

E-mail tartalomszűrés

Az e-mail tartalomszűrést sokan tévesen azonosítják a kéretlen levelek kiszűrésével, pedig a SPAM-ek távoltartása csak egy funkció a tartalomszűrés területéről. Az e-mailben áramló információ ugyanis számos egyéb kockázatot is jelent, a rosszindulatú kódok és jogsértő tartalmak bejutásától kezdve a bizalmas információk szivárgásig.

Websense E-mail Security

A Websense E-mail Security az egyik legkifinomultabb tartalomszűrő a piacon. Szabályrendszer segítségével részletesen meghatározható, hogy ki (akár LDAP azonosság vagy csoporttagság szerint), mit, hova és hogyan küldhet illetve fogadhat e-mailen keresztül. A levél teljes tartalmát és csatolmányait azok tartalma szerint vizsgálva komplex szabályrendszer hozható létre, melyben nagy segítség az intuitív, drag-and-drop alapú szabálykészítő.

Kapcsolati szintű védelem

A kapcsolati (SMTP) szintű védelem segítségével a rendszer már a kommunikációs csatorna felépülésekor képes elvégezni a legfontosabb szűréseket. Az SMTP-szinten történő ellenőrzés hatalmas terheléstől védi meg a tartalomszűrő megoldást, hiszen nincs szükség a levélállományok erőforrásigényes logikai feldolgozására.

Reputációs intelligencia

A Websense E-mail Security reputációs adatbázisának pontosságát a Websense biztonsági kutatólaboratóriuma, valamint menedzselt e-mail tartalomszűrő megoldásán, a Websense Hosted E-mail Security-n havonta áthaladó 3-4 milliárd e-mail garantálja. A menedzselt szolgáltatáson keresztülhaladó levélmennyiségből származó tapasztalat a legmagasabb szűrési pontosságot teszi lehetővé és a menedzselt szolgáltatásból származó információk automatikusan elérhetőek a telepített szoftveres Websense E-mail Security rendszerek számára is.

Tartalmi-logikai szűrés

A tartalmi-logikai feldolgozó modulok elemzik az átvett vagy küldött leveleket és megvizsgálják adat-tartalmukat. A Websense E-mail Security számos tartalomszűrő motorral rendelkezik, és ezek a motorok vagy a szűrési eredményeik logikai láncokba és elágazásokba fűzhetőek. Az egyes motorok szűrési eredményei újabb és újabb ellenőrzéseket kapcsolhatnak be, így akár a legbonyolultabb vizsgálatok is könnyen és gyorsan felépíthetőek, együttesen a legmagasabb biztonsági szintet garantálva.

Digitális lenyomat-alapú SPAM szűrés

A Digital Fingerprinting technológia lenyomat adatbázisát a Websense biztonsági laboratóriumában kézzel állítják össze. A segítségével elfogott SPAM-ek 100% biztonsággal nem tartalmaznak értékes információt, így ezen levelek további vizsgálat és archiválás nélkül eldobhatók.

Logikai SPAM szűrés

A heurisztikus és lexikális SPAM motorok a 0-day és csak URL-t vagy 1-2 szót tartalmazó SPAM levelek ellen nyújtanak védelmet. Ezeket a SPAM leveleket nem lehet kategorizálni és nem lehet róluk digitális lenyomatot készíteni, így a legtöbb hagyományos SPAM-motoron átcsúsznának.



3 rétegű anti-vírus, spyware, malware védelem

A Websense E-mail Security 3 szintű (rétegzett) vírusszűrési lehetőséggel bír. Az Authentium és Zero Hour vírusmotorok a hagyományos és 0-day vírusok ellen nyújtanak védelmet, de lehetőség van egy opcionális McAfee-motor bekapcsolására is, hogy a két különböző gyártótól származó anti-vírus megoldás 100%-os biztonsággal állítsa meg a fertőzött leveleket. További maximum 254 antivírus-motor csatolható a rendszerhez.

URL-adatbázis

A Websense E-mail Security felhasználja a Websense webtartalom-szűrő megoldásainak (Web Security Suite, Web Security Gateway) URL adatbázisát. A beérkező levelekben található linkeket ellenőrzi, és képes blokkolni a veszélyes tartalmak felé, vagy nem megengedett URL-kategóriákba tartozó oldalra mutató leveleket.

Csatolmányok vizsgálata

A beérkező vagy távozó levelek csatolmányait vizsgálva a Websense E-mail Security képes megállítani az érzékeny adatokat tartalmazó leveleket, blokkolja a sérült, hamisított, nem valós vagy veszélyes kódokat tartalmazó csatolmányokat. A csatolmány-vizsgálat a valós fájltypust vizsgálja, nem csak a kiterjesztést. A tömörített állományokat és egymásba ágyazott objektumokat is képes kibontani, és tartalmukat külön-külön megvizsgálni.

Képek vizsgálata

A Virtual Image Agent modul a képfájlok vizsgálatát végzi el, és nagy pontossággal megállapítja, hogy az érkező vagy távozó kép erotikus tartalmú-e.

Adatszivárgás elleni védelem

A Websense E-mail Security önmagában is rendelkezik olyan lexikális motorral, amely a kimenő levelekben képes felismerni az érzékeny adattartalmakat (Virtual Learning Agent), de össze is kapcsolható a Websense DLP megoldásával, a Websense Data Security Suite-tal, amely nem csak a szavakat, hanem mesterséges intelligenciával magát az információt elemzi.

Titkosítás

A Websense E-mail Security lehetőséget ad (érzékeny adattartalom, meghatározott cím, domain, stb. esetén) a kimenő levélforgalom csatornatitkosítására (TLS Delivery) vagy PKI-infrastruktúrával való integrációra.

Üzemeltetés és menedzsment

Automatikus karantén-menedzsment

A beérkező vagy távozó leveleket a Websense E-mail Security karanténokba tudja kényszeríteni. A karanténok tetszőlegesen meghatározhatóak és konfigurálhatóak. Az E-mail Security felügyeli a karanténok állapotát és a szabályoknak megfelelően automatikusan le tudja üríteni őket, így biztosítja, hogy ne telhessenek be a karanténokat tartalmazó diszkerületek. Az egyes felhasználókra egyéni karanténok hozhatók létre, melyeket akár ők maguk is tudnak kezelni, levéve az üzemeltetők válláról a terhet.

Jelentéskészítés

A Websense E-mail Security egyedülálló riportolási lehetőségekkel rendelkezik. Az interaktív „drill down” riporting segítségével az üzemeltetők a legváltozatosabb és legmélyebb elemzéseket is egyszerűen elkészíthetik. Az automatikus riportok mindenre kiterjedő képet adnak a vállalat levélforgalmáról és számos adatformátumba exportálhatóak.

Az Ön viszonteladója: