

When Less is More: Why Small Companies Should Think Outside the (Red / Yellow) Box for Protecting Endpoints

Endpoint security issues simply can't be ignored, regardless of the size of the organization. Small enterprises in particular often need to "do more with less" when it comes to protecting their endpoints from Internet-based threats and vulnerabilities. Based on Aberdeen's July research on *Vulnerability Management*, organizations with up to 1,000 users should make an explicit decision about selecting the best endpoint security solution for their current problems, rather than unnecessarily taking on by default the potential complexities, higher costs, or negative performance impact of anti-malware solutions from better-known providers such as McAfee and Symantec.

Business Context – Vulnerabilities Affect Us All

Size doesn't matter: any organization whose business operations involve networks, computers, and application software is at risk due to vulnerabilities in these assets that can potentially be exploited, leading to unauthorized access, exposure of sensitive data, disruption of services, or failure to comply with regulatory requirements. Vulnerabilities in computing infrastructure stem from many sources, including software defects, improper configurations, and simple human error. Small enterprises are just as susceptible to these threats and vulnerabilities – including *viruses, worms, Trojans, spyware, adware, bots* and *rootkits*, to name a few – as any other Internet-connected organization.

The quantity, diversity, and sources of software being installed at the endpoints exacerbate the problem. About half of all respondents in Aberdeen's recent benchmark studies reported a year-over-year increase in the average number of software agents installed and managed on endpoint devices, with no statistically meaningful differences between top performers and lagging performers in this regard. And this does not include the many applications, add-ins, players, readers, gadgets, toolbars and other endpoint software installed and "managed" unofficially by the end-users. Anecdotal conversations with organizations of all sizes indicate a growing concern in general over *software "bloat"* at the endpoints, the additional security risks it creates, and especially its negative impact on endpoint performance.

Although in many ways organizations of all sizes are the same, in certain important aspects the small enterprises are sharply different:

- Small businesses are **much more likely to "go it alone"** with their limited in-house resources. For example, 70% of small enterprises indicated that they do *not* use outside vendors or

Sector Insight

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

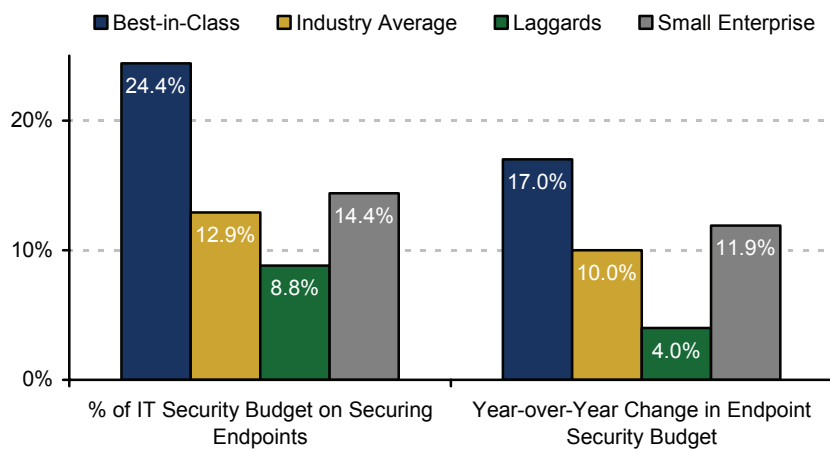
Sector Definition

For purposes of this Sector Insight, "small enterprise" was analyzed as organizations with up to 1,000 users, and as those with <\$50M in annual revenue, with substantially the same results. In this context, small enterprise includes not only many thousands of private sector companies, but also thousands of state and local government and educational institutions.

consultants as part of their approach to protecting their endpoints, as compared to about 50% of the companies with top results.

- Relative to other activities, small businesses **place a lower than average priority** on protecting their endpoints. For example, on a scale of 1 (lowest) to 5 (highest), small enterprises ranked endpoint security at 3.03, as compared to a rating of 3.20 by the top companies and 2.97 by those with relatively worst results.
- Small businesses are actually **spending more than the Industry Average** on protecting their endpoints, not only as a percentage of total IT security budget, but also in terms of year-over-year increase (Figure 1).

