Sector Insight

Aberdeen Group
A Harte-Hanks Company

January 2013

Modernizing Security for the Small and Mid-Sized Business – Recommendations for 2013

As small and mid-sized businesses (SMBs) take advantage of the compelling benefits of the transformations in their IT computing infrastructure – and struggle at times with the additional complexities that come along with it – they should also re-think how they deal with the corresponding vulnerabilities, threats and risks. SMBs relying solely on traditional *signature-based* approaches (i.e., **anti-virus** and **firewalls**) were actually found to be spending 1.5-times more on endpoint security and 4-times more on network security than companies adopting a more comprehensive, *defense-in-depth* approach. Specifically, **email security**, **web security** and **secure file sharing** should be considered foundational security capabilities for every small and mid-sized business, in addition to anti-virus and firewalls.

Business Context: Security Risks are Equal Opportunity

Over just the past couple of years, the typical IT computing infrastructure for organizations of all sizes has become considerably more flexible and powerful:

- **Endpoints** refers not only to the traditional PCs and laptops that are provisioned and managed by the company – but also to the highly mobile devices (such as *smart phones* and *tablets*) that are increasingly owned and managed directly by the end-users
- **Networks** refers not only to the electronic interconnections and protocols between systems (including *wired*, *Wi-Fi*, *remote access* over VPN or SSL VPN, *mobile access* over 3G / 4G networks) – but also to the social connections and collaboration between people, both within and across organizational boundaries
- **Back-end systems** refers not only to the traditional hosts, storage and applications that are managed directly by the company – but also to the *virtualized* instances of these resources, both on-premise and in the *cloud*
- **End-users** refers not only to employees – but also to *temporary employees* and *contractors*, *guests*, *mobile / remote users*, *business partners* and *external customers*

Just like everyone else, small and mid-sized businesses (SMBs) are taking advantage of the compelling benefits of these transformations in their IT computing infrastructure – and struggling at times with the additional complexities that come along with it. But this also means that they should be re-thinking how they deal with the corresponding vulnerabilities, threats and risks.

Sector Insight

Aberdeen's Sector Insights provide strategic perspective and analysis of primary research results by industry, market segment, or geography.

Sector Definition

For the purposes of this report, Aberdeen defines the following terms based on an organization's reported number of employees:

√ Small: <100

√ Mid-Sized: 100-1,000

√ Large: >1,000

Based on the above, the term **Small / Mid-Sized Business (SMB)** refers to companies with up to 1,000 employees.

Aberdeen sometimes defines these terms based on an organization's annual revenue in the most recent 12-month reporting period, with substantially similar results:

√ Small: <$50M

√ Mid-Sized: $50M - $1B

√ Large: >$1B

Aberdeen Group
A Harte-Hanks Company

SMBs are Not Too Small to Be of Interest to Attackers

Some SMBs may feel that their company is too small to be a target of interest to external attackers. But malware designed to exploit vulnerabilities in the most commonly deployed systems generally doesn't care about the size of the company – just as the sun rises and the rain falls on the good and the bad alike, companies of all sizes are affected by both the benefits and the risks of IT. In this sense, security vulnerabilities and risks are equal opportunity. And to the extent that large businesses (with more to lose) have invested more strongly in security measures, attackers may view SMBs as the lower-hanging fruit – for example, note that *two-thirds* (67%) of the data breaches investigated in a Verizon Business study occurred in organizations of less than 100 employees (see sidebar at right). In some cases, the SMB may not be the attacker's direct target, but the weakest link in a value chain that provides the easiest means to the attacker's ultimate objective.

Most of the incidents in the Verizon Business study involved *external hacking* (50% of breaches, 89% of records), but SMBs are not immune to internal attackers, either. The annual cost of internal fraud can be substantial – in the Association of Certified Fraud Examiners *2012 Global Fraud Study*, fraud accounted for an average of 5% of annual revenue, with a median loss per incident of $140K. Many of these are IT-related problems, with IT security controls as an important part of the solution.

SMBs are Just as Subject to Regulatory Compliance

To be sure, sustaining security and compliance requirements can be complex and costly – particularly in SMB environments where IT staff and security expertise is typically very limited or non-existent.

And yet the regulatory and moral obligation to security and compliance remains, as in the example of the Payment Card Industry (PCI) Data Security Standard (see sidebar at right). Regardless of their size, *all* organizations that store, process, or transmit cardholder information are required to implement the policies, processes, and enabling technologies necessary to achieve and sustain compliance with PCI DSS.

SMBs Need to Stay Current on Vulnerabilities and Risks

IT computing infrastructure is evolving – and the associated vulnerabilities and risks are evolving, too. A snapshot of the latest statistics and trends is summarized in Table 1. It's important to note that even with the many changes in **how** SMB end-users are accessing their IT resources, Aberdeen's research shows that **what** SMB end-users are actually doing hasn't really changed much at all – i.e., access company *email* (94%), *calendars* (89%) and *contacts* (89%); access *web* and *web-based applications* (87%); access or share *unstructured data* such as files, documents, worksheets, and presentations (54%). This amplifies the importance of security measures to protect the vast majority of SMB network traffic: **email**, **web** and **file transfer**.

Fast Facts: Data Breaches

The *2011 Data Breach Investigations Report* (Verizon Business) illustrates why SMBs should pay more attention to security:

- √ Two-thirds (67%) of breaches investigated occurred in *smaller organizations* (less than 100 employees), which were often small, independent *franchisees* of large firms
- √ Most incidents involved *external hacking* (50% of breaches, 89% of records), *malware* (49% of breaches, 79% of records), or both

Fast Facts: PCI Compliance

Small Merchants: *You* must secure cardholder data to meet Payment Card Industry rules!

Small merchants are prime targets for data thieves. It's *your* job to protect cardholder data at the point-of-sale.

If cardholder data is stolen – *and it's your fault* – you could incur fines, penalties, even termination of the right to accept payment cards!

Source: PCI Security Standards Council home page for Small Merchants, February 2012

Table 1: SMBs Need to Stay Current on Vulnerabilities and Risks; Latest Statistics and Trends

Malware continues to evolve	▪ In 2012, the total number of malware samples in the threat database topped 100 million ▪ Cleverly engineered stealth malware – e.g., *rootkits* – is designed to evade detection, persisting on endpoints for prolonged periods of time; SMBs may be infected but unaware ▪ New strains of malware target an area of endpoints that performs critical startup operations – the *master boot record* – and provides attackers with a wide variety of capabilities for penetration, persistence and control; SMBs may be infected but unaware ▪ One of the fastest growing areas of cybercrime – known as *ransomware* – is malware that takes a computer or its data hostage, so attackers can extort payment from their victims
Mobile malware is growing	▪ Malware and spyware targeting mobile devices (smart phones and tablets) is on the rise, with over 20,000 malware samples in the threat database ▪ The Google Android platform continues to be the largest target for malware; very few mobile threats are *not* directed at Android devices ▪ Aberdeen's most recent study on mobility found that nearly three-quarters (72%) of all respondents support corporate-owned smart phones and tablets; more than three out of five (62%) now support smart phones and tablets owned by their employees, the trend generally referred to as *Bring Your Own Device (BYOD)*; SMBs are no exception
Email threats (phishing, spam) continue to be an effective means to exploitation	▪ Phishing attacks are most frequently masquerading as financial sites, online shopping and auction sites, government sites, and online services ▪ Countries most heavily targeted are the United States, United Kingdom, Canada, South Africa, and Australia ▪ Spam subject lines related to prescription drugs are currently the most popular, with other leading subjects ranging from jobs to marketing to delivery status notifications
Web sites are increasingly used as a conduit for delivering malware	▪ The total number of suspect URLs is approaching 50 million, growing at an average of 2.7 million per month ▪ Suspect URLs refer to nearly 24 million domain names ▪ More than 90% of suspicious URLs host malware, exploits or code specifically designed to compromise the systems that visit them
Data loss or exposure can be costly	▪ The average cost of an incident involving loss or exposure of sensitive data in Aberdeen's data protection study was $640K, a finding which is quite conservative compared to many other widely circulated industry figures; for SMBs, *loss of reputation* can be devastating ▪ In the absence of *well-defined policies*, *awareness and education*, and *officially supported alternatives* for sharing files securely, knowledgeable end-users will often overlook policy, security and compliance in favor of getting their jobs done by taking advantage of free and readily available alternatives – i.e., the so-called *consumerization* of information technology ▪ For example, as of this writing the number of mobile applications available in the iTunes App Store under the search phrase "file sharing" was 365 for iPhone and 274 for iPad, with prices ranging from free to a few dollars

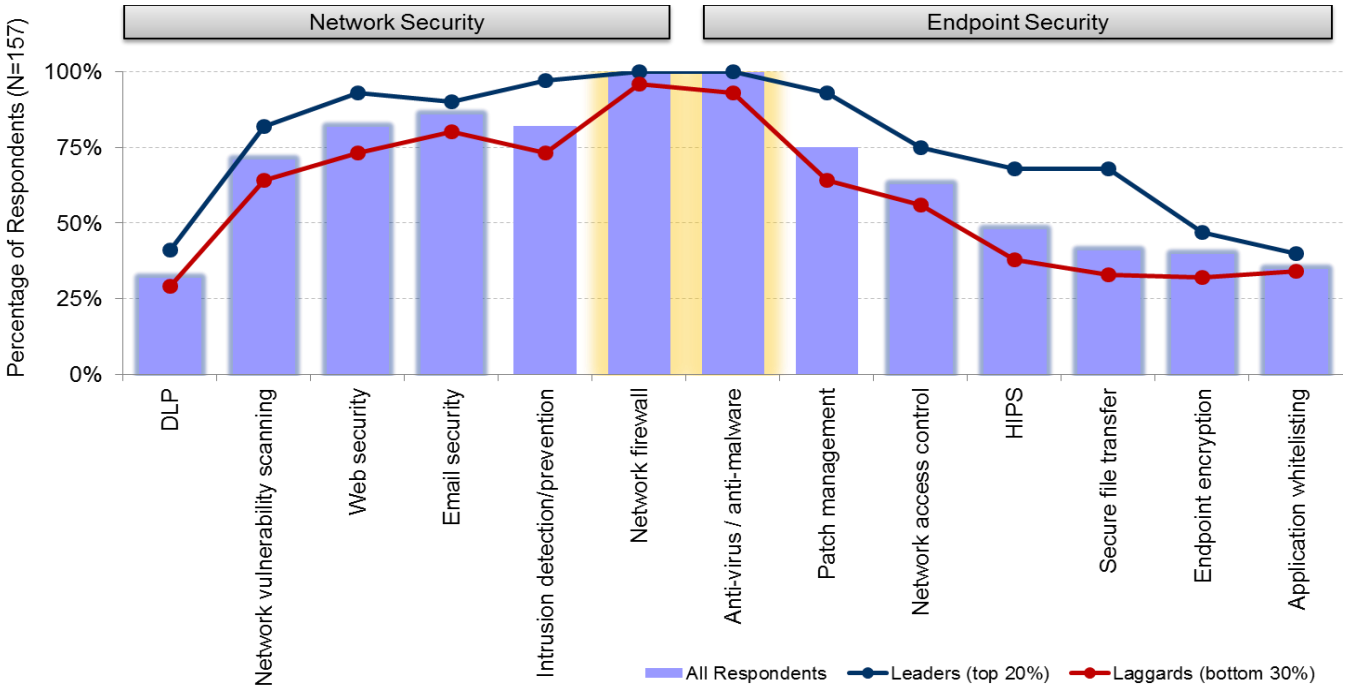
Source for threat data: *McAfee Threats Report*, McAfee Labs, 3Q 2012
Source: Aberdeen Group, January 2013

The inclusion of anti-virus solutions such as Microsoft's Forefront Endpoint Protection as part of the endpoint's underlying operating system may mislead some SMBs to make an erroneous conclusion – i.e., that "free A/V" is "good enough for me." In addition to *anti-virus* and *firewalls*, *email security*, *web security* and *secure file sharing* should be considered foundational security capabilities for every small and mid-sized business.

