

May 2009

## Shavlik Integrates Sunbelt Software Technology: Keeping Endpoints Secure, Compliant and Well-Managed

In April 2009, Shavlik Technologies announced its selection of technology from Sunbelt Software to integrate anti-virus and anti-spyware capabilities into its flagship Shavlik NetChk Protect patch management solution. This integrated solution is spot-on with the market preferences identified in Aberdeen's March 2009 benchmark study on [Endpoint Security, Endpoint Management](#). Overall, Shavlik's direction is well-aligned with the "first secure, then compliant, then well-managed" approach to IT Security taken by Best-in-Class organizations, as seen in Aberdeen's research.

### Business Context: Endpoint Systems Clean and Ready

In its benchmark study on [Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence](#) (March 2009), Aberdeen looked at the current and planned use of several enabling technologies for endpoint security and endpoint management. Figure 1 plots the research findings for *absolute adoption* by Best-in-Class organizations (i.e., the percentage of the Best-in-Class 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). From the perspective of profiling the current level of adoption of these technologies by Best-in-Class organizations, "baseline" technologies for endpoint security include:

- Anti-virus, anti-spyware
- Intrusion detection / prevention
- Personal firewalls
- Patch management, configuration and change management

Virtually all companies have deployed technologies for anti-virus, anti-spyware, intrusion detection / prevention, personal firewalls and patch management, and a majority has implemented configuration and change management. In broad terms, the findings in the [Endpoint Security, Endpoint Management](#) 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).

### Market Alert

Aberdeen's Market Alerts provide timely analysis of current market events, drawing upon independent fact-based research to lend insight into the topics that impact end-user organizations

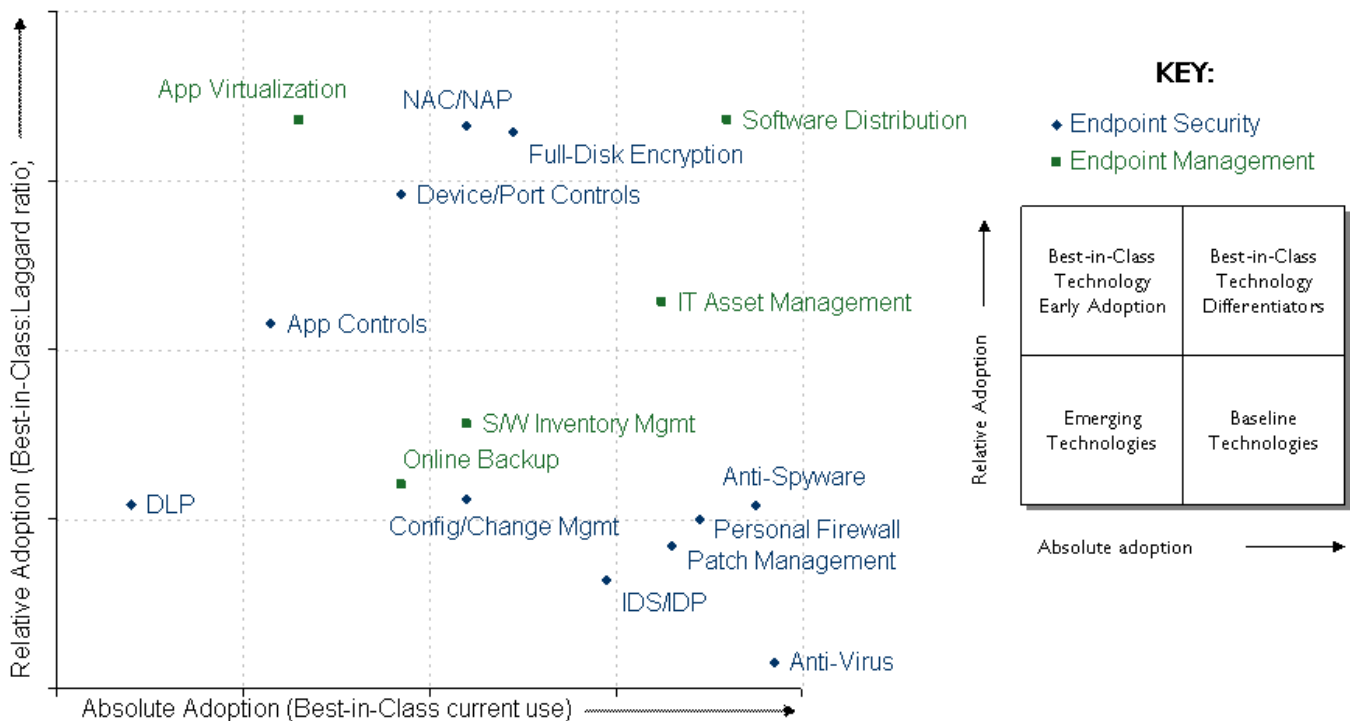
### Determining the Best-in-Class

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

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

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



Source: Aberdeen Group, March 2009

The findings make it clear that these 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). The policy, planning, process, and organizational elements of implementation are also critical success factors in the ability to realize the business benefits of enhanced security, sustained compliance, and more cost-effective management.

Given the sheer volume of endpoint systems to be protected and managed, it comes as no surprise that **automation** was found to be the friend of the companies with top results. Nearly all (92%) of the Best-in-Class pre-package and pre-configure endpoint software before deployment. Four out of five (77%) of the Best-in-Class have automated their 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. Overall, the research shows that the companies with top results excel not only at keeping their endpoint systems "clean and ready," but also at cutting the average total cost per endpoint for security, compliance, and management.

## **Shavlik, Sunbelt Software Announcement**

---

In April 2009, Shavlik Technologies announced its selection of technology from Sunbelt Software to integrate anti-virus and anti-spyware capabilities into its flagship Shavlik NetChk Protect patch management solution. The integrated solution, which is expected to be available as part of Shavlik's upcoming version 7 release, will feature a single software agent and a common management console.

This integrated solution is spot-on with the market preferences identified in Aberdeen's recent benchmark study on [Endpoint Security, Endpoint Management](#) (March 2009). Technical capabilities for endpoint security solutions – such as accuracy, minimal impact on performance, and scalability – top the list of relative importance for various features. Intertwined and only slightly lower in importance are desirable management capabilities, such as a common management console and a reduced number of software agents. Shavlik's selection of Sunbelt's anti-virus and anti-spyware, combined with the established management capabilities of NetChk Protect, hit these market preferences on all cylinders. For customer examples and analysis related to Sunbelt Software's VIPRE Enterprise solution, see Aberdeen's Sector Insight on [When Less is More: Why Small Companies Should Think Outside the Box for Protecting Endpoints](#) (February 2009).

The consistent thread running through Aberdeen's IT security research is that the Best-in-Class approach to IT security is to be secure, then compliant, then well-managed...in that order. Shavlik's stated strategy has been to simplify and automate essential endpoint security operations such as patching and configuration, thus helping its customers to sustain security and compliance while reducing the associated time, cost, and manpower. The technology relationship with Sunbelt Software will help Shavlik to expand its capabilities to keep endpoint systems secure and compliant, while leveraging its traditional strengths in automated and cost-effective management.

### **Case in Point: 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 – including Shavlik's NetChk family – 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. As the IT director said, "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. The IT director put it this way: "We now have the visibility and the confidence that the auditor will simply tell us what we already know."

## Solutions Landscape

Solution providers for endpoint security can range from smaller specialists to multi-billion dollar firms. Table 1 provides an illustrative list.

**Table 1: Solutions Landscape for Endpoint Security (illustrative)**

Company	Solution(s)	Description
<b>Shavlik Technologies</b> <a href="http://www.shavlik.com">www.shavlik.com</a>	Shavlik NetChk Protect	Shavlik NetChk Protect is designed to automate and simplify the tasks of identifying and remediating security vulnerabilities for patch management, application control, antivirus and antispyware, across both physical systems and virtual machines.
	Shavlik NetChk Configure	Shavlik NetChk Configure provides a centralized management interface that allows organizations to scan the network continuously to validate configuration settings against corporate security policies and regulatory frameworks.
<b>Sunbelt Software</b> <a href="http://www.sunbeltsoftware.com">www.sunbeltsoftware.com</a>	VIPRE Enterprise	Sunbelt Software's VIPRE Enterprise combines anti-virus, anti-spyware, anti-rootkit and other technologies into a single agent, handled through a central management console, while minimizing the negative performance and resource impact of traditional endpoint security products.
<b>AVG Technologies</b> <a href="http://www.avg.com">www.avg.com</a>	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.
<b>McAfee</b> <a href="http://www.mcafee.com">www.mcafee.com</a>	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.

Company	Solution(s)	Description
<b>Symantec</b> <a href="http://www.symantec.com">www.symantec.com</a>	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, May 2009

## Summary and Recommendations

For existing Shavlik customers, the release of Shavlik NetChk Protect 7 represents an opportunity to glean even more business value by managing anti-virus, anti-spyware, patch management and configuration and change management from a common console, while taking advantage of Shavlik's traditional approach to simplification and automation of essential endpoint security tasks. Prospective customers will view the Shavlik solution portfolio as addressing a broader set of their "baseline" endpoint security requirements.

In broad terms, Aberdeen's research indicates the following patterns of deployment by Best-in-Class organizations:

- Highest priority is given to the *platform* and *network* perspective of protecting and managing their endpoints (anti-virus, anti-spyware, intrusion detection / prevention, personal firewalls, patch management, and configuration and change management)
- Attention is next given to protecting and managing their *applications* (e.g., using application virtualization, application controls, application whitelisting, software distribution, and software inventory management)
- Newly emerging focus is being placed on protecting and managing their *data* (e.g., using data loss prevention and online backup and recovery)

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

**Related Research**

<p><u><a href="#">Endpoint Security. Endpoint Management: The Cost-Cutter's Case for Convergence</a></u>; March 2009</p> <p><u><a href="#">Leveraging Logs, Information and Events: Three Use Cases for What to Do with All That Data</a></u>; March 2009</p> <p><u><a href="#">Deploying IT Security: Keeping the Threats and Headaches Outside</a></u>; March 2009</p> <p><u><a href="#">When Less is More: Why Small Companies Should Think Outside the Box for Protecting Endpoints</a></u>; February 2009</p>	<p><u><a href="#">Secure, Compliant, and Well-Managed: The IT Security Approach to GRC</a></u>; February 2009</p> <p><u><a href="#">Securing and Managing the Endpoints</a></u>; October 2008</p> <p><u><a href="#">Unified Threat Management</a></u>; September 2008</p> <p><u><a href="#">Vulnerability Management: Assess, Prioritize, Remediate, Repeat</a></u>; July 2008</p> <p><u><a href="#">Sustaining Compliance</a></u>; September 2007</p>
<p><b>Author: Derek E. Brink, Vice President and Research Fellow, IT Security (<a href="mailto:derek.brink@aberdeen.com">derek.brink@aberdeen.com</a>)</b></p>	

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.