

# Clearswift URL Filtering

## Powered by Symantec Rulespace

### General Features

- Categorizing 99.9% of the active web, enabled by a Global Feedback Network of hundreds of millions of users worldwide
- More than 55 million sites categorized with 10 million new sites added and 10 million dead sites removed each year
- Coverage representing billions of web pages from around the world
- Over 100 categories using automated categorization technology (machine learning) that has been continually improved for over a decade.
- Additional Data Feeds (Government, illegal content, terrorism, etc.)
- Sophisticated deep learning system used for categorizing image heavy, text poor sites
- Experienced team to support override requests, with human support
- Sensitive categories such as Suicide and Hate are manually curated
- Unknown URLs returned from customers automatically processed
- Categorization Experts performing targeted discovery supporting customer requirements
- Daily manual review of Top Unknowns from each customer. Regularly maintained –URLs frequently rechecked.
- Pages analyzed in over 28 languages including: Arabic, Catalan, Chinese, Czech, Danish, Dutch, English, Estonian, Finnish, French, Greek, German, Hebrew, Hindi, Hungarian, Italian, Japanese, Korean, Lithuanian, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Thai, Turkish, and Vietnamese.

### Special Features

#### PHISHING CATEGORIZATION DATABASE (PCD)

The PCD is a comprehensive database of confirmed phishing URLs on the web. Phishing attacks use both social engineering and technical subterfuge to steal private information from users. Clever social-engineering schemes use 'spoofed' emails from well-known banks and other companies to lead users to counterfeit Websites designed to trick them into divulging secret financial and personal information like credit card numbers, pins, usernames and passwords.

#### MALWARE CATEGORIZATION DATABASE (MCD)

Symantec Malware data feeds are derived from deep, proprietary analysis of billions of events from the Symantec™ Global Intelligence Network. The Global Intelligence Network provides global visibility into the threat landscape, including:

- More than 41.5 million attack sensors in 157 countries
- An extensive anti-fraud community of enterprises, security vendors and more than 50 million end users
- More than 8 billion emails scanned per day - 1/3 of all enterprise email
- Monitoring of over 5 million decoy accounts
- More than 13 billion web requests handled per day

By combining this visibility with our automated analysis and human research efforts, the MCD provides unique, timely and actionable protection from Internet-based threats. These sites are organized into 4 different categories. The database is frequently updated and when integrated into a Web filtering solution to provide an effective protection against ever changing Internet-based malware threats.

## About Clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations to have 100% visibility of their critical information 100% of the time.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at [www.clearswift.com](http://www.clearswift.com)

### UK - International HQ

Clearswift Ltd  
1310 Waterside  
Arlington Business Park  
Theale, Reading, Berkshire  
RG7 4SA

Tel : +44 (0) 118 903 8903  
Fax : +44 (0) 118 903 9000  
Sales: +44 (0) 118 903 8700  
Technical Support: +44 (0) 118 903 8200  
Email: [info@clearswift.com](mailto:info@clearswift.com)

### Australia

Clearswift (Asia/Pacific) Pty Ltd  
Level 17 Regus  
Coca Cola Place  
40 Mount Street  
North Sydney NSW 2060  
Australia

Tel: +61 2 9424 1200  
Technical Support: +61 2 9424 1200  
Email: [info@clearswift.com.au](mailto:info@clearswift.com.au)

### Germany

Clearswift GmbH  
Im Mediapark 8  
D-50670 Cologne  
Germany

Tel: +49 (0) 221 8282 9888  
Technical Support: +49 (0)800 1800556  
Email: [info@clearswift.de](mailto:info@clearswift.de)

### Japan

Clearswift K.K  
Shinjuku Park Tower N30th Floor  
3-7-1 Nishi-Shinjuku  
Tokyo 163-1030  
Japan

Tel: +81 (3)5326 3470  
Technical Support: 0800 100 0006  
Email: [info.jp@clearswift.com](mailto:info.jp@clearswift.com)

### United States

Clearswift Corporation  
309 Fellowship Road, Suite 200  
Mount Laurel, NJ 08054  
United States

Tel: +1 856-359-2360  
Technical Support: +1 856 359 2170  
Email: [info@us.clearswift.com](mailto:info@us.clearswift.com)

CATEGORIES	DESCRIPTION
<b>Potential Malware Victim (MALVIC)</b>	Sites that clickfraud and adware components use when 'phoning home' which could signal that a device is infected with spyware or adware. This category should be used only for reporting, not for blocking as the target URLs can be perfectly legitimate sites.
<b>Malware Domain (MALDOM)</b>	Sites where the domain was found to either contain malware or take advantage of other exploits to deliver adware, spyware or malware.
<b>Malware Phishing (MPHISH)</b>	Sites containing characteristics of phishing techniques: transposition, misspellings, common phishkit paths, and other phishing keywords. Also includes phishing sites reported to eBay and Paypal as well as other 3rd-party phishing feeds.
<b>Malware Attack &amp; Botnet (MATTCK)</b>	Sites that have attempted a vulnerability exploitation or Denial of Service attack and any sites hosting a botnet command and control channel.

## Competitors

- Zscaler
- Cisco OpenDNS
- Check Point
- Forcepoint
- Palo Alto Networks