Aberdeen Group
A Harte-Hanks Company

Endpoint Security, Endpoint Management

The Cost-Cutter's Case for Convergence

March 2009

Derek Brink

Aberdeen Group
A Harte-Hanks Company

Executive Summary

This benchmark report is for any organization that relies upon end-user computing platforms (e.g., personal computers, workstations, laptops, notebooks) – and their associated applications, data, and network connectivity – to carry out strategic business objectives. It describes how the companies with top results keep these endpoints "clean and ready."

Best-in-Class Performance

To distinguish Best-in-Class companies from Industry Average and Laggard organizations in protecting and managing endpoints, Aberdeen used the year-over-year changes in the following performance criteria related to their endpoint systems:

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

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

Competitive Maturity Assessment

Survey results show that the firms enjoying Best-in-Class performance in protecting and management their endpoint systems shared several common characteristics, including the following:

- 93% have consistent policies for supported application software / licenses at the endpoints
- 85% have accurate inventory, tracking and reporting of supported application software / licenses and endpoint assets
- 77% have systematic implementation / rollout processes for endpoint software, updates, and configurations
- 64% have standardized responses for endpoint-related exceptions, security events, or incidents of non-compliance
- 54% have visibility into the current state / posture of the endpoint systems under management
- More than 80% have deployed anti-virus, anti-malware, personal firewalls, intrusion detection / intrusion prevention, patch management, software distribution, and IT asset management technologies

Recommended Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class status companies should focus first on the security of its endpoint systems, then on compliance, then on optimizing ongoing management for greater efficiency and lower cost.

Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth look into process, procedure, methodologies, and technologies; identify best practices; and make actionable recommendations

"Years ago we had a baseball coach who always used to tell us, 'If you *stay* ready, you don't have to *get* ready.' It meant that we shouldn't be wasting time or making mistakes because of something we were supposed to be doing anyway. Always be in the ready position; always be thinking ahead to the next play. I've always remembered that. I think the same thing applies to dealing with our endpoint systems: if we *stay* secure, we don't have to *get* secure. If we *stay* in control of our assets, we don't have to *get* in control of our assets. It takes more discipline, but in the long run everything works better and costs less."

~ IT Administrator,
Small (<$50M) Consulting / Services Firm

Aberdeen Group
A Harte-Hanks Company

Table of Contents

Figures

Tables

Aberdeen Group
A Harte-Hanks Company

Chapter One:
Benchmarking the Best-in-Class

Business Context: The Rifleman's Creed

Ask any member of the United States Marine Corps, active or retired, about the relationship between a marine and his rifle, and chances are that they will respond immediately with words that include the following:

- *This is my rifle. There are many like it, but this one is mine.*
- *My rifle is my best friend. It is my life. I must master it as I master my life.*
- *My rifle, without me, is useless. Without my rifle, I am useless.*
- *My rifle and I know that what counts is not the rounds we fire, the noise of our burst, or the smoke we make. We know that it is the hits that count.*
- *I will keep my rifle clean and ready, even as I am clean and ready.*

The full text, known as *The Rifleman's Creed,* is attributed to Major General William H. Rupertus and dates from late 1941 or early 1942. It is deeply engrained in the doctrine of the US Marine Corps and in the basic training of every marine.

How does calling this imagery to mind serve as an introduction to a benchmark study on protecting and managing endpoint systems? Because the core sentiments expressed in *The Rifleman's Creed* about the relationship between a marine and his rifle are analogous to the relationship between an organization's end-users and their respective endpoint systems. For the purposes of this study, the term endpoint or endpoint system refers generally to end-user computing platforms (e.g., personal computers, workstations, laptops, notebooks) and the associated applications, data, and network connectivity on which the end-users depend. The analogies to consider include:

- An enterprise has many endpoints, which may be similar in type and configuration, but the most common use case is that there is a specific endpoint system for a specific end-user.
- To master his work life, each user must master his endpoint system.
- Endpoints without end-users are useless. End-users without their endpoint systems are "useless," or presumably much less productive.
- What counts is not the volume of activities generated with the endpoints, but the achievement of the company's objectives through the work product of the individuals who use the endpoint systems. As one hard-driving high-tech CEO put it, "Let us not confuse activity with results."

Fast Facts

Year-over-year changes affecting the number of endpoints to protect and manage (all respondents):

√ Number of employees accessing protected resources: +6.7%

√ Number of authorized network users: +5.9%

√ Number of mobile / remote users: +8.7%

√ Number of wireless users: +7.5%

Definitions:

Where specifically noted, the term "endpoint" may also include *mobile endpoint devices* such as smart phones, PDAs, USB drives, removable media, hard drives, and other connected devices. A future Aberdeen benchmark report will focus on security for mobile endpoint devices.

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

- Endpoint systems are indispensable tools, and these tools should be kept clean and ready for use – or in the context of this benchmark report, endpoints should be kept **secure**, **compliant** and **well-managed**.

Endpoint Security, Endpoint Management

One important difference between the end-user and his endpoint system, in comparison to the marine and his rifle, is that each marine takes personal and individual responsibility to keep his weapon "clean and ready." In the typical enterprise, the burden for keeping endpoint systems secure, compliant and well-managed is nearly always a centralized function shouldered by the IT group. Table 1 provides an illustrative (i.e., not intended to be comprehensive) list of many of the enabling technologies which are commonly used in protecting and managing endpoint systems. The list is further categorized by the primary focus of these technologies with respect to endpoint systems, i.e., on platforms, networks, applications, or data.

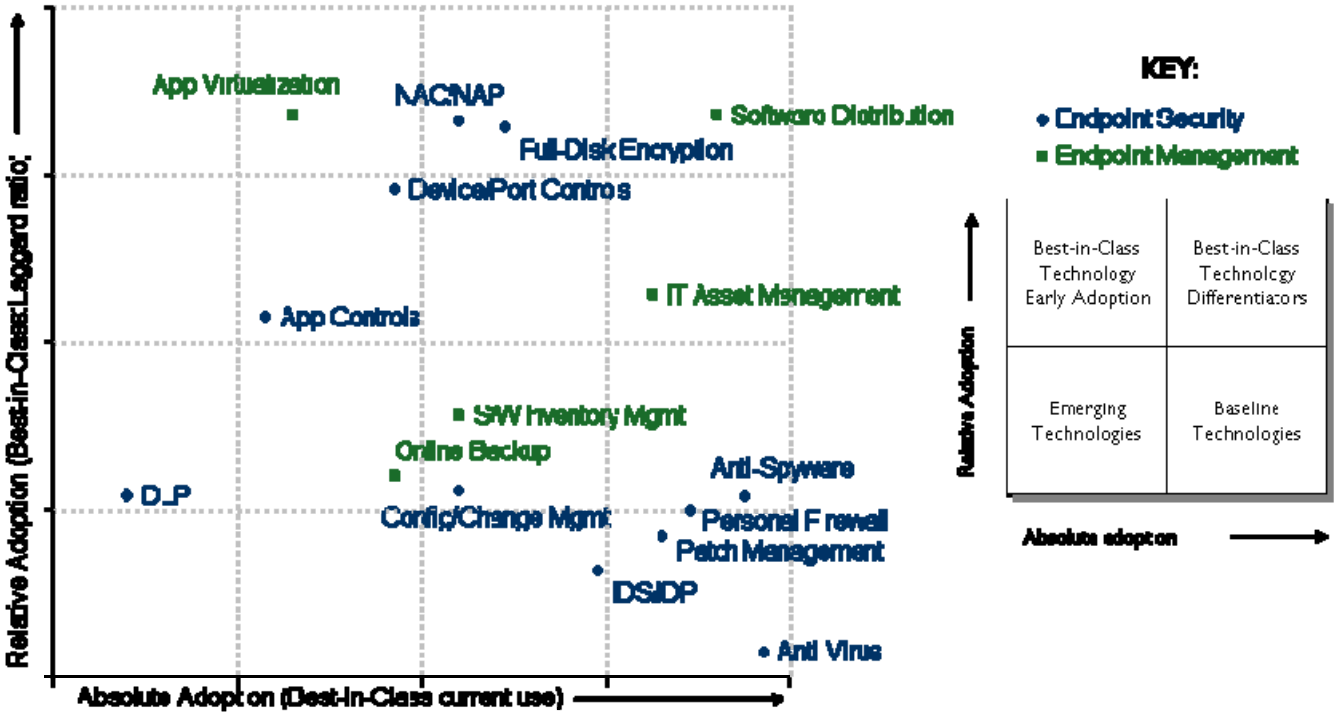
Table 1: Enabling Technologies Commonly Used in Protecting and Managing Endpoint Systems

