

## Webes fenyegetések

A web életünk szerves részévé vált, egyre több vállalati munkafolyamat épül webes szolgáltatásokra. Ezen folyamatok, továbbá a gyors információ-áramlás igénye lehetetlenné teszi a korábban gyakran alkalmazott védekezési módszert, a webhasználat szimpla tiltását. Szintén hatástalan az egyes URL-ek saját kezű tiltása, hiszen egyrészt legfeljebb a jéghegy csúcsa kezelhető házilagos módszerekkel, másrészt az ilyen tiltás könnyen kikerülhető.

A kontrollálatlan webhasználat számos problémát vet fel. Információbiztonsági kockázatot jelent, hiszen olyan kódok tölthetnek le, melyeket a vírusirtók nem képesek felismerni. Szintén problémát jelent, hogy a felhasználók (vagy a gépükre települt kémprogramok) véletlenül vagy szándékosan anélkül tudnak adatot kiszivároztatni, hogy a szivárgásnak bármi nyoma maradna. A letöltések leterhelik a hálózatot, jogvédett tartalmak illegális letöltése pedig jogi kockázatot jelent. A munkaidőben történő céltalan webezgetés pedig egyszerűen felesleges költséget jelent a cégnek, így ennek visszaszorítása szinte követelmény.

## A Websense ThreatSeeker Network és a Websense Security Labs

A Websense a webtartalom-szűrő piac vezetője, megoldásait több mint 50 millió felhasználó veszi igénybe világszerte. Biztonsági laboratóriumában folyamatosan kutatják a legújabb támadástípusokat. A web dinamikáját a ThreatSeeker Network segítségével vizsgálják, mely óránként több mint 40 millió website-ot keres fel, óránként több mint 2 millió domain és IP-cím reputációját állapítja meg. Segítségével egyedülálló módon kezeli a dinamikus tartalmakat, mely a web 2.0 korában elengedhetetlen, és jóval túlmutat a hagyományos URL-szűrésen.

## A Websense webtartalom-szűrő megoldásai

A Websense a különböző igényeknek és cégméreteknek megfelelő verziókkal a teljes webbiztonsági területet lefedi. A különböző verzióknak közös pontja, hogy precízen meghatározható: ki, mikor, mit és hogyan érhet el a weben. A szabályrendszer alapján a webhasználat kontrollálható, utólagos számonkérés helyett a megelőzésre helyezi a hangsúlyt, bátorítva ezzel a produktív és biztonságos webhasználatot. A komplexebb verziók integrálhatók a Websense Data Security Suite DLP-megoldással, biztosítva a kiszivárgó információk megállítását a webes, IM és p2p csatornákon. A webtartalom-szűrők egyik leglényegesebb funkciója a testreszabható, részletes és többszintű jelentéskészítés. Külön megközelítésben készíthetők jelentések az informatikai üzemeltetési, biztonsági munkatársak, valamint az üzleti vezetők, divízió- vagy osztályvezetők, felsővezetők számára. A jelentések szinte tetszőleges formában előállíthatók, időzítve illetve rendszeresen generálhatók, majd akár e-mailben továbbíthatók.



### A Websense webszűrők verziói

#### Websense Express

A Websense integrált, belépő szintű terméke kisvállalatok számára. Egyszerű üzembe helyezés, alacsony erőforrás- és karbantartás-igény jellemzi, ugyanakkor a kisvállalatok számára megfelelő biztonságot nyújt. Az összetett e-mailes és webes fenyegetések ellen ugyanúgy véd, mint a HTTP-től különböző protokollokon érkező támadások ellen, akár 30 protokoll részletes elemzése alapján.

#### Websense Web Filter

Azon közép- és nagyvállalatok ideális választása a Websense Web Filter, akik a biztonságra kevésbé kényesek, ám a munkaidő- és sávszélesség-felhasználást kontroll alatt szeretnék tudni. A rendszer később kiegészíthető biztonsági szűréssel is. Ezen verzió már elosztott architektúrában is telepíthető, erős jelentéskészítési lehetőségekkel rendelkezik.

#### Websense Web Security

A Websense korábbi zászlóshajója a Websense Web Filter összes funkciójával rendelkezik, de biztonsági szempontból jóval túlmutat azon. A Web Security az Instant Messaging és peer-to-peer protokollok részletes elemzését is képes elvégezni, ezekben a csatolmányok küldhetőségét kontrollálni. Valós idejű biztonsági frissítéseivel pedig a legújabb webes fenyegetések ellen percekben belül védelmet biztosít.

#### Websense Web Security Gateway

A webtartalom-szűrés csúcsa, a Websense Web Security Gateway nem csak az URL-eket, IP-címeket és HTTP fejléceket vizsgálja, hanem a teljes oldaltartalmat aktívan elemzi. Az Active Security Scanning funkció segítségével a beépülő kódokkal szemben is azonnali védelmet nyújt, egyedülálló biztonságot teremtve ezzel.

#### Websense V10000

A Websense V10000 vadonatúj, célhardver alapú webbiztonsági infrastruktúrája. A virtualizált környezetben a Web Security Gateway dolgozik, szükségtelenné téve a rendszer alapos méretezését. Nagyobb teljesítményigény esetén egyszerűen több célhardvert kell összekötni, melyek a menedzsment szempontjából egy egységet alkotnak, egyszerűsítve ezzel az üzemeltetést.

#### Websense Hosted Web Security

A Websense Hosted Web Security megoldásával kihelyezett módon, beruházás és üzemeltetés nélkül élvezheti a Websense webbiztonsági megoldásainak előnyeit.

#### Websense Content Gateway

A Content Gateway modul az ismeretlen weboldalak dinamikus kategorizálásán a HTTPS/SSL forgalom kontrolljára nyújt lehetőséget. A HTTPS forgalom terminálásával, majd újratitkosításával a titkosított forgalom kontrollálható. Meghatározható, hogy mely website-ok esetében vizsgáljuk a tartalmat, melyeket engedjük át kontroll nélkül, és melyek ne legyenek elérhetők titkosított kapcsolaton keresztül – mindezt akár felhasználónként vagy csoportonként definiálva.

#### Websense Remote Filtering

A Remote Filtering modul segítségével a vállalati webhasználati politika kiterjeszhető a távoli notebookokra is, csatlakozzanak azok otthon, egy partnercégnél vagy kávézóban.

Az Ön viszonteladója: