Why Cloud-Based Security and Archiving Make Sense

An Osterman Research White Paper

Published March 2010

SPONSORED BY

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com • www.ostermanresearch.com

Why You Should Read This White Paper

Cloud computing is one of the most significant trends in IT today. Organizations of all sizes are evaluating various cloud computing solutions that can improve their performance. Increased productivity, lower cost, better security and reliability are all benefits that can be achieved with cloud computing solutions.

Coincidentally, IT organizations are working to improve email security and add compliance and e-discovery capabilities. Spam and malware are bad and are getting worse and the risk and potential costs associated with e-discovery are increasing. As a result, organizations need a better way to solve these problems. Cloud-based email protection and archiving can do just that.

SOME BACKGROUND

Email is the lifeblood of virtually any organization that uses it: users spend an average of 152 minutes on a typical workday using email (more than attending in-person meetings and talking on the phone combined). They send and receive more than 120 emails each day, and the majority of the content they need is tied up in email[1].

In addition to the quite serious impositions on storage and bandwidth imposed by ever-increasing volumes of spam, there are the much more serious threats that can expose corporate data to unauthorized parties, resulting in substantial financial losses, violations of the law, loss of reputation, and other increasingly serious consequences. Further, because email contains a growing proportion of corporate business records and other important content, organizations of all sizes must preserve this content through the deployment of appropriate archiving technologies.

The cloud model can:
- be less expensive
- offer more predictable costs
- be more reliable
- offer better threat detection

While security and archiving are absolutely necessary, they are also quite expensive to deploy and maintain. On-premise security and archiving systems themselves can be expensive to deploy, but they are generally much more expensive to maintain using in-house IT staff. Further, IT staff that are responsible for maintaining these systems are not available to manage other systems that can enable a strategic advantage over their competitors – particularly important during periods of economic downturn.

ENTER THE CLOUD MODEL

Organizations of all sizes are considering the cloud paradigm as an option for managing their security and archiving capabilities. The cloud model can be much less expensive than its on-premise alternative and provide more predictable costs of ownership. Further, organizations that use the right cloud-based solution can achieve better reliability, better threat detection, and more robust archiving capabilities. Organizations

[1] Source: Various Osterman Research surveys

that manage both security and archiving in a coordinated fashion can realize even more benefits, such as easier policy management and more efficient deployment of future services.

ABOUT THIS WHITE PAPER

This white paper, sponsored by Google, discusses the critical and growing requirements for better email security and email archiving, and it illustrates the benefits of the cloud approach to manage both. Osterman Research developed a cost model specifically for this white paper that compares the five-year cost of ownership for both on-premise and cloud-based security and archiving capabilities. Cost data from the model is presented in this document.

Security is Getting Tougher to Manage

THREATS ARE BECOMING MORE NUMEROUS

The threats facing organizations that operate on-premise email systems, as well as the users who have become reliant on this most-important communication and file-transport mechanism, are bad, and getting worse. Consider:

- At least 75% of all email traversing the Internet is spam. On weekends, when legitimate email traffic typically drops, spam can represent as much as 95% of all email.

- Spam volume continues to grow. SpamCop reports that immediately after McColo was taken offline they received roughly 10 spam messages per second, but as of mid-May 2009 that figure was roughly 40 messages per second[2].

- Malware represents only about 0.1% of all email traffic on any given day, but even a small organization will receive several viruses, worms, Trojan horses or other threats each day. Imagine one threat that makes it through: infected PCs will need to be isolated, hard drives may have to be reformatted, IT will called off other tasks to attend to the emergency, users will wait for their machine to be reimaged and have data restored - or even lose data.

  Worse, however, is malware – such as a keystroke logger – that remains undetected for weeks or months and enables criminals to steal hundreds of thousands or millions of dollars before it is detected. The Federal Deposit Insurance Corporation estimated that in the third quarter of 2009 alone, online banking fraud cost more than $120 million[3].

- Phishing attempts – including their more targeted variants, spearfishing and whaling – are becoming more numerous.

[2] http://spamcop.net/spamgraph.shtml?spamyear
[3] Source: *Computerworld*, March 8, 2010

- Social engineering techniques are fooling larger numbers of users over time into clicking on links or opening attachments that can wreak havoc on corporate networks. The Koobface worm on Facebook and the Mikeyy work on Twitter are just the tip of the iceberg with regard to social networking threats.

- Blended content (which combines email and Web threats) is becoming more numerous.

- Spyware is becoming stealthier and is increasingly likely to give criminals access to sensitive and confidential information.

In short, spam, malware, spyware and a variety of other threats are bombarding corporate email systems and are increasing in number and sophistication.

THREAT MANAGEMENT IS BECOMING MORE DIFFICULT

Despite the fact that virtually all organizations have deployed anti-virus and anti-spam systems, things are not getting better for many firms: a large proportion of organizations are experiencing degrading spam and malware capture rates over time and nearly two in five organizations report that malware has infiltrated the corporate network through email at some point in the recent past.

Not only are threats become more frequent, stealthier and more sophisticated, detection and remediation are becoming more difficult to manage. For example, with spam volumes doubling roughly every year, organizations that manage an on-premise security infrastructure must either continue to add more servers and software or more appliances to their infrastructure to keep up with growing volumes of spam. Alternatively, they must greatly overspecify these infrastructure elements when deploying them and let spam volumes catch up with the overcapacity they have deployed. The costs associated with this can be multiplied for organizations with multiple Internet ingress/egress points where each one requires an appliance or other filtering mechanism. In either case, organizations incur additional expenses over the lifecycle of a security system, or they spend too much up front.

Add to this the significant impact that spam and malware have on storage and bandwidth. Consider these examples:

- If we assume that 75% of incoming email is spam, the average user receives 100 emails per day (based on Osterman Research surveys), the average spam is 15Kb, and spam is stored in a quarantine for 30 days, then an organization of 1,000 users will be storing roughly 33 gigabytes of spam at any given time. However, this number can be dramatically higher during spam storms and, even in the absence of these spikes, will continue to grow at a rapid pace over time.

- Bandwidth is also consumed by spam, requiring periodic upgrades to bandwidth or degraded network performance as spam volumes increase. For example, Commtouch estimated that peaks in image spam increased bandwidth requirements by 70% compared to non-peak levels.

Malware is also becoming a much more difficult and thorny issue, particularly with the advent of various threats like Conflicker, which can infect millions of computers in a very short period of time. "Scareware," deploying pop-ups or other gimmicks to intimidate recipients into purchasing an often bogus malware-remediation solution, is also on the rise. All of these threats require continual updates of on-premise security systems, IT staff time that must be devoted to managing the security infrastructure, and performing often unplanned and unexpected capacity upgrades.

THE FUTURE OF THE THREAT LANDSCAPE IS NOT A PRETTY ONE

If the past is any indication of what we can expect for the future of spam and malware, new threats will not be easy to address. Spammers and malware developers are well funded and are developing more sophisticated attack strategies, and they will attack on a larger number of fronts. For example:

- The well-publicized takedown of McColo as a major spam source in November 2008 significantly reduced spam volumes – temporarily. Within a few months, spammers had rebuilt their capacity through the expansion of existing botnets and development of new ones to get spam "production" back to its pre-takedown levels. This trend has accelerated since that time. After the ISP 3FN was taken off-line, spammers were able to recover to previous volumes in less than one month, and when Real Host was knocked out, only a few days were required before spammers were able to push spam volumes back to previous levels.

- Malware will be increasingly stealthy, focused more on intercepting confidential and sensitive information through threats like keystroke loggers. The reason for stealthier malware is simple: instead of simply damaging files, erasing disks, etc., new malware attempts to steal data over as long a period of time as possible – the harder malware is to detect, the longer it can remain in place and the greater value it has to those who put it in place.

- Threats will address a larger variety of endpoints, including not only the traditional venues of email clients and servers, but also mobile devices, VoIP systems, real-time communications platforms, SMS/text-messaging systems, social networking platforms, legitimate Web sites, and various Web 2.0 applications.

Despite the growth of threats directed toward the Web and Web 2.0 applications, email will continue to remain a primary threat vector for malware.

- Despite the growth of threats directed toward the Web and Web 2.0 applications, email will continue to remain a primary threat vector for malware.

- Spam volumes will continue to increase, driven in part by the growth in botnets and the relative success of anti-spam technologies that are driving spammers to deliver increasing quantities of content.

In short, we can expect a greater variety of threats aimed at more platforms that will be more difficult to detect and remediate. To manage these threats properly will require more IT resources, particularly for IT departments that choose to fight these threats with traditional, on-premise solutions.

Archiving is Becoming a Critical Best Practice

YOU NEED TO ARCHIVE

Along with the growing problem of spam and malware is the increasing need to archive email. Email archiving – which involves indexing incoming, outgoing and internal email communications, storing this content in an archival storage system and allowing it to be searched – is increasingly a best practice for organizations of all sizes. While many consider their nightly backup to be an "archive," backups and archives are not interchangeable, but instead serve different purposes:

- A nightly or other regular backup preserves a snapshot of the content available on an email server at any given time. Backups are important and clearly represent a best practice for any organization, but their purpose is to preserve email content in the event that a server fails and data needs to be restored. Backups are intended primarily as a short-term solution for the tactical purpose of restoring emails to a server.
- An archive, on the other hand, captures all email, not just what was housed on the server at a given point in time. Archives are much more strategic in nature and are intended to preserve information for a variety of purposes as discussed below. Archives do not preserve just a snapshot of the data available on a server, but instead preserve a continual stream of email content.

Further, it is important to note that email archiving is not simply for "regulated" industries, such as broker-dealers, hedge fund managers, or investment advisors. Instead, email archiving is a best practice for all organizations, regardless of the industry in which they operate or their size.

WHY SHOULD YOU ARCHIVE?

There are a variety of reasons that any organization should archive their email content, although some reasons will be more important than others depending on the size of the company or their industry focus. Among the reasons to archive email are:

- **E-discovery**
  Most discovery orders that require production of business records or other documents specify that email-borne content be part of the mix of information that is considered for discovery. An archiving system permits search and recovery of relevant business documents in a fraction of the time and for a small fraction of the cost that would be required if this content had to be recovered using backups alone.

  In many cases, the cost of just one e-discovery exercise using backup tapes would pay for the cost of an email archiving system many times over. For example, Intel

spent at least $3.3 million to process tapes containing emails as part of a discovery effort in its lawsuit with AMD.

- **Regulatory compliance**
  Some industries, such as financial services, healthcare or energy, are more regulated than others, and so must comply with a larger set of statutory requirements to preserve and produce business records. For example, the United States Securities and Exchange Commission (SEC) requires broker-dealers to preserve and produce communications with their clients, along with other business documents. Since a larger proportion of these communications are sent and stored in email systems, email archiving is a critical necessity for SEC-governed organizations.

- **Storage management**
  Because of increasing use of email and larger attachments, email stores are becoming bloated and less manageable over time. In fact, numerous Osterman Research surveys have demonstrated that growth in email storage is the leading problem cited by messaging-related decision makers. In fact, three out of five consider email storage growth to be a serious or very serious problem.

  An email archiving system can automatically migrate storage from email servers to archival systems, keeping server-based storage sizes manageable, while preserving the accessibility of email. By using email archiving as a storage management tool, backing up and restoring email servers is faster and more reliable, server performance is improved, and overall email system performance is enhanced.

- **Knowledge management**
  The majority of most computer users' information is somehow bound up in email. As a result, an email archiving system that preserves the information stored in emails will permit the organization to more effectively retain "corporate memory."

- **Self-service for end users**
  An email archiving system can also act as a self-service capability for end users to recover their own missing or deleted emails. Instead of requesting restoration of one or more emails from an IT staff person, individuals can access their own archive, search for the desired content, and restore it to their mailbox with no intervention from IT. Many IT departments simply do not have the manpower to respond to requests for recovery of missing or deleted emails – self-service access to an archive, therefore, can result in reduced help desk calls, higher user satisfaction, and greater productivity from employees who do not have to wait for emails to be recovered.

Corporate governance will be increasingly a front-of-mind issue for many decision makers in an era of growing government oversight in a variety of industries ranging from banking to auto manufacturing.

- **Disaster recovery and business continuity**
  An email archiving system can also be beneficial as part of a disaster recovery and business continuity system. In the event that a primary email system is disabled as the result of a natural disaster or other disruption, an archive can be used to populate a secondary email system to bring email back online – with a full set of data – in a short amount of time.

WHY EMAIL ARCHIVING IS CRITICAL (EVEN MORE SO DURING A RECESSION)

Email archiving will become more important in 2010 and beyond and should be on the short list of critical infrastructure enhancements for any organization. While many organizations are seeking to cut IT-related costs as a result of the current difficult economy, archiving should not be cut for two important reasons:

- Corporate governance will be increasingly a front-of-mind issue for many decision makers in an era of growing government oversight in a variety of industries ranging from banking to auto manufacturing. An email archiving system is a key component of any corporate governance system, allowing decision makers ready access to content that will be needed to support governance efforts.

- Many decision makers realize that they must preserve business records and make them readily accessible. Email archiving is the best way to accomplish this.

Leading cloud-based providers typically offer very high levels of threat detection and remediation owing to the fact that they can afford to deploy a carrier-grade infrastructure.

A December 2009 report funded by Osterman Research underscores the importance of email archiving, even in a difficult economy. The reports shows that 24% of the organizations surveyed actually plan to deploy email archiving for e-discovery purposes in 2010, and 28% plan to do so for email server data management.

Why You Should Switch to the Cloud Now

Cloud computing has been receiving increasing attention from analysts, press, vendors and others – and with good reason: cloud computing offers a number of important advantages compared to on-premise systems. While the cloud model is certainly not a panacea for all things computing, and while on-premise systems can deliver reasonable security and archiving capabilities, cloud-based systems generally provide many important advantages over an on-premise model.

LOWER OVERALL COSTS

As shown later in this white paper, cloud computing can provide a much lower total cost of ownership (TCO) for email security, email archiving and other email-related systems, often in excess of 80% compared to on-premise solutions. Since cloud-computing systems eliminate most of the need for in-house IT staff to manage on-premise infrastructure, and since cloud providers absorb the cost of infrastructure upgrades, the use of the cloud model typically results in lower overall IT expenditures compared to on-premise systems.

Related to the lower TCO usually provided through cloud-based computing is the fact that costs are shifted from capital expenditures to operating expenditures, resulting in lower up-front costs and, in some cases, significant tax advantages.

MORE PREDICTABLE COSTS

Cloud computing, by virtue of the typical flat rate pricing offered by most providers, results in much more predictability of IT-related costs. Whereas a sudden increase in the volume of spam, for example, can result in the immediate need for on-premise security systems to be upgraded, cloud providers absorb these unexpected changes, not their customers.

IT STAFF CAN BE FREED UP FOR OTHER INITIATIVES

Another important benefit of the cloud model for managing email-related capabilities is the fact that IT staff that used to manage on-premise infrastructure can now be freed up for other initiatives that will provide more value to the organization. For example, while email security and archiving are absolutely critical for any organization, managing them even extraordinarily well does not provide a competitive differentiator. However, if IT staff members' time could be freed up through the use of cloud-based services, that time could be put to use for initiatives and tasks that would provide more value, such as reducing technical support wait times, improving customer service, or making backend applications accessible to mobile workers.

VERY HIGH LEVELS OF DETECTION AND REMEDIATION

Leading cloud-based providers typically offer very high levels of threat detection and remediation owing to the fact that they can afford to deploy a carrier-grade infrastructure (redundant data centers, backup power sources, multiple communications links, very robust servers) – something that even large organizations often cannot afford to implement. This allows them to provide very high levels of security for their customers.

