

June 22, 2005

The Forrester Wave™: Client Security Suites, Q2 2005

by Natalie Lambert and David Friedlander

TECH CHOICES

June 22, 2005

The Forrester Wave™: Client Security Suites, Q2 2005

Lab-Based Evaluation Of Top Client Security Suites Vendors Across 170 Criteria

by **Natalie Lambert and David Friedlander**

with Jonathan Penn

EXECUTIVE SUMMARY

Since the first computer virus was created in 1981, the need for client security has grown monumentally. 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, antispymware, client firewall, and at least some host intrusion prevention (HIPS) capability — to protect endpoints from malware. To assess the state of the client security suite market and to see how the vendors stack up against each other, 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. Included in this report is an interactive vendor comparison tool that provides detailed product evaluations and customizable rankings.

TABLE OF CONTENTS

2 **The Emergence Of The Client Security Suite**

The Four Components Of Client Security Suites

3 **Client Security Suites Evaluation Overview**

Evaluation Criteria

Evaluation Methodology

Evaluated Vendors

6 **Client Security Suites Are Evolving — Expect Solid Solutions In 2006**

13 **Vendor Profiles**

Leaders

Strong Performers

15 **Supplemental Material**

NOTES & RESOURCES

Forrester conducted lab-based evaluations in March and April 2005, and interviewed vendor and user companies, including: Computer Associates, McAfee, Symantec, and Trend Micro.

Related Research Documents

“IT Security Threats In 2005: Viruses And Worms Top The List”

March 25, 2005, Trends

“Personal Firewall Adoption In 2005”

March 4, 2005, Trends

“Client Security Trends: Users Opt For Best-Of-Breed Tools”

February 28, 2005, Trends

“Antispymware Adoption In 2005”

February 10, 2005, Trends

“Best Practices: Desktop Security”

January 30, 2004, Planning Assumption

THE EMERGENCE OF THE CLIENT SECURITY SUITE

Viruses first emerged more than 20 years ago. Antivirus software was late to follow — the first antivirus program was developed almost 10 years later. Since then, antivirus software has been used to protect machines against malicious code. Yet today, viruses, worms, Trojan horses, and other malicious code have become more destructive and more complex. Antivirus tools alone are no longer able to protect machines adequately.

Simple signature-based antivirus tools worked well at the beginning, but these now need to be supplemented with additional tools. The increasing number of virus creators and viruses, as well as other types of malicious code, has made it impossible for antivirus vendors to keep up. In addition, organizations now face a multitude of different security threats that go well beyond traditional viruses and worms. While viruses and worms were rated as the No. 1 threat in January 2005, regulatory compliance, employees failing to follow security guidelines, spyware, and hackers also topped the list.¹

In order to fight the battle against malicious code, firms are beginning to use multiple client security tools: 80% of firms use antispyware tools on at least some systems in addition to antivirus typically deployed on all desktops and laptops.² However, even both of these traditional signature-based tools together don't provide adequate defense against zero-day attacks. Technology like client firewalls and host IPS (HIPS) supplements — but, despite some vendors claims, cannot replace — antivirus and antispyware. Alarming, only 23% of firms have deployed client firewalls on all of their desktops and laptops.³

The HIPS market is just emerging. Forrester estimates that less than 20% of firms have deployed or are piloting HIPS; but 31% of companies said that they would be investing in HIPS technology this year.⁴ Given the increasingly mobile and remote nature of the workforce and the rapidly changing nature of malicious code, traditional defenses desperately need to be supplemented by client firewalls and HIPS.

The Four Components Of Client Security Suites

Client security suites span this set of protective technologies in a bundled or integrated package. Although 65% of firms have opted to deploy best-of-breed tools today, Forrester expects the market to shift quickly toward client security suites as the leading security vendors enhance functionality across key areas.⁵ Client security suites offer customers a more layered approach to client security than using antivirus by itself, protecting against: known malicious code through signature-based technology; unknown malicious code or attacks using heuristics-based technology like HIPS; and network-based attacks or even outbound traffic from malicious applications using client firewalls.

