Presented by Cascadia Labs

COMPARATIVE REVIEW

Cascadia Labs URL Filtering and Web Security

Results from Q4 2008

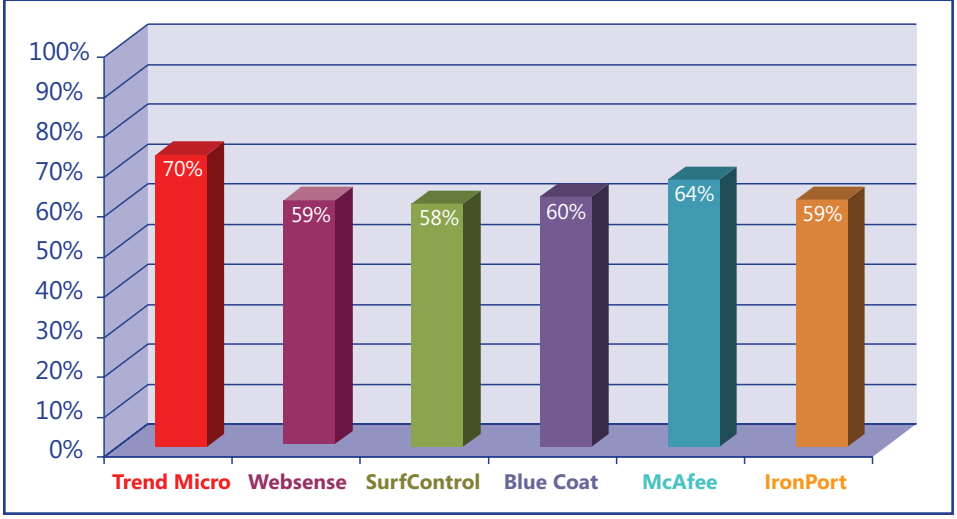
Executive Summary

Companies rely on URL filtering and Web security products to protect their employees, PCs, and networks from dangerous, inappropriate, and unwanted content on the Web. In addition to blocking Web pages that contain sexually explicit, violent, or illegal content, these products also play an increasingly important role in securing corporate networks – they can provide a first line of defense against malicious Web pages and restrict bandwidth-hogging downloads. While filtering of adult-oriented and productivity-wasting sites is something of a commodity, there are notable differences in how individual products perform against more challenging types of Web content, and a large variation when it comes to blocking security threats.

Cascadia Labs regularly tests the effectiveness of URL filtering products using URLs selected from its independent, living corpus of more than 1.5 million categorized Web pages. We test products' ability to block content in 22 specific categories within six broad groups of primarily English-language pages: Security, Adult, Bandwidth Usage, Communications, Liability, and Productivity & Recreation.

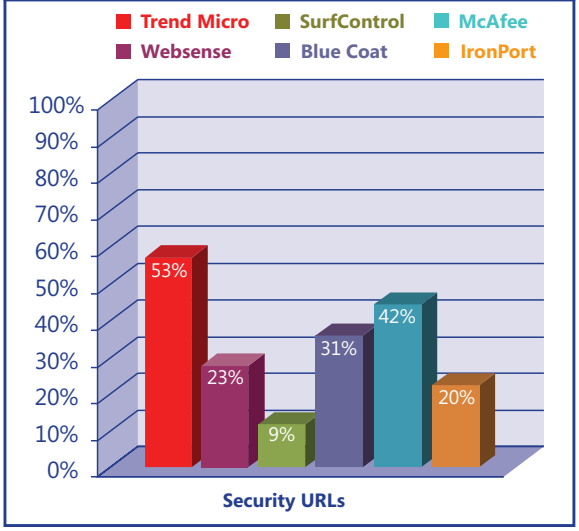
In our December 2008 Web Security Tests of six market-leading URL filtering and Web security products, including both perimeter appliances and server software, Trend Micro emerged as the clear winner. As shown in Chart 1, Trend Micro's InterScan Web Security gateway solution (IWSA) earned a weighted overall score of 70 percent, while the second-ranked product, the McAfee Web Security Appliance 3300 with Enhanced URL Filtering Database, earned 64 percent. In addition to posting the highest score overall, Trend Micro also ranked first at blocking URLs pointing at security threats.

***Chart 1* - Overall Blocking Effectiveness** (Weighted Average)



Blocking substantial numbers of URLs that lead to security threats, in fact, clearly differentiates the leading products from the rest, as shown in Chart 2. URL filtering products that include effective Web security capabilities can provide a first line of defense to help protect users and companies from malicious content. 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 and Productivity & Recreation URLs, and that all of them also fare adequately — though with some room for improvement — in the Bandwidth Usage, Communications, and Liability groups.

