



GFI WebMonitor

for ISA Server

Monitoraggio di HTTP ed FTP in tempo reale, antivirus e controllo di accesso

Una ricerca a cura di IDC dimostra che fino al 40% dell'attività internet dei dipendenti non è correlata al lavoro. Come amministratori di rete, si ha bisogno di strumenti per controllare le attività di navigazione su internet dei dipendenti e di garantire che tutti i file scaricati siano esenti da virus o altri codici maligni. GFI WebMonitor for ISA Server aumenta la produttività dei dipendenti, offrendo agli amministratori il controllo in tempo reale sugli utenti che navigano o scaricano file.

GFI WebMonitor è provvisto di WebGrade, un database di classificazione di siti, analizzati al 100% da persone, che offre il controllo sui siti che gli utenti possono esplorare e di bloccare l'accesso a siti web rientranti in determinate categorie, ad esempio, siti web per adulti, di giochi on line, delle email personali, P2P, Facebook, Myspace, di viaggi e molto altro.

GFI WebMonitor consente di monitorare quali file sono scaricati dai dipendenti, di bloccare determinati tipi di file, per esempio i file mp3, e di eseguire la scansione di tutti i file alla ricerca di virus, spyware e malware (codici maligni) tramite diversi motori antivirus. GFI WebMonitor abbassa il rischio di ingegneria sociale, bloccando l'accesso a siti web di phishing tramite il ricorso a un database, aggiornabile automaticamente, di URL di phishing.

GFI WebMonitor for ISA Server è disponibile in 3 edizioni:

- **L'edizione WebFilter**, che include il filtraggio degli indirizzi URL e la classificazione dei siti web.
- **L'edizione WebSecurity**, che prevede la scansione antivirus, antiphishing e spyware.
- **L'edizione UnifiedProtection**, che combina l'edizione WebFilter con l'edizione WebSecurity.

Tutte le edizioni supportano Microsoft ISA Server 2004 e Microsoft ISA Server 2006.

Caratteristiche di GFI WebMonitor – Edizione WebFilter

■ Attenuazione della responsabilità legale

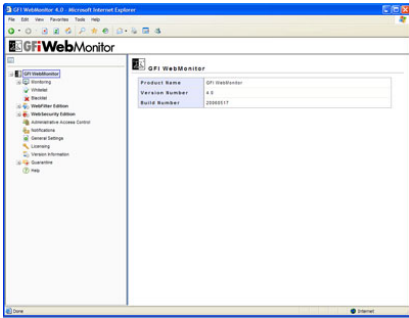
Senza la possibilità di esercitare una qualche forma di controllo su ciò che viene esplorato dai propri utenti, si può essere esposti ad azioni legali. I dipendenti possono richiedere un risarcimento danni all'azienda se non si è dimostrata la dovuta diligenza nel predisporre un ambiente di lavoro esente da molestie. A questo scopo, si devono installare strumenti che consentano di bloccare, o almeno monitorare, l'accesso ai siti web dal contenuto inopportuno, come siti pornografici o altri siti per adulti.

Benefici

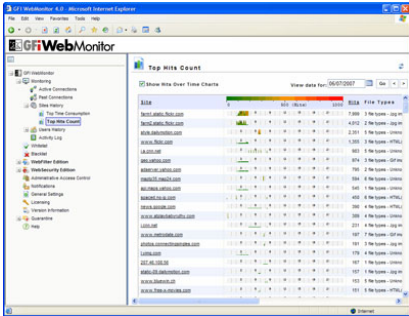
Perché adoperare GFI WebMonitor?

- Per migliorare la produttività attraverso il controllo delle abitudini di navigazione dei propri dipendenti
- Per proteggere in tempo reale la rete da download pericolosi
- Per ridurre il cyberslacking, cioè l'attività di navigazione su internet a fini personali da parte dei dipendenti durante l'orario di lavoro
- Per impedire o prevenire la fuga di informazioni attraverso siti web di ingegneria sociale
- Per trarre vantaggio dai diversi motori di scansione, in modo da garantire che i file scaricati siano esenti da virus o altri codici maligni.

