Security Task Manager

for Windows XP, 2000, NT, ME, 98

Provides advanced information about programs and processes

content

Features of Security Task Manager

Security Task Manager provides advanced information about programs and processes running on the computer. For each process it shows in addition in contrast with Windows Task-Manger:

- file name and directory path
- security risk rating
- description, start time, program icon, process type
- CPU usage graph
- contained hidden functions
  (keyboard monitoring, Browser supervision, manipulation)

SpyProtector can eliminate your Internet traces, warn when registry is changed and disable keyboard and mouse surveillance on your computer.

Using Security Task Manager

Security Task Manager shows all active processes on your computer. The Rating tells you all security relevant functions which a process contains.

The listed processes can be sorted by following properties. Click on **View** menu to chose, which properties are shown as column.

- Name
  Shows name of software or name of driver.
- Rating
  Shows the objective and security relevant process Rating. The longer the red Rating bar, the more dangerous functions the process contains. Highly rated programs do not always have to be dangerous: They just have some typical spyware properties. Click a process to learn more about it. Then you can assess trustworthiness of this software.
- CPU
  Shows CPU (processor) usage. Active program do keep the processor more occupied than inactive processes.
- Memory
  Shows working memory usage.
- File
  Shows directory path and name of the file.
- Type
  Shows file type. The file type can be a program, a system tray icon program, a Browser Helper Object, a driver or a service.
- Title and Description
  Shows Title and file description contained in the file. For a visible window the title corresponds to the text in the windows's title bar.
- Manufacturer and Product
  Shows name of manufacturer and product description found in the file.

Click a process to obtain more information about this processor to stop it. You can:

- see properties
- end process
- place process in quarantine

Note

- Click **Windows processes** button to see also all Windows internal processes. These processes belong to Windows operation system. Windows system processes are not shown by default.
- A process can be a program, driver, service or PlugIn - so every executed code which is active in your computers memory.

Process types

Security Task Manager distinguishes the following kinds of processes. Click **Type** on **View** menu, to see or hide the type as column in the main window.

Software

- Program

Labels a program with a visible window or a unvisible program without a window.

- Taskbar icon

This is a program with an icon in system tray (left beside the watch). Right-mouse click this icon on task bar to open a context menu and to get more information.

DLL files

- DLL
  A Dynamic Link Library (DLL) executes program code just like a program. A DLL file contains seldom used function outsourced by main program.
- SheelExecute
  This file was started by a Hook using the ShellExecute commend in the Windows registry. ShellExecute runs a process (almost a DLL) when any Windows program was started. This process should be examined exactly.

Internet PlugIns

Browser Helpers Objects
A Browser Helper Object (BHO) is a DLL that allows developers to customize and control Internet Explorer. Alexa, GetRight, Go!Zilla and other download manager uses a BHO. BHO's can monitor all your Internet activities. To deactivate BHO's, click in Internet Explorer on **Extras** menu **Internet Options**. Click **Advanced** tab. Under Browsing, click to clear the **Enable third-party browser extensions** check box.

Driver and Services

Driver and Services execute system functions at lower hardware level. (available only in full version)

device driver
A service type flag that indicates a Windows NT device driver to control hardware components (e.g. graphic adapter or scanner). Some software modules (e.g. Firewall, AntiVirus) are device driver therewith users cannot close it.

file driver
A service type flag that indicates a Windows NT file system driver.

Service (own process)
A service type flag that indicates a Win32 service that runs in its own process. A Win32 service starts automatically on Windows start, is always running and doesn't depend on users.

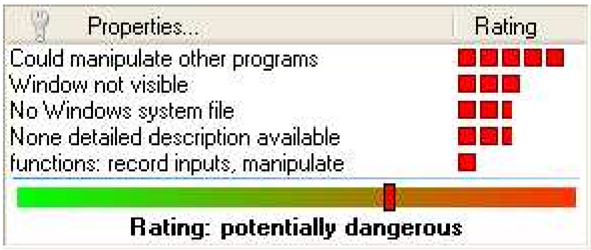
Service (own process with desktop interaction)
A service type flag that indicates a Win32 service (e.g. Firewall, AntiVirus) that runs in its own process and can interact with the desktop. A Win32 service starts automatically on Windows start, is always running and doesn't depend on users.

