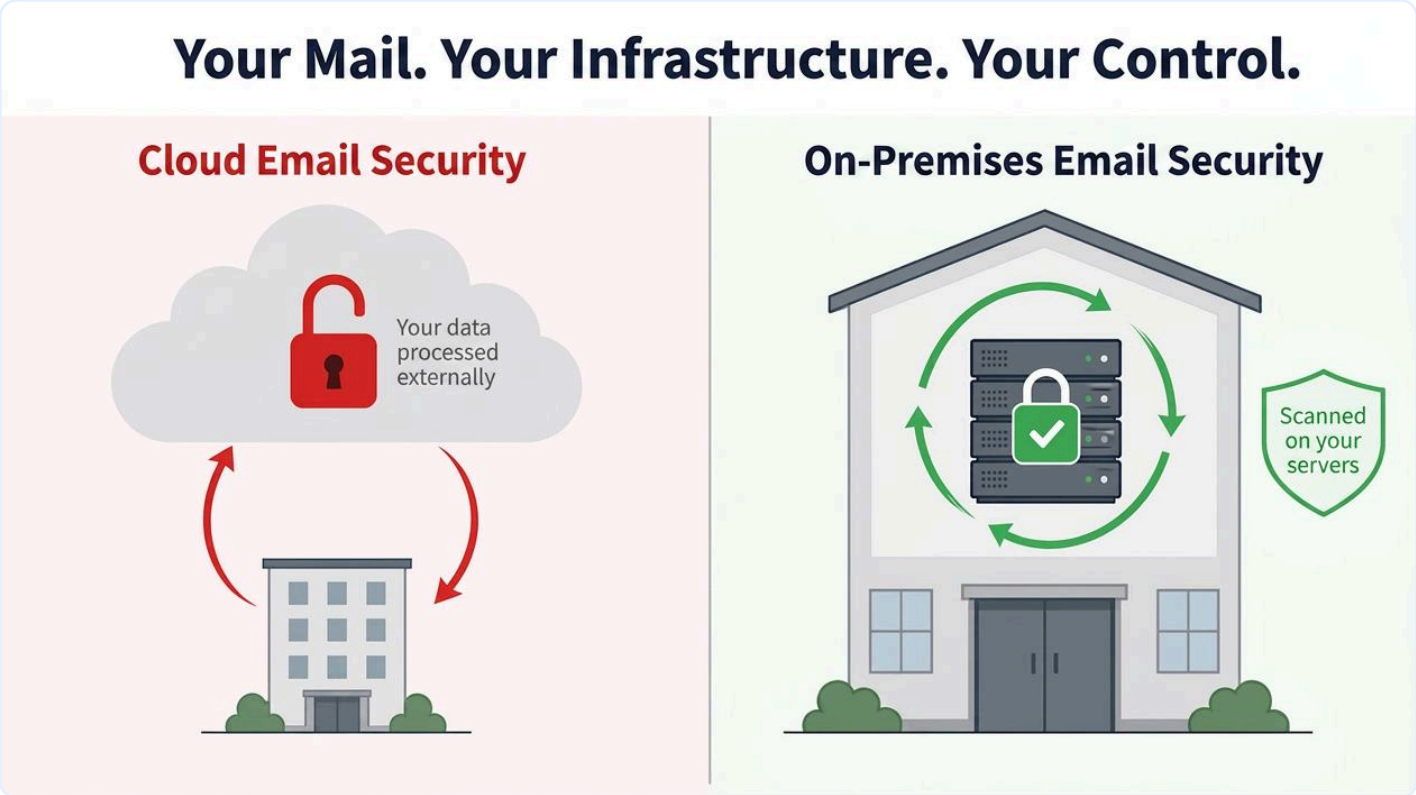
MailEssentials AI

USE CASE

The email security layer that never leaves your infrastructure

Exchange-native email security for organisations that cannot route mail through the cloud



The compliance question cloud email security cannot answer

Cloud email security routes your mail through the vendor's infrastructure for scanning: Mimecast, Microsoft Defender for Office 365, Proofpoint, all of them work this way. Your email leaves your control, gets processed on someone else's servers, and arrives clean.

For most organizations, that is a reasonable trade-off. For regulated ones, it raises a question that contract alone cannot resolve: can you legally route email containing financial records, patient data, legal communications, or government information through a cloud platform? GDPR transfer restrictions, HIPAA processing requirements, and public-sector data sovereignty mandates all point in the same direction.

Some organizations have concluded the answer is no. They need email security that processes mail on their own infrastructure, and never sends it anywhere else. That is what GFI MailEssentials AI is built for.

