Product Highlights

- Easy installation, optimized antivirus scanning, and minimum resource utilization.
- Robust and interoperable technology makes it one of the most dynamic antivirus software tools available.
- Reduced transfer time for updates guarantees that your server runs flawlessly under all circumstances.
- Enhanced user interface gives easy access to all four core areas of configuration.

Features List

Simpler and smarter security provides complete protection to your server. Low footprint of this suite ensures protection against latest threats without slowing your system.

Optimized antivirus scanning engine

Detects viruses before the system is infected.

- The antivirus engine is light on server resources and quick in detecting new and unknown threats.
- It scans critical system areas that are vulnerable to infection.
- The background scanning does not compromise server security and other popularly used applications

Virus Protection

Protects your server from virus infection by continuously monitoring and blocking virus attacks

- Blocks and prevents virus attacks from email attachments, Internet downloads, network, FTP, floppy, data storage devices, CD-DVD ROM file executable tools and during copying of suspected files.
- Displays virus warnings on a server system and notifies you only when a virus-infected file is found or a virus-like activity is detected.

Anti-KeyLogger

Programs called keyloggers stealthily record what a user types on their computer keyboard, and share the stolen information with the malware author. Anti-Keylogger protects valuable and sensitive data from getting stolen by such programs.

Vulnerability Scan

Detects known security vulnerabilities in the Operating System settings and applications. The feature also helps fix vulnerabilities found in the OS settings.

Intrusion Detection and Prevention System (IDS / IPS)

Advanced protection that proactively detects and prevents malicious activity which may exploit system vulnerabilities in the network.

Data Theft Protection

Con dential data on server is valuable but often vulnerable to theft.

» This feature blocks access to unauthorized removable drives such as USB drives, pen drives, and memory cards. This blocks transfer of data between the server and these drives thus ensuring strong network security.

Email Protection

Because email is the most widely used tool for communication, attackers may use it as a medium to spread virus infection. The Email Protection feature is redesigned to provide an efective countermeasure against such threats to servers.

» It ensures that only trusted or genuine email clients communicate on SMTP protocol and no worm uses the server as an infection spreading medium.

AntiSpam

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

Browsing Protection

This web security feature enables you to monitor and filter all virus-infected web traffic securing your online work environment. It is browser independent and has little impact on browsing speed.

Phishing Protection

This feature prevents you from accessing phishing and fraudulent websites. Phishing is a fraudulent attempt, usually made through email, to steal your confidential data such as banks details, user name and password, and personal information. As soon as you access a phishing website, it is blocked to prevent any phishing attempts.

USB Drive Protection

The autorun feature of removable devices is one of the ways through which malware is spread and hence your network security may come under threat. This feature secures removable devices such as pen drives, memory cards, and other USB devices and prevents spread of infection through autorun malware.

Autorun Protection

A preventive security measure for server antivirus, it blocks Autorun malware from entering the server by disabling the Autorun feature of the server.

AntiSpyware, AntiMalware and AntiRootkit

A comprehensive protection against spyware, malware and rootkits for best IT security management.

- The AntiSpyware feature provides real-time protection by blocking programs that behave like spyware. It also scans registry entries, system files, and installed programs for spyware activity and lists out threats, if found on the system.
- The combined AntiMalware feature prevents installation of rogueware and other potentially unwanted applications (PUA).
- Detects and cleans rootkits proactively through a deep system scan.

Firewall

Firewall offers multiple settings that you configure gure depending on the level of protection you desire for your network.You can set protection levels to High, Medium or Low for Internet traffic and applications that try to connect to your network. It also comprises the Stealth Mode which prevents hackers from tracing your system and attacking it.

Quick Heal Remote Device Management (RDM)

The Quick Heal Remote Device Management portal lets you manage your Quick Heal products. Via the portal, you can view the security status of the products, renew, and manage their licenses.

System Requirements

To use Quick Heal AntiVirus Server Edition, 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 Windows-based server operating systems.
- The requirements are applicable to the 32-bit and 64-bit of Windows-based server 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 Server OS

Microsoft Windows Server 2016

- Processor: 1.4 GHz (64-bit processor) or faster
- RAM: 2 GB

Note:

- Before installing Quick Heal AntiVirus Server Edition on Microsoft Windows Server 2016, you must remove Windows Defender. For more details, visit http://bit.ly/2uhCKkG
- If you are upgrading your existing OS to Windows Server 2016 with Quick Heal Server edition installed, we recommend you to uninstall Windows Defender after the upgrade. For more details, visit http://bit.ly/2uhCKkG

Windows Server 2012 R2 / Windows Server 2012

- Processor: 1.4 GHz Pentium or faster
- RAM: 2 GB

Windows Server 2008 R2 / Windows Server 2008

- Processor: 1GHz for 32-bit or 1.4 GHz for 64-bit
- RAM: Minimum 512 MB (Recommended 2 GB)

Windows Server 2003

- Processor: 550 MHz for 32-bit or 1.4 GHz for 64-bit
- RAM: 256 MB for 32-bit or 512 MB for 64-bit

Windows 2000 Server (Service Pack 4)

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

Supported Terminal Servers for Microsoft Windows Server

- Microsoft Windows Server 2012
- Microsoft Windows Server 2011
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Microsoft Windows Server 2000

POP3 email clients compatibility

Quick Heal AntiVirus Server Edition 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 AntiVirus Server Edition does not support

- IMAP
- AOL
- POP3s with Secure Sockets Layer (SSL)
- Web-based email such as Hotmail and Yahoo! Mail
- Lotus Notes

Note:

Quick Heal Technologies Ltd.

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