Features List

Ransomware Protection

Quick Heal anti-ransomware feature is more effective and advanced than other anti-ransomware tools.

- **Signature based detection**

  Detects known ransomware that try to infiltrate your system through infected emails and other mediums like USB drives or other infected systems in the network.

- **Proactively monitors the system for new ransomware infections**

  Monitors activity of downloaded files whose components could become a potential ransomware attack.

- **Runs on a behavior-based detection engine**

  Analyzes how a program behaves in real time, so that it can be stopped before it does any damage.

- **Has an inbuilt data backup and restore tool**

  The backup and restore tool proactively keeps a backup of all your important files and stores it in a secure location. These files can be restored in case of a ransomware attack. Read more about this here - http://bit.ly/2f6M9nd

Web Security

Attackers can compromise certain websites with hidden malicious codes that can infect your system without your knowledge. They can also create fake websites to trick you into giving away your personal or financial information. Web Security automatically detects such unsafe and potentially dangerous websites, and prevents you from visiting them.

Email Security

Using social engineering techniques, hackers can send you emails with infected attachments or links to compromised or fake and phishing websites. Email Security filters all incoming emails marked to you, blocks those that are harmful, and lets through only clean and genuine emails.

Safe Banking

Protects your online banking activities from fraudulent websites and malicious programs that steal financial information. It provides a safe desktop session where your financial transactions on banking portals, shopping and other e-commerce websites stay private and hidden from hackers.

Safe Banking can be easily used by clicking its shortcut on your desktop. You will be taken to a private window where you can shop and bank with complete security.

Browser Sandbox

Runs your Internet browsers in a secure, virtual environment that acts like a shield between your PC's operating system and malicious downloads. If any malicious file gets downloaded in this environment, it gets secluded and is blocked from reaching your real PC. Browser Sandbox is an important security technique that isolates malicious websites from your computer and its data.

Data Theft Protection

Having confidential and sensitive information on your computer may put your privacy at stake. Unauthorized users can steal such data using USB flash drives. With Data Theft Protection, you can easily block unauthorized copying of data from your computer to any unauthorized USB drives. This not only ensures data security but also reduces the risk of transfer of any harmful files.

Parental Control

Uncontrolled or unmonitored Internet usage can not only affect the academic career of children but also make them susceptible to coming in contact with potentially dangerous people. Parental Control helps parents empower their children while ensuring their safety online. This feature is now enhanced and allows parents to set the following settings

- **Internet Browsing Control** - to restrict children from visiting unwanted websites or inappropriate websites. Parents can block websites by their category (adult, game, chat, violence, crime, illegal downloads, etc.) or by directly blacklisting their URLs. A fixed timetable can also be set based on which children can have Internet access on certain days and timings.
- **Application Control** - to restrict children from accessing applications such as gaming programs, messaging tools, media players, etc., on their PC.
- **PC Access Control** - to fix a timetable based on which, children can access their computer on particular days and time.

Firewall

Firewall blocks external threats that try to reach your computer over the Internet. It also blocks threats that may arise within networks that are connected to your system. Besides allowing you to configure protection for incoming and outgoing Internet traffic, our enhanced Firewall lets you set a Firewall profile for network connections such as 'Home', 'Work', 'Public' or 'Restricted'. Stealth Mode is an added benefit. It hides your PC from the prying eyes of hackers.

- **Firewall**
  Blocks external threats that try to reach your system using the Internet. Firewall remains active in the background, and constantly detects and prevents malicious agents from infiltrating your machine.

Core Protection

Quick Heal's Core Protection is a multilayered defense mechanism made up of antivirus, antispyware, antimalware, anti-rootkit, firewall, and IDS/IPS that work together to offer the best Internet security.

- **Antivirus**
  Scans and removes viruses, worms, Trojans, and other threats that may get into your system via infected removal drives, file downloads, email attachments, compromised websites, etc.
- **Antispyware**
  Detects and blocks malware such as spyware that can record and steal your personal information and share it with hackers.
- **Antimalware**
  Rapidly scans multiple areas of your computer and removes hidden malicious and potentially dangerous programs.
- **Anti-rootkit**
  Rootkits are programs that can gain unauthorized entry into your machine and hide their presence or the presence of other malicious software. Anti-rootkit detects and blocks such programs.

Malware Protection

The existing Malware Protection of Quick Heal is now enhanced and offers more protection to your PC against spyware, adware, keyloggers, riskware, and other malicious programs. With this defense in place, your PC gets round-the-clock protection from all types of dangerous surprises on the Internet.

Anti-Keylogger

Keyloggers belong to a family of data-stealing malware called spyware. They record what you type on your keyboard while you are banking or shopping online or simply browsing the Internet. Having such malicious programs in your computer puts all your personal and financial data at the disposal of hackers and online scammers. Quick Heal Anti-Keylogger protects your information from such programs.

Improved Scan Engine

Our Scan Engine knows which files and folders have changed and not changed since the last time they were scanned for threats. Files that are found to be unchanged are not rescanned. This results in faster scans and better detections, without using too much system resources.

Advanced DNAScan

Quick Heal DNAScan technology detects and blocks unknown threats. It uses a combination of behavioral and characteristic inspection and

monitoring of unsafe programs. The feature allows users to select from three levels of detection.

- After detecting any suspicious behavior, the Behavior Detection System suspends further activities of the application and presents the user with Allow and Block options.
- If the application is blocked, the application is terminated and its executable is quarantined.
- Behavior Detection System's options can be configured from Files & Folders - Advanced DNAScan.
- There are three defined levels of Behavior Detection System that the user can select from. These are as follows:
  - **High**: the system closely monitors the behavior of a running application and issues an alert if any unusual application behavior is noticed.
  - **Moderate**: the system issues an alert if any suspicious activity of a running application is noticed.
  - **Low**: the system issues an alert only if any malicious activity of a running application is noticed

Vulnerability Scan

The Operating System (OS) settings and other applications in your system might have security vulnerabilities or weaknesses. Leaving these vulnerabilities unpatched can let hackers hijack your computer and your data. Vulnerability Scan helps you detect such weaknesses. The feature also helps you fix vulnerabilities found in the OS settings.

Virtual Keyboard

Attackers can steal your confidential information by installing spyware or keyloggers in your machine. These are data-stealing software that record what you type on your keyboard, and send the information to the attacker. This can be prevented by using the Virtual Keyboard. Any information typed on this keyboard gets encrypted and cannot be recorded or accessed by any malicious software.

Privacy Protection

Protecting your data and privacy is not only about storing or saving data properly. It also advocates the importance of disposing of your information securely. Data that you delete from your computer does not really get deleted permanently. It can still be recovered by using data recovery tools. So, it is important to remove sensitive information permanently. Privacy Protection provides an easy way to delete any data from your system permanently, so that it becomes impossible for any recovery tool to retrieve the deleted data.

Flash Drive Protection

Ensures your PC's safety against infected USB drives. Flash Drive Protection automatically scans external drives the moment they are connected to your PC. It also blocks autorun viruses that can execute on their own and can infect your computer the moment you open an infected flash drive.

Safe Mode Protection

This facility stops unauthorized users from changing Quick Heal security settings when the system is running on Safe Mode.

Enhanced Self-Protection

Protects Quick Heal's running processes and services.

Silent Mode

Mutes all prompts and notifications from Quick Heal so that you can use your PC without getting interrupted. Putting Silent Mode ON does not affect the security level of your system.

Import and Export Settings

You can export Quick Heal security settings from a single computer and import it to other computers. This is helpful in cases where reinstallations or multiple computer configurations are concerned.

Quick Heal Remote Device Management (RDM)

This is a free portal where you can add your Quick Heal enabled device, view its current status, and get notified of any critical situation such as malware infections. You can also renew your subscription via the portal. You can visit Quick Heal RDM at https://mydevice.quickheal.com

PCTuner

Helps you improve the performance of your PC, especially for resource-intensive tasks. It offers a PC optimization dashboard that lets you get rid of junk files and duplicate data, free up memory space, clean the registry and carry out other tasks that help speed up your computer.

PC2Mobile Scan

Mobile malware is on the rise. If your phone does not have a mobile security app, you can scan and clean your mobile device with PC2Mobile Scan. Connect your device to your PC, search for it, and clean detected malware infections. The feature supports Windows, Android, iOS, BlackBerry, and Symbian devices.

TrackMyLaptop

Register for our free TrackMyLaptop service and track your laptop if it gets lost or stolen. The service comes with every desktop product of Quick Heal at no extra cost.
Kindly note that, Quick Heal users have to register their Quick Heal Product License key at the TrackMyLaptop portal to avail this facility.

System Requirements

Supported Operating System

To use Quick Heal Total Security, your system must meet the following minimum requirements. However, we recommend that your system should have higher configuration to obtain better results.

Note:

- The requirements are applicable to all flavors of the operating systems.
- The requirements are applicable to the 32-bit and 64-bit operating systems unless specifically mentioned.

General requirements

- CD/DVD Drive
- Internet Explorer 6 or later
- Internet connection to receive updates
- 1.4 GB hard disk space

System requirements for various Microsoft Windows Operating Systems

Windows 10

- Processor: 1 gigahertz (GHz) or faster
- RAM: 1 gigabyte (GB) for 32-bit or 2 GB for 64-bit

Windows 8.1 / Windows 8

- Processor: 1 GHz or faster
- RAM: 1 GB for 32-bit or 2 GB for 64-bit

Windows 7

- Processor: 1 GHz or faster
- RAM: 1 GB for 32-bit or 2 GB for 64-bit

Windows Vista

- Processor: 1 GHz or faster
- RAM: 1 GB

Windows XP (Service Pack 2 and later)

- Processor: 300 Megahertz (MHz) Pentium or faster
- RAM: 512 MB

Windows 2000(Service Pack 4)

- Processor: 300 MHz Pentium or faster
- RAM: 512 MB