

September 2009

## McAfee Users Have Lower TCO for Endpoint Security, Endpoint Management

Aberdeen's benchmark study on *Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence* (March 2009) looked at best practices for keeping enterprise endpoint systems secure, compliant and well-managed, a task nearly always shouldered by a centralized IT group. Analysis of 35 current users of endpoint security and endpoint management solutions from McAfee in comparison with 85 non-McAfee users reveals that McAfee users demonstrated total cost of ownership savings of 21% for endpoint security and 17% for endpoint management.

### Business Context: Keeping Endpoints Clean and Ready

Aberdeen's benchmark study on *Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence* (March 2009) looked at best practices for keeping enterprise endpoint systems secure, compliant and well-managed, a task nearly always shouldered by a centralized IT group. An illustrative list of the enabling technologies which are commonly used in *protecting* and *managing* endpoint systems is provided in Table I. The list is categorized by the primary focus of these technologies with respect to endpoint systems, i.e., on *platforms, networks, applications, or data*. While not necessarily exhaustive, this listing and organization helps to extract several interesting insights when examining the trends in current use of these technologies, as reported by the participants in Aberdeen's study.

#### Research Brief

Aberdeen's Research Briefs provide an exploration of one or more specific findings from a primary research study, including key performance indicators, Best-in-Class insight, and vendor insight.

#### Definitions

For the purposes of this study, the term *endpoint* or *endpoint system* referred generally to end-user computing platforms (e.g., personal computers, workstations, laptops, notebooks, netbooks) and the associated applications, data, and network connectivity on which the end-users depend.

**Table I: Enabling Technologies Commonly Used in Protecting and Managing Endpoint Systems**

	Protect	Manage
<b>Data</b>	<ul style="list-style-type: none"> <li>▪ Full-disk encryption; File / Folder encryption</li> <li>▪ Endpoint device / port controls</li> <li>▪ Data Loss Prevention</li> </ul>	<ul style="list-style-type: none"> <li>▪ Online backup / recovery</li> </ul>
<b>Applications</b>	<ul style="list-style-type: none"> <li>▪ Application controls / application whitelisting</li> </ul>	<ul style="list-style-type: none"> <li>▪ Application virtualization</li> <li>▪ Software distribution</li> <li>▪ Software inventory / usage management</li> </ul>
<b>Networks</b>	<ul style="list-style-type: none"> <li>▪ Personal Firewalls</li> <li>▪ Intrusion Detection / Prevention</li> <li>▪ Network Access Control</li> </ul>	
<b>Platforms</b>	<ul style="list-style-type: none"> <li>▪ Anti-Virus</li> <li>▪ Anti-Spyware</li> <li>▪ Patch Management</li> <li>▪ Configuration / Change Management</li> </ul>	<ul style="list-style-type: none"> <li>▪ IT Asset Management</li> <li>▪ Patch Management</li> <li>▪ Configuration / Change Management</li> </ul>

For example, Figure 1 plots the research findings for *absolute adoption* of these technologies by the leading organizations in the study (i.e., the percentage of Best-in-Class companies indicating current use) versus *relative adoption* by the leaders in comparison to lagging organizations (i.e., the ratio of adoption by Best-in-Class organizations to that of Laggards). The scattergram data naturally lends itself to interpretation as a simple 2-by-2 matrix, with four distinct quadrants:

- **Baseline technologies.** These technologies have been adopted not only by a high percentage of the Best-in-Class, but also by a relatively high percentage of Laggards. In other words, most companies in the study – regardless of their level of performance – have broadly deployed these solutions. *Anti-virus, anti-spyware, intrusion detection / prevention, personal firewalls, patch management, configuration and change management, and software inventory management* solutions fall into the baseline technologies category.
- **Best-in-Class technology early adoption.** Best-in-Class organizations have adopted these technologies less broadly than the baseline technologies in absolute terms, but they have deployed them at a much higher rate relative to Laggards. In the current study, *application virtualization, application controls / application whitelisting, endpoint device / port controls, and network access control* fall into the early adoption category.
- **Best-in-Class technology differentiators.** For these technologies, Best-in-Class organizations have adopted at a high rate – both in absolute terms, and relative to the current adoption by Laggards – making them uniquely and highly correlated with top performance. In the current study *software distribution, IT asset management, and full-disk encryption* solutions fall into the technology differentiators category.
- **Emerging technologies.** Although these technologies have been adopted by Best-in-Class organizations at a higher rate than that of Laggards, in absolute terms the percentage of current use is still modest. Technologies falling into the emerging category in this study include solutions for *data loss prevention and online backup / recovery*.

In broad terms, the findings make it clear that leading organizations have given first priority to protecting and managing their endpoints from the *platforms* and *networks* perspective. Building on this foundation, they are currently focusing on protecting and managing their *applications*. And they are beginning to increase the focus on protecting and managing their *data*. In reference to Table 1, they are implementing from the bottom up.

The findings also make clear that endpoint *security* technologies (particularly from the *platforms* and *networks* perspective) have been made a high priority by virtually all organizations. In other words most companies should and have already deployed these solutions, but by themselves they do not differentiate top performance. Deployment of endpoint *management* solutions, on the other hand, is currently a strongly distinguishing

#### Determining the Best-in-Class

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

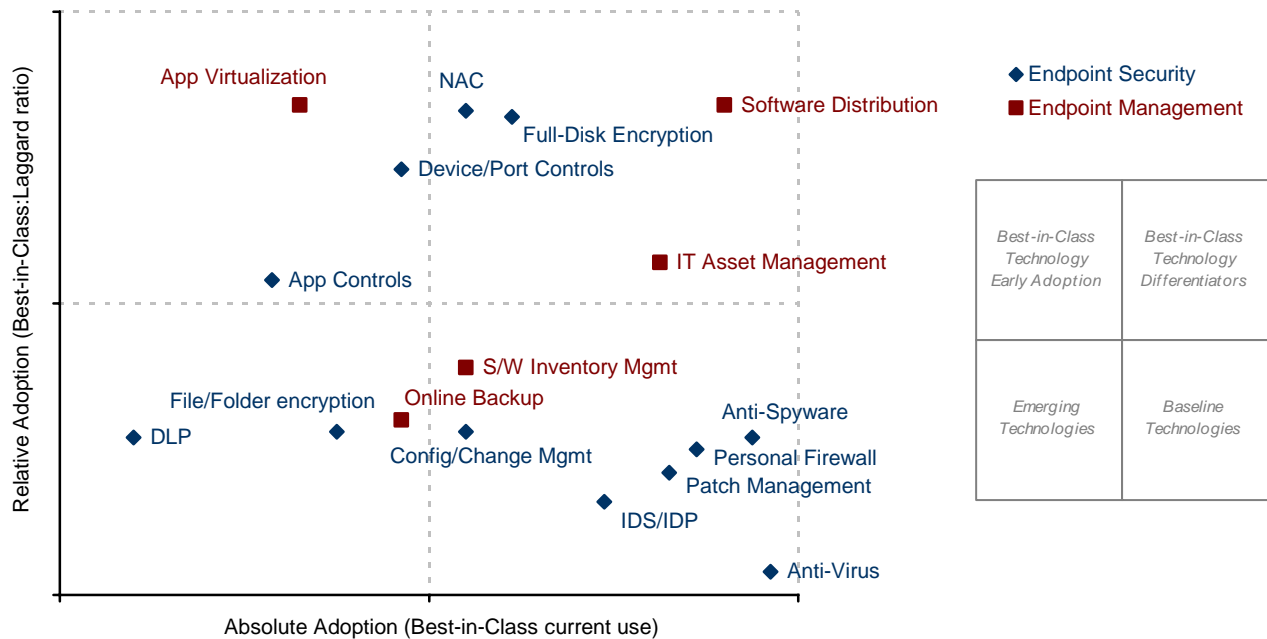
- √ Number of actual security-related incidents related to endpoints
- √ Number of non-compliance incidents (e.g., audit deficiencies) related to endpoints
- √ Total management costs related to endpoints

The first two criteria were selected as measures of an organization's performance in improving security and compliance, while the third was selected as an indicator of operational improvement. In this way, both effectiveness and efficiency were included in the determination of maturity classes for this study.

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

characteristic of the companies achieving Best-in-Class results. With respect to Table 1, they are implementing left to right: well-protected first, then well-managed.

