Competitive Comparison:
Proofpoint Enterprise vs. Google Message Security (Formerly Postini)
EXECUTIVE SUMMARY

Email is unquestionably the primary form of business communications. Unfortunately, it is also one of the most vulnerable channels for security attacks, data leakage, and fraud. This white paper compares how two email security solutions protect organizations from the risks associated with email-borne threats: Google Postini Services and Proofpoint Enterprise.

In mid-2011, email has resurfaced as the biggest focal point for security and compliance risk, as hackers and criminal syndicates are continually evolving their tactics and creating ever more effective, malicious, and costly attacks. Now they are sending highly customized and targeted spear-phishing attacks that include personalized information gained from social networks or data from other breaches. Their success rate? High enough to have compromised the secure keyfob technology at IT security leader RSA and to have purloined millions of email addresses from email marketing giant Epsilon, whose clients include Best Buy, Citibank, L.L. Bean, and Walgreens.

If a security leader was breached, all organizations are at risk. Email security and compliance products currently in place, especially those from Google, must be re-evaluated to ensure they can effectively protect end users, corporate data, and customer data from these new types of threats. Adequate protection against these targeted attacks includes the ability to uniquely handle phishing messages versus other types of annoying and less dangerous spam. Email security services must provide zero-day protection and reporting, must automate as much protection as possible, and must leave as little as possible to chance or human error.

Google Postini Services were originally developed by a company named Postini, which Google acquired in 2007. At the time, Postini was highly rated by analysts as a market leader that introduced regular innovations to its service. But since the acquisition, Google has done little to develop Postini’s security technology (now called Google Message Security), so now leave enterprises vulnerable to phishing and spear-phishing attacks.

Google’s quarantine structure and the workflow end users employ to manage their Junk Folder has not been updated since the acquisition by Google. As a result of this lack of investment, Google quarantines all types of blocked email (false positives, newsletters, spam, phishing) into a single Junk Folder accessible through the Message Center. As phishing emails use social engineering to appear legitimate, end-users are likely to release the emails from their quarantine using either the daily Quarantine Summary email or end-user accessible Message Center. This out-dated approach repeatedly exposes users to the wiles of hackers and increases the risk that enterprises will fall prey to security attacks that can result in lost data, lost productivity, damage to brand and reputation and applicable regulatory penalties and fines. Google’s out-dated technology further exposes organizations, as their service lacks real-time tools and reporting that security officers need on a daily basis to investigate these attacks.

In contrast, Proofpoint Enterprise detects and stops phishing attacks using advanced machine-learning techniques. Furthermore, phishing emails are securely kept away from end users in a separate quarantine, that only administrators can view or access. This is an example of how Proofpoint’s defenses evolve continuously to identify and stop the latest attacks, providing enterprises with 24/7 protection while also relieving end users of the burden of making critical security decisions that can lead to costly mistakes. Proofpoint’s innovative approach also enables security officers to follow a real-time action plan to investigate phishing attacks in case they, a customer, or a company in the same industry is publicly notified of a threat.

THE EVOLUTION OF SPAM: FROM ANNOYANCE TO TARGETED ATTACKS

Spam is changing, and enterprises need to take notice.

The original definition of spam included “bulk mail” and described email that was more annoying than malicious. Now hackers are using more sophisticated, targeted, and personalized “spear-phishing” attacks to trick users into opening malicious attachments or clicking on Web links that surreptitiously download malware. That malware, in turn, can shut down IT defenses and create a back-door for hackers to access an enterprise’s internal systems. Because of these new attacks, enterprises are losing intellectual property and customer data to hackers. In some cases, even the customers of attacked enterprises are finding themselves under attack.

Phishing attacks are effective because they’re plausible. That plausibility makes them harder to detect. The emails are targeted to end users and contain email addresses and subject lines that are relevant to the recipient. A phishing message might appear to be a message from the recipient’s bank, requesting that he or she log in to address a security issue or to receive a special offer. Or it might appear as an email from a friend or colleague, delivering an unexpected (and rigged) Microsoft Office file as an attachment.
Enterprises should assume that they are under attack, and they should continuously examine their email stream for instances of spear-phishing. By mid-2011, there have been at least six high-profile and very successful spear-phishing attacks that were publicly announced:

**February 2011**: Spear-phishing attacks gave hackers access to internal systems at the Canadian Finance Ministries; the ministries shut off Internet access in response¹

**March 2011**: Hackers spear-phish and infiltrate the French Ministry of Finances²

**March 2011**: A breach at RSA was the result of spear-phishing attacks on a small group of high-level employees³; as a result of the breach, RSA warned customers of its keyfob security service to be extra careful⁴; the breached keyfob security service were later used to hack into defense contractors L-3 Communications and Northrup Grumman⁵

**April 2011**: A spear-phishing attack initiated a data breach at Epsilon, a firm that manages email information for over 2,500 businesses; for several months, hackers had access to internal systems, including systems managing email lists for brands such as Best Buy, Citibank, Chase, Target, Walgreens, and Verizon⁶

**June 2011**: A breach at the global financial organization International Monetary Fund was triggered by a spear-phishing attack⁷

**July 2011 and April 2011**: Two spear-phishing attacks shut down email services and internet access at The Department of Energy’s Pacific Northwest National Laboratory and Oak Ridge National Labs⁸

These attacks show just how effective spear-phishing can be. When security companies and government agencies fall prey to attacks, one can assume that all enterprises are at risk.

The attack on Epsilon alone will likely fuel more successful attacks against enterprises and consumers. Epsilon is one of the world’s largest email service providers. Breaching Epsilon’s IT defenses gave hackers access to the names and email addresses of millions of customers of major brands. Hackers can use this information to create believable email messages purportedly sent from banks and other trusted organizations.

Because email addresses are so useful for spear-phishing attacks, hackers are stealing addresses from a wide variety of organizations. In addition to the Epsilon attack, other recent email thefts include:

**February 2011**: Hackers steal 400,000 email addresses from an Irish job site⁹

**July 2011**: Hackers steal 1.27 Million email addresses from the *Washington Post*¹⁰

**July 2011**: Hackers steal 90,000 military emails¹¹

Now that hackers and criminal syndicates have access to more email addresses than ever before, it’s all but certain they’ll use this data to unleash new, ever-more-effective phishing attacks. Enterprises need to be ready. They need email security solutions that go beyond filtering out ads and viruses. Enterprises must be prepared with an email security solution to stop phishing now and in years to come.

Let’s look at a complete list of enterprise email security requirements, including anti-phishing defenses.

**EMAIL SECURITY REQUIREMENTS IN 2011**

Spam fell in 2011 after police broke up criminal networks responsible for two major botnets (Mariposas in 2010 and Rustock in 2011), but spam volumes alone don’t convey the danger inherent in email. A few highly targeted, carefully designed attacks can cause much more damage than high volumes of cheesy advertisements. Enterprises must guard against all forms of email-borne attacks. Email security requirements include the following:

- **Ability to defend against a targeted blended threat, including phishing attacks**
  A blended threat is a threat that combines email and some other technology, such as a Web page or a YouTube video. Many phishing attacks are blended threats; for example, email messages that direct users to click on a link for a bank’s Web site. Blended threats can be difficult to detect because they might not contain any spam keywords or malware themselves. To be effective, email security needs to be able to detect and stop all these types of threats as soon as they appear.

- **Ability to respond to an attack**
  Comprehensive email security solutions deliver more than effective technology. They also provide prompt service around the clock for customers under attack. And they provide tools that email administrators and security officers can use to monitor email activity in real time in order to resolve problems as quickly as possible.
Security is not Google’s focus
“I think about our products in three separate categories. First, there is Search in our Ads products, the core driver of revenue for the company. Next, we have products that are employing high consumer success: YouTube, Android and Chrome. Then we have our new products, Google+ in commerce and local. We are investing in them to drive innovation and adoption.”

- Quote from Larry Page, Google CEO and co-founder

Security is Proofpoint’s focus
“Proofpoint continues to lead the market with a focus on security, innovation and customer satisfaction, delivering solutions for email security, encryption, data loss prevention and email archiving that help organizations reduce costs while making email safe, secure, compliant and easier to manage.”

- Quote from Gary Steele, Proofpoint CEO

VENDOR COMPARISON: GOOGLE (POSTINI) VS. PROOFPOINT
Now that we’ve described the requirements for email security in 2011, let’s examine how two major vendors in the email security market measure up against these requirements. In this paper, we’ll compare Google and its Postini email services and Proofpoint and its Proofpoint Enterprise services.

Vendor Overviews

Google (Postini)
Google Postini services comprise four SaaS security services for email: Message Security, Message Continuity, Message Discovery, and Message Discovery (Extended). These services provide a layer of security and compliance services for an enterprise’s existing email services, such as Microsoft Exchange servers running on premises, or for SaaS email services, such as Google’s own Gmail service.

Google Message Security provides a base level of security common to all four services. It filters inbound email for spam and viruses, filters outbound email for viruses and content that might violate content rules, and provides support for transport layer and ad-hoc email encryption. Message Continuity and Message Discovery extends Message Security with failover services and archiving, but are not discussed in this white paper.

Google Postini services were originally developed by a company called Postini, which was founded in 1999. Google bought the company in 2007. Since then, Google has done little to develop the services. In a recent earnings call with investors, Google’s CEO Larry Page listed three priorities for the company, and enterprise IT (including enterprise IT email services) wasn’t one of them.

Proofpoint
Proofpoint provides SaaS and on-premises solutions for email security and compliance, including inbound email security, outbound email security and data loss prevention, privacy protection, email encryption, email archiving, and eDiscovery. The company was founded in 2002 by Eric Hahn, the former CTO of Netscape, and now provides email security and archiving solutions for enterprises around the world.

Proofpoint Enterprise, the company’s email security and compliance solution, provides anti-spam, anti-virus, anti-phish detection, email policy enforcement, message tracing and email encryption—for both inbound and outbound email. Proofpoint Enterprise uses Proofpoint MLX™ machine learning technology to detect new forms of email-borne threats as soon as they appear. Proofpoint Enterprise also filters outbound messages for spam and provides email data loss prevention and native encryption to protect confidential and sensitive data. Proofpoint Enterprise is available as a SaaS service, an on-premises physical or virtual appliance, or a hybrid configuration combining SaaS and on-premises services.

Effective Defenses against Spam, Phishing, Malware, and Other Email-borne Attacks
Google’s spam filtering forces end users to make split-second security decisions against targeted and malicious messages twice – first through their Quarantine Summary and second within their Junk Folder accessible through the Message Center.

Comparing Defenses against Phishing Attacks and Other Blended Threats
Bottom Line: Google’s outdated Bulk Email category filters leaves end users and corporate data vulnerable. End users are required to make a split-second security decision by manually performing the email filtering that Google ignores. Proofpoint performs the security decision and alleviates this burden from end-users.

Ability to defend against outbound threats
Inbound threats aren’t the only type of email threats facing enterprises. Enterprises also have to guard against outbound spam from internal, malware-infected systems. They also need to guard against email that leaks confidential data, such as customer records, intellectual property, and confidential data (such as healthcare records) that is protected by industry regulations.
Since Google acquired Postini in 2007, Google has not made any improvements to the core Postini anti-spam service. Despite the variety and sophistication of new attacks, such as phishing, Google still characterizes all threats and spam as Bulk Mail, which it divides into four categories:

- Sexually Explicit ("sexually-oriented messages")
- Get Rich Quick ("money-making offers")
- Special Offers ("too-good-to-be-true offers")
- Racially Insensitive ("hate-oriented topics")

For each category, administrators can select a level of enforcement from completely lenient (turning filtering for that category off) to aggressive.

This coarse handling of incoming email turns out to be dangerous. The Google solutions mixes bulk email such as legitimate newsletters with spam, such as ads, and threats, such as phishing attacks. To sort the good email from the bad, users end up sorting through their Quarantine Summaries and their Junk Folders daily, making split-second decision about which messages to open. A phishing attack with a legitimate-sounding subject line is likely to be pass muster with end users and be opened. The anti-spam defenses themselves make no critical judgment about phishing and pass this increasingly critical screening work and security decision off to end users themselves.

Proofpoint Enterprise, in contrast, automatically detects phishing messages and quarantines them in a folder accessible only to email administrators. If administrators choose, users can still have the ability to review other, less malicious forms of spam in quarantine folders, such as bulk email and email with adult content. (In the Proofpoint solution, all quarantine workflows are configurable by the administrators.)

![Diagram comparing end user access to threats within their quarantine.](image)

The recent security breach at RSA happened because an end user released a dangerous message from their Junk Folder, and then clicked on a Microsoft Excel attachment titled “2011 Recruitment plan.” The breach became serious enough that some part of the proprietary security technology behind RSA’s SecurID keyfobs may have been compromised.

(For more information about how Proofpoint granularly detects spam and threats, including phishing attacks, see the white paper Proofpoint MLX: Machine Learning to Beat Spam Today and Tomorrow.)

Question to ask Google: How does your filtering technology handle targeted attacks, such as phishing? Are you comfortable putting the security decision in the hands of end-users?

**Technical Strengths: Defenses Against Targeted Attacks, Traditional Attacks and Outbound Threats**

Varied threats require varied defenses, whether the threat is a new inbound threat, a traditional inbound threat, or a bi-directional threat. Proofpoint Enterprise offers a number of features that are not available
from Google. As the matrix below shows, Proofpoint Enterprise is a more complete email security and compliance platform with better defenses against new, highly targeted attacks, traditional spam and virus attacks, and other types of inbound and outbound threats. Proofpoint also supports better administrative and self-service tools, as well as comprehensive SLAs to ensure industry-leading effectiveness.

<table>
<thead>
<tr>
<th>Technical Comparison between Google Message Security and Proofpoint Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Defenses Against Targeted Attacks (Phishing)</strong></td>
</tr>
<tr>
<td>Granular and configurable policies for phishing messages</td>
</tr>
<tr>
<td>Separate quarantine for phishing messages</td>
</tr>
<tr>
<td>Real-time notification and alerting of phishing messages</td>
</tr>
<tr>
<td>Automated delivery of reports for phishing messages</td>
</tr>
<tr>
<td><strong>Defenses Against Traditional Threats (Spam and Virus)</strong></td>
</tr>
<tr>
<td>Separate policies for spam, virus, bulk, and adult</td>
</tr>
<tr>
<td>Separate quarantine for spam, virus, bulk, and adult</td>
</tr>
<tr>
<td>99% spam effectiveness and 1:350,000 false positive SLA</td>
</tr>
<tr>
<td>100% anti-virus SLA</td>
</tr>
<tr>
<td>Reputation-based spam detection</td>
</tr>
<tr>
<td>Email connection throttling and termination</td>
</tr>
<tr>
<td>Machine learning technology for accurate content analysis</td>
</tr>
<tr>
<td>Zero-Hour Anti-Virus detection for zero-day protection</td>
</tr>
<tr>
<td><strong>Defenses Against Other Threats</strong></td>
</tr>
<tr>
<td>Outbound spam detection</td>
</tr>
<tr>
<td>Policy-based encryption</td>
</tr>
<tr>
<td>Content filtering within Office 2007, Office 2010, and PDF attachments</td>
</tr>
<tr>
<td>Pre-configured compliance policies for SSNs and all CCs</td>
</tr>
<tr>
<td>Pre-configured compliance policies for HIPAA, GLBA, PCI</td>
</tr>
<tr>
<td>Smart Identifiers – algorithmic checks of structured data</td>
</tr>
<tr>
<td>Managed Dictionaries – pre-defined and updated libraries</td>
</tr>
<tr>
<td>Advanced proximity and correlation analysis</td>
</tr>
<tr>
<td>Content rules based on regular expressions</td>
</tr>
<tr>
<td>Document fingerprinting for protecting digital assets</td>
</tr>
<tr>
<td>Flexible encrypted message delivery (including mobile devices)</td>
</tr>
<tr>
<td>End-user triggered encryption for sensitive data</td>
</tr>
<tr>
<td>Per-message encryption keys</td>
</tr>
<tr>
<td>DLP incident dashboard for administrative remediation</td>
</tr>
<tr>
<td><strong>Management and Reporting</strong></td>
</tr>
<tr>
<td>Zero-hour message tracing, with ability to find phishing messages</td>
</tr>
<tr>
<td>Zero-day reporting, with summary of phishing messages</td>
</tr>
<tr>
<td>Automated publishing, scheduling, and email delivery of reports</td>
</tr>
<tr>
<td>DLP Dashboard – consolidated view of compliance activity</td>
</tr>
<tr>
<td><strong>End User Controls</strong></td>
</tr>
<tr>
<td>Self-remediation for outbound spam and DLP violations</td>
</tr>
<tr>
<td>End-user revocation controls for encrypted messages</td>
</tr>
<tr>
<td>Streamlined reporting and auditing of spam messages</td>
</tr>
<tr>
<td><strong>Deployment Options</strong></td>
</tr>
<tr>
<td>Public cloud</td>
</tr>
<tr>
<td>Hybrid deployment options</td>
</tr>
<tr>
<td>Dedicated instances for segregation of data and downtime</td>
</tr>
</tbody>
</table>
Tools and Organizational Readiness for Responding to Attacks

**Bottom Line:** Google lacks the expertise and tools to investigate threats such as phishing.

Email attacks never stop. Spammers and hackers have declared war on governments and the world’s largest corporations, healthcare organizations, and financial institutions. Their primary attack vector is email. Enterprises must be prepared to withstand these attacks.

Every enterprise should have a preparedness checklist or action plan in place for responding to attacks and minimizing their damage. The action plan should identify who to contact for technical support and which tools to use to investigate attacks and phishing messages in real time. The plan should also include historical reports of past attacks to help administrators analyze new phishing attacks as quickly as possible. Administrators should also have the flexibility to tune or customize the phishing policy depending on the threat level. For example, enterprises might want their email security solution to take different actions based on the probability that a message constitutes an attack (e.g. delete obvious phish, quarantine and review probable phish).

As the next section will make clear, Google Postini services fall short in these key areas. Google leaves email administrators and their enterprises without the tools they need to mount the most effective defenses when they’re under attack.

**Comparing Email and Technical Support Expertise**

**Bottom Line:** Email security vendors must be experts in email security and attack patterns in order to help enterprises under attack. Google falls short in this area.

When an attack occurs, whether the attack is directed at one’s own organization or another organization in the same industry, the first step in any corporate action plan should be to engage the enterprise’s security vendor for assistance.

In the case of Google, this typically means relying on self-service tools such as public forums and FAQs—not a satisfactory response for most organizations during an emergency. Reaching a live support engineer at Google won’t necessarily make things better. Former Google customers, along with numerous posts on their forums, report having encountered Google support engineers with only limited email and product expertise. These customers also report that the quality of Google’s support services has declined over time. This isn’t surprising, since Google acquired Postini four years ago, and many of the original engineers have been reassigned or have left the company. Today, email security and compliance accounts for less than 1% of Google’s total revenue. As Google’s CEO Larry Page recently pointed out in an earnings call, Google is focused on advertising, consumer applications, and new products such as Google+, not enterprise IT. 15

Proofpoint has been focused on email security since the company was founded in 2001. Recognizing that email is the most common vector for IT security attacks, Proofpoint ensures that its support engineers, product engineers, and threat analysts are ready to help customers who come under attack or who require any kind of help with security planning. Third-party organizations and industry analysts have praised Proofpoint’s support services for their knowledge and responsiveness.

*Question to ask Google: Who do I telephone for help me when my company is under attack? What is your SLA for support responsiveness?*

**Comparing Real-time Analysis Tools**

**Bottom Line:** Google is missing zero-hour message tracing and zero-day reporting so it cannot help administrators and security officers investigate attacks when they occur. In contrast, Proofpoint provides detailed real-time reporting.

Self-service tools can be used by security officers and email administrators to investigate attacks as they occur or to show management the value and effectiveness of the security and compliance solution. However, some of Google’s largest customers are reporting that the self-service tools included with the Google Postini service are extremely deficient, and do not provide real-time information that is useful to their customers when they need it most, such as during an attack.

Message tracing, sometimes referred to as log searching, is a tool email administrators use to track the messages that flow through an email security service. Google’s message tracing tool, called “Message Log Search data is available within approximately 3 hours of message processing (sent or delivered through the message security service)...” – Text from Google Message Security Administration Guide
Report data is based on data from the previous day. The report shown is the latest report available. Generally reports for the previous day are available around noon (or earlier) Pacific Time the next day. The exact time of availability fluctuates with quantity of traffic processed.

- Text from Google Message Security Administration Guide

Proofpoint supports real-time investigation into attacks and real-time reporting. Proofpoint’s Smart Search functionality consolidates logs as they pass through the service, so that SaaS subscribers have the immediate reporting typically found only in on-premises solutions. Proofpoint also enables administrators to publish reports each morning that show the attack patterns of the previous day; these daily reports enable administrators to fine-tune defenses and plan effectively for the future.

Question to ask Google: How will I know when we are being targeted by phishing attack? How can I investigate this in real-time?

Comparing Historical Forensics Tools

Bottom Line: Google lacks a specific report for phishing messages and is unable to streamline delivery of reports, so security officers are left unaware of the danger or threat level to their organization.

Google also lacks tools to perform historical forensics, such as publishing a report on the number of phishing messages during a specific period of time. Administrators are not able to run historical reports that will help determine or assess the risk of an attack, or if phishing attacks have been ongoing over a long period of time.

For example, if another company within in the same industry has announced that they have been breached and that the attack has been occurring for the last month (such as the breach at Epsilon), an enterprise will want to assess its own risk level. A natural first step would be to examine the types of attacks that have been recently detected. Not counting Blatant Spam, a report from Google will show 98% of threats as “Bulk Mail.” It won’t distinguish phishing attacks from other types of spam, leaving administrators with no visibility into the precise types of attacks being waged against their infrastructure.

Google Report: “Inbound Spam by Filter Name (Inbound) – From 08-01-2011 to 09-11-2011 (42 Days)”

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Spam</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special Offers</td>
<td>0</td>
</tr>
<tr>
<td>Bulk Mail</td>
<td>2,931,012</td>
</tr>
<tr>
<td>Get Rich Quick</td>
<td>0</td>
</tr>
<tr>
<td>Sexually Explicit</td>
<td>5,409</td>
</tr>
<tr>
<td>Blocked Senders</td>
<td>42,897</td>
</tr>
<tr>
<td>Blocked Servers</td>
<td>2,452</td>
</tr>
<tr>
<td>Racially Insensitive</td>
<td>0</td>
</tr>
<tr>
<td>Blatant Spam Blocked</td>
<td>6,398,793</td>
</tr>
<tr>
<td>Grand Total</td>
<td>9,380,563</td>
</tr>
</tbody>
</table>

Figure 3: Google’s spam filter report does not show the number of phishing messages.

In contrast, Proofpoint provides tools for organizations to view the number of phishing messages captured by the service, whether it is over the last month or the last 24 hours. Proofpoint also supports automated reporting, so administrators are able to schedule or publish report deliver and view the reports on a daily basis within their email inbox.

Question to ask Google: Can I receive an automated report for email-borne threats?

Securing Outbound Communications: Blocking Spam and Preventing Data Leaks

Bottom Line: Google has limited features that address outbound threats, whether it is spam or leakage of confidential data.

Email security and compliance services should be able to address both inbound threats (such as phishing) and outbound threats (such as spam or leakage of confidential data). They should also offer flexible de-
Employment options so that customers have the option to deploy outbound threat protection closer to their network if they so choose.

**Comparing Protection against Outbound Spam**

*Bottom Line: Failure to accurately detect outbound spam will ruin your organization's brand and could stop email delivery of legitimate email.*

Outbound spam—spam sent inadvertently by an enterprise's employees, spam sent from compromised systems within the enterprise, or spam sent from compromised accounts at universities—can seriously damage a company or university reputation. Once email servers across the Internet identify the organization as a source of spam, they may block or drop legitimate email from the organization, disrupting business communications and cutting the organization off from its customers and partners.

Up until 2011, Google did not support outbound spam detection. Google recently provided an update to support outbound spam detection, but does not allow administrators to configure the outbound spam-filtering settings. This inflexibility could end up disrupting legitimate business communications, as Google's aggressive Bulk Mail filters may block business communications to an enterprise's customers or partners. Google also does not support proper self-remediation tools for end users, so end-users are forced to call on IT to troubleshoot issues with outbound mail that has been flagged as spam.

Proofpoint does detect outbound spam. Applying its robust, patent-pending machine-learning technology that evaluates hundreds of thousands of message attributes, Proofpoint several years ago became the first vendor that was able to accurately detect outbound spam. Proofpoint's outbound spam detection was a key reason why one of the largest publishers in the United States and some of the largest universities have switched from Google to Proofpoint. In 2011, Proofpoint also added Smart Send, which provides users with the ability to self-remEDIATE outbound messages that have been flagged as spam or possibly violating compliance policies. This functionality streamlines business communications and takes the burden off IT staff to investigate email delivery issues.

**Comparing Protection of Confidential Information (Inbound and Outbound)**

*Bottom Line: Limited compliance policies will leave your organization at risk of data leakage that result in fines, penalties, and a damaged brand.*

To ensure compliance with industry regulations such as HIPAA and PCI-DSS, and to protect against data leaks that transmit confidential data to unauthorized parties, email security solutions should include advanced policies for accurately detecting and protecting confidential data. The next sections examine the effectiveness of Google's compliance policies and the limitations associated when encryption is an OEM from a third party and then describes the benefits of native encryption technology.

Google Postini Services come pre-configured with only two pre-built compliance rules, and Google offers email encryption only through an OEM relationship. Google's two basic compliance rules also have surprising limitations that can leave customers vulnerable to data leakage and fines. It is unclear whether these rules are actively maintained by Google. What is clear, however, is that these rules were introduced in November of 2007 - and since then, there have been no other updates or additions to the policies that are provided by Google.

Google customers who fail to update and maintain these policies leave themselves vulnerable to data leaks and regulatory fines. For example, the Social Security Administration changed its SSN issuance rules in July 2011, but Google's Social Security Numbers compliance policies do not support the new SSN formats. Google customers may inadvertently leak data with new SSNs if they rely on Google's default policies.

Google's other compliance policy for credit card numbers also has a severe limitation that can result in data leakage, as the policy cannot detect 15-digit account numbers, such as those used by American Express or Diner's Club. These credit cards are common in industries such as finance, retail, and hospitality. Google's credit card policy also does not perform the Luhn algorithm check, so is prone to high false positive rates.

Unlike Google Postini Services, Proofpoint Enterprise offers advanced social security and credit card policies, its policies are more up-to-date, supports the latest SSN formats, supports 15-digit account numbers and performs the Luhn algorithm check. Proofpoint Enterprise also comes pre-configured with more advanced policies that support regulatory compliance, such as a pre-configured HIPAA policy using medical dictionaries and medical record number lexicons. Proofpoint's policies combine Smart Identifiers and Managed Dictionaries with proximity detection to provide the most accurate identification of messages that violate compliance policies.

Google's limited compliance policies give email administrators and compliance officers a false sense of security, because confidential and private data can leave enterprise networks undetected. To make things
Content Manager does not scan attachments that are:
- ZIP or other types of compressed files
- Microsoft 2007 Office documents
- Over 100 MB
- PDF files

-worse, there are also other limitations to Google’s filtering technology that can result in data leakage, as we’ll see below.

**Question to ask Google: How can my organization prevent confidential data from leaving my network if I am required to create policies for regulations, such as HIPAA or PCI-DSS?**

**Comparing Filtering Of Attachments**

**Bottom Line**: Limited attachment filtering will leave your organization at risk of data leakage that result in fines, penalties, and a damaged brand.

Google’s content-filtering technology, called “Content Manager,” is used for both outbound and inbound emails for compliance. Unfortunately, it’s outdated. The technology supports only cursory scanning of the attachments most commonly used by businesses and end users. Even now, according to Google’s online help pages, Content Manager filters only Office 2003 files, not Microsoft Office 2007, Microsoft Office 2010, compressed files, or PDF files, even though these files are ubiquitous in business today. Because these files are ignored, enterprise compliance policies end up being only partially enforced. In fact, Google’s content manager policies trigger only when rules match the text included in an email message. They don’t trigger when sensitive data, such as social security numbers or credit card numbers (or keywords from other manually created content rules), appears in attachments. In an age of increasing regulation, these glaring gaps in content-filtering leave enterprises vulnerable to compliance violations, costly penalties, and lost business.

Proofpoint’s content-filtering provides much more thorough coverage than Google does, detecting keywords in a broad range of attachments and minimizing the risk of compliance violations. Proofpoint supports scanning and filtering of document types that Google ignores, including Office 2007, Office 2010, compressed files, and Adobe PDF files. Enterprises can be confident that Proofpoint Enterprise is monitoring and protecting all their email communications, not just their communications that involve a subset of file types available in 2004.

**Question to ask Google: How can my organization prevent confidential data from leaving my network if they are contained within a Microsoft Office 2007 document?**

**Comparing Encryption Technology**

**Bottom Line**: Native and tightly integrated technology for email encryption simplifies management and lowers total cost of ownership.

Email encryption solutions can protect sensitive and confidential data during transmission and at rest. Common examples include encrypting a doctor’s correspondence with a patient or a business partner, or a loan officer’s correspondence with a client or business. Email encryption and decryption should be quick and easy regardless of the device used, whether it is a desktop, a laptop, or even a mobile device.

Google uses encryption technology from Zix, so their email security and compliance solution is a separate solution than their encryption solution, with two separate interfaces. This creates challenges for email administrators when they try to configure or troubleshoot email encryption. For example, in order for an administrator to track the status of an encrypted message, he or she would first need to wait three hours before using Google’s Log Search functionality. Then they would need to log into a separate interface provided by Zix to further troubleshoot the message. Quite possibly they would need to contact two different support organizations.

Proofpoint’s encryption technology is tightly integrated with Proofpoint Enterprise and enables end-users by providing one-click access to encrypted emails from any mobile device. Compliance officers have access to a compliance dashboard that provides a view of activity and sensitive information leaving through email. Administrators also have access to tools on a single user interface that can be easily used to search for and troubleshoot encrypted emails from a single interface, saving time and money.

**Question to ask Google: How much control do you have over the technology used by your encryption services?**
Summary: Google vs. Proofpoint Scorecard

The table below summarizes the capabilities of Google's Message Security services and Proofpoint Enterprise according to the security categories outlined earlier in this paper.

<table>
<thead>
<tr>
<th>Security Requirement</th>
<th>Google</th>
<th>Proofpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adequate defenses against attacks</td>
<td>Unique handling of targeted phishing attacks</td>
<td>•</td>
</tr>
<tr>
<td>Flexible, policy-based responses to attacks</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Ability to respond to an attack</td>
<td>Expertise in enterprise email security and technical support</td>
<td>•</td>
</tr>
<tr>
<td>Tools for real-time analysis and historical forensics</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Effective protection from other threats</td>
<td>Configurable protection for outbound spam, with end-user remediation</td>
<td>•</td>
</tr>
<tr>
<td>Protection of confidential data (inbound and outbound)</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>

* Ability to defend against a targeted blended threat, including phishing attacks
  Google puts end users on the front line of defenses against phishing attacks. End users, rather than automated defenses, are expected to make the security decision and distinguish between malicious phishing messages and legitimate email. Proofpoint Enterprise applies 24/7 defense monitoring and machine-learning to detect and stop all kinds of email-borne. Proofpoint gives administrators more fine-grained controls over email security, while reducing their security risks and workloads.

* Ability to respond to an attack
  Google does not have the necessary support coverage or investigative tools to aid their customers if and when they are attacked. Without adequate zero-hour or zero-day tools to investigate attacks, email administrators are not able to investigate attacks in real-time, such as when they are notified that companies in their sector have been breached or targeted. Proofpoint gives administrators and security teams access to real-time and historical reporting, along with fine-grained policy controls for fine-tuning responses to threats and possible threats. Proofpoint support teams and threat analysts are experts in their fields and always just a phone call away from Proofpoint customers.

* Ability to defend against outbound threats
  Google does provide configurable protection for outbound spam, and does not include end-user remediation tools to ensure business communications. Google also does not provide adequate protection against the outbound leakage of confidential data. In contrast, Proofpoint provides leading-edge DLP capabilities that enable enterprises to guard their confidential data and their reputations.

CONCLUSION

More than five years ago, Postini was one of the first cloud-based email security platforms. After the acquisition by Google—a company focused on advertising and consumers more than enterprise software and security—product innovation has come to a halt, leaving Google customers vulnerable to targeted attacks and data leakage. It seems unlikely that Google can turn things around, given that they are starting to integrate the features from Postini onto the Google Apps infrastructure. Momentum has been lost, leaving users and corporate data vulnerable to spear-phishing and other new forms of email-borne attacks. Not surprisingly, many customers are seeking alternatives.

Having grown disillusioned with Google Postini services, some of the nation’s largest corporations are switching to Proofpoint Enterprise to meet their email security and compliance requirements. Since it was founded in 2002, Proofpoint has remained focused on email security and compliance. Unlike Google, Proofpoint continues to innovate, introducing new features and products, especially around threat detection of targeted attacks (such as phishing and spear-phishing), email security and compliance, and email encryption. Proofpoint’s roster of major enterprise customers—which includes industry leaders in finance, healthcare, manufacturing, and retail, as well as major government agencies—testifies to the success and viability of Proofpoint’s technology and services.
ABOUT PROOFPOINT

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint’s dedication, expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint’s enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging. Learn more at www.proofpoint.com.

1 http://www.theregister.co.uk/2011/02/17/canada_cyber_espionage/
3 http://www.pcwar.com/article/2/2872/2383080.00.asp
6 http://news.cnet.com/8301-27080_3-20051796-245.html
8 http://www.cio.com/article/885763/Second_DOD_Lab_is_Likely_Victim_of_Spear_Phishing_Attack
9 Link: http://www.net-security.org/keeworld.php?id=10567
13 Article from http://blogs.rsa.com/ruvee/anatomy-of-an-attack/ that states “The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file.”
17 http://www.google.com/it/itpress/presse/20071113_postini.html
Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint’s expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint’s enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.