Google Message Security

ABOUT GOOGLE APPS

Google Apps is a suite of applications that includes Gmail, Google Calendar (shared calendaring), Google Talk (instant messaging and voice over IP), Google Docs & Spreadsheets (online document hosting and collaboration), Google Page Creator (web page creation and publishing), Start Page (a single, customizable access point for all applications) and Google Security & Compliance. Google Apps offers editions tailored to specific customer needs, including the Standard Edition (ideal for family domains), Education Edition (K-12 schools, colleges and universities) and Premier Edition (businesses of all sizes).

For more information, visit
www.google.com/a/security

Google Message Security, powered by Postini, provides highly effective inbound and outbound email security for organizations 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 organizations 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 organization, 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, 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 organization. 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.

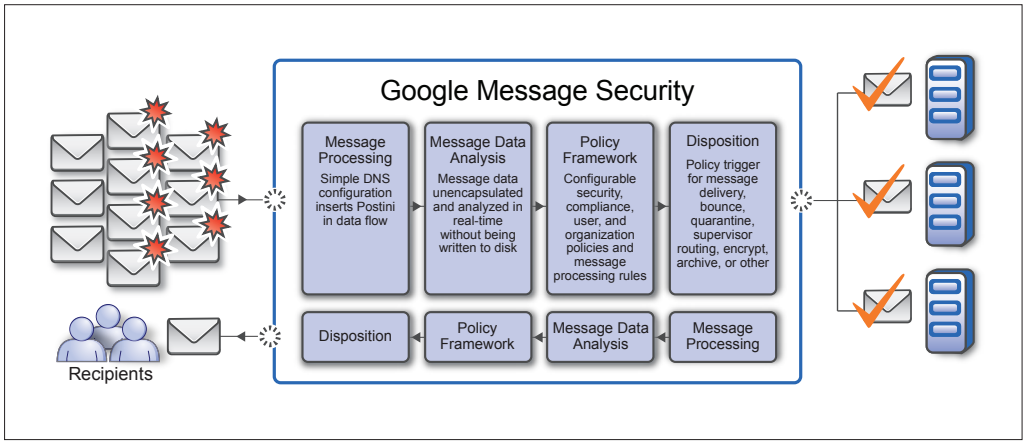

Figure 1: Google Message Security provides highly effective inbound and outbound email security for organizations of all sizes

Google Message Security provides a convenient web console for administration. The console provides 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 organizational directory structure for user synchronization.

Google Message Security includes multiple components that combine to deliver effective protection against email threats available today:

- Real-time threat identification, based on processing over 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 so that as 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 that provides 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 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 inspects archive files such as .zip and .rar files to evaluate the files' contents. It also lets you define specific policies for handling encrypted archive files.

Features	Benefits
Patented pass-through architecture	Delivers extremely effective spam filtering, extremely low false positives
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 of your email server goes down

Google™