16. számú melléklet: CTRL Menedzselt Emailvédelem

1. Szolgáltatás meghatározása

A szolgáltatás biztosítja a bejövő email forgalom spam-, vírus-, phishing- és ransomware, illetve a kimenő forgalom vírusszűrését, valamint véd az üzenetekbe ágyazott káros URL-ek hatása ellen. A szolgáltatás on-premise és felhős levelezési rendszerhez is illeszthető

Emailvédelmi szolgáltatási csomagok és funkcióik

	Standard	Emelt szint
Általános jellegű szolgáltatások		
Ügyfelenként dedikált tenant Minden ügyfél egy elkülönített, saját környezetet (tenant) kap a felhőszolgáltatáson belül, biztosítva az adatok és konfigurációk elkülönítését és biztonságát. Ügyfél adatai kizárólag az Európai Unió és az Európai Szabadkereskedelmi Társulás (EFTA) tagországainak adatközpontjaiban kerülnek tárolásra és feldolgozásra.	✓	✓
Magas rendelkezésre állású felhőszolgáltatás A Trend Micro felhőinfrastruktúrája redundáns és hibatűrő kialakítású, hogy minimalizálja a szolgáltatáskieséseket és folyamatos emailvédelmet biztosítson.	✓	✓

	Standard	Emelt szint
Email védelmi szolgáltatások		
Email authentikáció támogatás: SPF, DKIM, DMARC A szolgáltatás támogatja az Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) és Domain-based Message Authentication, Reporting & Conformance (DMARC) email-hitelesítési protokollokat a küldő fél azonosítására és az email hamisítás elleni védelemre.	✓	✓
Biztonságos üzenet kézbesítés (TLS) A Transport Layer Security (TLS) protokoll használatával titkosítja az email üzeneteket azok átvitele során, megakadályozva ezzel az illetéktelen lehallgatást és adatlopást.	✓	✓
Reputáció alapú spam szűrés A Trend Micro kiterjedt, valós idejű reputációs adatbázisaira támaszkodva azonosítja és blokkolja az ismert vagy gyanús spamforrásokból érkező kéretlen leveleket.	✓	✓
Minta alapú spam szűrés Az e-mailek tartalmát és jellemzőit elemzi előre definiált és folyamatosan frissülő spammintázatok alapján, hogy kiszűrje a kéretlen leveleket.	✓	✓
Manuális IP-alapú tiltó és engedélyező lista Lehetőséget biztosít az adminisztrátoroknak arra, hogy manuálisan adjanak hozzá IP-címeket tiltólistákhoz (blokkolt küldők) vagy engedélyezőlistákhoz (mindig elfogadott küldők), így finomhangolva a spamszűrést.	✓	✓
Geolokáció alapú küldő IP szűrés Lehetővé teszi az e-mailek szűrését a küldő IP-címének földrajzi	✓	✓

	Standard	Emelt szint
Email védelmi szolgáltatások		
elhelyezkedése alapján, így blokkolhatók a nem kívánt régiókból érkező üzenetek.		
Kimenő és beérkező levelezési forgalom szűrése A szolgáltatási elem mind a beérkező, mind a kimenő email forgalmat ellenőrzi a fenyegetések (vírusok, spam, adathalászat) és a házirend-sértések kiszűrése érdekében.	✓	✓
Hírlevél szűrés (közösségi média értesítések, tömeges hírlevelek) Képes azonosítani és külön kezelni a tömeges küldésű hírleveleket és közösségi média értesítéseket, hogy csökkentse a postaládák terhelését.	✓	✓
Szignatúra alapú vírus szűrés Ismert vírusok és kártékony programok egyedi azonosítói (szignatúrái) alapján ellenőrzi az emaileket és mellékleteiket, hogy megakadályozza a fertőzéseket.	✓	✓
Email melléklet szűrés név, kiterjesztés, fájl típus, MIME típus alapján Lehetővé teszi az email mellékletek szűrését és blokkolását azok neve, kiterjesztése, tényleges fájltípusa vagy MIME (Multipurpose Internet Mail Extensions) típusa alapján a potenciálisan veszélyes vagy nem kívánt tartalmak kiszűrésére.	✓	✓
Tárgy és üzenettörzs szótár alapú szűrése Meghatározott kulcsszavak, kifejezések vagy mintázatok alapján vizsgálja az emailek tárgyát és törzsét a nemkívánatos vagy kártékony tartalmak azonosítása érdekében.	✓	✓
Üzenet méret szűrés Lehetőséget biztosít az e-mailek méretének korlátozására, így megakadályozva a túl nagy üzenetek fogadását vagy küldését, amelyek terhelhetik a rendszert.	✓	✓
URL alapú szűrés Az emailekben található webcímeket (URL - Uniform Resource Locator) ellenőrzi a Trend Micro Web Reputation adatbázisa segítségével, és blokkolja a hozzáférést a kártékony vagy nem megbízható webhelyekhez.	✓	✓
Értesítő email karanténba került levélről Ügyfél értesítést kap azokról az email üzenetekről, amelyeket a rendszer biztonsági okokból karanténba helyezett.	✓	✓
Ütemezett riportok* Lehetőséget biztosít rendszeres, automatikusan generált jelentések készítésére az email forgalomról, a blokkolt fenyegetésekről és a szolgáltatás működéséről.	✓	✓
Kimenő üzenet titkosítása** Biztosítja a kimenő e-mailek titkosítását, hogy megvédje az érzékeny információkat illetéktelen hozzáféréstől, amikor azok elhagyják a szervezetet.	✓	✓
DLP** Az Adatvesztés Megelőzési (Data Loss Prevention) funkciók	✓	✓

	Standard	Emelt szint
Email védelmi szolgáltatások		
segítenek azonosítani és megakadályozni az érzékeny vagy bizalmas adatok illetéktelen kiszivárgását emaileken keresztül.		
Felhő alapú Sandbox (fájl és URL vizsgálat) Gyanús fájlokat és URL-eket egy izolált, felhőalapú környezetben (sandbox) futtat és elemez, hogy felismerje az új vagy ismeretlen (zero-day) fenyegetéseket, mielőtt azok elérnék a felhasználókat.	-	✓
Levéltovábbítási szolgáltatás (az ügyfél oldali levelezőrendszer elérhetetlensége esetén) Biztosítja az üzenetek ideiglenes tárolását és későbbi kézbesítését, ha az ügyfél saját levelezőrendszere átmenetileg nem elérhető, így fenntartva az email forgalom folytonosságát.	-	✓
Business Email Compromise (BEC) fenyegetések észlelése** Fejlett elemzési technikákat, például a küldő viselkedésének, a levél tartalmának és a szerzői stílusnak (Writing Style DNA) vizsgálatát alkalmazza az üzleti email kompromittációs (Business Email Compromise) támadások, például a vezetői csalások és a számlacsalások felismerésére és blokkolására.	-	✓
Jelszóval védett fájl átvizsgálása** Képes a jelszóval védett tömörített fájlokban található kártékony tartalmak vizsgálatára, amennyiben a jelszó ismert vagy a rendszer számára hozzáférhető.	-	✓
Email vizsgálati események tárolása Naplózza az email vizsgálatokkal kapcsolatos eseményeket (pl. blokkolt vírusok, spam, karanténba helyezett üzenetek) későbbi elemzés, riportálás és audit céljából.	30 nap	60 nap
Házirend események tárolása Rögzíti a beállított biztonsági házirendekkel kapcsolatos eseményeket, például a házirend-módosításokat vagy a házirend-sértéseket, a megfelelőség nyomon követése és a hibaelhárítás érdekében.	30 nap	60 nap

* Mail forgalmi riportok: Napi vagy Heti rendszerességű, az adatbekérő szerint, az adatbekérőben megadott email címre.

** A funkció hangolása Felek között együttműködést igényel, így például a funkció által biztosított konfigurációs lehetőségek egyeztetését és beállítását az Ügyfél által használt környezetnek és elvárásoknak megfelelően.

2. Gyakran használt emailvédelmi funkciók kifejtése

Reputáció alapú email szűrés

A reputáció alapú email szűrő modul segítségével a CTRL menedzselt email védelmi szolgáltatás a forrás IP címe alapján kapcsolat szinten blokkolja a megbízhatatlan forrásból kezdeményezett email küldési próbálkozásokat. A reputációs adatbázis valós időben történő frissítések alapján a megoldás rövid időn belül képes reagálni az új spam források megjelenésére, víruskitörésekre és még a levél átvétele előtt képes blokkolni a megbízhatatlan forrásból kezdeményezett üzenetek fogadását.

Többszintű vírus-, spam- és tartalomszűrés

A szolgáltatás többszintű védelmet biztosít az emailben érkező kártékony programok ellen. A mintaillesztés alapú és heurisztikus módszerek egyidejű használatával hatékonyan detektálja a

dokumentumokban érkező károkozókat és egyéb kártékony kódokat és a szabványostól eltérő formátumú, rosszindulatú csatolmányokat.

A szolgáltatás ismeretlen kártevőket úgy azonosítja, hogy összeveti a gyanús állomány elemzése során összegyűjtött paramétereket a felhőszolgáltatásban tárolt gyártói threat információkkal. Egy ismeretlen, vagy ritkán előforduló állomány vizsgálata során a keresőmotor elemzi a fájlt és annak részleteit továbbítja a machine learning (ML) modulnak. Az ML modul a kapott információt összeveti a gyártói malware modell adatbázissal, és az állományhoz egy pontértéket rendel, amely reprezentálja, hogy mekkora valószínűséggel tartalmaz kártékony kódot.

URL alapú szűrés

Az URL védelmi funkcióval a szolgáltatás módosítja a levéltörzsben szereplő gyanús web hivatkozásokat oly módon, hogy a hivatkozott oldal megnyitásakor a szolgáltató web tartalomszűrő rendszerére kerül átirányításra. A megnyitás pillanatában a tartalomszűrő elemzi a weboldalt, és káros tartalom észlelése esetén blokkolja az elérést.

Felhő alapú Sandbox (fájl és URL vizsgálat)

A mail szűrőhöz kapcsolódó sandbox rendszer feladata a gyanús fájlok és URL-ek valós idejű elemzése a levelezési forgalomban. A sandbox környezet olyan különálló virtuális gépek sokasága, melyek lehetővé teszik a gyanús állományok és URL-ek vizsgálatát és viselkedésük elemzését anélkül, hogy az az éles hálózati környezetet veszélyeztetné.

A i szolgáltatás azokat a gyanús fájlokat és URL-eket, melyekben a szignatúra alapú keresőmotor nem talált vírust, vizsgálatra továbbítja a sandbox felé. A sandbox rendszer statikus és viselkedés alapú elemzési módszerekkel, a különböző futási paraméterek vizsgálatával azonosítja a kártékony viselkedést. Az elemzés végén az értékelő algoritmus kockázati besorolást rendel a vizsgált mintához, ez alapján hoz döntést az állomány minősítéséről.

Levéltovábbítás szolgáltatás

Az Emelt szintű szolgáltatás feladata az email vesztés megakadályozása az ügyfél oldali mail szerver leállása, elérhetetlensége esetén. Amennyiben hálózati kimaradás vagy szerverhiba miatt leáll és elérhetetlenné válik az Ügyfél mail szervere, a levéltovábbítás szolgáltatási elem automatikusan átirányítja a mail forgalmát a Szolgáltatónál futó tartalék szerverre, amíg a mail szolgáltatás újra helyre nem áll Ügyfél mail szerverén. Szolgáltató az Ügyfél mail szerverének leállásának ideje alatt biztonságos hozzáférést engedélyez Ügyfélnek web-kliensen keresztül, aminek eléréséről Ügyfelet a létesítés során tájékoztatja. A szolgáltatás maximális áthidalási ideje 10 nap.

Ügyfél riportok

- Mail forgalmi riportok: Napi vagy Heti rendszerességű az adatbekérő szerint, adatbekérőben megadott email címre.
- Óránkénti karantén értesítő az Ügyfél végfelhasználójának, akinek az emaile (bejövő email és a végfelhasználó a címzett) karanténba került.

Bejövő levélforgalom feldolgozása

A szolgáltatás az alábbi feldolgozási sorrendben biztosítja a bejövő mail forgalom védelmét:

- **Kapcsolat alapú szűrés**

  A bejövő levélforgalomban kapcsolat szintű szűrés a küldő szerverre vonatkozik, amely a reputációs és manuális listák segítségével IP szinten utasítja el a kapcsolódást, valamint érvényesíti a Transport Layer Security (TLS) beállításokat.

- **Email authentikáció**

  Különböző egymásra épülő email authentikációs eljárások (SPF, DKIM, DMARC) segítségével biztosít védelmet a hamisított feladó címen alapuló támadások ellen.

- **Vírus szűrés**

Többszintű víruskeresési eljárások segítségével keres kártékony kódokat az email üzenet törzsben és a csatolmányokban.

- **Spam szűrés**

  Mintaillesztési módszerrel, spam pontérték alapon akadályozza meg a kéretlen levelek továbbítását, és szűri a rosszindulatú web hivatkozást tartalmazó leveleket.

- **Tartalomszűrés**

  Tartalomszűrő szabályok segítségével korlátozható és blokkolható a mail forgalom levélméret, csatolmány típus, aktív tartalom vagy kulcsszó alapon.

Kimenő levélforgalom feldolgozása

Az Ügyfél a kimenő levélforgalomra vonatkozó szolgáltatási igényét, a Szolgáltató adatbekérése során igényelheti a kifelé irányuló mail forgalom szűrését is. A feldolgozás lépései:

- Transport Layer Security (TLS) kapcsolat felépítés, kikényszerítés
- Vírusszűrés

3. Szolgáltatás igénybevételének feltételei

- Az Ügyfél a rendszereit ismerő szakértőt biztosít a szolgáltatás telepítése során.
- Előfizető rendelkezik a működéshez szükséges interneteléréssel.
- A szolgáltatás igénybevételéhez az Ügyfél által használt levelező szerveren és DNS szerveren szükséges konfigurációkat az Ügyfél végzi el.

4. Létesítés folyamata:

Az Ügyfél által hiánytalanul kitöltött Adatbekérő(k) a Szolgáltató részére történő átadásától számított két hét. Ezen időtartamba nem számít bele az az időtartam mely alatt Szolgáltató az Ügyfél által megadandó adatok pontosítására vár, mint az alábbiak:

- Ügyfél IT rendszereinek konfigurálása a Szolgáltató által átadott Létesítési útmutató alapján,
- A Szolgáltató által az Ügyfél bejövő email-forgalmának tesztelésére küldött email-ek megérkezésének visszaigazolása (sorrendjére és tartalmára vonatkozóan), valamint azok esetleges meg nem érkezésére vonatkozóan is. A nem megfelelően beérkezett teszt email-ekkel kapcsolatos további technikai információk biztosítása a Szolgáltató számára (a Szolgáltató és Ügyfél egyeztetése alapján).

A szolgáltatás létesítettnek minősül, ha Ügyfél bejövő email-forgalmának teszt-emailekkel való tesztelése sikeresen lezárult, azaz amennyiben a Szolgáltató által az email domainenként Ügyfél által az Adatbekérőn megadott teszt email címekre küldött teszt levelek mindegyike megérkezett, és ezt az Ügyfél emailben visszaigazolja. Szolgáltató ezen időponttól nyújtja a szolgáltatást és jogosult a számlázásra.

Ügyfél bejövő és kimenő levélforgalmának átterelése az emailvédelmi szolgáltatásra az Ügyfél saját hatáskörében történik Szolgáltató előzetesen átadott Létesítési útmutató alapján. Amennyiben Ügyfél elvégezte az átállást, úgy Szolgáltató az Ügyfél megkeresésére ellenőrzi az átállás eredményességét központi oldalon. A Szolgáltató kapcsolati pontja a Service desk.

5. Szolgáltatás díjazása

A szolgáltatás ellenértékét az Egyedi Szolgáltatási Szerződés tartalmazza.

6. Rendelkezésre állás

- **Szolgáltatási szintek (SLA)**:

Szolgáltatás megnevezése	Szolgáltatás tartalma	Értéke
A gyártó által kibocsátott frissítések, javítások telepítése	A frissítések folyamatosan történnek gyártói oldalon. Nincs szükség integrátori beavatkozásra.	–
Hibaelhárítás rendelkezésre állása	Szolgáltató vállalja, hogy a szolgáltatás nem megfelelő működése* esetén a hibaelhárítást az adott időszakra értelmezett szolgáltatásként biztosítja.	5 x 8 óra
Manuális hibaelhárítás megkezdése	Szolgáltató vállalja, hogy a szolgáltatás nem megfelelő működése* esetén a hiba elhárítását a hiba bejelentésétől legkésőbb az adott időn belül elkezdi, a hibaelhárítás rendelkezésre állási időtartamához igazodva.	Megkezdés 4 órán belül
Éves rendelkezésre állás	Az éves rendelkezésre állás 365 napra vetítve történik.	99,9%
Igénykezelés	A bejelentett igények (pl. kivételkezelés, egyedi konfigurációs igények) feldolgozását Szolgáltató legkésőbb két munkanapon belül megkezdi.	két munkanapon belül

*A szolgáltatás nem megfelelő működése azt jelenti, hogy az Ügyfél számára küldött bejövő levelek, vagy az általa kiküldött kimenő levelek a szolgáltatás hibájából fakadóan nem érkeznek meg a címzettekhez, a karanténértesítés, karanténból történő kiszabadítás funkció sikertelen, az ütemezett riportok nem kerülnek kiküldésre, vagy ha a szolgáltatás által végzett biztonsági ellenőrzések nem kerülnek végrehajtásra a leveleken. A hibák észlelése és bejelentése az Ügyfél felelőssége.

