



info

Sophos
www.sophos.it
02/662810-0
€ 421,00 + Iva (5 licenze)

pacchetto antivirus completo; nessun impatto misurabile sulle prestazioni del sistema; veloce da installare; sistema di aggiornamento delle firme semplice; buona gestione dell'abbonamento

soluzione di tipo aziendale, non indicata al singolo utente

Universal Binary si

Soluzione dedicata alle piccole e medie imprese per il rilevamento multiplatforma dei virus e la protezione in tempo reale

Sophos Anti-Virus per Mac OS X 4.8.4

Sophos è un produttore di software impegnato nell'ambito della sicurezza con un listino ricco di prodotti pensati per le imprese. Le soluzioni comprendono meccanismi di prevenzione contro malware, spyware e virus, sistemi contro le intrusioni, monitor per la verifica di applicazioni non autorizzate, sistemi antispam e tool per il controllo delle policy aziendali. Un quadro ricco, dedicato in buona parte all'area interna dell'azienda, dove operano gli utenti autorizzati e dove è facile incorrere in rischi per la sicurezza a causa di configurazioni "leggere", policy aziendali permissive e scarsa conoscenza e attenzione da parte degli operatori.

L'antivirus è in questo contesto fondamentale, allo scopo di prevenire un elevato numero di problemi legati all'uso disattento della posta elettronica e degli allegati che vengono recapitati. Sophos fornisce in tal senso prodotti della famiglia Small Business Solutions oppure soluzioni Enterprise, di tipo centralizzate. L'offerta è in buona misura dedicata a Windows ma il marchio fornisce anche il supporto per Linux e Mac OS X con ottimi prodotti, forse i migliori in ambito Mac.

Su *Applicando* ci siamo già occupati della versione Enterprise di Sophos Anti-Virus.

In questa sede verrà considerata la Security Suite della linea Small Business Solutions, provata in modalità stand-alone, quindi non agganciata a un server centrale: il minimo di licenze acquistabile è per cinque postazioni e l'installato può poi crescere a seconda delle esigenze dell'azienda.

Caratteristiche tecniche

Sophos Anti-Virus per Mac OS X dispone di molte caratteristiche interessanti: il pacchetto è Universal, supporta le versioni di Mac OS X client e server, include un motore di controllo contro virus, spyware, trojan e worm, con controllo su richiesta e in real-time. Il database delle firme virali è inoltre condiviso: il client in versione Mac OS X contiene lo stesso database della versione Windows. Qualunque virus, indipendentemente dalla piattaforma target, verrà riconosciuto dall'antivirus su Mac.

Il meccanismo di aggiornamenti via Internet è programmabile ed è impostabile dalla rete con accesso a un server centrale; è anche previsto un sistema di reportistica integrato. È infine interessante la tecnologia "Decision Caching", attraverso cui solo i file modificati subisco-

no una seconda scansione nella modalità di controllo in tempo reale. Questo meccanismo diminuisce il carico sul sistema da parte dell'antivirus.

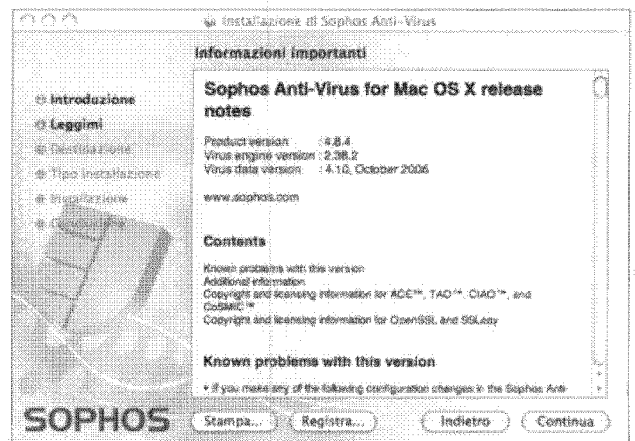
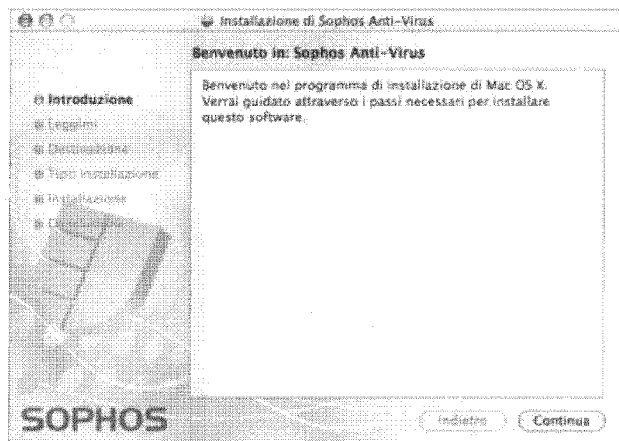
Installazione

L'installazione del prodotto è molto semplice: basta inserire il CD-ROM nel drive e aprire il pacchetto "Sophos Anti-Virus.mpkg". Viene in questo modo attivata la procedura di installazione guidata, al termine della quale l'antivirus si troverà dentro la cartella Applicazioni.

Al primo lancio verrà probabilmente indicato che il database non è aggiornato. Non resta che risolvere questa condizione andando nelle Preferenze di Sistema e cliccando sull'icona Sophos Anti-Virus presente in basso nella sezione Accessori. Attraverso questa icona è possibile regolare diversi aspetti del programma. La parte relativa agli aggiornamenti si trova nella sezione AutoUpdate.

Nel caso di uso stand-alone, si deve scegliere la prima voce (Sophos) e bisogna indicare più in basso uno user name e una password per accedere ai server di Sophos per gli aggiornamenti. Si deve poi scegliere la sezione Primary Proxy e verificare che la configurazione sia compati-

Due schermate della procedura di installazione



bile con la propria rete locale. Per default è selezionata la prima voce che recupera le configurazioni del proxy dalle impostazioni di rete del sistema locale.

A questo punto gli aggiornamenti dovrebbero essere eseguiti in forma del tutto automatica. Eventualmente è possibile cliccare sull'icona dell'antivirus presente nella barra di sistema, in alto, e scegliere Show AutoUpdate Window, per attivare un update manuale.

Attraverso l'icona presente nelle Preferenze di Sistema è possibile regolare altri aspetti del programma. Dalla sezione Scanning si può disattivare e riattivare manualmente l'antivirus e stabilire se deve essere visibile l'icona nella barra dei menu, in alto. Nella sezione Notification è invece possibile fare in modo che la rilevazione di un virus sia automaticamente notificata attraverso un messaggio e-mail. In questo pannello si dovranno specificare i dettagli del server di posta.

Uso del programma

Di default l'antivirus funziona in modalità "real-time": il sistema viene cioè continuamente scansionato alla ricerca di virus. Eventualmente è possibile eseguire anche scansioni manuali, a comando: basta attivare l'icona di Sophos Anti-Virus presente dentro la cartella Applicazioni, selezionare un drive e premere sul bottone con la freccia verde. In questo caso verrà eseguita una scansione completa del disco.

Le opzioni di scansione possono essere regolate premendo sulla prima icona a sinistra del gruppo di tre icone presente in alto a destra.

Interessanti le possibilità elencate nella prima voce, Scanning Options. In questa sezione è possibile stabilire se eseguire le scansioni anche all'interno dei file compressi, se controllare le caselle di posta e se cercare anche virus per Windows.

È consigliabile attivare quest'ultima opzione in quanto è bene eliminare qualunque tipo di virus, anche quelli che non possono nuocere al proprio sistema operativo: quando ad esempio un virus Windows fosse all'interno di un allegato nella mailbox, potrebbe capitare di inoltrare per errore questo messaggio a un destinatario esterno.

Una protezione antivirus corretta implica sempre il tentativo di proteggere an-

che l'ambiente circostante, non solo la propria macchina. Se questa regola fosse applicata da tutti, non sussisterebbe il problema della diffusione dei virus per posta elettronica!

La voce di configurazione Disinfection permette invece di stabilire il comportamento che l'antivirus deve seguire nel caso venga individuata una minaccia. Si sconsiglia di tentare la disinfezione in quanto, nella maggior parte dei casi, il virus danneggia il file oppure non vi è nulla che sia possibile ripristinare (il virus potrebbe trovarsi in un file eseguibile autonomo). La procedura migliore da seguire consiste nel cancellare il file: a tale scopo, si deve selezionare Action On Infected Files e poi Delete.

Tornando alla configurazione dell'antivirus, si incontra la voce laterale Reporting. Questa permette di stabilire il modo in cui deve essere gestito il file storico con le registrazioni circa il funzionamento del programma. La voce seguente è invece Desktop Alerts, da cui scegliere il modo in cui compariranno le segnalazioni a video in caso di infezione (si può cioè personalizzare il messaggio che l'utente vedrà in caso di individuazione di virus). Infine si trova la voce Log File, da cui si può impostare il modo in cui saranno trattati i log dell'antivirus.

Prestazioni

Durante i nostri test abbiamo utilizzato il prodotto di Sophos nella modalità di scansione real-time su un portatile MacBook con processore Core Duo da 2 GHz e 1 GB di memoria RAM. Il sistema operativo era Mac OS X Tiger.

L'antivirus si è comportato regolarmente, senza creare problemi di funzionamento o conflitti. Tutte le operazioni sono risultate discrete e non intrusive. Non si sono inoltre rilevati rallentamenti apprezzabili nell'uso del sistema durante attività di office automation.

Per verificare l'affidabilità del prodotto si è scaricato dal sito www.eicar.org il file campione di test "eicar.exe". L'antivirus ha immediatamente riconosciuto la stringa e fermato l'accesso al file. Questo test ha quindi provato la tempestività del meccanismo di scansione del prodotto.

