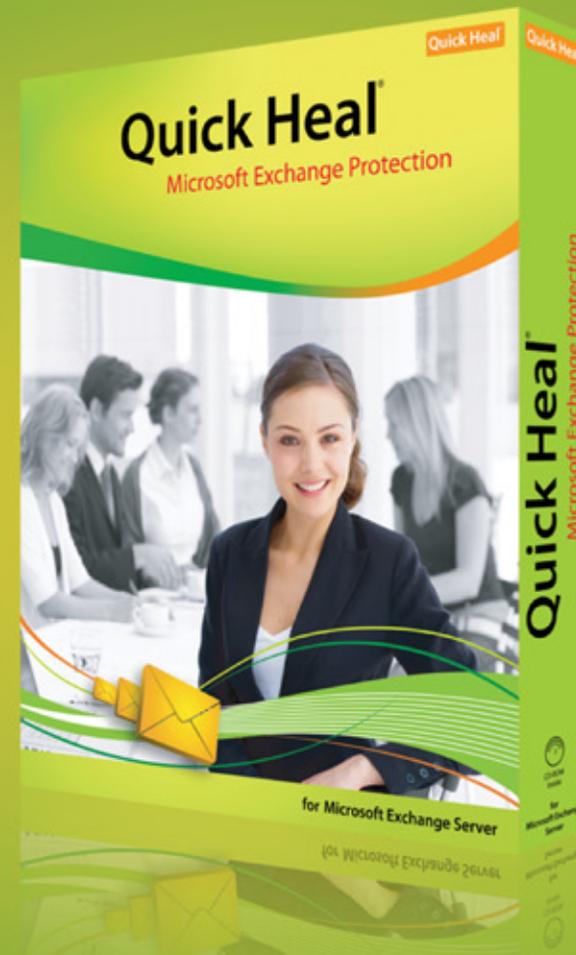


**Quick Heal**<sup>®</sup>

*Security Simplified*



# Quick Heal Microsoft Exchange Protection

Intuitive. Effective. Comprehensive.

# Feature List

Web-based console makes administrative management easy and simple. Comprehensive and rapid scanning of emails with reduced system resource usage.

- ▶ Monitor security status with in depth reports and daily statistics using the advanced notification system.
- ▶ Get automatic and incremental updates on-demand or as per schedule.



## DNA Scan

Detects new and unknown viruses. Detects and cleans viruses, worms, Trojans and all kinds of malware.

- ▶ The improved technology also scans file and archive attachments (ZIP, ARJ, GZIP, RAR, TAR, CAB etc).
- ▶ Effective protection against zero-day attacks. Code analysis and behavioral classification trace the gene of the malware and its intentions in real-time.



## Store Scan

Allows you to schedule on-demand scanning for all or specific user mailboxes and public folders.

- ▶ This can also be performed for mailbox and store attachments that violate corporate policy.
- ▶ Results in improved detection rate and performance.



## Powerful Spam filters

Intelligent technology carries out real-time scans for spam messages and attachments. Automatically blocks malicious emails like IFRAME Exploit emails.



## Back Scan

Saves time and reduces workload by prompting an automatic scan of mail stores after every successful update.

- ▶ Ensures that all mail stores are processed using the latest version of the antivirus databases without overloading the server.
- ▶ Scans can be carried out on-demand or on-schedule.



## White and Blacklists

Personal and global black lists and white lists can be maintained to restrict email communication from senders that are known to be malicious. These lists can be incorporated on server-wide basis or to machines on individual basis.



## Centralized management

Allows flexible and easy management via web-based console that gives system administrators quick response time and consolidated event status.

- ▶ Several reports are also presented via the cloud-based console.
- ▶ Remote administration allows companies to react to threats in real time as soon as they arise.



## Multi-functionality dashboard

The dashboard is easily accessible and its simple interface allows the administrator to view various indicators simultaneously.

- ▶ In case there are any threats detected, this is informed to the administrator via highly visible alerts.
- ▶ Advanced settings can also be easily configured.
- ▶ The notifications can be viewed through the Windows event log or via email as well.



## Personalized and In-depth reports

Timely and detailed reports can be obtained in the format and at the frequency desired.

- ▶ These reports can be sent directly to the administrator's hard disk or can be sent via email.

- ▶ The solution offers complete control to view, analyze and this speeds up the response time.



## **Export configurations with ease**

Administrative settings for the security solution can be configured based on prevalent company IT policies and regulations.

- ▶ Helps create individual response blueprints for separate categories of spam threats and this enhances the flexibility of response mechanisms. These configurations can then be easily exported to other servers, thus allowing multiple branches to work with the same configurations.

---

# Product Highlights

Web-based console makes administrative management easy and simple.

- ▶ Refine mail classification by defining categories to prevent any accidental loss of information.
- ▶ Assign security specifications based on company policy and hardware capabilities.
- ▶ Comprehensive and rapid scanning of emails with reduced system resource usage
- ▶ Intuitive scanning based on message attributes (IP address, email Id, size, attachments, etc)
- ▶ Monitor the security status with in depth reports and daily statistics using the advanced notification system.
- ▶ Get automatic and incremental updates on-demand or as per schedule.

# System Requirements

To use Quick Heal Exchange Protection, server must meet following system requirements:

## Operating System and Minimum System Requirements

Quick Heal Exchange Protection can be installed on system with any one of below operating systems:

### Operating system requirement

- ▶ Microsoft Windows 2000 Server (Service Pack 3 or above)
- ▶ Microsoft Windows 2000 Advance Server (Service Pack 3 or above)
- ▶ Microsoft Windows Server Standard 2003 (Service Pack 1 or above)
- ▶ Microsoft Windows Server Enterprise 2003 (Service Pack 1 or above)

### Additional software required for Quick Heal Exchange Protection system

Quick Heal Exchange Protection needs to have Microsoft Exchange Server and Web Server services of Microsoft Internet Information Server (IIS) on the system. The version requirements are follows:

- ▶ Exchange Server 2000 with Service Pack 3
- ▶ Exchange Server 2003
- ▶ IIS Version 5.0
- ▶ IIS Version 6.0

### Minimum system requirement

- ▶ 300 MHz Intel Pentium processor or equivalent
- ▶ 256 MB of RAM
- ▶ 100 MB of free disk space
- ▶ Monitor that supports 800\*600 Resolution at 256 colors or higher

### Other essential configuration on Quick Heal Exchange Protection system

- ▶ Administrator or Domain Administrator access on the system.
- ▶ File and printer sharing for Microsoft Networks installed.
- ▶ Internet Explorer 5.5 or above.

### Mail Client Supported

- ▶ Microsoft Outlook 98/2000/XP/2003/2007 for Microsoft Exchange Server based communications.
- ▶ Any other POP3/IMAP/HTTP email clients.