Az SLA alkalmazásának korlátjai

- A rendelkezésre állási időtartamban nem számítandó bele a Szolgáltató által szükségesnek ítélt sürgősséggel elvégzendő beavatkozások ideje alatti szolgáltatás kiesés, melyek célja az infrastruktúra biztonságát vagy stabilitását vagy integritását érintő veszélyek elhárítása.

7. Kapcsolattartás

Kapcsolattartók	Név	Elérés
A Szolgáltató oldaláról (ügyfélszolgálat):	**Servicedesk**	Tel.: +36/80/40-80-80 Mail: servicedesk@telekom.hu Fax.: +36/1/432-8290

8. Adatvédelmi rendelkezések

A Szolgáltatással kapcsolatban a Szolgáltató (a továbbiakban: Adatfeldolgozó) az Ügyfél (a továbbiakban: Adatkezelő) adatfeldolgozójaként jár el az IÁSZF törzsrésze szerint.

	CTRL menedzselt emailvédelem szolgáltatás
A) Az adatkezelés tárgya:	email forgalom vizsgálata és szűrése a szolgáltatás részeként
B) Az adatkezelés jellege és célja:	a szolgáltatás nyújtásához szükséges hozzáférés, szűrés, módosítás, tárolás, továbbítás, naplózás a szolgáltatás nyújtása és az Adatfeldolgozó szerződésszerű teljesítése céljából
C) Az adatkezelés időtartama:	IASZF törzsrész *A személyes adatok kezelésének időtartama* pont szerint
D) Az érintettek kategóriái:	az Adatkezelővel szerződő vagy vele egyébként ügyfélkapcsolatban, üzleti kapcsolatban vagy más hasonló jogviszonyban álló természetes

	személy ügyfelek, előfizetők, felhasználók, partnerek stb. (a továbbiakban együtt: Partnerek), továbbá az Adatkezelő, illetve Partnereinek munkavállalói vagy munkavégzésre irányuló egyéb jogviszony keretében velük kapcsolatban álló természetes személyek, esetlegesen a Partnerek ügyfelei, előfizetői, felhasználói, üzleti partnerei, illetve ezek munkavállalói vagy velük munkavégzésre irányuló egyéb jogviszonyban álló személyek (a továbbiakban együtt: Érintettek)
E) A kezelt személyes adatok típusai	az Érintettek üzleti, kereskedelmi életben, illetve munkaviszony vagy munkavégzésre irányuló egyéb jogviszony kapcsán szokásosan elektronikus levelezőrendszerben kezelt személyes adatai
F) Az igénybe vett és az Adatkezelő által jóváhagyott al-adatfeldolgozók:	Lásd külön táblázatban alább, F.1) alpontban
G) Az Adatfeldolgozó általi tevékenységhez kapcsolódó technikai és szervezési intézkedések	IASZF törzsrész *Az adatkezelés biztonsága* pont szerint

Ha az Adatkezelő bármikor a szolgáltatás nyújtása során azt észleli, hogy az adatfeldolgozás, illetve az érintett személyes adatok jellemzői a fent leírtaktól eltérnek, az Adatkezelő köteles kezdeményezni a fenti táblázatban leírtak aktualizálását.

F.1) Az igénybe vett és az Adatkezelő által jóváhagyott al-adatfeldolgozók:

	CTRL menedzselt emailvédelem szolgáltatás
1. Al-adatfeldolgozó megnevezése	Trend Micro Inc.
2. Al-adatfeldolgozó főbb adatai (székhely, nyilvántartási szám, elérhetőség)	225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
3. Al-adatfeldolgozó adatkezeléssel kapcsolatos feladatai	Felhőalapú emailvédelem, licencsz és végponti SW biztosítása MSSP szolgáltató számára, hogy Ügyfél emailvédelmét biztosítsa.
4. Aladatfeldolgozó kapcsán harmadik országba történő adattovábbítás	Nincsen, kizárólag európai központokban kerül biztosításra az európai ügyfelek részére a szolgáltatás

9. Jogszabálytól, az IÁSZF törzsszövegtől eltérő feltételek:
A kapcsolattartás és az ügyfélszolgálat elérhetősége eltér az IÁSZF törzsszövegben meghatározottaktól. Ügyfél tudomásul veszi, hogy a Szolgáltató – tekintettel a szolgáltatás jellegére - a szándékosan okozott, továbbá emberi életet, testi épséget vagy egészséget megkárosító szerződésszegés kivételével kártérítési felelősségét kizárja.