

January 6, 2006

# The Forrester Wave™: Enterprise Antispyware, Q1 2006

by Natalie Lambert

TECH CHOICES

FORRESTER®

Helping Business Thrive On Technology Change



January 6, 2006

## The Forrester Wave™: Enterprise Antispyware, Q1 2006

McAfee And Trend Micro Lead In Our Product Evaluation

by **Natalie Lambert**

with David Friedlander and Sarah Bernhardt

### EXECUTIVE SUMMARY

In the past few years, spyware has joined malicious code and hackers as a top IT security threat. It can steal both personal and corporate information, as well as slow down internal networks so that they are rendered useless — all while users never know it's there. Spyware can create a significant drain on IT support resources, and worse yet, it is used in corporate espionage and data theft. Firms may also get stuck footing the bill for spyware that affects employees and customers. Companies must take immediate steps to protect themselves and their customers against spyware. To assess the state of the enterprise antispyware market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top enterprise antispyware vendors across 105 criteria. The result: McAfee leads the pack with Trend Micro nipping at its heels. Both offerings scale to any size organization and include robust management and reporting capabilities. Webroot Software and Sunbelt Software also offer solid solutions thanks to their strong overall architecture and spyware detection capabilities. Included in this report is an interactive vendor comparison tool that provides detailed product evaluations and customizable rankings.

### TABLE OF CONTENTS

- 2 **Spyware Climbs The IT Security Threat Ladder**
- 5 **Enterprise Antispyware Evaluation Overview**
- 7 **Dedicated Security Vendors Win Out**
- 9 **Vendor Profiles**
- 12 **Supplemental Material**

### NOTES & RESOURCES

Forrester conducted evaluations in August and September 2005 and interviewed 18 vendor and user companies, including: Aluria Software, CA, McAfee, Tenebril, Trend Micro, Sunbelt Software, Symantec, and Webroot Software.

#### Related Research Documents

["The Forrester Wave™: Client Security Suites, Q2 2005"](#)

June 22, 2005, Tech Choices

["IT Security Threats In 2005: Viruses And Worms Top The List"](#)

March 25, 2005, Trends

["Antispyware Adoption In 2005"](#)

February 10, 2005, Trends

## SPYWARE CLIMBS THE IT SECURITY THREAT LADDER

Although spyware was first seen in its innocuous form almost 10 years ago, it was not until 1999 that researchers first discovered a free downloaded program that was actually sending personal information back to the software's author. In the past six years, spyware has evolved and now poses a more significant threat to enterprises than viruses or worms. In its most malicious form, spyware is used for corporate espionage — keyloggers installed on end point machines can give outsiders access to sensitive corporate information. Additionally, spyware can steal personal information, such as Social Security and credit card numbers, and send it back to its creator. Spyware is a global problem and has global consequences, as shown by recent spyware incidents:

- **Trojan horse leads to industrial espionage.** Israel and the UK: In a recent case of industrial espionage, a Trojan horse — installed on users' machines either by an external device or through email — was used to steal confidential corporate documents and send them to an FTP site. The FTP site was managed by competitors of the infected users' companies, which used the information to spy on their competitors.<sup>1</sup>
- **Spyware-infected email leads to bank account fraud.** Japan: A man in Tokyo was recently arrested for allegedly sending a spyware-infected email to a Japanese jewelry company. Once the spyware was installed, the man was able to obtain the user ID and password to the jeweler's bank account and thus was able to steal ¥210,000 by transferring the money into his own bank account. Furthermore, he is suspected of stealing more than ¥11.4 million from more than 10 companies using spyware.<sup>2</sup>
- **Spyware application used to hoard customer information.** United States: Antispyware vendor Sunbelt Software discovered a keylogger making its way around the Internet. This keylogger was logging users' Internet sessions, specifically items typed in HTML forms, which included login and password information for many bank sites. It was reported that this keylogger stole confidential information on customers from more than 50 different banks.<sup>3</sup>

