Google Message Security

Protect your email infrastructure from spam and viruses; easily set and manage usage policies

ABOUT GOOGLE SECURITY AND ARCHIVING, POWERED BY POSTINI

Google security and archiving products, powered by Postini, make email systems more secure, compliant and productive by blocking spam and other intrusions before they reach your network, and by providing encryption and archiving to help you meet compliance requirements. Google's hosted model leverages the "network effect" created by billions of daily email connections to detect and block threats in real time, without requiring on-site updates. Economies of scale in storage, along with simple deployment and maintenance-free service, drive a low total cost of ownership.

For more information, visit
www.google.com/postini

Make your email servers more secure, compliant, and productive. Block email threats before they reach your organization. Ensure proprietary information that must remain confidential stays where it's safe. Eliminate the need for the ongoing patching and updates required by appliance or software solutions. Leverage cloud services to reduce maintenance, conserve bandwidth, and improve the performance of your existing email infrastructure.

Product Summary

Google Message Security, powered by Postini, is a secure, hosted service that provides enterprise-grade spam and virus protection and email content filtering, delivering cost-effective email management. Google Message Security lets you:

- secure your inbound and outbound email from spam, viruses, phishing, and other email-borne threats
- set central email policies to manage content and compliance requirements
- receive email messages even if your email server goes down

Google Message Security automatically enforces your email security policies to help assure legal and regulatory compliance for both inbound and outbound email across your organization. The service also provides a convenient web console for administration, enabling real-time configuration and policy modifications, monitoring, and alerting, as well as comprehensive reporting for administrators. Define users in the console, or integrate Google Message Security with your organization directory for easy user synchronization.

Google Message Security also:

- includes patented anti-spam technology, which examines thousands of elements of an email message to determine safety

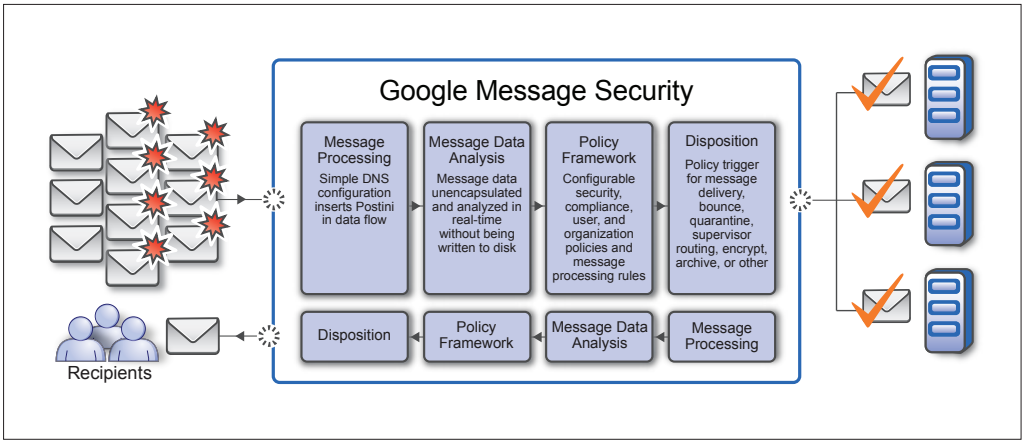

Figure 1: Google Message Security provides highly effective inbound and outbound email security for organizations of all sizes

- delivers exceptionally low false positive rates
- leverages global "network effect" based on billions of email messages per day to identify emerging threats, ensuring early blocking and prevention. Quickly self-corrects for safe IP addresses so that email flow is not interrupted
- eases IT management of policy configuration, ensuring appropriate user guidelines
- lets end users manage their own message quarantines and settings and fine-tune preferences within IT-set policies, via an easy-to-use web interface and without additional support
- includes Transport Layer Security (TLS) support, allowing encryption of sensitive email communications (can be automatically enforced for communications between designated email domains)

Google Message Security supports the following:

Mail servers The service supports common mail servers including Microsoft Exchange Server, Lotus Domino, Postfix, Sendmail, Macintosh OS X Server, Novell Groupwise, and is also included in Google Apps Premier Edition.

Service Providers (hosted email) The service is compatible with ISPs and domain name providers that host the email for your own domain but you must have the ability to change the MX records associated with your service.

Feature	Benefits
Spam and virus protection	Provide multi-layer threat identification including heuristic and signature-based detection, commercial anti-virus engines, and "zero-hour" protection from rapidly mutating viruses
Directory harvest attack/denial of service blocking	Prevents attacks with patented behavior analysis
Patented pass-through architecture	Ensures maximum privacy of your email
Content policy management	Enforces acceptable use policies and content compliance for inbound and outbound email
Scalability	Built-in scale for dealing with any kinds of spam spikes or targeted attacks
Web-based administration console	Allows real-time user and policy updates, configuration changes, and reporting
Log search	Retrieve and export log information on inbound and outbound message routing details
Email spooling	Continue to receive email messages even if your email server goes down
Domain-to-domain encryption	Transmit secure messages with policy-enforced Transport Layer Security protocols
Attachment filtering	Enforce policies including attachment size or file type limitations
Intelligent routing	Easily route email traffic to decentralized data center locations
Robust service level agreement	100% anti-virus and 99.999% service uptime

Google™