**Figure 1: Best-in-Class Absolute, Relative Adoption of Endpoint Security / Endpoint Management**



Source: Aberdeen Group, March 2009

### What is the TCO of the Average Endpoint System?

One way to appreciate the financial benefits of top performance in protecting and managing endpoints is from the perspective of the average **total cost of ownership (TCO)** per endpoint system (Figure 2). Across all respondents in Aberdeen's *Endpoint Security, Endpoint Management* study, the average replacement cycle for endpoint systems was **3.3 years**, and the average estimate of the total cost of ownership per endpoint over this period was **US\$3,120**. In Table 2, this total amount is broken down into 10 components and presented in terms of the annual cost for each. Observations and insights from these findings include:

- Roughly half (51.3%) of the total cost of ownership per endpoint is in the initial hardware configuration plus software licenses which are incremental to the initial configuration.
- This means that the other half of the total cost of ownership per endpoint is associated with supporting, upgrading, protecting and managing the endpoint system over its useful lifetime ... certainly a worthy target for greater efficiency and cost reduction, especially when multiplied by the entire population of endpoint systems under management.

#### Definitions (continued)

The term *mobile endpoint devices* was used to refer to smart phones, PDAs, USB drives, removable media, hard drives, and other connected devices. An Aberdeen benchmark report planned for 4Q2009 will focus on security for mobile endpoint devices.

For the purposes of this study, the term endpoint did *not* include server systems.

- At least \$114 per endpoint per year (12.1%) is associated with the costs for endpoint security, compliance, and endpoint management. Aberdeen's benchmark research showed that the relative advantage of Best-in-Class performance in these two areas combined, in comparison to the performance of Laggards, translates to approximately **\$50 per endpoint** over the average replacement cycle. Depending on the total number of endpoints in your organization, the cumulative effect of these savings can make a compelling business case for pursuit of best practices in endpoint security and endpoint management.

**Table 2: Breakdown of the Average TCO per Endpoint System**

TCO Component (all respondents)	% of TCO	Annual Cost
Hardware (initial configuration)	30.9%	\$292
Software licenses (incremental to initial config.)	20.4%	\$192
Upgrades (all types, over the average refresh cycle)	8.1%	\$76
Support (from vendors)	5.3%	\$50
Training (all)	7.4%	\$70
Support (internal, e.g., helpdesk)	9.1%	\$85
Reinstall / reimaging / recover	4.9%	\$46
<b>Endpoint Security / Compliance</b>	<b>6.7%</b>	<b>\$63</b>
<b>Endpoint Management</b>	<b>5.4%</b>	<b>\$51</b>
Other	1.9%	\$18
Total	100%	\$943

Source: Aberdeen Group, March 2009

## McAfee Users Enjoy Lower Total Cost of Ownership

Based on the findings from the *Endpoint Security, Endpoint Management* study, 35 current users of endpoint security and endpoint management solutions from **McAfee** ([www.mcafee.com](http://www.mcafee.com)) were analyzed in comparison to 85 non-McAfee users to see if there were any material differences in total cost of ownership (Table 2). Aberdeen's benchmark data shows that in comparison to non-McAfee users, McAfee users demonstrated TCO savings of:

- \$14 per endpoint per year in endpoint security and compliance, or \$46 per endpoint over the average replacement cycle (**20.6% less** than non-McAfee users)
- \$9 per endpoint per year in endpoint management, or \$30 per endpoint over the average replacement cycle (**16.7% less** than non-McAfee users)

- \$23 per endpoint per year in combined endpoint security and endpoint management, or \$76 per endpoint over the average replacement cycle (**18.9% less** than non-McAfee users)

Overall, McAfee users in Aberdeen's dataset spent \$95 less per endpoint per year, or **\$314 less per endpoint** over the average replacement cycle.

**Table 2: McAfee Users Have Lower TCO than Non-McAfee Users**

Annual Cost by TCO Component	McAfee Users	Other Users
Hardware (initial configuration)	\$282	\$297
Software licenses (incremental to initial config.)	\$171	\$204
Upgrades (all types, over the average refresh cycle)	\$82	\$73
Support (from vendors)	\$47	\$53
Training (all)	\$51	\$80
Support (internal, e.g., helpdesk)	\$95	\$80
Reinstall / reimaging / recover	\$44	\$47
<b>Endpoint Security / Compliance</b>	<b>\$54</b>	<b>\$68</b>
<b>Endpoint Management</b>	<b>\$45</b>	<b>\$54</b>
Other	\$11	\$21
<b>Total</b>	<b>\$882</b>	<b>\$977</b>