In addition, client security suites can be managed together, unlike multiple best-of-breed tools that require separate management consoles. The unified approach to client security also allows security managers to track threat information more easily across the organization.

Client security suites include many of the following:

- **Antivirus.** Antivirus software, the most fundamental form of client security, is generally a signature-based tool that protects machines against viruses. As new viruses are found, antivirus vendors create signatures, a form of digital fingerprint, to detect and remove specific viruses.
- **Antispyware.** Antispyware software, like antivirus products, provides a signature-based defense that protects machines against known spyware. As new spyware and adware are found, additional signatures are created to identify this malware.
- **Personal firewall.** Personal firewalls are the first line of defense for the endpoint machine. They are designed to prevent unauthorized access both to and from the machine. They can prevent hackers from taking control of a user's computer through inbound port blocking and can prevent worms and other malicious code from spreading using outbound port blocking.
- **Host IPS.** Unlike antivirus and antispyware, host IPS is a behavior-based technology. It monitors system activity and notifies administrators when it suspects suspicious activity; most products block suspicious executables or processes from running by default. Well-designed HIPS products allow administrators to create policies and rules for their firm's environment to select which applications to permit or block.

A comprehensive client security solution is essential. Today, companies have laptops entering and exiting the corporate network continuously (i.e., consultants, contractors, and mobile and remote employees). PCs that leave the corporate network will invariably connect to an insecure network and bring back any malicious code they picked up along the way. With computers popping in and out of the perimeter, securing the corporate network takes more than just antivirus.

CLIENT SECURITY SUITES EVALUATION OVERVIEW

To assess the state of the Client Security Suite market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top Client Security Suite 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 170 criteria, which we grouped into three high-level buckets:

- **Current offering.** To assess product strength, we evaluated each offering against seven groups of criteria: architecture, antivirus, antispyware, personal firewall, intrusion prevention and other features, administration and management, and standards and interoperability.

Figure 1 Evaluation Criteria

CURRENT OFFERING	
Architecture	How well is the product built for delivering stability, performance, and scalability?
Antivirus	Does the product include antivirus software?
Antispyware	Does the product include antispyware software?
Personal firewall	Does the product include personal firewall software?
Intrusion prevention and other features	Does the product include intrusion detection and prevention features?
Administration and management	How robust are the administration and management capabilities?
Standards and interoperability	What vendor-neutral standards does the platform support? What major third-party products does the platform interoperate with?
STRATEGY	
Cost	What is the cost of this product?
Focus	What percentage of the vendor's revenues are from security products and services versus other product lines?
Product strategy	How strong is the vendor's product strategy?
Vulnerability assessment and remediation	Does the vendor provide vulnerability assessment and remediation products? Do these integrate with the client security management suite?
Unified architecture	What enhancements does the vendor plan to make to its product architecture? Will it share a common architecture with other products in the vendor's portfolio?
MARKET PRESENCE	
Installed base	How large is the vendor's installed base of customers for this product and for all products?
Systems integrators	How strongly do systems integrator partners support this product?
Contact center	How strong is the vendor's customer service contact center?
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?
Revenue	How strong is the vendor's financial position?
Revenue growth	What is the vendor's year-over-year quarterly revenue growth?

Source: Forrester Research, Inc.

- **Strategy.** We compared the product and go-to-market strategies of each company with Forrester's forward-looking vision of the client security market to assess how well each vendor is positioned for future success.
- **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:

- **Hands-on lab evaluations.** Vendors spent one day with a team of analysts who performed a hands-on evaluation of the product using a scenario-based testing methodology. We evaluated each product using the same scenario(s), creating a level playing field by evaluating every product on the same criteria.
- **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.

