Research Brief

Aberdeen Group
A Harte-Hanks Company

May 2010

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

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

Business Context: On the Web, Every Day is a Bad Day

"Web security to me is like when the children go outside to play; on a bad day, you just know that they're going to track mud all over the house," noted a US-based IT director. "And obviously you can't always just keep them cooped up inside every time it's a bad day, because like everyone else in the family they have things to do and places to be. But here's the big difference: on the web, every day is a bad day."

The muck and mire that gets tracked all over the enterprise on the shoes of its web users is more than just an insult to good hygiene; the consequences of everyone being outside and exposed to the elements on the web can have a significant financial impact on the business, for example:

- Employee productivity
- Consumption of network bandwidth
- Unscheduled downtime
- Loss or exposure of sensitive data
- Cost of remediation
- Cost of audit and compliance

The challenge for enterprise web security initiatives is to strike the desired balance between providing the business with secure, convenient and reliable means to enable real-time collaboration, interactivity and information-sharing on the one hand, while on the other protecting the assets and identities of the enterprise and its end-users.

Web Security

The "muddy feet" analogy for web security is fitting, in that it includes the threats that can beset end-users without their knowledge, like the back-spatter that happens when you ride your bike on a wet and muddy street. At the same time, it encompasses threats that end-users embrace willingly, like deliberately seeking out and splashing through the biggest puddles. An illustrative compilation of current web security threats is given in Table 1.

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 web security solutions, users of cloud-based web security solutions had substantially better results:

√ 58% fewer malware incidents over the last 12 months

√ 93% fewer audit deficiencies

√ 45% less security-related downtime

√ 45% fewer incidents of data loss or data exposure

Definitions

For this Research Brief:

√ **Web Security** refers to web-borne malware; blended threats, drive-by downloads, or social engineering exploits involving web URLs; and monitoring / filtering of web-based applications

√ **Web Application Security** refers to vulnerabilities and exploits related to web applications and supporting frameworks, application servers, web servers, database servers, and computing platforms

Telephone: 617 854 5200
Fax: 617 723 7897

Table 1: Web Security Threats (illustrative)

Category	Examples	Recent Trends / Commentary
Web-borne malware	▪ Viruses, worms, Trojans ▪ Spyware, keyloggers, rootkits	*Socially engineered malware* is on the rise, for example *Antivirus 2009*, a fake anti-virus product that end-users willingly downloaded, installed and launched on their Windows PCs.
	▪ Bots ▪ Advanced persistent threats	Malicious use of *bots* ranges from the automation of email spam to the coordination of attacker operations across a large-scale network of computers. The implication of *advanced persistent threats* is that they involve human command and control, specific objectives and skilled, well-funded attackers.
Blended threats	▪ Phishing emails ▪ URL spam	*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. About 80% of spam includes a URL to one or more web sites. Corporate, personal and web email are all active targets.
Drive-by downloads	▪ Infected websites	The web sites your mother told you not to visit – including adult content, illegal gambling and illegal drugs, and representing between 5-10% of all web sites – are notorious hosts for malicious links. According to industry sources, about 1% of the 200,000 highest-traffic web sites are infected with malware.
	▪ Anonymous proxies	*Anonymous proxy* servers, which access Internet resources on behalf of the original requester, are increasingly being used by attackers to hide malicious target URLs from web security monitoring and filtering technologies.
	▪ Shortened URLs	The popularity of *shortened URLs* on social networking sites such as *Twitter* make it even easier for attackers to disguise malicious links and to exploit end-user trust through social engineering.
	▪ SEO poisoning	Attackers are leveraging the successful techniques of *search engine optimization* (SEO) to drive end-users to web sites infected with malicious code.
	▪ International domain names	In May 2010, the International Corporation for Assigned Names and Numbers (ICANN) activated support for domain names that contain no Latin characters, increasing the opportunity for attackers to exploit malicious, mixed-character URLs that are visually indistinguishable from their legitimate counterparts.
Social engineering	▪ Vishing	*Vishing* (a combination of "voice" and "phishing") refers to the use of fake phone sites as part of the attacker's ecosystem for getting end-users to voluntarily give up private information. For example, the end-user may receive an email requesting that they call a toll-free number, or they may receive a phone call requesting that they call a toll-free number or visit a website.
	▪ Smishing	*Smishing* (a combination of "SMS" and "phishing") refers to the use of short message service (SMS) text messages as part of the attacker's ecosystem for getting end-users to voluntarily give up private information. For example, the end-user may receive a text message requesting that they call a toll-free number or visit a website.

Category	Examples	Recent Trends / Commentary
Web 2.0 applications	▪ Social networking sites	The social networking sites your employer may have encouraged you to visit (or in many cases told you *not* to visit, particularly when it involves company time or resources) – including *LinkedIn*, *Facebook*, *Twitter*, blogs – have seen their privacy and security policies come under fire in the first half of 2010. Both enterprises and individual end-users must become more deliberate in balancing the risks and rewards of sharing information through these channels, and regulators such as the Financial Industry Regulatory Authority (FINRA) are starting to weigh in with guidance. Social networking APIs that make it easier for software developers to add value can also be expected to be exploited more aggressively by attackers.
	▪ Real-time applications	So-called *Web 2.0* applications are characterized by real-time collaboration, interactivity, and information-sharing. Instant messaging, chat and ad hoc, person-to-person file sharing (e.g., *YouSendIt*) are part of a growing culture of immediacy: who is available right now? Where can I get an immediate answer? How can I get or give immediate access to this information? Add to this a rich stew of multimedia applications – including voice over IP (e.g., *Skype*), web conferencing, streaming audio and streaming video (e.g., *YouTube*, *Windows Media Player*), podcasts and vodcasts. The result is that companies are confronted with a non-trivial challenge: to provide the secure, convenient and reliable means to enable collaboration, while ensuring that sensitive data flows reliably and leak-free to its intended destination.

Source: Aberdeen Group, May 2010

Web Application Security

A clear distinction should be made between **web security** (the focus of this Research Brief) and **web application security**, which refers to vulnerabilities and exploits that are specifically related to web applications and their supporting frameworks, application servers, web servers, database servers, and computing platforms. Industry sources note that nearly half of all reported vulnerabilities are related to web applications; surprisingly, about two-thirds of known web application vulnerabilities had no vendor-supplied patch available at end of 2009. More than 4 out of 5 web application vulnerabilities affect plug-ins (e.g., *Microsoft ActiveX*), as opposed to the underlying platforms, with a significant increase over the last year in vulnerabilities related to *Adobe PDF*. The overarching trend in web application security exploits is towards the mass-produced (e.g., using web exploit toolkits), rather than the purpose-built. Even the criminals value higher productivity and lower cost.

Aberdeen plans to address the important topic of web application security in a new benchmark study, currently scheduled for the second half of 2010. For now, the top ten web application security threats for 2010 – as defined by the collaborative work of the Open Web Application Security Project (OWASP) – are summarized in Table 2.

Table 2: Web Application Security Threats – OWASP Top 10 for 2010

Category	Examples	Commentary
Web application security threats	▪ Injections	*Injections* (e.g., SQL, OS or LDAP injections) occur when an attacker sends hostile data to an interpreter as part of a command or query, tricking it into executing unintended commands or accessing unauthorized data.
	▪ Cross-site scripting	*Cross-site scripting* occurs when an application sends untrusted data to a web browser without proper validation, allowing attackers to execute malicious scripts in the end-user's browser.
	▪ Authentication and session management	Flawed implementations of *user authentication* and *session management* can allow attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume end-user identities.
	▪ Direct object references	*Direct object references* occur when attackers are able to manipulate direct references to an internal implementation object (e.g., a file, directory or database key) to access unauthorized data.
	▪ Cross-site request forgery	A *cross-site request forgery* attack occurs when an attacker forces an end-user's browser to generate forged HTTP requests – including the user's session cookie and any other automatically included authentication information – which appear to be legitimate to a vulnerable web application.
	▪ Security misconfiguration	Attackers can exploit vulnerabilities from undefined, unimplemented or out-of-date *security configurations* for web applications, frameworks, application servers, web servers, database servers, and platforms.
	▪ Insecure cryptographic storage	Attackers may be able to access or modify poorly protected information such as cardholder data, authentication credentials, or other personally identifiable information to conduct credit card fraud, identity theft, or other criminal activity.
	▪ Failure to restrict URL access	Failure to check *access rights* before rendering protected links and buttons may allow attackers to forge URLs to access these hidden resources.
	▪ Insufficient transport layer protection	Flawed implementations of *transport layer authentication and encryption* can compromise the confidentiality and integrity of sensitive network traffic and expose it to attackers.
	▪ Unvalidated redirects and forwards	Improper validation of *redirect and forward requests* enables attackers to redirect end-users to phishing or malware sites, or use forwards to access unauthorized pages.

Source: Open Web Application Security Project, OWASP Top 10 Application Security Risks – 2010

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 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*.