Source: Aberdeen Group, September 2009

## McAfee Users Deploy a Range of Security Technologies

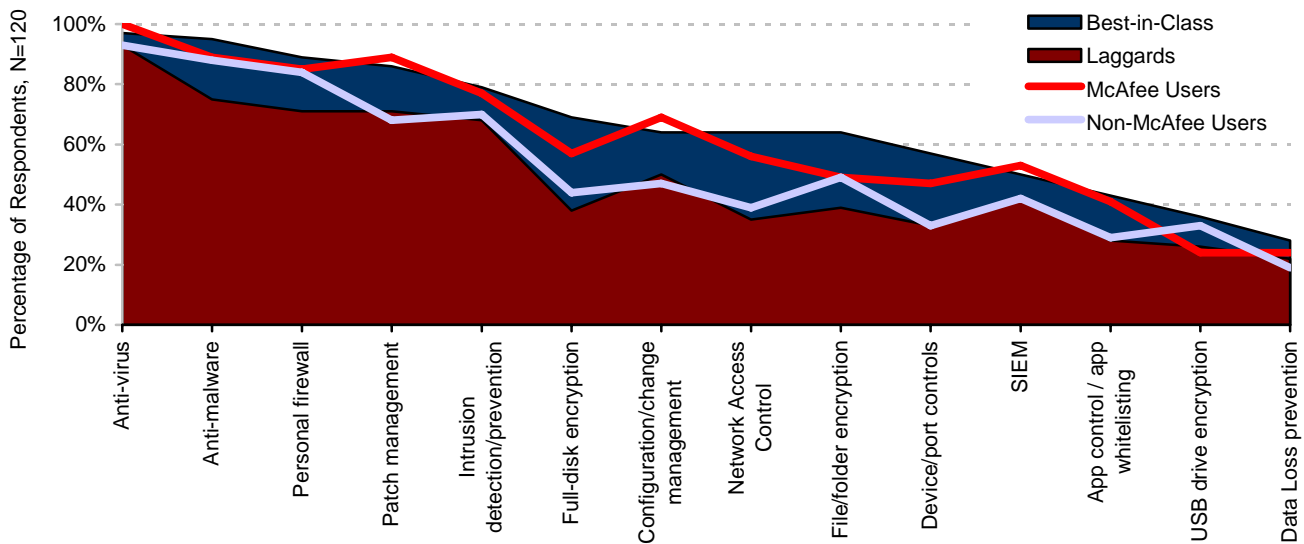
Virtually all organizations have deployed anti-virus solutions; these alone are obviously not enough to drive top results. In Figure 3, the endpoint security technologies currently deployed by McAfee users and non-McAfee users are shown in comparison to deployments by the leading and lagging organizations in Aberdeen's [Endpoint Security, Endpoint Management](#) study.

Inspection of the findings in Figure 3 show the biggest differences between McAfee and non-McAfee users to be in the areas of *patch management, configuration and change management, network access control, endpoint device/port controls, and information and event management*. These are consistent with McAfee's traditional success in addressing vulnerabilities in platforms and networks, ranging from anti-virus, spyware and malware to host intrusion, spam, phishing, and threats to Web 2.0 applications. As one indicator of its expertise, McAfee's global security research team (Avert Labs) identified and reported 1.5 million instances of malware in 2008, and 1.2 million in the first half of 2009.

In the realm of data protection, such as *file/folder encryption, USB drive encryption, and data loss prevention*, McAfee users and non-McAfee users are much closer in terms of current deployments. This is most likely because of the relatively short elapsed time between McAfee's acquisitions of SafeBoot

(November 2007) and Reconnex (August 2008) – for their encryption and data loss prevention solutions, respectively – and the dates of Aberdeen's benchmark survey (March 2009). This can be expected to change over time, as McAfee continues to execute against its mission "to provide the broadest range of solutions, to make it easy for our customers to secure their PCs, networks, mobile phones, and web sites from emerging and known threats."

**Figure 3: Endpoint Security Technologies in Current Use by McAfee, Non-McAfee Users**



Source: Aberdeen Group, September 2009

### Case in Point: Midwestern US Commercial Bank

For nearly 100 years, a Midwestern-based US commercial bank with assets of more than US\$10B has been helping its customers grow, manage and protect their assets. The bank offers a portfolio of financial solutions to privately-held mid-size businesses, as well as to small businesses and individuals who work and live in the communities they serve. Customers bank through more than 80 banking centers located throughout the region, most open seven days a week, as well as through automated services such as Internet banking, online bill payment, and telephone banking.

