

## Web 2.0: új platform, új kihívások és veszélyek

A legtöbb weboldal ma már web 2.0-ás szolgáltatásokat nyújt: blogok, fórumok, kommentelési lehetőségek mellett képek, videók és egyéb állományok tölthetők fel a megbízhatónak tartott weboldalakra is. Ezek a felhasználói tartalmak azonban kockázatokat jelentenek, például cross-site scripting, kártékony Javascript vagy AJAX-alapú támadásokra nyújtanak lehetőséget, így még a legismertebb weblapok látogatása is veszélyessé válhat. Ezen fenyegetések ellen a hagyományos URL-alapú szűrés kevés védelmet nyújt, ezért a Websense piacvezetőként kifejlesztette a webtartalom-szűrés csúcsát, a Web Security Gateway-t.

## Websense Web Security Gateway: megoldás a web 2.0 fenyegetései ellen

A Websense Web Security Gateway által nyújtott web 2.0 aktív tartalomszűrés és fenyegetések elleni védelem az iparág leghatékonyabb és legpontosabb megoldása. Használatával a vállalatok élvezhetik a web 2.0 előnyeit, anélkül, hogy aggódniuk kellene a nem kívánt adattartalmak és az adatszivárgás kockázata miatt.

A Websense Web Security Gateway valós időben azonosítja és blokkolja a rosszindulatú web-tartalmat, mialatt a legitim tartalmat felismeri és hozzáférhetővé teszi. Képesé tesz a Web 2.0 technológia biztonságos használatára, mert a tartalomszűrés mellett 130 protokoll ezernyi alkalmazását képes figyelni és korlátozni. Felismeri a valós fájl típusokat és tartalmukat, ráadásul a HTTPS/SSL csatorna terminálásával képes belelátni a titkosított adatforgalmakba is. Mindenre kiterjedő jelentéskészítő felületet biztosít a webhasználat, a kockázatok és a szabálysértések naprakész elemzéséhez.

A Websense Web Security Gateway tartalmazza a Websense ThreatSeeker Network fejlett elemző és valós idejű klasszifikációs tartalomszűrőjét. Az integrált klasszifikációs és elemzőtechnológia védelmet biztosít a korábban nem kategorizált vagy ismeretlen tartalmakkal szemben. Tartalom alapján képes az ismeretlen oldalak azonnali vizsgálatát és kategorizálását elvégezni. A Websense Web Security Gateway az egyetlen olyan megoldás a piacon, amely ahelyett, hogy a weboldalt csak önmagában vizsgálná, képes a weboldal speciális elemeit (például aggregált, több adatforrásból érkező információk, mashup-ok, RSS feedek, mini-alkalmazások) kategorizálni és átvizsgálni.



A Websense Security Gateway már a küldés pillanatában elemzi a Web 2.0-ás, közösségi, fórum és blog oldalakra küldött tartalmakat, így megakadályozható az érzékeny adatok és információk kiszivárgása. A rendszer integrálható a Websense Data Security Suite DLP-megoldásával, így biztosítva utólérhetetlen védelmet az adatbiztonság területén.

### A Websense Web Security Gateway védelmi mechanizmusai:

- A világ legnagyobb URL-adatbázisa
- A dinamikus webtartalom és adatforgalom teljes kontrollja
- Alkalmazás-felismerés (Pl. Facebook-on belüli alkalmazások, stb.)
- A bejövő és kimenő adatfolyam valós idejű ellenőrzése
- HTTPS/SSL forgalom transzparens kontrollja és átláthatósága
- Védelem a dinamikus szkriptek, AJAX, XSS támadások ellen
- Viselkedés-analízis, web-reputáció vizsgálat, web antivírus
- IM, p2p alkalmazások adatfolyam-szintű kontrollja
- 130 protokoll és több ezer alkalmazás kontrollja
- Integrált és nagykapacitású web-proxy cache
- Központosított és akár elosztott menedzsment
- DLP-integráció a Websense Data Security Suite-tal
- Mindenre kiterjedő jelentéskészítési lehetőségek

## Védelem a dinamikus Web 2.0 fenyegetéseivel szemben

### A világ legrészletesebb URL adatbázisa

A Websense sokmilliárd weboldalt tartalmazó URL adatbázisa lehetővé teszi a legpontosabb URL-alapú szűrések bevezetését is. A kategorizáló motorok az ismeretlen weboldalakat azonnal megvizsgálják és tartalmuknak megfelelően automatikusan besorolják valamely URL kategóriába.

### Integrált Web-Proxy cache

A Websense Web Security Gateway fejlett webproxyra és gyorstárra (cache) épül. A proxy használata nem csak a sávszélesség-használatot képes optimalizálni, ezáltal jelentős költséget megtakarítani, de biztosítja az érkező és távozó adattartalmak azonnali elemzését is.

### HTTPS/SSL adattartalom-ellenőrzés

A hagyományos URL- és tartalomszűrők nem látnak bele a HTTPS forgalomba. A Websense Web Security Gateway transzparens módon terminálja a titkosított adatkapcsolatot, és a kommunikációba beépülve képes a titkosított adattartalmakat is megvizsgálni. A terminálendő forgalom a céloldal típusa szerint választható, például a netbankok terminálás nélkül engedhetők át, a webmailek az átvizsgálandó kategóriába kerülnek, míg más weboldalakat látogatása HTTPS-el nem engedélyezett.

### Protokollok és alkalmazások felügyelete

Az üzenetküldők (IM) és a P2P alkalmazások nagy kockázatot jelentenek a kliens gépekre és a vállalati hálózatra, mert a támadók kihasználhatják az alkalmazások sebezhetőségeit, vagy felhasználhatják az alkalmazásokat (legegyszerűbb példák a sokak által ismert Messenger-vírusok és a Skype sebezhetőségei) a támadások során. A Websense Web Security Gateway 130 hálózati protokoll ezernyi alkalmazása felett biztosít felügyeletet, és a jogosulatlan alkalmazások adatfolyamszerű kontrolljával csökkenti a kockázatokat.

Az Ön viszonteladója: