

Cascadia Labs URL Filtering and Web Security

Results from Summer 2009

Executive Summary

In the summer of 2009, Cascadia Labs performed effectiveness tests on five market-leading secure Web gateways, including three perimeter appliances from Blue Coat and McAfee, software from Websense, and the Trend Micro InterScan Web Security Virtual Appliance.

Cascadia Labs tested with URLs that it independently collected, classified, and verified using its proprietary systems — URLs neither supplied by, nor known to, any of the companies

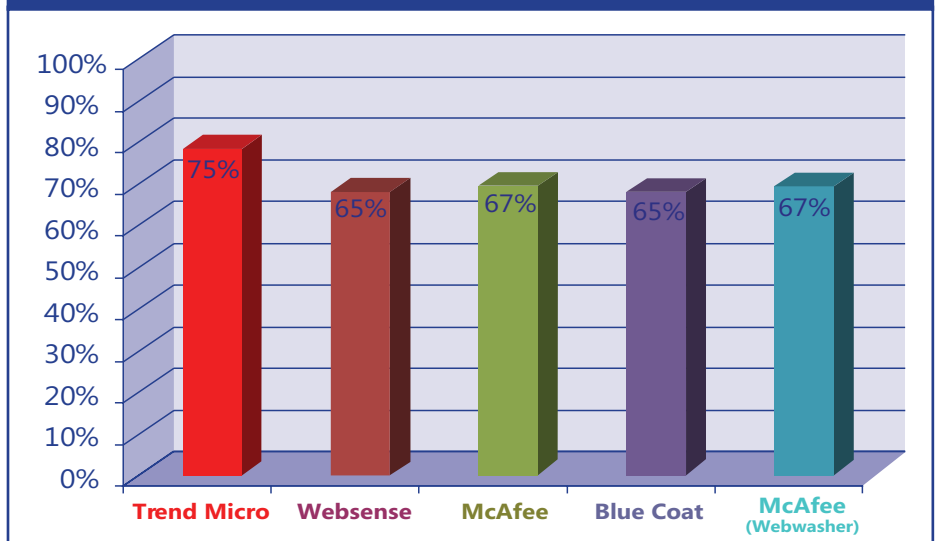
Trend Micro emerged as the clear winner, extending the leadership it established in 2008.

whose products were tested. We collected and verified security URLs in the days immediately before testing to ensure that they represented up-to-date threats including potential zero-day attacks actually occurring in the wild.

In these tests, Trend Micro emerged as the clear winner overall, extending the leading position it established in our testing in late 2008.

Trend Micro also demonstrated a decided advantage against security threats, with a significant contribution from its Web reputation services. In every security category — malware, exploits, phishing, proxies, and potentially unwanted applications —

Chart 1 - Overall Blocking Effectiveness (Weighted Average)



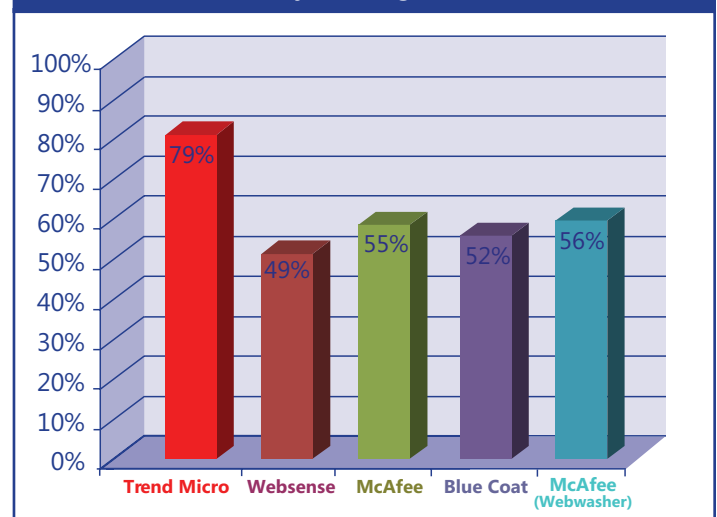
Trend Micro posted the best score. With an overall effectiveness at blocking security threats of nearly 80 percent, the Trend Micro IWSVA secure Web gateway stands distinctly apart from other products, whose averages ranged from just 49 to 55 percent.

on the Web. In addition to enforcing usage policies for Web pages that contain sexually explicit, violent, or illegal content, these products also can play a vital role in securing corporate networks against Web threats including drive-by downloads, malware, and phishing attacks.