VERY HIGH RELIABILITY

Similarly, the infrastructure that leading cloud-based providers can deploy includes things that most organizations simply could not afford: multiple data centers equipped with multiple backup power sources, redundant telecommunications links, automatic failover systems, and the like. This results in levels of uptime that are typically higher than for on-premise infrastructure. Some cloud providers offer SLAs of 99.999% (about five minutes of downtime per year), which is very expensive to achieve with an in-house solution.

SECURITY AND PRIVACY CAN BE BETTER IN THE CLOUD

While many decision makers fear that the use of cloud-based providers will somehow compromise the security and privacy of data managed in the cloud, these fears have simply not been borne out by reality. Instead, leading cloud providers usually offer extraordinarily high levels of physical and logical data security, as well as robust security systems to protect their customers' data.

DEPLOYMENT IS USUALLY MUCH FASTER

Another important advantage of the cloud model is that capabilities like email security or email archiving can most often be deployed more rapidly than on-premise systems. Instead of evaluating, piloting and deploying new infrastructure elements, as is the case with an on-premise model, using the services of a cloud provider typically involves little more than changing a domain's MX records and making a few other configuration changes. Using a cloud-based provider, new capabilities can be brought online in as little as a few hours compared to days or weeks for many on-premise deployments.

POWER SAVINGS

Another important benefit provided by the cloud model is the significant power savings that can be realized. For example, a security appliance that consumes 450 watts of power, and assuming electricity cost of $0.12 per kilowatt-hour, will cost an organization $473 per year to operate. Add to this the cost of the cooling and floor space necessary to support the on-premise infrastructure and the cost of ownership can be substantially higher. In addition to reducing costs, the cloud model can contribute to "green" computing initiatives and help an organization meet targets for reduced overall power consumption per user.

MORE FLEXIBLE ACCESS OPTIONS

Many organizations, concerned about the growing number of venues through which security threats can infiltrate an organization, are prohibiting the use of many potential threat sources, including thumb drives, mobile devices, home computers, etc. While this does reduce the number of potential access points for threats, it also makes employees far less productive and can negatively impact the way the employees do their job. Since a cloud provider can eliminate threats before they ever reach the corporate network, there is far less chance that these otherwise risky endpoints could become infected, allowing decision makers greater freedom in allowing their use.

COST EXAMPLES

Osterman Research has developed a custom cost model specifically for this white paper that compares the cost of on-premise email security and email archiving with their cloud-based counterparts. The model was developed using the following:

- Data from secondary sources about the cost of on-premise systems designed to provide security and archiving functionality.

- Data from Osterman Research surveys researching the number of hours spent per week by IT staff on managing on-premise security infrastructure and archiving systems.

- Estimates of the number of emails received per user per day and the average size of these emails.

The calculations in the tables below used the following assumptions:

Basic Assumptions
- 500 users in Year 1 growing at 5% per year.
- The on-premise infrastructure is refreshed every three years.
- Redundant security and archiving infrastructure is employed, adding 20% to the labor cost for managing the on-premise infrastructure.
- The fully burdened, annual salary of each IT staff member is $80,000.
- Annual salary growth is 3%.

Security Assumptions
- Appliances from a leading provider are used in this analysis.
- Appliance cost = $3,999; annual maintenance, updates, etc. for three years = $5,098
- 19.0 IT person-hours per week are required to manage the on-premise infrastructure; 20.0 IT person-hours are required to deploy the appliances.

Archiving Assumptions
- Appliances from a leading provider are used in this analysis.
- Appliance cost = $8,999; annual maintenance, updates, etc. for three years = $11,348.
- A mean of 60 emails per day need to be retained, and the average size of each email is 50 kilobytes.
- Storage costs $10.00 per gigabyte in Year 1 and is dropping at 10% per year.
- 8.8 IT person-hours per week are required to manage the on-premise infrastructure; 60.0 IT person-hours are required to deploy the appliances.

Based on these assumptions, the cost for on-premise and cloud-based security and archiving are as shown in the following tables.