Evaluated Vendors

Forrester included four vendors in the assessment: Computer Associates, McAfee, Symantec, and Trend Micro. Each of these vendors has:

- **Solutions that provide protection against known threats.** Because viruses and worms are the No. 1 threat to an organization, Forrester chose to evaluate products that first and foremost protect machines against these known threats. Some of the more mature products also provide protection against unknown threats.
- **Central management features for all product functionality.** Firms require centralized control of their client computing environment. The ability to schedule antivirus and antispyware scanning, create policies, and take action on infected machines from a central console is a necessity for enterprises. Forrester chose to evaluate these products that are catered toward the enterprise.
- **Revenues of more than \$500 million.** To ensure vendor viability, Forrester evaluated vendors that have substantial revenues to sustain them. Smaller firms can introduce new technology like antispyware tools before the established vendors but cannot compete effectively in the long term in the global market. Our criteria are geared toward large deployments as well as firms that may have other client security products already in house and/or want to add additional layers of security.

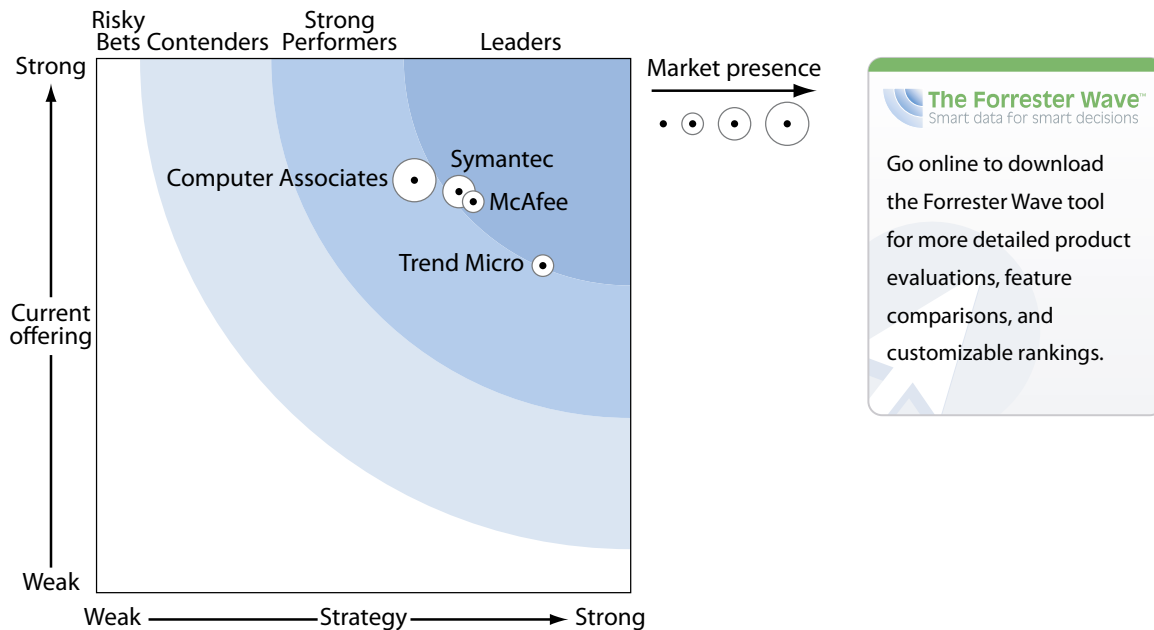
Our evaluation methodology depends in part on input from the vendors, including lab evaluations, questionnaires, and customer references.

CLIENT SECURITY SUITES ARE EVOLVING — EXPECT SOLID SOLUTIONS IN 2006

Client security suites are just beginning to evolve and emerge as viable solutions for comprehensive desktop and mobile security. Over the next two years, the client security market will transition from point products to product suites. The vendors we evaluated are at different stages of building out their client security suites, but all of them plan to offer suites by the end of 2006 that can protect endpoints against both known and unknown threats. Through the evaluation process, we discovered that each of the vendors had different strengths. To address this, we developed a Forrester Wave for each of the three most important features today:

- **Security tools for today’s known threats.** In this scenario, we focused on evaluating suites that provide strong protection against known threats, like antivirus and antispyware functionality. We also put significant weight on robust update features, to make sure that endpoints would always have the latest updates in a timely manner. Customers that have chosen to deploy best-of-breed firewall and HIPS products, or have a limited need for these tools, should focus on vendors that offer strong antivirus and antispyware protection (see Figure 2).

Figure 2 Forrester Wave™: Client Security Suites: Known Threats, Q2 '05



Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Client Security Suites: Known Threats, Q2 '05 (cont.)

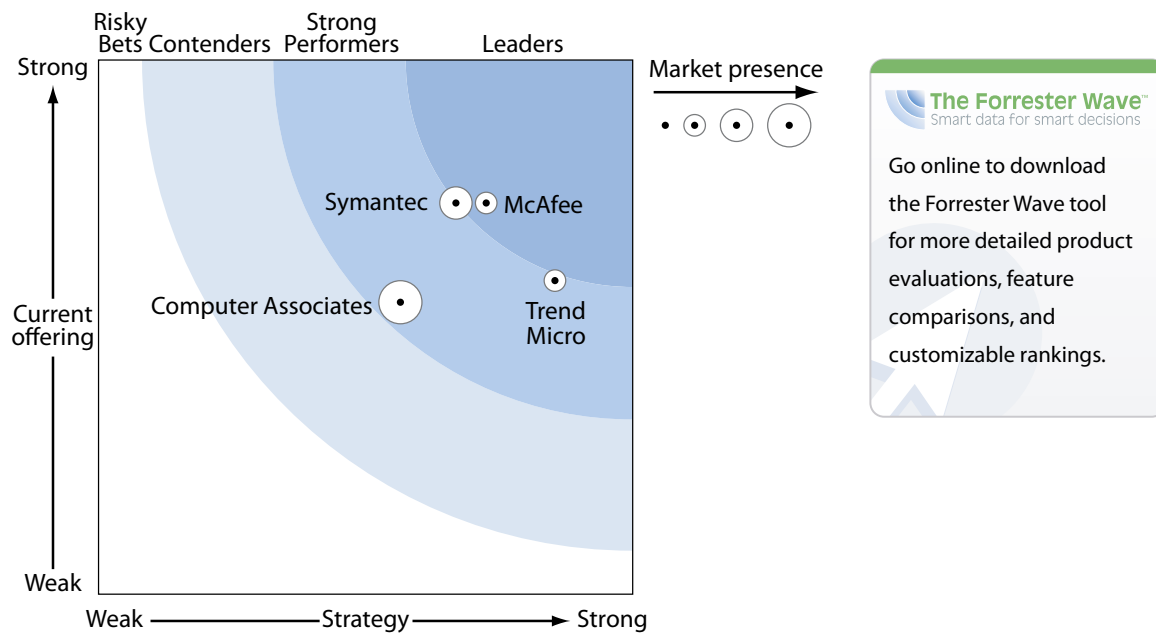
	Forrester's Weighting	Computer Associates	McAfee	Symantec	Trend Micro
CURRENT OFFERING	50%	3.82	3.65	3.73	3.04
Architecture	15%	3.77	3.32	2.91	3.13
Antivirus	47%	4.28	3.90	4.06	3.47
Antispyware	25%	3.63	3.60	3.98	2.53
Personal firewall	0%	0.00	3.85	3.70	1.30
Intrusion prevention and other features	0%	0.00	5.00	3.11	0.00
Administration and management	8%	3.01	3.69	4.44	3.80
Standards and interoperability	5%	1.88	2.44	0.68	0.20
STRATEGY	50%	2.98	3.52	3.39	4.18
Cost	10%	1.30	0.65	3.35	5.00
Focus	15%	1.00	5.00	3.00	5.00
Product strategy	45%	4.00	4.00	4.00	4.50
Vulnerability assessment and remediation	20%	4.00	3.00	4.00	3.00
Unified architecture	10%	1.00	3.00	0.00	3.00
MARKET PRESENCE	0%	3.40	2.24	2.98	2.66
Installed base	5%	4.25	0.00	4.25	3.70
Systems integrators	5%	2.00	0.00	0.30	5.00
Contact center	5%	4.10	3.50	3.20	4.20
Services	5%	4.25	2.85	3.25	4.35
Employees	20%	4.20	3.00	3.00	3.00
Technology partners	10%	0.75	5.00	0.50	3.75
Revenue	40%	4.00	2.00	3.50	1.25
Revenue growth	10%	1.50	0.25	3.75	3.25

