



## Google Gmail Security

### Overview

Our Google Gmail Security app allows businesses to enjoy the cost-savings of Google Gmail for their email and collaboration needs, while retaining the full policy-based control that only Sendmail can provide for content control, encryption, access, and authentication.

### Audience

Companies that need policy-based enforcement of company and regulatory compliance requirements, even though they outsource their mailboxes to Gmail to lower costs and simplify email management.

### Key Features and Functionality Overview

Many companies are turning to software-as-a-service (SaaS) solutions for a wide range of business applications they used to host and manage in-house. By outsourcing services via the Internet to expert providers with dedicated resources, businesses reduce their capital costs, free up network bandwidth, and redirect IT staff time toward more strategic projects.

When it comes to SaaS for email and collaboration, no one does it better than Google. You can rely on Gmail to deliver mail with 99.9% uptime, anti-virus/spam protection, disaster recovery, and a rich set of unified communication and collaboration features—all at a very affordable per-seat price. However, what Google can't do—and shouldn't do—is manage and enforce your email policies. You need to keep firm control over the policies that control email access, sender authentication, encryption, permissible content, data loss prevention, and regulatory compliance. The security, legal liability, and ultimately the profitability of your business all depend on it.

With the Google Gmail Security app, you can let Google manage the mail while you manage the policies. Depending on your email volume and scalability needs, our Professional Services team specially configures one or more Sentrion appliances, which can be deployed at your site or hosted by a co-location company such as RackSpace. Messages sent to or from your employees' Gmail accounts are automatically routed to the Sentrion for policy enforcement—and quarantine if necessary—and then routed to Gmail for delivery. You can use the solution to scan and apply policy to inbound email only, outbound email only, or both:

- Inbound email is first routed to the Sentrion, which authenticates the mail, eliminates unwanted or dangerous content, enforces regulatory and corporate compliance, and encrypts sensitive information before sending the message to Gmail for routing to the employee's mailbox. Mail can also be archived or quarantined based on your custom policies.
- Outbound email is routed from the employee's Gmail account to the Sentrion, which eliminates unwanted content, enforces compliance, encrypts sensitive information, and performs DKIM sender authentication to prevent your domain being used for phishing scams. Based on policy, messages can also be archived or quarantined before being returned to Gmail for routing to the recipient.

The solution easily scales and adapts to meet your needs, no matter how large your email volumes grow or how complex your policy requirements. With the Google Gmail Security app, you can let Google manage the mailboxes, but always retain complete control.