filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

Forcepoint Email Security Cloud

A Forcepoint Email Security Cloud vezető védelmet nyújt a mai több csatornás, email és internetes fenyegetések ellen. A Forcepoint Email Security Cloud megoldása csökkenti a költségeket és az infrastruktúra bonyolultságát, miközben lehetővé teszi a vállalkozások számára, hogy továbbra is megőrizzék az irányítást. Ez a dokumentáció segít megismerni a Forcepoint Email Security Cloud működését, megmutatja, hogy a bejövő és kimenő email forgalom miként konfigurálható a szervezeten belüli felhasználók és csoportok eltérő igényei szerint.

Miért egyszerű és biztonságos az Email Security Cloud használata?

Mivel nincs hardver vagy szoftver követelmény, a telepítéshez, a hibaelhárításhoz, valamint a javítások és frissítések alkalmazásához kapcsolódó üzemeltetési költségek és feladatok megszűnnek. A Forcepoint ThreatSeeker Intelligence folyamatosan figyeli az e-mailek tartalmát a felmerülő veszélyekkel kapcsolatban, napi több millió kérést elemez, napi több millió kéretlen levelet, adathalász és megtévesztő kampányokat rögzít. A ThreatSeeker továbbítja ezt az információt a Forcepoint e-mail, internetes és adatvédelmi megoldásainak, valamint azoknak a Forcepoint biztonsági elemzőknek, akik ezt az intelligenciát alkalmazzák, hogy gyorsan adaptálhassák a Forcepoint megoldásaiba.

Mire képes a Forcepoint Email Security Cloud?

A Forcepoint Email Security Cloud 99%-os spam felismeréssel bír, valamint egy West Coast Labs által kiadott prémium AntiSpam tanúsítvánnyal rendelkezik. A tartalomelemzést biztosító átfogó vizsgálat lehetővé teszi mind a bejövő, mind a kimenő levelezés ellenőrzését. A Forcepoint Email Security Cloud rendelkezik több, előre definiált lexikális szótárral, amelyek segítik a szervezeteket a HIPAA, SOX és a globális adatvédelmi szabványok betartásában. A titkosítás az üzleti partnerek és magánszemélyek közötti e-mail kommunikációt biztosítja annak biztosítása érdekében, hogy e-mail tartalmuk biztonságos és privát legyen. Az összefoglaló és a részletes jelentések, az Dashboard funkcióval kombinálva kriminalisztikai adatokkal szolgál a Forcepoint által biztosított valós idejű e-mail biztonsági védelemről. A rendszergazdák átruházhatják és ütemezhetik a riportolási hozzáférést a szervezet bármely részlegére, hogy a megfelelő vezetők automatikusan emailben értesülhessenek a biztonsági incidensekről. A Forcepoint több

filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

globális, ISO27001-es tanúsítvánnyal minősített adatközponttal rendelkezik, hogy a legmagasabb rendelkezésre állást tudják biztosítani. Az összes e-mailt 2 adatközpontba továbbítják a különböző földrajzi régiókban, hogy redundanciát és hibatűrést tudjanak biztosítani. A rendszer rendelkezésre állása 99,999%-os és magába foglalja a katasztrófa utáni helyreállításra vonatkozó rendelkezéseket is. A beépített redundancia, feladatátvétel és üzleti folytonosság biztosítja, hogy az e-mail mindig működőképes maradjon, még akkor is, ha a hálózat átmenetileg nem érhető el.

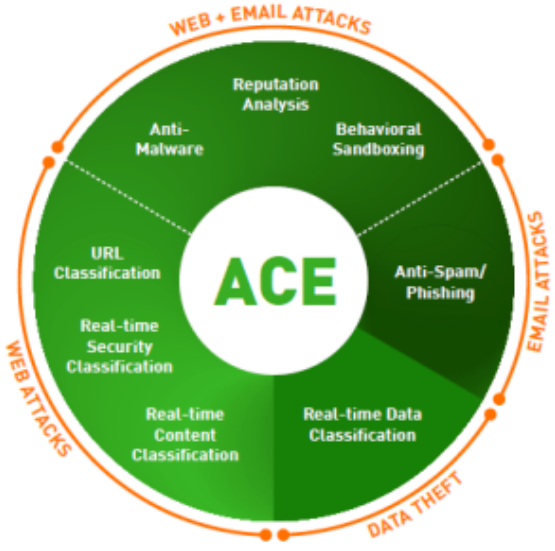
Adatgyűjtés

A Threatseeker hálózat sokféle gyanús vagy káros online tartalmat gyűjt, futtattható fileok, weboldalak, dokumentumok, scriptek emailek, mobile appok és más forgalmak formájában. Naponta több milliárd email és webkérés feldolgozásával keresi az új trendeket, veszélyforrásokat és új típusú megfigyelendő adatokat. A Forcepoint többek között minden Facebook-ra postolt URL-t is ellenőrzi 2011 óta, így egyszerre védi a Facebook felhasználókat és gyűjti az adatokat a legfrissebb trendekről.