	Protect	Manage
Data	▪ Full-disk encryption ▪ Endpoint device / port controls ▪ Data Loss Prevention (agent-based)	▪ Online backup / recovery
Applications	▪ Application controls / application whitelisting	▪ Software distribution ▪ Software inventory / usage management ▪ Application virtualization
Networks	▪ Personal Firewalls ▪ Intrusion Detection / Prevention ▪ Network Access Control	
Platforms	▪ Anti-Virus ▪ Anti-Spyware ▪ Patch Management ▪ Configuration / Change Management	▪ IT Asset Management ▪ Configuration / Change Management

Source: Aberdeen Group, March 2009

While not necessarily exhaustive, the listing and organization of the endpoint security and endpoint management technologies as provided in Table 1 helps to extract several interesting insights when examining the trends in current use, as reported by the participants in the current study. For example, Figure 1 plots the research findings for *absolute adoption* by the Best-in-Class (i.e., the percentage of Best-in-Class organizations indicating current use) versus *relative adoption* by the Best-in-Class (i.e., the ratio of adoption by Best-in-Class organizations to that of Laggards).

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



Source: Aberdeen Group, March 2009

Examination of the findings in this format yields the following observations:

- 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.** The 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*.

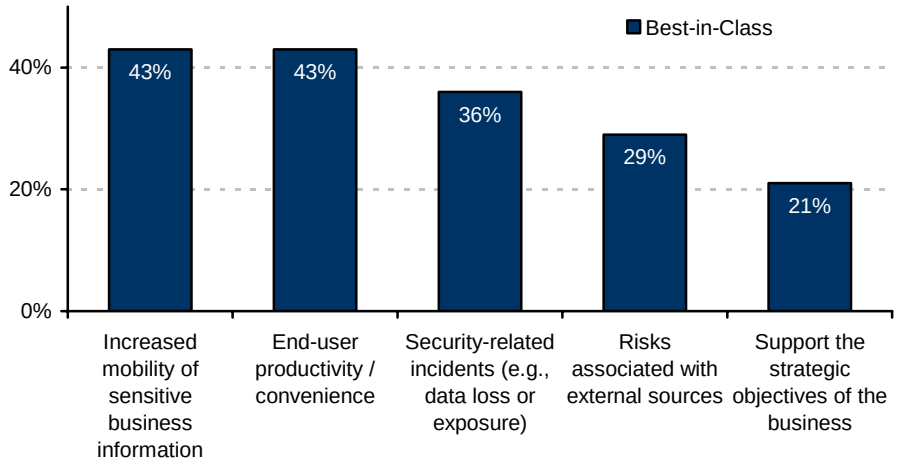
- In broad terms, the findings make it clear that leading organizations have given first priority to protecting and managing their endpoints from the *platform* and *network* perspective. Building on this foundation, they are currently focusing on protecting and managing their *applications*. And they 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 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.
- Best-in-Class companies are currently leading the way as early adopters for endpoint solutions related to protecting and managing their applications, including *application virtualization* and *application controls / application whitelisting*.
- Data-centric solutions, such as *data loss prevention* and *online backup and recovery*, are currently in the emerging category for the companies participating in this study. The exception is *full-disk encryption*, which is currently deployed by a much higher percentage of the Best-in-Class. See Aberdeen's October 2008 report on *Managing Encryption: The Keys to Your Success* for additional insights in this area.

Additional views of the current adoption of endpoint security and endpoint management solutions by the participants in this study are provided in Figure 10 and Figure 11, respectively.

Market Drivers and Inhibitors

The traditional tensions between **managing risk** and **enabling the business** are definitely at play in what currently drives the top performers to invest in protecting and managing their endpoints (Figure 2). Risk-oriented drivers include the *increased mobility of sensitive business information*, *actual security-related incidents* such as data loss or data exposure, and the risks represented by the unrelenting flow of *threats and vulnerabilities* from external sources. Interleaved with these as top drivers are the populist pressure to *increase convenience and productivity* for end-users, and the fundamental desire that endpoint systems contribute to *supporting the strategic objectives* of the business.

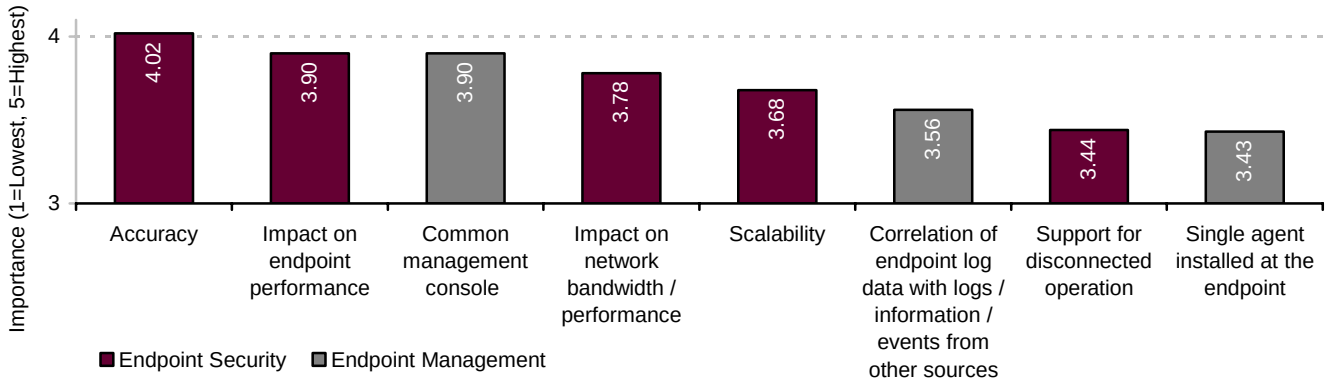
Figure 2: Top Pressures Driving Current Endpoint Investments



Source: Aberdeen Group, March 2009

Leading *inhibitors* to current investments in endpoint security and endpoint management, as identified by all respondents, include the **complexity** of the typical endpoint environment, and the perceived complexity of current endpoint security and endpoint management solutions. Additional inhibitors include the **cost of acquisition** and the **relative priority** of endpoint security and endpoint management solutions in comparison to a full plate of other current initiatives. Both of these latter notions represent opportunities for solution providers to educate buyers about the tangible benefits of successful implementations and Best-in-Class results.

Figure 3: Relative Importance of Endpoint-related Technology Features (all respondents)



Source: Aberdeen Group, March 2009

With respect to the relative importance of various features, **technical capabilities** for endpoint security solutions – such as *accuracy*, *impact on performance*, and *scalability* – top the list (Figure 3). Intertwined but slightly lower on the importance scale are desirable **management capabilities**, such as a *common management console*, *reduced number of software agents*, and *back-end integration*. Consistent with what Aberdeen has seen many times in the thread of its recent IT security research, the current study again provides strong evidence that the general Best-in-Class approach to IT security is to be secure, then compliant, then well-managed … in that order.

