McAfee Total Protection for Enterprise vs. Symantec Endpoint Protection

We put two endpoint security products through their paces

By Barry Nance

Total Protection for Enterprise protected against more threats, was more accurate, used less memory, and was easier to use than the less mature Endpoint Protection. Total Protection for Enterprise turns aside virtually all malware, is highly scalable, and uses fewer resources. Total Protection for Enterprise wins the Network Testing Labs World Class Award for providing the best desktop and server endpoint security.

Report Card

Grade scale is A through F, with F = Failing and A = Perfect

Category and weight (%)	McAfee Total Protection for Enterprise	Symantec Endpoint Protection
Identifying and thwarting malware (40%)	A	C
Performance (20%)	B	C
Ease of use (10%)	A	C
Reports (10%)	A	B
Deployment (10%)	A	A
Documentation (10%)	A	B
Overall score	A	C

Protecting thousands of enterprise endpoint systems from the threats targeted at them today is a daunting challenge. Not only are the number and complexity of threats increasing, but the days of huge budget and personnel increases to counter these threats are long gone. Security professionals are looking for a way to "do more with less" without compromising the quality of the protection they provide. We evaluated the "next generation" offerings from the two leaders in endpoint security to see which one does a better job.

The most important criterion in our evaluation is the ability to identify and thwart virtually all malware. We also looked at the breadth of threats covered, the relative resource consumption of the two products, the ability to protect against unknown or "zero-day" attacks, ease of management, scalability, ease of deployment, and agent efficiency.

At Network Testing Labs, we've created a special test environment (see the Testbed and Methodology section of this review) for evaluating anti-malware products. We used this test environment to evaluate the most recent versions of McAfee's Total Protection for Enterprise and Symantec's Endpoint Protection products.

Protect Your Data

We subjected both Total Protection for Enterprise and Endpoint Protection to the same battery of 200 malware instances. Total Protection for Enterprise succeeded in blocking 99 percent of the miscreants, while Endpoint Protection caught only 92 percent (see Table 1). With the potential cost of a single compromise running into the thousands of dollars, these results represent a significant difference in the overall effectiveness of the products.

We also noted that McAfee updates the malware definitions for Total Protection for Enterprise more often than Symantec updates Endpoint Protection's definitions.

Product	Success rate against a suite of 200 malware instances
Total Protection for Enterprise	99%
Endpoint Protection	92%

Table 1. Ability to block malware.

McAfee's Host Intrusion Prevention technology examines the behavior of application programs for malicious activity in addition to using known malware signatures to detect attacks. Behavioral technology is the key to protecting against not-yet-quantified (so-called "zero-day") attacks. In our tests, Symantec's zero-day protection, termed Proactive Threat Scan, was far less effective than McAfee's at stopping brand-new, just-distributed malware.

Malware detection is useless if a security product consumes excessive CPU, memory, or network resources. On either a client or a server, you want a security product to operate as far in the background and as quickly and unobtrusively as possible.

Product	Memory usage while examining traffic	Memory usage during system scan	CPU Usage
Total Protection for Enterprise	112 Mb	59 Mb	7%
Endpoint Protection	153 Mb	86 Mb	28%

Table 2. Agent memory footprints and CPU utilizations.

Our tests show that Total Protection for Enterprise has a memory footprint 41 Mb smaller than Endpoint Protection's for the modules that inspect incoming network traffic (Table 2). During scanning operations (which typically occur once a day), Total Protection for Enterprise's memory footprint was 27 Mb smaller than Endpoint Protection's. Furthermore, Total Protection for Enterprise's CPU usage was only 6 percent to 7 percent, even during times of high network access. Under the same test conditions, Endpoint Protection's

CPU usage ranged from 10 percent to 28 percent. Finally, our tests revealed that Total Protection for Enterprise (while receiving central console commands and updating the malware definition files) was much more frugal in its utilization of the network.

Product	On-demand scan elapsed times	On-access scan elapsed times
Total Protection for Enterprise	6 minutes 47 seconds	9 seconds
Endpoint Protection	9 minutes 12 seconds	1 minute 28 seconds

Table 3. Scan and clean times for infected files.

Total Protection for Enterprise scanned and cleaned desktop computers much more quickly than Endpoint Protection (Table 3). A quicker scan time translates directly into greater productivity because it means an administrator needs to spend less time putting a computer back to work. Both the administrator and the target computer benefit.

Total Protection for Enterprise examines HTTP, FTP, SMTP, and POP3 Internet traffic, looking for spyware and viruses. To keep users from inadvertently accessing malware-related web sites, it also detects malware URLs and IP addresses. For SMTP and POP3 traffic, the device identifies and blocks viruses, spam, and phishing attempts. Total Protection for Enterprise's file analysis even protects against malware encountered from "friendly" URLs, such as web mail downloads.

McAfee's architecture is much more sophisticated than Symantec's. The Endpoint Protection product is basically an anti-virus tool with other features (anti-spyware, firewall, and network access control) grafted on. In contrast, the Total Protection for Enterprise architecture is designed from the ground up to manage all aspects of client and server security. For instance, the Total Protection for Enterprise software modules load dynamically into memory more smoothly and with finer granularity than those of Endpoint Protection.

The management architecture of Total Protection for Enterprise provides actionable dashboards that allow administrators to quickly take action on security events or systems that may be out of compliance, providing increased visibility to the security state of endpoints enterprise-wide.

Ease of Use and Manageability

McAfee's central console for administering Total Protection for Enterprise is ePolicy Orchestrator® (ePO™). This central console greatly increases the scalability of McAfee's security defenses because of its span of control and the ability to manage up to 300,000 nodes under a single ePO server. The advertised scalability under a single management server for the Symantec Endpoint protection console is around 40,000 nodes.

ePO 4.0 provides a number of new features that don't exist with Symantec's Endpoint Protection console, including a web-based console which is accessible from any web browser, multi-level admin roles, and highly customizable dashboards.

Figure 1. The ePO dashboard provides, at a glance, the health of your security infrastructure.

Dashboards allow users to get a quick view of the state of their enterprise security not only from the endpoints using Total Protection for Enterprise but also from other McAfee and third-party products, including McAfee Network Access Control, Network IPS, messaging security appliances, and vulnerability management components.

Unique to ePO is the ability for the security administrator to take action directly from the reports produced by the system. For example when a report identifies systems with out-of-date signature files, the administrator can initiate an update directly from the report screen. As icing on the cake, ePO's report designer is a joy to use.

Automatically Identifying the Bad Guys—The Digital Detective

McAfee has automated its approach to knowing which web sites, for instance, contain malware or harvest email addresses for use in spamming or in phishing. This approach is a central feature of McAfee's SiteAdvisor component. SiteAdvisor always stays up to date on the latest threats. It continually crawls the Internet, using intelligent spiders. These spiders visit nearly every web site, download content from that site, and scan the results for various kinds of malware. The spiders even fill out registration forms to determine whether signing up for a site triggers spam.

If the site contains malicious code or other suspicious content, SiteAdvisor's spiders note the nature of the threat so SiteAdvisor can help you avoid that site.

SiteAdvisor knows which web sites produce excessive pop-ups, engage in fraudulent practices, contain browser exploits, and will target your email address with spam. In addition to its programmatic evaluation of the Internet, SiteAdvisor uses feedback from customers to characterize web sites.

The result of McAfee's constant examination of the Internet is the basis for the vendor's frequent and accurate updates to customers' malware definition files.

ePO gives enterprises a single, central point for enforcing security policies and controlling, managing, and reporting on malware and other threats. ePO's tab-folder metaphor is instantly and clearly intuitive, and ePO includes over 60 predefined reports.

