AberdeenGroup
A Harte-Hanks Company

Email Security in the Cloud: More Secure! Compliant! Less Expensive!

April 2010

Derek E. Brink, CISSP

Research Brief

Aberdeen Group
A Harte-Hanks Company

April 2010

Email Security in the Cloud: More Secure! Compliant! Less Expensive!

Drawing on the findings from multiple benchmark studies on best practices in email security and security software as a service, Aberdeen's analysis shows that **users of cloud-based email security had substantially better results** than users of on-premise email security implementations in the critical areas of security, compliance, reliability and cost.

Business Context: Much Ado about Cloud Computing

Cloud-based computing – including *Software as a Service*, *Platform as a Service*, and *Infrastructure as a Service* – is one of the hottest topics of conversation in IT for 2010. Unfortunately, the waves of marketing hype about the inexorable rush to the cloud inevitably leave the flotsam and jetsam of misinformation and market confusion in their wake. To help clarify any potential confusion about cloud-based computing terminology, for the purposes of this Research Brief Aberdeen uses the following high-level definitions:

- **Physical Servers** refers very generally to the traditional computer hardware, operating system, storage, networking and software services that together provide a computing platform for hosting an organization's applications and data.
- **Virtualization** (V12N) technologies break the traditional computing model of one physical server / one operating system / one application, by enabling the underutilized resources of a single physical machine to run multiple *virtual machines* – each of which in turn can run different operating systems and applications. In a fully virtualized computing environment, organizations can run their applications on a flexible pool of shared resources (networks, storage and hosts), which some companies refer to as a **Private Cloud**. Examples of leading server virtualization technologies include *VMware ESX*, *Microsoft Hyper-V*, *Citrix XenServer*, *Oracle VM Server*, and *Novell SLES*.
- **Infrastructure as a Service** (IaaS) provides a fully virtualized computing environment on which organizations can run their Internet-based applications, eliminating their need to install, operate and support their own private networks, storage and hosts. Example services include *Amazon Web Services EC2*, *Flexiant Flexiscale*, *GoGrid Cloud Hosting*, and *Rackspace Cloud*.
- **Platform as a Service** (PaaS) provides software services and application development interfaces, along with their underlying

Research Brief

Aberdeen's Research Briefs provide a deeper exploration of the principal findings derived from primary research, including key performance indicators, Best-in-Class insight, and vendor insight.

Fast Facts

Aberdeen's analysis shows that compared to companies using on premise email security solutions, users of cloud-based email security solutions had substantially better results:

√ 47% fewer incidents of spam / malware in the last year

√ 65% fewer audit deficiencies in the last year

√ 50% less security-related downtime in the last year

√ 11% lower total cost per end-user per year for email security

Definition

Following longstanding industry tradition, Aberdeen will sometimes refer to **virtualization** as *V12N* – as in the word formed by the letter V, followed by 12 additional letters, and ending with the letter N – just as **internationalization** is referred to as *I18N* and **localization** is referred to as *L10N*.

networks, storage and hosts, which organizations can use to develop, test and deploy their own Internet-based applications. Examples include *Google App Engine*, *Microsoft Windows Azure platform*, *Salesforce.com Force.com*, and *Zoho Creator*.

- **Software as a Service** (SaaS) provides one or more specific applications over the Internet, eliminating the need for organizations to install, operate and support these applications on their own private networks, storage and hosts. Examples include *Salesforce.com Salesforce CRM*, *Cisco WebEx*, and *Workday HCM*.

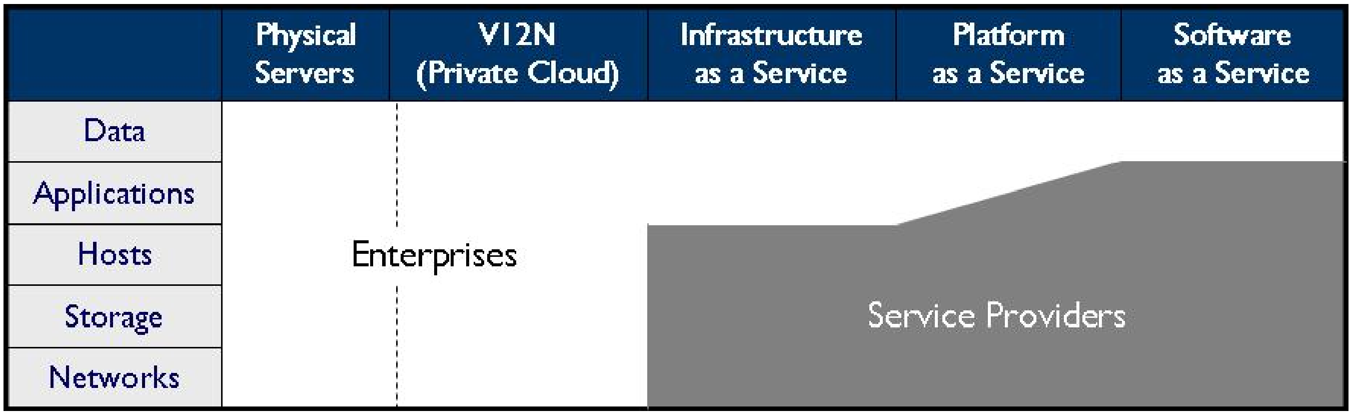
Web browsers are assumed as the ubiquitous *clients* in these cloud-based computing models. In addition to traditional endpoints, the typical enterprise is already teeming with network-connected smart phones, USB drives, and other mobile endpoint devices that are accessing corporate email, applications and data. Aberdeen's study on Going Mobile: Securing and Managing Mobile Endpoint Devices (January 2010) showed that Best-in-Class companies are more liberal than their counterparts in their formal support for mobile endpoint devices, and in doing so they are enabling their objectives of end-user convenience and productivity while sustaining the organization's requirements for security, compliance, and cost-effective management.

"The liberalization of end-user devices is unstoppable, particularly for knowledge workers … it's almost impossible to control what devices they use to access applications and data, especially email and web applications. As a matter of policy, we have formally standardized on Windows … but most of the cool people use Mac."

~ CEO, >$1B high tech firm

In Aberdeen's view, one straightforward way to differentiate the various levels of cloud-based computing is in consideration of the following question: who has ownership over the networks, storage, hosts, applications, and data – the enterprises, or the service providers?

Figure 1: Differentiating the Various Levels of Cloud-based Computing: Who Has Ownership of the Networks, Storage, Hosts, Applications and Data?



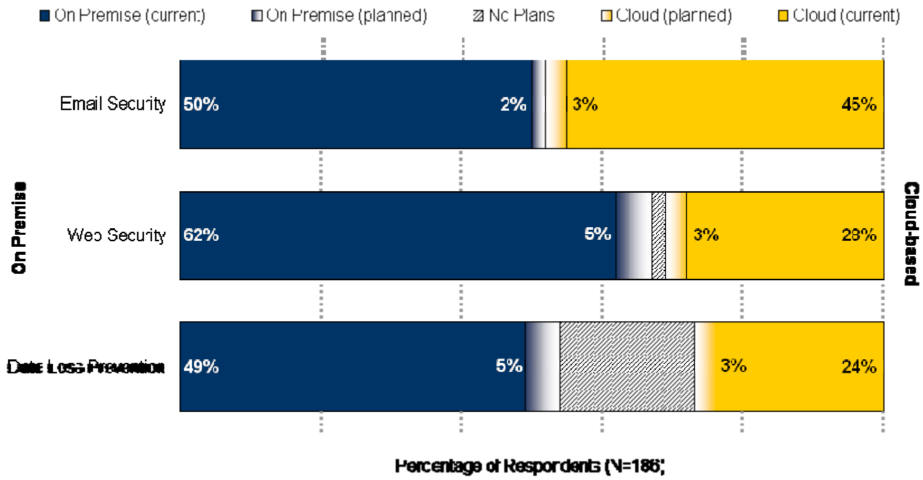
Source: Aberdeen Group, April 2010

As depicted in Figure 1, in all three of the "as a Service" models the service provider assumes ownership of the infrastructure for networks, storage and hosts. The service provider may also assume partial ownership (as in the PaaS model) or full ownership (as in the SaaS model) of the application infrastructure. But the enterprise always has ownership of its data, although in current cloud-based computing environments it no longer has direct *control* over its data. Concerns about assuring the confidentiality, integrity and reliability of sensitive data are in fact among the leading inhibitors to faster enterprise adoption of cloud-based computing. In a very positive sense, the marketing hype about cloud-based computing has elevated attention on IT Security as a critical enabler for the successful journey to cloud-based computing services, both public and private.

The #1 Cloud-based Security Service: Email Security

In light of the market hubbub on cloud-based computing, what practical examples of cloud-based security services can be found in Aberdeen's benchmark research? As identified in Aberdeen's June 2009 study on *Deploying IT Security: Keeping the Threats and Headaches Outside*, **email security is the number one use case for security software as a service**. Across all respondents, email security was very nearly split between *on premise* and *cloud-based* implementations, with indications of a net shift towards cloud-based implementations over the next 12 months (Figure 2). With respect to *web security* and *data loss prevention solutions*, Aberdeen's research showed that current implementations were more than 2-times more likely to be on premise than cloud-based.

Figure 2: Market Trends for On Premise vs. Cloud-based



Source: Aberdeen Group, April 2010

Given the snapshot of the market represented by the findings in Figure 2, it comes as no surprise that email security solution providers fall into four high-level categories:

- Those that offer only an on premise solution
- Those that offer only a cloud-based solution
- Those that offer a hybrid solution (e.g., an on premise appliance coupled with cloud-based intelligence)

"I don't know – and don't care – what or who is running my network and server infrastructure. But I do care about who's got access to my critical data."

~ CEO, >$1B high tech firm

Fast Facts

Average time respondents have been using email security services in the cloud: 4.1 years

Average contract length for cloud-based email security services: 2.3 years

Terms included in Service Level Agreement (SLA):

√ Service availability to end-users (uptime) 63%

√ Responsiveness to escalation of an event 53%

√ Time-to-acknowledgment of escalation 53%

√ End-user satisfaction 37%

√ Qualifications of service provider employees 33%

√ Compliance with regulations or standards 21%

Average percentage of SLA terms met in the last 12 months: 95%

- Those that offer their customers the flexibility and choice of both

Each camp has its zealous and eloquent proponents, but history and experience tells us that one model is unlikely to prevail to the exclusion of all others. On the contrary, each buyer will make their selection for email security services based on their own unique sense of balance between factors such as security, compliance, total cost, and degree of ownership and control.

In-depth comparisons of specific email security technologies is beyond the scope of Aberdeen's benchmarking style of research, but technical capabilities that are strongly correlated with the achievement of Best-in-Class results in secure email include the following:

- **Zero hour protection.** Leading solution providers work continuously to identify and protect against new vulnerabilities and threats, and organizations that update their email protection on an *ad hoc* or scheduled basis rather than immediately when new protections become available leave themselves needlessly exposed to data loss and downtime. At the same time, companies need to be diligent about keeping up with all previously known vulnerabilities, as attackers will always look for ways to take advantage of unpatched or misconfigured systems. Whether enterprises choose to manage these activities themselves or rely on the dedicated services of their cloud-based solution provider, they need to assess, prioritize and remediate email-related vulnerabilities "at the speed of crime."
- **Reputation and authentication.** *Reputation* has become an important element in distinguishing legitimate email ("ham") from unwanted email ("spam"). Both *sender-based* reputation and *receiver-based* reputation technologies are currently available in the market. *Authentication* techniques aim to verify that email comes from a legitimate site, although by themselves they cannot determine whether a specific message is ham or spam. In Aberdeen's study on *Safe Email: Seven Important Tips for Better Email Security* (June 2009), Best-in-Class organizations were more than 1.5-times more likely than all other organizations to verify the authenticity of the sender.
- **Data protection.** Leading solution providers have adapted the content monitoring and filtering technologies that underlie their email security and web security solutions to provide key data loss prevention capabilities as well, e.g., to block sensitive data from being transmitted, or to automatically encrypt email or attachments based on pre-established policy.

Drivers of Investments in Email Security (in General)

Productivity loss and **data loss** are the leading drivers for current investments in email security in general, based on the results of Aberdeen's *Safe Email* study. Spam, of all varieties – ranging from nuisance solicitations for prescription drugs and other fake product offerings, to malicious conveyances for malware and phishing attacks – continues to be a significant problem, globally representing between 75-95% of all email traffic at an estimated 200 billion messages per day according to leading vendors. Across all survey respondents, the quantity of spam (including that caught successfully before reaching end-user inboxes) increased on a year-over-year basis, and end-users are actively complaining about it: about half (46%) of all respondents indicated that their IT administrators receive complaints about spam on a daily or weekly basis.

Spammers and phishers are clever at evolving and adapting their techniques to take advantage of the emotional aspects of current events, with subject lines chronicling the headlines of the time, for example:

- Rising gas prices
- Mortgage foreclosures
- Economic bailout packages and government deposit guarantees
- Lower interest rates and mortgage refinancing strategies
- Natural disasters in Haiti and Chile
- Job offers for the unemployed

In all likelihood, a new wave of subject lines having to do with air travel and volcanic ash can be expected in the coming weeks. In many ways, an archeological dig through the sediment of spam would reveal an accurate historical record of fear and greed in our Internet-based society.

Growth in **social networking** has also given a boost to spammers and phishers; for example, the popularity of shortened URLs on sites like Twitter make it even easier for attackers to disguise malicious links and to exploit end-user trust through social engineering. The overarching point is that email security deals with a dynamic, always-changing, ever-evolving threat landscape – and for this reason it is no wonder that regardless of their choice of an on premise or cloud-based implementation, 100% of the respondents in Aberdeen's study had implemented some form of email security (Figure 2).

Best-in-Class Strategies and Best Practices for Secure Email

Best-in-Class companies focus not only on protecting end-users from the unwanted email (spam) and email-borne vulnerabilities coming into their organization, but also on preventing the dissemination of spam or infected email on the outbound side. As outlined in Aberdeen's study on *Safe Email*, the top performers:

- **Address email security from both directions.** That is, they proactively monitor and filter incoming email and the potential threats it may carry, including contaminated email carrying malware, phishing attacks and blended threats (i.e., seemingly innocuous email containing dangerous executables or web links). They address outbound email security as well, including monitoring for botnet

Determining the Best-in-Class

To distinguish Best-in-Class companies (top 20%) from Industry Average (middle 50%) and Laggard organizations (bottom 30%), Aberdeen used the following performance criteria:

√ Decreased volume of spam reaching end-users

√ Reduced incidents of viruses, Trojans, spyware, botnet or other malware infections contracted from email

√ Reduced data loss or data exposure incidents attributable to email

√ Reduction in lost productivity as a result of email

√ Decreased cost associated with recovery from email attacks

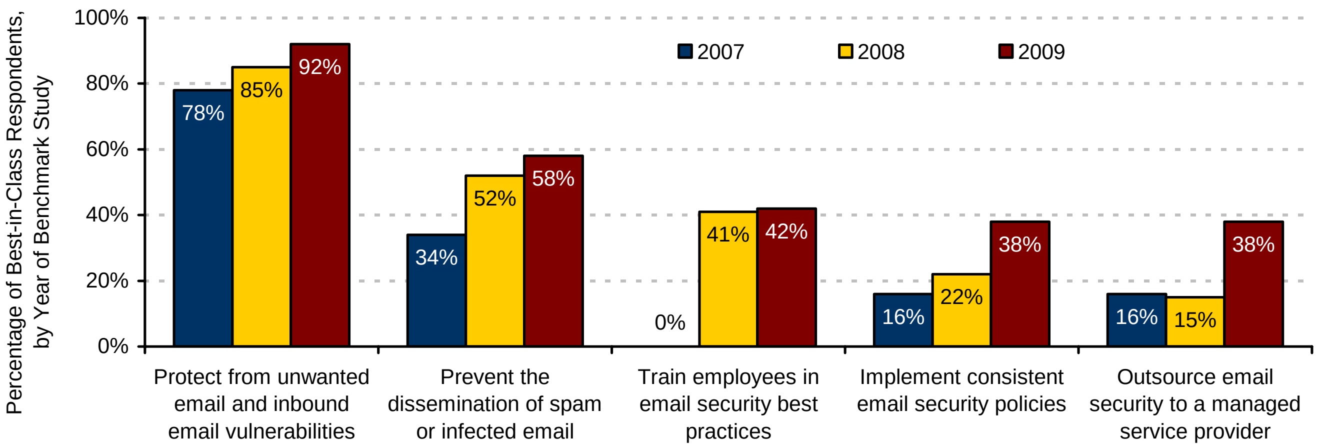
Companies with top performance based on these criteria earned "Best-in-Class" status.

activity, making sure that email sent from their organization is free from malware, preventing leakage of sensitive data (whether malicious, inadvertent, or intentional but non-malicious), and protecting legitimate email in transit.

- **Define and enforce email security policies.** The top performers pay specific attention to email as one of the most common channels for loss or exposure of sensitive data, and define and enforce consistent policies for acceptable use. Formal awareness and training programs for end-users is strongly correlated with Best-in-Class results; no matter how much technology is deployed, end-user behavior plays an important role in safeguarding sensitive corporate information and in protecting their own online identities.
- **Maintain email availability.** Best-in-Class companies take deliberate steps to reduce or eliminate outages and downtime that can leave the organization crippled without one of its most ubiquitous mission-critical applications.
- **Address email archiving.** Policies regarding how long email should be preserved should be intentional, not left to chance. The confidentiality, integrity and availability of email archives can be critical to business continuity, as well as to legal e-discovery requirements should the need arise.

For each of the last three years, Aberdeen has conducted benchmark studies on best practices in email security; **consistency of email security policies** and **use of cloud-based email security** solutions showed the biggest change over the previous year (Figure 3). Aberdeen's research provides strong evidence that the jump to email security in the cloud is being led by the companies achieving top performance.

Figure 3: Year-over-Year Trends – Three Years of Benchmark Research on Email Security



Source: Aberdeen Group, April 2010

Drivers of Investments in Email Security in the Cloud

Given *productivity loss* and *data loss* as the leading drivers for investments in email security in general, what are the top drivers for investments specifically in email security in the cloud? Aberdeen's analysis shows that users of cloud-based email security solutions are looking to **improve security** (67% of respondents using cloud-based email security solutions), **reduce their total cost** of email in general (58%) and of email security in particular (50%), and **gain access to security expertise** that is not available in-house (42%). The obvious question is: were they successful in achieving their goals of better security and lower total cost?

Framing "Return on Investment" for Email Security

Traditional return on investment calculations have always been difficult to apply to IT Security initiatives – for every dollar that an organization invests in the people, process and technology of a given IT Security project, the return is often expressed as "nothing bad seems to have happened." See Aberdeen's June 2009 Research Brief on *The Cost-Based Business Case for Data Protection* for a simple but powerful general framework for identifying and classifying the business value derived from investments in IT Security.

For the purposes of assessing the business value of email security, Aberdeen uses the following simple equation:

$$\frac{\text{(Total Email Security-related Costs Avoided)} \leftarrow}{\downarrow \text{(Total Cost of Email Security)} + \text{(Total Email Security-Related Costs Not Avoided)}}$$

The denominator includes the total cost of ownership for the organization's email security solution (e.g., expressed in terms of dollars per end-user per year). Also in the denominator, however, are the total email security-related costs from vulnerabilities and threats that were *not* avoided, in spite of the investments that have been made – these include the costs of spam, unscheduled downtime, malware infections, data loss or data exposure incidents, and so on. In the numerator are the best estimates for the total email security-related costs that *were* avoided as a result of the organization's investments. These will be imprecise, but as previously discussed spam alone represents between 75-95% of all email messages so it is not a giant leap of faith to assume that in comparison to the denominator, the numerator is relatively large. In Aberdeen's *Safe Email* study, the average for all respondents was $63 per end-user per year in the denominator, versus the enormity of email security-related costs avoided in the numerator, arguably making investments in email security one of the best enterprise investments in town.

The more general way to think about this simple equation is that any investments in technologies and services that **lower the total cost of email security** (*efficiency*) and cause a greater **shift from the denominator to the numerator in terms of email security-related**

costs avoided (*effectiveness*) will have a strongly positive impact on the overall return on investment.

So Which Users Had Better Results: On Premise, or Cloud?

Based on the findings from the *Safe Email* study, Aberdeen's analysis of 66 organizations using on premise email security solutions and 38 organizations using cloud-based email security solutions reveals that **users of cloud-based email security had substantially better results** in the critical areas of security, compliance, reliability and cost.

In terms of the total cost of email security, the average reported by users of on premise solutions was $45 per end-user per year, while the average reported by users of cloud-based solutions was $40 per end-user year – **an 11% cost advantage for cloud-based implementations.** In terms of email security-related costs not avoided, a summary of the average number of incidents experienced in the last 12 months is provided in Table 1.

Table 1: Email Security in the Cloud is More Effective

Average Number of Incidents (last 12 months)	On Premise	Cloud-based	Cloud Advantage
Harassing / offensive email received	21	13	38%
Virus, worm or Trojan infection	14	4	71%
Spyware or key logger installed	9	6	33%
Zombie machines	1	1	-
Security-related downtime	4	2	50%
Data loss / exposure (email)	2	2	-
Data loss / exposure (attachments)	2	2	-

Source: Aberdeen Group, April 2010

Overall, cloud-based email security deployments in this study experienced 47% fewer incidents of spam/malware than on premise deployments, and 50% less security-related downtime. In this dataset, there were no differences between on premise and cloud-based implementations in terms of data loss or data exposure incidents.

Were these findings just a fluke? Aberdeen's analysis of 41 companies using on premise email security solutions and 24 companies using cloud-based email security solutions – based on its study on *Deploying IT Security: Keeping the Threats and Headaches Outside* – confirms again that cloud-based implementations are more effective (Table 2). Overall, cloud-based email security deployments in this study experienced 75% fewer incidents of malware and 65% fewer audit deficiencies. In addition, on a year-over-year basis the advantages of the cloud-based implementations include:

- 34% greater reduction in associated data loss or data exposure incidents

- 5.9-times greater reduction in associated help desk calls
- 2.2-times greater reduction in associated downtime

Table 2: Email Security in the Cloud is More Effective

Average Number of Incidents (last 12 months)	On Premise	Cloud-based	Cloud Advantage
Malware infections	32	8	75%
Data loss or data exposure (insiders)	2	3	-
Audit deficiencies	23	8	65%

Source: Aberdeen Group, April 2010

Note that in both studies, there was negligible difference between on premise and cloud-based approaches to email security in terms of data loss or exposure. Examples of these types of incidents are part of our everyday experience with email, for example inadvertently sending a message to an unintended recipient, or intentionally forwarding a file to a private email account to continue working on a project from home. As noted above, these findings give credence to the increasing integration of data loss prevention capabilities into the email security and web security offerings from the leading solution providers.

Case in Point: Research University, Eastern US

A leading liberal arts research university in the eastern United States provides IT services to some 15,000 students, 700 full-time faculty, and 145,000 alumni. All incoming email is scanned and filtered, with legitimate messages delivered to their target inboxes as usual, while spam and virus-infected messages are quarantined in the university's anti-spam message center. End-users receive regular reminders to review their quarantined email, which they then have the option to *delete*, *read safely*, or *deliver*. The university also gives its email users the flexibility to *add and delete approved senders* and to *adjust or even turn off spam filters*, although all messages are always scanned for malware. All quarantined messages not deleted or delivered by end-users are automatically deleted after 14 days.

Before the current cloud-based email security services were put in place, the volume of spam being processed by the university's email systems -- which was estimated at 99% of their total email volume -- was bringing overall performance and reliability to its knees, with frequent failures and significant slowdowns in email delivery. Evaluations of several solutions eventually led to the deployment of Message Security from Google Postini Services, in part because it requires no on premise hardware or software and in part because of its adaptability to meet the university's requirements for flexibility and scale.

