

# Cascadia Labs URL Filtering and Web Security

## Results from October 2008

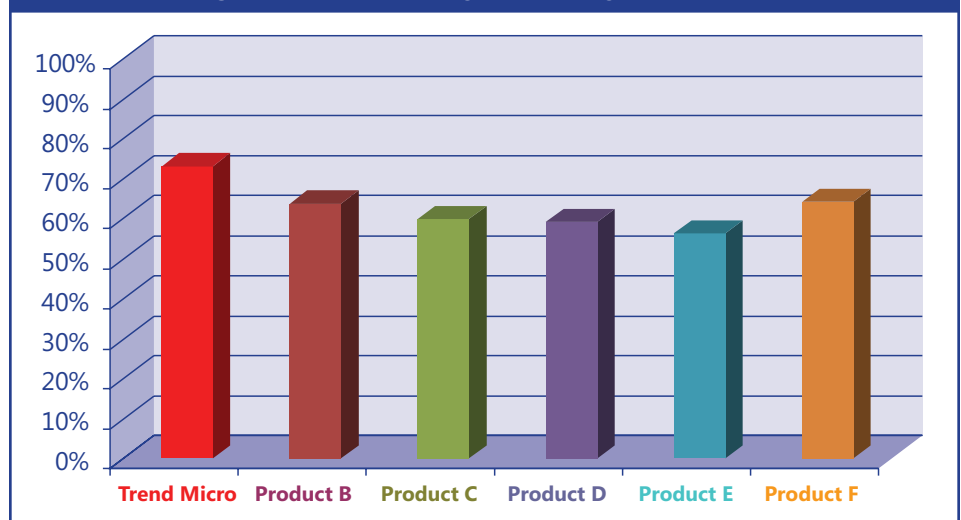
### Executive Summary

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-draining sites is something of a commodity, there are vast differences in how individual products perform against more challenging types of Web content and security threats in particular.

Cascadia Labs regularly tests the effectiveness of URL filtering products using URLs selected from its independent 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 October 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. The Web Security technology in Trend Micro's InterScan Web Security gateway solution (IWSA) earned a weighted overall score of 73 percent, while the second-ranked

Overall Blocking Effectiveness (Weighted Average)



product earned just 64 percent. In addition to posting the highest score overall, Trend Micro also ranked first at blocking URLs containing security threats.

The InterScan Web Security gateway product leverages Trend Micro's Smart Protection Network which includes an in-the-cloud URL database and Web reputation capabilities. This approach provides customers immediate protection against new URL threats as soon as Trend Micro posts them on its remote servers and without the need to manage database updates.

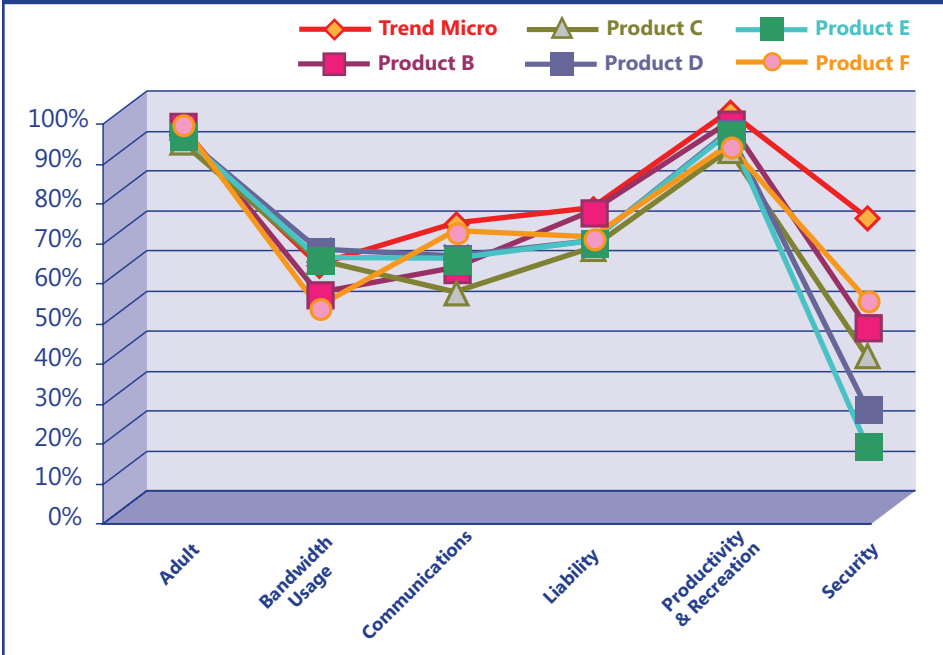
We derived the overall results by applying weights to raw blocking results that represent what we believe to be the relative priorities of typical enterprise customers: Security, 25 percent; Adult, 20 percent; Bandwidth Usage, 20 percent; Liability, 15 percent; Communications, 10 percent; and Productivity & Recreation, 10 percent.

