



# Quick Heal Total Security<sup>®</sup> per Mac

Protezione facile, veloce e  
continuativa per Mac.

**Quick Heal**

*Security Simplified*

# Caratteristiche Principali

- » Protezione dai virus veloce e molto reattiva.
- » Protezione della Navigazione e Protezione Anti Phishing per tenere a bada siti dannosi.
- » La protezione email monitora il traffico email in cerca di malware, compresi tutti gli allegati inviati da utenti.
- » Una sola chiave prodotto per attivare i desktop Windows paralleli.

## Caratteristiche

Un sistema di sicurezza affidabile creato per proteggere il tuo Mac da minacce zero-day, software dannosi, spam e altri rischi online. Gli aggiornamenti automatici mettono in sicurezza il tuo Mac dai più recenti rischi senza rallentare la funzionalità.



### Sicurezza per il Mac

Protezione automatica e personalizzabile che tiene costantemente il tuo Mac al riparo da worm, Trojan e altri programmi dannosi senza rallentare le prestazioni

- » **Protezione Virus:** monitora continuamente e individua le minacce (virus, Trojan e worm) sul tuo Mac. Le opzioni di default riguardo alla scansione manuale sono generalmente adeguate; tuttavia, se necessario, le opzioni per la scansione manuale possono essere ricalibrate.
  - **Antimalware:** scansiona file e cartelle molto velocemente, individuando e ripulendo spyware, adware, rogueware, dialer, riskware e altre potenziali minacce. La protezione contro tutti i malware multiplatforma rende sicuri gli scambi di file sia per il singolo utente che negli ambienti aziendali.
  - **Antispyware:** gli spyware sono solitamente associati a software che mostrano annunci. Una volta installato, il software tenta di modificare le impostazioni del sistema, aggiungere elementi o estensioni al tuo browser e tracciare le tue attività e informazioni online. Questa caratteristica individua e elimina gli spyware che tracciano informazioni personali e sensibili.
- » **Scan My Mac:** consente di scegliere tra una scansione dell'intero sistema o una scansione personalizzata dei virus in specifici file e cartelle.
  - Scan my Mac, una volta abilitato, esegue una scansione completa del tuo Mac. Questa opzione fa sì che si esegua una scansione approfondita dell'intera macchina, dei file e delle cartelle (ad esclusione di drive di rete)
  - La Scansione Personalizzata permette di svolgere una ricerca dei virus in specifici campi, drive, cartelle e file.

Questa funzione aiuta nel caso in cui serva scansionare solo alcuni file e non l'intero sistema.

- » **Scansione pianificata:** consente di impostare le tempistiche di avvio della scansione automatica sulla tua macchina. Questa funzione garantisce flessibilità grazie alla possibilità di impostare pianificazioni multiple in base alle tue esigenze. E' possibile impostare anche la frequenza delle scansioni.
- » **Escludi file e cartelle:** consente di stabilire quali file e cartelle non devono essere inclusi nelle scansioni virus. Questo aiuta a evitare ripetizioni di scansioni non necessarie su file sui quali si è già effettuata scansione o che non dovrebbero essere scansionati. L'esclusione di file o cartelle è consentita dai moduli di scansione sia della funzione Scan My Mac che da quella di Protezione Virus.
- » **Quarantena e Backup:** aiuta a isolare file infetti o sospetti. Quando un file viene aggiunto alla Quarantena, il software cripta il file e lo tiene in custodia nella Quarantena. Impedisce così al file infetto o sospetto di eseguirsi e diffondersi. L'opzione di backup, quando selezionata, mantiene una copia del file infetto prima di ripararlo. Questa caratteristica consente anche di rimuovere i file dopo un certo periodo di tempo.

- » **Protezione Navigazione:** tiene a bada i siti dannosi mentre si naviga in Internet. Al giorno d'oggi però, non sono solo siti dannosi a diffondere codici malevoli. Ogni sito web che non sia ben protetto può essere compromesso dagli autori di malware, i quali possono immettere codici dannosi anche in siti web autentici per infettare le macchine dei visitatori. Gli autori di malware possono anche creare codici che colpiscano il sistema operativo o le vulnerabilità delle varie applicazioni. La Protezione Navigazione organizza un report di tutti i tentativi di exploit delle vulnerabilità dei software durante la navigazione sul web.
- » **Anti-phishing:** impedisce l'accesso a siti di phishing e fraudolenti. Il phishing è un tentativo, condotto solitamente via email, di rubare informazioni personali/sensibili/finanziarie. L'email cerca di convincerti a visitare un sito e a inviare informazioni personali come carte di credito, account e password, numeri di telefono ecc..La funzione Anti-phishing scansiona automaticamente tutte le pagine web a cui si accede in cerca di attività truffaldine e ti protegge da ogni tentativo di phishing mentre navighi. Previene il furto di identità bloccando siti web specifici: può così garantirti una esperienza senza rischi di navigazione sul web, di shopping online e di banking online.