***Chart 2* - Overall Security Group Blocking Effectiveness**



Cascadia Labs

We derived the 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 quarter's testing, 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 & Recreation, 10 percent. (Because Trend Micro's effectiveness was highest or close to highest in virtually every category, it would place first using almost any reasonable set of weights we chose.)

While this weighting reflects the heightened importance of URL filtering as a component of a defense-in-depth security strategy, it also recognizes companies' continuing need to block visible content, such as offensive Web pages. In this latter area, Trend Micro led in the Liability, Communications, and Productivity & Recreation groups, while SurfControl was best in Bandwidth, and McAfee was first in the Adult group.

Products Tested

Cascadia Labs tested the following six products for this report during Q4 2008:

- **Trend Micro InterScan Web Security Appliance 2500** v3.1_sp1_Build_Linux_1218
- **Websense Enterprise and Web Security Suite v7.0** (database versions 03026-03211)
- **SurfControl Web Filter for Microsoft ISA Server v5.5.3.201 SP3** (database versions 2170-2173)
- **Blue Coat ProxySG 200 v5.3.2.1** (database versions 20086322-200900104)
- **McAfee Web Security Appliance 3300 with Enhanced URL Filtering Database v5.0** (database versions 14789-14869)
- **IronPort Web Security Appliance S650 v5.6.0-626** (database versions 2170-2173)

Trend Micro's IWSA relies on an in-the-cloud database, so it has access to ratings for URLs as soon as they are posted on Trend Micro's servers, rather than waiting for a periodic update to the appliance's local database. Trend Micro, McAfee, Blue Coat, and IronPort also incorporate Web reputation capabilities. Since Web reputation is targeted primarily against security URLs, we only enable it for that group's testing.

Cascadia Labs' testing and analysis focuses exclusively on the blocking effectiveness of the products' URL databases and Web reputation capabilities. In order to isolate products' core URL filtering capabilities, Cascadia Labs did not enable protocol filtering, anti-virus scanners, or anti-spyware 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 potentially high latency for users.

Selected Results and Analysis

Cascadia Labs conducts quarterly testing of URL filtering products using its proprietary corpus of over 1.5 million categorized URLs. Each quarter, Cascadia Labs adds new URLs to reflect the current state of the Web, removes expired or obsolete URLs, and collects fresh security threats URLs just prior to testing. Cascadia Labs uses a variety of vectors, not just search-engine results, to identify candidate Web pages for its corpus. We apply a rigorous quality-assurance process that ensures that URLs are accurate and appropriate, so that our testing yields meaningful results and specific insights about product behavior.

Traditionally, products have blocked URLs using local databases which are updated frequently by the vendors. In recent years, more products have added remote database lookup, often described as in-the-cloud or Security as a Service (SaaS) protection, to provide more timely responses to a fast-changing Web. Products have also added Web reputation and real-time categorization capabilities to complement database-driven approaches. 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. As our test results show in Chart 4, below, the Trend Micro IWSA, which does include both remote rating and Web reputation capabilities, was consistently at or near the top at blocking effectiveness for each group of content.

Security

The best products demonstrated that they can serve as a valuable first line of defense against security threats. Cascadia Labs' security group contains real-world threat URLs in five categories: malware, drive-by download, phishing, proxy, and potentially unwanted applications. To ensure timeliness and accuracy, we verified URLs as malicious within an hour of product testing. Cascadia Labs uses security URLs that point directly to malicious content such as a malware binary, a URL that is itself or ultimately redirects to a drive-by download, or a phishing URL.

Trend Micro won the top score in our security testing, blocking 53 percent of threat URLs and McAfee had the next best score at 42 percent. Other products scored between 9 and 31 percent. Chart 3 illustrates how each product fared in our five security categories.

Malware

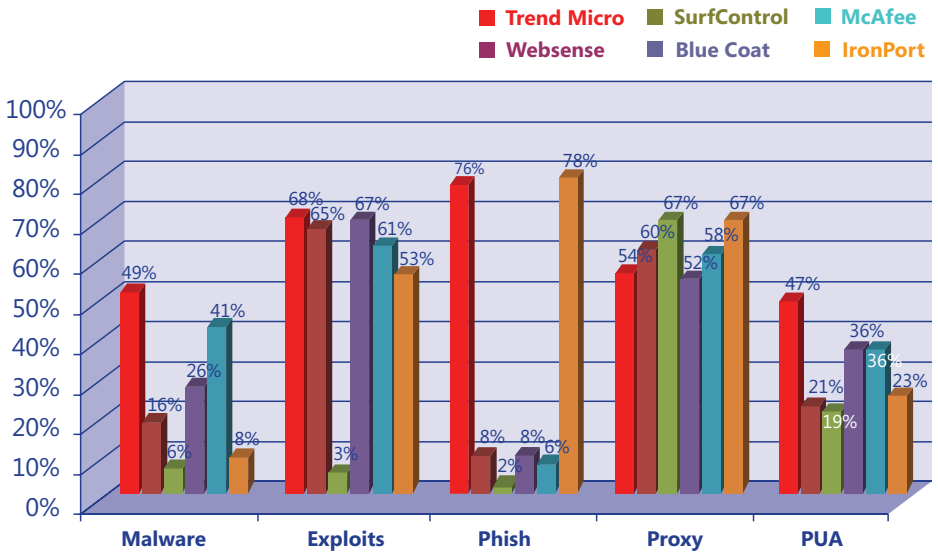
Malicious downloads – including

Trojans, worms, and viruses – continue to be a threat to Web users, and Trend Micro turned in the best overall blocking in this category. It blocked 49 percent of malware URLs, providing a useful first line of defense against URLs that point to malicious files. The next best score, McAfee's, was 41 percent. The rest of the products blocked very poorly, from 26 percent to only 6 percent for SurfControl.

Exploits
Exploits, or "drive-by" downloads, present a unique challenge to URL filtering products. They are often transient and can appear suddenly even on high-traffic, reputable sites. When pitted against 100 Web-based exploits, Trend Micro, Blue Coat, and Websense were the best, blocking between 65 and 68 percent of the threats. McAfee scored 61 percent, and IronPort blocked a respectable 53 percent, but SurfControl only blocked a dismal 3 percent of drive-by download URLs.

Phishing
Phishing URLs typically have very short lifetimes and present a real challenge for URL filtering products. Cascadia Labs collected a variety of phishing threats, including phish targeting eBay and PayPal, as well as banks such as Abbey and Chase. Only Trend Micro and IronPort fared well against these URLs, blocking 76 and 78 percent respectively. The other products all blocked less than 10 percent of these threats. Phishing effectiveness indicates that companies are working in near real-time to analyze and publish threats.

***Chart 3* - Security Blocking Effectiveness by Threat Category**



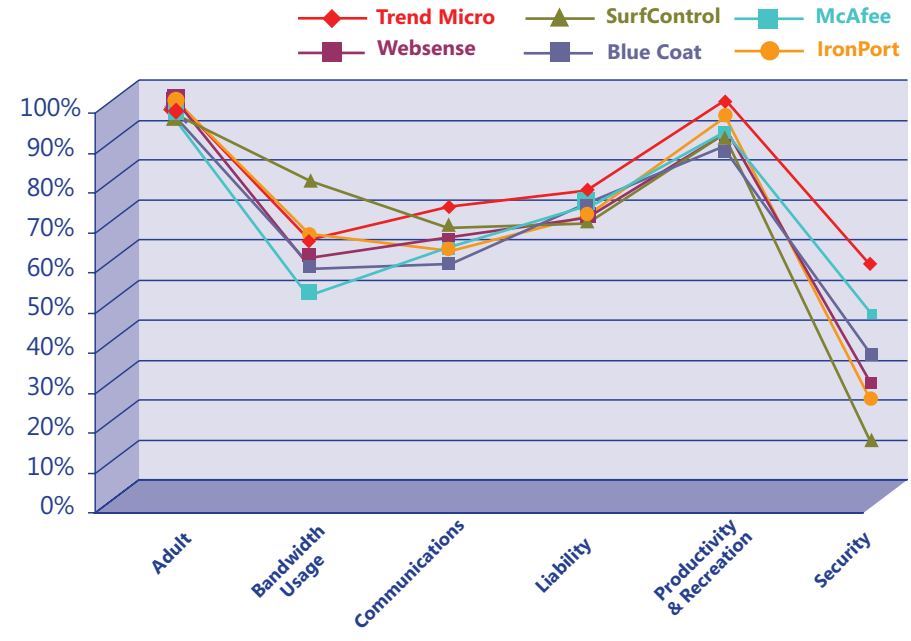
Proxy
Sites that host a proxy service or publish lists of public proxies and anonymizers are a potential concern for companies because they can allow employees to subvert URL filtering rules. Among these URLs, SurfControl and IronPort fared best at 67 percent, with the other products blocing between 52 and 60 percent.

Potentially Unwanted Applications
PUAs include questionable, but not necessarily malicious, URLs such as adware downloads. Trend Micro blocked 47 percent, leading a group that only blocked 30 percent on average. McAfee and Blue Coat tied for second place, blocking 36 percent of these URLs.

Adult
URL filtering originated to block adult content, and not surprisingly for such a mature category, all six products blocked over 90 percent of adult URLs. No product will ever block every last objectionable URL, but when products all reach a level of 80 percent or better, we consider the differences too insignificant to influence a purchasing decision.

Bandwidth Usage
The Bandwidth Usage group contains downloads, peer-to-peer, and

***Chart 4* - Blocking Effectiveness** (By Group)



Cascadia Labs

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 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
The Communications group includes both personal communications such as e-mail and chat and also community-based communication such as blogs and forum sites. In it, Trend Micro placed first with a 69 percent block rate — 4 percentage points better than the second-place finisher and 7 points above the group average. Trend Micro did especially well in the blog category, blocking 80 percent of URLs, or 12 percentage points above the category average.

Liability
Our Liability group includes categories such as criminal activity, hate and violence, and illegal drugs — highly-charged content that companies are especially interested in blocking. URLs in this group are often more challenging for products to block because their creators often try to hide them from mainstream audiences. Trend Micro performed best in this group by a small margin, blocking 71 percent of the URLs, while the least-effective product blocked 62 percent.

Productivity & Recreation
This group includes potential time-wasting categories such as sports, games, and entertainment. As in the Adult group, all products performed at a high level here; Trend Micro's 94 percent block rate made it number one in this category.

Methodology and Test Corpus

Cascadia Labs provides objective, independent evaluations of technology products. For our December 2008 Web Security Tests, Cascadia Labs measured the effectiveness of the URL blocking capabilities provided by six market-leading products. Cascadia Labs did not assess the products' user interface, features, functionality, or scalability, nor did we test binary scanning or protocol-based blocking.

The Corpus
We maintain our English-language URL corpus to address the requirements of the enterprise market. The corpus contains more than 1.5 million URLs from approximately 100,000 unique domains, organized into six groups representing 22 unique categories. Cascadia Labs randomly selects at least 1,000 samples — enough to draw statistically significant conclusions — for each of the categories in the Adult, Bandwidth Usage, Communications, Liability, and Productivity & Recreation groups. Cascadia Labs selects 1,000 URLs in total for the Security group: 750 malicious binaries of various types, 100 exploits, 50 phishes, 50 proxies, and 50 potentially unwanted applications.

Groups and Categories
We chose the categories and URL distribution in our corpus to address the requirements of large enterprises. For example, our corpus includes content categories such as sexually explicit, illegal drugs, criminal activity, shopping, streaming media, and malware. Our corpus does not include categories such as art, health and medicine, philanthropic sites, education, and culture, because these categories are targeted more at K-12 educational customers, who typically block everything and then use these categories in "allow" rules (white lists). Our corpus contains URLs from both popular and obscure sites across a variety of top-level domains and countries, with content predominantly in English.

Each vendor uses its own set of categories for classifying URLs. We create category mappings from our categories to the vendor's chosen categories to ensure we used comparable blocking configurations for each product. We perform preliminary tests to ensure that we have appropriate category mappings for each of the products.

Test Methodology
We test blocking accuracy against live servers on the Internet. We configured each product to block an entire group of categories so that our blocking results would not be affected by the slight differences that vendors make in their category choices. For example, some vendors might place a bowling URL in the sports category, while other vendors might place it in the hobbies and recreation category. In our testing, the bowling page would register as blocked in either case, because both sports and hobbies and recreation are in our Productivity & Recreation group.

We configured all test products in a proxy configuration. We integrated SurfControl and Websense with Microsoft ISA Server; the other products are appliances. We let all products update at least once a day, and logged the database versions used during testing for each product that employed a local database.

Cascadia Labs enabled Trend Micro's anti-phishing module and Blue Coat's suspicious URL category for testing. In addition, Trend Micro, McAfee and IronPort all offer Web reputation features, which we enabled for security testing.

URLs that we use in testing, with the exception of those from high-traffic sites such as amazon.com and espn.go.com, are discarded from our corpus to prevent any vendor from gaining an advantage in future testing. ▲

Independent evaluations of technology products

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

This comparative review, conducted independently by Cascadia Labs in December 2008, 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, and gives each company whose products are included the opportunity to participate by providing input on Cascadia Labs' test plan and feedback on our findings.