Quick Heal
Internet Security Premium

Bank, chat, email, and browse online
with round-the-clock security.

Quick Heal

Security Simplified

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

Using emails, calls, SMSs and other mediums, attackers can trick you into visiting websites that have hidden malware or are designed to steal your personal or financial information. Web Security detects such websites and automatically restricts you from visiting them.

Email Security

Strictly checks incoming emails to filter out those that can infect your system or redirect you to phishing websites to steal your personal information. Email Security ensures that only genuine emails reach your inbox.

Safe Banking

Secures your financial details while you are banking or shopping on the Internet. When launched, this antivirus feature begins a safe desktop session with the supported Internet browsers. Quick Heal Safe Banking prevents you from landing on fake and bogus websites that can steal your personal and financial information. It also blocks data-stealing programs such as keyloggers that record what you type on your keyboard.

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

Browser Sandbox is a virtual environment where you can run your Internet browsers. Any malicious or malfunctioning program downloaded in this environment is isolated and restricted from causing any damage to your real PC. This security technique especially helps in protecting your computer from malicious websites that can infect your system the moment you visit them.

Parental Control

Uncontrolled or unmonitored Internet usage can have a bad influence on children. Parental Control helps parents ensure that their kids not only get to use the Internet constructively, but are also protected from all its dangers. This feature is now enhanced to let parents configure the following:

» **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 is an essential antivirus security feature that keeps your PC safe against external threats that use the Internet to reach your computer. This feature 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'. It also includes the Stealth Mode feature which makes it difficult for hackers to trace your system.

Core Protection

Multilayered defense mechanisms such as antivirus, antispyware, antimalware, anti-rootkit, firewall, and IDS/IPS work together to form the Core Protection.

» **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 like 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.

» **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.

Malware Protection

Enhanced Malware Protection detects spyware, adware, keyloggers, and riskware and efficiently blocks them from getting into your machine.

Anti-Keylogger

Keyloggers are data-stealing malicious programs that record what you type on your keyboard and share the information with hackers.

If a keylogger is present in your computer, typing confidential information like login ID and passwords, banking details like credit/debit card number, etc., can be risky. Quick Heal's Anti-Keylogger prevents such programs from stealing your information.

Improved Scan Engine

Our scan engine does not utilize the system resources in scanning files that show no sign of changes since the last time they were scanned. This helps the software scan files and folders for threats in lesser time without slowing down your system.

Advanced DNAScan

Quick Heal DNAScan technology combines behavioral and characteristic inspection and monitoring of unsafe programs. This protects your PC against unknown malware and other threats. 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

Vulnerability Scan helps you detect known security vulnerabilities that can be misused by hackers to steal your data or infect your computer with viruses and malware. Scanning your system with this feature detects vulnerabilities that could be present in the Operating System (OS) settings and other applications in your system. It also helps you fix any vulnerability in the OS settings.

Virtual Keyboard

Virtual Keyboard is a defense mechanism to prevent your confidential information from getting tracked or recorded by malicious programs like spyware and keyloggers. As the name suggests, this feature lets you type without using a physical keyboard. Whatever information you type on the Virtual Keyboard is encrypted and reaches its destination securely, without being intercepted by hackers or malware. Virtual Keyboard is mostly used by banking websites for added security of customer data.

Flash Drive Protection

Automatically scans external storage devices for infections and other threats. This is especially helpful if your work involves using unknown USB drives. This feature 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

When in Safe Mode, your computer can be tampered by any unauthorized user who can also change its Quick Heal settings. Such risks are reduced when the Safe Mode Protection is ON.

Enhanced Self-Protection

Prevents Quick Heal's running processes and services from getting tampered by malicious users.

Silent Mode

This feature comes in handy at times when you are busy working or watching a movie on your computer. With the Silent Mode ON, all antivirus prompts and notifications are muted. Choosing this option does not affect the security of your PC.

Import and Export Settings

Helps you export your Quick Heal security settings from a single computer and import it to other computers. This is helpful when you uninstall and reinstall the software, and during multiple computer configurations.

Quick Heal Remote Device Management (RDM)

The RDM portal lets you manage your Quick Heal products. You can login to the portal, you can view the security status of the products, renew, and manage their licenses. The portal also notifies you about any critical situations such as a malware infection in your PC. You can visit Quick Heal RDM at https://mydevice.quickheal.com

TrackMyLaptop

Quick Heal TrackMyLaptop Service helps you track the whereabouts of your lost or stolen laptop. The service is a social initiative that 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. Non-Quick Heal users have to register their Laptop's MAC ID. To know more, visit http://trackmylaptop.net

Stay Connected

Access our social media pages such as Facebook and Twitter to stay up-to-date with the latest findings and news of computer security.

Other Features

» **Forgot Password**

If you forget the password of your Quick Heal copy, the Forgot Password option can help you reset it. The feature is restricted to registered and activated copies of Quick Heal, and not trial copies.

» **Emergency Disk**

Helps you start your computer if it becomes infected with a virus and refuses to boot, by scanning and cleaning the machine.

» **Boot Time Scan**

Allows you to schedule a Boot Time Scan on your PC. It scans and cleans all drives before the Operating System triggers any stubborn viruses, rootkits, Trojans, or other malware.

Product Highlights

» Safe Banking keeps your personal and financial details hidden and protected from hackers.

» Automatically blocks access to infected, fake and bogus websites.

» Blocks emails carrying malicious links and attachments.

» Prevents data-stealing programs such as keyloggers from recording what you type on your keyboard.

» Blocks all types of malware and potentially dangerous programs from getting in your machine.

System Requirements

Supported Operating System

To use Quick Heal Internet 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

◉ 1.1 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

POP3 email clients compatibility

Quick Heal Internet Security supports

- Microsoft Outlook Express 5.5 and later

- Microsoft Outlook 2000 and later

- Netscape Messenger 4 and later

- Eudora

- Mozilla Thunderbird

- IncrediMail

- Windows Mail

Quick Heal Internet Security does not support

- IMAP

- AOL

- POP3s with Secure Sockets Layer (SSL)

- Web-based email such as Hotmail and Yahoo! Mail

- Lotus Notes

Note: The Email Protection feature of Quick Heal Internet Security is not supported on encrypted email connections that use Secure Sockets Layer (SSL).

The following features of Quick Heal Internet Security follow specific compatibility

Application Control

- Is not supported on Microsoft Windows 2000 with Service Pack 4.

- For Microsoft Windows XP, this feature is supported only if Service Pack 1 or later is installed.

Anti-Keylogger

- Is not supported on Microsoft Windows 2000, Windows XP 32-bit with Service Pack 1 or previous, and Windows XP 64-bit.

Browser Sandbox

- Is not supported on Microsoft Windows 2000 and Microsoft Windows XP 64-bit.
- This feature supports Internet Explorer, Google Chrome, and Mozilla Firefox browsers only.
- This feature does not support Microsoft Edge browser of Windows 10 operating system.

Firewall

- The Monitor Wi-Fi Networks feature is not supported on Microsoft Windows 2000 and Windows XP 64-bit.

Safe Banking

- Is not supported on Microsoft Windows 2000 and Microsoft Windows XP 64-bit.
- This feature supports Internet Explorer, Google Chrome,and Mozilla Firefox browsers only.
- This feature does not support Microsoft Edge browser of Windows 10 operating system.

Self-Protection

- Is not supported on Microsoft Windows 2000 OS.
- For Microsoft Windows XP operating system, this feature is supported only if Service Pack 2 or later is installed.
- Process protection functionality of Self-Protection is supported on Microsoft Windows Vista Service Pack 1 and later.

Anti-Rootkit

- Is supported on 32-bit OS only

Remotely Manage Quick Heal

- Is not supported on Microsoft Windows 2000 OS.
- Supports Internet Explorer 9 and later.

Emergency Disk

- Creating Emergency Disk using CD/DVD is not supported on Microsoft Windows 2003 and earlier versions. However, you can create Emergency Disk on USB drives.

Quick Heal Technologies Ltd.

Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune 411 014