

Quick Heal Endpoint Security 5.3

Managing Endpoint Security for Complex Next-Gen Networks Made Simple.

Product Highlights

All new and intuitive web-based user interface simplifies security management from a single console.

- ▶ Award winning Quick Heal endpoint protection.
- ▶ Robust Web Security with phishing and browsing protection.
- ▶ Simplified configurations and maintenance with flexible Group Policy Management, Multiple Update Manager, and Tuneup.
- ▶ Combines threat-centric intrusion prevention and other protection technologies.

Features List

Simpler and smarter security that provides complete protection to your Server and client computers. Low footprint of this all-new-suite ensures up-to-date protection without slowing your system.



Enhanced Graphical Dashboard

Advanced graphical Dashboard gives immediate status of health of endpoints and highlights critical security situations that need immediate attention. Projects a 360° view of the network and related events and activities.

- ▶ Gives complete statistics of all deployed endpoints and unprotected systems in the network. Also shows the number of updated and non-updated endpoints in the network.

The Quick Heal Endpoint Security Dashboard also includes:

- ▶ **Web Security** - Shows statistics of the blocked websites.
- ▶ **Application Control** - Gives statistics of the number of unauthorized applications blocked.
- ▶ **Storage Device Control** - Provides statistics of blocked CDs/DVDs and USB Devices.
- ▶ **Top Vulnerabilities** - Provides a list of the top vulnerabilities found in the network.
- ▶ **Vulnerability Severity** - Provides information on the critical vulnerabilities in the network that require immediate attention.
Sends alerts to the administrator about critical system events such as license expiry date, outdated virus database, and so on.



Easy deployment and maintenance

Multiple methods of deploying clients. Deployment methods include:

- ▶ **Synchronization with Active Directory** - Easy and hassle free deployment with full active directory integration and synchronization support. This allows the Administrator to synchronize the Active Directory groups with Quick Heal Endpoint Security (QHEPS). Synchronization helps to deploy endpoint security clients on all computers in the domain network. The client automatically gets deployed on any new system that is added to the existing group in the network.
- ▶ **Remote Install** - Installation through remote access of web console on any system in the network.
- ▶ **Notify Install** - Installation through email notification (containing URL) for endpoint client installation.
- ▶ **Client Packager** - Creation of client installer for manual set up.
- ▶ **Login script setup** - Assigning the login script for installation.
- ▶ **Disk Imaging** - Creation of a disk image of Endpoint Security 5.3 client and deployment of it across the network.



IDS/IPS

Advanced defense detects attacks from various sources such as IDS/IPS, Port scanning attack, Distributed Denial of Service (DDOS) and so on. This detection implements a security layer to all communications and cordons your systems from unwanted intrusions or attack.

- ▶ **Intrusion Prevention** - Blocks malicious network activities and attempts to exploit software vulnerabilities of the applications.
- ▶ **Port Scanning Attack Prevention** - Essentially, a port scan attack consists of sending a message to each port in the network, one at a time. Depending on the response received the attacker determines if the port is used and can therefore be probed further for vulnerabilities. This feature blocks intruder attempts aimed at attacking any open port in the network.
- ▶ **DDOS Attack Prevention** - DDOS (Distributed Denial of Service) is a type of DOS Attack where multiple compromised systems – which are usually infected with malware – are used to target single system resulting in Denial of Service. QHEPS successfully blocks any attempt to initiate any DDOS attack to any system in the network.



Intelligent Firewall

Blocks unauthorized access to business network. Allows customization rules to be set to either Low, Medium or High based on observed network traffic. Admin can also configure exceptions for specific IP addresses or ports to be allowed or blocked. The three Firewall customization levels are:

- ▶ **Low** - Firewall configured at Low allows access to all incoming and outgoing traffic.
- ▶ **Medium** - Allows all outgoing traffic but blocks incoming traffic.
- ▶ **High** - Blocks all incoming and outgoing traffic.

This feature also gives the flexibility to configure exceptions to the Firewall rules. For example, if the configuration has been set on 'High', an exception to allow all connections can be added for a specific IP address or port.



Web Security

Blocks malware infected, phishing and malicious websites. Prevents threats transferred through websites hosting malicious codes while accessing the Internet.

- ▶ **Browsing Protection** - Thwarts attacks transferred through malicious websites.
- ▶ **Phishing Protection** - Scans all web pages while accessing the Internet for fraudulent activity to protect against any phishing attack.



Web Filtering

Allows blocking the websites based on categories such as Social Networking and Games or user-specified websites to limit web access and increase productivity.

