Guardian
Total Security

The ultimate security from all types of cyberattacks
Powerful. Fast. Multilayered.

Malware Protection

Helps you protect your system from threats such as spyware, adware, keyloggers, and riskware at real time whether you are connected to the Internet or working offline.

Behavior-based Detection (DNA Scan)

Continuously monitors the activities performed by an application in your system. If the application deviates from its normal behavior or carries out any suspicious activity, Behavior detection system suspends that application from executing further activities that may cause potential damage to the system.

Anti-Ransomware & Data Backup

Stops ransomware attacks on your computer and protects your data from getting encrypted. Helps you back up your data in a secure location. Data can be restored from this backup in case of a ransomware attack.

Firewall

Firewall shields your system from intruders and hackers by monitoring and filtering incoming and outgoing network traffic. Any suspicious program that may be harmful to your computers or systems is blocked. Firewall protects your computers from malicious programs either from outside internet connection or from within networks incoming into your system.

Safe Banking

With online banking, you can check your accounts, pay bills, buy and sell shares, and transfer money between different accounts. For doing these things, you visit a banking website, enter your identity credentials, and carry out the required transactions. However, while visiting a banking website, you can become a prey to a fake banking website or when you type your credentials, the information can be phished to a fraudster.

Safe Banking shields you from all possible situations where your identity or credentials can be compromised. Safe Banking launches your entire banking session in a secure environment that protects your vital data.

Browsing Protection

When users visit malicious websites, some files may get installed on their systems. These files may spread malware, slow down the system, or corrupt other files. These attacks can cause substantial harm to the system.

Browsing Protection ensures that malicious websites are blocked while the users access the Internet. Once the feature is enabled, any website that is accessed is scanned and blocked if found to be malicious.

Phishing Protection

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. These emails usually appear to have been sent from seemingly well-known organizations and websites such as banks, companies and services seeking your personal information such as credit card number, social security number, account number or password.

Phishing Protection prevents users from accessing phishing and fraudulent websites. As soon as a website is accessed, it is scanned for any phishing behavior. If found so, it is blocked to prevent any phishing attempts.

Data Theft Protection

Allows you to block transfer of data between the system and external devices such as USB drives and CD/DVD devices. Data Theft Protection ensures no files or data can be copied from your system to any external devices or vice versa. It ensures data security and also eliminates the possibility of transfer of any harmful files.

IDS/IPS (Intrusion Detection and Prevention System)

With IDS/IPS, your computer remains secure from unwanted intrusion attempts or attacks by the hackers.

Anti-Trojan

Trojans are malicious software that look like harmless programs to trick users into downloading and installing them on their computer. And once inside, they can be used by attackers to carry out malicious activities like data theft, download additional malware, destroying data, and letting an attacker take control of the computer. Guardian's Anti-Trojan feature blocks such programs from getting inside your computer.

Anti-Spyware

Spyware is a malicious software that secretly monitors unsuspecting users and steals their data. It is used by attackers to obtain sensitive information, such as login ID and passwords, from the infected computer. Spyware is often attached to free online software downloads or to links that are clicked by users. Guardian's Anti-Spyware protects your computer from such data-stealing malware.

Anti-Keylogger

Keyloggers are malicious programs that record all information typed by you on the keyboard of your computer or laptop and share that information with the hackers. You may lose confidential information such as usernames, passwords, or PIN to the hackers. Anti-Keylogger helps you prevent information getting recorded by keystroke logger malware.

Virtual Keyboard

Virtual Keyboard helps you enter the required information without pressing any keys on the physical keyboard. It reduces the risk of getting your information recorded by a possible keystroke logger malware.

Adware Protection

Blocks adware from getting installed on your computer. Adware is a software designed to display ads on your computer. Although not necessarily harmful, adware can expose your computer to threats.

Rogueware Protection

Also known as scareware, rogueware is a program designed to frighten users with fake warnings of virus detection and trick them into purchasing and downloading fake antivirus software. Rogueware can be any types of malware, adware, spyware or a Trojan. Rogueware Protection blocks such malicious software from getting installed on your computer.

USB Drive Protection

Whenever any external drives are connected to your system, the autorun feature starts automatically and all programs in the drive may also start. The autorun malware may also be written in the drives so that it starts as soon as the drive is connected and spreads malware to your system. This feature helps you safeguard your USB devices from autorun malware

On Demand Scan

Guardian Total Security allows you to scan your computer as and when you require. At the same time, you can select to scan only a certain area. This helps you avoid slowing down of your computer while you're working. Also, you can schedule Auto Scanning.

