Symantec Endpoint Protection 12.1 vs. McAfee Total Protection for Endpoints

Competitive Advantage Card

Date Created	February, 2009
Last Updated	March, 2011
Audience	Symantec Partner and Customers

Overview of McAfee's Endpoint Products

McAfee offers several suite configurations for the endpoint bundled under the "Active" and "Total Protection" brand. They market the solutions as offering comprehensive system protection, scalable network access control, with anti-spyware, anti-virus, anti-spam, firewall, and host intrusion prevention. McAfee attributes recent growth to upgrading customers to the ToPS suite from AV, cross selling and up selling their security products, and through acquisitions.

Quick Comparison

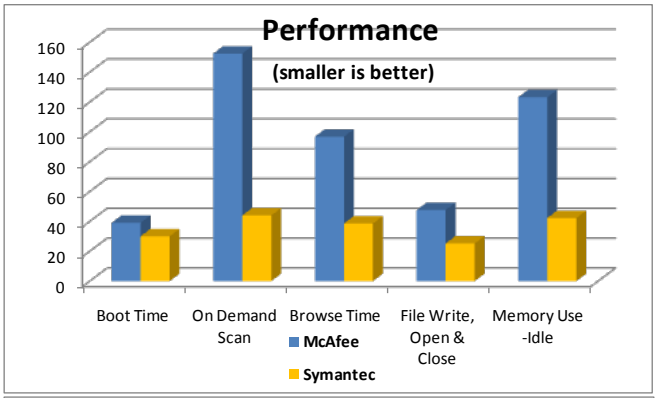
Symantec Endpoint Protection consistently outperforms McAfee in independent testing, and version 12.1 includes a new state-of-the art protection system, Symantec Insight™, which allows Endpoint Protection to offer fast, powerful security for endpoints. Symantec Endpoint Protection also has a set of features that makes it ideal for securing virtual environments. It offers advanced defense against all types of attacks for both physical and virtual systems.[i]

Functionality[ii]

	Management		Protection Technologies					Zero Day		
	Consoles	Agents	AV/ AS	FW	IPS	App C	DC	File Reputation	RTB	AC
Symantec	**1**	**1**	●	●	●	●	●	●	●	●
McAfee	**1**	**4**	●	●	●	●	●	○	○	●

Performance[iii]

In comprehensive testing by PassMark Software, Symantec was the best performing product in its class. In head to head performance tests, Symantec Endpoint Protection blew past McAfee– scanning 3.5 times faster and using 66% less memory.

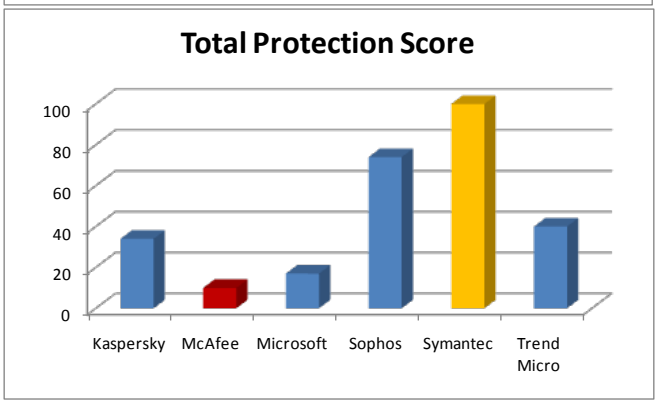


Detection[iv]

McAfee's solution essentially failed real-world detection tests from the industry's leading detecting test organization, AV-Test.org. In a test of 6 enterprise class endpoint protection products, McAfee came in last,

scoring 10 out of a possible 104 points. Symantec Endpoint Protection 12.1 scored highest with a total detection score of 100.

Symantec also continues to hold a leadership position compared to competitors in the Gartner Magic Quadrant for Endpoint Protection Platforms 2010.[v]