Overview

Secure Web gateways contain a rich set of capabilities to manage, block, and control Web content at the perimeter. Companies rely on these products to protect their employees, PCs, and networks from dangerous, inappropriate, and unwanted content

Chart 2 - Overall Security Blocking Effectiveness



As these Web-borne security threats increase in frequency, volume, and sophistication, it is clear that additional layers of a defense-in-depth strategy are increasingly valuable. While filtering of adult-oriented and productivity-wasting sites is something of a commodity, there are large variations in how effectively products combine features such as URL databases and Web reputation services to block security threats.

In the summer of 2009, Cascadia Labs tested five market-leading secure Web gateways: perimeter appliances from Blue Coat and McAfee (including a former Webwasher product), Websense software, and the Trend Micro virtual appliance. Trend Micro emerged as the clear winner overall, with a decided advantage against security threats.

As shown in Chart 1, Trend Micro's InterScan Web Security Virtual Appliance (IWSVA) earned a weighted overall score of 75 percent. The two McAfee products tied for second place, each earning 67 percent. In addition to posting the highest score overall, Trend Micro also ranked first at blocking URLs leading to security threats, with a dominant 79 percent score, compared with other products' scores of approximately 50 percent.

Security aside, URL filtering products also serve an important function in enforcing companies' broader Web usage policies. Our testing shows that all of them block a great majority of adult-oriented and productivity and recreation URLs, and that all of them perform adequately — though with room for improvement — in the bandwidth usage, communications, and liability groups.

Products Tested

Cascadia Labs tested the following five products during August 2009:

- **Trend Micro InterScan Web Security Virtual Appliance v5**

- **Websense Security Suite v7.1**
- **McAfee Email and Web Security Appliance 3000**
- **Blue Coat Proxy SG 210A v5.4.1.12**
- **McAfee Web Gateway WW500E (formerly Webwasher) v6.8**

IronPort declined to allow us to purchase its software for this test.

Note that Websense has renamed its product "Websense Web Security".

In this report, Cascadia Labs focuses exclusively on the blocking effectiveness of the products' URL databases and Web reputation capabilities.

Results and Analysis

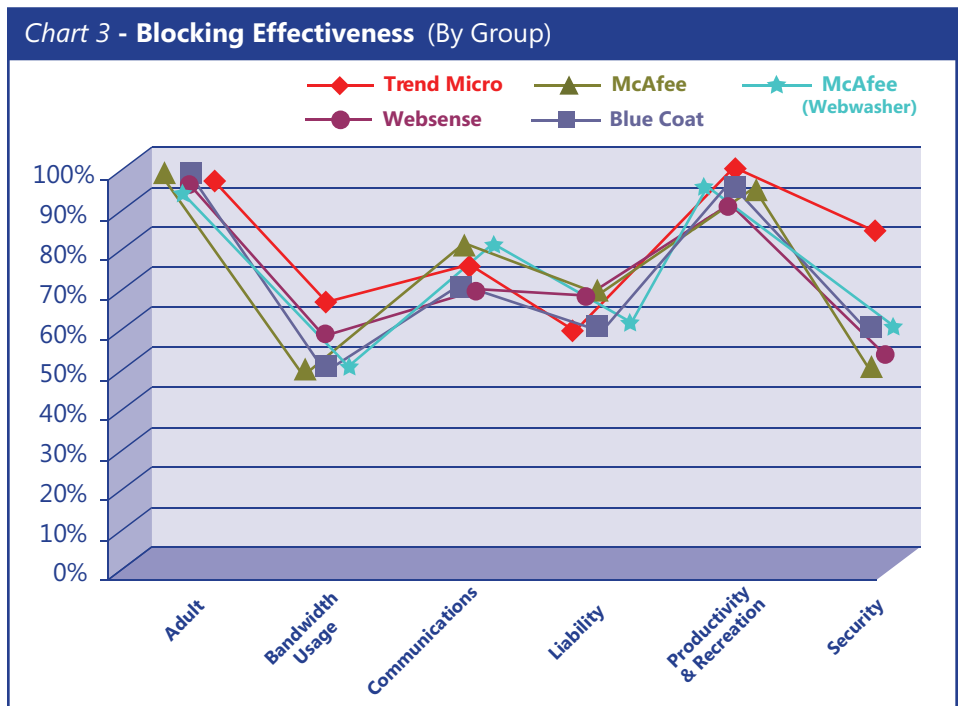
The Trend Micro IWSVA, which includes both remote rating and Web reputation capabilities, was consistently at or near the top at blocking effectiveness for each type of content (Chart 3).

