Comparing Google Message Security and Leading Messaging Security Solutions

An Osterman Research White Paper

Published February 2008

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 866 842 3274 • info@ostermanresearch.com • www.ostermanresearch.com

Executive Summary

Osterman Research was commissioned by Google to undertake a market research survey of organizations that are using Google Apps Security and Compliance Solutions, as well as solutions offered by nine other leading vendors. The goal of this research was to determine how organizational decision makers perceive the offerings with which they are most familiar, and to determine if there are quantifiable differences between Google's solutions and those offered by the other vendors.

The data presented in this white paper discusses the results of the research program that was conducted during August and September 2007, focusing on Google Message Security results independently from an aggregate of the other nine vendors' results. Google Message Security is not compared directly to any particular vendor in this analysis, but instead to the results from all of the other vendors.

Our research found that customer satisfaction with the innovation of Google Message Security solutions was higher than the average of its competition on things like the amount of spam captured, virus capture efficiency and the amount of technical support that the solution required.

Our research found that with Google Message Security customer satisfaction was higher than the average of its competition on things like the amount of spam captured, virus capture efficiency and the amount of technical support that the solution required. Further, Google Message Security's results for the amount of IT time required to manage the system was decidely better than the average of the other systems, not surprising given that most of the other solutions are on-premise solutions. In some other areas, Google Message Security and its competition were viewed as roughly similar.

Overview and Methodology

Google commissioned Osterman Research to conduct a study of organizations' use of various messaging security products, the goal of which was to compare Google Message Security's anti-virus and anti-spam capabilities with those of several of its leading competitors. The goals of this project were several:

- To gather quantitative information on Google Message Security offering, as well as those of nine of its leading competitors.

- To gather qualitative information on the efficacy of these ten solutions in reducing the impact of spam and viruses on corporate messaging systems and networks.

- To compare Google Message Security versus an amalgam of its leading competitors, not to single out specific solutions for comparison with Google Message Security.

The solutions surveyed, as well as the number of surveys completed for each solution, are shown in the following table.

Number of Respondents Surveyed per Vendor

Vendor	Number of Surveys Completed
Barracuda	14
Google Message Security	28
IronPort	13
MessageLabs	5
Microsoft Forefront	12
MX Logic	4
Secure Computing	10
Symantec	24
Trend Micro	22
Websense (Blackspider)	8

Organizations of various sizes in North America and Europe were surveyed for this project, but the median number of employees at the organizations surveyed was 3,100 and the median number of email users was 2,600. The respondent organizations covered a wide range of industries.

The organizations using Google Message Security averaged a greater number of employees and email users than the other organizations. The firms surveyed were drawn primarily from the Osterman Research Survey Panel; the individuals surveyed had to be involved in the management of their organizations' messaging and/or networking systems in order to qualify for participation in the survey. Surveys were conducted between August 21 and September 23, 2007.

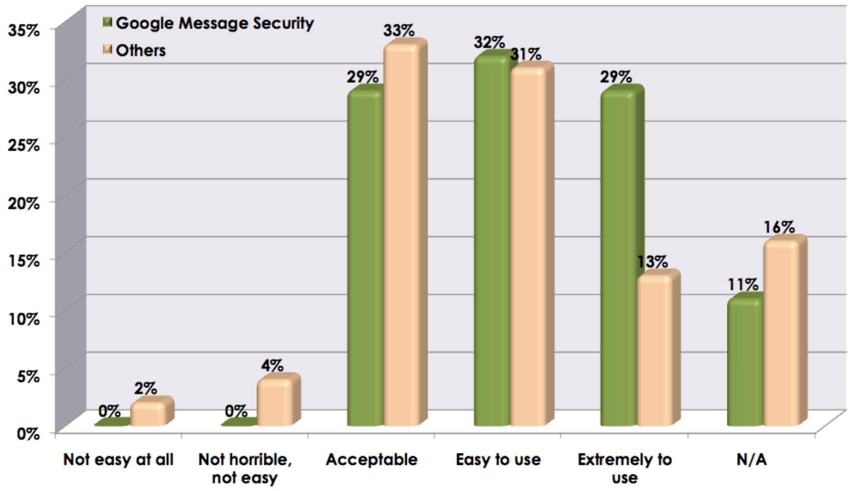
Research Findings

Ease of Use for End Users is a Key Issue

While many organizations do not allow end users to gain access to spam quarantines, the vast majority do. As a result, ease of use for security solutions is a key issue given the potential impact this has on IT management time, help desk, etc. In other words, the easier a system makes it for non-IT staff to manage their own quarantines, the less impact users will have on IT staff.