Inside the pipeline, not in front of it

GFI MailEssentials AI integrates directly with your mail infrastructure in two modes: as an Exchange Transport Agent for Exchange environments, or as a standalone SMTP Relay for any other mail server. In each case, scanning happens inside your infrastructure, on your hardware. Not intercepted before it arrives. Not redirected to a cloud service. Scanned inside Exchange itself, on your hardware, under your control.

The practical difference from a cloud gateway matters in three ways:

- **Outbound DLP is enforced.** Content policies apply before sensitive data leaves the organization, at the transport layer, before the message is sent.
- **No external routing dependency.** If your internet connection goes down, mail continues to be processed locally.

For organizations that also need to protect non-Exchange servers (GFI KerioConnect®, Zimbra, MDaemon), GFI MailEssentials AI can be deployed in Gateway Mode, a dedicated SMTP relay server that scans perimeter mail before passing it on. The same engines, the same policy model, without requiring Exchange.

What runs in the pipeline

Every message passes through three overlapping protection layers:

Three independent antivirus engines. Avira and BitDefender are included, with Sophos available as an addition. Each maintains its own definition database and updates independently. If one vendor's update delivery has a problem, the others maintain current protection. Different heuristics, different threat intelligence, different coverage angles on the same threat.

15+ anti-spam filters. GFI MailEssentials AI deploys each one to target a different attack vector: SpamRazer reputation scoring, Bayesian analysis trained on your mail stream, anti-phishing URL inspection, anti-spoofing detection for domain impersonation, SPF and DMARC enforcement, greylisting, IP and URI blocklists, directory harvest protection, and header checking. Together they form a complete inbound protection stack.

Inbound and Outbound DLP. Content filtering rules are built manually or generated by GFI MailEssentials AI. The AI is a cloud-based rule-generation tool: you describe your compliance requirements in plain language and optionally share an existing policy in XML format. No email content, no message data, and no personal information ever leaves the organization. The resulting rules are imported back into the on-premises product, enforced entirely within your infrastructure, and applied to outbound mail before it leaves the organization. Sensitive content can be blocked, quarantined, or redirected for compliance review.

The Exchange EOL context

Exchange Server 2016 and 2019 reached end of life on 14 October 2025. organizations that moved to Exchange Server Subscription Edition (SE), the actively supported on-premises successor, can run GFI MailEssentials AI without any architectural change. The same security layer that worked on Exchange 2019 works on Exchange SE. No migration to cloud security tooling required, no gap during the transition.

For those still on EOL versions while planning migration, GFI MailEssentials AI provides the layered AV, anti-spam, and DLP controls that substantially reduce the attack surface in the interim.

Who this is for

GFI MailEssentials AI is not positioned as a cloud alternative for the whole market. It is built for the segment where routing email through a cloud platform is a compliance decision that has already been made, or where regulation has made it.

Organization type	Why on-premises security is required
Financial services (50–2,000 seats)	Audit trail obligations, data handling rules, BEC risk; Exchange on-premises common
Healthcare providers	HIPAA ePHI processing requirements; Business Associate Agreement complexity with cloud vendors
Government and public sector	Data sovereignty mandates; sensitive data cannot transit commercial cloud
Legal practices	Client confidentiality obligations; professional ethics on data processing
Mid-market Exchange operators	Not on M365; need stronger security than Exchange's native protection provides
MSPs managing Exchange environments	Standardized on-premises security baseline across multiple client instances

How it compares

What matters	GFI MailEssentials AI	Microsoft Defender for O365	Mimecast / Proofpoint
Mail processed by a third-party cloud	✅ Never	❌ **Always**	❌ **Always**
Works on Exchange on-premises (inc. SE)	✅ Yes	❌ **Requires M365**	⚠️ **Via MX redirect**
Internal mail scanning	✅ Yes (Exchange-integrated)	✅ **M365 only**	❌ **Perimeter only**
Works with non-Exchange mail servers	✅ Yes (Gateway mode)	❌ **No**	✅ **Yes**
CLOUD Act / data transfer exposure	✅ Email never routed externally for scanning	⚠️ **US platform**	⚠️ **US platform**

The position: For organizations where mail cannot leave the building for security processing, GFI MailEssentials AI is purpose-built to satisfy that requirement, keeping every byte of email inside the organization's own infrastructure.

Ready to Get Started?

If your organization runs Exchange on-premises and cannot route email through external cloud services, the first question is whether your current security layer matches that constraint.

Talk to GFI | Find a partner

Copyright © GFI USA, LLC, All rights reserved.