Service (shares process)
A service type flag that indicates a Win32 service that shares a process with other services. A Win32 service starts automatically on Windows start, is always running and doesn't depend on users.

Service (shares process with desktop interaction)
A service type flag that indicates a Win32 service that shares a process with other services and can interact with the desktop. A Win32 service starts automatically on Windows start, is always running and doesn't depend on users.

Risk Rating of processes

Security Task Manager judges the safety relevant risk of a process after objective criteria. To this Security Task Manager examines if a process contains critical function calls or suspicious properties. Depending on potential dangerousness of these functions and properties points are allocated. The sum results in the Security Task Manager Risk Rating (0 to maximum 100 points).



Properties...	Rating
Could manipulate other programs	🟥🟥🟥🟥🟥
Window not visible	🟥🟥🟥
No Windows system file	🟥🟥🟥
None detailed description available	🟥🟥🟥
functions: record inputs, manipulate	🟥

Rating: potentially dangerous

Security Task Manager examines the processes after the following functionalities (sorting by dangerousness):

- Able to record keyboard inputs
  The process monitors each keyboard input. This is realize by a Hook function. Serious programs don't use this Hook function.
- File is hidden
  The file hides from the Windows Explorer. Please not mistake for the harmless file attribute "hidden".
- Keyboard driver, could record inputs
  It is a keyboard driver and can read every keyboard input you make.
- Could manipulate other programs
  The process can manipulate any programs or Windows operation system. A Hook is set for this one. A Hook is a Windows internal function that can feign a forged file list for example. This manipulates the dir command. Thus the program (that starts the process) is not visible for other programs like AntiVirus software.
- Able to monitor Internet browser
  A Browser Helper Object (BHO) is a DLL that allows developers to customize and control Internet Explorer. Alexa, GetRight, Go!Zilla and other download manager uses a BHO. BHO's can monitor all your Internet activities. To deactivate BHO's, click in Internet Explorer on **Extras** menu **Internet Options**. Click **Advanced** tab. Under Browsing, click to clear the **Enable third-party browser extensions** check box.
- Starts when starting of programs
  This file was started by a Hook using the ShellExecute commend in the Windows registry. ShellExecute runs a process (almost a DLL) when any Windows program was started. This process should be examined exactly.
- Listen on port <*No.*>
  The process can receive information from the Internet. Hackers use such leaks to take control over such computer. You can prevent such attacks with a good firewall.
- Send to <*computer name*> on port <*No.*>
  The process connects to the named computer or IP address and can send any information to this. You can prevent such connections with a good firewall.
- unknown program listens or sends
  A port was opened to receive or send information over network or Internet. Please find out which program it is. You can prevent such connections with a good firewall.
- Monitor program starts
  The process monitors when which programs are started or closed.
- Window not visible
  The program doesn't have any visible window and runs in the background. In the most favorable case, e.g. it is device driver software.

- Start when Windows starts
  The program is started at every Windows start because it wrotes a autostart key in the registry.
- None detailed description available
  Some important standard descriptions in the file were not found. Every file contains internally fields for descriptions by default.
- No Windows system file
  The file is not part of the Windows operating system. Windows system files are checked and protected specially by Windows.
- No description of the program
  Descriptions were not found in the file. Every file contains internally fields for descriptions by default.
- functions: Internet, monitor, record inputs, hide, manipulate
  The file contains function calls with the named properties. But this hasn't much influence on the Rating, since there is no evidence if this function comes in action.
- functions: not determinable
  No dangerous function calls were found in the file. But these could be integrated hiddenly.
- Unknown manufacturer
  The software manufacturer cannot be found in file description fields. Every file contains internally fields by default to name the software developer.

Trusted properties (reduces risk):

- Microsoft signed file
  This file was signed by Microsoft. You can trust this file like you also trust Microsoft.
- Verisign signed file
  This file was signed by VeriSign. You can trust this file like you also trust VeriSign.
- Certificated by *<registrar>* for company *<manufacturer>*
  This file was signed by a registrar. You can trust this file like you also trust this registrar and the software manufacturer.
- Own comment
  You can wrote an own comment in order to influence the risk rating.

Note

- Highly rated programs do not always have to be dangerous: They just have some typical spyware properties.
- Click **Windows processes** button to see also all Windows internal processes. These processes belong to Windows operation system. Windows system processes are not shown by default.

Viewing process details

Click on a process to see more information about this process. Follwing properties are shown:

- Name
  Shows name of software or name of driver.
- Rating
  Shows the objective and security relevant process Rating. The longer the red Rating bar, the more dangerous functions the process contains. Highly rated programs do not always have to be dangerous: They just have some typical spyware properties. Click a process to learn more about it. Then you can assess trustworthiness of this software.
- File
  Shows directory path and name of the file.
- Type
  Shows file type. The file type can be a program, a system tray icon program, a Browser Helper Object, a driver or a service.
- Title and Description
  Shows Title and file description contained in the file. For a visible window the title corresponds to the text in the windows's title bar.
- Manufacturer and Product
  Shows name of manufacturer and product description found in the file.

Note

- Click **Windows processes** button to see also all Windows internal processes. These processes belong to Windows operation system. Windows system processes are not shown by default.
- Click on **View** menu to chose which properties are shown as column in the main window.

Learning more about a process

1 Click on a process you want to examine.

2 Click **Google** button on tool bar.

An information web page is displayed on www.neuber.com/taskmanager where you can write your opinion about this software/driver software or read other user comments. You can search for further information about this process at Google.com from this web page.

Note

- Your Internet Browser transmits information (e.g. operating system, language setting). Neither the program Security Task Manager nor one of his components make a connection to the Internet.
- Google.com is one oft the most used search engines provides you with good results.

Ending a process

1 Click on a process you want to close.

2 Click the button ✖ **Remove**.

3 Then select one of following options:

- End process
  The process will be removed from the memory. If the process wrote a own autostart entry in the Registry (Windows configuration data base), then it is however active again at the next Windows start.
- Move file to quarantine
  The process will be removed from the memory too. In additional Security Task Manager put the corresponding file into quarantine folder and deletes corresponding Autostart entries in Registry. File and registry entries are saved. Thus you can restore the process at any time.

Note

- Ending a process can cause system instability, including crashes. Software that needed Adware programs could not work. Please save opened documents.

Using quarantine folder

The quarantine folder works like the windows recycle bin (trash). When you put a file into quarantine folder , the file is renamed and moved to a isolated folder. Corresponding Autostart keys in Windows registry are deleted. Thus the process cannot be started again. Restoring the whole process is possible at any time:

Restoring processes

1 Click **quarantine** button on tool bar.

2 In quarantine folder click on process you want to restore.

3 Click **Restore** button.

Exporting process list

1 On File menu click **Export to**.

2 Chose a file type:

- Text file (*.txt)
- Website (*.html)

Printing process list

1 On File menu click **Print**.

2 Chose a printer and perhaps necessary properties (e.g. duplex print).

Note

- Click **Windows processes** button to see also all Windows internal processes. Then you be able to save or print Windows processes too. Windows system processes are not shown by default.
- Please save process list from time to time. Thus you can find new processes. A saved process list can serve as exhibit.

Writing a comment

You can write a own remark to each process. This is visible in the process properties. You can vote the process to change the Security Task Manager Rating.

To write a comment

1 Right mouse click a process you want.

2 Click **Comment...** on appearing context menu.

3 Enter you comment and your opinion about the process.

Protecting your computer with SpyProtector

To run SpyProtector, click icon in the system tray of your task bar.