Symantec Endpoint Protection 12.1 vs. McAfee Total Protection for Endpoints

Competitive Advantage Card

Key Symantec Endpoint Protection 12.1 Differentiators

Symantec Key Differentiators/Advantages	Business Benefit	McAfee Claims & Symantec Response
Symantec Insight	Insight is an innovative approach to security that analyzes files in context, using the age, frequency and source along with other security metrics to expose threats others miss	**McAfee claim:** McAfee offers reputation based security with Global Threat Intelligence technology (Artemis). **Symantec response:** • McAfee's Global Threat Intelligence does not track all executable files, rate security based on how many people are using the file, or how long it has been on the internet • McAfee's approach of looking for virus signatures is reactive • McAfee's technology looks for signatures for known malware in the cloud For additional information about Artemis, see McAfee's KB articles
Superior detection	Protects against viruses, worms, Trojans, spyware, bots, zero-day threats and rootkits	**McAfee claim:** McAfee claims to be number one in malware detection **Symantec response:** • The tests referenced by McAfee, from av-test.org, are two years old and are no longer available. • More recent tests by av-test.org consistently show McAfee providing poor detection**. McAfee has failed virus detection certification for Windows XP, Vista and Windows 7** • Symantec consistently leads in malware detection and removal in tests by av-test.org, av-comparatives.org and Dennis Labs
Single agent for multiple technologies	Consolidates antivirus, antispyware, desktop firewall, intrusion prevention, device and application control and network access control into a single agent	**McAfee claim:** McAfee claims SYMC security solutions require multiple agents and SEP is difficult to deploy. **Symantec response:** • Endpoint Protection requires a single agent to manage: o Antivirus o Antispyware o IPS o Device Control o Application Control o Firewall o Network access control • Our single agent means one task for upgrading the above functionality. With multiple agents, such as McAfee uses, each point solution must be updated separately • We have a full installer and also provide multiple ways to upgrade/migrate that involve a package of 30MB or less
Secure virtual environments	Provides protection for both physical and virtual environments	**McAfee claim:** McAfee claims Symantec has a limited virtualization offering **Symantec response:** Symantec Protects a wide range of virtual environments, offering: • Optimized protection that is Hypervisor agnostic • Virtual client tagging • Virtual image exception • Shared insight cache • Resource leveling

Symantec Key Differentiators/Advantages	Business Benefit	McAfee Claims & Symantec Response
		• Offline VM scan tool
Broad coverage across endpoint, network and storage systems	Consolidates antivirus, antispyware, desktop firewall, intrusion prevention, device and application control and network access control	**McAfee claim:** McAfee claims Symantec's HIPS and endpoint security is weak **Symantec response:** • Gartner recognizes that Symantec continues to perform well in numerous malware tests in the latest Gartner Magic Quadrant for Endpoint Protection Platforms
Symantec offers the best desktop firewall in the industry	Consolidates antivirus, antispyware, desktop firewall, intrusion prevention, device and application control and network access control	**McAfee claim:** McAfee claims to offer a strong personal firewall. **Symantec response:** Gartner says Symantec has, "the best firewall of any ranked vendor"[vi]

Business Value of Symantec Endpoint Protection 12.1

Symantec Endpoint Protection 12.1 combines Symantec AntiVirus with advanced threat prevention to deliver an unmatched defense against malware for laptops, desktops, and servers in both physical and virtual environments. It provides protection against even the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and mutating spyware. And it reduces costs associated with managing multiple endpoint security solutions and complexity of endpoint security environments. Symantec Endpoint Protection 12 is the fastest, lightest security solution in its class.

Key Questions to Ask

- How important is virus detection in an antivirus product? In independent tests, McAfee's solutions consistently lag behind the competition in detecting and in removing viruses, trojans and worms.
- Are you prepared for a world with hundreds of millions of viruses? Symantec uses the reputation of files to separate files at risk from those that are safe. Symantec Insight identifies rapidly mutating threats and is designed to handle the explosion of new malware.
- Are you interested in a solution that examines programs as they run, stopping malicious behavior even for previously unknown threats? Symantec's real-time SONAR 3 examines programs as they run, identifying and stopping malicious behavior even for new and previously unknown threats.
- How are you planning to protect your systems from browser intrusions? Symantec Endpoint Protection 12.1 scans for attacks directed at browser vulnerabilities.
- Do you need a solution built for virtual environments? Symantec Endpoint Protection 12.1 protects your virtual infrastructure, whether you are using VMware, Citrix or Microsoft.

How to get more information

Check out the following reports for more info on how SYMC compares with McAfee

- PassMark Symantec Endpoint Protection Enterprise Edition Performance Test - SEP outperforms McAfee in several performance tests
- Look at the latest antivirus certifications
- See how your antivirus solution stacks up in detecting real-world threats:
- Berry Plastics Customer Case study - replaced McAfee with Symantec and experienced a threefold performance improvement.

[i] *"Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change. Any future release of the product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making purchasing decisions."*

[ii] Table Legend

AV/AS Antivirus and Antispyware	FW Firewall
App C Application Control A vulnerability facing network inspection technology as defined by Gartner in G00127317 page 2, May 2005	IPS Deep Packet Inspection IPS - attack-facing network inspection technology as defined by Gartner in G00127317 page 2, May 2005
DC Device Control - behavioral application hardening technology as defined by Gartner in G00127317, page 3, May 2005	File Reputation – the ability to provide the age, prevalence and security rating of executable files.
RTB Real-time behavioral analysis – monitor applications as they execute for indications of malicious activity.	AC Access Control – the ability to limit network access based on the client's conformation to security standards

[iii] Enterprise Endpoint Protection Performance 2011, PassMark Software, February 2011
[iv] 2. AV-Test.org, "Real World Testing", February 2011
[v] Gartner Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, John Girard, Neil MacDonald, Dec 17, 2010
[vi] ibid