Aberdeen's Research Findings: Are SMBs Keeping Pace?

What security solutions are companies deploying to cope with the transforming IT computing infrastructure and keep pace with the ever-evolving security threat landscape? Aberdeen routinely asks respondents about their *current use*, *planned use* and *current evaluations* of a wide range of IT Security technologies; the results for selected endpoint security technologies from a study of more than 160 organizations are shown in Figure 1.

Figure 1: All Have Deployed Some Endpoint Security (Anti-Virus) & Network Security (Firewalls)



Source: Aberdeen Group, January 2013

Endpoint Security: All Respondents, Leaders and Laggards

As indicated by the light blue bars, Figure 1 shows that all (100%) respondents have deployed *anti-virus / anti-malware*; three out of four (75%) have deployed *patch management*; half (48%) have deployed *host-based intrusion detection and prevention* (HIPS); and so on.

Meanwhile, the blue and red lines which are superimposed on the light blue bars in Figure 1 indicate the percentage of the **leaders** and **laggards** from Aberdeen's study (for definitions, see the sidebar at right) that have deployed these selected endpoint security technologies. In general, the leaders have consistently deployed these technologies to a higher degree than have the laggards – and by inspection, one can easily see from the *gap* between the two lines which endpoint security technologies have the **strongest correlation with top performance** (e.g., *patch management*, *host-based intrusion detection and prevention*, *secure file transfer*).

Defining Maturity Classes

To distinguish *leading* (top 20%) from *lagging* organizations (bottom 30%) for topics in IT Security, Aberdeen generally uses the following criteria:

- √ Number of actual security-related incidents
- √ Number of audit deficiencies
- √ Operational costs

Respondents with top results based on these criteria earn *leading* or *Best-in-Class* status (for detail see *Related Research*).

Network Security: All Respondents, Leaders and Laggards

Similarly, all (100%) respondents have deployed *network firewalls*, while more than four out of five have also deployed network security technologies such as *email monitoring and filtering* (86%), *web monitoring and filtering* (82%), and *intrusion detection and prevention* (82%). Once again, the leaders have consistently deployed these technologies to a higher degree than have the laggards – and by inspection, one can easily see from the *gap* between the two lines which network security technologies have the **strongest correlation with top performance** (e.g., *intrusion detection and prevention*, *web monitoring and filtering*).

Endpoint Security and Network Security: SMB vs. Large

Figure 2 breaks down respondents by size of company (**SMB** and **Large**), and by companies whose endpoint security and network security strategies are based on a *defense-in-depth approach*, as opposed to an *anti-virus only* or *firewall only* approach. Some immediate observations:

- Twenty-six percent of SMBs report endpoint security consisting solely of an anti-virus / anti-malware solution
- Twenty-one percent of SMBs report network security consisting solely of a firewall

Research Demographics

Aberdeen's study examined more than 160 enterprises, with these demographics:

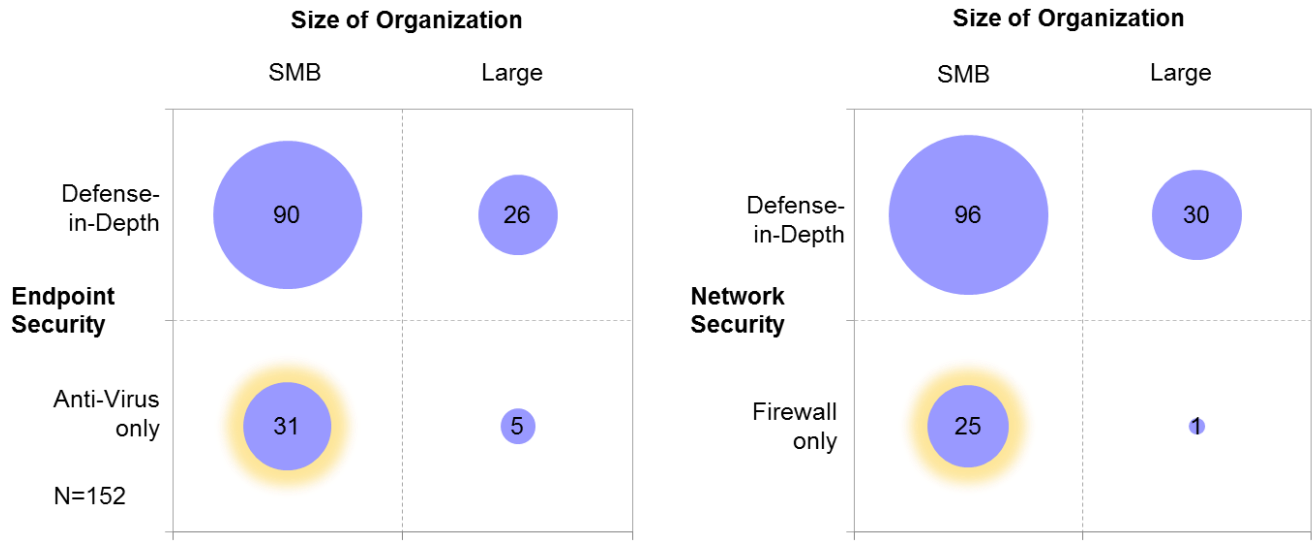
√ **Job title:** C-level management (27%); Vice President (8%); Director (15%); Manager (24%); Staff / Consultant (23%)

√ **Industry:** the largest segments included financial services (17%); government / aerospace / defense (14%); telecommunications (11%); and education (9%)

√ **Geography:** Americas (55%), Europe / Middle East / Africa (29%); all other (16%)

√ **Company size:** Large (20%); Mid-sized (39%); Small (41%)

Figure 2: SMBs are More Likely than Large Enterprises to Implement Anti-Virus, Firewall Only



Note: figures represent the number of respondents for each respective quadrant (not percentages), adding to N=152
Source: Aberdeen Group, January 2013

In contrast:

- Eighty-four percent of large organizations take a defense-in-depth approach to endpoint security, augmenting anti-virus with patch management, secure file transfer and other complementary technologies

- Virtually all large organizations (97%) take a defense-in-depth approach to network security, augmenting firewalls with intrusion detection / prevention, email security, web security and other complementary technologies

We can see that SMBs are much more likely to implement endpoint security consisting solely of anti-virus, and network security consisting solely of a firewall – but are these effective strategies? Can the differences, if any, be quantified? These questions were the motivation for Aberdeen's previously published Analyst Insights noted at right – a summary of which follows below.

Related Research

√ *Network Security: Firewalls Alone are Not Enough* (April 2012)

√ *Endpoint Security: Anti-Virus Alone is Not Enough* (April 2012)

Aberdeen's Analysis: Defense-in-Depth Does Pay Off

For this analysis, Aberdeen compared the 36 companies whose endpoint security is based on anti-virus software alone, e.g., no patch management, etc. (the "**anti-virus group**") – with the 116 companies whose endpoint security includes anti-virus and a range of other endpoint security solutions (the "**defense-in-depth group**"). The leading performers (top 20%) from Aberdeen's benchmark study are also included for reference.

Based on their survey responses, Table 2 summarizes the following averages for these three groups, normalized as a percentage of annual revenue:

- Number of IT Security-related incidents experienced in the last year
- Total cost of IT Security-related incidents – i.e., *costs not avoided* – calculated based on an average cost per incident of $120,000
- Total cost of IT Security initiatives (includes estimates for all related costs for people, process and technologies)

Table 2: Endpoint Security Costs Invested, Costs Not Avoided (Normalized % of Annual Revenue)

Averages per Group (last 12 months), normalized as a percentage of annual revenue	Anti-Virus Group	Defense-in-Depth Group	Leaders (Top 20%)
Total cost of IT Security incidents (costs not avoided) (Note 1)	0.12%	0.09%	0.07%
Total annual cost of IT Security-related initiatives (Note 2)	0.06%	0.06%	0.05%
Total annual investment in IT Security	0.18% 1.5-times higher	0.15% 1.3-times higher	0.12%
Percentage of IT Security-related risk effectively accepted (Note 3)	68%	58%	58%