Comparison of On-Premise and Cloud-Based Email Security
Mid-Sized Organization

	Year 1	Year 2	Year 3	Year 4	Year 5	
Number of users	500	525	551	579	608	
ON-PREMISE						**TOTAL**
Security infrastructure costs	$18,194	$0	$0	$18,194	$0	**$36,388**
Security labor, deployment	$1,538	$0	$0	$1,681	$0	**$3,219**
Security labor, ongoing administration	$45,600	$46,968	$48,377	$49,828	$51,323	**$242,096**
TOTAL	**$65,332**	**$46,968**	**$48,377**	**$69,703**	**$51,323**	**$281,703**
GOOGLE						
Security fees for cloud services	$6,000	$6,300	$6,615	$6,946	$7,293	**$33,154**
Security labor, total	$2,308	$2,060	$2,122	$2,185	$2,251	**$10,926**
TOTAL	**$8,308**	**$8,360**	**$8,737**	**$9,131**	**$9,544**	**$44,080**
					TOTAL SAVINGS OVER ON-PREMISE	**84%**

Comparison of On-Premise and Cloud-Based Email Archiving
Mid-Sized Organization

	Year 1	Year 2	Year 3	Year 4	Year 5	
Number of users	500	525	551	579	608	
ON-PREMISE						**TOTAL**
Archiving infrastructure costs	$40,694	$0	$1,203	$42,204	$1,763	**$85,864**
Archiving labor, deployment	$4,615	$0	$0	$5,043	$0	**$9,658**
Archiving labor, ongoing administration	$21,120	$21,754	$22,406	$23,078	$23,771	**$112,129**
TOTAL	**$66,429**	**$21,754**	**$23,609**	**$70,325**	**$25,534**	**$207,651**
GOOGLE						
Archiving fees for cloud services	$16,500	$17,325	$18,191	$19,101	$20,056	**$91,173**
Archiving labor, total	$8,508	$8,446	$8,699	$8,960	$9,229	**$43,842**
TOTAL	**$25,008**	**$25,771**	**$26,890**	**$28,061**	**$29,285**	**$135,015**
					TOTAL SAVINGS OVER ON-PREMISE	**35%**

Summary of Costs
Mid-Sized Organization

ON-PREMISE						**TOTAL**
Total on-premise costs	$131,761	$68,722	$71,986	$140,028	$76,857	$489,354
Total Google costs	$33,316	$34,131	$35,627	$37,192	$38,829	$179,095
TOTAL SAVINGS	**$98,445**	**$34,591**	**$36,359**	**$102,836**	**$38,028**	**$310,259**
					TOTAL SAVINGS OVER ON-PREMISE	**63%**

Synergies From Managing Capabilities Together

Security and archiving are among the two most critical functions that an organization can deploy for its email infrastructure. It simply makes sense to manage both of them in a coordinated fashion for a variety of reasons:

- **Policy management is simpler**
  Email managers must manage security policies (e.g., what types of content is allowed to reach end users, what groups are allowed to view certain types of content, etc.), and they must manage archiving policies (e.g., what types of content must be archived, what data retention requirements are imposed for specific types of content, what users should have access to data, etc.). If security and archiving are managed through a single interface, policy management is simpler than if administrators must manage policies through two separate interfaces.

- **It is easier to provision new users**
  If a new user can be added to the system and provisioned through a single interface instead of two separate ones, administrators' jobs are made easier. Similarly, it is easier and more efficient to manage existing users when policies need to be updated, or if a user is assigned a new role and their profile must be updated.

- **More granular control is available**
  Management through a single interface can provide more granular control over policies than if multiple interfaces and systems must be managed.

- **Content is managed in one repository**
  Managing content in a single repository can make life easier for administrators than if two separate repositories must be managed.

- **Overall costs are lower**
  As when multiple products or functions are procured from a single vendor, there are synergies that can be realized if security and archiving are sourced and managed in a coordinated fashion, reducing the overall cost of managing the infrastructure.

- **Coordinated management can provide a better roadmap for future services**
  Finally, coordinated management can position an organization for easier and faster provisioning of future services as these become available. For example, a customer of security and archiving functions from a single vendor can implement an email encryption policy more easily than if the encryption policy must be implemented in one vendor's security system and then separately implemented in another vendor's archiving system.

About Google's Enterprise Cloud Computing Services

GOOGLE APPS PREMIER EDITION

Google Apps Premier Edition offers simple, powerful communication and collaboration tools for enterprises of any size in business, education, or government – all hosted by Google to streamline setup, minimize maintenance, and reduce IT costs. With Gmail (including Google email security, powered by Postini), Google Calendar, and integrated IM, users can stay connected and work together with ease, even in private domains.

Google Apps enables secure, real-time collaboration among workgroups of all sizes. With hosted documents – word processing, spreadsheets, and presentations – web-based video access, and easy site-building tools, Google makes information usable from any browser or smart phone, whenever and wherever users work. They can share files and collaborate in real-time, keeping versions organized and available wherever and whenever users work. SAML-based Single Sign-On (SSO) services integrate seamlessly with established security and authentication systems. Google Apps bring easy, secure productivity to any work team, without the need for additional hardware or software.

GOOGLE MESSAGE 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. Google Message Security is included with Google Apps Premier Edition and is also available stand alone to protect existing, on-premise email servers.

Leveraging a patented 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 as a cloud computing service, saving money and IT resources because there is no hardware or software to install and maintain.

Google Message Security can automatically enforce your email security policies. This 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.

GOOGLE MESSAGE DISCOVERY

Google Message Discovery, powered by Postini, goes beyond the functionality of our security offering to give you maximum control and flexibility over your electronic records archive, while meeting discovery, and compliance objectives.

Google Message Discovery is a secure, hosted email archiving service that allows you to cost-effectively protect and access archived email data. Google Message Discovery enables you to:

- Create a centralized and searchable email repository for your organization
- Quickly search across the archive to collect email for legal discovery
- Secure your email from spam, viruses, and other threats

Google Message Discovery is delivered as a cloud computing service model, so you don't have to worry about planning for current and future storage capacity needs – Google does it for you. By storing your messages in Google's secure data centers, you can ensure that messages will not be lost in the event of an onsite server failure. You can archive all mail without worrying whether you have enough disk space and eliminate storage quota headaches by allowing users to access historical mail. In addition, by offloading excessive mail from your existing servers, you can decrease backup windows and reduce recovery times.

With Google Message Discovery, access to all your archived messages is always at your fingertips. What's more, legal, human resources, and compliance staff does not need to rely on IT personnel to conduct searches and inquiries. Google's easy-to-use web-based interface lets anyone – even end users – manage and search the message archive according to policy and depending on specific roles and authorizations. And because Google Message Discovery saves all messages based on your defined retention policies, indexes them, and stores them in a centralized repository, you can quickly and easily pinpoint relevant messages, place them on litigation hold to disable message deletion, and share as needed with legal counsel, law enforcement officers, or regulatory officials.

Best of all, it's hosted by Google. So there's no hardware or software to download, install or maintain. Google Message Discovery improves litigation readiness, eases IT administration burdens, and lowers the total cost of ownership compared to software or appliance based solutions.

Google Message Discovery works together with Google Apps Premier Edition or with existing on-premise email servers.

Summary

Security and archiving are critical functions that all organizations, regardless of their size or the industries in which they operate, must deploy and manage. However, security is becoming more difficult to manage because of a growing variety of security threats, the increasing sophistication of these threats, and the enormous financing that spammers and malware developers have at their disposal. Archiving is also becoming more critical as government increases its oversight of organizations in a variety of industries, and as e-discovery becomes more common.

Therefore, organizations need to implement robust security and archiving capabilities but, in an era of shrinking IT budgets, they must do so as inexpensively as possible. Organizations of all sizes should seriously consider the use of cloud-based services for a variety of reasons:

- To improve their spam and malware capture rate
- To reduce their costs for security and archiving functions – as noted in the examples above, a mid-sized organization can reduce their security and archiving cost of ownership by 63% when using hosted services.
- A key component of the cost savings is significantly reduced labor requirements with the added benefit of making this IT staff time available for other projects.
- To make their costs more predictable
- To free IT staff for other tasks that will provide more strategic advantage

Enterprise cloud computing services from Google can help your organization realize these benefits.

For more information, please visit: www.google.com/a.