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

Source: Forrester Research, Inc.

- **Unified product architecture and manageability.** A unified architecture lowers administration costs and often allows security managers to set policies across several security functions. Configurability is important in allowing administrators flexibility in managing their environment. Here we focused on products with unified architectures; centralized management and reporting consoles; strong updating features; scalability; and configurable actions, alerts, and notifications. Firms that need to manage client security centrally across a global, distributed enterprise should focus on suites with robust manageability and a unified architecture (see Figure 3).

Figure 3 Forrester Wave™: Client Security Suites: Architecture And Mgmt., Q2 '05



Source: Forrester Research, Inc.

Figure 3 Forrester Wave™: Client Security Suites: Architecture And Mgmt., Q2 '05 (cont.)

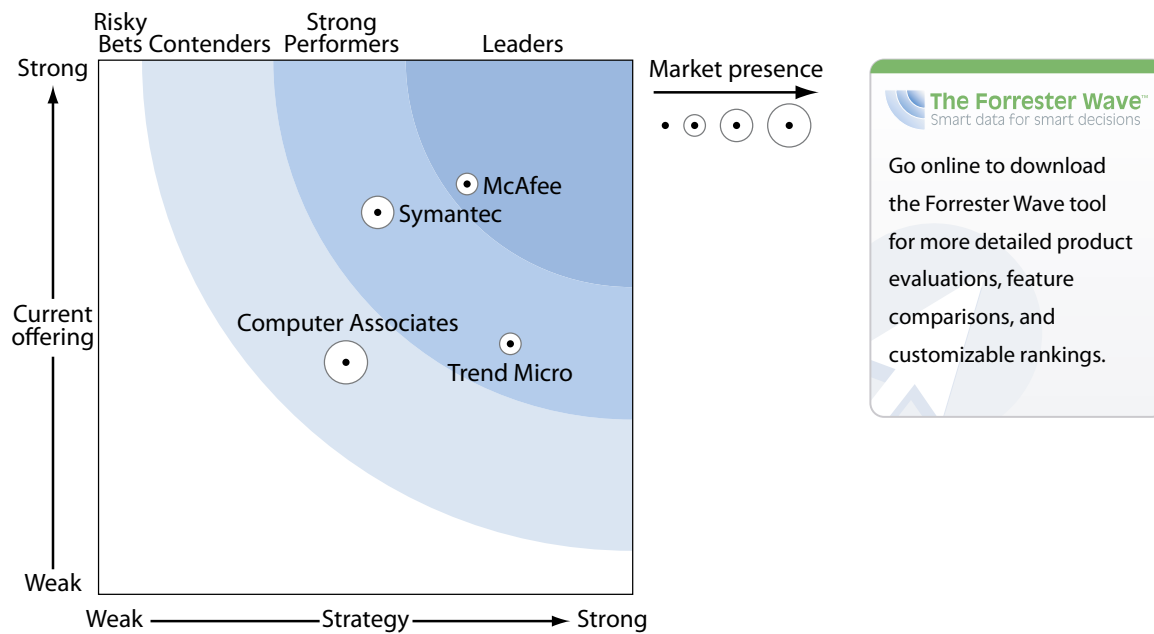
	Forrester's Weighting	Computer Associates	McAfee	Symantec	Trend Micro
CURRENT OFFERING	50%	2.71	3.64	3.62	2.92
Architecture	25%	2.90	3.48	3.48	3.77
Antivirus	20%	3.98	3.85	3.90	3.50
Antispyware	15%	3.08	3.65	3.88	1.98
Personal firewall	5%	0.00	3.85	3.70	1.30
Intrusion prevention and other features	5%	0.00	5.00	3.11	0.00
Administration and management	25%	2.53	3.55	4.07	3.63
Standards and interoperability	5%	1.88	2.44	0.68	0.20
STRATEGY	50%	2.83	3.62	3.34	4.28
Cost	10%	1.30	0.65	3.35	5.00
Focus	20%	1.00	5.00	3.00	5.00
Product strategy	45%	4.00	4.00	4.00	4.50
Vulnerability assessment and remediation	15%	4.00	3.00	4.00	3.00
Unified architecture	10%	1.00	3.00	0.00	3.00
MARKET PRESENCE	0%	3.40	2.24	2.98	2.66
Installed base	5%	4.25	0.00	4.25	3.70
Systems integrators	5%	2.00	0.00	0.30	5.00
Contact center	5%	4.10	3.50	3.20	4.20
Services	5%	4.25	2.85	3.25	4.35
Employees	20%	4.20	3.00	3.00	3.00
Technology partners	10%	0.75	5.00	0.50	3.75
Revenue	40%	4.00	2.00	3.50	1.25
Revenue growth	10%	1.50	0.25	3.75	3.25