This weighting reflects the heightened importance of security but also recognizes companies' need to block visual content such as offensive Web pages.

### Project Background

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 changed URLs, and collects fresh security threats including malware, drive-by download, phishing, and proxy 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.

## Blocking Effectiveness (By Group)



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, Web reputation, anti-phishing, and real-time categorization capabilities to keep up with the fast-changing Internet. For example, Trend Micro Web Security technology leverages a remote database, anti-phishing, and Web reputation in its product. While we analyze the contribution of various approaches such as these, it's ultimately the products' ability to block unwanted URLs that matters to customers. And as the chart below illustrates, the Trend Micro Web Security technology was consistently at or near the top at effectiveness blocking each group of content.

### Testing Scope

Cascadia Labs' testing and analysis focuses exclusively on the blocking effectiveness of the products' URL databases and Web reputation capabilities. Since products use Web reputation primarily against security URLs, we only enable it for that group's testing. In order to focus on products' core URL filtering capabilities, Cascadia

Labs tested products without included or optional perimeter anti-virus or anti-spyware scanners, which also introduce potentially high latency for users.

## Selected Results and Analysis

### Security

Cascadia Labs' security group contains real-world threat URLs in five categories (malware, exploits, phishing, proxy, and potentially unwanted applications) in a distribution that mimics their real-world prevalence. To assure timeliness and accuracy, we verified URLs as malicious within an hour of product testing. Trend Micro won the top score in our security testing, blocking 68 percent of threat URLs. By contrast, most competing products blocked less than 10 percent of the phishing and exploit URLs in our corpus; even the best blocked just 48 percent.

**Malware:** Trend Micro blocked 68 percent of malware URLs – including Trojans, worms, viruses, and other downloads – making it an effective and fast first line of defense against URLs that point to malicious files. The next best competing product's score was only 49 percent.

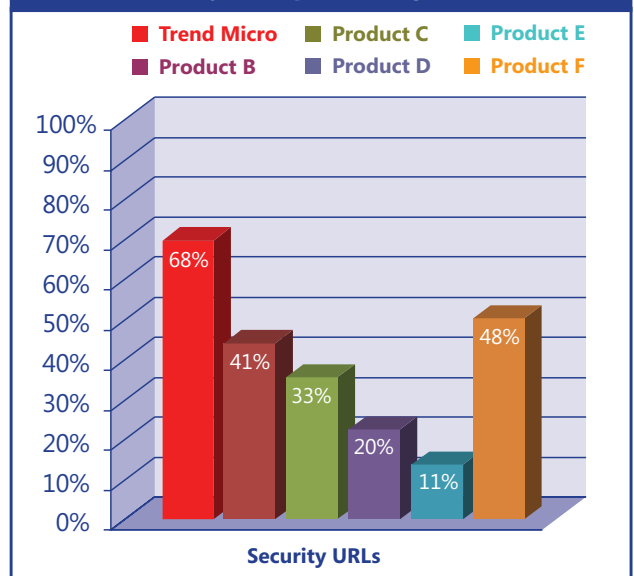
**Exploits:** When pitted against exploits, or "drive-by" downloads, Trend Micro was by far the best product we tested. It blocked 73 percent of these threats, while the next-best product blocked only 33 percent.

**Phishing:** Trend Micro blocked 74 percent of these URLs, compared with an average of just 20 percent. Two competing products blocked no phishing URLs at all.

