15. számú melléklet: CTRL Menedzselt Végpontvédelem

1. Szolgáltatás meghatározása

A szolgáltatás keretében Szolgáltató biztosítja Ügyfél számára a végpontok kártékony kódok elleni védelmét. A szolgáltatás a munkaállomások és szerverek folyamatos ellenőrzését végzi, hagyományos és új generációs módszerekkel is.

A szolgáltatás igénybevételéhez nem szükséges az Ügyfél hálózatában központi felügyeleti szerver telepítése, a végpontvédelmi komponensek disztribúcióját és védendő gépekre történő feltelepítését kell megoldani Ügyfélnek.
A Szolgáltató a központi rendszerével **menedzselt végpontvédelmi szolgáltatást nyújt** az Ügyfél hálózatában.
Ennek keretében a Szolgáltató az Ügyfél számára dedikált tenant-ot létrehozza, a központi konfigurációt és a házirendeket kialakítja, valamint a végpontok védelméhez szükséges kliens oldali telepítő szoftvereket az Ügyfél rendelkezésére bocsátja.
A szoftverek a Trend Micro által kiadott és márkanévvel ellátott alkalmazások, amelyet Ügyfél számára helyben történő használatra bocsát rendelkezésre Szolgáltató. Az alkalmazás magában foglalja Ügyfél rendelkezésére bocsátott telepítési útmutatót és az online frissítést. Sem az alkalmazás, sem annak forráskódváltozata semmilyen esetben és semmilyen körülmények között nem kerül felajánlásra, licenszelésre vagy más módon Ügyfél rendelkezésére bocsátásra, illetve letétbe helyezésre.
Szolgáltató az Ügyfél részére, a szolgáltatás központi és végponti szoftverkomponenseinek rendszeres frissítését biztosítja, valamint lehetővé teszi az esetleges meghibásodások bejelentését, és elvégzi a rendszer hibáinak elhárítását.

2. Szolgáltatás elemei

A szolgáltatás keretében rendelkezésre álló funkciók

CTRL menedzselt végpontvédelmi szolgáltatás	**ALAP SZINTŰ**	**EMELT SZINTŰ**
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.	✓	✓
Több szintű adminisztratív hozzáférés (Role based access)	✓	✓
Beállítható házirend sablonok	✓	✓
Csoport alapú házirend kezelés elérhető	✓	✓
Végpontok bevonása többféle módon (telepítő link, telepítő csomag letöltése és disztribúciója 3rd party eszközzel, közvetlen telepítés a konzolt futtató végponton)	✓	✓
Biztonsági szolgáltatások		

CTRL menedzselt végpontvédelmi szolgáltatás	ALAP SZINTŰ	EMELT SZINTŰ
Gyártói felhős threat adatbázis	✓	✓
Klasszikus antivírus (szignatúra alapú vírusvédelem)	✓	✓
Új generációs antivírus (NGAV)	✓	✓
Zsarolóvírusok elleni célzott védelem	✓	✓
On-access scan	✓	✓
On-demand scan	✓	✓
Web reputáció és URL szűrés	✓	✓
URL fekete- és fehérlisták	✓	✓
Automatizált riportküldés	✓	✓
Device Control / USB control *	✓	✓
Mobile security – Android *	✓	✓
Application control *	✓	✓
Desktop Firewall *	✓	✓
Bitlocker kezelése (encrypt/decrypt) **	✓	✓
Vulnerability Protection **	✓	✓
Data Loss Prevention **	✓	✓

* A funkció hangolása a Felek között együttműködést igényel, így például a funkció által biztosított konfigurációs lehetőségek egyeztetését és beállítását az Ügyfél által használt környezetnek és elvárásoknak megfelelően. Ezek a funkciók csak Windows-alapú végpontokon érhetők el.
** A funkció központi szolgáltatási elem, a végpontokon nem kerül aktiválásra.

