

17

SurfControl plc., CyberPatrol 7.6

SurfControl's CyberPatrol provides blocking, monitoring and logging functionality.

Its support of platforms and languages is summarised in the table below:

Type	Client	Server	Service						
Platforms	Win95	Win98	WinME	Win2k	Win03	WinNT	WinXP	Linux	MacOS
Protocols / Applications	browser	instant msg	chat	e-mail	news	file transfer	peer2peer	VoIP	Stream
Languages User Interface	Czech	Danish	Dutch	English	Estonian	Finnish	French	German	Greek
	Polish	Portuguese	Slovak	Slovenian	Spanish	Swedish	Lithuanian	Maltese	
Languages Filtering Criteria	Czech	Danish	Dutch	English	Estonian	Finnish	French	German	Greek
	Polish	Portuguese	Slovak	Slovenian	Spanish	Swedish	Lithuanian	Maltese	

The feedback given by the User Reference Group is summarised as follows:

Test domain	Score	Actual score	Average all tools	Best tool
(Un)installing and updating the tool	●●○	2,5	2,3	2,8
Tailoring and monitoring the filtering	●●○	2,9	2,5	3,2

The scores of the Lab tests are summarised as follows:

Test domain	Score	Actual score	Average all tools	Best tool
Local language support	●●○○	2,0	2,6	4,0
Effectiveness for kids	●●○	2,5	2,0	4,0
Effectiveness for adolescents	●●○	2,5	1,8	2,5
Effectiveness for kids (porn only)	●●○	2,5	2,6	4,0
Effectiveness for adolescents (porn only)	●●●○	3,0	2,5	4,0
Speed of filtering	●●●●	4,0	3,2	4,0
Security Integrity	●●●●	4,0	2,7	4,0
Legal Compliance	●●○	2,5	2,4	3,5

1. Configurability

CyberPatrol provides a useful default filtering policy, with several harmful content categories that can be easily fine-tuned by the child carer. The child carer can also choose between pre-set filter settings for several ages. CyberPatrol provides the option to maintain black and white lists for websites, keywords, applications, chat programs and newsgroups.

New users can be created, but it is not possible to work with user groups.

CyberPatrol can be updated both manually and automatically.

2. Usability

The user interface is well structured, easy to understand and each setting is well explained. The user interface is not really adaptable to the user wishes, but can be controlled with the keyboard only.

Help information is available and easily accessible. The manual is detailed, user-friendly and to the point.

3. Filtering Algorithm & Effectiveness

The scores of the Lab tests for the individual effectiveness tests are:

Content Type	Score
Web ICRA filtering	N/A
Instant Messaging	Disable
Chat	1
Email	N/A
Newsgroup	1
File Transfer Protocol	N/A
Voice over IP	N/A
Streaming media	N/A
Peer-to-peer	N/A

Web filtering: URL based filtering

CyberPatrol provides the option for the child carer to maintain a white list (allowed access) and black list (denied access) of website URLs.

Web filtering: Content filtering

CyberPatrol provides the option to block websites based upon several content categories. It is also possible for the child carer to add keywords which the website should not contain. If these words are found in the website, access to the site is denied.

Instant messaging MSN

CyberPatrol provides the option to block an instant messaging application or restrict the use of it in time, by adding it to the blocked programs list.

CyberPatrol also provides the option to check all instant messages (both sending and receiving) for certain words that are specified by the child carer. When found, the word should be masked by CyberPatrol. We have not found a list of objectionable words provided by CyberPatrol. The child carer has to enter all the words. When we tested the filtering without adding words ourselves, we noted that nothing was filtered.

It is also possible to block websites that provide instant messaging services.

Chat IRC filtering

CyberPatrol provides the option to block an IRC chat application or restrict the use of it in time, by adding it to the blocked programs list.

CyberPatrol also provides the option to check all IRC chat messages (both sending and receiving) for certain words that are specified by the child carer (the ChatGarded wordlist). When found, the word should be masked by CyberPatrol. We have not found a list of objectionable words provided by CyberPatrol. The child carer has to enter all the words. When we tested the filtering without adding words ourselves, we noted that nothing was filtered.

Email filtering

CyberPatrol does not provide specific email policies. However, it is possible to block email client applications or restrict the use of them in time, by adding them to the blocked programs list.

Newsgroup filtering

CyberPatrol provides the option to block newsgroups with objectionable content based upon several content categories. When enabled, the user cannot make connection to the newsgroup.

However, messages with objectionable content that were downloaded in accessible newsgroups have not been filtered by CyberPatrol.

File Transfer (FTP) filtering

CyberPatrol does not provide specific FTP policies. However, it is possible to block FTP applications or restrict the use of them in time, by adding them to the blocked programs list.

Voice over IP, streaming media, peer-to-peer blocking

CyberPatrol does not provide filtering or blocking for VoIP, streaming media and peer-to-peer. However, these applications can be added to a list of blocked programs, so they cannot be loaded.

It is also possible to add the peer-to-peer application to the list of ChatGarded programs (see Chat IRC filtering). When trying to look for files that contain words from the ChatGarded wordlist, the words are replaced by ";" in the 'search field', so the searches do not work.

4. Performance

Based on the values observed during our tests, we determined that the impact on memory consumption and CPU usage for the tool CyberPatrol was low.

Based on the HTTP loading tests for this tool, it scored a 4, meaning that there was a very low impact in terms of delays and therefore was almost not noticeable.

5. Transparency

When logging in, the user is not notified of the logging, monitoring and filtering activities of the product.

The child carer can choose between several blocking styles, going from child-friendly (with cartoons) to more serious styles and even stealth (no blocking warning is shown, only a standard message that "the page cannot be displayed". Except from the last style, all others provide the current user profile, the reason for the blocking and the content category. The blocking can also be overruled by providing the child carer's password.

Logging is available per user and can be done for all web pages or only the blocked ones. The activities are only logged for the past 14 days.

The monitoring report shows a summary of monitored activity for the past 7 days. It contains the number of blocked web pages, the number of overridden web pages, the total of all visited web pages and the browsing time per user. When going into detail, it is possible to view the same summary by day (for the past 14 days) or to see the full activity log.

The activity log contains date and time of the event, if the event was blocked or not, the URL of the website, the category and the reason why the website was blocked (inappropriate website, inappropriate content ...)

6. Security Integrity

Network tests

The network security tests performed did not identify security issues caused by the tool.

Local tests

The local security tests performed did not identify significant security issues.

7. Legal Compliance

The vendor displays on its website simple, user-friendly information about the product and its functionalities. It is positive that the solution is described in short but also in longer texts (by clicking through relevant hyperlinks). A good number of other means provide illustrative information about the product, being: screenshots, user guides, testimonials and product demonstration. The vendor completes all this information with more generic educational material about organisations on child protection or practical tips to parents and case-studies.

Before subscription (obligatory in order to download the solution), users are guided to approve the Software License Agreement and the terms of subscription, which are in fact the commercial terms and conditions). The information provided in terms and conditions does not raise serious legal concerns. For instance, the vendor's liability is limited throughout the warranty period (30 days) and the vendor can be held liable for replacing/repairing the defective software after the user's appropriate notice. It is less obvious, however, that the law applicable to the transaction is stated to be the Californian, US law or the UK law alternatively (if Californian law cannot be accepted in a given jurisdiction).

On the contrary, more concerns arise from the privacy statement. The vendor states explicitly that any information disclosed by users upon the vendor's explicit request (e.g. filling in a pre-requested registration form) are collected and stored by the vendor. It is the same with any data that users communicate while interacting with the vendor. Users' data may be shared with

business partners or the vendor's entities in other countries, whilst no guarantees are given regarding processing by third parties. No further explanation is given regarding the processing modalities (who processes, period of storage, etc.).