



GFI EndPointSecurity

Śledź wykorzystywanie przenośnych urządzeń magazynujących takich jak karty pamięci USB, karty SD i inne

GFI EndPointSecurity pozwala administratorom odnotowywać działania i zarządzać dostępem użytkowników do takich urządzeń jak:

- odtwarzacze multimedów, np iPod, Creative Zen i inne
- pamięci USB, CompactFlash, karty pamięci, płyty CD, dyskietki i inne przenośne urządzenia magazynujące
- PDA, komputery przenośne BlackBerry, telefony komórkowe i podobne urządzenia komunikacyjne
- karty sieciowe, laptopy i inne urządzenia sieciowe

■ Jak to działa

Aby kontrolować dostęp, GFI EndPointSecurity instaluje mały serwis monitorujący na komputerze. Usługa zajmuje zaledwie 1,2 MB więc użytkownik nawet nie dostrzeże jej działania. GFI EndPointSecurity zawiera narzędzie zdalnego rozmieszczania oparte na technologii GFI LANguard pozwalające na rozlokowanie serwisu na setkach komputerów przez wykonanie zaledwie kilku kliknięć. Po instalacji serwis pyta usługę Active Directory o zalogowanego użytkownika i zezwala na korzystanie z odpowiedniego węzła. Jeśli użytkownik nie należy do grupy posiadającej dostęp do danego urządzenia, dostęp zostaje zablokowany.

Korzyści

Dlaczego GFI EndPointSecurity?

Uniemożliwia wewnętrzną kradzież danych przez pełną kontrolę urządzeń przenośnych jak karty pamięci, pamięci USB i inne

Zapobiega wprowadzaniu wirusów i nieautoryzowanego oprogramowania przez kontrolę nad wszystkimi podłączanymi urządzeniami jak PDA, laptopy i inne

Pozwala administratorom sprawować kontrolę nad grupami o różnym poziomie dostępu do danych bez ingerowania w działania użytkowników z pełnym dostępem

Zapobiega obniżaniu produktywności pracowników wynikającej z instalowania gier i innych prywatnychplików z nośników przenośnych

Trójkierunkowa polityka ochrony: dla laptopów, komputerów stacjonarnych i serwerów

■ Kontroluj dostęp użytkowników i chroń swoją sieć przed zagrożeniami ze strony urządzeń przenośnych.

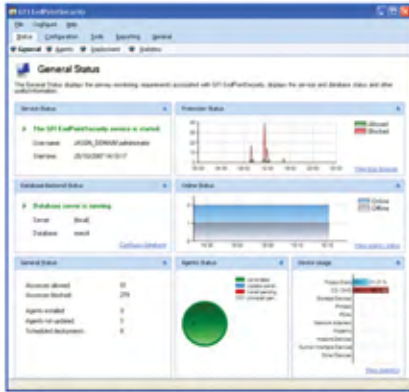
Za pomocą GFI EndPointSecurity można uniemożliwić użytkownikom sieci korzystanie z przenośnych odtwarzaczy mediów i zapobiec wnoszeniu i wynoszeniu danych szkodliwych dla sieci, takich jak wirusy, trojany i szkodliwe oprogramowanie. Pomimo że możliwe jest zablokowanie korzystania z urządzeń magazynujących takich jak CD czy dyskietki z poziomu BIOSu, to jest to rozwiązanie niepraktyczne: Należałoby wówczas fizycznie znaleźć się przy każdym komputerze, aby tymczasowo wyłączyć ochronę i zainstalować oprogramowanie. W dodatku doświadczeni użytkownicy mogliby sami ingerować w BIOS. GFI EndPointSecurity pozwala na kontrolowanie szerokiej gamy urządzeń takich jak:

- Dyskietki
- Płyty CD i DVD
- iPody
- pamięci przenośne
- drukarki
- PDA
- Adaptery sieciowe
- Modemy
- Aparaty fotograficzne i kamery
- i wiele innych!

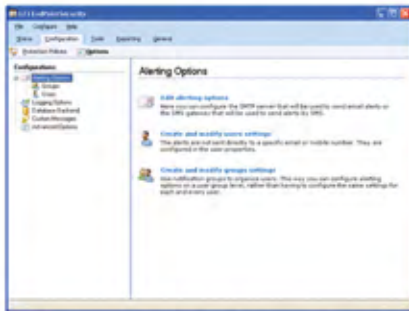
■ Wykrywa aktywność urządzeń przenośnych jak USB, karty pamięci SD i inne

Pamięci USB są jednym z głównych zagrożeń gdyż są małe, łatwo je ukryć i mogą pomieścić do 4 GB danych. Dla przykładu, podłączając aparat cyfrowy do portu USB dajemy dostęp do pamięci o dużej pojemności; karty SD są dostępne w kilku pojemnościach, włączając 2 GB i więcej. Oprócz blokowania dostępu do kart pamięci, GFI EndPointSecurity odnotowuje także przypadki używania urządzenia zarówno w rejestrze zdarzeń, jak i na serwer w SQL. Lista plików, na których wykonywano operacje (odczytywanie/zapisywanie) na urządzeniu jest zapisywana zawsze kiedy użytkownik włącza urządzenie do sieci.

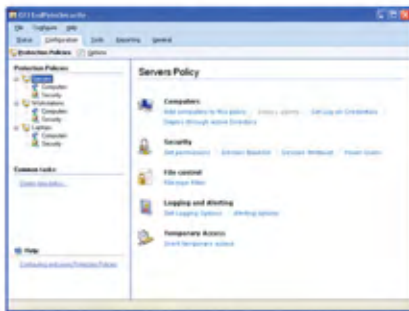
GFI EndPointSecurity



GFI EndPointSecurity Management Console

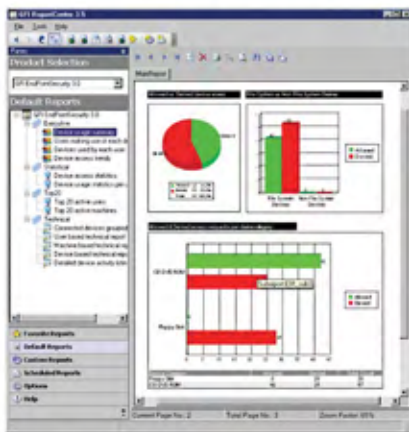


GFI EndPointSecurity configuration options



Default protection policies

GFI EndPointSecurity ReportPack



Device usage report

■ Łatwa konfiguracja kontroli grupowej przez Active Directory

Komputery można konfigurować i kategoryzować w oparciu o przynależność do różnych grup ochrony: Dla każdej grupy można określić inny poziom ochrony i zakres urządzeń jakie mogą być wykorzystywane. Można również modyfikować stopień ochrony dla grupy i stworzyć z wszystkich pracowników danego departamentu jedną grupę aby łatwo dostosowywać ustawienia dla wszystkich jej użytkowników jednocześnie. Konfiguracja GFI EndPointSecurity jest łatwa, a wpływanie na Active Directory nie wymaga od administratora śledzenia polityki bezpieczeństwa przypisanej do każdego komputera. Inne oprogramowanie kontrolujące urządzenia magazynujące wymagają kłopotliwego administrowania każdym komputerem oddzielnie, zmuszając do konfigurowania wszystkich jednostek zanim nowe ustawienia będą działały.

■ Śledź wykorzystywanie przenośnych urządzeń magazynujących takich jak karty pamięci USB, karty SD i inne

Pamięci USB są jednym z głównych zagrożeń gdyż są małe, łatwo je ukryć i mogą pomieścić do 4 GB danych. Dla przykładu, podłączając aparat cyfrowy do portu USB dajemy dostęp do pamięci o dużej pojemności; karty SD są dostępne w kilku pojemnościach, włączając 2 GB i więcej. Oprócz blokowania dostępu do kart pamięci, GFI EndPointSecurity odnotowuje także przypadki używania urządzenia zarówno w rejestrze zdarzeń, jak i na serwerze SQL. Lista plików, na których wykonywano operacje (odczytywanie lub zapisywanie) na urządzeniu jest zapisywana zawsze kiedy użytkownik włącza urządzenie do sieci.

■ Granularna kontrola dostępu

GFI EndPointSecurity pozwala dopuszczać lub odmawiać dostępu do urządzenia, jak również nadawać pełne uprawnienia lub tylko do odczytu przy każdym obsługiwany urządzeniu (jak PDA) spersonalizowane dla każdego użytkownika.

■ Scentralizowana kontrola ułatwiająca tymczasowy dostęp

Czasowy dostęp może być czasem konieczny, ale nie musi oznaczać utraty kontroli przez resztę czasu. Ze względu na łatwość dodawania/usuwania użytkownika z grupy w Active Directory, można zezwolić na tymczasowy dostęp użytkownika do przenośnych urządzeń lub dysków.

■ Zdalny dostęp

Narzędzia zdalnego dostępu GFI EndPointSecurity umożliwiają konfigurowanie komputerów w całej sieci w przeciągu zaledwie kilku minut. Konfiguracja może odbywać się dla całej domeny, pojedynczych komputerów lub listy jednostek.

■ Pozostałe cechy

Wsparcie dla każdego system operartego w języku zgodnym z Unicode.

■ Jesteś w dobrym towarzystwie

Wiele czołowych firm wybrało GFI EndPointSecurity. Pośród nich: Best Western Sterling Inn, Fair Trades Ltd, Central Highlands Water, Aurum Funds i wiele innych.

Wymagania systemowe

- Operating system: Windows 2000 (SP4), XP, 2003, Vista and 2008 (x86 and x64 versions)
- Internet Explorer 5.5 or later
- .NET Framework version 2.0
- Database Backend: SQL Server 2000, 2005, 2008
- Port: TCP port 1116 (default).

Nagrody



Pobierz wersję testową z <http://www.gfi.com/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

ed&r Polska SP. z o.o.
Biuro Handlowe
ul. Nowy Świat 32/106
Lublin 20 - 418
PL
Tel. +48/ 81/ 534-83-25
Fax. +48/ 81/ 534-83-26
gfi@edr.pl