As shown in the following figure, twice as many organizations using Google Message Security report that their system is 'extremely easy to use' for end users, while about the same number report that the system is 'easy to use'.

System Ease of Use for End Users

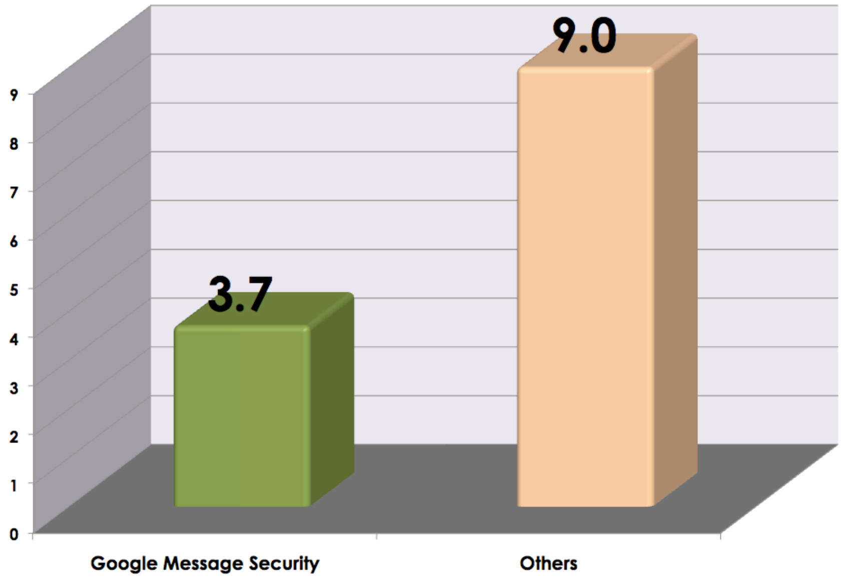


One of the key differentiators the research found was in the amount of IT management time that must be devoted to the maintenance of each solution. Organizations using Google Message Security require significantly less IT management time on a weekly basis relative to organizations using other solutions.

Google Message Security Requires Less Management Time

One of the key differentiators the research found was in the amount of IT management time that must be devoted to the maintenance of each solution. As shown in the following figure, organizations using Google Message Security require significantly less IT management time on a weekly basis relative to organizations using other solutions.

Total Hours Spent per Week Per 1,000 Users Managing the System
(Hours per 1,000 Email Users)

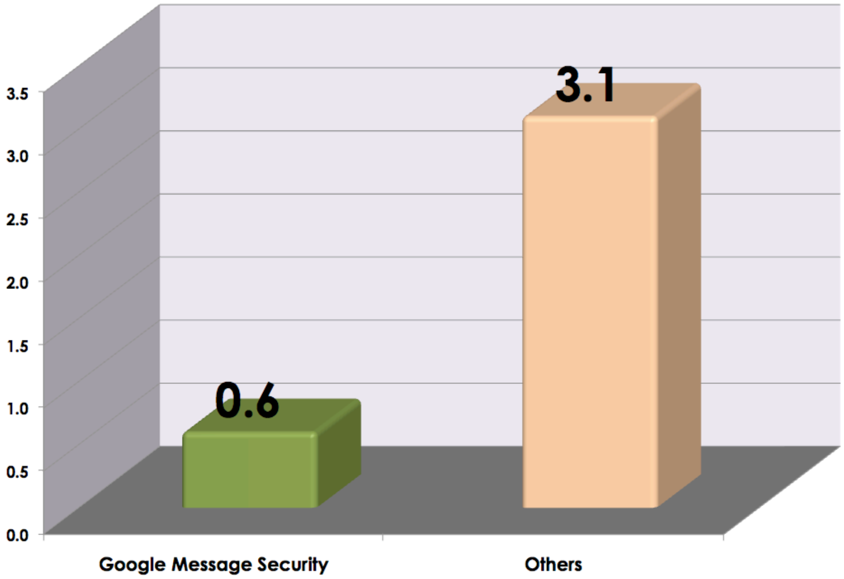


In an organization of 2,500 users, this would translate to a savings of nearly $26,000 annually for organizations using Google Message Security, or the equivalent of just over 0.3 full-time equivalent (FTE) IT staff members.

If we assume that a fully burdened salary for an IT administrator is $80,000 annually, the data in the figure above translates to annual maintenance expenditures of $7.43 per user per year for organizations using Google Message Security, and $18.00 per user per year for organizations using other solutions. In an organization of 2,500 users, this would translate to a savings of $27,000 annually for organizations using Google Message Security, or the equivalent of just over 0.3 full-time equivalent (FTE) IT staff members.

Because the organizations surveyed using Google Message Security were, on average, larger than other organizations, we also compared IT time investments only for those organizations with at least 1,000 email users in order to provide more of an 'apples-to-apples' comparison. A comparison of organizations using Google Message Security and other solutions is shown in the following figure, demonstrating an even more decided advantage for Google Message Security.

Total Hours Spent per Week Per 1,000 Users Managing the System
(Organizations With 1,000 or More Email Users)



Our analysis demonstrated that those involved in managing their organizations' messaging and/or networking systems view Google Message Security as an excellent solution for stopping spam, viruses and other messaging-related threats; and that they invest less IT staff time in managing Google Message Security.

Again, if we assume that a fully burdened salary for an IT administrator is $80,000 each year, the data in the figure above translates to annual maintenance expenditures of $1.11 per user per year for organizations using Google Message Security and $6.15 per user per year for other organizations. In an organization of 2,500 users, this would translate to a savings of nearly $12,600 annually, or the equivalent of just over 0.16 FTE IT staff members.

Google Message Security Customer Satisfaction is Very High

Overall, Google Message Security fared better than the amalgam of leading competitors in this analysis in terms of customer satisfaction. As shown in the following table, customer satisfaction with Google Message Security is significantly higher in terms of the amount of spam captured, the amount of technical support required, the up-front cost of the solution and the flexibility of policy management offered in the solution. Google Message Security fared moderately better in terms of virus capture efficiency, the ongoing cost of the solution and in the quality of the technical support provided.

Satisfaction Level on Various Attributes
% Responding Satisfied or Very Satisfied

Attribute	Google Message Security	Others
The amount of spam captured	96%	78%
Virus capture efficiency	93%	87%
The amount of technical support required	93%	78%
The amount of your IT effort required	82%	73%
The up-front cost of the solution	81%	64%
The number of false positives generated	79%	67%
The ability to manage policies the way you want	79%	59%
The ongoing cost of the solution	74%	72%
The quality of the technical support provided	74%	70%
The vendor's addition of new capabilities	70%	63%

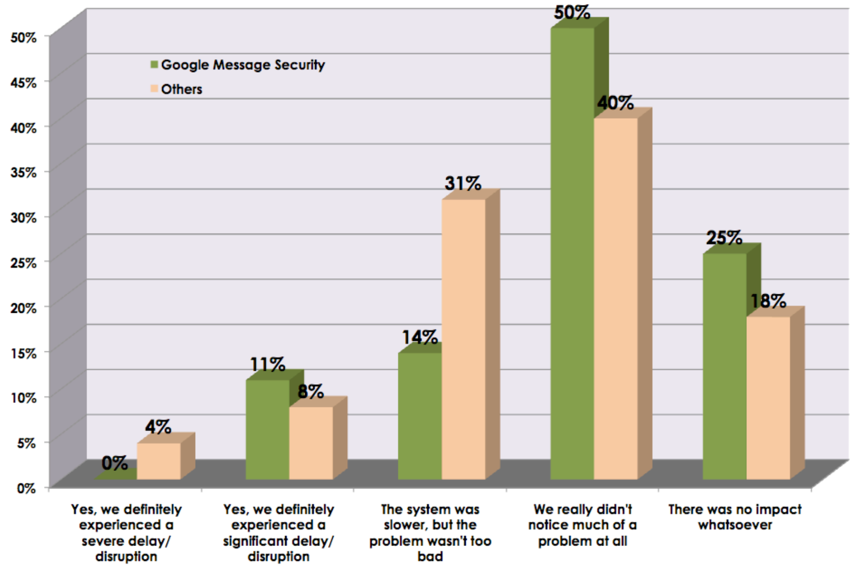
The vendors with whose products Google Message Security was compared in this analysis offer very good capabilities and are all worthy of consideration for organizations that seek to provide robust messaging security capabilities. Our analysis demonstrated that those involved in managing their organizations' messaging and/or networking systems view Google Message Security as an excellent solution for stopping spam, viruses and other messaging-related threats; and that they invest less IT staff time in managing the Google Message Security solution.

96% of organizations using Google Message Security report that the system is mostly or always available versus 87% of organizations using other solutions. Even more telling, however, is the fact that nearly three out of five Google Message Security customers report that the system is 'always available'.

The August Spam Storm Impacted Google Message Security Customers Less

During the period August 7-9, 2007, there was a significant storm of PDF spam. As shown in the following figure, 75% of Google Message Security customers reported that they saw little or no problem from this particular storm versus only 58% of organizations using other solutions that reported seeing this minimal impact from the storm.

"During the August 7-9, 2007 storm of PDF spam, did you experience performance degradation?"

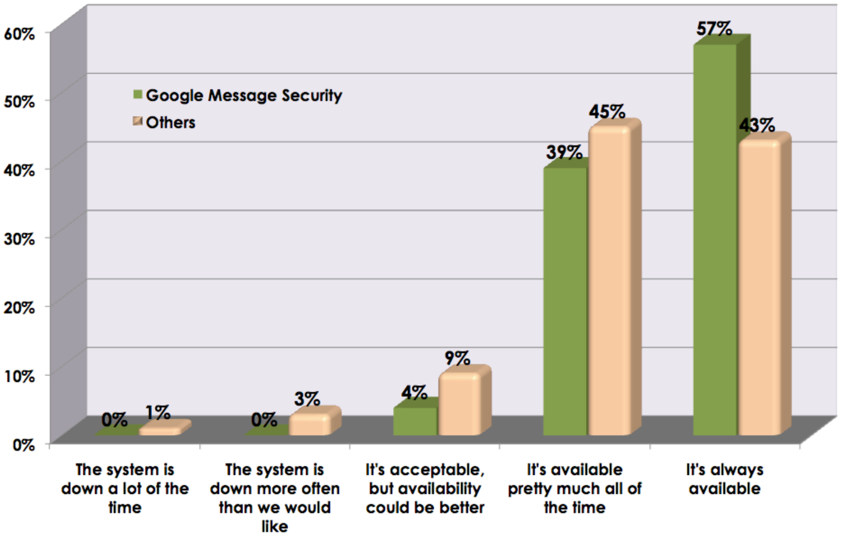


Availability of a messaging security solution is a critical issue given the almost continual flow of messages that users receive.

Availability is a Critical Issue

Availability of a messaging security solution is a critical issue given the almost continual flow of messages that users receive. As shown in the following figure, 96% of organizations using Google Message Security report that the system is mostly or always available versus 87% of organizations using other solutions. Even more telling, however, is the fact nearly three out of five Google Message Security customers report that the system is 'always available'. Conversely, while 12% of organizations using other solutions report that system availability is poor or simply acceptable, only 4% of Google Message Security customers report this minimal level of availability.

System Availability During the Past Three Months

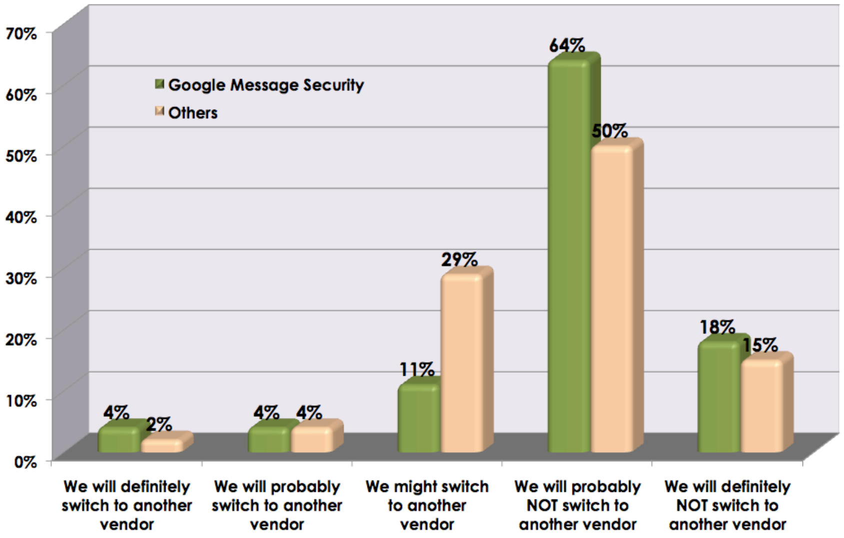


Vendors' ability to maintain or improve false positive rates is even better than their spam capture efficiency. Google Message Security has a slight edge in this regard, with a somewhat larger proportion organizations using Google Message Security reporting that false positive efficiency is improving over time.

Google Message Security Customers Are Less Likely to Switch

More than four out of five organizations using Google Message Security report that they are unlikely to switch to another vendor's offering, while only two-thirds of organizations using other solutions report this level of loyalty, as shown in the following figure.

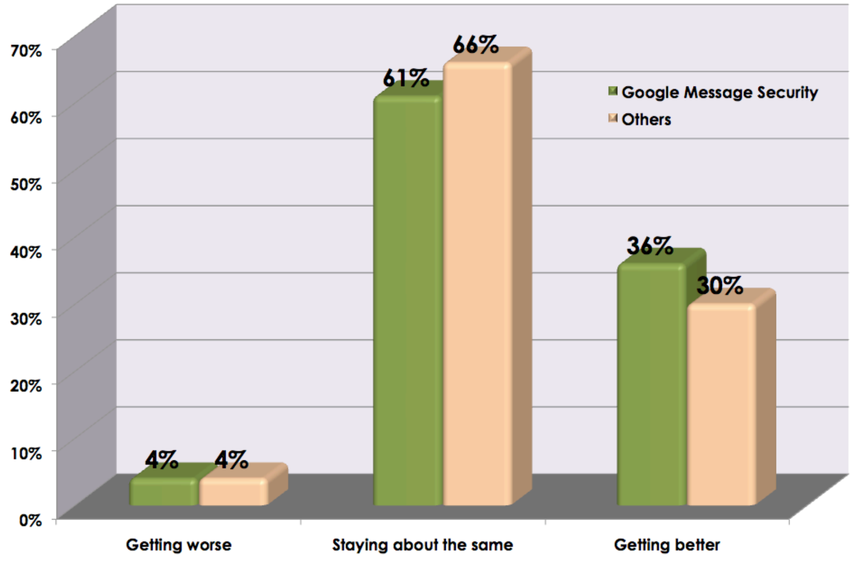
Likelihood of Staying With Vendors Over the Long Term



False Positive Innovation is Very Good for All Vendors

Vendors' ability to maintain or improve false positive rates is even better than their spam capture efficiency, as shown in the following figure. Google Message Security has a slight edge in this regard, with a somewhat larger proportion of organizations using Google Message Security reporting that false positive efficiency is improving over time; only four percent of Google Message Security and organizations using other solutions report that false positive efficiency is getting worse.

Changes in Vendors' Spam False Positive Capabilities Over Time



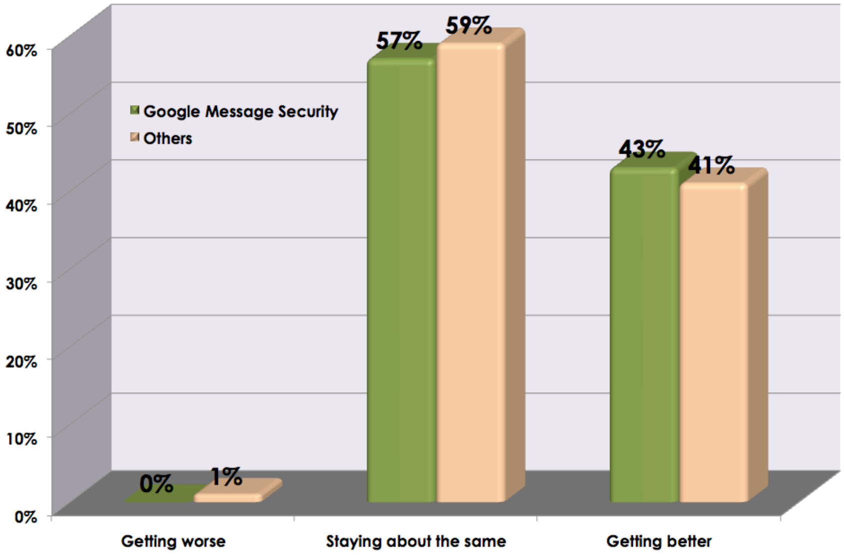
Vendors' ability to capture viruses is improving even more than either their innovation in spam capture efficiency or their generation of false positives. Here, too, Google Message Security has a slight edge.

