NETWORK TESTING LABS REVIEW:

ACHIEVING INTERNET SECURITY AT THE CLIENT

MCAFEE'S TOTAL PROTECTION FOR ENTERPRISE VS. MICROSOFT'S FOREFRONT CLIENT SECURITY

By Barry Nance

August, 2007

Effective security at the desktop or server depends on having an accurate, resource-frugal, scalable, easy-to-administer and highly integrated defense against malware threats such as spyware, phishing attempts, viruses, trojans, rootkits and other threats. In this test , we compare two products intended for the enterprise, the market-leading McAfee Total Protection for Enterprise and a relative newcomer, Microsoft Forefront Client Security.

After extensive research and testing of the two products, we concluded that McAfee Total Protection for Enterprise wins Network Testing Labs' World Class Award for best desktop and server endpoint security.

Malware is spreading explosively across the Internet. You can no longer afford to accept the risks that the threat of malware holds over your head. More specifically, you can no longer afford to use less than the absolute best anti-malware tool to keep malware at bay.

At this very moment, criminal organizations are probing your network. They're trying to disrupt your organization and steal anything of value stored on your computers – passwords, proprietary business information, customer data, trade secrets and financial data. Several shadowy companies exist for the sole purposes of stealing your data or forcing your users to view unsolicited and unwanted advertisements. Individual programmers, many with disturbing psychological problems, also want to pry into the data on your servers and clients.

Spyware, phishing attempts, viruses, trojans, rootkits and malicious Web sites (collectively, "malware") are no longer a problem you can ignore. You may think you're

safe because your users visit only “good” Web sites. but with the increased sophistication of threats and attacks no one is safe.

Spyware authors have adopted a new approach, we’ve noticed, to get their software onto your computers. The bad guys hijack one or more Web pages of an otherwise “clean,” innocuous Web site. Unaware that someone’s hacked it, one of your users visits the site. Your user expects news, weather or sports information. Instead, the user gets an unexpected warning message. With one wrong click on the warning message, he or she downloads spyware onto a corporate PC.

For example, miscreants recently hacked the weather-reporting site Intellicast.com to replace the usual precipitation radar image Web pages with warning messages telling you that you immediately need to run something called “Drive Cleaner.” Even clicking on the warning message’s “cancel” button downloads the spyware. Fortunately, Intellicast quickly repaired its Web site. Similarly, the Israeli newspaper site Haaretz.com was briefly infected with “Drive Cleaner.” Visitors to the site got spyware instead of news of the Middle East.

Network Testing Labs has 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 put McAfee’s Total Protection for Enterprise and Microsoft’s Forefront Client Security products through their paces. 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 ability to protect against unknown or “zero day” attacks, ease of management, scalability, ease of deployment and agent efficiency.

Total Protection for Enterprise protected against more threats, was more accurate, less resource-intensive and easier to use. It turned aside virtually all spyware, and it is highly scalable. Total Protection for Enterprise wins the Network Testing Labs World Class Award for best desktop and server Internet security package.

Stop Malware Cold

Total Protection for Enterprise thwarted an impressive 98% of the malware we threw at it. In contrast, Forefront Client Security only caught 89% of the same suite of malware instances. We also noted that McAfee updates the malware definitions for Total Protection for Enterprise more often than Microsoft updates Forefront Client Security’s definitions.

	Success rate against a suite of 200 malware instances
Total Protection for Enterprise	98%
Forefront Client Security	89%

Table 1. Ability to block malware.

Especially on a server but also on a client, you want a security product to operate as far in the background and as unobtrusively as possible. Our tests show that Total Protection for Enterprise uses one third the CPU, memory and disk resources as Forefront Client Security does.

Forefront Client Security defaults to Quick Scan mode, which means that its daily examination of the client computer's processes, files and registry contents isn't as comprehensive and thorough as that of Total Protection for Enterprise. Nonetheless, Forefront Client Security's consumption of computer resources means you'll want to schedule its daily scans for off-hours, when users aren't accessing the computers.

Automatically Identifying the Bad Guys

McAfee has automated its approach to knowing which Web sites contain malware and which sites harvest e-mail 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*, or virtual computers. 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 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 e-mail address with spam. In addition to its programmatic evaluation of the Internet, SiteAdvisor uses feedback from customers to characterize Web sites.

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 webmail downloads.

Unlike Forefront Client Security, Total Protection for Enterprise is comprised of anti-virus, anti-spyware, host intrusion blocking and e-mail server security modules. McAfee's architecture is much more sophisticated than Microsoft's.

Of particular significance is the inclusion of Host Intrusion Prevention. This technology examines the behavior of application programs for malicious activity rather than relying solely on signatures to detect attacks. This capability is the key to protecting against unknown of "zero day" attacks without the need for signature updates and takes protection to a whole new level that Forefront is not addressing.

While Forefront Client Security is completely Windows-centric, Total Protection for Enterprise also supports Linux and Mac platforms. Remember – non-Windows operating systems are vulnerable to trojans and worms, and any browser on any machine might access a malicious Web site.

Ease of Use

McAfee's central console for administering Total Protection for Enterprise is McAfee ePolicy Orchestrator (ePO). This central console greatly increases the scalability of McAfee's security defenses because of its span of control. Forefront Client Security in contrast requires numerous different management components to function. ePO costs less to administer and use. ePO gives enterprises a single, central key for enforcing security policies and controlling, managing and reporting on malware and other threats, whether Web-based or e-mail-based. ePO's tab-folder metaphor is instantly and clearly intuitive, and ePO includes over 60 predefined reports.

The Forefront Client Security central console, just like ePO, integrates tightly with Active Directory. Based on the Microsoft Management Console (MMC) paradigm, Forefront Client Security is considerably less intuitive to use than ePO. Moreover, ePO's report designer is a joy to use.

Conclusion

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

What's Bad About Malware

Malware is, collectively, damaging or annoying software and data files that you didn't knowingly install on your computers. Typically, malware deletes files, changes files, reveals file contents, throws pop-up advertisements onto your screen, slows down a computer, allows a remote attacker to control your computer, attempts to convince you to supply credit card and password data, tracks your keystrokes, threatens to blackmail you, sends e-mail to everyone in your address book and otherwise ruins your day (or perhaps your life). Malware typically also propagates itself and can install additional malware instances on your computers.

Malware leverages the Windows operating environment, both server and client, in clever ways. Because virtually all users' logons are Administrator-privilege accounts, all the software that users run, even inadvertently, can fully control any aspect of the PC that the software (or malware) developer wishes.

With free rein over a PC's files and programs, including Windows operating system files, a malware instance can configure a computer to run the malware perpetually and thwart attempts to remove the malware (i.e., a ***rootkit***). The malware thus becomes part of Windows itself.

Malware can cost your company the time, effort and expense of extricating its residue from infected computers. A study by The Radicati Group, entitled "Corporate Anti-Spyware Market, 2005-2009," says the number of anti-spyware tool licenses will increase from 16 million in 2005 to over 540 million in 2009. Companies are concerned about spyware's security risks, regulatory compliance and employee productivity losses, the report says. The study also revealed that the administrative cost of dealing with spyware-infected computers was $265 per user in 2005 and is expected to continue to rise as spyware programs become increasingly devious.

The following table identifies five common types of spyware.

Category	*Typical Action*
Keystroke Logger (AKA Trackware)	Captures keystrokes (including personal information and passwords) or tracks the Web sites you visit.
Trojan	Enables remote control of your computer by a hacker, often for Distributed Denial of Service (DDoS) attacks.
Droneware	Sends spam via your address book or turns your PC into an unwitting host for offensive Web images.
Dialer	Auto-dials area code 900 or expensive long distance calls via your modem.
Adware	Pops up unsolicited and annoying advertisement-laden browser windows or hijacks your Internet search (Yahoo, Google, etc.) results.

Testbed 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 e-mail 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.

Security Report Card

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

Category and weight (%)	McAfee Total Protection for Enterprise	Microsoft Forefront Client Security
Identifying and thwarting malware (40%)	A	C
Performance (20%)	B	B
Ease of Use (10%)	A	B
Reports (10%)	A	B
Deployment (10%)	A	A
Documentation (10%)	A	B
Overall score	A	C +

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 e-commerce Web-based 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 e-mail him at barryn@erols.com.

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 Comdex, PC Expo and other venues. In addition, they've created industry standard network benchmark software, database benchmark software and network diagnostic utilities.