enforcement at the speed of business, eliminating the technical bottleneck and reclaiming hundreds of hours of specialist time.

2. The business challenge: when compliance waits on expertise

Organizations using single-engine security face three measurable risks that often trigger procurement rejections:

- **Prolonged exposure windows:** Every hour a policy sits in a “testing queue” is an hour the organization is vulnerable to a breach or regulatory fine.
- **The specialist bottleneck:** Regex and DLP expertise are scarce. When only one or two people can “write the rules,” security becomes a single point of failure.
- **The complexity tax:** Manually written rules are difficult to tune. If a rule is too strict and blocks legitimate billing emails, the typical response is to disable the rule entirely, recreating the security gap.

3. Real-world scenarios: the “why now?” moments

Scenario A: the “Friday Afternoon” urgent mandate

At 3:00 PM on Friday, Legal issues an emergency order: “Immediately block all outbound Patient IDs and Credit Cards. Exception: Allow our billing department to email our payment processor.”

Without AI	With MailEssentials AI
IT scrambles to research ID formats. The risk window stays open over the weekend while the rule is manually coded.	The Admin types: “We are a healthcare provider. Block outbound patient record numbers and credit cards. Exception: allow traffic to @securebilling.com.” The rule is generated, imported, and active by 3:05 PM.

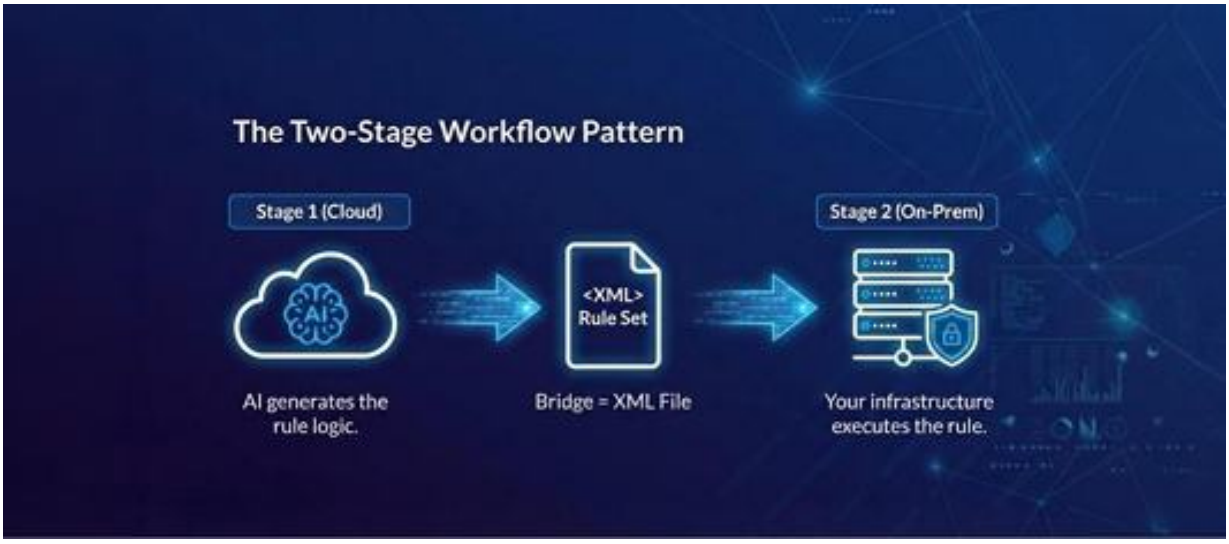
Scenario B: rapid global expansion

A US company expands into Germany and the UK. They must suddenly comply with local data privacy formats (e.g., German National IDs and UK National Insurance numbers).

Without AI	With MailEssentials AI
The team spends weeks researching international data formats and testing new patterns.	The Admin provides context: “We are now operating in Germany and the UK. Update our DLP rules to include local National ID formats.” The AI references its regulatory knowledge base and generates precise regional patterns automatically.

4. How it works: cloud intelligence, on-premise enforcement

GFI MailEssentials AI utilizes a secure “Cloud-to-Ground” architecture designed for maximum data sovereignty.



1. **Cloud intelligence (the author):** you interact with the AI in a secure cloud portal (meai.gfi.com). You provide the context (industry, geography, data types). The AI translates this intent into a technical XML rule file.
2. **On-premise enforcement (the guard):** crucially, your live email traffic never goes to the cloud. You download the XML file and import it into your local GFI MailEssentials AI in AI stance.
3. **Local Inspection:** all email scanning, filtering, and blocking happen entirely on your local infrastructure. Your data sovereignty remains absolute.

5. What it generates: from plain English to technical rules

The AI bridges the gap between a business request and a technical configuration.

Admin input	AI output
"Block all outbound IBANs and Credit Card numbers, but quarantine them for review instead of deleting them."	A technically precise XML file containing complex Regex patterns for international bank accounts and major credit card providers (Visa, Amex, etc.), pre-configured with the "Quarantine" action.

Supported patterns: the AI is trained on global regulatory frameworks including GDPR, HIPAA, PCI-DSS, and SOX, as well as regional identifiers for dozens of countries.

6. Measurable ROI & success metrics

Supported patterns: the AI is trained on global regulatory frameworks including GDPR, HIPAA, PCI-DSS, and SOX, as well as regional identifiers for dozens of countries.

Metric	Traditional Manual Process	With GFI MailEssentials AI
Time-to-enforcement	Hours (Research + Coding)	Minutes
Specialist labor cost	High/rule (rate/hour)	Insignificant
Policy coverage	Limited (exposed)	Extensive (covered)

7. Competitive positioning

Feature	GFI MailEssentials AI	Traditional DLP / Cloud Gateways
Expertise barrier	**None.** Uses natural language.	**High.** Requires Regex/DLP specialists.
Data sovereignty	**100% On-Premise.** Email stays local.	**Variable.** Often requires cloud transit.
Deployment speed	**Instant.** XML import.	**Slow.** Manual coding and testing.
Democratization	Any Admin can secure the network.	Only specialists can secure the network.

8. Competitive positioning

Contact: sales@gfi.com

Required Disclaimer

GFI MailEssentials AI is a rule-authoring assistant. AI-generated rules should be reviewed and tested by an administrator before production deployment. The AI portal processes requirement descriptions only; actual email content remains on-premise and is never uploaded to the cloud. Feature availability is subject to licensing levels and version requirements (v22.x+).

Copyright © GFI USA, LLC, All rights reserved.