Figure 1: Small Enterprises are Spending More than the Average



Source: Aberdeen Group, February 2009

Small enterprises are spending more, but has it led to better results? Unfortunately, the small enterprises in Aberdeen's benchmark research were found to be below the Industry Average in most aspects of security and compliance, and well below the leading companies across the board. Figure 2 and Figure 3 present the average year-over-year change reported by respondents in the study for selected security- and compliance-related metrics, respectively indicating the responsiveness and effectiveness of their endpoint security activities. In this case, Best-in-Class results are represented by a year-over-year *decrease*, while a year-over-year *increase* is indicative of Laggard performance. The relative outcomes of the Industry Average and Small Enterprises are shown as a colored bar, with worse results indicated by the color red and better results indicated by green. Examination of Figure 2 and Figure 3 illustrates that small enterprises in Aberdeen's benchmarks were:

- Below the Industry Average in terms of time to identify and address threats and vulnerabilities

Maturity Class Definitions

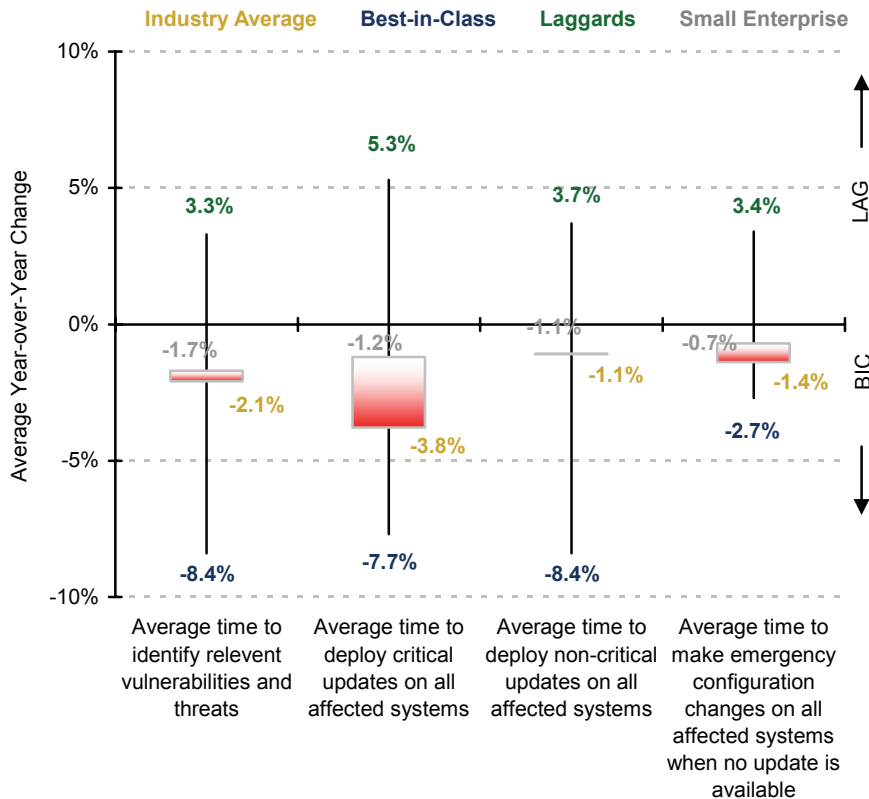
To distinguish Best-in-Class companies from Industry Average and Laggard organizations, Aberdeen used the year-over-year change in the following criteria:

- ✓ Average time to identify relevant vulnerabilities and threats
- ✓ Average time to deploy critical updates to all affected systems
- ✓ Average time to make emergency configuration changes on all affected systems when no update is available
- ✓ Total number of penetration incidents
- ✓ Total number of data loss incidents

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

- Above the Industry Average (but well below the level of the Best-in-Class) in terms of the number of penetration incidents or data loss incidents
- Below the Industry Average in terms of audit deficiencies related to compliance requirements

Figure 2: Small Enterprises are Below Average in Responsiveness



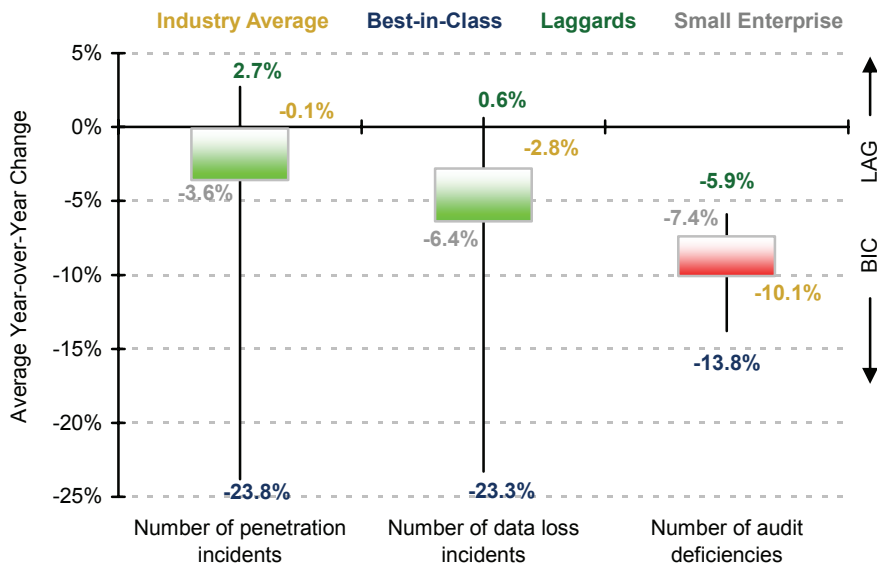
"The scanning time for our incumbent antivirus solution was unacceptable, and it was a resource hog especially on some of our older machines. We needed a solution that was more streamlined."

~ Kerry Kirk,
 VP of Information Technology
 HCSB, a Texas-based State
 Banking Association

Source: Aberdeen Group, February 2009

To be clear, the selection and deployment of the optimal solution from a credible vendor is obviously a key success factor for protecting an organization's IT infrastructure from the never-ending flow of new threats and vulnerabilities. As important as the solution itself, however, are the important choices to be made in terms of policy, planning, process, and organizational elements of implementation and ongoing management. As a whole, each organization's unique blend of "people, process and technology" is the key to their ability to manage vulnerabilities in a sustainable, cost-effective way. Solutions whose features can reduce or remove inefficiencies in these areas have the tangible benefits of being faster to get up and running, and more cost-effective to support and manage over time.

Figure 3: Small Enterprises Need Large Gains in Effectiveness



Source: Aberdeen Group, February 2009

Benchmarking the Small Enterprise: What They Want

What are the leading drivers for investments made by small enterprises in protecting their endpoints from network-based vulnerabilities and threats? Relative to the Best-in-Class, Aberdeen's research shows that smaller enterprises indicated stronger focus on the pressures of **keeping the business up and running** and **protecting their IT infrastructure**, and less focus on pressures related to compliance and data protection. In the IT security version of Maslow's hierarchy of needs, the research indicates that small enterprises are focused heavily on the base of the pyramid.

In terms of their strategic responses to these pressures, small enterprises and Best-in-Class organizations indicated similar approaches for protecting their endpoints, for example, conducting regular vulnerability assessment scans and implementing consistent policies and procedures for managing threats and vulnerabilities. Unfortunately, good strategy is not always linked to good execution. Best-in-Class organizations were about 1.4-times more likely than small enterprises (87% versus 67%) to indicate regular vulnerability scans as a current capability, and about 1.7-times more likely (70% versus 41%) to have consistent threat and vulnerability management policies in place.

