

September 27, 2006

The Forrester Wave™: Client Security Suites, Q3 2006

by Natalie Lambert

TECH CHOICES



September 27, 2006

The Forrester Wave™: Client Security Suites, Q3 2006

McAfee Leads, With Symantec And Sophos Offering Viable Alternatives

by **Natalie Lambert**

with Jonathan Penn and Sarah Bernhardt

EXECUTIVE SUMMARY

Forrester evaluated leading client security suite vendors across 83 criteria and found that McAfee leads the market with its comprehensive functionality set and robust management capabilities. Symantec and Sophos are Strong Performers with feature-rich solutions for the threat mitigation market; however, both lack network access control and competitive administration features that can compete with McAfee. Finally, Panda Software and F-Secure offer strong threat protection and access control technologies but do not have a vision of — nor the resources to pursue — client security as anything more than a threat management solution. This is critical to client security solutions as they evolve beyond threat management to serve as an element of risk management and align more closely with business, not technology, threats.

TABLE OF CONTENTS

2 **The Advance Of Client Security Suites**

The Five Components Of Client Security Suites

The Additional Components Of Tomorrow's Client Security Suites

4 **Client Security Suite Evaluation Overview**

Evaluation Criteria: Offering, Strategy, And Market Presence

Evaluated Vendors: Virus Protection And More

6 **Client Security Suites Are Still Evolving**

Conducting Your Own Forrester Wave Analysis

9 **Vendor Profiles**

Leader

Strong Performers

Contenders

11 **Supplemental Material**

NOTES & RESOURCES

Forrester conducted survey-based evaluations in August 2006 and interviewed eight vendor companies: CA, F-Secure, Kaspersky Lab, McAfee, Panda Software, Sophos, Symantec, and Trend Micro.

Related Research Documents

["Getting The NAC Of It: 2006 Network Access Control Adoption"](#)

May 12, 2006, Trends

["Client Antivirus And Firewall Adoption In 2006"](#)

February 23, 2006, Trends

["Fear Factor: Information Assets And Viruses And Worms Top IT Security Threat List"](#)

February 23, 2006, Trends

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

June 22, 2005, Tech Choices

TARGET AUDIENCE

Security and risk professional, IT operations/engineering professional

THE ADVANCE OF CLIENT SECURITY SUITES

What is client security? Antivirus software? A personal firewall? The answer to this question has changed significantly over the past few years. Before the time of regulations, the only threat a PC posed was its ability to get infected with a virus or to possibly be used as a back door for a hacker. These virus infections had the ability to bring a corporate network to its knees.

Threats are evolving. We still worry about viruses, but spyware and Trojans are also concerns, and a more mobile workforce also means that corporate PCs are exposed to direct hacking. Client security suites have tried to keep pace; they have come a long way even in just the past year and a half. In mid-2005, McAfee released the most advanced suite in this market.¹ Its solution incorporated antivirus, antispymware, personal firewalls, and host intrusion prevention systems. However, this was not an integrated suite — management was still performed in silos, and client agents worked autonomously. Today, numerous other security vendors have come to the table with their own security suites. Unfortunately, client security suites lag behind the current threats posed by PCs.²

The Five Components Of Client Security Suites

Today's client security suites provide protection against malicious code, hackers, and unauthorized network access — in essence, they go after the threat of yesterday. These 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. The more advanced antivirus solutions have added behavior-based technologies to identify suspicious behavior that may be an indication of an infection. 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, defends against specific forms of malicious code. Unlike viruses, this code does not self-propagate; rather, it spies on the user to obtain passwords and other sensitive information like corporate data. Like antivirus, antispyware defense is primarily signature-based and sometimes behavior-based. As new spyware is found, additional signatures are created to identify this malware.
- **Personal firewall.** A personal firewall is client software that controls network connections to and from a user's PC, permitting or denying these connections based on a security policy. It is designed to prevent unauthorized access both to and from the machine. It 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 by using outbound port blocking.

- **Host intrusion prevention system (HIPS).** HIPS is a behavior-based technology that monitors network traffic in and out of the PC. When it suspects suspicious activity, it notifies administrators. More importantly, though, it can respond to suspicious activity by blocking traffic over a suspicious port or blocking a suspicious program from running.
- **Network access control (NAC).** NAC is a mix of hardware and software technologies that dynamically control client systems' access to networks based on their compliance with policy.

The Additional Components Of Tomorrow's Client Security Suites

Viruses as we know them are becoming less common. They have been replaced by much more targeted attacks that seek financial gain or competitive intelligence. Furthermore, the risk of noncompliance, both regulatory and corporate, is becoming too severe to ignore. The risk of not protecting confidential information opens a company up to mandatory disclosure laws, which in turn can sufficiently harm its reputation and thus sales. Consequently, client security needs to adapt to the changing threat of the client environment.

Security vendors are beginning to see this bigger picture. The best way to prevent malicious code is to make sure that systems are patched, and the best way to prevent unauthorized applications and devices is to make sure that systems are configured appropriately based on the risk profile of the user.³ Vendors know that protecting an organization's information is a top concern, and thus, making sure that information is protected on every machine — and encrypted if there is a breach — is a requirement. Consequently, Forrester believes that client security suites will evolve to include the following technologies:

- **Configuration management.** Configuration management tools combine vulnerability assessment, patch management, automated remediation, and configuration compliance capabilities. They give firms the ability to assess system configurations against known vulnerabilities and desired corporate compliance policies and take the appropriate actions.⁴
- **Encryption.** Client encryption can protect an entire hard drive or select files on the PC, and it can also be used to enable secure email. If the PCs or messages are compromised, then encryption ensures that the data is unreadable to unauthorized users. For this reason, encryption provides safe harbor from mandatory data breach disclosure laws.
- **Information leak prevention (ILP).** ILP software products identify confidential data: either structured database records and personal information or unstructured information like important fragments of a sensitive document or other file. They can monitor network activity across a range of ports and protocols or monitor user behavior at the desktop and then alert or take action against policy violations.⁵

CLIENT SECURITY SUITE 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: Offering, Strategy, And Market Presence

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 83 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, antimalware, personal firewall, host intrusion prevention system, network access control, administration and management, and interoperability features.
- **Strategy.** We considered how well each vendor's plans for product enhancement position it to meet future demands from companies and, furthermore, the financial resources the company has to support its strategy, both product and corporate. We looked at the company resources dedicated to corporate client security and how the vendor prices its product to compete in this market.
- **Market presence.** To establish a product's market presence, we combined information about each vendor's installed base, revenues (overall and product), services, employee numbers, and partnerships.

Evaluated Vendors: Virus Protection And More

Forrester included eight vendors in the assessment: CA, F-Secure, Kaspersky Lab, McAfee, Panda Software, Sophos, Symantec, and Trend Micro. Each of these vendors has:

- **Solutions that provide protection against viruses and worms.** Viruses and worms are consistently cited as the No. 1 threat to organizations.⁶ Consequently, Forrester chose to evaluate products that first and foremost protected — and when necessary, cleaned — machines from these threats.
- **Solutions that provide protection against the broader threat portfolio.** Viruses and worms are just one set of threats that organizations face. In addition, organizations must protect themselves against spyware, hackers, unknown malicious code, employees acting in unauthorized ways, and unauthorized access to the corporate network — to name a few. As a result, Forrester chose to evaluate products that protected machines against some subset of these threats.

Figure 1 Evaluation Criteria

CURRENT OFFERING	
Architecture	How well is the product built for delivering stability, performance, and scalability?
Antimalware	Does the product include antivirus and antispymware functionality?
Personal firewall	Does the product include personal firewall software?
Host intrusion prevention system	Does the product include intrusion detection and prevention features?
Network access control (NAC)	Does the product include network access control or integrate with other network access control frameworks?
Administration and management	How robust are the administration and management capabilities?
Interoperability features	Which other widely used systems and component formats does the platform interoperate with?
STRATEGY	
Product strategy	What is the overall product strategy and vision for client security suites?
Corporate strategy	What is the overall corporate commitment to the client security suite space?
Financial resources to support strategy	Is the vendor profitable, and what is its cash flow? Does the company have sufficient revenues, profits, and cash flow to support its security strategies?
Cost	What is the cost of this product?
MARKET PRESENCE	
Installed base	How large is the vendor's installed base of customers for this product and for all products?
Revenue from suite	What is the vendor's revenue from the client security suite product over the past four quarters?
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?
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?

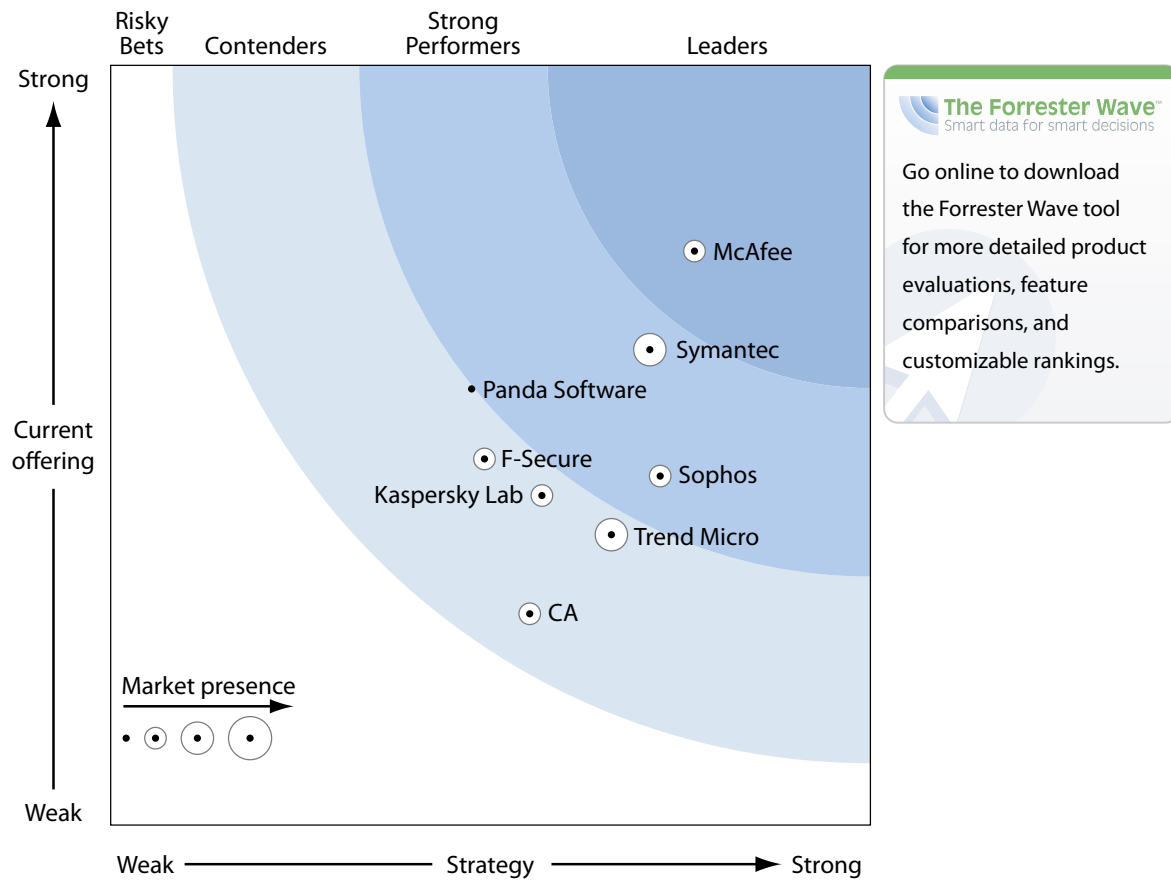
Source: Forrester Research, Inc.

CLIENT SECURITY SUITES ARE STILL EVOLVING

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

- **McAfee leads the pack.** Since Forrester's last evaluation, McAfee has integrated its personal firewall and HIPS technologies, bringing them into the ePolicy Orchestrator (ePO) management framework, and it finally added network access control. Total Protection for Enterprise Advanced offers the most integrated *and* feature-rich solution on the market today, all managed with its ePO management solution. And McAfee is not done yet. McAfee plans to add more configuration, compliance, remediation, and patch management technologies into its security suite, kick-starting a more proactive, broader risk management market.⁷
- **Symantec and Sophos offer competitive options.** Only a few steps away, these two solutions have a lot to offer. Symantec offers antimalware, personal firewall, and HIPS functionality through its use of generic exploit blocking signatures. Sophos offers a similar solution to Symantec, as its HIPS functionality comes through its behavior-based Genotype technology. Symantec provides strong management features, including role-based administration and robust reporting, whereas Sophos' solution is less flexible in this area. Both vendors' strategies include improvement to their HIPS solutions and will eventually offer more proactive — risk-management-orientated — security with technologies such as patch and configuration management.
- **Panda Software and F-Secure offer rich solutions but lack a concrete strategy.** These two solutions offer functionality that rivals the top players in the market, from their architecture and administration features to their threat protection technologies, which include antimalware, personal firewall, HIPS, and network access control. However, a vendor's current offering is not enough in this market. Panda Software and F-Secure offer competitive price points, given their functionality, but they lack a strategic vision of the future of the client security market that evolves toward the convergence of operational and security functionality.
- **Trend Micro, Kaspersky Lab, and CA lack advanced threat technologies.** Antimalware protection is just the entry point to a client security suite; thus, these three vendors have a ways to go. Trend Micro is the furthest along with its OfficeScan product. It provides antimalware, a basic personal firewall, and email security, and it also provides network access control when used within the Cisco Network Admission Control (NAC) framework or in conjunction with Trend Micro Network VirusWall. Kaspersky's only add-on to antimalware is its intrusion detection system, which provides behavior-based scanning and application and memory monitoring. CA does not offer any advanced threat defenses but will be adding personal firewall and HIPS functionality in 2007.