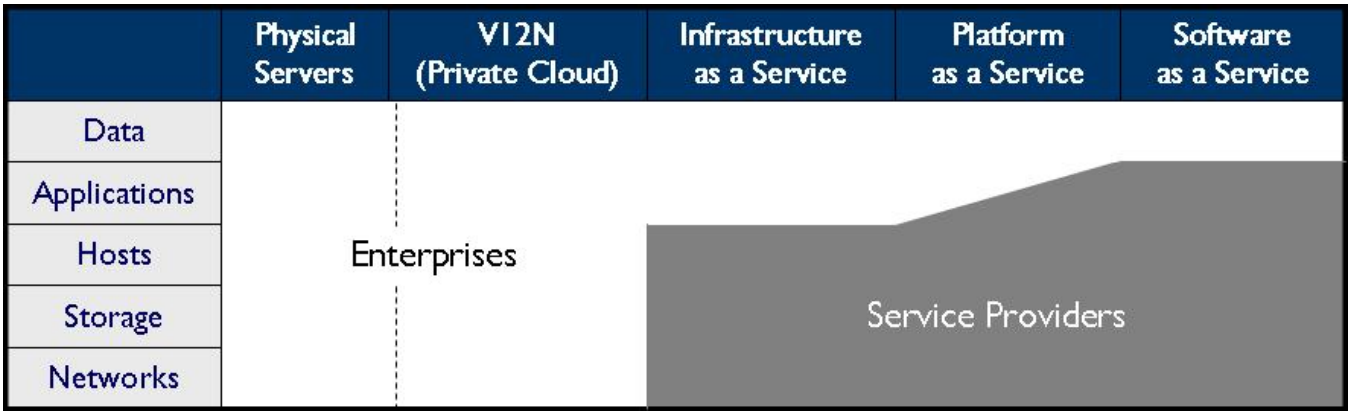
In Aberdeen's view, one straightforward way to differentiate the various levels of cloud-based computing is in consideration of the following question: who has ownership over the networks, storage, hosts, applications, and data – the enterprises, or the service providers? As depicted in Figure 1, in 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

"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

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.

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



Source: Aberdeen Group, May 2010

Cloud-based Security: Security Software as a Service

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 a 50/50 split between *on premise* and *cloud-based* implementations, with indications of a net shift towards cloud-based implementations over the next 12 months. With respect to **web security** solutions, Aberdeen's research showed that implementations were currently more than 2-times more likely to be on premise than cloud-based (i.e., a 60/30 split, with 10% not implementing).

Given the snapshot of the market represented by these findings, it comes as no surprise that web 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)
- 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 web

Fast Facts

Average time respondents have been using web security services in the cloud: 4.4 years

Average contract length for cloud-based web security services: 2.7 years

Terms included in web security Service Level Agreement (SLA):

√ Service availability to end-users (uptime) 83%

√ Responsiveness to escalation of an event 67%

√ Time-to-acknowledgment of escalation 67%

√ End-user satisfaction 56%

√ Qualifications of service provider employees 41%

√ Compliance with regulations or standards 39%

Average percentage of SLA terms met in the last year: 94%

security services based on their own unique sense of balance between factors such as security, compliance, total cost, and degree of ownership and control.

Drivers of Investments in Web Security in the Cloud

What are the top drivers for investments in web security in the cloud? Aberdeen's analysis shows that users of cloud-based web security solutions are looking to **reduce their total cost** of web security (59% of respondents using cloud-based web security solutions), **reduce the burden of managing** web security solutions (55%), **improve security** (50%), and **gain access to security expertise** that is not available in-house (32%). The obvious question is: were they successful in achieving their goals of better security and lower total cost?

Framing "Return on Investment" for Web 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 web security, Aberdeen uses the following simple equation:

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

The denominator includes the total cost of ownership for the organization's web security solution (e.g., expressed in terms of dollars per end-user per year). Also in the denominator, however, are the total web 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 URL spam, malware infections, unscheduled downtime, data loss or data exposure incidents, and so on. In the numerator are the best estimates for the total web security-related costs that *were* avoided as a result of the organization's investments. These will be imprecise, but as previously noted URL spam alone represents between 60-75% 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.

The more general way to think about this simple equation is that any investments in technologies and services that **lower the total cost of web security** (*efficiency*) and cause a greater **shift from the denominator to the numerator in terms of web 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 responses collected as part of its *Safe Email* study, Aberdeen's analysis of 36 organizations using on premise web security solutions and 22 organizations using cloud-based web 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 web security-related costs not avoided, a summary of the average number of incidents experienced in the last 12 months for both groups is provided in Table 1.

Table 3: Web Security in the Cloud is More Effective

Average Number of Incidents (Last 12 Months)	On Premise	Cloud -based	Cloud Advantage
Malware infections	26	11	58%
Web site compromise	9	2	78%
Data loss or data exposure	11	6	45%
Security-related downtime	11	6	45%
Audit deficiencies	30	2	93%

Source: Aberdeen Group, May 2010

On the efficiency side of the equation, analysis of the two groups also shows that users of cloud-based web security solutions realized a 42% greater reduction in associated help desk calls over the past year, in comparison to users of on premise solutions.

Translating the advantages of web security in the cloud is an exercise unique to each organization, but the following back-of-the-envelope calculations based on the findings in Table 3 provide a general flavor:

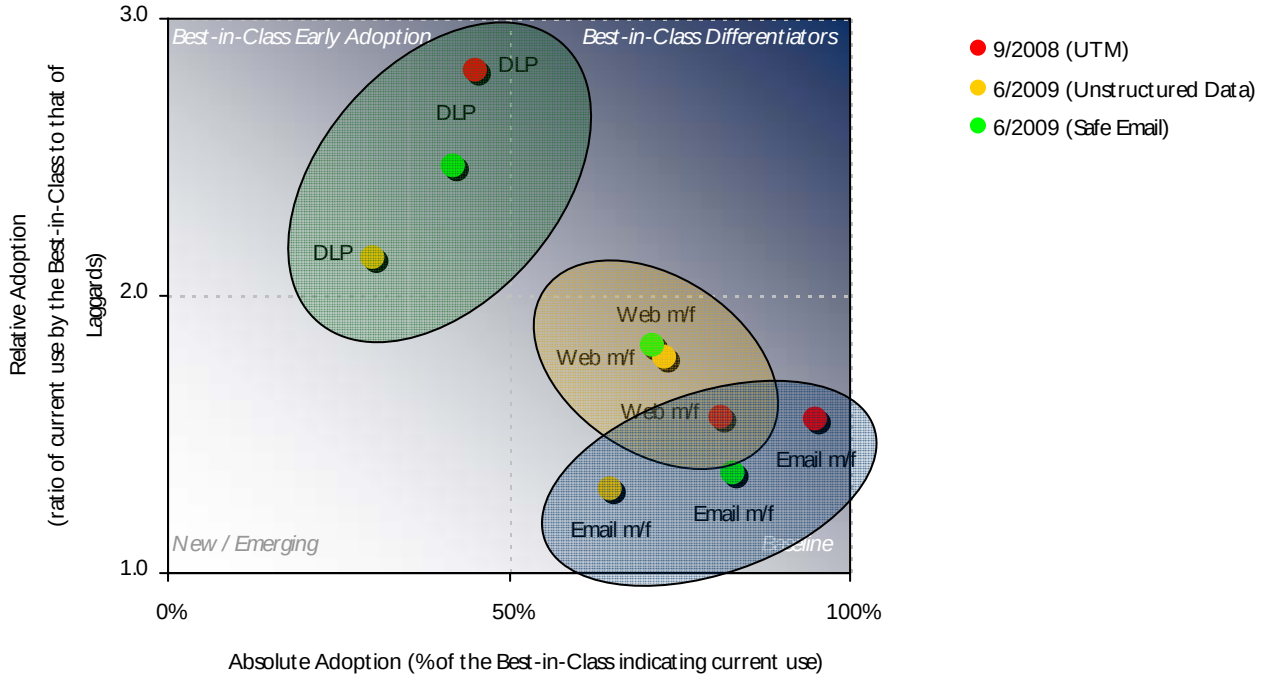
- 5 fewer incidents of data loss or data exposure, at an average total cost of US$640,000 per incident (as found in *The 2009 Aberdeen Report*), translates to more than $3 million in costs avoided
- 28 fewer audit deficiencies, at an average cost of US$7,000 per item to remediate (as found in Aberdeen's *PCI DSS* research), translates to roughly $200,000 annually in cost savings
- At an average cost of $40 per help desk call, a 42% reduction translates to a savings of $16 per call, or more than $60 per end-user per year in cost savings based on one call per end-user per quarter
- Based on an average revenue per employee of US$175,000 per year, unplanned downtime costs about $100 per employee per

hour; cloud-based web security users effectively reduce this to $55 per employee per hour for security-related downtime

Content-Aware: The Convergence of Email, Web, DLP

Aberdeen's examination of the current use of monitoring / filtering technologies from three previous benchmark studies shows a consistent pattern of **convergence** between email security, web security and data loss prevention (Figure 2). Email security and web security have become established as *baseline technologies* (i.e., high adoption by the top performers, as well as by other organizations in the study). Data loss prevention is in *early adoption* by the top performers (i.e., modest adoption by the leading companies, but high adoption by the leading performers relative to the laggards). 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 across these three areas.