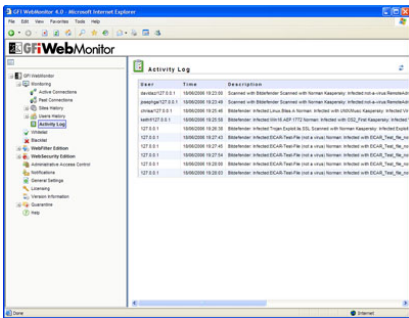
Caratteristiche di GFI WebMonitor - Edizione WebSecurity



Videata principale di GFI WebMonitor

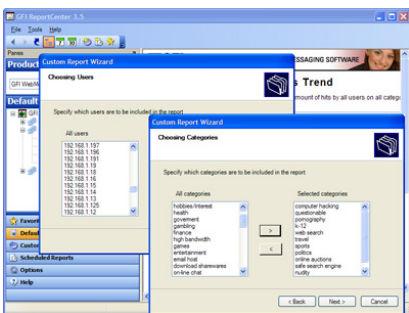


Controllo delle connessioni e presentazione di statistiche



Controllo dell'attività online degli utenti

GFI WebMonitor ReportPack



Personalizzazione guidata dei rapporti



Elenco dei rapporti predefiniti

■ Scansione dei file scaricati, grazie a diversi motori antivirus

GFI WebMonitor adopera più scanner antivirus per eseguire la scansione dei file in corso di scaricamento. L'utilizzo di più scanner riduce drasticamente il tempo medio di ottenimento delle firme antivirus che combattono le minacce più recenti, cioè riduce notevolmente le probabilità d'infezione. Una singola azienda antivirus, infatti, non potrà mai essere SEMPRE la più rapida a rispondere. In occasione di ogni attacco, le aziende di antivirus rispondono in tempi diversi, a seconda del luogo in cui il virus è stato scoperto, ecc. L'utilizzo di più motori antivirus aumenta le probabilità di disporre di almeno un motore aggiornato e quindi in grado di proteggere dai virus più recenti. Inoltre, poiché ogni motore è dotato di euristiche e metodi propri, mentre un motore antivirus può essere in grado di scoprire un determinato virus e le sue varianti, un altro motore antivirus può fare altrettanto con un virus diverso. Presi nel complesso, più motori antivirus equivalgono a una migliore protezione.

■ Protezione antivirus con Norman Virus Control e BitDefender

GFI WebMonitor è venduto in un unico pacchetto con Norman Virus Control e BitDefender. Norman Virus Control è un motore antivirus di applicazione industriale che ha ricevuto il premio "100% Virus Bulletin" per 19 volte consecutive. È inoltre provvisto delle certificazioni ICSA e Checkmark. BitDefender è un motore antivirus rapido e flessibile, e primeggia per il numero di formati che è in grado di riconoscere e sottoporre a scansione. BitDefender è provvisto della certificazione ICSA e ha vinto il premio 100% Virus Bulletin e innumerevoli riconoscimenti per la sua protezione impeccabile. GFI WebMonitor controlla e aggiorna in modo automatico i file di definizione di Norman Virus Control e BitDefender non appena questi si rendono disponibili. Il prezzo di GFI WebMonitor comprende aggiornamenti per un anno.

■ Blocco di codici maligni (trojan, spyware, ecc.) tramite Kaspersky (facoltativo)

Per ottenere una protezione persino maggiore e trarre vantaggio dalla scansione ottenuta con più motori antivirus, gli utenti hanno la facoltà di aggiungere il motore antivirus Kaspersky SuperSecure, disponibile come componente aggiuntivo facoltativo. Il database di Kaspersky SuperSecure presenta la funzionalità di scoperta dei software maligni in grado di eseguire l'amministrazione da remoto, lo spionaggio della tastiera, la scoperta di password, la connessione automatica a siti a pagamento, lo scaricamento automatico di file contenenti materiale esplicito e molto altro. GFI WebMonitor controlla e aggiorna in modo automatico i file di definizione di Kaspersky non appena si rendono disponibili.

■ Protezione dai siti web di phishing di ingegneria sociale

Il phishing è una tecnica di ingegneria sociale utilizzata in modo disonesto dagli hacker per acquisire informazioni quali nomi utenti, password e dettagli su carte di credito, facendo credere agli utenti che stanno trasferendo tali dati alla vera società. I siti web delle società di shopping on line e di carte di credito sono tra quelli più bersagliati in termini di phishing. GFI WebMonitor protegge gli utenti dai possibili rischi dell'ingegneria sociale bloccando l'accesso ai siti web di phishing, grazie a un database di URL di phishing, che si autoaggiorna.

■ Controllo dei tipi di file che gli utenti possono scaricare

Si possono creare più criteri di controllo dei download, basati su utenti, gruppi e IP, al fine di bloccare lo scaricamento di determinati tipi di file (ad esempio, Javascript, MP3, MPEG, exe, e altri) da parte di particolari utenti. File pericolosi, come i programmi di scaricamento trojan, spesso tentano di penetrare in un sistema mascherati da file innocui. GFI WebMonitor si avvale del suo scanner interno di controllo della firma di file per analizzare e individuare le firme del VERO tipo di file HTTP e FTP scaricati.

Caratteristiche di GFI WebMonitor - Edizione UnifiedProtection (funzionalità comuni)

Le seguenti caratteristiche sono disponibili in tutte le edizioni.

■ Monitoraggio o blocco di una connessione in tempo reale

Gli amministratori sono in grado di vedere i siti web esplorati e i file scaricati in quel momento dagli utenti. È possibile bloccare con facilità connessioni, sessioni di navigazione o download attivi, facendo semplicemente clic sull'icona "Blocca connessione". Ad esempio, si può decidere di interrompere il download di un grosso file che l'utente sta scaricando in quel momento.

■ Monitoraggio e blocco dello scaricamento nascosto di applicazioni

Alcune applicazioni software si connettono automaticamente alle loro home page per scaricare gli aggiornamenti servendosi del tunnelling HTTP. Benché questo possa ridurre la quantità di amministrazione, può anche rappresentare un rischio di sicurezza, in quanto applicazioni sconosciute o trojan possono avvalersi della stessa tecnica per scaricare file pericolosi sul PC di un utente, compresi spyware, adware e software pornografici, all'insaputa dell'utente stesso. GFI WebMonitor consente di controllare i siti cui è consentito distribuire gli aggiornamenti (ad esempio, www.microsoft.com).

■ Controllo della larghezza di banda

Attraverso le funzioni di monitoraggio della larghezza di banda del sito e dell'utente, l'amministratore ha la facoltà di tener traccia del traffico scaricato e caricato e del numero di hit di URL (visite a siti) nel tempo, per utente o per sito web. Il monitoraggio in tempo reale può essere ottenuto con rapporti di drill-down, muniti da grafici, visualizzati nell'interfaccia utente.

■ Possibilità di consentire eccezioni attraverso le blacklist e le whitelist

È possibile aggiungere qualsiasi URL, utente o IP alle whitelist o blacklist, temporaneamente o in modo definitivo, al fine di superare tutti i criteri di filtraggio e sicurezza del web. Ad esempio, si può voler concedere a un determinato utente solo l'accesso temporaneo al suo account di webmail personale per un periodo di tempo specificato.

■ Accesso controllato alle interfacce di configurazione e monitoraggio

GFI WebMonitor consente di selezionare gli utenti che possono avere accesso alle sue interfacce di configurazione e monitoraggio. Si possono attribuire tali diritti in base all'IP del computer da cui viene effettuato l'accesso ovvero tramite il nome utente autenticato dal dominio del client che prova a caricare la configurazione. L'accesso verrà conferito unicamente agli utenti presenti nell'elenco di utenti e/o IP autorizzati di GFI WebMonitor.

Requisiti di sistema

- Sistemi operativi Windows 2000 (SP4) e 2003
- Microsoft ISA Server 2004 o successivi
- Internet Explorer 6 o successivi
- .NET Framework 2.0.

Premi



Scaricate la copia di valutazione da <http://www.gfi-italia.com/italia/webmon/>

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

GFI
www.gfi.com