CTRL menedzselt végpontvédelmi szolgáltatás főbb funkciói

Általános szolgáltatások (felügyeleti funkciók)
A környezet biztosítja, hogy minden ügyfél részére egyedileg kialakított, más ügyféltől virtuálisan szeparált tenant-ban kerüljön kialakításra a szolgáltatás.

A szolgáltatói nézet teljes körű elérést és kontrollt biztosít a szolgáltatás által nyújtott biztonsági eseményekre, ezen keresztül történik a rendszer beállítása és karbantartása, valamint a központi létesítést követően a telepítő készletek biztosítása az Ügyfél részére, házirendek módosítása és a licencek Szolgáltató általi kezelése, megújítása, valamint a használattal kapcsolatos kimutatások elkészítése.

Klasszikus antivírus

A CTRL menedzselt végpontvédelmi szolgáltatás klasszikus antivírus képességei biztosítják az első védelmi vonalat a végpontokon kezelt fájlok írási és olvasási műveleteinek folyamatos ellenőrzésével,

valamint a memóriában futó alkalmazások vizsgálatával. A kreatív tömörítési módszerekkel elrejteni kívánt kártevők felismerésére kifejlesztett heurisztikus eljárás hatékonyan emeli a biztonsági szintet.

Az optimalizált ellenőrzési funkciónak köszönhetően a számítógépeken csak kisebb méretű vírusvédelmi adatbázist szükséges tárolni, ami nagy mértékben csökkenti a teljesítmény igényt, egyúttal az új kártevők felismeréséhez szükséges időtartamot is (közel valós idejű vírus adatbázisok). Az esetek többségében a lokális adatbázis alapján a döntést a helyi kliens-szoftver végzi, a kérdéses esetekben pedig a felhőszolgáltatásban elérhető információk alapján kerül sor blokkolásra vagy engedélyezésre.

A végpontvédelem kizárólag azokat az állományokat ellenőrzi, melyek a tényleges fájltípusuk alapján kártékony kódot tartalmazhatnak, ezzel tovább javítva a rendszer teljesítményét.

A veszélyesnek ítélt állományokat a fenyegetettség típusától függően karanténba helyezi és megőrzésre kerül vagy tisztítja a megoldás. Szükség esetén az eredeti fájl mindkét esetben a szolgáltatás ideje alatt visszaállítható az Ügyfél által.

Új generációs antivírus (NGAV)

Amíg a klasszikus vírusvédelmi megoldások kódrészeket és más, nem változó ismert jeleket keresnek, az új generációs víruskereső (NGAV) képes a hagyományos végpontvédelmet megkerülő fenyegetéseket jellegzetességeik, felépítésük és viselkedésük alapján megállítani.

Az NGAV modul képes fájl-alapú és csak memóriában futó (fileless) malware-k azonosítására. A tradicionális fenyegetéseken felül a zsaroló vírus viselkedést és kriptovaluta bányászatot is fel tudja ismerni.

Web reputáció és URL szűrés

A végponti URL szűrés segítségével szabályozhatja az Ügyfél a webhelyekhez való hozzáférést, csökkentheti a nem produktív internethasználatot és sávszélesség kihasználást, valamint biztonságosabb internet használatot kényszeríthet ki. Meghatározható az URL szűrés védelmi szintje, és a kategóriák alapján tételesen beállíthatja az Ügyfél, hogy mely típusú webhelyeket kíván korlátozni vagy szűrni.

A szolgáltatás megakadályozza, hogy a felhasználók kártékony vagy tiltott oldalakhoz férjenek hozzá, és biztosítja, hogy a megtekintett oldalak mentesek legyenek a rosszindulatú programoktól, kémprogramoktól és adathalász csalásoktól.

A szűrés akkor is működik, ha a végpont a határvédelmi eszközök (proxy, tűzfal) hatókörén kívül van.

A CTRL menedzselt végpontvédelmi szolgáltatás mögött álló web reputációs technológia folyamatosan nyomon követi az internetes domain-ek megbízhatóságát. Egyebek mellett a webhely kora, lokációs változásai és viselkedés-elemzés során felfedezett gyanús minták alapján súlyozott pontszámot rendel hozzájuk. A pontosság növelése és a fals pozitív találatok csökkentése érdekében a szolgáltatás egyes aloldalakhoz, vagy webhelyeken belüli hivatkozásokhoz rendeli hozzá a pontértékeket a teljes webhely osztályozása vagy blokkolása helyett.

3. Szolgáltatás igénybevételének feltételei

- Ügyfél köteles biztosítani a fizikai hozzáférést a szerverhelyiségbe az újonnan telepítendő eszközök beüzemeléséhez, amennyiben az Ügyfél kérése alapján Szolgáltató végzi a telepítést
- Az Ügyfél a rendszereit ismerő szakértőt biztosít a szolgáltatás telepítése során.
- A telepítés végrehajtásához az Előfizető végpontvédelmi kliens telepítését végző szakértőinek, esetlegesen felhasználóinak helyi rendszergazdai jogosultsággal kell rendelkezniük a végpontokon.
- Az Ügyfél rendelkezik internet eléréssel.
- Amennyiben Ügyfél munkaidőn túli (hétköznap 16:30-at követően) igényli a telepítést az Egyedi Szolgáltatási Szerződésben meghatározott költséget köteles megfizetni.
- A szolgáltatás igénybevételéhez szükséges, hogy a védett végpontok elérjék a felhőalapú központi szolgáltatást. Ennek biztosítására Ügyfél elvégzi az eléréshez az általa használt tűzfalon, router-en vagy web proxy-n megadandó engedélyező szabályok, kivételek beállítását.

- Az Ügyfél által a végpontvédelembe bevonni kívánt számítógépek meg kell felelniük az alábbi követelményeknek:

    - **Processzor**

Processzor	Operációs rendszer	Órajel
• Intel™ Pentium™ 4 x86 or compatible processor • x64 processor supporting AMD64 and Intel EM64T technologies	Windows 11, Windows 10	1 GHz
	Server 2016, Server 2019, Server 2022	1.4 GHz
1vCPU	Windows 365	-
• Intel™ Core • Apple Silicon	macOS Catalina v10.15 vagy újabb verzió	-

    - **Memória és tárhely**

Operációs rendszer	Agent-nek szükséges memória	Agent-nek szükséges tárhely
Windows 10, 11	Minimum: 1 GB Javasolt: 2 GB	Minimum: 1.5 GB Javasolt: 2 GB
Windows Server: 2016, 2019, 2022	Minimum: 2 GB Javasolt: 8 GB	
macOS Catalina v10.15 vagy újabb verzió	512 MB	Alapszintű csomag esetén: 300 MB Emeltszintű csomag esetén: 500 MB

Támogatott mobil operációs rendszer	**Android (Android 10.0 vagy újabb verzió)**

4. Létesítés folyamata

- A létesítés határideje 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.
- A szolgáltatás létesítettnek minősül, ha Szolgáltató elvégezte a központi konfiguráció kialakítását és átadta az Ügyfélnek a telepítőkészleteket. A telepítőkészlet átadásának időpontja egyben a létesítés lezárásának és a számlázás megkezdésének időpontját jelenti.
- Ügyfél a telepítőkészlet birtokában saját hatáskörében telepíti azt végpontjaira.

A létesítésben érintett rendszerek hozzáféréséhez szükséges jogosultságokat az Ügyfél a Szolgáltató számára biztosítja a létesítés ideje alatt, amennyiben Ügyfél Szolgáltatótól kéri a kliens(ek) telepítését.

- Az Ügyfél biztosítja a feladatok elvégzésében érintett eszközökhöz történő hozzáférést (mind fizikálisan, mind virtuálisan)
- Ügyfél biztosítja a munkavégzés helyére történő bejutást (pl. telephelyre, szerverszobába)
- A felmérés ideje alatt kompetens személyek elérhetőségének biztosítása konzultációs céllal.

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 gyártó által díjmentesen kibocsátott frissítések, biztonsági javítások telepítésére automatikusan sor kerül Szolgáltatói beavatkozás nélkül.	-
Hibaelhárítás rendelkezésre állása	Szolgáltató vállalja, hogy a szolgáltatás nem megfelelő működése* esetén a hibaelhárítást az adott időszakra értelmezett szolgáltatásként biztosítja.	5 x 8 órában
Manuális hibaelhárítás megkezdése	Szolgáltató vállalja, hogy a szolgáltatás nem megfelelő működése* esetén a bejelentett hibák elhárítását legkésőbb az adott időn belül elkezdi, a hibaelhárítás rendelkezésre állási időtartamához igazodva.	Megkezdés 4 órán belül
Igénykezelés	A bejelentett igények (egyedi finomhangolás, pl. kivételkezelés esetén) feldolgozását Szolgáltató legkésőbb két munkanapon belül megkezdi.	két munkanapon belül

*A szolgáltatás nem megfelelő működése azt jelenti, hogy a központi végpontvédelmi menedzsment rendszer nem elérhető, nem működik megfelelően, vagyis a központi szolgáltatás hibájából fakadóan az Ügyfél védett végpontjai tömegesen (a gépek legalább 40 százaléka érintett) nem kapják meg megfelelő beállításokat, vagy nem hajtják végre a gyártó által biztosított biztonsági ellenőrzéseket, funkciókat, vagy a központi szolgáltatás hibájából fakadóan az Ügyfél védett végpontjai tömegesen (a gépek legalább 40 százaléka érintett) nem tudják letölteni a rendszeresen frissülő gyártói biztonsági mintákat, adatbázisokat, vagy nem kerülnek kiküldésre az automatizált riportok.
A központi végpontvédelmi menedzsment rendszerből ellenőrizhető működési paramétereket a Szolgáltató is monitorozza, de a hibák észlelése és bejelentése az Ügyfél felelőssége.
Az egyes végpontvédelmi klienseket érintő, nem tömeges hibák adott végpont operációs rendszerén, vagy egyéb paramétereiben történő változtatással, esetleg a végpontvédelmi kliens újratelepítésével történő javításáért az Ügyfél felel.

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 CTRL menedzselt végpontvédelmi szolgáltatással kapcsolatban a Szolgáltató (a továbbiakban: Adatfeldolgozó) az Ügyfél (a továbbiakban: Adatkezelő) adatfeldolgozójaként jár el az IÁSZF törzsrésze szerint.

	CTRL menedzselt végpontvédelmi szolgáltatás
A) Az adatkezelés tárgya:	A szolgáltatás részeként kártékony kódok elleni végpontvédelem, végponti vizsgálat
B) Az adatkezelés jellege és célja:	A szolgáltatás nyújtásához végponti vizsgálat, végponti eseményekkel kapcsolatos adattárolása szolgáltatás nyújtása és az Adatfeldolgozó szerződésszerű teljesítése céljából
C) Az adatkezelés időtartama:	IÁSZF 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 kezelt személyes adatai; egyedi azonosítói (pl. MAC-cím, felhasználónév)
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 végpontvédelmi szolgáltatás
1. Al-adatfeldolgozó megnevezése	Trend Micro Inc.
2. Al-adatfeldolgozó főbb adatai (székhely, nyilvántartási szám, elérhetőségei)	225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
3. Al-adatfeldolgozó adatkezeléssel kapcsolatos feladatai	Felhőalapú végpontvédelem, licensz és végponti SW biztosítása MSSP szolgáltató számára, hogy Ügyfél végpontvédelmét biztosítsa
4. Aladatfeldolgozó kapcsán harmadik országba történő adattovábbítás	Nincs, kizárólag európai központokból biztosítja európai ügyfeleinek a szolgáltatást.

9. Jogszabálytól, az IÁSZF törzsszövegtől eltérő feltételek:

A kapcsolattartás és az ügyfélszolgálat elérhetősége eltér az IÁSZF törzsszövegben meghatározottaktól. Ügyfél továbbá 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.