## Sicurezza Web

Il sistema di sicurezza basato su cloud impedisce che siti falsi e di phishing possano rubare informazioni sensibili o soldi. Impedisce automaticamente agli utenti di visitare siti fraudolenti, compromessi, infetti e di phishing.





## Parental Control

Consente ai genitori il pieno controllo delle attività in Internet dei propri figli o di altri utenti.

- » **Restringere gli accessi a siti internet di specifiche categorie:**  
Questa funzione ha una vasta gamma di categorie di siti web verso i quali si può concedere o negare l'accesso sulla base di certe caratteristiche. Una volta ristretto o concesso l'accesso a una categoria di siti web, tutti i siti di quel tipo ricadranno nella categoria dei siti bloccati oppure, al contrario, accessibili. Garantisce anche la possibilità di concedere l'accesso a siti web appartenenti ad una categoria bloccata, tramite l'inserimento nella Lista di Esclusione.
- » **Restringere l'accesso ai siti web specificati dall'utente:**  
questa funzione aiuta a bloccare specifici siti web. Risulta molto utile quanto si vogliono bloccare certi siti, ma la lista è più ridotta di quella che potrebbe comporre una intera categoria. E' utile anche quando un sito internet non ricade sotto una precisa categoria oppure quando il sito risulta accessibile nonostante il blocco della categoria di appartenenza.
- » **Restringe l'accesso ai siti web specificati dall'utente**  
Questa funzione aiuta a bloccare specifici siti web. Risulta molto utile quanto si vogliono bloccare certi siti, ma la lista è più ridotta di quella che potrebbe comporre una intera categoria. E' utile anche quando un sito internet non ricade sotto una precisa categoria oppure quando il sito risulta accessibile nonostante il blocco della categoria di appartenenza.



## Antispam e sicurezza email

La sicurezza email, basata su cloud, impedisce in tempo reale che spam, phishing e altri tipi di email infette possano raggiungere la tua mailbox.

- » **Protezione email:** consente di abilitare regole di protezione per tutte le email in arrivo. Blocca allegati contenuti nelle email che hanno una natura sospetta e potrebbero rivelarsi malware, virus o spam. Consente anche la personalizzazione delle azioni da intraprendere nel caso in cui venga individuato un malware in una email. Questa funzione è abilitata di default. Si raccomanda di tenerla abilitata per assicurare la protezione dalle email dannose.
- » **Protezione spam:** impedisce a tutte le email non desiderate (email di spam, di phishing, con contenuti pornografici) di raggiungere la tua mailbox. Si raccomanda di tenere questa funzione sempre abilitata.



## Chiave di prodotto singola

Questa funzione consente agli utenti di attivare la propria copia del desktop parallelo con la stessa chiave stessa di attivazione già esistente per il Total Security per Mac.

\* Il desktop parallelo per il Mac è una caratteristica disponibile dalla versione 8 in poi.

## Requisiti di sistema

Per usare Quick Heal Total Security il tuo sistema deve rispettare i seguenti requisiti minimi. Tuttavia consigliamo di utilizzare il nostro software su un sistema che abbia caratteristiche superiori per ottenere risultati migliori.

### Note:

- \*I requisiti sono applicabili a ogni versione di sistema operativo.
- \* Dove non specificato, il requisito in questione è applicabile alle versioni a 32-bit e a quelle a 64-bit.

- ⦿ Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10 & 10.11
- ⦿ Computer Mac con Processore Intel
- ⦿ 512 MB di RAM
- ⦿ 700 MB di spazio libero su Hard Disk
- ⦿ Connessione a Internet per ricevere gli aggiornamenti
- ⦿ Internet Explorer 6 o ultima versione del browser.
- ⦿ Lettore DVD

### Sistemi operativi supportati:

- ⦿ Microsoft Windows 2000 Professional (Service Pack 4 e successivi)
- ⦿ Microsoft Windows XP Home / Professional (Service Pack 2 e successivi)/ Professional 64-bit
- ⦿ Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate
- ⦿ Microsoft Windows 7 Starter / Home Basic / Home Premium / Professional / Enterprise / Ultimate (
- ⦿ Microsoft Windows 8 / Windows 8 Pro / Windows 8 Enterprise
- ⦿ Microsoft Windows 8.1 / Windows 8.1
- ⦿ Non può essere installato su server OS.

### Minimum Hardware Requirements

- ⦿ Processore 300 MHz o superiore per Microsoft Windows 2000 Professional, Microsoft Windows XP
- ⦿ 1 GHz per Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1
- ⦿ 512 MB RAM per Microsoft Windows 2000 Professional, Microsoft Windows XP
- ⦿ 1 GB RAM per Microsoft Windows Vista (32-bit)
- ⦿ 1GB RAM per Microsoft Windows 7 (32-bit), Microsoft Windows 8 (32-bit), Microsoft Windows 8.1 (32-bit)
- ⦿ 1 GB RAM per Microsoft Windows Vista (64-bit)
- ⦿ 2GB RAM per Microsoft Windows 7 (64-bit), Microsoft Windows 8 (64-bit), Microsoft Windows 8.1 (64-bit)

Quick Heal Technologies Ltd.



**SECURITY LAB**  
sicurezza on line