Figure 2 Forrester Wave™: Client Security Suites, Q3 '06



Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Client Security Suites, Q3 '06 (Cont.)

	Forrester's Weighting	CA	F-Secure	Kaspersky Lab	McAfee	Panda Software	Sophos	Symantec	Trend Micro
CURRENT OFFERING	50%	1.39	2.41	2.17	3.78	2.88	2.30	3.13	1.92
Architecture	15%	2.75	3.33	2.94	3.24	3.54	3.44	3.04	3.32
Antimalware	20%	3.40	3.00	4.20	3.80	4.20	3.80	3.80	3.40
Personal firewall	20%	0.00	1.70	0.30	3.80	2.35	1.80	3.15	0.60
Host intrusion detection system	15%	0.00	2.20	2.00	5.00	3.20	1.60	4.20	0.00
Network access control (NAC)	10%	0.50	2.20	0.00	2.85	1.55	0.25	0.50	2.35
Administration and management	15%	1.50	2.80	3.25	4.40	2.40	2.35	3.80	2.55
Interoperability features	5%	0.50	0.00	0.90	1.60	0.90	0.90	0.70	0.00
STRATEGY	50%	2.76	2.46	2.84	3.84	2.38	3.62	3.56	3.30
Product strategy	40%	2.40	2.40	2.60	3.60	2.20	3.80	4.40	3.00
Corporate strategy	30%	1.00	3.00	2.00	3.00	2.00	4.00	1.00	2.00
Financial resources to support strategy	30%	5.00	2.00	4.00	5.00	3.00	3.00	5.00	5.00
Cost	0%	3.25	3.50	4.50	1.50	3.00	2.75	3.50	2.50
MARKET PRESENCE	0%	2.83	2.50	2.58	2.80	0.88	2.98	3.73	3.18
Installed base	10%	1.00	3.00	4.00	1.00	0.00	3.50	0.00	4.50
Revenue from suite	30%	3.00	2.00	2.00	3.00	0.00	3.00	5.00	3.00
Revenue	25%	5.00	2.00	1.00	4.00	2.00	2.00	5.00	4.00
Revenue from growth	10%	1.00	4.00	5.00	2.00	0.00	2.00	1.00	2.00
Services	5%	2.50	3.00	3.50	2.50	1.50	3.50	2.50	4.00
Employees	10%	3.00	3.00	2.50	2.25	1.00	4.50	4.50	3.75
Technology partners	10%	0.50	2.50	4.00	2.50	2.00	4.00	3.00	0.50

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

Source: Forrester Research, Inc.

Conducting Your Own Forrester Wave Analysis

This evaluation of the client security suite market is intended to be a starting point only. To determine which platforms best fit your business needs, view the detailed evaluations by downloading the Excel spreadsheets behind Figure 2 in the online version of this report. Three steps will help you to customize Forrester's analysis:

- **Understand the evaluation criteria.** The "criteria" tab in the spreadsheet includes a description and grading scale for each criterion. Peruse these descriptions and mark the ones that are most important to you.

- **Change weightings as needed.** Forrester weighted the evaluation criteria based on what we feel is most important to meet our clients' needs as a whole. But every company is different. For example, larger companies may have a strong need to protect the network and network resources and hence may want to adjust the weightings in favor of vendors that provide network access control. Alternatively, a financial institution with multiple branch offices may not need multiplatform support and instead would prefer role-based administration and more robust reporting and logging features.
- **Determine your vendor shortlist with your customized Forrester Wave™.** The "Forrester Wave" tab will automatically update the Wave graphic and vendor ranking, placing the best fits for your needs in the Leader category. You may also decide to develop your request for proposal (RFP) based on our evaluation criteria, as these are the areas in which we identified vendor differentiation.⁸

VENDOR PROFILES

Leader

- **McAfee.** As the leading client security suite in our evaluation, McAfee's Total Protection for Enterprise Advanced is a comprehensive solution that gives customers the option of antivirus, antispyware, personal firewall, host intrusion prevention, email antivirus and antispam, and network access control functionality. Furthermore, Forrester expects McAfee to keep its lead in this market with its strategy of delivering a broader risk management solution, including technologies such as policy, threat, and risk management.⁹

Strong Performers

- **Symantec.** Symantec is getting ready to play ball against McAfee, but it isn't quite there yet. During the next 12 months, Symantec will add the functionality that it has acquired from its Sygate, WholeSecurity, and Platform Logic acquisitions to its Symantec Client Security suite. Symantec still has a compelling offering today, providing customers with antivirus, antispyware, personal firewall, and partial HIPS functionality. Full HIPS and NAC products are in the Symantec portfolio as standalone offerings for customers that require this functionality.¹⁰
- **Sophos.** Sophos is a dedicated security vendor that focuses on the endpoint and email security markets. As a smaller vendor, Sophos has made a lot of traction in the other security markets by OEMing its threat engine to vendors such as Blue Coat Systems, Microsoft, and Internet Security Systems (recently acquired by IBM). Sophos Endpoint Security offers Windows platform users antivirus, antispyware, and personal firewall functionality. In its next release, Sophos will be adding application control and behavioral intrusion prevention. The firm is beginning to see the larger risk management picture and will be adding patch management and asset inventory capabilities within the next 12 months.¹¹

Contenders

- **Trend Micro.** Trend Micro's OfficeScan suite offers antivirus and antispymware protection, a basic personal firewall, email security, and network access control using either the Cisco NAC framework or the Trend Micro Network VirusWall appliance. Through Trend Micro's partnership with Cisco Systems, OfficeScan customers can add HIPS functionality by purchasing the Cisco Security Agent, which will work seamlessly through the Trend Micro management console. However, the functionality that OfficeScan lacks from its personal firewall is top of mind for the OfficeScan team — more advanced firewall features and behavioral scanning will be added to the suite in Q1 2007. Further down the line, Trend Micro has plans to add support for the Mac platform, as well its own full-blown HIPS solution.¹²
- **Panda Software.** Panda Software created a security suite that is architecturally strong — thanks to its management server architecture, scalability, and modularity — and also functionally rich. ClientShield offers customers a comprehensive suite for the Windows platform, which includes antivirus, antispymware, personal firewall, antispam, content filtering, HIPS, and network access control. Strong in the small and medium-size business (SMB) market, Panda has placed a new emphasis on the enterprise market for 2006 and beyond. Its solid architecture and functionality will help it succeed.¹³
- **Kaspersky Lab.** Kaspersky Lab is a leading antimalware vendor. Its antivirus engine is integrated into many network appliances and email security solutions provided in the market today, including products from vendors such as Microsoft and Juniper Networks. Kaspersky Anti-Virus Business Optimal consists of antivirus, antispymware, and intrusion detection capabilities. It provides customers with protection from both known and unknown malicious code, as well as from hackers. In future releases, Kaspersky will be adding support for mobile devices and peripheral device control, but most importantly, it will be adding integration into the Cisco NAC and Microsoft Network Access Protection (NAP) frameworks.¹⁴
- **F-Secure.** F-Secure Anti-Virus Client Security offers customers a little bit of everything. Its solution includes antivirus, antispymware, a personal firewall with limited HIPS capabilities, and host-based network access control. Furthermore, as more than 40% of its entire employee base works in R&D for the client security products, F-Secure has committed to offering a full-scale HIPS product along with behavior-based antimalware and sandboxing functionality in its next release.¹⁵
- **CA.** CA Integrated Threat Management, released in January 2006, is CA's first foray into the enterprise client security suite market. This suite includes CA's eTrust Antivirus and eTrust PestPatrol Anti-Spyware Corporate Edition, both managed from the CA Integrated Threat Management console. While this suite works as separate products on the client, CA is working toward a unified antimalware solution that will bring together its dual-engine antivirus product

and its antispyware product. In addition, the vendor is planning to release a broader suite offering that will include personal firewall and HIPS functionality, which Forrester expects to appear in late 2007.¹⁶

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.

