

Google Message Security



ABOUT GOOGLE SECURITY AND ARCHIVING

Google security and archiving services, powered by Postini, make your existing email system more secure and compliant. Built on a hosted service platform, these products block spam, phishing, malware and other intrusions before they reach your network, and provide content management and archiving to help you meet legal challenges. Google's hosted model offers several distinct advantages. Leveraging the "network effect" of tens of thousands of email networks, Google technology detects new threats in real time and blocks them across the entire Google security network – without requiring on-site updates. Similarly, economies of scale in storage, simple deployment and maintenance-free service drive a low total cost of ownership.

For more information, visit www.google.co.uk/postini

Google Message Security, powered by Postini, provides highly effective inbound and outbound email security for organisations of all sizes. It simplifies the task of managing security and compliance of email messages and frees up valuable IT resources. Google Message Security is always on and always current, so organisations are assured of having effective and reliable protection for their email at all times.

Leveraging a patented, on-demand architecture, Google Message Security blocks spam, phishing, viruses, and other email threats before they reach your organisation, reducing load on your email servers, conserving bandwidth and improving the performance of your existing messaging infrastructure. Google Message Security is delivered in a Software-as-a-Service (SaaS) model, saving money and IT resources because there is no hardware or software to install and maintain.

Google Message Security conserves IT resources by eliminating the constant patching and updates that are required by other appliance or software solutions. It also reduces the burden on your IT help desk by empowering your end users to manage their own message quarantines and settings with an easy-to-use, web-based interface. Rather than calling your help desk, end users can inspect their message quarantines and deliver any desired messages. Users regularly receive a quarantine summary email with their quarantine details. They are also able to fine-tune their spam protection settings to their own preferred levels. All of these end user controls are totally configurable on a policy level, giving you complete control over what end users are allowed to do.

Google Message Security can automatically enforce your email security policies. This policy enforcement helps assure legal and regulatory compliance for both inbound and outbound email across your organisation. Transport Layer Security (TLS) support is included to encrypt sensitive email communications and can be automatically enforced for all communications between designated email domains. This ensures that sensitive or regulated communications are always delivered with the appropriate level of security.

Google Message Security also provides a convenient web console for administration. This console enables real-time configuration and policy modifications, monitoring, and alerting, as well as comprehensive reporting for administrators. Users can be defined in the console, or Google Message Security can be integrated with your organisational directory structure for user synchronisation.

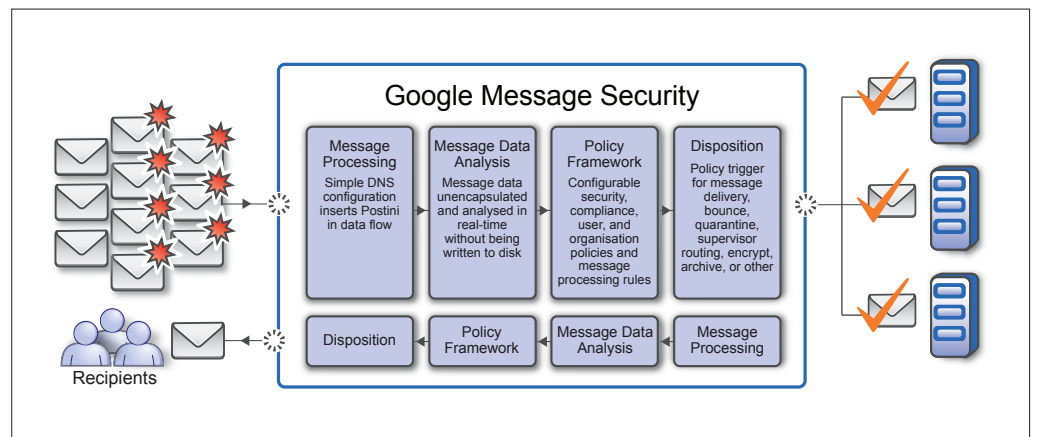


Figure 1: Google Message Security provides highly effective inbound and outbound email security for organisations of all sizes

Google Message Security includes multiple components that combine to deliver effective protection against email threats. Specific capabilities include:

- Real-time threat identification, based on processing more than two billion email messages per day, provides global visibility to emerging threats. This “network effect” automatically identifies and tracks internet protocol (IP) addresses that are issuing attacks such as spam, viruses, denial of service (DoS), etc. As soon as a threat is identified, it is blocked for all Google Message Security customers. The threat identification is also self-correcting. As identified IP addresses stop attacking they are again allowed to establish simple mail transfer protocol (SMTP) connections to send legitimate email messages.
- Patented, real-time anti-spam technology examines thousands of elements of an email message in order to determine if it is spam. It provides extremely effective spam filtering and exceptionally low false positive rates.
- Anti-virus protection builds on the anti-spam detection and includes zero-hour heuristics and signature-based detection methods, together with multiple commercial anti-virus engines.
- Content management allows you to define policies for both inbound and outbound email, providing an additional layer of protection against external threats. It also delivers protection from inadvertent or malicious leaks of confidential data in outbound email messages and their attachments.
- Attachment management technology enables you to define specific policies regarding file attachments and allows messages to be blocked or quarantined based on the types or sizes of files that are attached to email messages. Attachment management also inspects archive files such as .zip and .rar files to evaluate the files’ contents, and lets you define specific policies for handling encrypted archive files.

Feature	Benefits
Patented pass-through architecture	Delivers extremely effective spam filtering and low false positive rates
Multiple-layer virus blocking, heuristic and signature-based detection	Provides “zero-hour” protection from rapidly mutating viruses, 100% anti-virus SLA
Highly scalable, highly available SaaS platform, 99.999% filtering uptime SLA	Provides always on, always current protection with lower TCO
Web-based administration console	Allows real-time user and policy updates, configuration changes and reporting
Directory harvest attack/denial of service blocking	Prevents attacks with patented behavior analysis
Policy based TLS encryption	Secures transmission of emails
Attachment filtering	Enforces email attachment policies
Content policy management	Enforces acceptable use policies and content compliance
Email spooling	Continue to receive email messages even if your email server goes down