Trusted Email Client Protection

Lets you configure a list of trusted email clients which will be allowed to send emails. Since email happens to be the most widely used medium of communication, it is used as a convenient mode to deliver malware and other threats. Attackers always look for new methods to automatically execute their viral codes using the vulnerabilities of popular email clients. Worms also use their own SMTP engine routine to spread their infection. This feature helps in keeping a check on the proliferation of malware.

Emergency Disk

Create your own emergency bootable Disk that will help you boot your Windows computer system and scan and clean all the drives including NTFS partitions. This disk helps in cleaning badly infected system from the file infecting viruses that cannot be cleaned from inside Windows. The Emergency Disk will be created with the latest virus signature pattern file used by Guardian Total Security on your system.

Sandbox

When you browse the Internet, you are clueless about which sites are trusted and verified. Trusted sites are those that publish their identity so that they are established as known entities. However, all untrusted sites are not fake sites or phishing sites. Untrusted websites may be commercial websites, suppliers, sellers, third parties, advertisements, and entertainment websites.

Malicious sites mask their identity to run a covert operation. These sites can hack your confidential credentials, infect your computer, and spread spam messages.

Browser Sandbox keeps you safe from any kind of malicious attacks. Browser Sandbox applies a strict security policy for all untrusted and unverified websites. If you open any downloaded files with Browser Sandbox turned on, such files open in Browser Sandbox to isolate any possible infection.

Hijack Restore

If you have modified the default settings of Internet Explorer or if the settings have been modified by any malware, spyware, and sometimes genuine applications, you can restore the default settings.

Hijack Restore helps you restore the settings of Internet Explorer browser, and also of critical operating system settings such as Registry Editor and Task Manager.

Track Cleaner

Most of the programs store the list of recently opened files in their internal format to help you open them again for quick access. However, if a system is used by more than one user, the user's privacy may be compromised. Track Cleaner helps you remove all the tracks of such most recently used (MRU) programs and prevent privacy breach.

System Explorer

This tool provides you all the important information related to your computer such as running process, installed BHOs, toolbars installed in Internet Explorer, installed ActiveX, Hosts, LSPs, Startup Programs, Internet Explorer settings and Active network connection. This helps you diagnose the system for any new malware or riskware.

Windows Spy

Helps you find more information about an application or process. Sometimes we keep getting dialog boxes or messages that are actually shown by spyware or some malware that we are unable to locate. In such a case, this tool can be used to find out more information about the application by dragging the target on to the dialog or window that appears on the screen. This tool will provide following information about the dialog or a window.

- Application Path
- Application Name
- Original File Name
- Company Name
- File Description
- File Version
- Internal Name
- Product Name
- Product Version
- Copyrights Information
- Comments

Self-Protection

This feature helps you protect Guardian Total Security so that its files, folders, configurations and registry entries configured against malware are not altered or tampered in any way. It also protects the processes and services of Guardian Total Security. It is recommended that you always keep Self-Protection on.

Guardian
Total Security

Password Protection

Allows you to restrict unauthorized people from modifying the Guardian Total Security settings so that your security is not compromised. It is recommended that you always keep Password Protection turned on.

Silent Mode

Mutes prompts and notifications from Guardian Total Security. This does not affect the security level of your system.

Automatic Update (Internet)

Helps you take automatic updates of latest virus signatures. This protects your system from the latest malware. To take the updates regularly, it is recommended that you always keep Automatic Update turned on.

Offline Update (Through LAN)

If your computer is not connected to the Internet and you want to update your antivirus on one or more PC, you can use the offline updater in Automatic Update.

System Requirements for Guardian Total Security

General requirements

- Internet Explorer 6 or later
- Internet connection to receive updates
- Free disk space 750 MB

System requirements for various Microsoft Windows OS

Windows 10
Processor: 1 gigahertz (GHz) or faster
RAM: 256 MB

Windows 8.1 / Windows 8
Processor: 1 GHz or faster
RAM: 256 MB

Windows 7
Processor: 1 GHz or faster
RAM: 256 MB

Windows Vista
Processor: 1 GHz or faster
RAM: 256 MB

Windows XP
(Service Pack 2 and later)
Processor: 300 Megahertz (MHz) Pentium or faster
RAM: 256 MB

Windows 2000
(Service Pack 4)
Processor: 300 MHz Pentium or faster
RAM: 256 MB

Guardian antivirus
(A division of Quick Heal Technologies Ltd.)
Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India
Customer Service Telephone Support : +91-8669667399 | E-mail: support@guardianav.co.in