EICAR è un'organizzazione che si occupa di sicurezza dei sistemi e ha sviluppa-

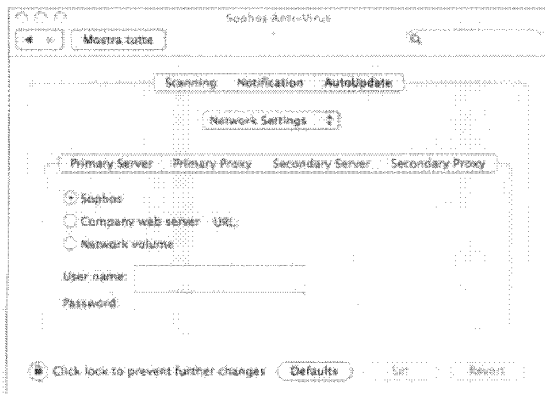
to una stringa di test per antivirus. Tutti i maggiori produttori hanno aderito a questo standard e riconoscono la stringa EICAR durante le procedure di scansione. Per verificare il buon funzionamento di un antivirus non è quindi necessario manipolare virus attivi, ma semplicemente scaricare la stringa di prova.

Durante l'utilizzo nel tempo si è optato per una ricerca almeno quotidiana di nuove firme antivirus dal sito del produttore. Gli aggiornamenti frequenti sono una condizione imprescindibile per un'adeguata protezione contro i malware. Nessun problema da segnalare circa gli aggiornamenti.

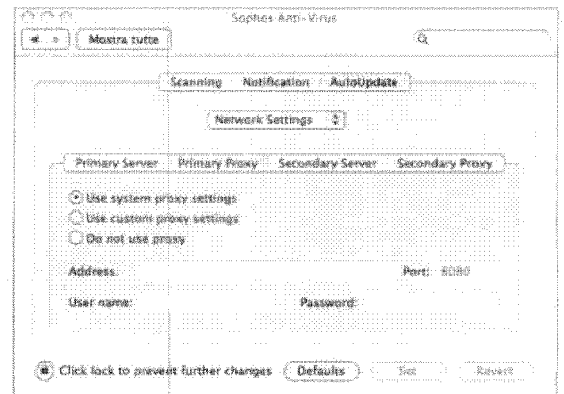
Il prodotto è infine risultato di facile installazione e amministrazione nel tempo, certamente migliore di altre alternative antivirus commerciali per Mac. Forse solo la procedura di rimozione è un po' meno chiara. Ad esempio, nel caso sia necessario disinstallare l'antivirus, bisogna aprire il disco di sistema e cliccare due volte su Libreria/Application support/Sophos Anti-Virus, poi fare doppio clic sull'icona Remove Sophos Anti-Virus.pkg e infine seguire la procedura guidata.

Sophos Anti-Virus rappresenta una buona soluzione per chi desidera mettere in opera un meccanismo continuo di scansione del proprio sistema e per coloro che hanno la necessità di conformarsi al D.Lgs 196/2003, normativa che impone la presenza di un antivirus aggiornato nelle postazioni in cui sono trattati dati personali di qualunque natura.

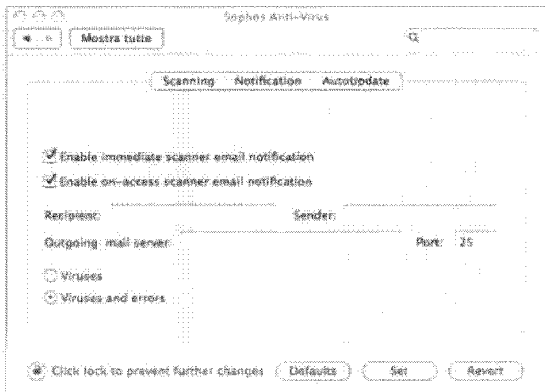
—Silvio Umberto Zanzi



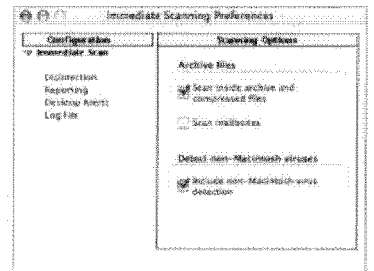
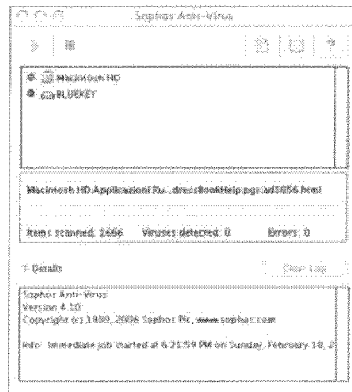
Pannello per la configurazione di Sophos Anti-Virus



Configurazione dei dettagli di rete per gli aggiornamenti



Impostazione dei dettagli della notifica e-mail



Opzioni di scansione

Scansione del disco di sistema