- Figyelemmel kíséri a népszerű webhelyeket, hogy megbizonyosodjon arról, hogy veszélyeztettek-e ezek az oldalak, vagy eltérítették-e esetleg őket.
- Követi a legfrissebb híreket, a trend témákat és a közösségi médiát, hogy meghatározza az értékelni kívánt kiegészítő tartalmat.
- Követi a földrajzi pontokat új URL-ek és esetleges gyanús internetes tevékenységek felismerése céljából.

Adatelemzés

A ThreatSeeker-el karöltve Forcepoint Advanced Classification Engine (ACE) motorja a biztonsági kutatók állandó felügyelete mellett folyamatosan és valós időben klasszifikálja a tartalmakat, hogy a Zero Day és egyéb veszélyektől megvédje a szervezeteket.



- Big Data analitika alapján a kutatók vizsgálják a potenciálisan gyanús új típusú veszély forrásokat.
- Az ismeretlen futtatható tartalmakat alaposan megvizsgálja a rendszer IOR (indacators of risk) jelek után kutatva, valamint a Forcepoint Sandboxban detonálja az összes ilyen tartalmat a potenciálisan veszélyes működések kiszűrésére.

filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

A rendszer felépítése

Dashboard

A legfrissebb grafikus adatok megtekintése az e-mailek mennyiségéről, a bejövő e-mailek összetételéről és a spam észlelésének arányáról.

Kategóriák, amelyeket a Dashboard foglal össze:

- Email aktivitás összefoglaló az elmúlt 7 nap alapján.
- Inbound és Outbound kategóriák felsorolása.

Spam	A spamfilter szabályok alapján megjelölt üzenetek.
Valid	Az elemzett vagy engedélyezett levelek listája.
Content	Azon üzenetek, melyeken a tartalomszűrő ellenőrzés lefutott.
Viruses	Az Antivirus vagy a ThreatSeeker által vírust tartalmazó üzenetek listája.
Phishing	Olyan üzenetek, amelyek rosszindulatú kódokkal ellátott oldalakra mutatnak, amelyek alkalmasak felhasználói adatok eltulajdonítására.
Commercial Bulk	Kereskedelmi üzenetek listája.
Backscatter	Visszapattanó üzenetek, valamint spoofing emailek listája.
Access	Értesítési üzenetek listája.
Other	Más okokból megjelölt üzenetek, például hurok, titkosítás vagy rendszer üzenetek listája.

- Top 5 Virus, amely tartalmazza az 5 legfontosabb vírusos levelet.
- URL kategóriák, amelyeket a Forcepoint Email Security Cloud osztályoz a szervezet e-mailjeinek ellenőrzése során.

filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

Directory Synchronisation

Leegyszerűsíti a felhasználókezelést és megakadályozza a címtárgyűjtési támadásokat az Active Directory vagy a Lotus Domino Forcepoint Email Security Cloud közötti szinkronizációja közben.

A Microsoft Active Directoryt, a Lotus Domino-t és más LDAP-szolgáltatásokat használó szervezetek szinkronizálhatják az elsődleges és másodlagos e-mail címeket és csoportokat a portálra.

Ennek a következő előnyei vannak:

- A rendszergazdák az e-mail címeket és a csoport részleteit az Active Directory-ból kezelhetik, nem pedig a felhőalapú portálról, ezáltal jelentősen csökkentve a szolgáltatáskonfiguráció fenntartására fordított időt.

- Az ütemezett szinkronizálás azt jelenti, hogy a vállalat új alkalmazottai automatikusan hozzáadhatók a felhőalapú szolgáltatáshoz. Hasonlóképpen, az elhagyók automatikusan eltávolíthatók a szolgáltatásból.

- Javítja a spam észlelését az ismeretlen felhasználóknak küldött e-mailek karanténba helyezése által.

- Segíti a címtárgyűjtési támadások megelőzését, mivel ellenőrzi az e-mail címek és a tartományok érvényességét, amikor egy szerver nagyszámú üzenetet próbál küldeni a könyvtárgyűjtés céljából.

Policies and Fine-Tuning

Az Forcepoint Email Security Cloud alapértelmezett házirendje lehetővé teszi a legtöbb szervezet számára, hogy minimális konfigurációval gyorsan és egyszerűen felálljon. Az adminisztrátor szükség szerint módosíthatja vagy létrehozhat új irányelveket az e-mail forgalom kezeléséhez, hogy megfeleljen a szervezet üzleti igényeinek, céljainak.

A szabályok több elemet magukban foglalnak, többek között:

- Spam és vírusvédelem szabályai.
- Kifejezések és lexikai szabályok a tartalom szűrésére.
- Értesítések a karanténba helyezett e-mailekről.

A szakmai döntések és az ellenőrzés szintje eltérő lehet a különböző felhasználói csoportok között, de minden esetben úgy kell megtervezni, hogy lehetővé tegyék a felhasználók számára az e-mailek üzleti eszközként történő hatékony felhasználását, miközben megóvják a társaságot a spam, a kifogásolható vagy illegális tartalom és a vírusok ellen. A Forcepoint Email Security Cloud alapértelmezett házirendet biztosít, és az

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

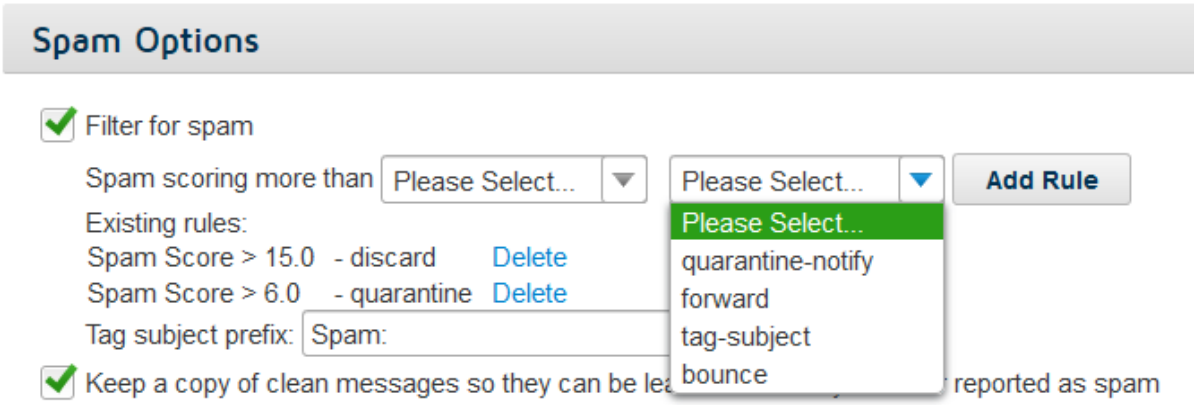
adminisztrátorok egyéni házirendeket is létrehozhatnak az eltérő konfigurációt igénylő e-mail aliasok vagy tartományok támogatására.

AntiSpam szabály lehetőségei

A becslések szerint az összes e-mail 90-95% -a spam. A Forcepoint Email Security Cloud piacvezető spam-ellenes védelmet nyújt a ThreatSeeker Intelligence által támogatott technikák kombinációjával. A Forcepoint megközelítés egyedülálló abban a tekintetben, hogy webes intelligenciánkat integráljuk az e-mail védelmi motorunkba, amely lehetővé teszi a szolgáltatás számára, hogy valós időben észlelje a vegyes fenyegetések támadásait. A ThreatSeeker Intelligence technológiák magukban foglalják a Forcepoint reputáció szolgáltatást, az integrált Forcepoint URL adatbázist, heurisztikát, ujjlenyomatot, automatikus tanulási technológiákat és egyebeket. Az e-mail védelmi technika, technikák kombinációját használja az egyes e-mailek elemzéséhez és az üzenet „spam pontszám" hozzárendeléséhez. Ezt a spam-pontot használják annak a valószínűségének meghatározására, hogy az üzenet spam lett-e. A különböző spam tesztek eredménye lehet pozitív (spam jelzésére) vagy negatív pontszám (érvényes e-mail jelzésére). Az ügyfél által a „spam küszöbérték" feletti üzenet pontozás spamnek minősül. Az összes teszt eredményét figyelembe veszik, és ez hozzájárul a pontosság javításához.

A Spam filter beállításainál a Forcepoint Email Security Cloud lehetőséget biztosít arra, hogy a leveleket a Spam-Score alapján általunk létrehozott szabályok alapján szelektálhassuk.

A Forcepoint Email Security Cloud egyik nagy előnye, hogy a megadott értékek alapján tagging segítségével megjelöljük a spamnek minősített leveleket.

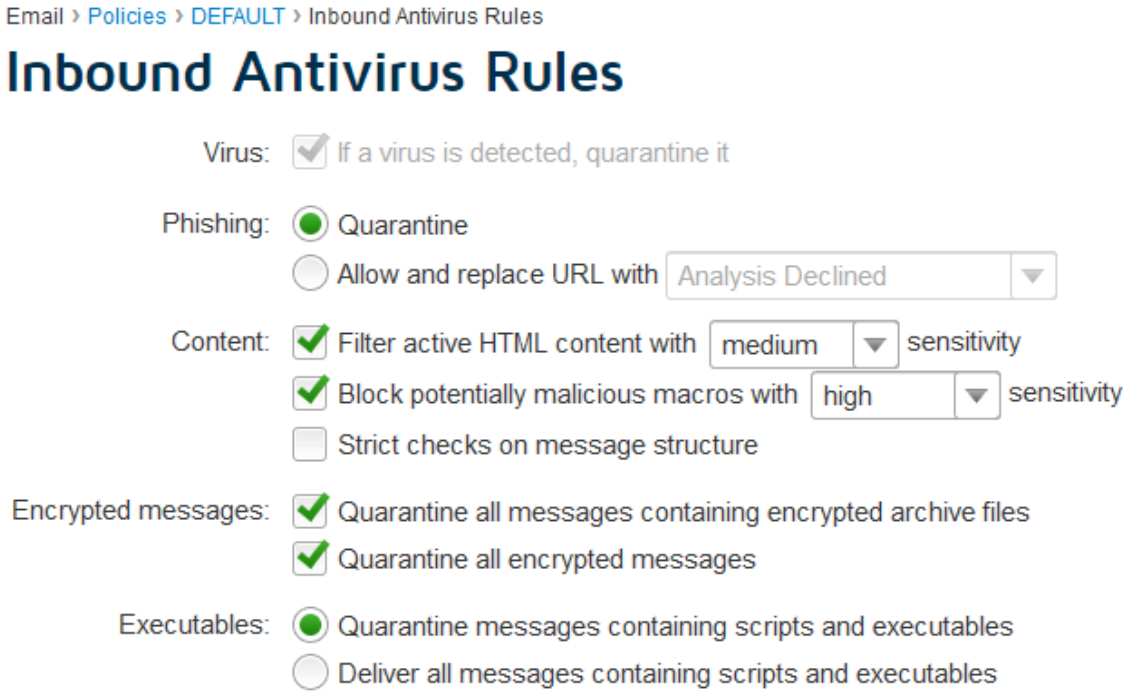


filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

AntiVirus szabály lehetőségei

Az AntiVirus szabály módosításaira is ad lehetőséget a Forcepoint Email Security Cloud, amelyeket az alábbi formában hajthatjuk végre.



- Virus: Amennyiben vírust talál az ellenőrzés, a rendszer karanténozza, ebben nincsen lehetőség a módosításra.

- Phishing: Lehetőség nyílik arra, hogy az adathalász leveleket a rendszer milyen formában kezelje. Karanténozzuk vagy engedjük át a levelet, de a benne található URL-eket módosítsuk a gyártó által definiált action-ök használatával.
  Ezek az action-ök az alábbiak lehetnek: Analysis Declined, Certificate Error, Malicious Threat Detected, Phishing Attack Blocked, Promt for Analysis, Uncategorized URL, Unreachable URL, Unsupported Protocol, URL verified.

- Content: Szűrhetjük a HTML tartalmakat megadott érzékenységek alapján (Low, Medium, High, Very High).

  Blokkolhatjuk a potenciális fenyegetést jelentő makrókat különböző érzékenységek alapján (Low, Medium, High, Very High).

  Lehetőség nyílik a levelek szerkezetének szigorú ellenőrzésére is.

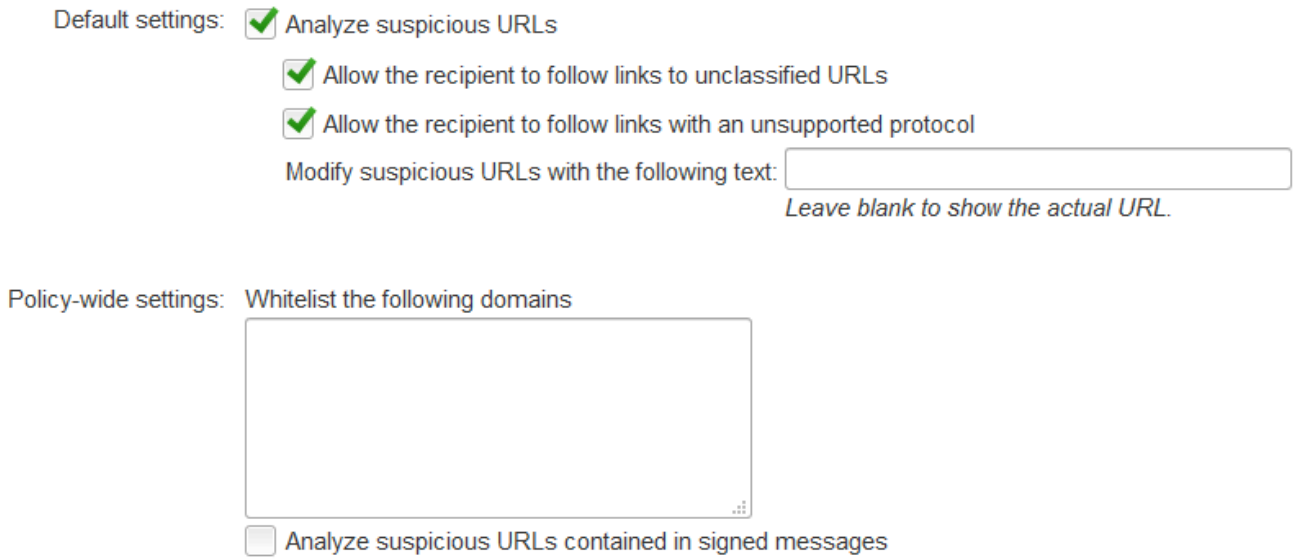
filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

- Encrypted messages: Lehetőség nyílik a rendszerben arra, hogy a titkosított leveleket, vagy titkosított archív file-okat mellékletként tartalmazó leveleket karanténozzuk.
- Executables: A rendszerben beállítható, hogy a futtatható file-okat tartalmazó levelek karanténba kerüljenek, vagy kézbesítésre.

URL Sandboxing szabály lehetőségei

Az URL Sandboxing szabály használatával ellenőrizhető, hogy a levelekben megtalálható URL-ek nem mutatnak olyan weboldalra, amely esetleges fenyegetést jelenthet.



Amennyiben engedélyezzük ezt az opciót, abban az esetben a rendszer a felismert gyanús URL-eket képes felülírni is akár, ezáltal ártalmatlanítani a gyanús oldalra mutató URL-t.

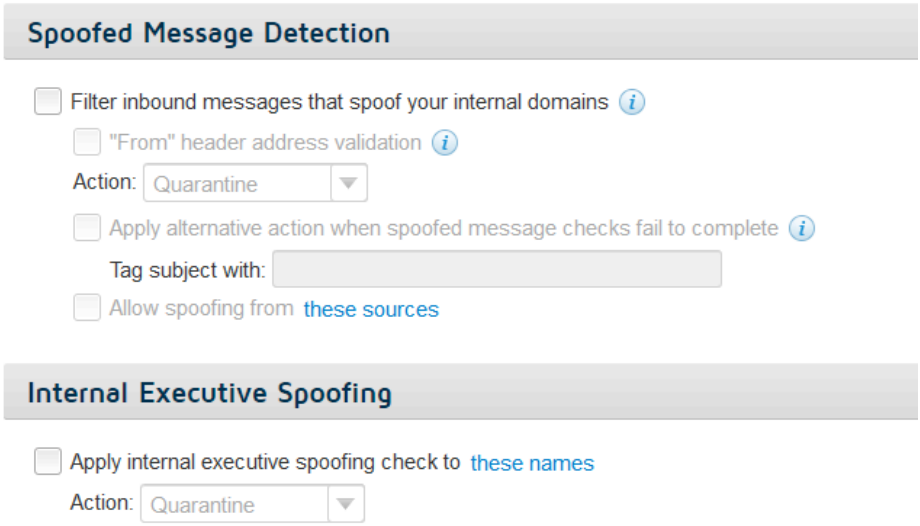
Természetesen van arra lehetőség, hogy adott URL-eket engedélyezzünk a whitelist segítségével, így az ide felvett URL-ek nem kerülnek módosításra.

filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

AntiSpoofing szabály lehetőségei

Az AntiSpoofing szabály megakadályozza, hogy visszapattanó, esetlegesen kézbesítési jelentésnek tűnő spam üzenetek érkezzenek a postafiókokba.



A szabályban definiálható, hogy az ellenőrzés során a „From” mezőt ellenőrizze és milyen módon kezelje a levelet.
A tagging opció itt is elérhető természetesen, amennyiben az action-ben kiválasztjuk.

Content Filter szabály lehetőségei

A Forcepoint Email Security Cloud lehetőséget biztosít arra, hogy a bejövő és kimenő levelezést alávesse a tartalom ellenőrzésnek, ezáltal kiszűrve olyan file-okat is, amelyeket a korábbi szabályok alapján nem definiáltunk.
A szűrési lehetőséget két részre szedve kezeli, külön a bejövő levelezést és külön a kimenőt.

- Végrehajtható elemek - A szkripteket és a végrehajtható fájlokat tartalmazó üzenetek karanténba helyezhetők. Ez a szolgáltatás felhasználónként beállítható egy irányelvben.

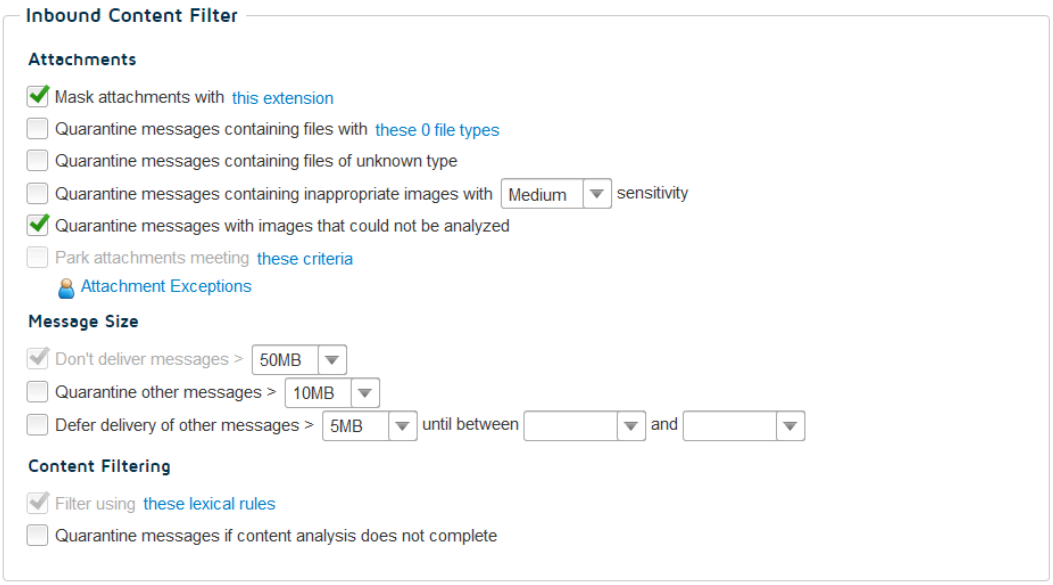
- Mellékletek - A mellékletek fájlok szerint karanténba helyezhetők. Ez a szolgáltatás bizonyos fájltípusok bevonásával vagy kizárásával vezérelhető. Maszkolhatja a mellékleteket is; ez megváltoztatja a fájlt az automatikus végrehajtás megakadályozása érdekében.

filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

- Tárolás - A mellékleteket a felhőalapú szolgáltatás infrastruktúrájába lehet tárolni, és az eredeti e-mailt el lehet küldeni a címzettnek egy URL-lel, amellyel megkeresheti a mellékletet a későbbi letöltéshez, ha szükséges. Ez lehetővé teszi az Internet sávszélesség minimalizálását.

