

GFI WebMonitor

Web tartalom- és URL szűrő megoldás

Az munkaidő alatti dolgozói internethasználat több mint 40%-a nem a munkával kapcsolatos oldalakra irányul, melyek egy része ráadásul biztonsági kockázatot jelent. A munkaidő alatti Internet felhasználás szabályozására fejlesztette ki a GFI a WebMonitor eszközt, amellyel az üzemeltetők monitorozhatják vagy akár korlátozhatják, hogy az alkalmazottak milyen tartalmakat érhetnek el a világhálón.

Weblapok kategorizálása és szűrése

A WebMonitor WebGrade kategória-adatbázisa több mint 165 millió domain-nevet tartalmaz. Segítségével lehet engedélyezni vagy tiltani bizonyos típusú oldalakat, például szabályozható, hogy a híroldalak, informatikával foglalkozó oldalak vagy akár a felnőtt tartalmak csak bizonyos időszakokban elérhetőek, vagy egyáltalán nem elérhetőek a felhasználók meghatározott csoportjainak számára.

WebGrade Online

A Webgrade Online teljessé teszi a rendszer védelmét azzal, hogy ha a kliens által látogatott oldal nincs a helyi adatbázisban (kategorizálatlan), akkor a rendszer beküldi a központi adatbázisba feldolgozásra. A feldolgozás néhány órán belül megtörténik és a helyi adatbázis is frissül.

Spyware, vírus és phishing támadások elleni védelem

A WebMonitor tartalom- és URL-szűrő alkalmazásával bizonyos file-típusok letöltése blokkolható, minden egyéb adat csak ellenőrzés után juthat a felhasználók gépére. A letöltött file-ok minden esetben vírus, spyware és trójai-mentesek. Az adathalász (phishing) oldalak sem juthatnak át az automatikusan frissülő adatbázisnak köszönhetően.

Active Directory integráció

A WebMonitor együttműködik az AD és LDAP alapú címtárakkal, így a szabályrendszert felhasználókhöz vagy csoportokhoz lehet rendelni. Az integráció biztosítja, hogy csak azonosított felhasználók böngésszenek az Interneten, és csak azokat az oldalakat és kategóriákat tekinthessék meg, amelyeket a jogosultságuk megenged.

Funkcionális felépítés

A GFI WebMonitor két, különálló verzióban és egy integrált, minden funkciót tartalmazó verzióban érhető el:

- WebFilter Edition

Kategóriarendszer alapú URL szűrő, valós idejű monitorozó és szabályozó alkalmazás

- WebSecurity Edition

A letöltések kezelésére, szabályozására szolgáló tartalomszűrő és anti-vírus alkalmazás

- UnifiedProtection Edition

Mindkét komponenst tartalmazó, integrált biztonsági megoldás

WebFilter Edition

URL- és kategória-szűrés

Kategóriarendszer alapú URL-szűrő, valós idejű monitorozó és szabályozó alkalmazás.

Használatával az üzemeltetők képesek kontrollálni a web használatát, IP vagy akár felhasználói vagy csoport szinten (Active Directory vagy LDAP) megadva, hogy ki milyen kategóriába tartozó oldalakat böngészhet. Kizárhatóak a jogsértő vagy veszélyes tartalmat közvetítő weboldalak, így az adminisztrátor mérsekelheti a rosszindulatú weboldalokról a vállalati hálózatba jutó károkozók kockázatát.

Idő alapú szűrés

Az idő alapú szabályozás lehetővé teszi, hogy bizonyos tartalmak csak bizonyos időszakokban legyenek elérhetőek. Kizárhatóak vagy időszakokra korlátozhatóak a sávszélességet felemészítő streaming media (videó megosztók, rádiók, stb.) szolgáltatások, vagy megadható, hogy pl. a híroldalakat csak ebédszünetben érheti el a felhasználó.

Sávszélesség-figyelés, monitorozás

A sávszélesség monitorozó rendszer segítségével az üzemeltetőnek lehetősége van felhasználóra, weboldalra,



vagy kategóriára bontva visszanézni a forgalmazott adatmennyiséget (feltöltés/letöltés). A riport alapján „toplista” készíthető. Ennek a megoldásnak a segítségével jól kiszűrhetők azok az adatforgalmak, melyek feleslegesen terhelik a hálózatot, illetve előjelzést adhat az esetleges adatszivárgásokra, a nem megfelelő Internethasználatra.

Fekete/fehér lista

Bizonyos esetekben szükség van kivételkezelésre, például a hírkategóriába eső oldalakat tiltani kell, de kivételnek meg kell adni olyan oldalakat, amelyeknek az elérése a cég tevékenységéhez szükséges (pl. portfolio.hu).

WebSecurity Edition

Letöltött állományok ellenőrzése több vírusmotorral

A több vírusirtó alkalmazása drasztikusan csökkenti a vírusok megszületése és felismerése között eltelt időt, ezáltal minimálisra csökkentve a fertőzés esélyét. A magyarázat nagyon egyszerű: egyik gyártó sem lehet mindig a leggyorsabb. A víruskitörésekre az egyes gyártók más-más válaszdővel reagálnak a vírusok típusa és megjelenésük helyének függvényében. Több vírusirtó használata esetén nagyobb az esély arra, hogy ezek közül a programok közül legalább egy képes azonosítani és megállítani a legújabb vírusokat. Fontos még kiemelni, hogy minden vírusirtó egyedi keresési mechanizmussal rendelkezik. Egyesek nagy pontossággal találnak meg egy bizonyos vírust és annak variációit, míg egy másik antivírus-motor más vírusokat képes azonosítani. Összefoglalva: a több vírusirtó nagyobb védelmet biztosít.

Vírusvédelem: Norman Virus Control és BitDefender

A GFI WebMonitor alapértelmezésben tartalmazza a **Norman** és **BitDefender** víruskeresőket, amelyeknek vírusinformációs adatbázisa automatikusan frissül.

Rosszindulatú kód (trójai, spyware, exploit) elleni védelem (opcionális Kaspersky motor)

A legmegbízhatóbb védelem kialakításához lehetőség van a **Kaspersky SuperSecure vírus-és malware** védelmi

motorját integrálni a WebMonitorba, így akár egyszerre három biztonsági megoldás is ellenőrzi a letöltendő tartalmakat. A Kaspersky motor segítségével kiszűrhetőek a keyloggerek, spyware-ek, tárcsázó alkalmazások, jelzőrögzőtök vagy akár a háttérben láthatatlanul letöltődő, veszélyes kódokat tartalmazó alkalmazások.

Megoldás az adathalász támadásokra

A megtévesztésen alapuló, banki vagy kártyaadatok kicsalására specializálódó phishing támadások ellen is megoldást nyújt a GFI WebMonitor. Automatikusan frissülő és karbantartott phishing URL adatbázisa alapján képes felismerni és megakadályozni az adathalász oldalakra irányuló web forgalmat.

Letöltés-menedzsment és kontroll

A WebMonitor segítségével olyan tartalomszűrő szabályrendszer hozható létre, amely kontrollálja, hogy felhasználók, felhasználói csoportok vagy IP címek csoportja milyen állományokat (doc, pdf, jpg, exe, stb.) tölthetnek le az Internetről. Az ellenőrzés nem a kiterjesztést, hanem a fájl valós tartalmát, szignatúráját veszi figyelembe, így nem kijátszható.

IM kontroll

Az azonnali üzenetküldők (IM) lehetővé teszik, hogy a dolgozó kapcsolatba léphessen másokkal az interneten. Ez a lehetőség magában hordozza a kontrollálatlan adatáramlás lehetőségét (adatszivárgás) és a munkaidőben való privát beszélgetés lehetőségét. A WebMonitor képes blokkolni az azonnali üzenetküldő szoftvereket (pl. MSN Messenger), csökkenti az adatszivárgás kockázatát és növeli a felhasználó produktivitását.

UnifiedProtection Edition

Az URL és kategóriaszűrőt, valamint tartalom- és vírusszűrőt tartalmazó, integrált biztonsági rendszer. Egy termékbe foglalva nyújtja mindkét WebMonitor verzió szolgáltatásait, így kialakítható vele az egységes és minden igényre kiterjedő védelmi megoldás.

Rendszerkövetelmények

- Windows 2000(SP4)/2003
- Microsoft ISA Server 2004 vagy magasabb verzió
- Internet Explorer 6 vagy magasabb verzió
- .NET Framework 2.0

Díjak



Az Ön viszonteladója:

