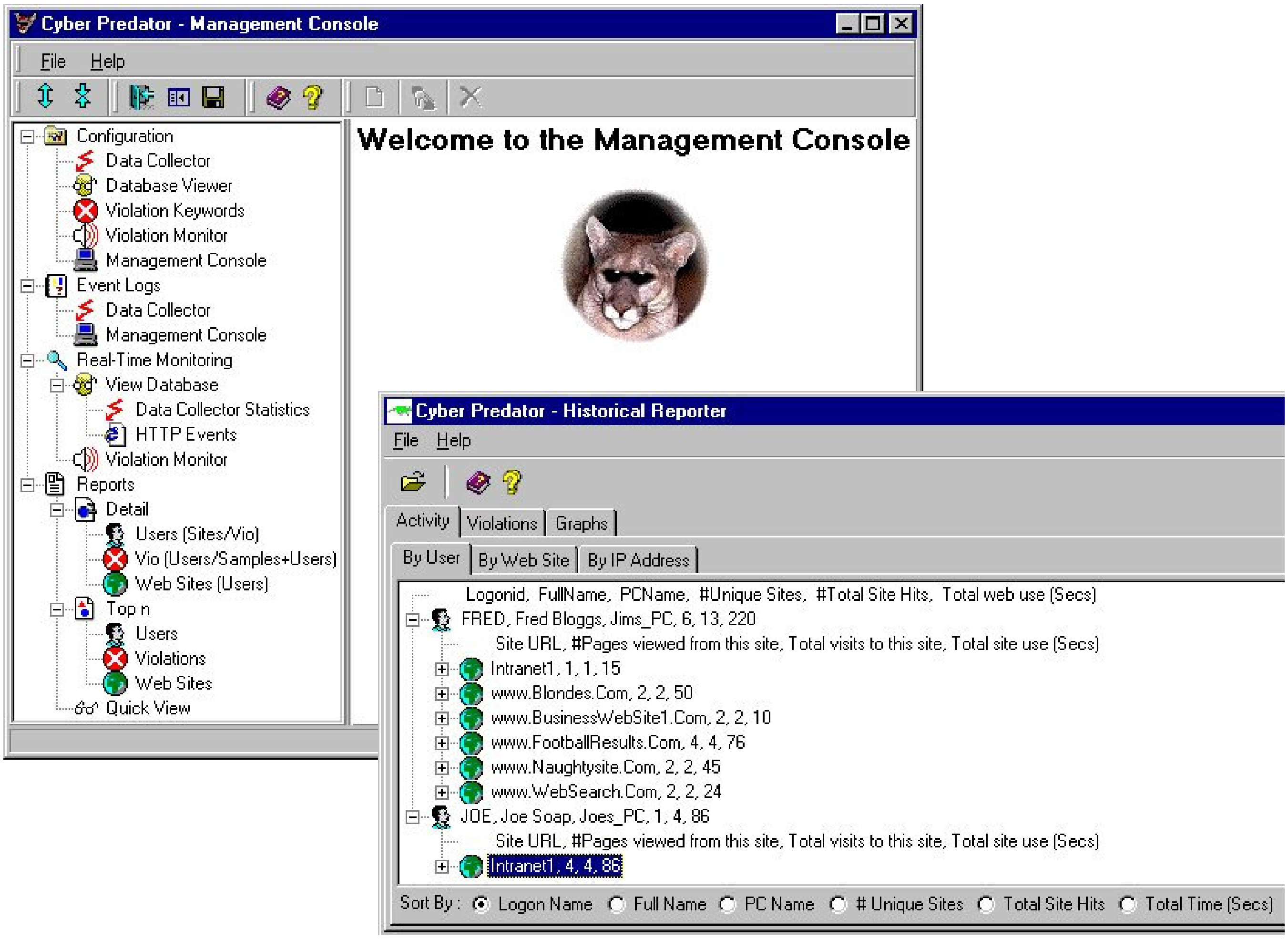
Cyber Predator Internet and Email Activity Monitoring

Cyber Predator is an Internet/network security and activity monitor. In real-time it detects all internet, intranet and extranet traffic to and from a client's browser and scans for keywords in the content. In real time it will then alert a manager/administrator of the activity, so the appropriate action can be taken. But that's not all; it also logs browser activity, so you can see what your traffic patterns are, who visited what site and when. This product not only identifies the client IP address, but (if they are using Microsoft Windows™ and Microsoft Networking) it will tell you the PC Name, and the user logged onto that PC at the time, Logon name and Full Name.