Remote rating and Web reputation capabilities have, in recent years, made many secure Web gateway products more responsive to a complex and fast-changing Web. Instead of just consulting a local copy of a URL

database, products with remote rating can query remote servers to provide up-to-the-second data. Likewise, products with Web reputation capabilities can use heuristics to detect unusual patterns beyond those apparent in the content of the page itself. While we analyze the contribution of these various approaches, customers ultimately care about the products' ability to block unwanted URLs regardless of the underlying technology, and so our published reports show only the top-line blocking effectiveness results.

The big challenge for these products continues to be security threats. Average blocking rates stand at 58 percent — relatively low compared with other categories, though the average has improved over the past year. In this area, Trend Micro showed a marked advantage over the other products we tested.

In non-security categories, variations in effectiveness were modest. Products blocked liability URLs at an average of 59 percent, with no individual product showing a marked lead. Bandwidth usage blocking was less effective across the board, at an average 47 percent.



Products blocked communications URLs, including the omnipresent social media category, at 69 percent on average. As with previous quarters, the adult and productivity and recreation groups are effectively handled by all products, with little meaningful difference.

Security

Trend Micro's blocking average of 79 percent across all security categories placed it dramatically ahead of the other products, which ranged in effectiveness from 49 to 55 percent. The ability to block as many as four out of five threats, even without perimeter scanning enabled, illustrates the value that secure Web gateways can add as part of a defense-in-depth security strategy.

Malware

Trend Micro blocked three-quarters of all malware URLs, followed by the McAfee 3000 at 62 percent. The other products blocked between 53 and 55 percent. We define "malware URLs" to include both URLs pointing directly to malicious binaries (which often use social-engineering tricks to confuse users into unwittingly downloading and installing them) and URLs to payloads delivered during drive-by downloads.

Blocking malware URLs is a low-latency alternative to scanning binaries at the perimeter. To focus on products' URL-based blocking capabilities, Cascadia Labs did not enable any available malware scanning for these tests.

Exploits

Trend Micro blocked nearly 80 percent of exploit URLs, with the other products blocking between 48 and 58 percent. Exploits, or drive-by downloads, are insidious threats that can exploit the vulnerabilities found in browsers and third-party applications when users do nothing more than simply visit a Web page. It's especially important for secure Web gateways to block these threats, since they are invisible and even trusted and highly-trafficked sites can deliver them — typically as a result of being hacked with SQL injection attacks or being compromised by user-generated content.

Phish

Trend Micro blocked over 80 percent of phishing URLs. Websense and Blue Coat blocked 55 and 47 percent, respectively, and the McAfee products blocked under 40 percent. Phishing is a familiar problem, and while e-mail security products can remove many of the e-mails themselves, secure

Web gateway products can provide an additional layer of protection by blocking the link to the dangerous phishing URL in e-mails that are not otherwise filtered or that users access through an unprotected third-party e-mail provider.

Anonymizing Proxies

As in the other security categories, Trend Micro posted the best score, blocking 91 percent of proxies. The two McAfee products and Websense followed, blocking more than 60 percent; Blue Coat was last with an effectiveness of under 40 percent. Anonymizing proxies are not themselves dangerous, but they provide a way for users to bypass usage policies to access unsavory or potentially dangerous content. The proxy URLs we tested with in this report are Web-based proxies where users enter a URL into a form field.

Potentially Unwanted Applications

Trend Micro and the McAfee 3000 blocked 59 percent of these URLs, with Blue Coat and the McAfee Webwasher product blocking over 50 percent as well. Websense only blocked 23 percent of these URLs. Our definition of "potentially unwanted applications" includes tools that have some legitimate uses but many companies want to block, including certain system utilities, network-probing tools, and adware.

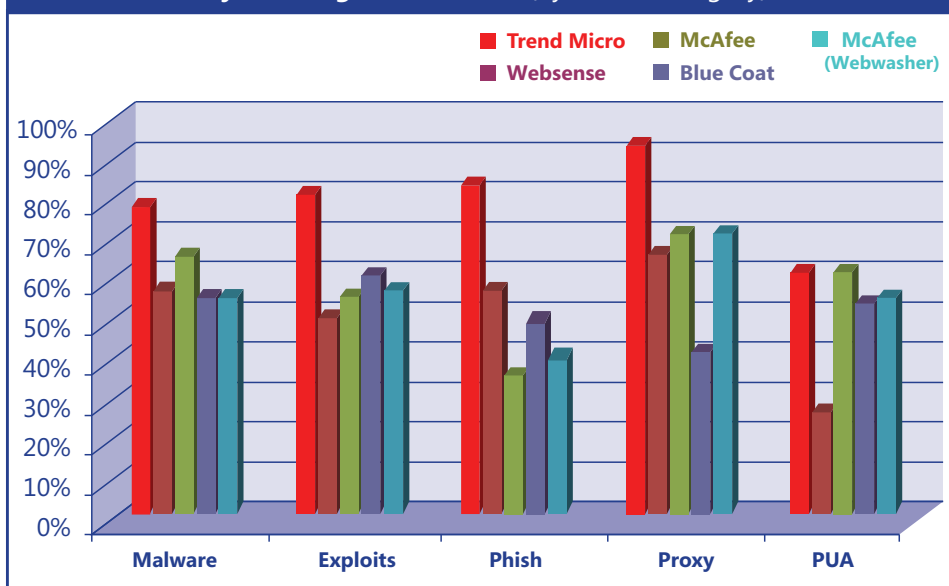
Adult

As is typical for this group, all products performed better than the 90 percent effectiveness Cascadia Labs expects to see. The adult group contains sexually explicit content and swimsuit and intimate apparel that may be considered inappropriate for the workplace.

Bandwidth Usage

The bandwidth usage group contains downloads, peer-to-peer, and streaming media URLs, and includes Torrent sites and video content on the Web. SurfControl was the winner in this category by a sizable margin, scoring

Chart 4 - Security Blocking Effectiveness (By Threat Category)



75 percent against the average of 59 percent. IronPort and Trend Micro were next, at 62 and 59 percent respectively, with the lowest score at 47 percent. Note that our bandwidth usage testing tests products' ability to block URLs based on the URL itself, rather than on protocol or file type — complementary approaches that companies can also adopt.

Communications

McAfee's Webwasher product led in this group, blocking nearly three-quarters of all URLs. The rest of the products blocked between 62 and 69 percent. This group encompasses social media sites, blogs, and personal communications and forums.

Liability

The McAfee 3000 posted the best score, 63 percent, followed closely by Websense at 61 percent. Other products blocked just over half of the content in this group, which includes criminal activity, hate and violence, illegal drugs, and the offensive content. As with the adult categories, companies typically block these categories to provide a more comfortable work environment free from unsuitable or lawsuit-prone content.

