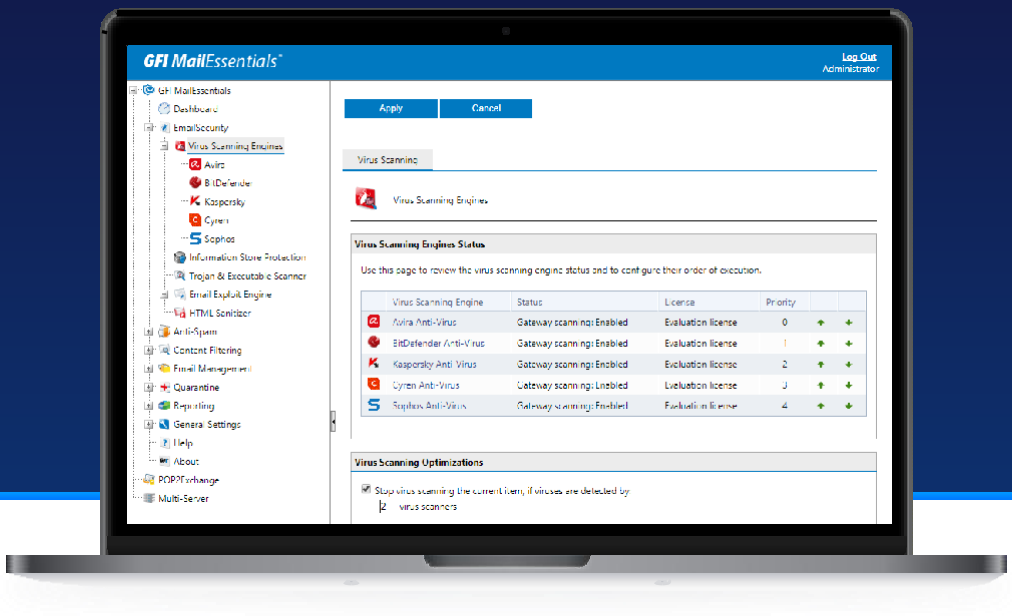
DATASHEET

GFI MailEssentials



Get 14 anti-spam filters, 4 anti-virus engines plus malware scanning in one email security package

With billions of emails sent and received each day, email is frequently an intruder's means to attack your organization. GFI MailEssentials is easy-to-use and o"ers a comprehensive set of defences to protect your company and improve email productivity.

- **Block email-borne viruses and malware—** Why trust email security to one antivirus engine when you can have the combined power of four? GFI MailEssentials can engage the power of leading brands including BitDefender, Avira, Kaspersky, and Cyren. Each engine features its own heuristics and detection methods. You gain maximum protection for your email environment to block email-borne viruses and other malware more e"ectively.
- **Filter spam & detect phishing attacks—**Filter spam out before it hits email boxes to save your server space and productive time. GFI MailEssentials uses 14 advanced email filtering technologies you can see in action. The GFI MailEssentials anti-phishing module detects and blocks threats posed by phishing emails by comparing the content of the spam with a constantly updated database and phishing URLs.
- **Make email safe and productive…simply—** GFI MailEssentials is compatible with di"erent email servers, not just Exchange. It fits seamlessly into your current setup—whether on-premise, virtual, or hosted in your cloud infrastructure. IT admins are in full control of their email security.

GFI™
Aurea SMB Solutions

For enquiries, you may email sales@sgen.com.au or call (02) 9416 0416

Up to four anti-virus engines

GFI MailEssentials ships with the powerful Avira and BitDefender Antivirus engines. Add the Kaspersky and Cyren antivirus engines for the ultimate protection. Antivirus engine vendors have di"erent response times to new viruses and malware. This capability ensures your system can always detect new threats in the shortest possible time.

Advanced malware protection

GFI MailEssentials delivers advanced malware protection with scanning engines that connect to a cloud service whenever they find unknown, executable attachments. These attachments are thoroughly scanned to determine if the attachment is malicious or not.

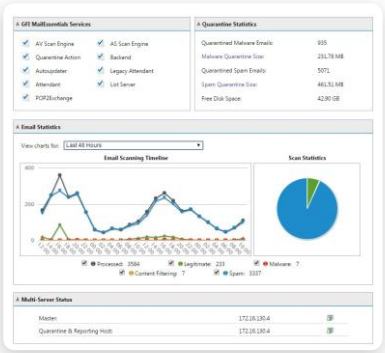
An arsenal of anti-spam filters

GFI MailEssentials features a variety of anti-spam technologies. SPF blocks spoofed emails. Greylisting blocks emails sent with non-RFC compliant techniques used by spammers. Directory harvest protection blocks emails sent using random and exhaustive email address-generation techniques. DNS blacklists utilize a wealth of information gathered from distributed community data collection techniques to fend o" botnet spamming.

Web console with integrated reporting

You can handle all your anti-spam and email security functionality including spam and malware quarantine, as well as reporting from a single web-based console. The console includes the dashboard that gives you a graphic view in real time of the software status as well as the email flow on the server.

Quarantine management



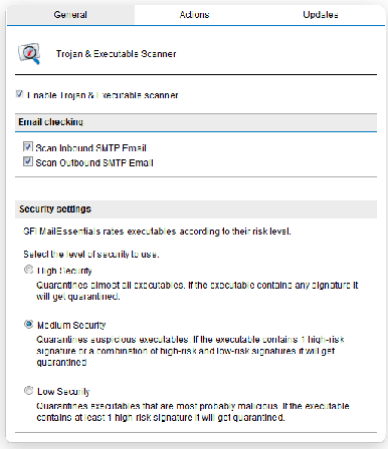
GFI MailEssentials gives you the flexibility to choose what to do with spam and malware emails. Users can mark emails as spam. You can quarantine suspected spam and notify users. You can establish central quarantine locations for malware.

Email content enforcement & data leakage prevention

The keyword-checking functionality in GFI MailEssentials can be used to scan inbound and outbound emails for keywords, and the attachment-checking functionality scans emails for attachments.

You can choose to block all incoming emails with potentially malicious attachment types, or block bandwidth and productivity wasters such as mp3 and Mpeg files.

Advanced user-based email filtering rules enable you to block emails based on patterns that you define, such as regular expressions. This is far more powerful than simple keyword checking.



Protect your company against email exploits and Trojans

The GFI MailEssentials Trojan and executable scanner detects unknown, malicious executables by analyzing what they do. The scanner uses built-in intelligence to rate the risk level by disassembling the executable, detecting what it might do and comparing its actions to a database of malicious actions. The scanner then quarantines any executables that perform suspicious actions, for example, making network connections or accessing the address book.

Protect your users against phishing and spyware

The GFI MailEssentials anti-phishing module detects and blocks threats posed by phishing emails by comparing the content of the spam with a constantly updated database and phishing URLs. This ensures all the latest phishing emails are captured. As extra protection, it also checks for typical phishing keywords in every email sent to your organization.

GFI MailEssentials also detects email-borne spyware via its antivirus engine, which incorporates a dedicated spyware and adware definition file that has an extensive database of known spyware, Trojans and adware.

SoftGen Australia Pty Ltd
P: (02) 9416 0416
E: sales@sgen.com.au
A: Suite 2, Level 3, Gordon, NSW 2072