



GFI EndPointSecurity

Controllo completo sull'utilizzo di iPod, stick USB e altri dispositivi portatili

GFI EndPointSecurity consente agli amministratori di gestire attivamente l'accesso degli utenti e di registrare l'attività di:

- riproduttori di file multimediali, compresi iPod, Creative Zen e altri
- unità USB, CompactFlash, schede di memoria, CD, floppy e altri dispositivi di memoria portatili
- PDA, palmari BlackBerry, telefoni cellulari, smartphone e dispositivi di comunicazione analoghi
- schede di rete, computer portatili e altre connessioni di rete.

■ Modalità di funzionamento

Per controllare l'accesso, GFI EndPointSecurity installa un piccolo agente di area di impronta sul computer. L'agente occupa solo 1,2 MB di memoria: l'utente non verrà a mai a sapere che è lì. GFI EndPointSecurity incorpora uno strumento di distribuzione da remoto basato sulla tecnologia di GFI LANguard, che consente di distribuire l'agente su centinaia di computer con soli pochi clic del mouse. Dopo l'installazione, l'agente interroga Active Directory quando l'utente si collega e, di conseguenza, imposta le autorizzazioni ai vari nodi. Se l'utente non fa parte di un gruppo al quale è consentito l'accesso, detto accesso al dispositivo viene bloccato.

Benefici

Perché scegliere GFI EndPointSecurity?

- Per impedire la fuga o il furto di dati attraverso un controllo completo dell'accesso ai dispositivi di memoria portatile, impiegando uno sforzo di amministrazione minimo
- Per impedire l'introduzione di malware o di software non autorizzati sulla rete
- Perché offre agli amministratori un maggiore controllo, grazie alla possibilità di bloccare i dispositivi per categoria, estensione del file, porta fisica o ID del dispositivo
- Perché consente agli amministratori di concedere l'accesso temporaneo al dispositivo o a una porta per un dato intervallo temporale
- Compatibilità con piattaforme a 32 e 64 bit, comprese Windows Vista e l'ultima RC di Windows Server 2008.

■ Controllo dell'accesso utente e protezione della rete dalle minacce rappresentate dai supporti di memoria portatili

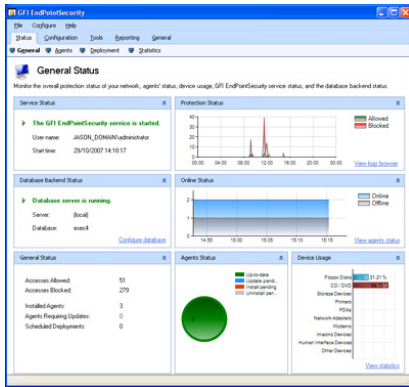
L'utilizzo di GFI EndPointSecurity consente, a livello centrale, di disabilitare gli utenti dall'accesso ai supporti di memoria portatili, impedendo agli utenti di sottrarre illecitamente dati o di introdurre altri che potrebbero nuocere alla rete, quali virus, trojan e altro malware. Benché sia possibile disattivare l'accesso a dispositivi di memoria portatili come CD e/o floppy dal BIOS, in realtà questa soluzione non è pratica; infatti, ci si dovrebbe recare fisicamente presso il computer per disattivare temporaneamente la protezione e installare eventuali software. Inoltre, gli utenti esperti sono in grado di manipolare il BIOS. GFI EndPointSecurity consente di controllare una vasta gamma di dispositivi, compresi:

- floppy disk
- CD e DVD ROM
- iPod
- dispositivi di memoria
- stampanti
- PDA
- adattatori di rete
- modem
- dispositivi per l'acquisizione di immagini
- e molto altro!

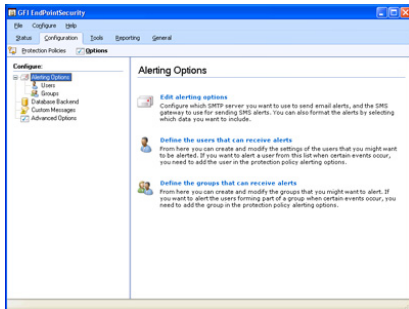
■ Registrazione dell'attività di supporti di memoria portatili, come stick di memoria USB, schede SD e molto altro

Gli stick USB costituiscono una delle principali minacce perché sono piccoli, possono essere occultati facilmente e sono in grado di immagazzinare fino a 4 GB di dati. Ad esempio, il collegamento di una macchina fotografica digitale a una porta USB dà modo agli utenti di memorizzare dati su una scheda SD; le schede SD sono disponibili in diverse dimensioni, compresi 2 GB e superiori. Oltre a bloccare l'accesso a supporti di memoria portatili, GFI EndPointSecurity registra l'attività utente correlata al dispositivo, sia sul log dell'evento sia su un Server SQL centrale. Ogni volta che un utente collega un dispositivo alla rete, viene registrato un elenco dei file cui è stato effettuato l'accesso o che sono stati letti o copiati.