Productivity & Recreation

As in the adult group, there is little differentiation among the products when it comes to productivity and recreation categories; all products blocked around 90 percent of URLs. These categories include potential time-wasters such as entertainment, games, news, and shopping sites.

Rankings, Corpus, and Methodology

Scoring and Rankings

We derived overall results by applying weights to raw blocking results that represent what we believe to be the relative priorities of typical enterprise customers. Cascadia Labs re-evaluates this weighting on a quarterly basis, and over the last few years, security has

continued to increase in importance; for this report, the security group contributes 30 percent to our overall scores. Adult counts for 20 percent; bandwidth usage, 15 percent; liability, 15 percent; communications, 10 percent; and productivity and recreation, 10 percent. While this weighting reflects the heightened importance of secure Web gateways as a component of a defense-in-depth

Security URLs represent up-to-date threats, and are neither supplied by, nor known to, any of the companies whose products we tested.

security strategy, it also recognizes companies' continuing need to block visible content, such as social media or offensive Web pages.

Note that these rankings do not consider performance, scalability, user interface, features, or functionality — only blocking effectiveness against our summer 2009 corpus.

The Corpus

We created our independent URL corpus to address the requirements of the enterprise market, with a particular emphasis on security. The corpus contains 22 unique categories organized into six groups with more than 1,600,000 URLs from approximately 100,000 unique domains, primarily those of interest to English-language users.

Our corpus includes security threats in five different categories: malware, exploits, phishing, proxy, and potentially unwanted applications (PUAs). We collect and verify security URLs in the days immediately before testing to ensure that they represent up-to-date threats including potential zero-day attacks actually occurring in the wild. This timeliness is crucial

to differentiating products' ability to handle realistic, transient Web-borne threats.

For this report, Cascadia Labs tested with more than 2,000 security URLs, including approximately 250 malware, 1,100 exploit, 200 phish, 400 proxy avoidance, and over 200 potentially unwanted application URLs.

The URLs that Cascadia Labs uses for testing are gathered from sites in the wild, using a variety of proprietary discovery, analysis, and verification techniques. They are neither supplied by, nor known to, any of the companies whose products were tested.

Test Methodology

We configured tested products as proxies. For Websense, we used Microsoft ISA Server integration.

We let all products use any available remote rating capability and update continuously throughout the testing timeframe.

Because each vendor uses its own set of categories for classifying URLs, we create category mappings from our categories to the vendors' chosen categories to ensure we used comparable blocking configurations for each product. For our testing, we configured each product to block an entire group (defined to contain similar categories), so our blocking results would not be affected by slight differences that vendors might make in their category choices.

Since Web reputation is targeted primarily against security URLs, we only enable it for that group's testing.

In order to isolate products' core URL filtering capabilities, Cascadia Labs did not enable protocol filtering or malware scanners on any of the products. Protocol filtering can be an effective additional measure to block instant messaging and other unwanted services, though of course, protocol

filtering is not practical for HTTP itself (and the URLs we tested) given the importance of the Web. Scanning binaries at the perimeter offers another layer of protection as well, but can introduce additional latency for users, and we did not include it as part of our testing for this report.

To enable testing of real-time and remote rating capabilities without compromising the ongoing integrity of our URL corpus, Cascadia Labs uses a sample of 1,000 randomly-selected URLs in each category (and 2,000 for the entire set of security categories), which allows us to state blocking

results in most categories with confidence interval of plus or minus 3 percent (at the 95-percent confidence level). After use, these URLs are discarded, with the exception of URLs for high-traffic sites, to avoid giving any product an advantage in subsequent testing. ▲



Independent evaluations of technology products

Contact: info@cascadialabs.com
www.cascadialabs.com



This comparative review, conducted independently by Cascadia Labs in summer 2009, was sponsored by Trend Micro. Cascadia Labs aims to provide objective, impartial analysis of each product based on hands-on testing in its security lab.