Maturity Class Framework: Defining the Best-in-Class

To distinguish Best-in-Class companies from Industry Average and Laggard 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 year-to-year 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, as described in Table 2. (For additional details on the Aberdeen Maturity Class Framework, see Table 7 in Appendix A.)

Aberdeen Group
A Harte-Hanks Company

Table 2: Top Performers Earn Best-in-Class Status

Definition of Maturity Class	Mean Class Performance (year-over-year change)
Best-in-Class: Top 20% of aggregate performance scorers	▪ 3.8% **decrease** in the number of actual security-related incidents related to endpoints ▪ 2.3% **decrease** in the number of audit deficiencies related to endpoints ▪ 1.7% **decrease** in total management costs related to endpoints
Industry Average: Middle 50% of aggregate performance scorers	▪ 0.9% **increase** in the number of actual security-related incidents related to endpoints ▪ 0.8% **decrease** in the number of audit deficiencies related to endpoints ▪ 1.1% **increase** in total management costs related to endpoints
Laggard: Bottom 30% of aggregate performance scorers	▪ 9.7% **increase** in the number of actual security-related incidents related to endpoints ▪ 5.7% **increase** in the number of audit deficiencies related to endpoints ▪ 9.1% **increase** in total management costs related to endpoints

Source: Aberdeen Group, March 2009

The Best-in-Class PACE Model

Using endpoint security and endpoint management solutions to protect and manage endpoints requires a combination of strategic actions, organizational capabilities, and enabling technologies – referred to by Aberdeen as the Best-in-Class PACE Framework (for a description of the Aberdeen PACE Framework, see Table 6 in Appendix A). The characteristics exhibited by Best-in-Class organizations in this study are summarized in Table 3.

Table 3: Best-in-Class PACE Framework for Protecting and Managing Endpoints

Pressures	Actions	Capabilities	Enablers (% of Best-in-Class Adoption)
▪ Increased mobility of sensitive business information ▪ End-user productivity / convenience ▪ Security-related incidents (e.g., data loss or exposure)	▪ Establish and enforce consistent policies and procedures related to endpoints ▪ Educate end-users about endpoint security, compliance, and management policies and practices	▪ Consistent policies for supported application software / licenses at the endpoints ▪ Consistent access policies based on context at the endpoint ▪ Systematic implementation / rollout processes for endpoint software, updates, and configurations ▪ Standardized response for endpoint-related exceptions, security events, or incidents of non-compliance	▪ Anti-virus (97%) ▪ Anti-malware (95%) ▪ Personal firewall (89%) ▪ Intrusion detection / intrusion prevention (79%) ▪ Patch management (86%) ▪ Configuration and change management (64%) ▪ Network access control (64%) ▪ Data Loss Prevention (agent-based) (28%)

Pressures	Actions	Capabilities	Enablers (% of Best-in-Class Adoption)
	▪ Strive towards common security and management solutions for all endpoints ▪ Augment existing endpoint security solutions with centralized management	▪ Responsible executive or team with primary ownership for security, compliance and management of endpoint systems ▪ Documented workflow for endpoint provisioning / deployment ▪ Inventory, tracking and reporting of supported application software / licenses and endpoint assets ▪ Visibility into current state / posture of endpoint systems under management ▪ Standardized endpoint systems, standardized endpoint configurations ▪ Pre-packaging of endpoint software / configurations before deployment ▪ Automated endpoint provisioning / deployment process	▪ Software distribution (92%) ▪ IT asset management (85%) ▪ Software inventory / usage management (64%) ▪ Online backup and recovery (57%) ▪ Application virtualization (46%)

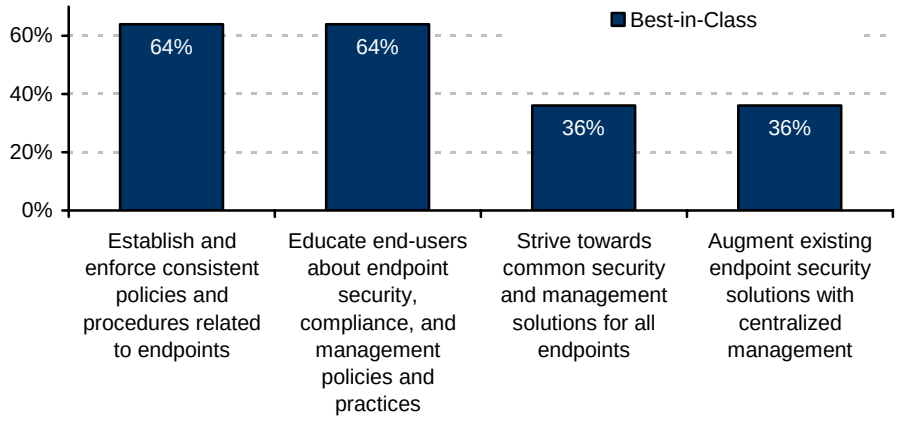
Source: Aberdeen Group, March 2009

Best-in-Class Strategies and Results

The dominant strategies indicated by the companies with top performance are to **establish consistent policies** and procedures related to their endpoint systems, and to **educate their end-users** about endpoint security, compliance and management (Figure 4). In many ways, this is again reminiscent of *The Rifleman's Creed* in terms of the concept of "clean and ready" becoming deeply ingrained in the corporate culture.

Compared to all respondents, the Best-in-Class companies in the study are about 11% more likely to strive for an integrated security and management solution for all endpoints, as opposed to implementing endpoint security and management solutions deemed most appropriate for the immediate problem at hand. This long-arching trend towards a "platform" approach, versus the perpetuation of existing, independently-managed "silos," is another characteristic of the Best-in-Class that repeats itself consistently in the thread of Aberdeen's IT security research.

Figure 4: Top Strategies Driving Current Endpoint Investments



Source: Aberdeen Group, March 2009

Security/Management Integration: The Cost-Cutter's Case

The research shows that Best-in-Class organizations have reduced the costs related to endpoint security and endpoint management in several ways, including year-over-year reductions in:

- The number of security incidents related to endpoints, and the average time and cost to identify and address them
- The number of audit deficiencies related to endpoints, and the average time and cost to address them
- Factors related to management costs on the end-user side of the ledger, including human error, help desk calls and end-user disruption due to endpoint-related downtime
- Factors related to management costs on the administrative side, including the total number of full-time equivalent staff, time spent on administrative tasks, and time spent on analysis and reporting

Table 4 summarizes the *annual advantage* enjoyed by the Best-in-Class, in comparison to Laggards, based on the average year-over-year changes in key performance indicators such as these. For each metric in Table 4, it should be straightforward for any individual company to estimate an approximate dollar amount to be gained by achieving Best-in-Class performance in that area.

Why does each company have to make an individual calculation? Suppose the research showed that installation of an energy-saving heating system would cut your home heating bill by 14% – this has much greater impact for those who live in New Hampshire, where winters are cold and energy costs are high, than for those who live in Arizona. Likewise, saving 11% annually on the cost of heating an outdoor swimming pool means one thing in the north of England, and another in the south of France. Thus, individual context matters.

Table 4: Benefits of Being Secure, Compliant and Well-Managed

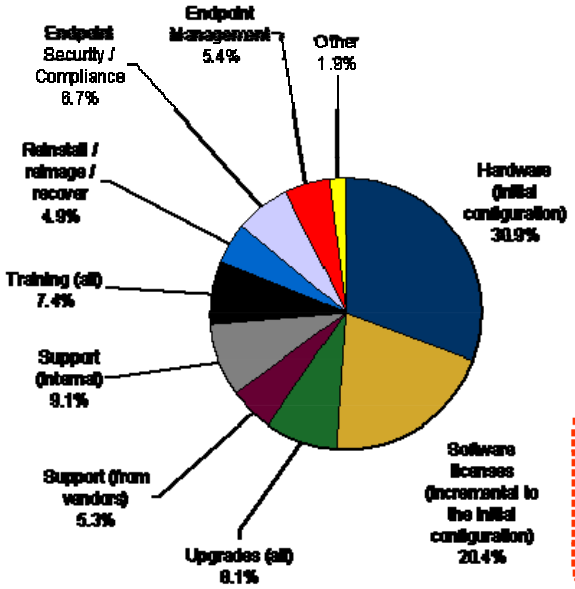
Key Performance Indicators (average year-over-year change)	Best-in-Class Annual Advantage
Number of actual security-related incidents	13.5%
Average time to identify security-related incidents	3.2%
Average time to address security-related incidents	6.8%
Total cost of addressing security-related incidents	9.3%
Number of non-compliance incidents	8.0%
Average time to identify non-compliance incidents	4.6%
Total cost of addressing non-compliance incidents	6.0%
Amount of human error related to endpoints	9.6%
Number of help desk calls related to endpoints	9.3%
End-user disruption due to endpoint-related downtime (both planned and unplanned)	9.4%
Total management costs related to endpoints	10.9%
Total number of staff (full-time equivalent) dedicated to endpoint security, compliance and management	4.5%
Time spent on endpoint-related administrative tasks	5.8%
Time spent on endpoint-related analysis, reporting and management	4.6%

Source: Aberdeen Group, March 2009

As a back-of-the-envelope example, based on assumptions of eight Full-Time Equivalent (FTE) staff members at a fully-loaded cost of $125K/year, a 4.5% reduction in FTE translates to an approximate annual savings of $45K for Best-in-Class performance in comparison to that of Laggards. (Another point of view would be that top performance frees up this amount of additional resources to invest in other desirable projects.) In addition, assuming a weighted average cost of capital of 10%, $45K per year in perpetuity has a net present value of $450K.

This represents an upper bound, of course, but it provides a concrete illustration of how to estimate – based on the findings summarized in Figure 4 – the positive financial impact of improving performance in security, compliance, and operational efficiency. Try it yourself for this, or one of the other key performance indicators in Table 4.

Figure 5: Breakdown of Average Total Cost of Ownership per Endpoint System



Component	% of TCO	Annual Cost
Hardware (initial configuration)	30.9%	$291
Software licenses (incremental to the initial configuration)	20.4%	$191
Upgrades (all upgrades 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 / reimage / recover	4.9%	$46
Endpoint Security / Compliance	6.7%	$63
Endpoint Management	5.4%	$51
Other	1.9%	$18

Source: Aberdeen Group, March 2009

Another 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 per endpoint system (Figure 5). Across all respondents in the 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 **$3,120**. In Figure 5, this amount is broken down into 10 components and presented in terms of the annual cost for each. Observations and insights from these findings include:

- About half (51.3%) of the total cost of ownership per endpoint is in the initial hardware configuration and in software licenses which are incremental to the initial configuration.
- This means that about half of the total cost of ownership per endpoint is associated with protecting and managing the endpoint system over its useful lifetime … a worthy target for greater efficiency and cost reduction.
- At least $245 per endpoint per year (26.3%) is associated with the costs for internal support (e.g., help desk); reinstallation, reimaging, and recovery; endpoint security and compliance; and endpoint management.
- A back-of-the-envelope calculation for the annual financial impact of Best-in-Class performance for each of these four areas is as follows:
    - Internal support (e.g., help desk) = $85 (from Figure 5) x 9.3% (from Table 4) = $7.90 per endpoint per year

  - Reinstallation, reimaging, and recovery = $46 x 9.4% = $4.30 per endpoint per year
  - Endpoint security and compliance = $63 x 9.3% = $5.90 per endpoint per year
  - Endpoint management = $51 x 10.9% = $5.60 per endpoint per year
- So Best-in-Class performance in all four of these areas translates to a savings of about $24 per endpoint per year, or approximately $80 per endpoint over the average replacement cycle. Regardless of company size, the cumulative effect of these numbers contributes to the cost-cutter's case for convergence of endpoint security and endpoint management.

In the next chapter, we will see what the top performers are doing to achieve these gains.

Aberdeen Insights – Strategy

Security and compliance of the endpoints, and management of the endpoints, are like peanut butter and chocolate – each good by themselves, and surprisingly good when combined together. Proactively seeking opportunities to integrate these two commonly separate functions can drive a number of technical and business benefits, which are especially attractive in difficult economic times:

- Standardization and integration of baseline endpoint security technologies such as anti-virus, anti-spyware, personal firewall, intrusion detection and prevention
- Flexibility for the future deployment of additional endpoint security technologies, such as endpoint device / port controls, application controls, network access control, and data protection – and the ability to expand endpoint security functionality without additional software deployments at each endpoint
- Significantly improved endpoint management efficiencies, through automation and elimination of manual processes, and the ability to spend less time on administration tasks and more time on higher value management, analysis and reporting activities
- Lower total cost of ownership per endpoint

The widely-used phrase "do more with less" sums up the current reality for many organizations – but how? The Best-in-Class demonstrate that endpoints which are both secure *and* well-managed help to hit the target.

"We had all these little semi-autonomous data centers in each of our facilities. As we consolidated, we didn't really know all of the assets we had … some had spreadsheets, one had a Word document … asset management was a big problem. Now a change and configuration management database is feeding our centralized security information and management system, which gives us much better visibility. Our systems are more secure, and we also have a better view of what's going on. It's definitely a change in mindset, though; people just can't do what they like, as they've been able to do in the past."

~ Senior Security Analyst,
US Manufacturing Company

Telephone: 617 854 5200
Fax: 617 723 7897

Aberdeen Group
A Harte-Hanks Company

Chapter Two:
Benchmarking Requirements for Success

Strategies to protect and manage endpoints ultimately lead to the selection and deployment of one or more specific endpoint security and endpoint management solutions. 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 more cost-effective management.

Case Study – Global Hotel and Hospitality Leader

A global leader in hotels and hospitality, headquartered in Europe, operates nearly 4,000 hotels in approximately 100 countries with more than 150,000 employees worldwide. In the North American segment of the business, a very small central support group has responsibility for supporting more than 6,000 endpoints and 2,000 servers at more than 900 locations, many of which are highly remote.

Regulatory compliance, in particular the Payment Card Industry Data Security Standard (PCI DSS), was a leading driver for the company's increased investments in protecting and managing its endpoint systems. "We were always so busy," said the organization's IT Director, "but at the time it's fair to say that we were always out of compliance, and we certainly didn't have the visibility we needed to be confident about upcoming audits." In the early phases of assessing systems for its PCI compliance initiative, the team uncovered a long list of issues – in one extreme example, they found cardholder data that was eight years old stored on local hard drives.

After extensive testing and evaluation, the group selected and deployed security solutions that could centrally manage the continuous process of assessing, prioritizing, and remediating security and compliance issues in its far-flung network of endpoint systems. Automation and simplicity of management were highly prized solution attributes; "We simply don't have the resources to devote to inefficient or manual efforts."

Achieving PCI DSS compliance was an important milestone, but the group knows that their journey to maintain secure, compliant and well-managed endpoint systems lies on a never-ending road. The good news is that they can sleep better at night, with much less concern about the unexpected knock on the door; "We now have the visibility and the confidence that the auditor will simply tell us what we already know."

Fast Facts

Average endpoint replacement cycle (all respondents): 3.3 years

Expected change in endpoint replacement cycle going forward:

√ Increase (longer time to replace): 21%

√ About the same: 62%

√ Decrease (shorter time to replace): 17%

Average estimate of the total cost of ownership per endpoint over the entire replacement cycle (all respondents): $3,120

Competitive Assessment

Aberdeen analyzed the aggregated metrics of surveyed companies to determine whether their performance in protecting and managing their endpoints ranked as Best-in-Class, Industry Average, or Laggard. In addition

to having similar performance levels, each class also shared characteristics in five important categories: (1) **process** (the approaches taken to execute daily operations); (2) **organization** (corporate focus and collaboration among stakeholders); (3) **knowledge management** (putting business intelligence in context and exposing it to relevant stakeholders); (4) **technology** (the selection of appropriate tools, and the effective deployment of those tools); and (5) **performance management** (the ability of the organization to measure results to improve the business). These characteristics, identified in Table 5, serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the associated metrics.

Table 5: Competitive Framework for Protecting and Managing Endpoint Systems

	Best-in-Class	Average	Laggards
Process	Consistent policies for supported application software / licenses at the endpoints		
	93%	64%	63%
	Consistent access policies based on context at the endpoint (e.g., configuration, "health", device ID)		
	62%	47%	41%
	Systematic implementation / rollout processes for endpoint software / updates / configurations		
	77%	56%	43%
	Standardized response for endpoint-related exceptions, security events, or incidents of non-compliance		
	64%	50%	33%
	Centralized collection, normalization and correlation of endpoint-related security and compliance information		
	62%	36%	33%
Organization	Responsible executive or team with primary ownership for security, compliance and management of endpoint systems		
	79%	68%	65%
	Documented workflow for endpoint provisioning / deployment		
	69%	53%	24%
Knowledge Management	Inventory of supported application software / licenses		
	85%	75%	69%
	Tracking and reporting of supported application software / licenses		
	85%	72%	61%
	Identification / inventory of endpoint assets		
	85%	69%	61%
	Tracking and reporting of endpoint assets		
	62%	60%	53%
	Visibility into current state / posture of endpoint systems under management		
	54%	25%	24%

	Best-in-Class	Average	Laggards
Technology	Standardized endpoint systems		
	85%	58%	57%
	Standardized endpoint configurations		
	86%	63%	61%
	Pre-packaging of endpoint software / configurations before deployment		
	92%	54%	53%
	Automated endpoint provisioning / deployment process		
	77%	40%	34%
	For endpoint security and endpoint management technologies currently in use, see **Figure 10** and **Figure 11**, respectively. Also refer to **Figure 1**.		
Performance Management	Effective measurement of the total costs associated with protecting and managing endpoints		
	31%	23%	16%

Source: Aberdeen Group, March 2009

Capabilities and Enablers

Based on the comparisons within the Competitive Framework and interviews with select respondents, analysis of the Best-in-Class highlights the degree to which they have developed their ability to protect and manage their endpoints beyond that of their Industry Average and Laggard counterparts.

"We're working to change the mentality. I don't want my team to focus on security technologies, I want them to focus on managing our endpoint systems – and this obviously includes security – over their full lifecycle, from cradle to grave. Our mission is to ensure that our endpoints are ready and in line with policy, so they can support our end-users for their intended business purposes. And we want to do that as efficiently and as cost-effectively as we possibly can."

~ IT Director,
Global Services Firm

Process

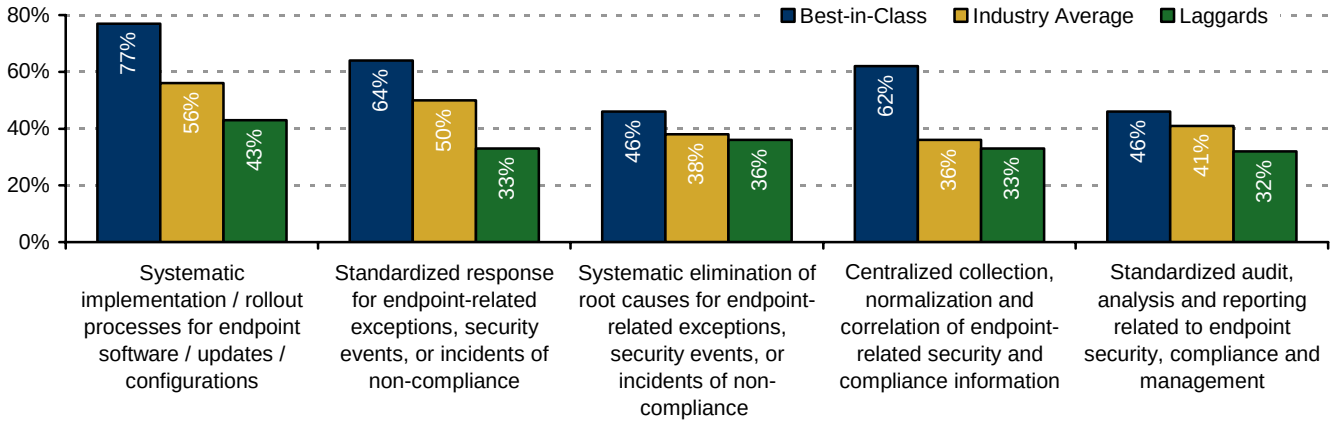
Consistent policies based on the supported applications, approved configurations and current posture at the endpoints are the biggest differentiators between Best-in-Class companies (93%) and all others (63%). This corresponds with the top strategies, showing that the companies with top results are successfully linking strategy with execution.

The findings show that **standardization** is the friend of top performance in protecting and managing endpoint systems. Four out of five (77%) Best-in-Class companies have systematic processes for software rollout, updates, and configurations, compared to just two out of five (43%) of Laggards (Figure 6). The Best-in-Class are nearly two-times more likely than Laggards to have developed standardized responses for endpoint-related exceptions, security incidents, or incidents of non-compliance … although interestingly, less than half (46%) of the Best-in-Class indicate that they systematically seek to eliminate the root causes. Aberdeen continues to note that proficiency at catching the dogs running around the back yard is good, but taking steps to keep them from getting loose in the first place is better.

In addition, the Best-in-Class are nearly two-times more likely than Laggards to centralize the collection, normalization and correlation of endpoint-related security and compliance data, giving them better **visibility** the current posture of their infrastructure. See the March 2009 report

Leveraging Logs, Information and Events: Three Use Cases for What to Do with All that Data for additional information on the benefits of this approach.

Figure 6: Standardization is the Friend of Top Performance

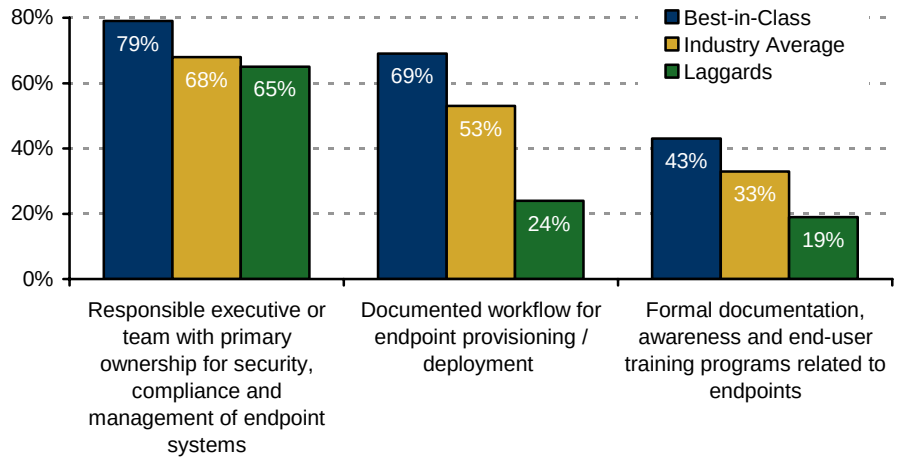


Source: Aberdeen Group, March 2009

Organization

As usual, Aberdeen's research confirms what common sense tells us: establishing primary ownership for an important cross-enterprise initiative is more likely to deliver the desired results. The current study supports this pattern: nearly four out of five (79%) of Best-in-Class companies have assigned primary ownership to a responsible executive or team (Figure 7). In addition, the Best-in-Class were more than two-times more likely to invest in documenting their workflow and in documentation, awareness and training for end-users related to the endpoints. This also rings true with common sense, yet in absolute terms the investments in end-user training are made by just 43% of the Best-in-Class.

Figure 7: One Throat to Choke; Documentation and Training

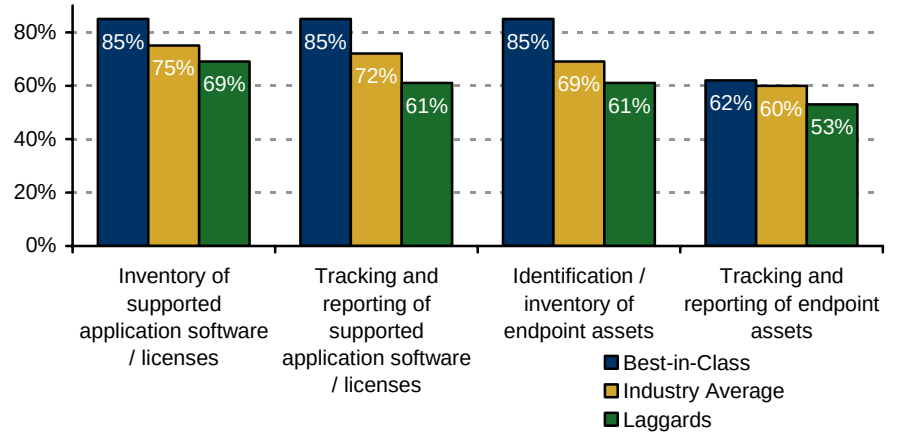


Source: Aberdeen Group, March 2009

Knowledge Management

It seems obvious, but knowing **what you have** and **where it is** correlates strongly with Best-in-Class performance in protecting and managing endpoint systems. Most (85%) Best-in-Class organizations maintain an inventory of their supported application software and licenses, and maintain tracking and reporting on them over time (Figure 8). The same is true for identifying and inventorying their endpoint systems, although in this case there is a material drop-off (from 85% to 62%) among the Best-in-Class when it comes to tracking and reporting.

Figure 8: Tracking What You Have and Where it is Located

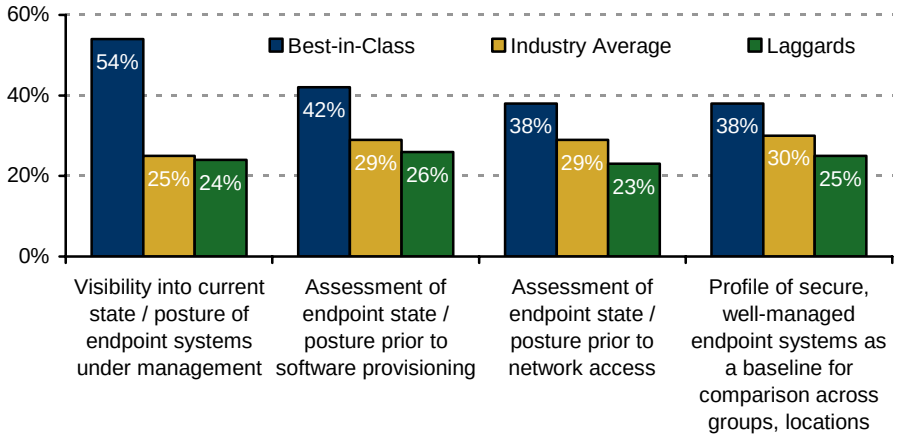


Source: Aberdeen Group, March 2009

Visibility into the current state, and using that visibility before provisioning additional software or enabling network access, is also a characteristic of the Best-in-Class companies in this study relative to their Industry Average

and Laggard counterparts (Figure 9). In absolute terms, however, such visibility is still an emerging capability. See the March 2009 Aberdeen report *Leveraging Logs, Information and Events: Three Use Cases for What to Do with All that Data* for additional information and insights on this topic.

Figure 9: Visibility into the Current State



Source: Aberdeen Group, March 2009

Technology

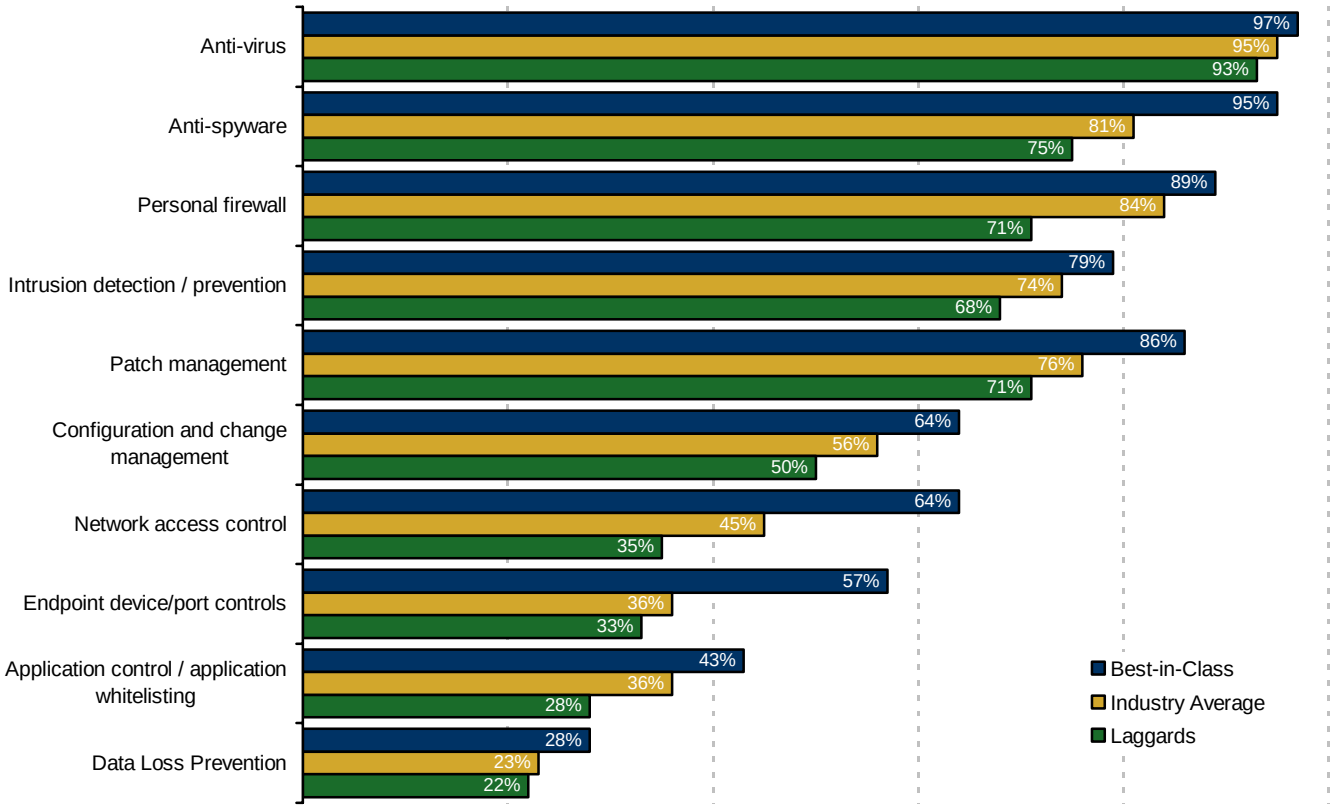
The current use of select enabling technologies for endpoint security and endpoint management – in both absolute and relative terms – has been thoroughly discussed in Chapter One. From the perspective of profiling the use of these technologies by the Best-in-Class organizations:

- Baseline technologies include anti-virus, anti-spyware, intrusion detection / prevention, personal firewalls, patch management, configuration and change management, and software inventory.
- Early adoption technologies include application virtualization, application controls / application whitelisting, endpoint device / port controls, and network access control.
- Technology differentiators include software distribution, IT asset management, and full-disk encryption.
- Emerging technologies include data loss prevention and online backup / recovery.

Given the sheer volume of endpoint systems to be protected and managed, it comes as no surprise that the companion to standardization as the friend of companies with top results is **automation**. Nearly all (92%) of the Best-in-Class pre-package and pre-configure endpoint software before deployment (Figure 12). Four out of five (77%) of the Best-in-Class have automated the endpoint provisioning and rollout process, outpacing Laggards by a two-to-one margin. The Best-in-Class are also two-times

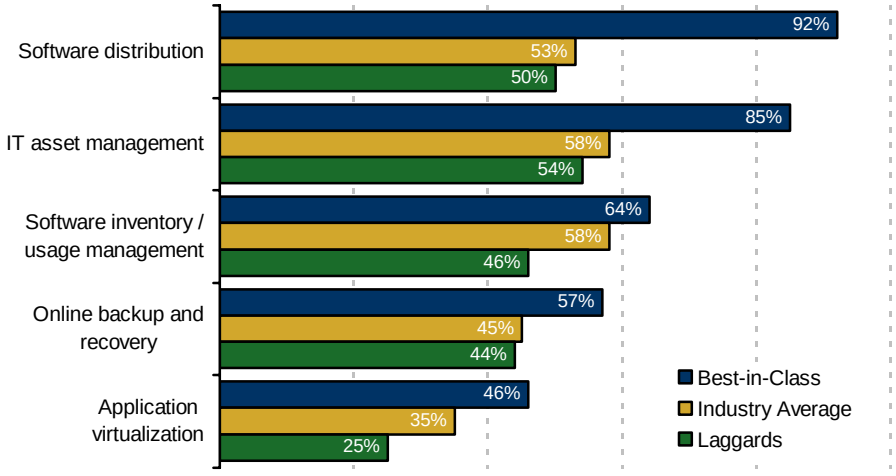
more likely to automate the migration of endpoint configurations, which is not only a cost savings but also a major convenience for end-users.

Figure 10: Current Use of Select Enabling Technologies for Endpoint Security



Source: Aberdeen Group, March 2009

Figure 11: Current Use of Select Enabling Technologies for Endpoint Management

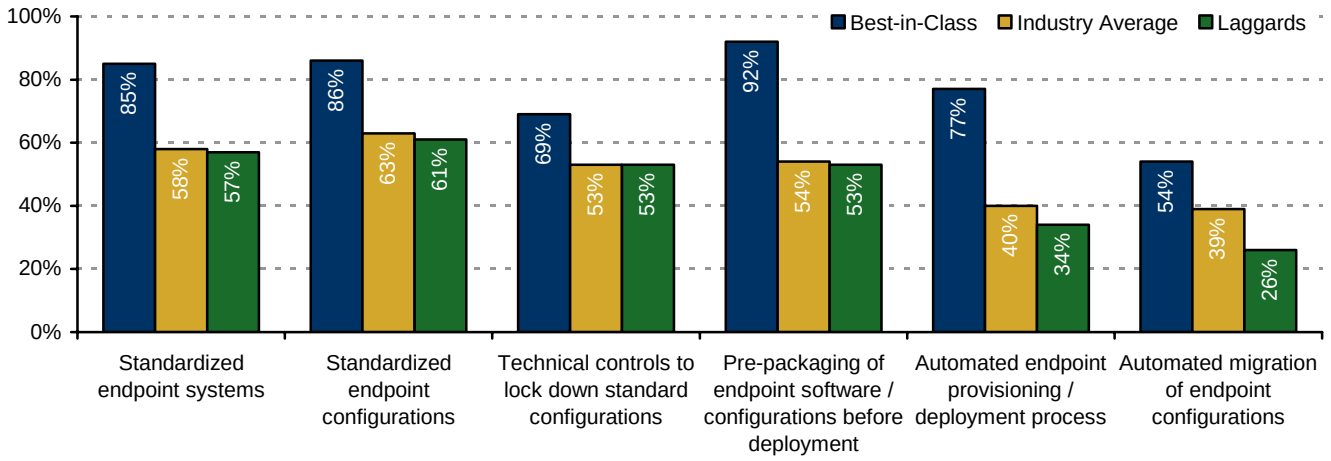


Source: Aberdeen Group, March 2009

Performance Management

The research shows that one current challenge for all respondents is the effective measurement of the total costs associated with protecting and managing endpoints. Just 31% of the Best-in-Class indicated having this capability, and while this is nearly two-times that of Laggards (16%) it is clearly an area for incremental improvement.

Figure 12: Standardization's Other Friend – Automation



Source: Aberdeen Group, March 2009

Aberdeen Insights – Technology

Virtually all companies have deployed technologies for anti-virus, anti-spyware, intrusion detection / prevention, personal firewalls and patch management, and a majority have implemented configuration and change management. In broad terms, the findings in the current study make clear that leading organizations have given first priority to the *platform* and *network* perspective of protecting and managing their endpoints. Building on this foundation, they are currently focusing on protecting and managing their *applications* (e.g., using application virtualization, application controls, application whitelisting, software distribution, and software inventory management). Looking forward, they are beginning to increase the focus on protecting and managing their *data* (e.g., using data loss prevention and online backup and recovery).

continued

Aberdeen Insights – Technology

The findings also make it clear that baseline **endpoint security** technologies by themselves do not differentiate top performance (although it should go without saying, any company would be unlikely to earn Best-in-Class status without them). Deployment of **endpoint management** solutions, on the other hand, is currently a strongly distinguishing characteristic of the companies achieving Best-in-Class results. The current study adds to the growing body of evidence in Aberdeen's IT security research that Best-in-Class organizations first ensure that their mission-critical systems are secure, then compliant, then optimized and well-managed. First order, then progress.

Sidebar: Mobile Endpoint Devices

Increasingly, the term "endpoint" must be expanded to include *mobile endpoint devices* such as smart phones, PDAs, USB drives, removable media, hard drives, and other connected devices that have become so common in the typical enterprise. Best-in-Class companies in the current study were 1.8-times more likely than Laggards to explicitly take mobile endpoint devices under management – and on average, they indicated a 3.5% year-over-year increase in number. At the same time, they estimated a 1.7% year-over-year increase in the number of mobile endpoint devices owned and managed by individual end-users. The age-old balancing act between giving end-users the flexibility and convenience they want, safeguarding the enterprise's infrastructure and data, and working within the limits of available resources is playing out again with respect to mobile endpoint devices. For these reasons, Aberdeen plans a future benchmark report on security for (and by) mobile endpoint devices later in the year.

Telephone: 617 854 5200
Fax: 617 723 7897

Aberdeen Group
A Harte-Hanks Company

Chapter Three: Recommended Actions

Whether a company is trying to move its performance in protecting and managing endpoints from Laggard to Industry Average, or Industry Average to Best-in-Class, the following sequence of actions will help drive the desired performance improvements.

General Steps to Success

1. Identify and inventory the endpoint systems being protected (from the perspective of platforms, networks, applications and data), and establish capabilities to track and report on these assets over time
2. Prioritize your organization's security control objectives for these assets as a function of risk, audit and compliance requirements, and establish consistent policies and procedures
3. As much as possible, standardize on endpoint systems, configurations, and implementation and rollout processes
4. Establish an overall approach to endpoint protection and endpoint management; the findings from this benchmark can serve as a guideline for a rational order of appearance:
    - First security and compliance, then management
    - *Integration* of security and management correlates with Best-in-Class results
    - "Platform" and "network" technologies include anti-virus, anti-spyware, patch management, configuration and change management; personal firewalls, intrusion detection / prevention, network access control; and IT asset management
    - "Application" technologies include application controls / application whitelisting; application virtualization; software distribution; and software inventory / usage management
    - "Data" technologies include full-disk encryption; endpoint device / port controls; data loss prevention (agent-based); and online backup and recovery
5. Automate, as much as possible, the process of assessing, prioritizing and remediating security-related issues; also automate the process of packaging, provisioning and installing software and configuration changes
6. Assign clear ownership and accountability for endpoint security and management initiatives to an executive or cross-functional team
7. Invest in documentation, awareness and training for end-users
8. Establish a consistent, unified view of information and events related to endpoint systems; standardize audit, analysis and reporting
9. Measure and monitor regularly; drive continuous improvements by finding and eliminating root causes for exceptions, security events, and audit deficiencies

Fast Facts

√ 49% of all respondents reported a year-over-year-increase in the average number of software agents installed at their endpoint systems

Laggard Steps to Success

In this study, Laggards have already implemented baseline endpoint security technologies such as anti-virus, anti-spyware, personal firewalls, intrusion detection / intrusion prevention, and patch management. Assuming that their organization's scale (i.e., total number of endpoints) is large enough to warrant additional investments, increasing the focus on standardization and automation of these technologies would help to improve security as well as reduce costs. See Aberdeen's July 2008 report *Vulnerability Management: Assess, Prioritize, Remediate, Repeat* for additional insights and recommendations for improvement.

Industry Average Steps to Success

Based on the findings, *consistency*, *standardization* and increased *automation* are the areas in which the Industry Average companies can make the greatest incremental improvements. In many of these areas (see Table 5, and the many Figures in Chapter Two) the Industry Average are marginally better than Laggards, but more substantially below the Best-in-Class in terms of current capabilities. With respect to current use of enabling technologies, the Industry Average seem well-positioned to take advantage of the emerging trend towards convergence of endpoint security and endpoint management capabilities from leading solution providers. Asset management, software inventory and usage management, and software distribution capabilities will help them to support higher scale at lower total cost. Aberdeen's September 2007 report on *Sustaining Compliance* makes a good reference for this phase of an initiative's maturity and growth.

"Regulatory compliance was our major driver. We had to get a handle on our endpoint systems; we just didn't know what we didn't know. In many ways the saying 'ignorance is bliss' is so true, because once we started to find out what was really going on we had to double our efforts to get these systems in control. And with a very small central support staff, we need to remain highly efficient at keeping them in control."

~ IT Director,
Hotel and Hospitality Industry

Best-in-Class Steps to Success

The research shows that Best-in-Class organizations can still improve their visibility into the current state of their endpoint systems, and use that intelligence to optimize ongoing operations. By establishing a consistent, unified view of the information and events related to endpoint systems, the Best-in-Class can drive continuous improvements – for example, by finding and eliminating root causes for exceptions, security events, and audit deficiencies. See Aberdeen's March 2009 report *Leveraging Logs, Information and Events: Three Use Cases for What to Do with All that Data* for additional information and insights on best practices in this area.

Aberdeen Insights – Summary

As a matter of doctrine "every marine is a rifleman," meaning that even in an age of specialization and advanced technologies every marine is expected to be proficient with a rifle, and every weapon is expected to be kept clean and ready. By analogy all knowledge workers, regardless of function or role, are expected to contribute to the achievement of the company's objectives, through their proficiency in the use of endpoint systems which are secure, compliant and well-managed. The *integration* of endpoint security and endpoint management – traditionally separate activities – correlates strongly with achievement of Best-in-Class results.

Appendix A: Research Methodology

Between January and February 2009, Aberdeen examined the use, the experiences, and the intentions of more than 120 enterprises in a diverse set of industries with respect to their approaches for protecting and managing their endpoint devices. Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on their respective strategies, experiences, and results.

Responding enterprises had the following demographics:

- *Job title / function:* The research sample included respondents with the following job titles: C-level (23%); Vice President / General Manager (6%); Director (14%); Manager (17%); Staff / Consultant (38%); and other (2%). The largest segment by functional responsibility was IT, representing 52% of the total sample.
- *Industry:* The research sample included respondents from a wide range of industries. The largest segments included financial services (9%), government / aerospace / defense (8%), and telecommunications (5%).
- *Geography:* A majority of respondents (66%) were from the Americas. Remaining respondents were from the Asia-Pacific region (11%) and Europe / Middle East / Africa (23%).
- *Company size:* Twenty-seven percent (27%) of respondents were from large enterprises (annual revenues above US $1 billion); 36% were from midsize enterprises (annual revenues between $50 million and $1 billion); and 37% of respondents were from small businesses (annual revenues of $50 million or less).

Solution providers recognized as sponsors were solicited after the fact and had no substantive influence on the direction of this report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to its readers at no charge.

Focus of the Study

Respondents completed an online survey that included questions designed to determine the following:

√ The degree to which technologies to secure and management endpoint systems are deployed in their IT operations, and the financial impact of these technologies

√ The efficiency and effectiveness of existing implementations

√ Benefits that have been derived with respect to enhancing security, sustaining compliance, or reducing operational costs

The study aimed to identify current and emerging best practices for protecting and managing endpoints, and to provide a framework by which readers can assess their own current capabilities.

Aberdeen Group
A Harte-Hanks Company

Table 6: PACE Framework Key

Overview
Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows: **Pressures –** external forces that impact an organization's market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive) **Actions –** the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product / service strategy, target markets, financial strategy, go-to-market, and sales strategy) **Capabilities –** the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing) **Enablers –** the key functionality of technology solutions required to support the organization's enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)

Source: Aberdeen Group, March 2009

Table 7: Competitive Framework Key

Overview	
The Aberdeen Competitive Framework defines enterprises as falling into one of the following three levels of practices and performance: **Best-in-Class (20%) –** Practices that are the best currently being employed and are significantly superior to the Industry Average, and result in the top industry performance. **Industry Average (50%) –** Practices that represent the average or norm, and result in average industry performance. **Laggards (30%) –** Practices that are significantly behind the average of the industry, and result in below average performance.	In the following categories: **Process –** What is the scope of process standardization? What is the efficiency and effectiveness of this process? **Organization –** How is your company currently organized to manage and optimize this particular process? **Knowledge –** What visibility do you have into key data and intelligence required to manage this process? **Technology –** What level of automation have you used to support this process? How is this automation integrated and aligned? **Performance –** What do you measure? How frequently? What's your actual performance?

Source: Aberdeen Group, March 2009

Table 8: Relationship Between PACE and the Competitive Framework

PACE and the Competitive Framework – How They Interact
Aberdeen research indicates that companies that identify the most influential pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices it makes and how well it executes those decisions.

Source: Aberdeen Group, March 2009

Aberdeen Group
A Harte-Hanks Company

Appendix B:
Related Aberdeen Research

Related Aberdeen research that forms a companion or reference to this report includes:

- *Leveraging Logs, Information and Events: Three Use Cases for What to Do with All That Data*; March 2009
- *When Less is More: Why Small Companies Should Think Outside the Box for Protecting Endpoints*; February 2009
- *Securing and Managing the Endpoints: The Case for Convergence*; October 2008
- *Unified Threat Management*; September 2008
- *Vulnerability Management: Assess, Prioritize, Remediate, Repeat*; July 2008
- *PCI DSS and Protecting Cardholder Data*; June 2008
- *Data Loss Prevention: Little Leaks Sink the Ship*; June 2008
- *Application and Infrastructure Monitoring and Management*; June 2008
- *Security Governance and Risk Management*; November 2007
- *Who's Got the NAC?*; October 2007
- *Sustaining Compliance*; September 2007
- *Aberdeen Security Assessment for Mid-Size Companies*; interactive online assessment tool

Information on these and any other Aberdeen publications can be found at www.aberdeen.com.

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