

## ■ Websense Data Security Suite



A szervezetek egyik legnagyobb üzleti és IT biztonsági kihívása napjainkban a bizalmas adatok védelme a szándékos és véletlen adatszivárgás ellen.

Összetett probléma a vállalati és a külső szabályozásoknak megfelelően megelőzni a bizalmas adatok nyilvánosságra kerülését. Egy-egy ilyen incidens komoly költségeket jelenthet a vállalat versenyképességének csökkenésén, valamint az ügyfelek bizalmának megrendülésén keresztül.

A Websense Data Security Suite piacvezető megoldás az adatszivárgás megakadályozásában - induljon kívülről, belülről, legyen véletlen vagy szándékos.



### Feltárás

Websense Data Security Suite képes felderíteni a hálózaton található adatállományokat, akár a szerverről akár a végpontokról van szó. A bizalmas adatok helyének tudatában a szervezetek lehetőséget kapnak az üzleti folyamatokban található biztonsági rések szabályozására, és előírásokkal szabályozhatják a bizalmas adatok kezelését.

A Websense Data Security Suite magába foglalja a PreciseID-t, egy harmadik generációs ujjlenyomat készítő technológiát, amely segítségével azonosíthatjuk strukturált és strukturálatlan adatainkat. Fájlonként több ujjlenyomatot készít egy matematikai algoritmussal, elemzi a tartalmat a dokumentumon belül. Ennek segítségével felismeri az adatokat, függetlenül attól, hogyan próbálják manipulálni azt.

### Monitoring

Websense Data Security Suite valós időben monitorozza az adatokat, vizsgálja, hogy mely információk vannak a szerveren vagy a végpontokon. Folyamatosan figyeli a kilépési pontokat akár fizikai portok (pl. USB, optikai meghajtók), akár hálózati protokollok szintjén (pl. FTP, http, instant messaging stb.). Az adminisztrátorok monitorozhatják és szabályozhatják, ki, milyen adatokat, milyen csatornán és hova mozgathat, illetve riasztásokkal, részletes riportlással támogatják az üzemeltetést.

### Védelem

A felhasználó és tartalom alapú előírások automatikus blokkolást, titkosítást, karanténozást, naplózást és a potenciális biztonsági incidensek megelőzését, kivédését teszik lehetővé.

Szükség esetén a Websense DSS automatikusan titkosít, meghatalmazást kér az adatok tulajdonosaitól annak használatáról, vagy engedély-kérelmet küld a felelősöknek.

A Websense Data Security Suite főbb jellemzői:

- Választható működési módok: monitoring, blokkolás, endpoint
- Inline vagy offline monitoring mód
- Websense Web Security Gateway integrálási lehetőség (SSL terminálási képességgel)
- Web Security Suite kategóriák használatának lehetősége
- Figyelt csatornák: SMTP, HTTP, HTTPS, FTP, IM, tetszőleges...
- Precise ID & NLP: harmadik generációs lenyomatkészítés, strukturált vagy strukturálatlan adatfelismerés, illetve natív nyelvi támogatás
- Valós fájl típus felismerés
- Végpontokon külső adattároló eszközökre kiírt adatok monitorozása, blokkolása
- Végpontokon a vágólapok használatának, képernyőképek készítésének adattól függővé tett korlátozása
- Beágyazott fájlok dekompozíciója
- Agentek: Nyomtató szerver, ISA
- Adatbázis integráció: adatok kiolvasása, felismerése ODBC-n keresztül
- Támogatott címtárak: Active Directory, Novell, LDAP
- Központi menedzsment: szabályok és naplók központi kezelése
- Incidensek kezelése: blokkolás, karanténozás, riasztás
- Jelentéskészítés: azonnali időzített