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

Source: Forrester Research, Inc.

- **Breadth of client security suite.** In this scenario, we focused on complete client security suites that include all of the functional areas in our evaluation — antivirus, antispyware, personal firewall, and HIPS. We put significant weight on products that offer HIPS and personal firewall functionality. HIPS technology protects PCs against zero-day viruses and other unknown malicious code. Signature-based antivirus and antispyware software only provide complete protection against known malicious code. Firms that have not deployed HIPS or client firewalls and are in the process of re-evaluating their client security solutions should look to complete client security suites (see Figure 4).

Figure 4 Forrester Wave™: Client Security Suites, Q2 '05



Source: Forrester Research, Inc.

Figure 4 Forrester Wave™: Client Security Suites, Q2 '05 (cont.)

	Forrester's Weighting	Computer Associates	McAfee	Symantec	Trend Micro
CURRENT OFFERING	50%	2.15	3.82	3.55	2.32
Architecture	20%	3.25	3.60	3.53	3.69
Antivirus	15%	3.73	3.85	3.90	3.55
Antispyware	15%	3.08	3.65	3.88	1.98
Personal firewall	15%	0.00	3.85	3.70	1.30
Intrusion prevention and other features	15%	0.00	5.00	3.11	0.00
Administration and management	15%	2.55	3.53	4.18	3.67
Standards and interoperability	5%	1.88	2.44	0.68	0.20
STRATEGY	50%	2.31	3.45	2.62	3.86
Cost	10%	1.30	0.65	3.35	5.00
Focus	20%	1.00	5.00	3.00	5.00
Product strategy	20%	4.40	4.40	4.40	4.30
Vulnerability assessment and remediation	20%	4.00	3.00	4.00	3.00
Unified architecture	30%	1.00	3.00	0.00	3.00
MARKET PRESENCE	0%	3.40	2.24	2.98	2.66
Installed base	5%	4.25	0.00	4.25	3.70
Systems integrators	5%	2.00	0.00	0.30	5.00
Contact center	5%	4.10	3.50	3.20	4.20
Services	5%	4.25	2.85	3.25	4.35
Employees	20%	4.20	3.00	3.00	3.00
Technology partners	10%	0.75	5.00	0.50	3.75
Revenue	40%	4.00	2.00	3.50	1.25
Revenue growth	10%	1.50	0.25	3.75	3.25

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

Source: Forrester Research, Inc.

The evaluation uncovered a market in which McAfee offers a strong solution for any company requirement. Its full product portfolio, robust management features, and strong architecture make it a great fit for companies looking for a client security solution. Digging deeper, we also found that:

- **Computer Associates offers the best protection against known threats.** Although Computer Associates is the newest entrant to the client security market, its eTrust Antivirus 7.0 is loaded with functionality. Its dual scanning engines, Vet and InoculateIT, are impressive; they allow administrators to run scans with both engines, essentially giving customers an extra layer of antivirus capability. In addition, CA's system cure functionality will restore system settings upon removal of a virus. CA also offers beta signatures to its customers, giving them access to immediate protection against emerging threats while the final version is being created. In many instances, the beta signatures are released a few hours before the final ones. Unfortunately, CA's PestPatrol is not as impressive as its antivirus product. The product lacks many key features, including the ability to customize how different categories of spyware are handled.

Symantec offers the strongest antispyware protection. Symantec offers spyware detection and removal tools and includes privacy controls for every client. This allows end users to enter personal information, such as social security or credit card number, into the client console. The system will monitor all outbound traffic to make sure that users' personal information never leaves the computer without their consent — a common trait of spyware.

- **Trend Micro excels in unified architecture, Symantec in manageability.** Trend Micro's OfficeScan 7.0 has the most unified architecture of the products we evaluated. A single management console controls all functions of the product — antivirus, antispyware, and a personal firewall — from deployment to reporting on incidents, and a single console on the client keeps its presence to a minimum. Because the management console is Web-based, administrators have the ability to manage the product remotely — a real advantage when in a distributed environment.

Symantec offers robust management features. The console and all alerts, errors, and notification messages are customizable to the needs of organization. However, Symantec's reporting console, Event Manager, is not integrated with the client security management console. This forces customers to purchase an additional reporting component that should come integrated with Symantec Client Security. Nevertheless, Symantec's reporting features are strong.

- **McAfee and Symantec offer the broadest client security suites.** McAfee and Symantec both offer complete protection for endpoint PCs, including antivirus, antispyware, personal firewalls, and host IPS. McAfee has the most comprehensive security suite; it is the only one that has full HIPS functionality. Unfortunately, Entercept, the HIPS product, is not fully integrated into the ePO management console, forcing customers to run two separate management consoles to get the full functionality of both products. McAfee plans to integrate the components in Q1 2006.

Symantec offers limited HIPS functionality but is fully integrated. Symantec provides all functionality through the Symantec Client Security suite. The limited HIPS functionality uses “generic exploit blocking” that protects customers from new variants of old viruses, without the need for new signatures. It also protects customers from buffer overflows from known vulnerabilities. Furthermore, Symantec will add a full-fledged HIPS product to its portfolio — Symantec Critical System Protection 4.5 — in June 2005. However, like McAfee’s Enterecept product, it will use a separate management console.

This evaluation of Client Security Suites is intended as a starting point only. Readers are encouraged to view detailed product evaluations and adapt the criteria weighting to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

VENDOR PROFILES

Although any of these vendors’ products provide robust client security functionality, companies need to closely examine their own needs to get the best vendor match. Companies should adjust the Forrester Wave spreadsheet weightings to reflect their own priorities, using the vendor profiles as general guidance.

Leaders

- **McAfee.** McAfee is the only vendor to offer a complete suite for endpoint security; but it is not fully integrated — yet. Its customers can use the ePolicy Orchestrator (ePO) management console to fully manage McAfee VirusScan Enterprise 8.0i, McAfee Anti-Spyware Enterprise, and McAfee Desktop Firewall. Enterecept, McAfee’s host IPS product, can currently be deployed and reported on through ePO but requires its own management. McAfee plans to offer a fully integrated product in early 2006.⁶
- **Symantec.** Symantec Client Security 3.0 (SCS) is a complete solution, including antivirus, antispysware, a personal firewall, and limited host IPS functionality. Symantec uses its “generic exploit blocking” functionality to protect customers against unknown virus/spyware variants and buffer overflows. Symantec will also enhance its host IPS functionality significantly in June 2005. Symantec is well-positioned to maintain a leadership position in the client security market.⁷