Osterman Research found relatively little difference between Google Message Security and its competition in terms of the vendors' improvements in their ability to capture spam over time: 36% of Google Message Security customers believe their solution is getting better over time versus 34% for the other vendors.

Innovation in Anti-Virus Capabilities Are Even Better

Vendors' ability to capture viruses is improving even more than either their innovation in spam capture efficiency or their generation of false positives, as shown in the following figure. Here, too, Google Message Security has a slight edge, with more organizations using Google Message Security reporting that their anti-virus capabilities are getting better over time; virtually no organizations reported that these capabilities are worsening over time.

Changes in Vendors' Anti-Virus Capture Capabilities Over Time

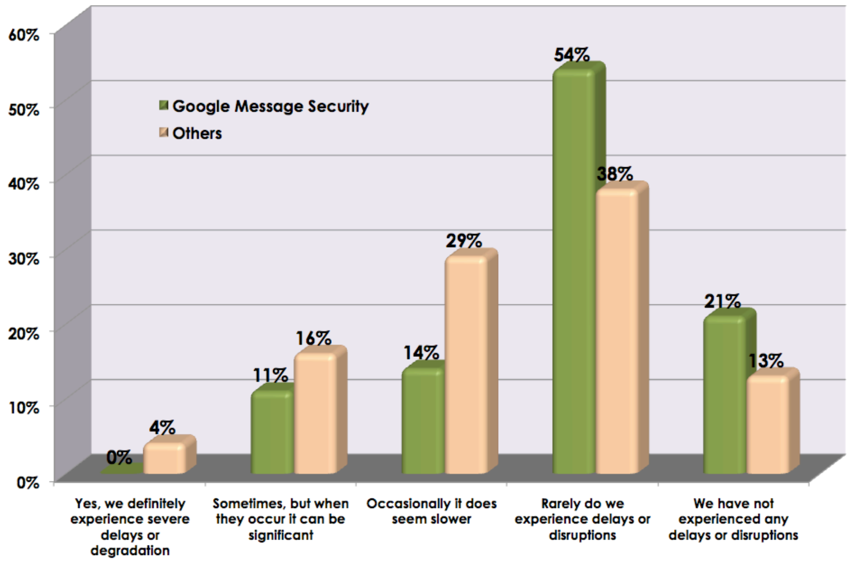


75% of organizations using Google Message Security report that they rarely or never experience any sort of performance degradation in their system versus 52% of organizations using other solutions that report this lack of performance problems.

Performance Degradation is Another Key Issue

As shown in the following figure, 75% of organizations using Google Message Security report that they rarely or never experience any sort of performance degradation in their system versus 51% of organizations using other solutions that report this lack of performance problems. Conversely, whereas 11% of organizations using Google Message Security report that the system sometimes experiences significant performance degradation, 20% of organizations using other solutions report this level of performance problem.

"Overall, during the past six to 12 months, during major spam storms do you experience performance degradation?"



Summary and Conclusions

This analysis found that all of the products surveyed provide good performance and will adequately protect a messaging infrastructure. However, comparing the aggregated results of Google Message Security competitors with Google Message Security offerings shows that Google Message Security offers a significantly lower cost of management per user and greater customer satisfaction.

Comparing the aggregated results shows that Google Message Security offers a lower cost of management per user and greater customer satisfaction.

1600 Amphitheatre Pkwy.
Mountain View, CA 94043

Toll Free (US/Canada)
+1 866 767 8461

Toll Free (Germany)
0800 67 37 97 6

Europe
+44 20 7082 2000

Other
+1 650 486 8100

www.google.com/a/security

Sponsor of this White Paper

Postini is a wholly owned subsidiary of Google, Inc. 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 Sites (team site creation and publishing), Start Page (a single, customizable access point for all applications) and Google Apps Security & Compliance. The security and compliance products, powered by Postini, are available to businesses and organizations who want to make their existing email infrastructures more secure, compliant and productive. Businesses of all sizes can now get best-in-class email security, archiving and e-discovery and Google Apps innovation is making it easier and more affordable than ever before. These products work with virtually any email server that supports SMTP such as Lotus Notes/Domino, Microsoft Exchange, Novell Groupwise and others.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.