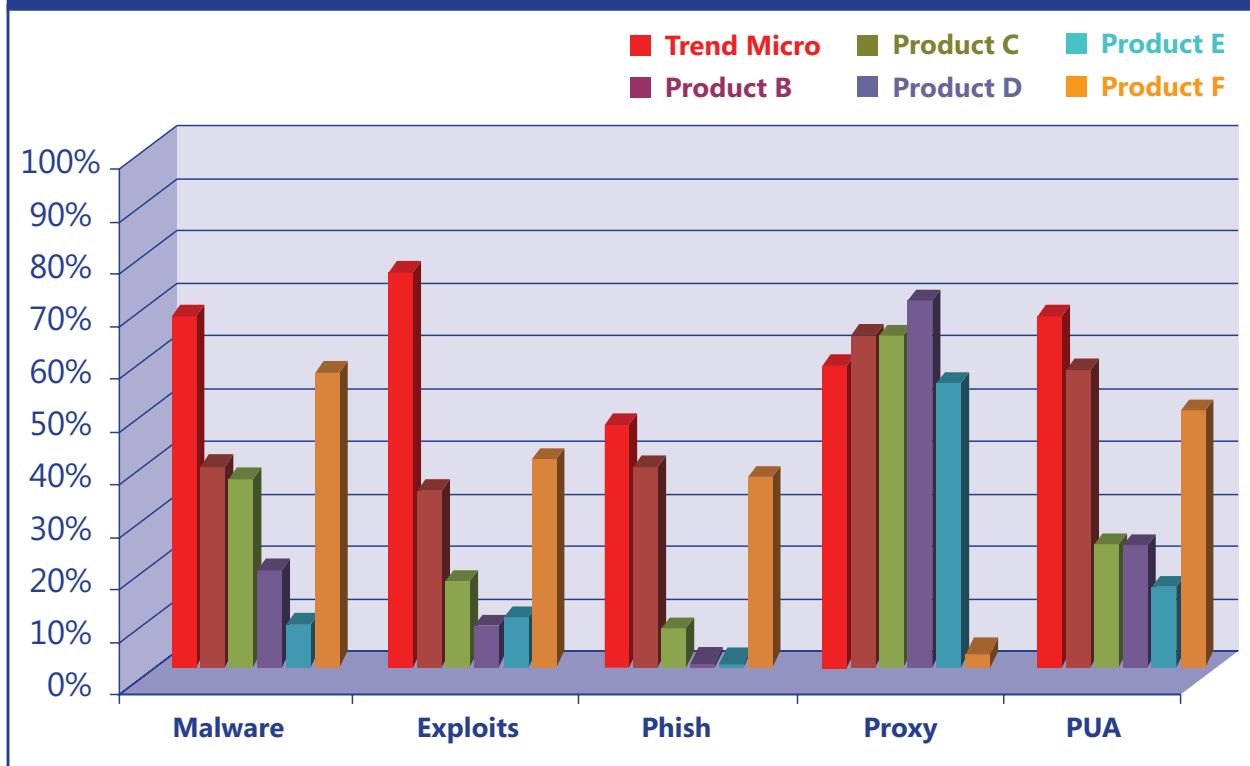
**Proxy:** Sites that host a proxy service or publish lists of public proxies and anonymizers are a potential concern for companies because they can allow employees to subvert URL filtering rules. Among these URLs, Trend Micro blocked 57 percent, placing third, only 4 percent behind the second place product.

**Potentially Unwanted Applications:** URLs in this category include questionable, but not necessarily

## Overall Security Group Blocking Effectiveness



## Security Blocking Effectiveness by Threat Category



malicious, URLs such as adware downloads. Trend Micro blocked 64 percent, leading a group that only blocked 39 percent on average.

### Adult

All six products we tested blocked more than 80 percent of URLs, a level that Cascadia Labs considers sufficient for corporate applications. No product will ever block every last objectionable URL, but beyond this point, we consider the tiny differences unimportant in making a purchasing decision. Trend Micro blocked 90 percent of all Adult URLs.

### Bandwidth Usage

The Bandwidth Usage group contains downloads, peer-to-peer, and streaming media URLs. This group has grown in importance given the growth of Torrent sites and video content on the Web. Note that our Bandwidth Usage testing tests products' ability to block URLs based on the URL itself, rather than on protocol, an alternative that many companies will adopt. We found that Trend Micro blocked 56

percent of these URLs, 2 percentage points above the average.

### Communications

Trend Micro won the top score in the Communications group, which includes blogs and communication sites, with a 67 percent block rate — 3 percentage points better than the second-place finisher and 8 percentage points above the group average. Trend Micro did especially well in the blog category, blocking 79 percent of URLs, or 14 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, blocking 71 percent of the URLs.

### 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 95-percent block rate made it number one in this category also.

## Methodology and Test Corpus

Cascadia Labs provides objective, independent evaluations of technology products. For our October 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.

### Groups and Categories

We chose the categories and URL distribution in our English-language

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, which 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.

### 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.

### Sampling and Statistics

To enable the testing of real-time and remote rating capabilities without revealing the composition of our entire corpus, Cascadia Labs uses a randomly chosen sample of at least 1,000 URLs in each category, enough to draw statistically meaningful conclusions. URLs that we use in testing, with the exception of URLs from high-traffic sites such as amazon.com and espn.go.com, are then discarded from our corpus to prevent any vendor from gaining an advantage in future testing. ▲



Independent evaluations of technology products

Contact: [info@cascadialabs.com](mailto:info@cascadialabs.com)  
[www.cascadialabs.com](http://www.cascadialabs.com)



*This comparative review, conducted independently by Cascadia Labs in October of 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.*