- ▶ Swiftly and accurately filters millions of websites in over 40+ categories such as crime and violence, pornography, games, and so on without affecting bandwidth or productivity.
- ▶ Helps manage end-user access to the Internet. Eliminates time wasted on social networking sites, streaming media, gaming etc.
- ▶ IT-admin can allow access to certain websites that belong to blocked categories by creating an exclusion list. For example, if Social Networking & Chat category is blocked, the admin can allow access to Facebook by adding it in the 'Exclude list'.



Application Control

Categories of applications can be either authorized or unauthorized from being executed in the network. This feature also gives the flexibility to add custom applications to existing blocked list.

- ▶ Allows entire categories of applications to be either authorized or unauthorized.
- ▶ Custom applications that do not exist in the predefined blocked list can be added.
- ▶ Gives an extensive overview of all applications (authorized, unauthorized) installed in the network.



Storage Device Control

Prevents threats from the use of unauthorized devices and media (DVDs, CDs and USB devices).

- ▶ Allows policies to be set to give read-only or full access to USB-devices and block DVDs/CDs.
- ▶ This robust feature also prevents data leak by making USB-devices accessible only on systems within the organization's network.
- ▶ Storage Device Control is supported on Windows and Mac platform.



Vulnerability Scan

This feature scans known vulnerabilities of installed applications and operating systems in the network. It helps frame security measures against known vulnerabilities and protect against security breaches by threat agents.

- ▶ Scans vulnerabilities in applications such as Adobe, Safari, Mozilla, Oracle, etc.
- ▶ Notifies regarding unpatched operating systems of computers in the network.



Scan

This feature allows virus and malware scan of all the computers in the network from a central location. The scans can also be scheduled as per convenience.



Update

Networked computers can be updated from a central location. Endpoints can be configured to take updates at a specified time.



Email Scan

Effectively scans your end-user Inboxes for spam, phishing attacks and unsolicited email messages. Allows whitelist and blacklist and self-learning to be set up separately for certain email address or domains.



Multiple Update Managers

This feature allows deployment of multiple Update Managers across the network. This helps in load balancing and in avoiding network congestion that usually happens when there is a single Update Manager.



Email and SMS Notifications

This feature allows notifications to be sent to configured email addresses and numbers.

- ▶ These notifications would alert the network administrator of critical network events such as detection of viruses, virus outbreaks, attempts to access of an unauthorized device, license expiry date etc.



Tuneup:

This feature helps to improve the performance of computer systems by cleaning junk and invalid registry / disk entries.

- ▶ Tuneup can be carried out for all endpoints from the Endpoint Security Server.
- ▶ Maintenance can also be scheduled at a specific time and date.



Group Policy Management

Different user groups can be defined and policies can be set accordingly.



Reports

Provides a range of graphical and tabular reports.

- ▶ Reports can also be exported and saved in a variety of formats such as PDF, HTML, and DOC.
- ▶ Reporting can be scheduled according to the requirements.
- ▶ Automatic emails of reports can be sent to specific email addresses.












Others

- ▶ Quick Heal 2014 Windows client builds are integrated into QHEPS5.3. The following Windows client settings can also be configured from QHEPS Server:
 - a. Behavior Detection System settings - Behavior Detection System detects unknown threats by inspecting application behavior.
 - b. Safe Mode Protection settings - Safe Mode Protection avoids unauthorized access to computers when they are in safe mode.

Certifications:



Flavor Comparison

Features		Quick Heal Endpoint Security 5.3	
		Business Edition	Total Edition
	IDS/IPS Protection	✓	✓
	Firewall Protection	✓	✓
	Phishing Protection	✓	✓
	Browsing Protection	✓	✓
	Vulnerability Scan	✓	✓
	SMS Notification	✓	✓
	Spam Protection		✓
	Web Filtering		✓
	Application Control		✓
	Storage Device Control		✓
	PC Tuner		✓

Get Additional Feature Packs for Business Edition at an Extra Cost

Feature Pack	Features
Productivity	AntiSpam & Web Security
Compliance	Application Control & Storage Device Control
Performance	PCTuner

System Requirements

Quick Heal Endpoint Security server can be installed on a system with any one of the following operating systems:

- ▶ Microsoft Windows 2000 SP4 Professional / Server / Advanced Server
- ▶ Microsoft Windows XP Professional (32-bit/64-bit)
- ▶ Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- ▶ Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- ▶ Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- ▶ Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- ▶ Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- ▶ Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- ▶ Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)

- ▶ Microsoft Windows SBS 2011 Standard / Essentials
- ▶ Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- ▶ Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- ▶ Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)

Minimum System Requirement for Console System

- ▶ 1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium processor or equivalent
- ▶ 1 GB of RAM
- ▶ 3250 MB of free disk space
- ▶ Monitor that supports 1024*768 resolution in 256-color mode

Additional Software Required for Console System

Console needs to have Web Server services of either Microsoft IIS or Apache Web Server on the system.