It also has several pages of tree-views (like Explorer) so you can drill down into users to see what sites they visited and what pages they viewed and how long they were looking at each page. You can look at sites, and see what users visited them, and you can look at PC's to see what sites they have visited and what pages they viewed. You also can see the violation words and associated users.



```
Logonid, FullName, PCName, #Unique Sites, #Total Site Hits, Total web use (Secs)
FRED, Fred Bloggs, Jims_PC, 6, 13, 220
    Site URL, #Pages viewed from this site, Total visits to this site, Total site use (Secs)
    Intranet1, 1, 1, 15
    www.Blondes.Com, 2, 2, 50
    www.BusinessWebSite1.Com, 2, 2, 10
    www.FootballResults.Com, 4, 4, 76
    www.Naughtysite.Com, 2, 2, 45
    www.WebSearch.Com, 2, 2, 24
JOE, Joe Soap, Joes_PC, 1, 4, 86
    Site URL, #Pages viewed from this site, Total visits to this site, Total site use (Secs)
    Intranet1, 4, 4, 86
```

Sort By : ● Logon Name ○ Full Name ○ PC Name ○ # Unique Sites ○ Total Site Hits ○ Total Time (Secs)

Why is Cyber Predator so good?

Most security and monitor tools around at the moment get their information from proxy server log files, and whilst the products themselves may be very good, this method of working has several failings:

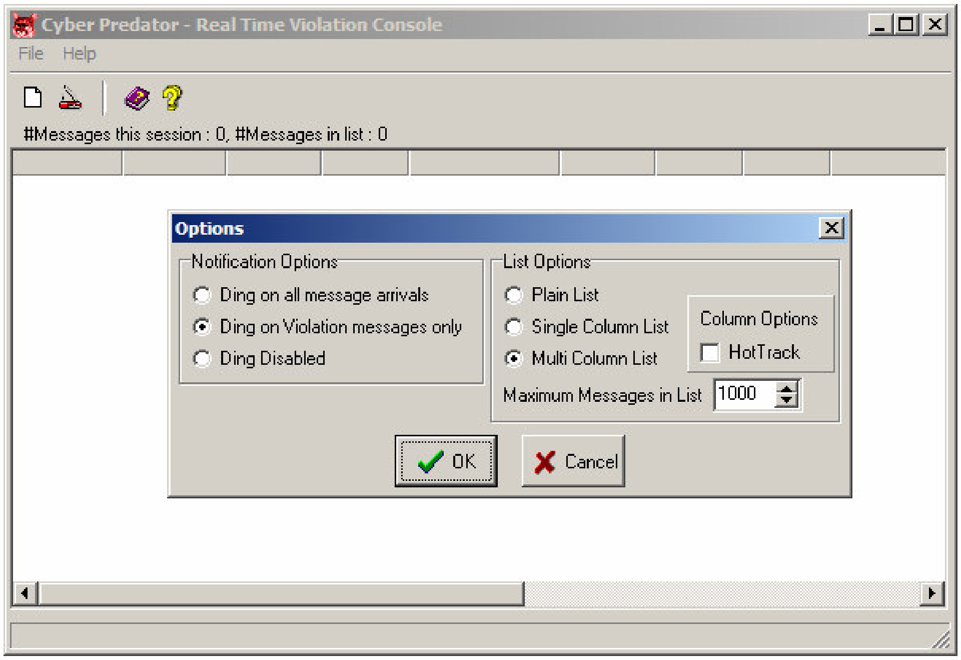
- Proxy servers normally only provide the logon ID (Cyber Predator will give you the users FullName, ideal for colleges/universities where users have non obvious logon IDs).
- It will tell you how many seconds each page was viewed by each user.
- The information is historical (Cyber Predator works in real-time).
- Proxy servers cost money (Cyber Predator doesn't need a proxy server to perform its function).
- Proxy servers log the URL's that people type into the address box in their browsers, if this doesn't contain violation words then the trick is missed (Cyber Predator actually detects all of the data on the network, to and from the browser, thereby allowing it to pick up any occurrence of a violation word in any part of the data, not just the URL).
- Proxy Servers only log traffic going through them, which in the main does not include intranet traffic. (Cyber Predator monitors all browser traffic on your network).
- There is NO client software to install on any or every PC, just install Cyber Predator onto any current platform and that's it.

Some other security tools actually block sites so the user can't see them at all, a good idea, but:

- Most of them block the whole site, so the 99% of useful information on that site is also blocked.
- Most of them require continuous updating, adding URLs of violation sites, this takes time, of course you can buy into an updating service, but that costs money too.
- They sit in the data stream slowing it down - Cyber Predator listens unobtrusively to the data, therefore does not slow it down.

So, you can spend time and or money on a continuous basis, to be one step behind your monitored users! Why, when you can have Cyber Predator, a zero admin, one time purchase, real-time activity monitoring system which will alert you of the violation content of a site before it's even displayed on your users screen!

Cyber Predator doesn't have to be deployed onto each and every workstation, installation takes a few minutes, and you're up and running.



#Messages this session : 0, #Messages in list : 0

Notification Options

○ Ding on all message arrivals
● Ding on Violation messages only
○ Ding Disabled

List Options

○ Plain List
○ Single Column List
● Multi Column List

Column Options

□ HotTrack

Maximum Messages in List 1000

What will it do for you?

It gives you peace of mind, if you're console isn't making noises then you know people aren't visiting the sites containing those violation words.

It also protects you from the legal point of view too:

- Visitors to a lot of web sites are monitored; this at the very least exposes you to that web site, what happens to that information? It wouldn't be very nice to see that employees from your company for example are the most frequent visitors to a certain kind of web site.
- Harassment, imagine the cost and hassle of court proceedings, because one employee has something displayed on their PC that offends another employee.
- Increase your company's bottom line! At the end of the day, companies employ people to work, and ultimately they contribute to the profit of the company. If they are not working, they are losing you money! Not only one person either, when people find something interesting on the web, they quite often tell their friends, so that means even more time is wasted whilst they discuss it.
- Increase your company's bottom line; one assumes you pay for your connection to the internet? So then this extra non business traffic is costing you real money too, and slowing down the link for the rest of the users.
- Increase your company's bottom line; if a user spends only 10 minutes a day, looking at non business related material on the web, this has cost you the equivalent of more than a week's salary (based on 220 working days per year and a 36 hour working week). But the really bad thing is if they tell 3 friends, you could be losing a month per year of man power?
- Some magazines quote 90 minutes per day of non-business surfing! That's 9 weeks per year not working per user.

Why do you need it?

If all your employees are completely trust worthy, work hard and don't waste time on non business activities, then you may not need Cyber Predator. One also assumes that, as you have a workforce of angels, then you don't lock the petty cash tin, expenses aren't checked, every employee can sign the company cheque book etc. We don't really mean to be sarcastic, but how do you know they aren't abusing this resource, if you don't keep an eye on it?

What dependencies does it have?

- The main monitor program runs as a service on a PC running Microsoft Windows NT, Windows 2000, Windows 2003 and XP.
- 256Mb RAM Memory, 1Gb free hard disk space and an Ethernet card that supports promiscuous mode (Most Ethernet cards do).
- An Ethernet network (LAN) that connects all your PCs together.
- Some users to monitor.

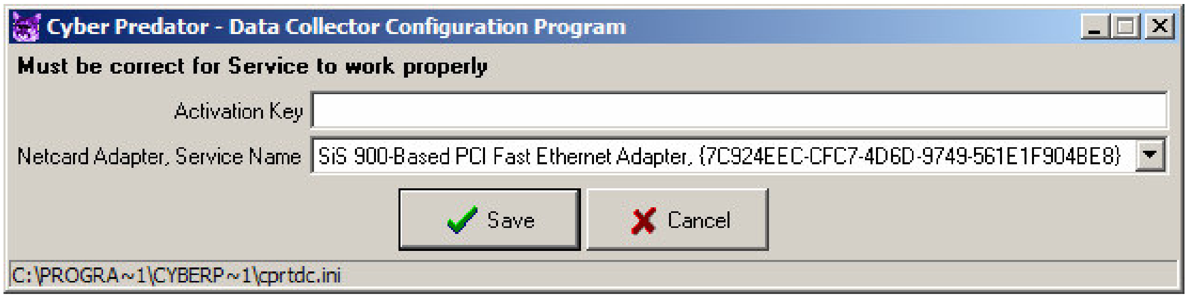
I don't even have to be running Microsoft Windows™ on the users PCs - as long as they access the internet/intranet/extranet using TCP/IP across your local LAN, you can monitor them.

What programs do I get with Cyber Predator?

The Cyber Predator suite consists of:

- The **Real-time Data Collector** (running on Windows NT, 2000, 2003 or XP this scans the network, monitoring and logging activity).
- The **Management Console** a fully integrated control centre, it deals with configuration, reports and all the real-time monitoring capabilities. It includes a built in **Real-Time Violation Monitor**, which collects the messages generated by the Real-Time Data Collector. This is normally run on an administrator or manager's PC.
- The **Setup Program**, this is where the initial Data Collector configuration is done, the fine tuning is carried out in the Management Console.

All these applications can be run on the same machine, as would probably be the case for a small network, or each one can run on a different machine, as would probably be the case in larger networks.



Cyber Predator - Data Collector Configuration Program

Must be correct for Service to work properly

Activation Key

Netcard Adapter, Service Name SiS 900-Based PCI Fast Ethernet Adapter, {7C924EEC-CFC7-4D6D-9749-561E1F904BE8}

C:\PROGRA~1\CYBERP~1\cprtdc.ini

Is it easy to configure?

Yes, all configuration is done from the user's workstation, you answer a few questions, tune the keyword list to suit your requirements, and sit back.

The keyword list can contain any words you wish, e.g. Football, Soccer, any browser activity containing the words Football or Soccer would be reported. You can modify this list whenever you wish.