MailEssentials AI

USE CASE

Multi-Engine AV Defense

Eliminating single points of failure in email threat detection

1. Executive summary

Email remains the primary vector for malware delivery because it arrives in formats users trust: invoices, shipping notifications, and HR documents. Most email security stacks rely on a single malware scanning engine: if that vendor misses a threat or their update infrastructure fails, the entire organization is exposed.

GFI MailEssentials AI eliminates this "Single Point of Failure" by supporting multiple independent antivirus engines (commonly Avira, BitDefender, and Sophos) within a single, on-premise workflow. This is a deliberate defense-in-depth strategy grounded in operational reality.

---

2. The business challenge: three single-vendor risks

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

- **The signature gap:** no single AV vendor has 100% global coverage. Response times to new exploits vary by hours or days between labs. A delay in one vendor's update is an open door for ransomware.
- **Infrastructure fragility:** antivirus engines depend on external delivery networks (CDNs) for updates. If a single provider's update server goes down, protection remains stale. This is not theoretical; it happens.
- **The procurement firewall:** modern Vendor Risk Management (VRM) filters often flag single-engine solutions as a "concentration risk." Regulated verticals now require proof of redundant security controls to pass audits.

3. Operational proof: resilience in real-world scenarios

Scenario: update infrastructure outages

A vendor-specific delivery network issue can cause definitions for a major engine to become stale for over a month. In this case, single-engine deployments were left entirely vulnerable, GFI MailEssentials AI users maintained protection because their other engines continued to pull fresh definitions from other sources.

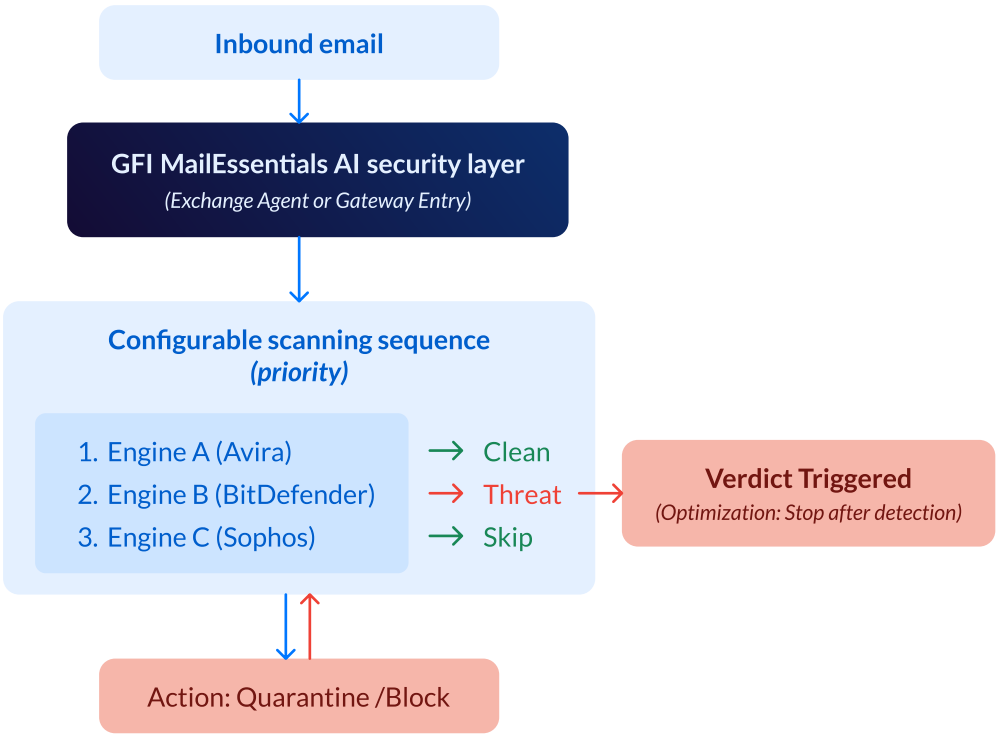
---

4. Technical architecture: how it works

GFI MailEssentials AI provides a transparent architecture where the administrator controls the scanning logic. Depending on your infrastructure, the engines are integrated either directly into the Exchange Transport pipeline or deployed as a Dedicated Email Gateway to filter traffic at the perimeter.

Regardless of deployment type, mail is processed through a high-performance scanning sequence.

Typical MSP structure in GFI AppManager



- **Flexible deployment:** install directly on the Exchange server for simplicity or on a dedicated gateway server to offload processing and provide perimeter protection.
- **Configurable priority:** administrators define the engine execution order (top-to-bottom), ensuring the most trusted or resource-efficient engines process mail first.

- **Performance optimization:** admins can enable “stop scanning after N detections” to save CPU cycles once a threat is confirmed by a specified number of engines.
- **Independent update paths:** each engine pulls definitions independently from the GFI CDN. A failure in one vendor’s update pipeline does not impact the operational status of the others.

5. Competitive positioning: the sovereign advantage

What Matters	GFI MailEssentials AI	Standard Gateways
Vendor Risk	**Distributed:** No single point of failure.	**Concentrated:** Reliant on one vendor.
Detection Logic	**Redundant:** 3-5 Engines.	**Single:** 1 proprietary engine.
Reliability	**Continuous:** Protection persists if an engine fails.	**Fragile:** Update failure = zero protection.
Data Residency	**Sovereign:** Scans on-server.	**Cloud:** Data transits vendor infra.
Transparency	**High:** Verifiable update status per engine.	**Low:** Opaque, vendor-managed stack.

6. Compliance & MSP Value

- **For compliance officers:** this architecture provides the “Architectural Attestation” needed for GDPR, HIPAA, and DORA by demonstrating redundant, vendor-independent controls.
- **For MSPs:** standardizing a customer base on a multi-engine baseline reduces provider liability. If a global vendor experiences an outage, your customers remain protected by the alternate engines in the stack, and the dashboard allows you to quickly identify if an issue is vendor-wide or customer-specific.

7 Next Steps

Contact: sales@gfi.com

Copyright © GFI USA, LLC, All rights reserved.