Examining the *inhibitors* to investments in endpoint security shows that the perceived **absence of compliance as a driver** – the number one inhibitor indicated by small enterprises in the study – often means “do not invest.” The second leading inhibitor (and the greatest gap between small enterprises and all respondents) was **lack of in-house IT skill sets**. This should not be taken as IT staff in small companies being less capable, of course, but rather that in most small companies they tend to be jacks-of-all-

"A key consideration, which I think is as important as all the others, is tech support. That alone is reason enough for serious purchase consideration. Technicians that communicate well and that really do stay with you until the problem is solved are invaluable."

~ Kerry Kirk,
VP of Information Technology
HCSB, a Texas-based State
Banking Association

trades as opposed to the more highly-specialized roles to be found in larger organizations. When one combines the lack of in-house expertise with the fact that small enterprises are more inclined to go it alone, it seems clear that many small enterprises are not doing more with less, but doing less with less.

The inhibitor representing the second greatest gap between small enterprises and all respondents was **no financial loss expected**. Both industry headlines and Aberdeen's benchmark research consistently indicate otherwise, pointing to a high need for additional awareness and education about the probability and financial impact of a material incident. But overall the profile is consistent: small businesses are most likely to invest to keep the business running, if they are compelled to do so (compliance), or if they expect non-investment to cost them money.

Selection Criteria for Endpoint Security Solutions / Vendors

Small companies participating in Aberdeen's benchmark research placed the highest priority for selection criteria on **total cost of ownership** – which includes not only the cost of acquisition, but also the cost of deployment and the cost of ongoing management – by a factor of 1.6-times more than the Best-in-Class (Figure 4). Although acquisition costs are easiest for making a direct comparison, Aberdeen's research consistently shows that top results are actually gained (or not) by top performance in deployment and ongoing management. For the typical small enterprise, solutions that are effective and simplest to manage should be given strong consideration.

Solution providers with **domain expertise, demonstrated success** in similar projects, and commitment to **customer service** are valued highly by all respondents, including the small enterprise. Small organizations also place relatively higher value on **recommendations made by their peers**.

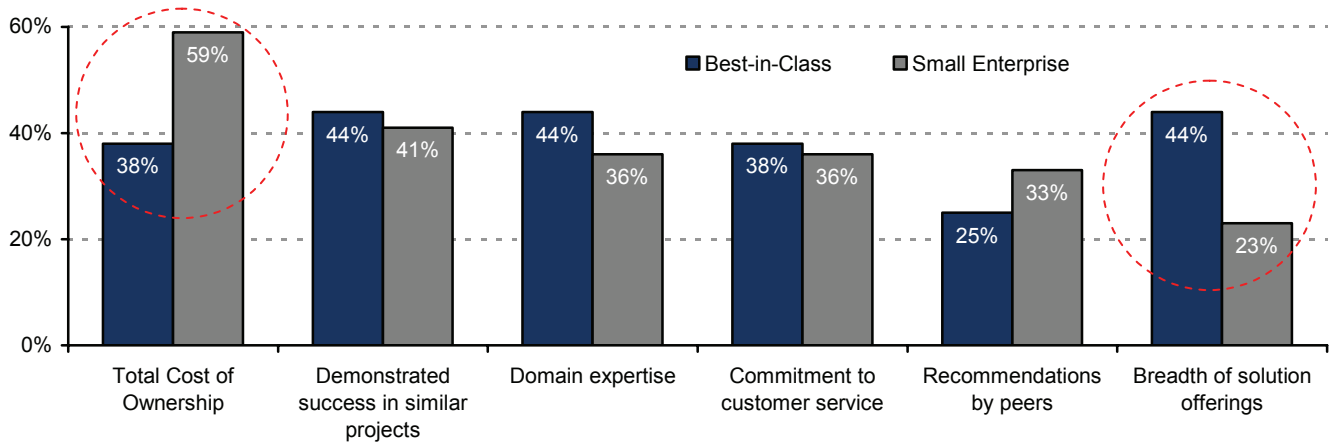
Figure 4 also illustrates that **breadth of solution offerings**, such as the product strategies being pursued by the larger category leaders such as McAfee and Symantec, is **much less important** to small businesses. The advanced capabilities of these solutions (e.g., data loss prevention, network access control, asset management, backup and recovery) are addressing the evolving security needs of the Global 2000, but they are beyond the immediate needs of many small enterprise customers, and the additional complexity of the management consoles is an unnecessary burden. It is in this sense that small enterprises focused on anti-virus / anti-malware solutions should think outside the red and yellow boxes of the respective market leaders, and give deliberate consideration to smaller, more focused endpoint security vendors (for an illustrative solutions landscape, see Table I).

Solution Selection Criteria

Based on the research, the following selection criteria for endpoint security (anti-virus, anti-malware) solutions are valued most highly by small companies:

- √ Cost to acquire
- √ Cost and time to deploy
- √ Cost of ongoing operations
- √ "Footprint" of software at the endpoints, particularly in terms of its impact on resources required and endpoint performance
- √ Expertise and customer service of the solution provider

Figure 4: What Small Businesses Look For in Solutions / Vendors



Source: Aberdeen Group, February 2009

Case in Point

Colonial Mills, Inc. (CMI), based in Pawtucket, Rhode Island, combines "old school craftsmanship" with "new age innovation" to produce braided-texture products such as area rugs, accessories, and custom designs with superior customer service. The company manufactures its award-winning products near the historic Slater Mill (circa 1793) in the Blackstone River Valley, considered to be the birthplace of the American textile industry.

CMI has worked hard to drive new efficiencies in a well-established manufacturing process, by aligning its efforts across departments using "lean manufacturing" techniques, in which new orders are typically shipped within 5 days. CMI has made significant investments in technologies to improve its capabilities in order processing and customer relationship management, including real-time queries of order status.

In such a lean, focused IT environment, CMI could ill afford the lost productivity caused by excessive viruses, spyware, and other malware attacking their endpoints. At the same time, they could not afford the lost productivity caused by the performance of their initial endpoint security solution. "When a scan would kick off with our previous installation of Symantec Corporate Edition, the PC would be sooo slow," said Bill Turgeon, Chief Information Officer for Colonial Mills. After evaluating solutions from both Symantec and McAfee, CMI ultimately selected VIPRE Enterprise from Sunbelt Software, with positive results. "With VIPRE, our users don't even realize the scan is taking place," said Turgeon.

"When a scan would kick off with our previous installation of Symantec Corporate Edition, the PC would be sooo slow. With [Sunbelt Software's] VIPRE, our users don't even realize the scan is taking place."

~ Bill Turgeon,
Chief Information Officer
Colonial Mills, Inc.

For CMI, the most importance decision criteria were a combination of performance and price. "We are a small business, with 65 users and a very small budget," notes Turgeon. "For anti-virus / anti-spyware, the VIPRE product simply outperformed the others. The fact that it was about one-half the price was a bonus. Sometimes the 'big players' are not the best solution

for our environment." Performance is "no longer a problem" at Colonial Mills, and disruption due to viruses has been virtually non-existent.

Sunbelt's commitment to customer service was also an important element of CMI's decision to go with a smaller provider. "Previously, I would be on hold for long periods, waiting for technical assistance," said Turgeon. "I no longer have that issue with Sunbelt, which has done a great job of communicating with us about new releases. They make it very easy to want to do business with them."

Solutions Landscape

Solution providers for endpoint security can range from smaller specialists to multi-billion dollar firms. Table I provides an illustrative list.