Data Sources Used In This Forrester Wave

Forrester used a combination of two 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.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with one of each vendor's current customers.

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

- ¹ 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. See the June 22, 2005, Tech Choices [“The Forrester Wave™: Client Security Suites, Q2 2005.”](#)
- ² The top five security concerns to an organization include viruses and worms, employees acting in unauthorized ways, poor protection of information assets, failure to comply with regulations, and spyware. See the February 23, 2006, Trends [“Fear Factor: Information Assets And Viruses And Worms Top IT Security Threat List.”](#)
- ³ Firms’ current approach to client security isn’t working — and they know it. Why? Because their users are increasingly mobile and can easily bypass the network perimeter, which exposes the core to malicious code and information theft. Consequently, organizations must lock down their devices and data. However, companies can’t operate efficiently with computing environments that resemble data prisons. Therefore, security managers need to shed the old processes that are based purely on protection from malicious code. By establishing risk profiles that focus on three aspects — users, data, and devices — firms can take the guessing out of securing their client systems. See the June 19, 2006, Best Practices [“Client Security: A Framework For Protection.”](#)
- ⁴ Effective security configuration management products help firms manage security proactively. By combining elements of vulnerability assessment, patch management, automated remediation, and configuration compliance, these products can help reduce risks by ensuring that systems are configured properly. See the October 26, 2005, Tech Choices [“The Forrester Wave™: Security Configuration Management, Q4 2005.”](#)
- ⁵ During the past few years, solutions have emerged that provide more sophisticated approaches to making sure that confidential data does not end up in the wrong hands. See the April 4, 2006, Best Practices [“Protecting Communication In The Emerging Information Workplace.”](#)
- ⁶ Survey results in both 2005 and 2006 show that viruses and worms are a top threat to organizations. See the March 25, 2005, Trends [“IT Security Threats In 2005: Viruses And Worms Top The List,”](#) and see the February 23, 2006, Trends [“Fear Factor: Information Assets And Viruses And Worms Top IT Security Threat List.”](#)
- ⁷ Forrester defines proactive endpoint risk management as policy-based hardware and software technologies that proactively manage risk by integrating endpoint security, access control, identity, and configuration management.
- ⁸ We published additional guidance on the Forrester Wave evaluation process and instructions on how to customize our vendor comparison tool. See the April 6, 2005, Trends [“The Forrester Wave™ 2005.”](#)
- ⁹ View the vendor summary for more detailed analysis on how McAfee fared in this evaluation. See the September 27, 2006, Tech Choices [“McAfee Leads In The Client Security Suite Market.”](#)

- ¹⁰ View the vendor summary for more detailed analysis on how Symantec fared in this evaluation. See the September 27, 2006, Tech Choices [“Symantec Is A Strong Performer In The Client Security Suite Market.”](#)
- ¹¹ View the vendor summary for more detailed analysis on how Sophos fared in this evaluation. See the September 27, 2006, Tech Choices [“Sophos Offers A Strong Client Security Suite Alternative.”](#)
- ¹² View the vendor summary for more detailed analysis on how Trend Micro fared in this evaluation. See the September 27, 2006, Tech Choices [“Trend Micro Offers Rich Mobility Support And Cisco Integration With Its Client Security Suite.”](#)
- ¹³ View the vendor summary for more detailed analysis on how Panda Software fared in this evaluation. See the September 27, 2006, Tech Choices [“Panda Software: A Solid Contender In The Client Security Suite Market.”](#)
- ¹⁴ View the vendor summary for more detailed analysis on how Kaspersky Lab fared in this evaluation. See the September 27, 2006, Tech Choices [“Kaspersky Delivers Flexible And Fine-Grained Management In Its Client Security Suite.”](#)
- ¹⁵ View the vendor summary for more detailed analysis on how F-Secure fared in this evaluation. See the September 27, 2006, Tech Choices [“F-Secure Is An Up-And-Comer In The Client Security Suite Market.”](#)
- ¹⁶ View the vendor summary for more detailed analysis on how CA fared in this evaluation. See the September 27, 2006, Tech Choices [“CA Is Playing Catch-Up With Its Client Security Suite.”](#)

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	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.*

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 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.