“As a commercial bank, safeguarding confidential information – especially customer information – is essential,” notes the bank’s Senior Vice President of Information Technology. “We subscribe to a layered approach to security, and securing and managing our endpoint systems is just one of many points of protection.”

The bank’s most recent implementation was a data loss prevention (DLP) solution from their incumbent provider of platform- and network-focused endpoint security solutions. The objective: to help them identify and inventory sensitive data, gain visibility into how confidential data is being

used throughout the corporate network, and implement consistent policies to prevent confidential data from leaving the organization.

Integration with the bank's existing security and management infrastructure was an important technical selection criterion. On the commercial side, the bank also weighed the solution's total cost of ownership – the initial cost, the cost of integration and deployment with existing endpoint systems and infrastructure, and the cost of ongoing operations and support – in comparison to its overall effectiveness.

So far, the bank is satisfied with the effectiveness of the DLP solution. Consistent with its deep Midwestern roots, the bank takes a straightforward, highly practical approach to addressing its endpoint security challenges. "Our philosophy is to identify the issue, find a solution, get on down the road and then loop back when the situation requires it," says the Sr. VP of IT. "We always keep in mind that our goal is to serve the business, and to solve business problems. Too many times, IT can dwell on technologies rather than implement solutions."

## Summary and Recommendations

Aberdeen's research shows that about half of the total cost of ownership of the average enterprise endpoint system is associated with supporting, upgrading, protecting and managing the endpoint system over its useful lifetime. At least \$114 per endpoint per year is associated with the total cost for endpoint security, compliance, and endpoint management. Analysis of 35 current users of endpoint security and endpoint management solutions from McAfee in comparison with 85 non-McAfee users reveals that McAfee users demonstrated total cost of ownership savings of about \$76 per endpoint over the average replacement cycle. To the extent that TCO is a leading decision criterion, buyers should look closely at McAfee's solutions portfolio for endpoint security and endpoint management.

Breadth of solution offerings, such as the product strategies being pursued by the larger category leaders such as McAfee, is another important decision factor. The advanced capabilities of these solutions (e.g., data loss prevention, network access control, asset management, backup and recovery) are designed to address the evolving security needs of the Global 2000, but they may be beyond the immediate needs of many small enterprise customers, and the additional complexity of the management consoles may be an unnecessary burden. As Aberdeen noted in [\*When Less is More: Why Small Companies Should Think Outside the Box for Protecting Endpoints\*](#) (February 2009), it is in this sense that small enterprises interested primarily in anti-virus / anti-malware solutions have also had success with smaller, more focused endpoint security vendors.

For more information on this or other research topics, please visit  
[www.aberdeen.com](http://www.aberdeen.com).

Related Research	
<a href="#"><u>Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence</u></a> ; March 2009	<a href="#"><u>Enterprise Rights Management: Persistence Pays Off</u></a> ; August 2009
<a href="#"><u>Leveraging Logs, Information and Events: Three Use Cases for What to Do with All That Data</u></a> ; March 2009	<a href="#"><u>Microsoft SharePoint: The Comedy (and Tragedy) of the Commons</u></a> ; July 2009
<a href="#"><u>When Less is More: Why Small Companies Should Think Outside the Box for Protecting Endpoints</u></a> ; February 2009	<a href="#"><u>The Cost-Based Business Case for DLP</u></a> ; June 2009
<a href="#"><u>Managing Encryption: The Keys to Your Success</u></a> ; October 2008	<a href="#"><u>Securing Unstructured Data: How Best-in-Class Companies Manage to Serve and Protect</u></a> ; June 2009
<a href="#"><u>Unified Threat Management</u></a> ; September 2008	<a href="#"><u>Shavlik Integrates Sunbelt Software Technology: Keeping Endpoints Secure, Compliant and Well-Managed</u></a> ; May 2009
<a href="#"><u>Vulnerability Management: Assess, Prioritize, Remediate, Repeat</u></a> ; July 2008	<a href="#"><u>Secure, Compliant and Well-Managed: The IT Security Approach to GRC</u></a> ; February 2009
<a href="#"><u>PCI DSS and Protecting Cardholder Data</u></a> ; June 2008	<a href="#"><u>Data Loss Prevention: Little Leaks Sink the Ship</u></a> ; June 2008
Author: Derek E. Brink, Vice President and Research Fellow, IT Security ( <a href="mailto:Derek.Brink@aberdeen.com">Derek.Brink@aberdeen.com</a> )	

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>

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc. (071309b)