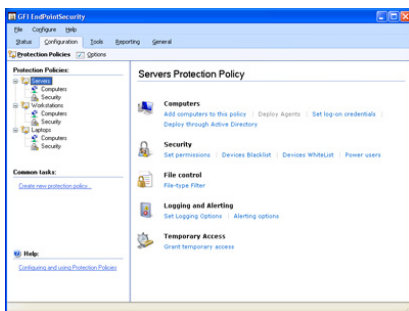
GFI EndPointSecurity



Consolle di gestione di GFI EndPointSecurity

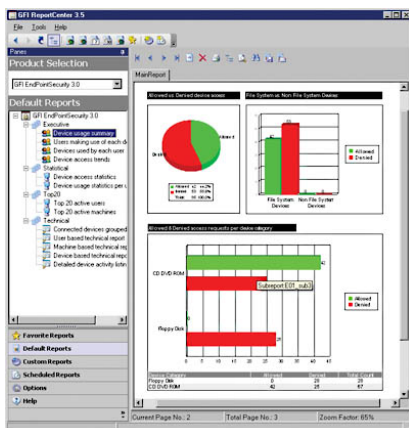


Opzioni di configurazione di GFI EndPointSecurity



Criteri di protezione predefiniti

GFI EndPointSecurity ReportPack



Rapporto sull'utilizzo del dispositivo

Facile configurazione del controllo di protezione basato su gruppi, grazie ad Active Directory

È possibile configurare e classificare i computer in gruppi di protezione diversi: per ogni gruppo è possibile indicare livelli di protezione e dispositivi diversi ai quali consentire o negare l'accesso. Inoltre, si può sfruttare il potere dei gruppi e rendere membro del gruppo un intero reparto o ufficio, modificando con facilità le impostazioni per l'intero gruppo. La configurazione di GFI EndPointSecurity è facile, sfrutta la potenza di Active Directory e non richiede all'amministratore di ricordare e tener traccia dei criteri distribuiti sui vari computer. Altri software di controllo delle memorie richiedono una ponderosa amministrazione per ogni computer, obbligando a effettuare modifiche per singolo computer e ad aggiornare la configurazione su ognuno di essi prima che le impostazioni abbiano effetto.

Controllo di accesso granulare avanzato, whitelist e blacklist

GFI EndPointSecurity consente di autorizzare o negare l'accesso a una gamma di categorie di dispositivi, nonché di bloccare il trasferimento di file in base all'estensione del nome file, alla porta fisica o all'ID del dispositivo (l'ID attribuito dal produttore riportato sull'etichetta di tutti i dispositivi). È inoltre possibile specificare gli utenti o i gruppi che devono sempre avere pieno accesso ai dispositivi. GFI EndPointSecurity consente altresì agli amministratori di definire whitelist e blacklist di dispositivi, al fine di autorizzare l'accesso solo a dispositivi aziendali e di bloccare tutti gli altri.

Monitoraggio dello stato e avvisi in tempo reale

GFI EndPointSecurity fornisce il monitoraggio dello stato del dispositivo in tempo reale, attraverso la sua interfaccia utente che visualizza i dati statistici per mezzo di grafici, lo stato dell'agente in diretta e molto altro. GFI EndPointSecurity permette inoltre di inviare avvisi quando vengono collegati alla rete dei dispositivi specifici. È possibile inviare gli avvisi a uno o più destinatari via email, messaggi di rete e notifiche SMS inviate tramite un gateway o servizio email verso sms.

Rapporti completi sull'utilizzo del dispositivo con il componente aggiuntivo ReportPack di GFI

Il ReportPack di GFI EndPointSecurity rappresenta un prodotto complementare, del tutto sviluppato, per GFI EndPointSecurity. Questo pacchetto di reporting può essere programmato per generare, in maniera automatica, rapporti grafici per il personale tecnico informatico e dirigente, sulla base dei dati raccolti da GFI EndPointSecurity, consentendo così di ottenere rapporti sui dispositivi connessi alla rete, sull'attività endpoint dell'utente, sui file copiati da e verso i dispositivi (compresi i veri nomi dei file copiati) e molto altro.

Facile agente di distribuzione che non ha bisogno di amministrazione

GFI EndPointSecurity offre agli amministratori la possibilità di programmare la distribuzione automatica dell'agente successivamente all'implementazione di modifiche di criteri o di configurazione. Nel caso in cui una distribuzione non dovesse riuscire, viene riprogrammata finché non è distribuita correttamente. Inoltre, lo strumento di distribuzione da remoto di GFI EndPointSecurity è in grado di distribuire l'agente su tutta la rete in pochi minuti. GFI EndPointSecurity permette inoltre la distribuzione di Active Directory tramite MSI.

■ Accesso temporaneo al dispositivo

È possibile concedere agli utenti un accesso temporaneo a un dispositivo (o gruppo di dispositivi) su un determinato computer e per un periodo di tempo dato. Tale autorizzazione può essere concessa persino se l'agente di GFI EndPointSecurity non è collegato alla rete!

■ Altre caratteristiche:

- Scansione e rilevamento di un elenco di dispositivi usati in passato o ancora in uso
- Agenti protetti da password per evitare manomissioni
- Impostazione messaggi pop-up personalizzati destinati agli utenti cui si blocca l'accesso a un dispositivo
- Esplorazione di log dell'attività utente e dell'utilizzo dispositivo attraverso un database terminale
- Funzione di manutenzione che consente di eliminare le informazioni più vecchie di un certo numero di giorni
- Compatibilità con sistemi operativi in qualsiasi lingua aderente al linguaggio Unicode

■ Molti altri ci hanno scelto...

Molte aziende importanti hanno scelto GFI EndPointSecurity. Ecco solo alcuni esempi: Best Western Sterling Inn, Fair Trades Ltd, Central Highlands Water, Aurum Funds e molte altre.

Requisiti di sistema

- Sistema operativo: Windows 2000 (SP4), XP, 2003, Vista e 2008 (versioni a 86 e 64 bit)
- Internet Explorer 5.5 o successivi
- .NET Framework versione 2.0.
- Terminale database: SQL Server 2000, 2005, 2008
- Porta: TCP 1116 (predefinita)

Premi



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

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