



# Heimdal®

*Megfelelés a NIS 2 irányelvnek*

*Heimdal  
Security*

*Kibervédelmi megoldásai*

## ARLITECH

BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

# *Heimdal által nyújtott védelem*



TÁVOLI ELÉRÉS



DNS FORGALOM  
VIZSGÁLATA



ZSAROLÓVÍRUSOK  
ELLENI VÉDELEM



PATCH  
MANAGEMENT



EMELT SZINTŰ  
JOGOSULTSÁGOK  
KEZELÉSE



ÚJGENERÁCIÓS  
VÍRUSVÉDELEM

**ARLITECH**

BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK



## Újgenerációs vírusvédelem

*A hagyományos vírusvédelmi megoldások ugyan szükségesek, de nem nyújtanak megfelelő védelmet a fejlett támadásokkal szemben.*

*A Heimdal Security újgenerációs végpontvédelmi megoldása a tradicionális, megszokott technológiák mellett olyan funkciókat is tartalmaz, melyekkel hatékonyabb védelmet biztosít a még ismeretlen támadások ellen is.*

**Főbb tulajdonságok:**

- SandBox technológia
- Zero Trust védelem az ismeretlen fenyegetések ellen
- BruteForce támadások elleni védelem
- Fejlett tűzfal menedzsment
- Helyi és felhős adatbázis
- Heurisztika és viselkedés elemzés
- Mobile Device Management

## DNS forgalom vizsgálata



*A sikeres támadások több, mint 90%-ában a támadók használnak valamilyen internetes kommunikációt, mint a malware vagy adathalász oldalak, külső irányító szerverek (CnC) és a DNS átirányítás.*

*A Heimdal Security DNS szűrő megoldása nem egy szimpla URL szűrő megoldás, hanem egy hatékony kiegészítő védelem a végpontokon és hálózati szinten, mely megakadályozza a kártékony kommunikációt a HTTP, HTTPS és DNS forgalom ellenőrzésével.*

*A hagyományos vírusvédelmi megoldások jelentős hányada az internetes forgalmat ilyen mélységben nem ellenőrzi.*

**Főbb tulajdonságok:**

- HTTP, HTTPS, és DNS forgalom biztonsági ellenőrzése, a kártékony forgalmak blokkolása
- Kategória szerinti URL szűrés
- Helytől független működés (munkahelyi, publikus vagy otthoni hálózat)
- 96%-os pontosságú hatékonyság a még jövőbeni fenyegetések esetén is
- Felhasználótól független, rejtett kommunikáció ellenőrzése és a kártékony folyamatok blokkolása

**ARLITECH**

BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK



## Zsarolóvírusok elleni védelem

*Napjainkban a szervezetek számára az egyik legnagyobb veszélyforrás a zsarolóvírus támadás, melynek következtében a cégek adatait egy rosszindulatú kód vagy folyamat segítségével titkosítják, használhatatlanná teszik a támadók.*

*Jellemzően az adatok titkosításának visszafejtésére nincs mód, ezért a megelőzés a legjobb védelem.*

*A Heimdal Security Ransomware Encryption Protection megoldása egy célszköz a zsarolóvírusok ellen, mely kiegészíti a hagyományos vírusvédelmi megoldásokat, melyek a leginkább fertőző, úgynevezett nulladik napi zsarolóvírusok ellen nem tudnak védelmet biztosítani.*

**Főbb tulajdonságok:**

- **Kiegészítő védelem bármely más végpontvédelmi megoldás mellé**
- **Adatbázis nélküli működés**
- **Input/Output és Read/Write folyamatok ellenőrzése**
- **Káros folyamatok blokkolása**
- **Hálózati aktivitás figyelése**
- **Részletes forensic adatok, mélységi elemzés**

## Patch Management



**Telepítés, hibajavítás és szoftver menedzsment**

*A sikeres támadások 90%-ában valamely szoftver ismert sérülékenységet használják ki a kiberbűnözők, melyre sok esetben a gyártó már kiadta a frissítést, de azt még nem telepítették az eszközökre.*

*Éppen ezért a szoftverek - beleértve az operációs rendszert is - naprakész állapota a biztonság, a hibajavítások és az új funkciók elérése szempontjából elengedhetetlen.*

*Megfelelő eszköz nélkül szinte lehetetlen a szervezeteknél a rendszerek naprakész állapotának fenntartása, új szoftverek központi telepítése és eltávolítása, illetve a meglévő szoftver licenzek nyilvántartása.*

**Főbb tulajdonságok:**

- **Microsoft és Linux operációs rendszerek központi, automatizált frissítése**
- **Közel 170 3rd party szoftver központi, automatizált frissítése, telepítése, és eltávolítása**
- **Szoftver leltár**
- **Szoftver előfizetések kezelése**

**ARLITECH**

BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK



## Emelt szintű jogosultságok kezelése



*Az elmúlt, lassan három évben a megváltozott munkavégzési folyamatok (Home Office, Hybrid Office) következtében az informatikusok egyik legnagyobb kihívása a felhasználói jogosultságok kezelése.*

*Gyakran a munkavégzéshez szükséges folyamatokhoz vagy akár egyes programok frissítéséhez helyi rendszergazdai jogosultság szükséges. Sokszor, kényelemből vagy időhiány miatt, a felhasználóknak állandó rendszergazdai jogosultságot biztosítanak, pedig ez egy esetleges incidens esetén sokkal sebezhetőbbé teszi a rendszert, illetve sokkal szabadabb kezet ad a felhasználónak.*

*Olyan programokat telepíthet, amelyek nincsenek ellenőrizve, vagy nincsen szükség rájuk a munkavégzéshez (például torrent vagy játék), szolgáltatásokat kapcsolhat ki, illetve programokat törölhet véletlenül vagy szándékosan.*

*Erre ad megoldást a Heimdal Security központi jogosultság kezelő modulja, melynek segítségével a felhasználók részére ideiglenesen adhat a helyi rendszergazda jogot.*

**Főbb tulajdonságok:**

- **Ideiglenes rendszergazdai jog kiosztása egy adott folyamatra**
- **Ideiglenes rendszergazdai jog kiosztása egy adott időtartamra**
- **Meglévő rendszergazdai jog visszavonása központilag**
- **96%-os pontosságú hatékonyság a még jövőbeni fenyegetések esetén is**
- **Felhasználótól független, rejtett kommunikáció ellenőrzése és a kártékony folyamatok blokkolása**



## Távoli elérés

**Főbb tulajdonságok:**

- **Titkosított kapcsolat**
- **Képernyő átvétel és megosztás**
- **Fájl műveletek végrehajtása**
- **Többféle elérési lehetőség**
- **Chat funkció**
- **Automatikus videó felvételi lehetőség a csatlakozásról**
- **Audit logok a csatlakozásról**
- **Csatlakozási folyamatok naplózása**

*A napjainkra jellemző vegyes munkavégzés, vagy több telephelyes szervezetek részére a rendszergazdák egyik legfontosabb kihívása a megfelelő távoli segítségnyújtás.*

*A Heimdal Security megoldásának segítségével az adminisztrátorok helytől függetlenül, titkosított, ellenőrzött módon csatlakozhatnak a távoli számítógépekre.*