SpyProtector contains following tools to protect your computer from keylogger, spyware and trojans:

Delete history
Check this option to eliminate the traces of Internet activities (cookies, cache, history, typed URLs) in InternetExplorer. You can furthermore delete the recent used file list of programs (e.g. Word, ACDSee, PDF, WinZip, Mediaplayer) and the recent used program list of Windows Start menu.

Disable keyboard monitoring
Check this option to block most of keyloggers for the current Windows session. The redirection of all keyboard inputs over an keylogger is blocked. Such a keyboard redirection is realized by programing a Hook function. Even keyboard utilities like macro and autotext programs don't use such dirty Hooks.

Disable other monitoring
Check on of these options to block programs that log following data for the current Windows session:

Keyboard inputs (indirect)
This prevents monitoring of internal Windows messages (e.g. keyboard inputs) by other programs.

Mouse activities
This prevents monitoring of mouse movements and mouse clicks

Macro
This prevents recording of user activities. That methode often used by macro programs is not usual for keyloggers.

Starting and ending of programs
Program starts and ends are logged. This function is frequently used by tutorial programs (CBT) to the interaction with the software to be learned.

Attention: Some serious programs (e.g. some Macro programs) use these "dirty" Hook functions. If such a program shouldn't work any more, then activate the corresponding option or restart your computer.

Warning when registry is changed
Check this option to get a messagebox if a program tries to wrote its name on the Windows registry as autostart key. The software is started with such an key secretly at every Windows start. All dangerous programs need such an key to be active at a computer restart!

Changing the language

Security Task Manager recognizes the used language Sprache (English, Deutsch, ...) automatically. To change the language make the following:

1. On **View** menu click Language ▶
2. Then click the language you want.

Note

- The software can be easily translated to any language. Simply translate the lgs_english.txt text file in the program's folder and send it to info@neuber.com. You will receive a free registration for your translation.

Adding a language file

You can download additional language files at www.neuber.com/taskmanager.

1 Go to www.neuber.com/taskmanager.

2 Here you can see all available languages.

3 Copy the lastest version in the Security Task Manager directory. for exapmle c:\program files\Security Task Manager

4 Change the language and then run Security Task Manager.

Note

- The German and English language files lgs_deutsch.txt and lgs_english.txt are contained by default.

Contacting the Security Task Manager Team

Technical Contact:

address: Alexander and Matthias Neuber GbR
PF 11 05 25
D-06019 Halle
Germany
fax: (+49) 0700-11 777 000
Internet:
WWW: www.neuber.com/taskmanager
email: info@neuber.com

The registration is executed by the international registration service ShareIt (Greensburg/U.S.A, Köln/Germany, London/UK, Roissy/France, Upplands Väsby/Sweden).

Uninstalling Security Task Manager

1 Click Start-Settings-Control panel.

2 Click **Software**.

3 Click the **Remove** button to delete Security Task Manager from your Computer.

Note

- You can also run uninstal.exe in the Security Task Manager directory

Remarks about the shareware version

Security Task Manager is distributed as shareware. Shareware is a distribution method based on honor, and is not a type of software. You are free to use it for a trial period of up to 30 days. If you find this program useful and would like to continue using Security Task Manager, then you are required to register for $29 (29.EUR). You will receive a registration code that you can use to unlock the shareware. The registration code will turn off all nag screens and shareware limitations, and work with future updates.

As a registered user, you will get:

- legal license for the software
- your personal key to unlock trial version
- free updates for lifetime
- free software SpyProtector
  Spyprotector eliminates your Internet traces, warns when Autostart key in registry is changed and disables keyboard and mouse surveillance
- free technical support (via email or mail)

On **Help** menu click **Info...** to see whether your version is registered.

Switching the shareware to a registered version

1. On **REGISTER** menu click **Unlock the shareware version**.
2. Enter the Name and Code in the registration dialog **exactly** as shown in the information sent to you.
3. Click **Unlock**.