The Symantec Endpoint Protection central console, like ePO, integrates tightly with Active Directory. However, the Endpoint Protection UI lacks the maturity of Total Protection for Enterprise, and it's considerably less intuitive to use.

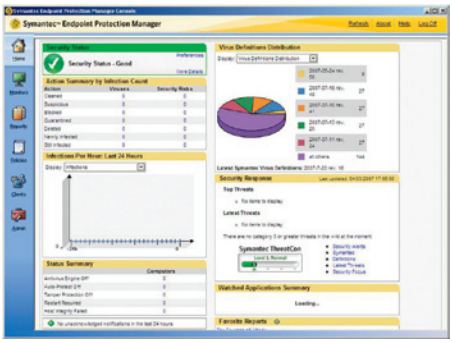

Figure 2. White Symantec's management console looks similar to ePO, it lacks the flexibility to be customized.

Conclusion

The combination of McAfee's Total Protection for Enterprise plus ePolicy Orchestrator is accurate, resource-frugal, scalable, robust, reliable, and intuitive to use. Total Protection is a highly effective roadblock against malware of all types. We strongly recommend you take a closer look at Total Protection for Enterprise and ePO.

About the Author

Barry Nance is a networking expert, magazine columnist, book author, and application architect. He has more than 29 years experience with IT technologies, methodologies, and products. Over the past dozen years, working on behalf of Network Testing Labs, he has evaluated thousands of hardware and software products for *ComputerWorld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World*, and many other publications. He's authored thousands of magazine articles as well as popular books such as *Introduction to Networking* (4th Edition), *Network Programming in C, and Client/Server LAN Programming*.

He's also designed successful web-based e-commerce applications, created database and network benchmark tools, written a variety of network diagnostic software utilities, and developed a number of special-purpose networking protocols.

You can email him at *barryn@erols.com*.

Test bed and Methodology

We primarily looked for the ability to identify and block malware (such as viruses, spam, phishing attempts, keystroke loggers, browser hijackers, adware, rootkits, dialers, data miners, and Trojans). We wanted a product to prevent malware from sending data from our network (i.e., "phoning home"), identify already-infected clients, scan traffic quickly, receive frequent spyware definition updates, and produce helpful reports on infection attempts and traffic statistics.

We collected a suite of 200 malware samples, and we moved the collected material to an isolated, quarantined network. We thus were able to simulate the Internet within our lab.

The quarantined network consisted of three subnets.

- Subnet 1 had 25 client machines with a variety of operating systems, including Windows NT, 98, 2000, 2003, ME, XP, Vista, Red Hat Linux, and Macintosh OS X.
- Subnet 2 contained three web servers (Microsoft IIS, Netscape Enterprise Server and Apache), three email servers (Exchange, Notes and Sendmail), two file servers (Windows 2003 Advanced Server and Netware), and two database servers (Oracle 8i and Microsoft SQL Server).
- Subnet 3, simulating the "Internet," had web servers containing the malware instances and which sported "bad guy" IP addresses and URLs. Systems on the first two subnets accessed the third subnet as if it were the real Internet.

To measure performance, we examined both the network traffic each product caused and the computing resources (CPU, memory, disk) each product consumed.

Client and server machines started off in a pristine state for each test. Our clients and servers attempted to download malware from the simulated "Internet." We noted how well the products identified malware traffic and blocked attempts by the malware to send data back to the source. We gauged success or failure by examining each machine for malware after each test. We looked for running malware processes, new program files (EXE, DLL, or OCX, possibly marked with the "Hidden" attribute) and directories as well as Registry and Start Menu changes.

About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

Network Testing Labs' experts have written hardware and software product reviews, state-of-the-art analyses, feature articles, in-depth technology workshops, cover stories, buyer's guides and in-depth technology outlooks. Our experts have spoken on a number of topics at Interop, Comdex, PC Expo, and other venues. In addition, they've created industry-standard network benchmark software, database benchmark software, and network diagnostic utilities.