Strong Performers

- **Trend Micro.** Trend Micro OfficeScan 7.0 offers a client security suite that includes antivirus, antispysware, and personal firewall capabilities. To fill the host intrusion prevention system (IPS) gap and give its customers protection against zero-day viruses, Trend will partner with Cisco to offer its customers the Cisco Security Agent as an add-on to the Trend Micro Office Scan Suite beginning in early 2006.⁸

- **Computer Associates.** Computer Associates offers strong antivirus and sufficient antispysware functionality through its eTrust Threat Management product line — CA will improve its antispysware manageability in the next release. While the two feature sets, eTrust Anti-virus 7.1 and eTrust PestPatrol Antispysware 5.0 Corporate Edition, are offered as different products today, CA will be integrating the management functionality later this year. It will add client firewall functionality in 2005 and HIPS to its portfolio by late 2006.⁹

SUPPLEMENTAL MATERIAL

Online Resource

The online versions of Figures 2, 3, and 4 are Excel-based vendor comparison tools that provide detailed product evaluations and customizable rankings.

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 narrow our final list to those presented here. 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 this 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 weighting 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

- ¹ In January 2005, Forrester surveyed 200 technology decision-makers at North American companies about their approaches to IT security. Sixty-eight percent of respondents rated viruses and worms one of the top three threats to their organization. See the March 25, 2005, Trends “IT Security Threats In 2005: Viruses And Worms Top The List.”
- ² Although respondents ranked spyware fourth out of a list of nine possible threats to the organization, 80% of companies currently use antispymware tools. See the February 10, 2005, Trends “Antispymware Adoption In 2005.”
- ³ We learned that 63% of firms currently have personal firewalls deployed somewhere in their organization. However, many PCs remain unprotected from network worms, Trojans, and other security threats; only 23% of companies have personal firewalls deployed on all client machines. Enterprises should implement personal firewalls as a standard on all PCs. See the March 4, 2005, Trends “Personal Firewall Adoption In 2005.”

- ⁴ Sixty-five percent of the companies surveyed will be investing in antispyware tools this year. In addition, 57% will invest in client antivirus, 42% will invest in personal firewalls, and 31% will invest in host-based IDS or IPS. Companies have recognized that they can no longer rely on network and gateway products to protect the organization. See the March 25, 2005, Trends “IT Security Threats In 2005: Viruses And Worms Top The List.”
- ⁵ 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. See the February 28, 2005, Trends “Client Security Trends: Users Opt For Best-Of-Breed Tools.”
- ⁶ View the scorecard summary for more detailed analysis on how McAfee fared in this evaluation. See the June 22, 2005, Tech Choices “Client Security Suites Scorecard Summary: McAfee.”
- ⁷ View the scorecard summary for more detailed analysis on how Symantec fared in this evaluation. See the June 22, 2005, Tech Choices “Client Security Suites Scorecard Summary: Symantec.”
- ⁸ View the scorecard summary for more detailed analysis on how Trend Micro fared in this evaluation. See the June 22, 2005, Tech Choices “Client Security Suites Scorecard Summary: Trend Micro.”
- ⁹ View the scorecard summary for more detailed analysis on how Computer Associates fared in this evaluation. See the June 22, 2005, Tech Choices “Client Security Suites Scorecard Summary: Computer Associates.”

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
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

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

*For a complete list of worldwide locations,
visit 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. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester is an independent technology research company that provides pragmatic and forward-thinking advice about technology's impact on business. Business, marketing, and IT professionals worldwide collaborate with Forrester to align their technology investments with their business goals. Established in 1983, Forrester is headquartered in Cambridge, Mass.