In addition to the security-related and performance-related benefits of implementing email security in the cloud, significant cost-related benefits realized by the university include much lower demand on a small IT staff.

"We no longer have to dedicate people just to deal with spam," says the university's chief information security officer. "Our limited staff can focus on other critical tasks necessary to keep our systems running smoothly." Help desk calls related to spam have also decreased dramatically under the new system, from more than 100 per week to just a handful of calls per month.

Solutions Landscape (illustrative)

Solution providers for email security in the cloud range from email-only specialists to vendors who offer a full suite of cloud-based email, web and data protection services. Given the underlying foundation of content monitoring and filtering technologies and the strong synergies between email security, web security and data loss prevention, Aberdeen expects to see an acceleration of cloud-based implementations that integrate email security, web security and data protection. Table 3 provides an illustrative list of solution providers for enterprise email security in the cloud, including select examples of hybrid approaches.

Vendor Selection Criteria

As seen in Aberdeen's benchmark studies, the leading selection criteria for an email security service provider were as follows (note up to 2 responses were accepted, so percentages do not add to 100%):

- Cost of service 54%
- Reputation of service provider 38%
- Flexibility in contract terms 17%
- Ease of integration 13%
- Ease of use 13%
- Already doing business with this service provider 13%
- Local support 13%

Table 3: Cloud-based Solutions for Email Security, Web Security (illustrative)

Vendor	Email Security	Web Security
McAfee www.mcafee.com	SaaS Email Protection	Web Protection Service
	McAfee Global Threat Intelligence	
Symantec Hosted Services www.messagelabs.com	MessageLabs Hosted Email Security	MessageLabs Hosted Web Security
	Symantec Global Intelligence Network	
Cisco www.ironport.com	IronPort Managed Email Security	ScanSafe
	IronPort Threat Operations Center	
Trend Micro www.trendmicro.com	Hosted Email Security	Hosted Website Security
	Trend Micro Smart Protection Network	
Google Postini Services http://www.google.com/postini/	Message Security	Web Security for Enterprise
	Google Postini Services	
Websense www.websense.com	Hosted Email Security	Hosted Web Security
	TRITON (integrated email, web, and data security)	
	Websense ThreatSeeker Network	
M86 Security www.m86security.com	Secure Messaging Service	Secure Web Service Hybrid
	M86 Security Labs	
Webroot www.webroot.com	Email Security Service	Web Security Service
MailGuard www.mailguard.com.au	MailGuard	WebGuard
Verizon Business www.verizonbusiness.com	Managed Security Services	Managed Security Services
Sophos www.sophos.com	Managed Email Appliances	Managed Web Appliances
	SophosLabs	
Proofpoint www.proofpoint.com	Proofpoint Enterprise	
Sendmail www.sendmail.com	Sentrion Cloud Services	
Panda Security www.pandasecurity.com	Panda Cloud Email Protection	
BoxSentry www.boxsentry.com	RealMail, TrustCloud	
Mimecast www.mimecast.com	Unified Email Management	
Sendio www.sendio.com	Sendio Full Defense	
Abaca www.abaca.com	Email Protection Gateway, ReceiverNet Protection Network	

Source: Aberdeen Group, April 2010

Summary and Recommendations

Strategies to secure enterprise email ultimately lead to the selection and deployment of a specific approach to email security: on premise, cloud-based, or hybrid. These choices – along with the policy, planning, process, and organizational elements of implementation – are critical success factors in the ability to realize the business benefits of enhanced security, sustained compliance, and lower-cost operations. Based on analysis of the top performers and interviews with select survey respondents, Best-in-Class approaches to email security include the following:

- **Protect email against viruses, worms, Trojans, and other malware.** All (100%) of the leading performers in Aberdeen's studies have done so, as compared to less than three-fourths (74%) of the lagging performers. This is a must-have for every email account holder in every organization, without exception. Nearly three-fourths (71%) of the top performers **filter their email attachments**, which are known to harbor malicious code, as well as the body of the email. The risk of data loss through increasingly sophisticated phishing attacks is of primary concern to most respondents, and the top performers have deployed **anti-phishing, anti-spyware, anti-key logging, and anti-fraud solutions** designed to detect and thwart these types of attacks.
- **Train end-users in safe email practices.** In a perfect world, there would be no email-based data breaches or attacks. In an ideal world, technology would transparently protect us against every possible attack and prevent every data breach. In the real world, however, keeping end-users aware of current threats helps to reduce the likelihood of their falling prey to the latest trap. Likewise, uneducated users may be more likely to email sensitive data inappropriately only because they aren't aware that they shouldn't. Two-thirds (67%) of the organizations earning top performance provide formal awareness and training in safe email practices for their end-users.
- **Integrate email and web security.** Blended threats – i.e., threats in which a seemingly innocuous email contains a malware executable or a URL that points to a malicious site – are increasingly common. The top performers either scan email to evaluate all embedded links and check the sites to which they point, or deploy tightly coupled web security that prevents clicking on a link contained in an email from resolving at a contaminated site.
- **Integrate email and attachments as part of a broader data loss prevention strategy.** Scanning outbound email and attachments for sensitive data is a good place to start; information contained in spreadsheets, documents, presentations, and so on may well be data that is sensitive to the organization or subject to regulatory data protection requirements. Insider threat is an unpleasant topic but one that should not be overlooked, especially

"Our recent transition to cloud-based email was pretty painful. As just one example, it was inexplicably decided that the 100-plus end-users in our business unit should independently migrate their existing email, calendar and contact data from the client side, rather than have just 1 administrator consistently migrate everyone's data from the server side. The result was predictably chaotic – including lost data, lost communication with our clients, and about three days of lost productivity for virtually everyone. In compensation costs alone, this was literally the equivalent of paying 2 full-time people to do nothing for an entire year, not to mention the opportunity costs of lost business. Email in the cloud may be less expensive than managing email in-house, but bad execution in the transition can quickly make the payback period a whole lot longer. But this experience made one thing certain, which is that email is a mission-critical application for this organization."

Vice President,
100-person business unit of
>$1B global direct marketing
company

in a troubled economy; many insiders have the both the knowledge and the technical skills to get around the organization's security policies and controls to access sensitive data or disrupt operations.

- **Leverage the cloud.** Cloud-based email security solutions, or hybrid solutions that leverage intelligence from the cloud, can help to ensure that "what happens in the cloud, stays in the cloud" – i.e., that spam and other email threats are eliminated before they touch the enterprise network, reducing risk and moving costs from the "not avoided" to the "avoided" category. Aberdeen's analysis shows that users of cloud-based email security had substantially better results than users of on-premise email security implementations in the critical areas of security, compliance, reliability and cost.

Based on the strong synergies with email security in the cloud, Aberdeen's upcoming research agenda includes closely related research publications on *Web Security in the Cloud* (May 2010) and *Content-Aware: The 2010 Data Loss Prevention Report* (June 2010). For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

Laptop Lost or Stolen? Five Questions to Ask and Answer; February 2010

Going Mobile: Security for Mobile Endpoint Devices; January 2010

Full-Disk Encryption On the Rise; September 2009

Enterprise Rights Management: Persistence Pays Off; August 2009

File Transfer is Not What it Used to Be: It's Secure, Reliable and Well-Managed; July 2009

Microsoft SharePoint: The Comedy (and Tragedy) of the Commons; July 2009

Safe Email: Seven Important Tips for Better Email Security in 2009; June 2009

Securing Unstructured Data: How Best-in-Class Companies Manage to Serve and Protect; June 2009

The Cost-Based Business Case for Data Protection; June 2009

Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence; March 2009

Managing Encryption: The Keys to Your Success; October 2008

Data Loss Prevention: Little Leaks Sink the Ship; June 2008

Managed Security Services; January 2008

Author: Derek E. Brink, Vice President and Research Fellow, IT Security (Derek.Brink@aberdeen.com)

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen http://www.aberdeen.com or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to http://www.harte-hanks.com