



GFI EndPointSecurity

Controllo su tutta la rete 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
- PDA, palmari Blackberry, telefoni cellulari 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 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 bloccare il furto di dati mediante il controllo totale dell'accesso a dispositivi di memoria portatili quali schede di memoria, CD, unità USB e altro
- Per prevenire l'introduzione di virus e software non autorizzati, mediante il controllo di tutti i dispositivi collegabili ai punti finali, come PDA, computer portatili e altro
- Per consentire agli amministratori di esercitare il controllo, basato su gruppi, su un'ampia rete di dispositivi portatili senza, tuttavia, che ne risentano gli utenti autorizzati
- Per impedire la perdita di produttività, attraverso il blocco del caricamento non autorizzato di giochi e altri file personali dai dispositivi di memoria portatili
- Perché è provvisto di tre criteri di protezione: per computer portatili, stazioni di lavoro e server.

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

L'utilizzo di GFI EndPointSecurity consente di disabilitare, a livello centrale, 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!

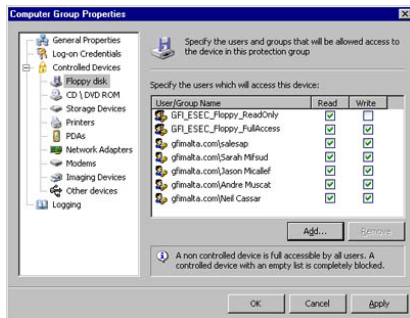
■ Registrazione dell'attività di supporti di memoria portatili, come stick di memoria USB, schede SD e molto altro

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 ad 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. Ogniquale volta un utente collega un dispositivo alla rete, viene registrato un elenco dei file cui è stato effettuato l'accesso o che sono stati trasferiti da e verso il dispositivo.

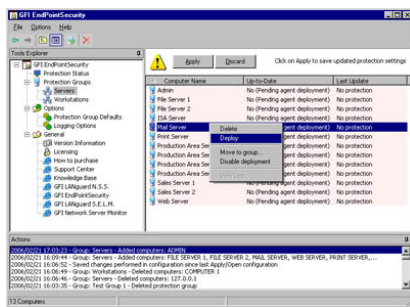
GFI EndPointSecurity



Configurazione di GFI EndPointSecurity

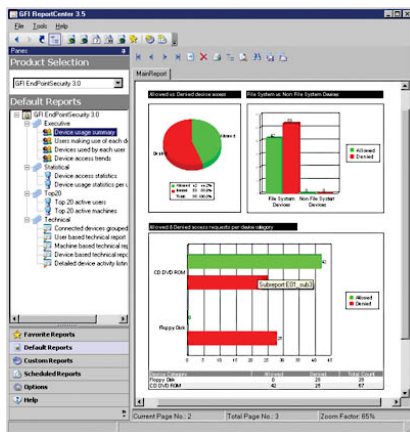


Consenso o rifiuto dell'accesso ai gruppi di Active Directory



Facile distribuzione di agenti su tutta rete

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 le impostazioni per l'intero gruppo con facilità. La configurazione di GFI EndPointSecurity è facile, sfrutta il potere 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 ad effettuare modifiche per singolo computer e ad aggiornare la configurazione su ognuno di essi prima che le impostazioni abbiano effetto.

■ Controllo di accesso granulare

GFI EndPointSecurity consente di autorizzare o negare l'accesso ad un dispositivo e di attribuire privilegi di sola lettura o di accesso completo (ove applicabile) su ogni dispositivo supportato (ad esempio, PDA), utente per utente.

■ 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'andamento dell'utilizzo del dispositivo, sui file copiati da e verso i dispositivi (compresi i veri nomi di file copiati) e molto altro.

■ Incorporazione di uno strumento di distribuzione remoto

Lo strumento di distribuzione remoto di GFI EndPointSecurity è in grado di distribuire l'agente su tutta la rete in pochi minuti. Si può configurare la distribuzione su tutto il dominio, per singolo computer o per un elenco di computer.

■ Controllo centralizzato che agevola l'accesso temporaneo

Poiché è facile aggiungere o rimuovere un utente da un gruppo con Active Directory, diventa semplice concedere l'accesso temporaneo a supporti rimovibili, floppy o CD. L'accesso temporaneo può essere necessario in alcune occasioni, ma questo non deve comportare l'impossibilità di controllare l'accesso al di là di tali periodi.

■ Altre caratteristiche:

- Supporto di sistemi operativi in qualsiasi linguaggio aderente a 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.