



# GFI WebMonitor

for ISA Server

Monitoring HTTP/FTP w czasie rzeczywistym, anty-wirus i kontrola dostępu

Badania przeprowadzone przez IDC pokazują, że aż do 40% czasu poświęconego przez pracowników na pracę przy Internecie jest niezwiązana z obowiązkami służbowymi. Jako administrator sieci jesteś zobowiązany także do kontrolowania czynności związanych z korzystaniem przez pracowników z sieci, aby mieć pewność, że ściągane pliki są wolne od wirusów i szkodliwego oprogramowania. GFI WebMonitor dla ISA Server zwiększa produktywność pracowników dając możliwość kontrolowania w czasie rzeczywistym co pracownicy robią w sieci.

GFI WebMonitor jest dostarczany z bazą WebGrade, w 100% sprawdzoną przez człowieka bazą danych skategoryzowanych stron internetowych, która daje Ci kontrolę nad tym co robią w Internecie pracownicy i blokowania dostępu do wybranych treści, takich jak: strony „tylko dla dorosłych”, gry on-line, osobiste skrzynki mailowe, P2P, Facebook, Myspace, portali podróżniczych i innych.

GFI WebMonitor pozwala monitorować jakie pliki pracownicy pobierają z Internetu, aby blokować pliki typu mp3 i skanować wszystkie pliki pod kątem wirusów i złośliwego oprogramowania za pomocą wielokrotnych silników anty-wirusowych. GFI WebMonitor obniża także ryzyko ulegnięcia socjotechnikom przez blokowanie dostępu do phishingowych stron dzięki użyciu automatycznie uaktualnianej bazy danych phishingowych adresów URL.

## ■ Ochrona sieci przed atakami wirusów, spyware, malware i phishingu

GFI WebMonitor pozwala monitorować jakie pliki pracownicy pobierają z Internetu, aby blokować pliki typu mp3 i skanować wszystkie pliki pod kątem wirusów i złośliwego oprogramowania za pomocą wielokrotnych silników anty-wirusowych. GFI WebMonitor obniża także ryzyko ulegnięcia socjotechnikom przez blokowanie dostępu do phishingowych stron dzięki użyciu automatycznie uaktualnianej bazy danych phishingowych adresów URL.

GFI WebMonitor dla ISA Server jest dostępny w 3 edycjach:

- **WebFilter Edition:** zawiera filtrowanie URL i kategoryzację stron.
- **WebSecurity Edition:** zawiera moduł anty-wirusowy, anty-phishingowy i anty-szpiegowski.
- **UnifiedProtection Edition:** łączy w sobie WebFilter Edition i WebSecurity Edition.

Wszystkie wersje obsługują Microsoft ISA Server 2004 i Microsoft ISA Server 2006.

## Korzyści

### Dlaczego stosować GFI WebMonitor?

**Wzrost produktywności przez kontrolowanie zwyczajów korzystania z sieci**

**Ochrona sieci w czasie rzeczywistym przed niebezpiecznym ściąganiem**

**Ograniczenie cyberslacking-u - marnowanie przez pracowników czasu w sieci**

**Zapobieganie wyciekom danych przez strony manipulujące socjotechnikami**

**Korzyści z wielokrotnych silników skanujących zapewniają bezpieczeństwo pobieranych plików od wirusów i szkodliwych programów.**

## Cechy GFI WebMonitor - WebFilter Edition

### ■ Filtrowanie przeglądanych stron za pomocą bazy danych WebGrade

GFI WebMonitor pozwala kontrolować odwiedzanie przez pracowników stron internetowych. Korzystając z WebGrade Database – w pełni zweryfikowanej przez ludzi filtrującej bazy danych – firmy mogą dokładnie blokować dostęp pracowników do milionów niewłaściwych stron takich jak strony „tylko dla dorosłych”, gry on-line, osobiste skrzynki mailowe, P2P, Facebook, Myspace, portali podróżniczych i innych. Możesz ustawić opcje filtrowania w oparciu o użytkownika/grupę/IP zgodnie z polityką dostępu do danej kategorii treści. Na przykład, możesz zablokować dostęp użytkowników do stron z wiadomościami lub stron obciążających przepustowość zawarty na nich streaming. Strony mogą być albo całkowicie zablokowane, albo dopuszczane po uprzednim powiadomieniu użytkownika o blokadzie.

### ■ Programowalne filtrowanie

Każde ustawienie filtrowania może być zaplanowane zgodnie z harmonogramem czasowym. Oznacza to, że administrator może konfigurować produkt tak aby był dostosowany do każdego użytkownika/grupy i pozwalał na dostęp do stron z wiadomościami, rozrywką itd. poza godzinami pracy lub w określonych przedziałach czasowych.

### ■ Obniżanie odpowiedzialności cywilnej

Bez możliwości regulowania kontroli nad treściami do których dostęp mają użytkownicy sieci, możesz być narażony na pozew sądowy. Pracownicy mogą domagać się zadośćuczynienia za niedołożenie starań w stworzeniu środowiska pracy wolnego od nękania. Aby tego dopilnować musisz zainstalować narzędzia pozwalające na blokowanie, lub przynajmniej monitorowanie, nieodpowiednich zawartości takich jak pornografia lub strony „tylko dla dorosłych”.

## Cechy GFI WebMonitor - WebSecurity Edition

### ■ Skanowanie ściągniętych plików przez wielokrotne silniki

GFI WebMonitor wykorzystuje wielokrotne skanery anty-wirusowe sprawdzające pobrane pliki. Zastosowanie skanowania wielokrotnego drastycznie ogranicza średni czas otrzymania sygnatur wirusów, które zwalczają najnowsze zagrożenia i znacznie ograniczają ryzyko infekcji. Jest to spowodowane tym, że pojedyncze skanowanie nigdy nie będzie najszybsze w reagowaniu. Dla każdej epidemii, firmy zajmujące się wirusami mają różny czas reakcji na danego wirusa, w zależności od tego gdzie został on wykryty itd. Stosując wielokrotne skanowanie mamy większe szanse na to, że nasz silnik anty-wirusowy będzie obecny w najnowszej wersji. Dodatkowo, ponieważ każdy silnik ma swoją własną heurystykę i metody, jeden silnik może być lepszy w wykrywaniu danego wirusa i jego odmian, a drugi w wykrywaniu innego. Tak więc, im więcej silników tym lepsza ochrona.

### ■ Ochrona anty-wirusowa dzięki Norman Virus Control i BitDefender

GFI WebMonitor jest skojarzony z Norman Virus Control i BitDefender-em. Norman Virus Control jest silnikiem anty-wirusowym, który otrzymał nagrodę 100% Virus Bulletin 32 razy z rzędu. Zawiera on także certyfikaty ICSA i Checkmark. BitDefender jest bardzo szybkim i elastycznym silnikiem wyróżniającym się ilością formatów, które rozpoznaje i skanuje. BitDefender posiada certyfikat ICSA, jest zdobywcą nagrody 100% Virus Bulletin i European Information Technologies Prize 2002. GFI WebMonitor automatycznie sprawdza uaktualnienia definicji Norman Virus Control i BitDefender-a jak tylko są dostępne. Cena GFI WebMonitor zawiera cenę uaktualnień na 1 rok.

### ■ Złośliwe oprogramowanie (trojany, spyware, itp) blokowane dzięki Kaspersky – opcjonalnie

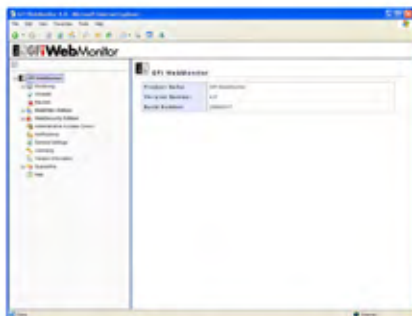
Aby osiągnąć większe bezpieczeństwo i korzystać ze skanowania wielokrotnymi silnikami, użytkownicy mogą dodać silnik anty-wirusowy Kaspersky SuperSecure, dostępny jako opcja dodatkowa. Baza danych Kaspersky SuperSecure obsługuje wykrywanie złośliwego oprogramowania, które może zdalnie administrować komputer, śledzić pisanie na klawiaturze, wykrywać hasła, automatycznie przekierowywać na płatne strony internetowe, automatycznie ściągać pliki z obelżywymi treściami. GFI WebMonitor automatycznie sprawdza i uaktualnia definicje Kaspersky-ego, gdy tylko są dostępne.

### ■ Ochrona przed stronami stosującymi socjotechniki phishingowe

Phishing jest socjotechniką złośliwie używaną przez hakerów do pozyskiwania informacji takich jak nazwy użytkowników, hasła, informacje o kartach kredytowych. Sklepy internetowe i firmy obsługujące karty kredytowe są najczęstszymi celami witryn phishingowych. GFI WebMonitor chroni użytkowników przed potencjalnym ryzykiem ulegnięcia takim socjotechnikom przez blokowanie dostępu do stron phishingowych. Odbywa się to za pomocą ciągle uaktualnianych baz danych adresów URL witryn phishingowych.

### ■ Kontrola typów plików dozwolonych do pobierania

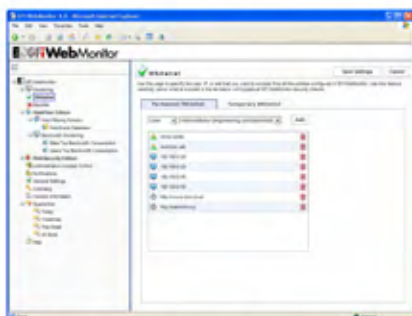
Możesz stworzyć różne reguły blokowania pobierania określonych typów plików (takich jak Javascript, MP3, MPEG i inne) zgodnie z ustalonym kluczem według użytkownik/grupy/IP itp. Niebezpieczne pliki (takie jak programy pobierające trojany) często starają się penetrować system udając nieszkodliwe pliki. GFI WebMonitor stosuje skaner sygnatur, który analizuje prawdziwe sygnatury pobranych przez HTTP/FTP plików.



GFI WebMonitor main screen



Monitors user online activity



User, IP and URL whitelists



User, IP and URL blacklists



Manage web access based on configurable web filters

## Cechy GFI WebMonitor UnifiedProtection Edition (cechy wspólne)

Poniższe cechy są dostępne we wszystkich wersjach.

### ■ Monitorowanie i blokowanie połączenia w czasie rzeczywistym

Administrator może na bieżąco śledzić co przeszukują pracownicy i jakie pliki są pobierane. Aktywne połączenie, sesja wyszukiwarki lub pobierania może być łatwo zablokowane przez naciśnięcie odpowiedniej ikony połączenia. Na przykład, możesz zdecydować przerwać pobieranie dużego pliku, który użytkownik próbuje ściągnąć.

### ■ Monitorowanie i blokowanie ukrytego pobierania

Niektóre aplikacje automatycznie łączą się ze swoimi stronami domowymi i pobierają uaktualnienia przez protokół HTTP. Może to ograniczać administrację, ale może także stwarzać ryzyko, ponieważ złośliwe aplikacje i trojany mogą stosować tę samą metodę do ściągania na komputer użytkownika programów szpiegujących, adware czy programów pornograficznych. GFI WebMonitor pozwala kontrolować z jakich stron można pobierać uaktualnienia (np. [www.microsoft.com](http://www.microsoft.com)).

### ■ Dopuszczanie wyjątków dzięki białym i czarnym listom

Każdy URL/użytkownik/IP może być czasowo lub na stałe dodany do białej lub czarnej listy aby obejść filtrowanie i zasady polityki bezpieczeństwa. Na przykład, możesz chcieć przydzielić danemu użytkownikowi dostęp do jego prywatnego konta mailowego przez określony czas.

### ■ Kontrolowanie dostępu do konfiguracji interface-u i monitoringu

GFI WebMonitor pozwala wybierać, który użytkownik może uzyskać dostęp do interface-u monitoringu. Możesz przydzielić dostęp na podstawie IP komputera uzyskującego dostęp lub nazwy uwierzytelnionej w domenie, której klient będzie miał dostęp. Tylko użytkownicy na liście IP/użytkowników GFI WebMonitor-a uzyskują dostęp do interface-u.

## Wymagania systemowe

- System operacyjny Windows 2000 (SP4), 2003 ,
- Microsoft ISA Server 2004 lub nowszy,
- Internet Explorer 6 lub nowszy
- .NET Framework 2.0.

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

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

GFI Software GmbH  
Bargkoppelweg 72  
22145 Hamburg  
Germany  
Tel +49 (0)40 3068 1000  
Fax +49 (0)40 3068 1010  
sales@gfisoftware.de

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

**ed&r**  
IT Experts United  
**GFI**  
Authorised distributor  
SECURITY SPECIALIST