- Lexikális elemzés - A lexikai szabályok funkciók segítségével szavak és kifejezések keresése mind az előre definiált, mind az egyéni szótárakkal összehasonlítva a logikai operátorokkal, valamint az egyedi súlyozással és küszöbökkel történik.

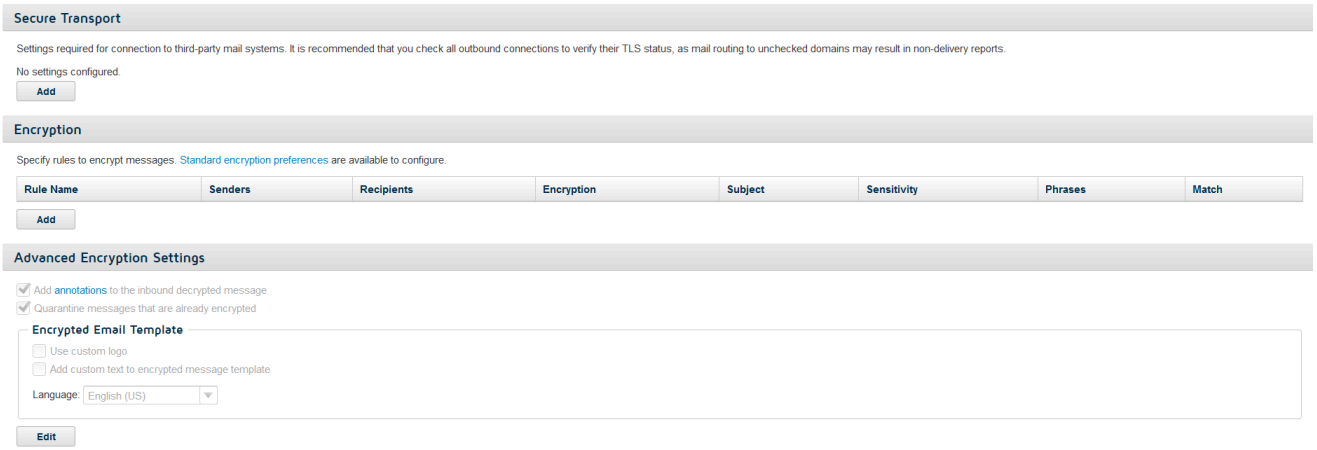


filter:max
az erőforrásbiztonsági cég

T.: +36 1 398-1098
1016 Budapest, Hegyalja út 7-13
filtermax@filtermax.hu
www.filtermax.hu

Encryption szabály lehetőségei

A Forcepoint Email Security Cloud Encryption modulja lehetőséget biztosít arra, hogy a kommunikáció és a levelek továbbítása titkosított csatorna használatával történjen.
Ez lehetővé teszi az adminisztrátorok számára a biztonságos e-mail kommunikáció beállítását az üzleti partnerek és magánszemélyek között, akár szállítási réteg titkosított "alagút" segítségével a megadott e-mail szerverek vagy az e-mail továbbító Agent között, eseti titkosítás a TLS-t nem támogató levelező Agent-ek számára, vagy fejlett identitás-alapú titkosítás érhető el.



Reporting

A Forcepoint Email Security Cloud kivételes riportolási funkciókat kínál, amelyek 360 fokos képet nyújtanak az e-mailek forgalmáról és használatáról. Az adminisztrátorok megtekinthetik az összefoglaló riportokat és részletesebb kriminalisztikai riportokat készíthetnek. A riportok időzítetten elindíthatók úgy, hogy automatikusan e-mailben eljuthassanak egy kijelölt kezelőhöz. Az e-mailes Report Builder-ben megtalálható egy Report Catalog, számos előre definiált jelentéssel, amelyek általános szcenáriókat fednek le, valamint egy Report Builder eszköz, amely rugalmas, többszintű jelentések készítéséhez használható, ezekkel elemezheti a különböző szempontokból származó információkat, és betekintést nyerhet a szervezet e-mail üzenetének trendjeibe.

Message Center

A Forcepoint Email Security Cloud Message Center egy hatékony üzenetkövetési és -kezelő eszköz, amely hozzáférést biztosít a fiókja összes karanténba helyezett üzenetéhez és üzenetnaplójához. Az Üzenetközpont eléréséhez kattintson a portál főmenüjében az E-mail elemre, majd válassza az Üzenetek> Üzenetközpont lehetőséget.