Note 1: based on an average cost per security incident for this study of $120,000. Industry estimates for these figures can vary dramatically; Aberdeen strongly encourages readers to substitute values which are deemed reasonable for their own organization.
Note 2: includes estimates for all related costs for people, process and technologies
Note 3: calculated as (Costs Not Avoided) / (Costs of Initiatives + Costs Not Avoided)
Source: Aberdeen Group, April 2012

Compared to the leading performers, for example, we can see that the anti-virus-only group actually **spent 1.5-times more in total**. Part of this is due to the anti-virus-only group being *less efficient* – i.e., the leaders

generally tend to manage their IT Security initiatives at higher scale and lower cost. But the biggest difference is due to the anti-virus-only group being *less effective* – i.e., the anti-virus-only group bore the burden of *higher costs not avoided* in comparison to companies who deployed greater defense-in-depth.

Similarly, Aberdeen compared the 26 companies whose network security is based on firewalls alone – e.g., no intrusion detection / prevention, email security, web security, etc. (the "**firewall group**") – with the 126 companies whose security includes firewalls and a range of other network security solutions (the "**defense-in-depth group**"). Table 3 summarizes selected averages for each group, normalized as a percentage of annual revenue.

Table 3: Network Security Costs Invested, Costs Not Avoided (Normalized % of Annual Revenue)

Averages per Group (last 12 months), normalized as a percentage of annual revenue	Firewall Group	Defense-in-Depth Group	Leaders (Top 20%)
Total cost of IT Security incidents (costs not avoided) (Note 1)	0.37%	0.09%	0.07%
Total annual cost of IT Security-related initiatives (Note 2)	0.09%	0.06%	0.05%
Total annual investment in IT Security	0.46% 4.0-times higher	0.15% 1.3-times higher	0.12%
Percentage of IT Security-related risk effectively accepted (Note 3)	81%	58%	58%

Note 1: based on an average cost per security incident for this study of $120,000. Industry estimates for these figures can vary dramatically; Aberdeen strongly encourages readers to substitute values which are deemed reasonable for their own organization.
Note 2: includes estimates for all related costs for people, process and technologies
Note 3: calculated as (Costs Not Avoided) / (Costs of Initiatives + Costs Not Avoided)
Source: Aberdeen Group, April 2012

Comparing again to the leading performers, we can see that the firewall-only group actually **spent 4.0-times more in total**. Part of this is due to the firewall-only group being *less efficient* – i.e., the leaders generally tend to manage their IT Security initiatives at higher scale and lower cost. But the biggest difference is due to the firewall-only group being *less effective* – i.e., the firewall-only group bore the burden of *higher costs not avoided* in comparison to companies who deployed greater defense-in-depth.

Summary and Recommendations

Technology mega-trends (e.g., *social*, *mobile*, *cloud*) are dramatically transforming our IT computing infrastructure with respect to **endpoints**, **networks**, **end-users**, and **back-end systems**. Just like everyone else, small and mid-sized businesses (SMBs) are taking advantage of the compelling benefits of these transformations in their IT computing infrastructure – and struggling at times with the additional complexities that come along with it. But this also means that they must re-think how they deal with the corresponding vulnerabilities, threats and risks. Malware continues to evolve; mobile malware is growing; email and phishing attacks

Analyst Insight: Signature-based

The traditional, *signature-based* approach to protecting against malware is increasingly under stress. Most new malware represents slight variations of previously identified malware, a malevolent engineering process which is repeated continuously by attackers. The traditional approach of determining what is "good" by detecting and subtracting what is known to be "bad" is not being discarded, but increasingly it must be augmented by complementary endpoint security and network security technologies in a *defense-in-depth* approach.

continue to be used effectively to penetrate high-value targets; web sites are increasingly being used as a conduit for delivering malware; and data loss or exposure of sensitive data can be costly. SMBs are not immune from attackers – whether external or internal – because of their size, nor are they exempt from requirements for regulatory compliance.

