Quick Heal AntiVirus for Server

The best security solution for server machines. Low on Resources. Strong on Technology.

Comprehensive Protection

- Our robust scan engine provides security against known and unknown malware, phishing, and virus attacks in real time.
- Blocks malware download on your server machine.
- Ever vigilant, Quick Heal AntiVirus for Server protects your data against known and emerging ransomware attacks.
- Ensures that you browse the Internet securely

Lightweight Footprint

Lightweight yet powerful antivirus uses minimal system resources and lets you enjoy the full power of your system.

Ease of Use

Simple interface and optimum default security settings ensure minimal user intervention. Just install and register the product, and enjoy your secure digital world.

Best-in-class support

Toll free number, online support, and a knowledge base information platform for all your queries.

Highlights

Proven scan engine

Virus Protection

- Blocks virus infections that try to infect server machines to gain admin control and steal data.

Malware Protection

- Detects all kinds of malware, viruses, worms, Trojans, and spyware that try to inflict your system from various sources and removes them instantly.

Advance DNAScan

- DNAScan, our indigenous and proven detection technology, detects and eliminates polymorphic threats that change code/file information in real time. It successfully traps suspected files and quarantines them so that malware does not harm your system.

Prevent data breaches

Data Theft Protection

- Blocks unauthorized copying of data from your system to any USB drive.

Prevent Ransomware attacks

Total Ransomware Protection

- Keeps your data and system safe from ransomware attacks.
- Smart data backup and restore features act as a safety net to get your valuable data (including Tally accounting data) back in case of a ransomware attack.

No fear of intrusion attack

Firewall

- Protects your system from network attacks.

IDS/IPS

- Blocks all kinds of malware intrusion and hacking attempts. Detects and blocks Remote Desktop (RDP) brute-force attempts and IP of remote attackers.

Secure email communications

Email Protection

- Prevents all kinds of malware coming through emails.

Spam Protection

- The powerful spam filter identifies junk and unwanted emails as spam.

Surf the online world safely

Browsing Protection

- Blocks suspicious and harmful websites that can download malware and worms to your system or steal your data.

Phishing Protection

- Prevents all kinds of phishing attempts that try to steal your data. Fraudsters impersonate legitimate email notifications asking for login or banking credentials. This feature detects such attempts.

Anti-Keylogger

Blocks all keystrokes spyware that can record your data and send to the hackers.

Anti-Trojan

Trojans are malicious software programs that come in disguise to trick you to download and install them on your system. Attackers using Trojans can steal data, download more malware, destroy data, and take control of your system. Anti-Trojan blocks such programs from getting inside your system.

Anti-Spyware

Spyware is a malicious software that secretly monitors unsuspecting users and steals their data. Spyware tries to steal crucial information such as login credentials from the infected system. Anti-Spyware protects your system from such data-stealing malware.

Adware Protection

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

Rogueware Protection

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

USB Drive Protection

When you attach a USB drive to your computer, and run Secure Removable Drive, your USB drive becomes secure from autorun malware. If you connect the vaccinated drive to any computer, the drive will not execute autorun malware.

Auto Silent Mode

Stops notifications or pop-ups from Quick Heal while antivirus runs in the background. Any scheduled scan is also deferred to the next schedule until Auto Silent Mode is turned off. This allows you to run any application in full screen mode like when you watch a movie or play games.

Automatic Update (Internet)

We release new updates to fight against the latest threats regularly. You can set to take the updates automatically whenever they are available. It is recommended that you always keep the Automatic Update feature turned on.

System Requirements

Operating System Windows Server 2003 or later	RAM 2 GB or more
CPU Intel Pentium 4 or higher	Disk Space 1.6 GB or more
Browser Internet Explorer 6 or higher	Additional requirements Internet connection to receive updates and for activation.

Please visit our website **www.quickheal.com** to know more about our security products and related system requirements.