MailEssentials AI

USE CASE

# Anti-Spoofing & Reducing Business Email Compromise

## Reducing BEC (CEO fraud) and invoice/payment impersonation risk in on-prem email environments

### 1. Executive summary

Business Email Compromise (BEC) rarely starts with “a virus.” It starts with trust: an email that looks like it came from your CEO, your finance team, or a known supplier, arriving right when a payment is due or bank details are “changing.”

The weakness attackers exploit is simple: email identity is easy to fake. GFI MailEssentials AI reduces that risk by adding an on-premise, admin-controlled security layer that focuses on identity signals before the message reaches the inbox.

- **Anti-spoofing controls** (stop external senders impersonating your internal domains)
- **Sender / IP reputation checks** (reduce exposure to known risky infrastructure)
- **Email authentication support** (validates SPF and complements your DMARC policies, without requiring mail to be routed to a third-party cloud for scanning)

---

### 2. Why organizations care

BEC shows up as a finance problem and a security problem:

- **Fraud risk:** spoofed or impersonated emails can trigger wire transfers, supplier bank detail changes, payroll updates, gift card purchases, or “urgent” approval requests.
- **Operational disruption:** investigations, emergency rules, and “is this real?” escalations slow down payment cycles and create internal friction.
- **Reputation risk:** once attackers successfully impersonate your domain (or abuse it), partners begin distrusting your email, even legitimate invoices and statements.
- **Audit / governance pressure:** regulated environments need controls over financially material communications, not only malware.

**Key point:** A spam filter is judged on inbox cleanliness. A BEC control is judged on whether it prevents the one message that causes a five- or six-figure loss.

## 3. What GFI MailEssentials AI does in this use case

GFI MailEssentials AI focuses on two practical outcomes:

### A) Stop external impersonation of internal identities (anti-spoofing)

GFI MailEssentials AI can flag or block emails that claim to be from your internal domain (e.g., @company.com) but arrive from an external, unauthenticated source.

This is a common backbone of CEO fraud and “internal finance team” impersonation.

### B) Reduce exposure to risky senders (reputation filtering)

GFI MailEssentials AI can apply reputation checks (for example via SpamRazer) so you can:

- block or quarantine higher-risk senders earlier
- tune sensitivity to your tolerance for false positives vs. aggressive blocking
- avoid relying only on “content looks suspicious” logic (BEC often looks normal)

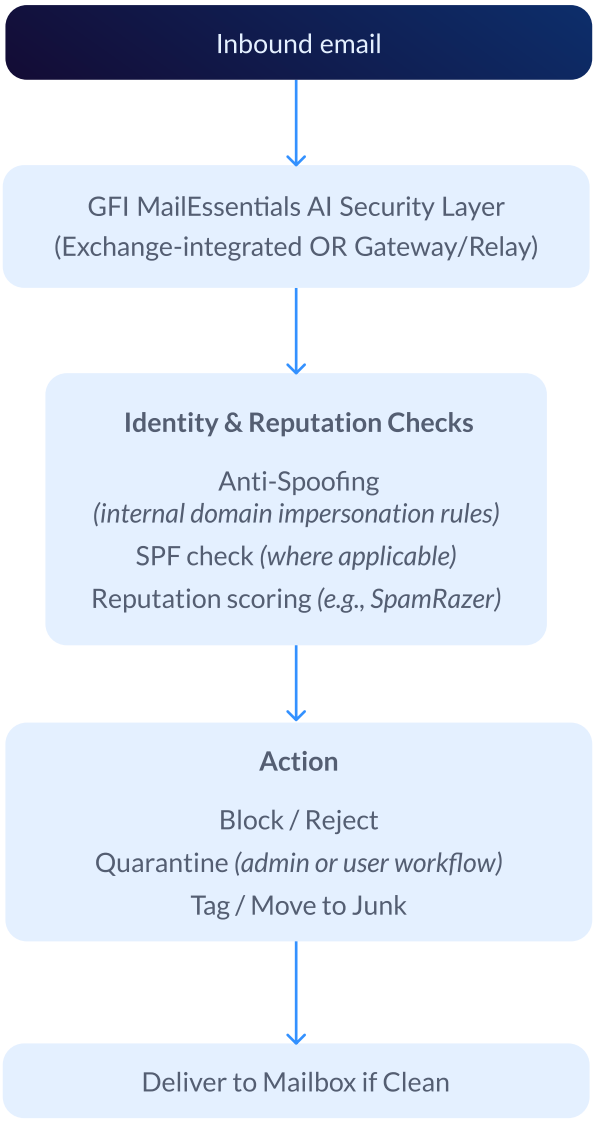
---

## 4. How it works

GFI MailEssentials AI can be deployed in the pattern that matches your environment:

- **Exchange-integrated pattern (transport agent):** mail is inspected inside the Exchange transport pipeline.
- **Gateway / relay pattern:** GFI MailEssentials AI sits in front of your mail server to filter mail before it hits Exchange (or other on-prem mail systems).

Either way, the security logic is similar:




## 5. What to configure first

You don't need a 20-page runbook to get value. Start here:

### Anti-spoofing (core BEC control)

- Define your internal domains that should not be legitimately sent "from the outside."
- Choose the action:
  - → **Block/Reject** (most protective)
  - → **Quarantine** (safer when you expect legitimate edge cases)
  - → **Tag** (lowest friction, but relies on user judgement)

### Reputation filtering (SpamRazer)

- Start conservatively (quarantine/tag suspicious senders)
- Tighten to blocking as you tune
- Decide who reviews quarantine and how exceptions are approved (finance-related exceptions should be controlled)

### Authentication

- SPF Validation: GFI MailEssentials includes an SPF filter. Ensure it's enabled and prioritized above Whitelist filters.
- DKIM Signing: if your organization uses DKIM, MailEssentials can sign outbound mail.

## 6. What success looks like

- Spoof/impersonation attempts blocked or quarantined (trend line)
- BEC escalation volume (“is this real?” tickets to IT/Sec/Finance)
- False positive rate for trusted partners (business continuity)
- Time-to-release for legitimate quarantined mail (operational friction)

## 7. Competitive positioning

| What matters | GFI MailEssentials AI | Traditional DLP / Cloud Gateways |
|---|---|---|
| BEC control model | Anti-spoofing + reputation + on-premise workflows | Often cloud-first or gateway-only approaches |
| Deployment flexibility | Exchange-integrated and/or gateway/relay patterns | May require MX reroute / external dependency |
| Operational control | Admin-defined rules, quarantine actions, tuning | Can be more opaque depending on vendor |
| Audit story | Clear local configuration + logs you control | Often relies on vendor portals/attestations |

## 8. Competitive positioning

Contact: sales@gfi.com

---

### Required Disclaimer

*GFI MailEssentials AI supports fraud-risk reduction by helping detect and block impersonation and suspicious senders; it does not guarantee prevention of all BEC attempts. Results vary by environment, configuration, user workflows, and the organization's broader controls.*

Copyright © GFI USA, LLC, All rights reserved.