If Microsoft IIS is to be configured as web server, the version requirements are as follows:

- ▶ IIS Version 5.0 on Windows 2000
- ▶ IIS Version 5.1 on Windows XP
- ▶ IIS Version 6.0 on Windows Server 2003
- ▶ IIS Version 7.0 on Windows Vista and Windows Server 2008
- ▶ IIS Version 7.5 on Windows 7 and Windows Server 2008 R2
- ▶ IIS Version 8.0 on Windows 8 and Windows Server 2012
- ▶ IIS Version 8.5 on Windows 8.1 and Windows Server 2012 R2

If Apache is to be configured as web server, the version requirement is as follows:

- ▶ Apache Web Server 2.0 or later

Other Essential Configuration on Console System

- ▶ Administrator or Domain Administrator access on the console system.
- ▶ File and printer sharing for Microsoft Networks installed.
- ▶ Transmission Control Protocol/Internet Protocol (TCP/IP) support installed.
- ▶ Internet Explorer Version 7, 8, 9, 10 or 11.

Network Deployment Scenarios

- ▶ If the network is configured using DHCP, the Endpoint Security server system on which Quick Heal Endpoint Security will be installed and the DHCP server system should be configured using a static IP address.
- ▶ If Quick Heal Endpoint Security is to be installed on a server with two network cards and Quick Heal client agents are to be deployed on both the networks, then during installation of Quick Heal Endpoint Security the administrator has to configure Domain Name based communication.

Client side requirements

Windows Workstations supported

- ▶ Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server
- ▶ Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit/64-bit)
- ▶ Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- ▶ Microsoft Windows Vista Home Basic / Home Premium / Ultimate / Business / Enterprise (32-bit/64-bit)
- ▶ Microsoft Windows Server 2008 Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- ▶ Microsoft Windows Server 2008 R2 Web / Standard / Enterprise Datacenter (64-bit)
- ▶ Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- ▶ Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- ▶ Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- ▶ Microsoft Windows SBS 2011 Standard / Essentials

- ▶ Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- ▶ Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- ▶ Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)

Minimum System Requirements for Windows Clients

- ▶ 256 MB of RAM
- ▶ 1800 MB of free disk space
- ▶ 1 GHz 32-bit (x86) or 64-bit (x64) processor for Windows Vista, Windows 2008 Server, and Windows 7
- ▶ 1 GB of RAM for Windows Vista and Windows 7
- ▶ 512 MB of RAM for Windows 2008 and Windows 2008 R2
- ▶ For Windows 2000 Service Pack 4 or later
- ▶ Internet Explorer 5.5 or later
- ▶ Administrative privilege is required for installation

Mac Workstations supported

- ▶ Mac OS X 10.6, 10.7, 10.8, 10.9
- ▶ Mac Computer with Intel Processor

Minimum System Requirements for Mac Client

- ▶ 512 MB of RAM
- ▶ 1200 MB free hard disk space

Linux Workstations supported

32-Bit:

- ▶ Redhat 9
- ▶ Redhat Enterprise Linux 4, 5.3, 6.0
- ▶ Fedora 7, 12, 13, 14
- ▶ SuSE 7.3, SuSE ES 10, SuSE ES 11
- ▶ BOSS
- ▶ Mandrake 9.2
- ▶ Mandriva 2008
- ▶ CentOS 5
- ▶ Ubuntu 7.10, 10.04 LTS, 10.04.1 LTS

64-Bit:

- ▶ Redhat Enterprise Linux 5.3, 6.0
- ▶ Fedora 13, 14
- ▶ SUSE ES 11
- ▶ Ubuntu 10.04 LTS, 10.04.1 LTS

Minimum System Requirements for Linux Clients

- ▶ 133 MHz or later Intel based (or compatible) processor
- ▶ 128 MB or later RAM
- ▶ 500 MB of free hard disk space

Quick Heal Technologies (P) Ltd.

603, Mayfair Tower II, Wakdewadi, Shivajinagar, Pune - 411 005, India.

Copyright © 2013 Quick Heal Technologies (P) Ltd. All Rights Reserved.

Quick Heal is a registered trademark of Quick Heal Technologies (P) Ltd., Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

This document is current as of the initial date of publication and may be changed by Quick Heal at any time.