Table I: Solutions Landscape for Endpoint Security (illustrative)

Company	Solution(s)	Description
Sunbelt Software www.sunbelt-software.com	VIPRE Enterprise	Sunbelt Software's VIPRE Enterprise combines anti-virus, anti-spyware, anti-rootkit and other endpoint security technologies in a single integrated product, designed "by admins for admins" to be a clean, fast, and powerful anti-malware solution for the small enterprise.
	Sunbelt Network Security Inspector	The Sunbelt Network Security Inspector is a low-cost network vulnerability scanner, supporting over 4,000 ranked vulnerabilities across Windows, Mac OS X, Unix and Linux.
AVG Technologies www.avg.com	AVG Internet Security Network Edition	The AVG Internet Security Network Edition solution provides anti-virus, anti-spyware, anti-rootkit and other security technologies for protecting the endpoints. The solution includes a real-time vulnerability scanner and automatic updates to ensure continuous protection.
McAfee www.mcafee.com	Total Protection for Endpoint	McAfee Total Protection for Endpoint combines McAfee endpoint security technologies, ongoing research into emerging threats, and scalable management from a single console. Advanced compliance features limit access to non-compliant systems, automate reporting, and integrate with third-party compliance tools.
	ePolicy Orchestrator	McAfee ePolicy Orchestrator is designed to be a central hub for managing multiple layers of protection, enforcing policy, monitoring security status, making updates, and generating detailed graphical reports.
Symantec www.symantec.com	Endpoint Protection 11.0	Symantec Endpoint Protection 11.0 integrates anti-virus, anti-spyware, personal firewall, intrusion prevention, device control, and application control in a single agent managed by a single management console.
	Endpoint Management Suite 1.0	Symantec Endpoint Management Suite 1.0 is designed around a common architecture to support security, system management, and recovery functionality for advanced automation, system interoperability, and increased visibility and control for Windows-based endpoints.

Source: Aberdeen Group, February 2009

Summary and Recommendations

Based on Aberdeen's benchmark research and interviews with select respondents, small enterprises should consider the following:

- **Make endpoint security a priority.** It may not be pleasant, but managing the threats and vulnerabilities that put your endpoints at risk is a necessary function for any organization with business operations that involve Internet-facing networks, computers, and application software. Improving capabilities in all three phases of the vulnerability management lifecycle (i.e., "assess," "prioritize," and "remediate") pays off in two ways. First, it reduces the risks and costs associated with the flood of new threats and vulnerabilities that emerge on a weekly basis. Second, it reduces the total costs of managing threats and vulnerabilities and protecting the endpoints, which frees up limited resources to invest in more strategic IT initiatives.
- **Optimize your limited resources.** Most small organizations don't have a large or dedicated IT staff, and the research shows that in spite of having limited internal resources they tend to "go it alone". Small enterprises should make an explicit decision about selecting the best endpoint security solution for their current problems, rather than taking on by default the unnecessary complexities, cost, and performance-crippling bloat of solutions that provide more functionality than the organization currently needs.
- **Think outside the (red / yellow) box.** Small organizations should be open to endpoint security solutions from vendors other than McAfee and Symantec, especially those that address the key selection criteria identified in the research: total cost of ownership, domain expertise / demonstrated success in similar projects, minimal footprint and impact on performance, and commitment to customer service.

Endpoint security issues simply can't be ignored, regardless of the size of the organization. In a tough economy, small enterprises in particular need to "do more with less" when it comes to protecting their endpoints from Internet-based threats and vulnerabilities. The research shows that they can compete most effectively by consciously choosing the right tool for the job.

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

"It was a wonderful thing to find a nice tight little footprint that doesn't kill our client systems while scanning."

~ Bill Turgeon,
Chief Information Officer
Colonial Mills, Inc.

"You don't always have to go with the 'big guys' for software. After working with several very large vendors in the past, working with a smaller provider [Sunbelt Software] has been a breath of fresh air."

~ Kerry Kirk,
VP of Information Technology
HCSB, a Texas-based state
banking association

Related Research

[Unified Threat Management: What's In, What's Next, and Why](#); September 2008

[Vulnerability Management: Assess, Prioritize, Remediate, Repeat](#); July 2008

[Data Loss Prevention: Little Leaks Sink the Ship](#); June 2008

[PCI DSS and Protecting Cardholder Data](#); June 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>

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. 043008a