

TECH CHOICES



September 27, 2006

McAfee Leads In The Client Security Suite Market

The Forrester Wave™ Vendor Summary, Q3 2006

by **Natalie Lambert**

with Jonathan Penn and Sarah Bernhardt

EXECUTIVE SUMMARY

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 patch management.

TARGET AUDIENCE

IT operations/engineering professional, security and risk professional

MCAFFEE IS BEST SUITED FOR COMPANIES THAT REQUIRE COMPREHENSIVE PROTECTION

McAfee is the largest dedicated security vendor, with almost US\$1 billion in revenue and approximately 3,500 employees. McAfee's overall revenue grew 15% from 2004 to 2005, and it has more than \$1.25 billion in cash and cash equivalents to its name. Forrester estimates that approximately 60% of its revenue can be attributed to its client security products.

Forrester evaluated McAfee's current offering and strategy for client security suites against 83 criteria (see Figure 1). Overall, McAfee offers the richest suite in terms of security components and boasts strong administrative features. However, it lacks multiplatform support, thus keeping it off the shortlist of non-Windows-centric firms. This means that the product is an especially good fit for buyers that:

- **Are ready for, and can afford, a complete client security suite.** While the McAfee Total Protection solution offers a jam-packed functionality set for the Windows platform, customers on tight budgets may not be able to foot the bill. The product starts at more than \$80 per node for a 1,000-person organization — more than four times higher than its closest competitor, Symantec. However, there is no doubt that companies with the budget will save time and money in administration and management, as well as malicious code outbreak costs.
- **Want a vendor that will protect them now and into the future.** McAfee is a dedicated security vendor that has always remained a step ahead of its competitors on functionality.¹ Having just released its Total Protection suites in April 2006, McAfee is already talking about the next

generation of products that will move beyond threat management and onto risk mitigation. This will allow companies to further consolidate vendors, as McAfee will bring together traditional threat technologies with more policy compliance and risk management technologies.

To see how McAfee stacks up against seven other competitors, see the Forrester Wave™ evaluation of the client security suites market.²

Figure 1 McAfee Total Protection For Enterprise Advanced Evaluation Overview

CURRENT OFFERING

Architecture	McAfee Total Protection for Enterprise Advanced offers Windows platform customers the most comprehensive client protection of all the suites Forrester looked at. It includes antivirus, antispyware, host intrusion prevention (with personal firewall functionality), and network access control. It also includes email security functionality that was not included in this evaluation. The management of Total Protection and other McAfee products is done through McAfee's ePolicy Orchestrator (ePO) — this management solution is the policy store and update repository for the McAfee solution. It is a hierarchical solution that scales to 250,000 nodes. The product's deployment options are very flexible, and architecture updates easily support both on-site and remote systems. McAfee's only drawback is that the client requires multiple agents if the entire solution is deployed.
Antimalware	McAfee's antimalware solution is both signature- and behavior-based, allowing it to detect known and unknown viruses, as well as buffer overflow exploits. The product supports multiple actions when malicious code is detected, including deletion, moving the file, or denying access to the file. McAfee, in its AVERT Labs, has a team of researchers who work with all forms of malware. This team releases updated signature files daily — sooner when there is an outbreak.
Personal firewall	While McAfee does not specifically have a personal firewall, this functionality is built into its HIPS product. It can control both inbound and outbound traffic based on factors such as port and applications accessing the network. The product offers customers a learning mode that allows the product to monitor all client activity and then easily allow administrators to create policies from the logged information. The product can also monitor applications, preventing both hooks into other applications and access to the Internet on a policy basis. In addition, the product supports application and Web site blacklisting and can monitor and block the use of media devices.
Host intrusion prevention system (HIPS)	McAfee Host Intrusion Prevention combines signature, behavioral, and firewall protection to deliver a solid HIPS solution. This product protects against zero-day attacks and buffer overflows and is able to monitor memory with kernel-level filter drivers. The product also has the capabilities to define rules for applications, therefore allowing only predefined behaviors. Lastly, the product includes a learning mode, allowing administrators to observe what is happening in their environment and then define acceptable use policies.
Network access control (NAC)	McAfee Policy Enforcer is McAfee's proprietary network access control solution. It offers both host- and infrastructure-based access control — infrastructure control meaning that SNMP commands are sent to a switch (or other infrastructure) to reconfigure ports. Administrators can create policies based on multiple vendors, and these policies can be enforced on both managed and unmanaged Windows systems. The product is able to remediate systems using a portal that users go to for self-remediation.
Administration and management	McAfee ePO offers client-server administration for both management and reporting. The product supports role-based administration, allowing four levels of administrator accounts to be created. Administrators can also delegate control of the product to end users, giving them control over their scans and updates. In addition, safeguards are in place to protect the product from disablement. Reporting is comprehensive with both custom reporting and drill functionality available. In addition, the product ships with 40 prebuilt reports, including top 10 infected machines, top 10 malware detections, and top 10 unwanted programs.

