

Google Message Filtering



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 Filtering, powered by Postini, provides inbound email filtering for organizations of all sizes. Leveraging a patented, on-demand architecture, Google Message Filtering blocks spam, phishing, viruses, and other email threats before they reach your organization, reducing message volume and increasing capacity on your email servers and infrastructure. Google Message Filtering 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 Filtering processes over two billion messages each day. This enables the service to harness the latest and most accurate threat intelligence – in real time – and apply it to every message flowing through the service network. This “network effect” enables Google to alert, update, and protect all client communications instantly, making Google Message Filtering highly efficient and reliable.

Google Message Filtering simplifies messaging infrastructure, eases IT administration burdens, and lowers the total cost of ownership compared to software or appliance based solutions. Google Message Filtering offers a 99.999% filter uptime performance SLA and is constantly updating anti-spam and anti-virus filters to ensure that clients are always protected from the latest threats.

It’s easy to get started with Google Message Filtering. All it takes is a simple change to your email MX records to route email through our data centers. There, messages are analyzed in real time rather than stored to disk to help ensure minimal latency and maximum privacy of your mail. During this process, spam, viruses, and other attacks are stopped. This significantly reduces the volume of mail passed to your network, enabling you to increase scalability with your current systems.

Google Message Filtering reduces the burden on your IT team by empowering your end-users to manage their own messages. Rather than calling your help desk, end-users are empowered to 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.

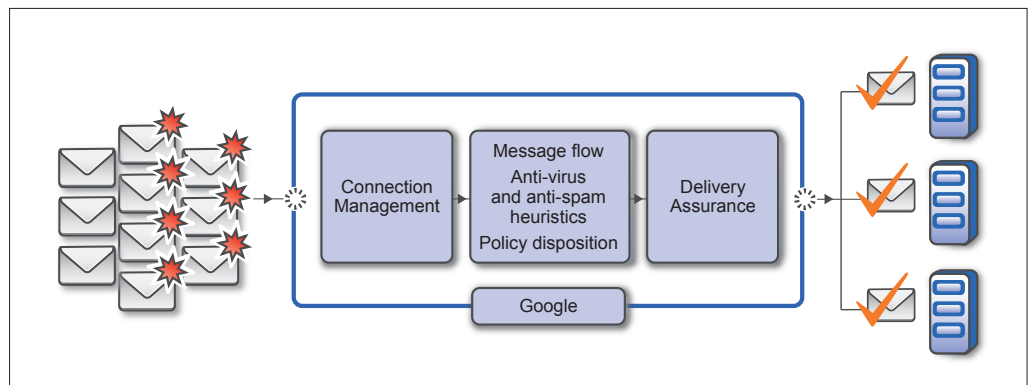


Figure 1: Google Message Filtering provides highly effective inbound email security for organizations of all sizes

GOOGLE MESSAGE FILTERING

Features	Benefits
On-demand architecture	Easy implementation, reduced administration, and reduced load on your infrastructure
Patented proxy filtering	Maximum privacy and minimal latency
Spam and virus blocking	Extremely high catch rates, virtually zero false positives, and “zero-hour” protection from rapidly
Directory harvest attack/ Denial of service attack blocking	Prevents attacks with patented behavior analysis
Attachment filtering	Enforces email attachment policies defined by the administrator