Figure 2: Convergence of Content-Aware Technologies: Current Use of Email, Web and DLP



Source: Aberdeen Group, May 2010

Solutions Landscape (illustrative)

Solution providers for web security in the cloud range from web-only specialists to vendors who offer a full suite of cloud-based email, web and data protection services. Table 3 provides an illustrative list of solution providers for enterprise web security in the cloud, including select examples of hybrid approaches.

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

Vendor	Web Security	Email Security
McAfee www.mcafee.com	Web Protection Service	SaaS Email Protection
	McAfee Global Threat Intelligence	
Symantec Hosted Services www.messagelabs.com	Hosted Web Security	Hosted Email Security
	Symantec Global Intelligence Network	
Cisco www.ironport.com	ScanSafe	IronPort Managed Email Security
	IronPort Threat Operations Center	
Trend Micro www.trendmicro.com	Hosted Website Security	Hosted Email Security
	Trend Micro Smart Protection Network	
Google Postini Services http://www.google.com/postini/	Web Security for Enterprise	Message Security
	Google Postini Services	
Websense www.websense.com	Hosted Web Security	Hosted Email Security
	TRITON (integrated email, web, and data security)	
	Websense ThreatSeeker Network	
M86 Security www.m86security.com	Secure Web Service Hybrid	Secure Messaging Service
	M86 Security Labs	
Webroot www.webroot.com	Web Security Service	Email Security Service
MailGuard www.mailguard.com.au	WebGuard	MailGuard
Sophos www.sophos.com	Managed Web Appliances	Managed Email Appliances
	SophosLabs	
Armorize www.armorize.com	HackAlert	
BlueCoat www.bluecoat.com	WebPulse, Secure Web Gateway	
Barracuda Networks www.barracudanetworks.com	Barracuda Purewire Web Security Service	
Damballa www.damballa.com	Failsafe	
nexTier Networks www.nextiernetworks.com	Compliance Enforcer	
WatchGuard www.reputationauthority.org	ReputationAuthority	
Zcaler www.zscaler.com	Zscaler Services	

Source: Aberdeen Group, May 2010

Summary and Recommendations

Strategies to secure enterprise use of the web ultimately lead to the selection and deployment of a specific approach to web 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 web security include the following:

- **Protect 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 web user in every organization, without exception. The risk of data loss through increasingly sophisticated phishing attacks is also 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 practices and acceptable use policies.** In a perfect world, there would be no web-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.
- **Integrate email and web security.** Blended threats – e.g., 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 scan email to evaluate all embedded links and check the sites to which they point, and deploy tightly coupled web security that prevents clicking on a link contained in an email from resolving at a contaminated site.
- **Leverage the cloud.** Cloud-based web 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 web-borne 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 web security had substantially better results than users of on-premise web security implementations in the critical areas of security, compliance, reliability and cost.

Based on the strong synergies between recent research on email security and web security, Aberdeen's upcoming research agenda includes closely related research publications on *Content-Aware: The 2010 Data Loss Prevention Report*, *Web Application Security*, and *Security and the Software*

Vendor Selection Criteria

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

√ Cost of service 59%

√ Flexibility in contract terms 27%

√ Reputation of provider 18%

√ Already doing business with this provider 18%

√ Range of services provided 14%

√ Ease of integration 9%

√ Ease of use 9%

Aberdeen Group
A Harte-Hanks Company

Development Lifecycle. For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
Email Security in the Cloud: More Secure! Compliant! Less Expensive!; April 2010	*Safe Email: Seven Important Tips for Better Email Security in 2009*; June 2009
Laptop Lost or Stolen? Five Questions to Ask and Answer; February 2010	*Securing Unstructured Data: How Best-in-Class Companies Manage to Serve and Protect*; June 2009
Going Mobile: Security for Mobile Endpoint Devices; January 2010	*The Cost-Based Business Case for Data Protection*; June 2009
Full-Disk Encryption On the Rise; September 2009	*Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence*; March 2009
Enterprise Rights Management: Persistence Pays Off; August 2009	*Managing Encryption: The Keys to Your Success*; October 2008
File Transfer is Not What it Used to Be: It's Secure, Reliable and Well-Managed; July 2009	*Data Loss Prevention: Little Leaks Sink the Ship*; June 2008
Microsoft SharePoint: The Comedy (and Tragedy) of the Commons; July 2009	*Managed Security Services*; January 2008

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