Source: Forrester Research, Inc.

Figure 1 McAfee Total Protection For Enterprise Advanced Evaluation Overview (Cont.)

CURRENT OFFERING

Administration Interoperability features	McAfee's ePolicy Orchestrator supports enterprise directories through Active Directory. In addition, McAfee integrates with IBM Tivoli and ArcSight and can integrate with all help desk systems via SNMP.
--	--

STRATEGY

Product strategy	McAfee currently has the most comprehensive client security tool set, including a suite solution with antivirus, antispymware, personal firewall, host IPS, email security, and network access control. While McAfee does not have many technology partnerships, it is still known as a best-of-breed security vendor. The vendor has a number of road map items for its Total Protection Solution, notably Cisco NAC integration and broader support for non-Windows operating systems. However, McAfee's long-term risk management strategy is impressive and will keep it as the top-of-mind security player for the foreseeable future.
Corporate strategy	McAfee is a dedicated security vendor that targets all customer segments. It offers a vast array of host and network security products. On the client, McAfee offers a suite solution with antivirus, antispymware, personal firewall, host IPS, and network access control — this solution positions the vendor as a leader in the client security suite market.
Financial resources to support strategy	<ul style="list-style-type: none"> • McAfee is profitable. • Based on 2005 financial statements, McAfee has \$1.26 billion in cash (cash and cash-equivalent investments). • McAfee's revenues in 2005 outgrow the pace of the market by 14%, reaching approximately \$1 billion and deferred revenues of \$746 million, which represents an all-time high for the company. • McAfee was debt-free as of December 31, 2005.
Cost	McAfee sets the pricing based on the number of nodes, with discounts based on volume pricing. For 1,000 nodes, McAfee Total Protection for Enterprise Advanced sells for \$82.63 per node, including ePolicy Orchestrator and the first year of support.

Source: Forrester Research, Inc.

Figure 1 McAfee Total Protection For Enterprise Advanced Evaluation Overview (Cont.)

MARKET PRESENCE

Installed base	McAfee has not disclosed details of its installed base. However, since the product’s release in April 2006, Forrester estimates that McAfee has fewer than 5,000 customers using McAfee Total Protection for Enterprise Advanced.
Revenue from suite	Forrester estimates that McAfee Total Protection accounts for less than \$10 million in revenue. However, the product has only been available since April 2006 (score reflects year approximation).
Revenue	<ul style="list-style-type: none"> • \$987.3 million for 2005. • \$272 million for Q1 2006. • \$253.3 million for Q4 2005. • \$253 million for Q3 2005. • \$245 million for Q2 2005.
Revenue growth	<ul style="list-style-type: none"> • McAfee’s yearly revenues grew by 15% in FY06. • McAfee’s quarterly revenues grew by 16% year-over-year in Q1 2006. • McAfee’s quarterly revenues grew by 4.4% year-over-year in Q4 2005. • McAfee’s quarterly revenues grew by 20% year-over-year in Q3 2005. • McAfee’s quarterly revenues grew by 32% year-over-year in Q2 2005.
Services	McAfee offers on-site and classroom training sessions for its customers.
Employees	McAfee has approximately 3,500 employees — Forrester estimates that roughly 10% of them are in sales.
Technology partners	McAfee’s technology partners include the 12,500 firms that resell its product. McAfee has no license partners.

Source: Forrester Research, Inc.



Go online to download additional in-depth data and scores for this vendor and other vendors included in this Forrester Wave evaluation.



SUPPLEMENTAL MATERIAL

Online Resource

The underlying spreadsheet for Figure 1 is available online. The spreadsheet includes more detailed data and scores for this vendor.

This detailed data and scores for this vendor are also available online through 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

- ¹ To assess the state of the client security suite market in 2005 and the enterprise antispyware market in 2006, Forrester evaluated the strengths and weaknesses of top client security suites and enterprise antispyware vendors across multiple criteria. The result: McAfee leads the pack, with Symantec nipping at its heels. See the June 22, 2005, Tech Choices "[The Forrester Wave™: Client Security Suites, Q2 2005](#)," and see the January 6, 2006, Tech Choices "[The Forrester Wave™: Enterprise Antispyware, Q1 2006](#)."
- ² 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. See the September 27, 2006, Tech Choices “The Forrester Wave™: Client Security Suites, Q3 2006.”