Even with the many changes in IT computing infrastructure and the corresponding threat landscape, however, what SMB end-users are actually doing hasn't really changed. The vast majority of network traffic is related to **email**, **web** and **file transfer**.

Aberdeen's research shows that SMBs are more likely than larger organizations to implement endpoint security consisting solely of anti-virus (one in four), and network security consisting solely of a firewall (one in five) – but Aberdeen's analysis confirms that these are not effective strategies. On the contrary, compared to the top 20% of all respondents:

- **An anti-virus-only strategy actually resulted in 1.5-times more per year in total cost** related to IT Security. Not investing in additional endpoint security solutions is shown to be a *false economy* – in reality, **the anti-virus-only group is ignoring (and therefore effectively accepting) 68% of the risk** and the associated costs of security-related incidents.
- **A firewall-only strategy actually resulted in 4-times more per year in total cost** related to IT Security. Not investing in additional network security solutions is also shown to be a *false economy* – in reality, **the firewall-only group is ignoring (and therefore effectively accepting) 81% of the risk** and the associated costs of security-related incidents.

Like all organizations, **SMBs should adopt a more comprehensive, defense-in-depth approach** to protecting their endpoints, servers, networks, applications and data. Specifically, *email security*, *web security* and *secure file sharing* should be considered foundational security capabilities for every small and mid-sized business, in addition to *anti-virus* and *firewalls*.

With respect to deployment options, Aberdeen's research has shown that *on-premise* implementations of representative security solutions continue to be 2-times more prevalent than *software-as-a-service* (*SaaS*) deployment models. Planned adoption over the next 12 months for these same solution categories, however, is 4-times more likely to favor SaaS – and on average, more than two-thirds of the planned growth in Security SaaS implementations is from existing on-premise deployments making the switch to the cloud. Why is this? Aberdeen's analysis in higher-growth categories such as *email security*, *web security*, *secure file transfer*, *end-user authentication* and *single sign-on* helps to quantify the advantages that companies have realized in adopting Security SaaS – particularly in the critical areas of **security**, **compliance**, **reliability** and **total annual cost**.

Analyst Insight: On-Premise, or Security Software-as-a-Service?

Aberdeen's analysis has shown that users of *cloud-based* email security and web security solutions had substantially better results than users of *on-premise* implementations. Companies using cloud-based email security experienced:

- √ 47% fewer incidents of spam / malware over the last year
- √ 65% fewer audit deficiencies
- √ 50% less security-related downtime
- √ 11% lower total cost per end-user per year

Companies using cloud-based web security experienced:

- √ 58% fewer malware incidents over the last year
- √ 93% fewer audit deficiencies
- √ 45% less security-related downtime
- √ 45% fewer incidents of data loss or data exposure

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

Related Research	
Evolving Your Datacenter? Evolve Your Datacenter Security; January 2013	*Email and Web Security, Differentiated: Protecting Content is King*; November 2011
Nine Best Practices in IT Security for Mid-sized Companies; October 2012	*To Patch, or Not to Patch? (Not If, But How)*; October 2011
The Virtues of Virtual Patching; October 2012	*Security and Cloud: Adoption of Security Software-as-a-Service*; August 2011
Fighting Fraud with Big Data Visibility and Intelligence; September 2012	*Security and Cloud: Augment, or Abdicate?*; July 2011
The New Breed of Servers: Platforms for Server Virtualization; August 2012	*Is Your Vulnerability Management Program Leaving You at Risk? (Most Likely, Yes)*; June 2011
Successful IT Security Projects Invest Not Only in Technologies, But Also in People; May 2012	*Managing Vulnerabilities and Threats (No, Anti-Virus is Not Enough)*; Dec. 2010
Endpoint Security: Anti-Virus Alone is Not Enough; April 2012	*The State of IT (In)Security, and How to Avoid Costs by Investing More*; November 2010
Network Security: Firewalls Alone are Not Enough; April 2012	*Web Security in the Cloud*; May 2010
Left to Their Own Devices: Does Your Enterprise Have a "Dropbox Problem"?; January 2012	*Email Security in the Cloud*; April 2010

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