Unfortunately, the threat of spyware is only getting worse. Advertising companies like Claria use spyware or greyware that hides on users' PCs and displays ads, driving revenue to the firms.<sup>4</sup> In addition, organized crime is now turning to spyware to steal bank account and credit card numbers. Virus creators have turned their efforts to creating spyware, seeking out greater financial gain. In January 2005, Forrester conducted a survey of roughly 200 technology decision-makers from North American SMBs and enterprises — the results show that spyware was considered the No. 4 threat to these organizations.<sup>5</sup> However, when we asked this same question in June 2005 to SMBs, the spyware threat had moved up to No. 2, while viruses and worms took the No. 1 spot.<sup>6</sup>

Traditional antivirus (AV) software cannot fully protect users against the threat of spyware, nor can client firewalls. Another tool is needed to help mitigate the spyware threat. Specific antispyware

tools have been developed to fight the intricacies of this type of malicious code. Today's endpoint antispyware tools are offered as either standalone solutions or as part of a client security suite.

### Standalone Antispyware Versus An Integrated Client Security Suite

When organizations deploy an antispyware solution, they need to decide between a standalone solution that is dedicated to the detection and removal of spyware and a solution that is part of an endpoint security suite. To date, best-of-breed solutions have won out — only 24% of organizations use client security suites when deploying an antispyware tool, whereas 65% use standalone solutions.<sup>7</sup> However, organizations will begin to switch to client security suites as these tools catch up to best-of-breed tools and offer the same level of functionality with less administration and management overhead. Because of this, vendors offer different options to win market share — some offering both standalone and suite solutions.

- **Standalone antispyware vendors.** Companies that have AV software from a vendor that does not offer antispyware protection would most benefit from standalone antispyware. While the number of vendors in this category will continue to decline due to acquisitions by the large security suite vendors, standalone antispyware vendors have been able to maintain some advantages. They have been in the antispyware market longer than the suite vendors, allowing them to offer customers a more customizable product with more granular control over scanning. These vendors include: Aluria Software, CA (formerly PestPatrol), Tenebril, Trend Micro (whose standalone antispyware tool came through an acquisition of InterMute), Sunbelt Software, and Webroot Software.<sup>8</sup> In addition, McAfee offers a standalone antispyware product for those companies that do not want a client security suite.
- **Client security suite vendors.** Companies that use AV software from a vendor that also offers antispyware should add the antispyware functionality to their current solution. The suite solutions offer solid antispyware protection and help keep administrative overhead to a minimum. While client security suites that include antispyware protection generally do not have the advanced customization of the point products, the suite vendors have something more to offer — an integrated client security tool set that offers protection far superior to point products alone.<sup>9</sup> Today's suites can include AV, antispyware, personal firewalls, and host IPS functionality all in a single agent. Firms with distributed environments and a significant number of mobile users will need the additional functionality offered by a client security suite. Vendors in this category include: CA, Check Point, McAfee, Panda Software, Sophos, Symantec, and Trend Micro.

In addition to the security vendors listed above, systems management vendors such as BigFix and LANDesk have started to offer antispyware protection as part of their security configuration management suites. More significantly, Microsoft will enter the enterprise antispyware market in the middle of 2006. Microsoft has already entered the consumer antispyware space, but plans to release an enterprise suite — Microsoft Client Protection — including AV, antispyware, personal firewall,

and host IPS to compete with the large security vendors. With Microsoft entering the market, should companies wait to see if Microsoft can deliver? Companies without an antispyware solution need to deploy one immediately — waiting for Microsoft's enterprise product is not an option. However, companies looking to switch out their current solution would benefit most from waiting a year to see what Microsoft comes up with.

### Other Security Tools Provide A Layered Defense, But More Protection Is Needed

Antispyware protection goes beyond the endpoint. Many vendors have developed antispyware solutions or content-filtering tools that sit at the gateway and are able to block spyware *before* it is downloaded and executed on an endpoint machine; however, these solutions cannot clean machines after an infection and cannot protect them outside of the corporate network. Gateway solutions are offered from vendors such as Barracuda Networks, Blue Coat Systems, McAfee, and Trend Micro. In addition, there are many other tools available to help mitigate the threat of spyware, including:

- **Content/URL filtering solutions.** Solutions from vendors such as SurfControl and Websense can prevent users from going to known spyware sites where drive-by downloads can easily infect systems. This type of solution is able to block specific Web sites or types of Web sites, but it is unable to stop malicious downloads from unknown sites or clean an infected machine.
- **Application and device control.** Control solutions from vendors such as Centennial Software, Safend, and SecureWave can prevent unauthorized applications and devices from being loaded onto an endpoint. This helps prevent malicious code from being installed through the use of applications and devices. Again, however, there are no remediation capabilities.
- **Access control.** SSL VPN products from vendors like Aventail and Juniper Networks and network quarantine capabilities from vendors like Cisco and Symantec/Sygate can scan endpoints to make sure that they satisfy all security policies before they are allowed onto the corporate network.<sup>10</sup> This type of solution is ideal for enterprises that want to assure that unmanaged devices are scanned for corporate compliance; however, these tools in themselves have no “scan-and-block” or malicious code removal capabilities. In addition, these solutions typically have many moving parts and complicated policies, creating a costly barrier to entry.<sup>11</sup>

While all of these solutions have their place in client and network security, none of them offer customers complete protection against spyware. Effectively combating spyware requires a comprehensive set of tools that can both detect and block the changing mutations of spyware and remove spyware from infected machines. In addition, what is spyware to one organization is an important business tool for another — remote control tools, for example, are used for support calls by many organizations, while they are seen as a remote access back door by others. Antispyware tools must allow administrators to choose which threats to block.

## ENTERPRISE ANTISPYWARE EVALUATION OVERVIEW

To assess the state of the enterprise antispyware market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top enterprise antispyware vendors.

### Evaluation Criteria

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria (see Figure 1). We evaluated vendors against approximately 105 criteria, which we grouped into three high-level buckets:

- **Current offering.** To assess product strength, we evaluated each offering against three groups of criteria: architecture, antispyware functionality, and administration and management. We did not, however, assess the product's strength in signature database and detection rates. Our goal was to evaluate these products on functionality that cannot easily be tested — their ability to be used in an enterprise environment.
- **Strategy.** A vendor's plan to further link pure-play antispyware with a unified client security suite is a crucial component of its strategy. Companies will benefit from deploying integrated tool sets that let the security/desktop team easily manage all client security components. We also evaluated each vendor's overall focus on the security market and its financial resources to support its future strategy. Finally, we included total product cost as part of the strategy evaluation.
- **Market presence.** We combined information about each vendor's installed base, recent sales momentum, revenues, employee numbers, and partnerships to determine market presence.

### Evaluation Methodology

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution:

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their product's functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with at least one of each vendor's current customers.

**Figure 1** Evaluation Criteria

CURRENT OFFERING	
Architecture	How well is the product built for delivering stability, performance, and scalability?
Client functionality	How does the product detect spyware? What technologies does the product use to protect systems against spyware? How much control do administrators have over the functionality of the product?
Administration and management	How robust are the vendor's administration and management capabilities?
STRATEGY	
Product strategy	What is the vendor's product strategy?
Corporate strategy	What is the vendor's corporate strategy?
Financial resources to support strategy	Is the vendor profitable? What is the vendor's cash flow? Does the vendor have sufficient revenues, profits, and cash flow to support its strategies?
Cost	What is the cost of the product?
MARKET PRESENCE	
Installed base	How large is the vendor's installed base of customers for this product and for all products?
Revenue	What is the vendor's revenue over the past four quarters?
Revenue growth	What is the vendor's year-over-year revenue growth over the past four quarters?
Systems integrators	How many integrator partners have completed three or more deployments of any version of this product in the past 18 months?
Services	How strong are the vendor's implementation and training services?
Employees	How many engineers does the vendor have dedicated to this product? How big is the vendor's sales presence?
Technology partners	How strongly do technology partners support this product?

Source: Forrester Research, Inc.

## Evaluated Vendors

Forrester included eight vendors in the assessment: Aluria Software, CA, McAfee, Tenebril, Trend Micro, Sunbelt Software, Symantec, and Webroot Software. Each of these vendors has:

- **A client-based solution.** While gateway antispyware products are important, they are unable to: 1) protect users when they are outside of their corporate network; and 2) clean up spyware already installed on an endpoint. Because of this, Forrester evaluated only products that are client-based.
- **Enterprise scalability.** Because enterprises have different needs than consumers, Forrester only evaluated products that were developed with enterprises in mind. Each of the products that we evaluated can support at least 1,000 nodes — the more mature products can support hundreds of thousands — and manage them through a single console.
- **Advanced customizability.** Enterprises will have different requirements and will often have different antispyware policies. Forrester spoke with end users to learn about what was on the top of their lists when choosing an antispyware vendor — all of the large enterprises told us that the ability to customize which applications are allowed/not allowed on their endpoints is essential. They also mentioned the importance of setting policies and scanning schedules — all of which they customize to different groups of users. Therefore, Forrester only evaluated products that give granular control to administrators.

## DEDICATED SECURITY VENDORS WIN OUT

The evaluation uncovered a market in which (see Figure 2):

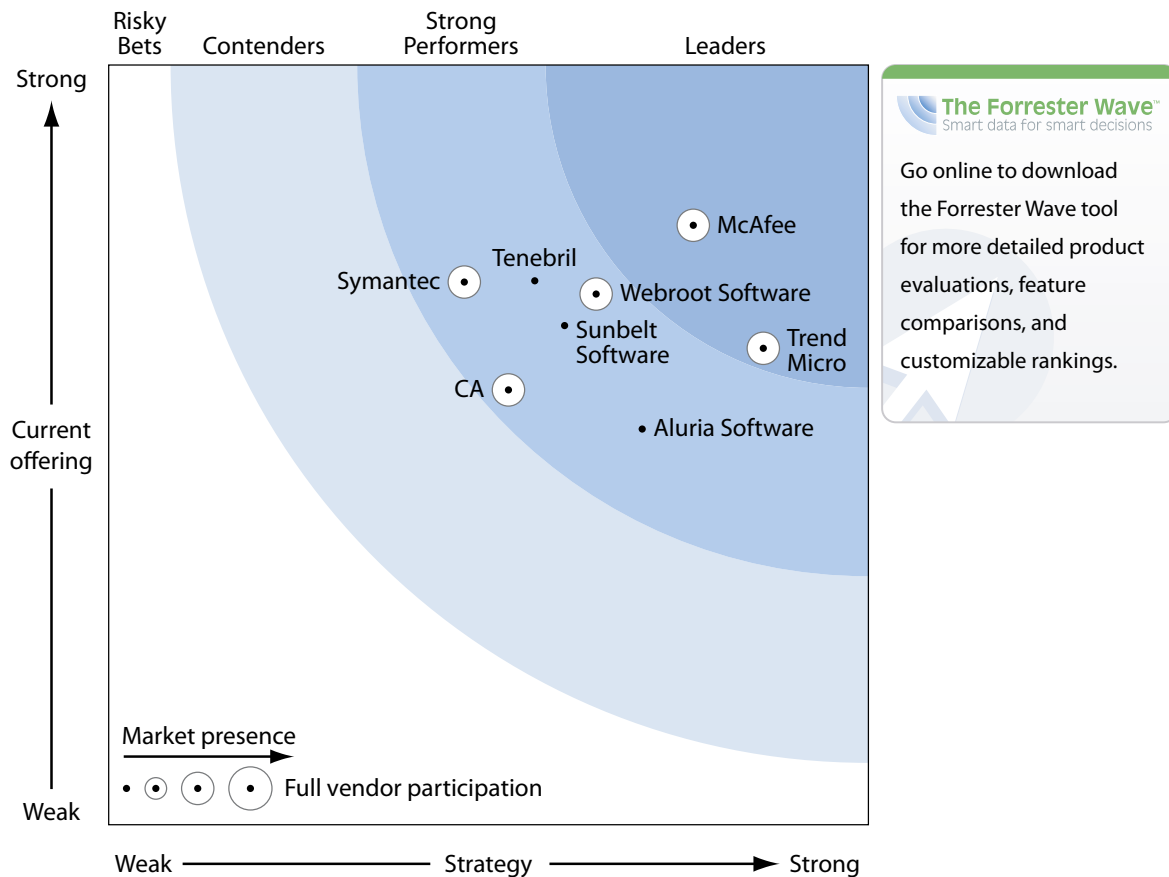
- **McAfee and Trend Micro lead the pack.** As dedicated security vendors, McAfee and Trend Micro are able to dedicate significant resources to their antispyware products. Their offerings are designed for the enterprise, scaling to a virtually limitless number of nodes. Both products offer a single management console for all aspects of the product, including very detailed reporting. McAfee's distinguishable strength is its protection against unknown spyware, while Trend offers full remote administration. Going forward, McAfee and Trend Micro will benefit from their multiple form-factor antispyware products, include standalone, suite, and gateway solutions.
- **Webroot, Sunbelt, Tenebril, and Aluria offer competitive standalone options.** As standalone antispyware vendors, all four vendors have been in the antispyware market for longer than their suite competitors. Because of this, they are able to offer more customizable scanning options as well as increased antispyware functionality, such as Web site filtering and user-defined spyware detection rules. However, these products tend to fall behind their large security vendor counterparts in scalability and reporting features. To stay competitive, these vendors must move beyond spyware protection to overall malicious code and hacker protection.

Standalone antispyware vendors that do not expand into other areas will either become acquisition targets or fade into obscurity.

- **Symantec and CA have strong products but lack focus.** Both firms offer antispyware products with a solid architecture that are highly scalable and offer customers a fail-safe way to ensure that all machines are constantly updated. However, Symantec and CA have broad product portfolios that cross into systems and storage management and lack the focus of dedicated security vendors. In addition, their products are more expensive than most of their competitors.

This evaluation of the enterprise antispyware market is intended to be a starting point only. Readers are encouraged to view detailed product evaluations and adapt the criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

**Figure 2** Forrester Wave™: Enterprise Antispyware, Q1 '06



Source: Forrester Research, Inc.

**Figure 2** Forrester Wave™: Enterprise Antispyware, Q1 '06 (Cont.)

	Forrester's Weighting	Aluria Software	CA	McAfee	Sunbelt Software	Symantec	Tenebrill	Trend Micro	Webroot Software
<b>CURRENT OFFERING</b>	50%	2.61	2.86	3.95	3.29	3.57	3.58	3.14	3.49
Architecture	30%	2.60	3.26	3.83	3.71	3.97	3.70	3.73	3.90
Client functionality	50%	3.04	2.60	3.98	3.19	3.21	3.78	2.93	3.74
Administration and management	20%	1.54	2.93	4.05	2.92	3.85	2.93	2.78	2.28
<b>STRATEGY</b>	50%	3.51	2.63	3.85	3.00	2.34	2.81	4.31	3.21
Product strategy	30%	1.70	3.10	3.50	2.00	2.80	1.70	3.70	1.70
Corporate strategy	20%	5.00	1.00	5.00	3.00	3.00	5.00	5.00	5.00
Financial resources to support strategy	20%	4.00	3.00	3.00	3.00	3.00	2.00	5.00	4.00
Cost	30%	4.00	3.00	4.00	4.00	1.00	3.00	4.00	3.00
<b>MARKET PRESENCE</b>	0%	1.76	2.75	3.07	1.80	2.31	1.03	2.15	3.17
Installed base	30%	0.85	2.55	3.30	2.45	0.00	1.60	0.85	4.60
Revenue	10%	1.00	5.00	4.00	1.00	5.00	0.00	3.00	2.00
Revenue growth	20%	5.00	1.00	3.00	3.00	3.00	0.00	3.00	5.00
Systems integrators	10%	0.00	2.00	5.00	0.00	0.00	0.00	0.00	0.00
Services	10%	2.50	3.50	1.50	0.00	2.50	2.50	4.50	1.50
Employees	10%	1.00	2.80	1.80	0.60	4.60	1.00	2.90	2.40
Technology partners	10%	0.50	4.50	2.50	3.00	5.00	2.00	2.50	2.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

## VENDOR PROFILES

### Leaders

- McAfee.** McAfee Anti-Spyware Enterprise is an add-on module to its McAfee VirusScan Enterprise 8.0i. Customers with the AV product already in-house can easily upgrade and be up and running with antispyware protection in minutes. As with most McAfee products, ePolicy Orchestrator (ePO) is the central management console for the antispyware module, which allows for very granular administration. In addition, McAfee's recent release of a standalone version of its antispyware protection allows non-McAfee AV customers to use McAfee Anti-Spyware Enterprise. McAfee is a good choice for any company looking to deploy client security.<sup>12</sup>

- **Trend Micro.** Trend Micro is delivering what enterprise customers want — an option for either a standalone or an integrated antispyware solution. Forrester evaluated Trend's standalone antispyware solution called Trend Micro Anti-Spyware Enterprise Edition (ASEE). ASEE works best when paired with Trend's enterprise management console, Trend Micro Control Manager (TMCM). Together, the two products can manage an unlimited number of endpoints and can produce comprehensive reports on all protected machines. Trend does not offer protection against unknown spyware.<sup>13</sup>

### Strong Performers

- **Webroot Software.** Webroot's Spy Sweeper Enterprise is a standalone antispyware solution that will easily work in any Windows environment. Its flexible architecture allows administrators to easily localize distribution points for large enterprise environments. Webroot's differentiator is Phileas, its automated spyware crawler that proactively searches the Web for new spyware. Phileas aims to find spyware at the moment of release and thus protect customers against zero-day spyware. However, for Webroot to remain competitive, it needs to compete with the suite vendors by at least offering customers antivirus functionality.<sup>14</sup>
- **Tenebril.** Tenebril's SpyCatcher Enterprise is a solid enterprise-class antispyware solution. While the product only supports up to 10,000 workstations, SpyCatcher has all of the advanced functionality that enterprises need, such as integration with LDAP and Active Directory, as well as customized application blacklists. However, as a small player in a niche market, Tenebril's days are numbered. We predict that ongoing security consolidation will likely force SpyCatcher to be incorporated into a security giant's product suite.<sup>15</sup>
- **Sunbelt Software.** Sunbelt Software's CounterSpy Enterprise is a standalone antispyware solution. It is highly scalable, as each CounterSpy server can support approximately 1,500 nodes, and the management console can support an unlimited number of servers. The product pulls information from Active Directory and Network Neighborhood, allowing administrators to create groups and policies based on existing directory structures. However, policy creation and reporting can only be done on a per-server basis — an organization with multiple CounterSpy servers cannot create policies or report on the agents in aggregate. As a result, we feel Sunbelt is a good fit for smaller companies with primarily fixed-location users and desktops.<sup>16</sup>
- **Aluria Software.** Aluria Software's Paladin standalone antispyware solution currently protects more than 120,000 enterprise nodes — and more than 30 million consumer PCs rely on Paladin's underlying technology to keep them spyware-free. The product features kernel-level protection, which blocks known spyware before installation and supports multiple scanning options. However, Paladin neither protects users from unknown spyware nor allows administrators to create custom application blacklists.<sup>17</sup>

- **Symantec.** Symantec AntiVirus Corporate Edition 10.0 (SAV 10) offers customers protection against both viruses and spyware in its single AV agent — at no additional cost. While this is a great addition for Symantec customers, non-Symantec AV customers should look elsewhere for their antispyware protection, unless they are willing to completely swap out their current AV. This is a missed opportunity for Symantec — a standalone antispyware offering would give Symantec the opportunity to win new customers.<sup>18</sup>
- **CA.** CA offers its eTrust PestPatrol Anti-Spyware Corporate Edition r8 as both a standalone and an integrated solution; the suite solution includes a single AV and antispyware client agent. Managed through CA's Web-based Threat Management server, the product supports up to 5,000 nodes per redistribution server and an unlimited number of redistribution servers, which allows the product to support even the largest environment. For CA to remain competitive, it must add advanced antispyware functionality, including protection against unknown spyware and user-defined spyware definitions.<sup>19</sup>

## SUPPLEMENTAL MATERIAL

### Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

### The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and readers are encouraged to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

## ENDNOTES

- <sup>1</sup> Source: The Register ([http://www.theregister.co.uk/2005/06/09/spyware\\_probe\\_pi\\_injured/](http://www.theregister.co.uk/2005/06/09/spyware_probe_pi_injured/)).
- <sup>2</sup> Source: The Japan Times (<http://www.japantimes.co.jp/cgi-bin/makeprfy.pl5?nn20051111a7.htm>).
- <sup>3</sup> Source: Computer Crime Research Center (<http://www.crime-research.org/news/13.08.2005/1426/>).
- <sup>4</sup> Source: <http://www.benedelman.org/>.
- <sup>5</sup> In January 2005, Forrester surveyed 200 technology decision-makers at North American companies about their approaches to IT security. Although the vast majority of companies have deployed antivirus products at both the host and the gateway level, respondents ranked viruses and worms as the most significant threat to their organizations. Employees acting in unauthorized ways ranked as the second most significant threat. To help counteract these threats, companies are deploying client and gateway antivirus programs, personal and network firewalls, antispyware, and host- and network-based intrusion detection systems (IDS) or intrusion protection systems (IPS). See the March 25, 2005, Trends “[IT Security Threats In 2005: Viruses And Worms Top The List.](#)”

- <sup>6</sup> SMB IT groups consider viruses, worms, and spyware to be their most dangerous security threats. For that reason, 59% of them will purchase network firewalls, 57% will purchase antispyware software, and 45% will purchase host antivirus software in 2005. However, only 21% of SMBs will purchase host-based IPS, and only 13% will buy patch management — key technologies used to prevent viruses and worms. See the September 21, 2005, Data Overview “[The State Of Security In SMBs And Enterprises: Business Technographics® North America.](#)”
- <sup>7</sup> In January 2005, Forrester surveyed 200 technology decision-makers at North American companies about their approaches to IT security. We learned that companies overwhelmingly prefer best-of-breed client security products to client security suites by nearly a 3-to-1 margin. Despite consolidation in the client security market, firms like to pick and choose the components of their IT architecture rather than rely on one vendor to watch over all of their endpoint clients. That most of the product suites aren't yet fully integrated also drives buyers toward a best-of-breed approach. See the February 28, 2005, Trends “[Client Security Trends: Users Opt For Best-Of-Breed Tools.](#)”
- <sup>8</sup> Trend Micro's acquisition of InterMute gives Trend entrée to the millions of InterMute's SpySubtract users. This instantly establishes Trend's presence in the North American antispyware market and gives it an important beachhead in the heated battle for desktop security leadership. The move could not have come at a better time for Trend Micro. This year, a full 65% of companies will invest in antispyware tools. Moreover, organizations express strong preference for best-of-breed solutions over integrated client security suites. Trend will rebrand SpySubtract as its own best-of-breed tool for both consumers and businesses and start getting its foot in the door of coveted Symantec and McAfee enterprise shops prior to the inevitable client security vendor rationalization that customers will begin undertaking in 12 to 18 months. See the May 13, 2005, Quick Take “[Trend Micro Enhances Antispyware Offering.](#)”
- <sup>9</sup> Today, endpoint machines are vulnerable to all types of attacks. Antivirus and perimeter defenses alone no longer provide adequate defense against malicious code, particularly as workers become increasingly mobile. Malicious code is also changing too rapidly for traditional defenses to keep up. Firms must look to a suite of client security products — typically, these include antivirus, antispyware, client firewall, and at least some host intrusion prevention (HIPS) capability — to protect endpoints from malware. Forrester evaluated the strengths and weaknesses of top client security suite vendors across 170 criteria. The result: McAfee and Symantec lead the pack for complete and robust client security tool sets; Trend Micro offers a comprehensive solution for known threats; and Computer Associates will offer a strong suite by the end of 2006. See the June 22, 2005, Tech Choices “[The Forrester Wave™: Client Security Suites, Q2 2005.](#)”
- <sup>10</sup> SSL VPNs provide better endpoint security. Closely tied to granularity, SSL VPNs leverage the additional application-level information to apply security policies to incoming users. This allows enterprises to apply more flexible security instead of the one-size-fits-all approach that IPsec requires. This comes in handy: A user may be identified as connecting from a trusted laptop, but what if that laptop's Symantec antivirus app is out of date? Resources like remediation portals redirect users to the Symantec Web site for updates before further passage to the network. See the December 31, 2004, Trends “[SSL VPNs Poised For Significant Growth.](#)”

- <sup>11</sup> Enterprises are eager to deploy network quarantine — technologies that dynamically restrict client systems' access to networks based on their compliance with policy. But a proper solution requires the complex integration of security software, networking hardware, and policy servers. So, how should firms prepare? By following three phases prior to enterprisewide rollout: 1) creating granular access and endpoint compliance policies; 2) deploying an interim overlay solution while updating LAN switch infrastructure; and 3) testing interoperability and consolidating endpoint security components. See the November 4, 2005, Best Practices ["Best Practices To Prepare For Network Quarantine."](#)
- <sup>12</sup> View the vendor summary for more detailed analysis on how McAfee fared in this evaluation. See the January 6, 2006, Tech Choices ["McAfee Leads In Enterprise Antispyware."](#)
- <sup>13</sup> View the vendor summary for more detailed analysis on how Trend Micro fared in this evaluation. See the January 6, 2006, Tech Choices ["Trend Micro Offers Large Enterprises Strong Standalone Enterprise Antispyware."](#)
- <sup>14</sup> View the vendor summary for more detailed analysis on how Webroot Software fared in this evaluation. See the January 6, 2006, Tech Choices ["Webroot Software Delivers Strong Best-Of-Breed Enterprise Antispyware For All Enterprises."](#)
- <sup>15</sup> View the vendor summary for more detailed analysis on how Tenebril fared in this evaluation. See the January 6, 2006, Tech Choices ["Tenebril Offers A True Best-Of-Breed Solution Without Staying Power In Enterprise Antispyware."](#)
- <sup>16</sup> View the vendor summary for more detailed analysis on how Sunbelt Software fared in this evaluation. See the January 6, 2006, Tech Choices ["Sunbelt Software Caters To The Non-Mobile Workforce With Its Enterprise Antispyware."](#)
- <sup>17</sup> View the vendor summary for more detailed analysis on how Aluria fared in this evaluation. See the January 6, 2006, Tech Choices ["Aluria Software Caters To Small Enterprises With Its Enterprise Antispyware Solution."](#)
- <sup>18</sup> View the vendor summary for more detailed analysis on how Symantec fared in this evaluation. See the January 6, 2006, Tech Choices ["Symantec Offers An Integrated Malicious Code Agent In Enterprise Antispyware."](#)
- <sup>19</sup> View the vendor summary for more detailed analysis on how CA fared in this evaluation. See the January 6, 2006, Tech Choices ["CA Bridges The Standalone And Integrated Suite Divide In Enterprise Antispyware."](#)

# FORRESTER®

Helping Business Thrive On Technology Change

## Headquarters

Forrester Research, Inc.  
400 Technology Square  
Cambridge, MA 02139 USA  
Tel: +1 617/613-6000  
Fax: +1 617/613-5000  
Email: [forrester@forrester.com](mailto:forrester@forrester.com)  
Nasdaq symbol: FORR  
[www.forrester.com](http://www.forrester.com)

## Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations,  
visit [www.forrester.com/about](http://www.forrester.com/about).*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or [resourcecenter@forrester.com](mailto:resourcecenter@forrester.com). We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice about technology's impact on business and consumers. For 22 years, Forrester has been a thought leader and trusted advisor, helping global clients lead in their markets through its research, consulting, events, and peer-to-peer executive programs. For more information, visit [www.forrester.com](http://www.forrester.com).