CYBERSECURITY
maxvalor
Heimdal's Leading CEE Distributor

AZ IT-BIZTONSÁG SZÜRKE FOLTJAI

M365 • helyi admin jogok • frissítések • AI Containment

Heimdal®

AUGMENTT

Pentest Tools

Kik vagyunk és milyen gyártókkal dolgozunk?

MaxValor: helyi szakértelem, egymást kiegészítő kiberbiztonsági technológiák

MAXVALOR

25+ év — IT-márkák és gyártók piaci felépítésében

CEE — regionális jelenlét és partneri együttműködés

100% — channel modell, helyi presales és technikai támogatás

Magyar nyelvű támogatás • gyártói eszkaláció • oktatás és webinárok

H — Heimdal®

Egységes kiberbiztonsági platform

10+ integrált modul • XDR/MXDR • endpoint, identitás, e-mail és hozzáférés

A — AUGMENTT

Microsoft 365 Security & Management

Multi-tenant audit, monitorozás, biztonsági baseline-ok és automatizált riportok

P — Pentest Tools

Offenzív biztonság és validáció

Attack Surface, webes és hálózati vizsgálatok, folyamatos sérülékenység-felderítés

Három technológiai réteg, egy helyi disztribútori és támogatási háttér.

CYBERSECURITY maxvalor Heimdal's Leading CEE Distributor

Heimdal®

Agenda

Négy üzleti kockázati terület és egy 90 napos cselekvési terv

01 Miért vezetői kérdés?

02 Microsoft 365 fiókok

03 Helyi admin jogosultság

04 Elmaradt frissítések

05 AI-használat: statisztikák és kockázatok

06 Heimdal AI Containment

07 Vezetői KPI-k és 90 napos terv



Miért vezetői kérdés az IT-biztonság?

A technikai incidens üzleti veszteséggé alakul.

MŰKÖDÉS

Leálló levelezés, fájlmegosztás, ERP vagy ügyfélkiszolgálás.

PÉNZÜGY

Csalás, helyreállítás, kieső árbevétel és kötbérek.

BIZALOM

Ügyfelek, partnerek, reputáció, GDPR és felelősség.

Mennyi idő alatt állna meg a működés e-mail és fájlhozzáférés nélkül?

A támadás tipikus láncolata

A négy témát ugyanaz a logika kapcsolja össze.

BELÉPÉS

Adathalász levél, sérülékeny alkalmazás vagy engedély nélküli AI.

HOZZÁFÉRÉS

Ellopott identitás, helyi admin jog vagy túl széles AI-engedély.

ÜZLETI KÁR

Csalás, leállás, adatvesztés és reputációs kár.

A megelőzés célja a láncolat korai megszakítása.

1. Microsoft 365 fiók kompromittálása

Egy ellopott identitás hozzáférést adhat a teljes digitális környezethez.

RÖVID FORGATÓKÖNYV

A pénzügyi vezető hamis bejelentkezési értesítést kap. A támadó belép, megfigyeli a levelezést, majd egy valós ügyletbe beilleszkedve módosított bankszámlaszámot küld.



Üzleti hatás: pénzügyi csalás • adatszivárgás • bizalomvesztés

Mit érhet el a támadó egy M365 fiókkal?

A kár a szerepkörtől és a hozzáférésektől függ.

LEVELEZÉS ÉS NAPTÁR

Üzleti levelezés, számlák, naptárak és visszaállító üzenetek. A támadó kereshet pénzügyi folyamatokra, partnerekre és jelszó-visszaállításokra.

FÁJLOK ÉS TEAMS

OneDrive-, SharePoint- és Teams-tartalmak a felhasználó meglévő jogai szerint. A megosztott linkek és szinkronizált fájlok tovább növelhetik a kitettséget.

MEGSZEMÉLYESÍTÉS

Belső és partneri megszemélyesítés, postaláda-szabályok létrehozása, beszélgetések eltérítése és üzleti e-mailes csalás.

Az identitás elsődleges vállalati védelmi vonal.

Megelőzés az M365 környezetben

E-mail védelem és biztonsági állapotfelügyelet.

AUGMENTT

MFA-lefedettség, örökölt hitelesítés, túl széles jogosultságok, külső megosztások, baseline-eltérések és konfigurációs drift folyamatos láthatósága.

HEIMDAL EMAIL SECURITY

Adathalászat, BEC, káros linkek és mellékletek szűrése; gyanús feladók, domainek és kommunikációs minták vizsgálata.

VEZETŐI KONTROLL

Mérje az MFA-lefedettséget, a magas kockázatú bejelentkezéseket, a privilegizált fiókokat, a külső megosztásokat és az incidensreakció idejét.

Cél: a veszélyes üzenet megállítása és a hibás beállítás láthatóvá tétele.

2. A helyi rendszergazdai jog veszélye

A kényelmi jogosultság a kártevő számára gyorsítópálya.

RÖVID FORGATÓKÖNYV

Egy munkatárs helyi admin joggal nyit meg fertőzött mellékletet. A kártevő magasabb joggal települ, rendszerbeállítást módosít, hitelesítő adatot gyűjt és továbbterjed.



A támadó a kompromittált felhasználón keresztül kapja meg a főkulcsot.

A helyi admin jog következményei

A felhasználói hiba rendszerszintű incidenssé válhat.

RENDSZERMÓDOSÍTÁS

Szolgáltatások, registry, biztonsági beállítások és védelmi komponensek módosítása; tartós hozzáférés és védelemkikapcsolás.

HITELESÍTŐ ADATOK

Böngészőben, kliensben vagy memóriában használt hitelesítő adatok és tokenek megszerzése, majd más fiókok átvétele.

TOVÁBBTERJEDÉS

VPN-, megosztás- és hálózati hozzáféréseken keresztüli oldalirányú mozgás, több végpont és szerver kompromittálása.

A helyi admin jog a számítógép digitális főkulcsa.

Megelőzés: legkisebb szükséges jogosultság

Heimdal PEDM és Application Control.

NORMÁL JOG

Alaphelyzetben normál felhasználói jogosultság. Az admin fiók legyen külön, névre szóló, MFA-val védett és csak adminisztrációra használt.

KONTROLLÁLT EMELÉS

Feladathoz kötött, jóváhagyott és időkorlátos jogosultságemelés. Minden emeléshez indoklás, napló és visszavonás tartozzon.

ALKALMAZÁSKONTROLL

Engedélyezési lista, kiadói tanúsítvány, fájlútvonal és hash alapján korlátozható az ismeretlen vagy nem jóváhagyott programok futása.

Az állandó admin jog ne alapállapot, hanem naplózható kivétel legyen.

3. Elmaradt frissítések

Az ismert sérülékenységek nyitva maradnak.

RÖVID FORGATÓKÖNYV

Egy böngésző, PDF-olvasó vagy VPN-kliens hónapok óta nem frissült. A támadó ismert hibát használ ki, bejut, majd adatot lop vagy zsarolóvírust indít.



Hétfő reggel: nincs fájlszerver, nem működik az ERP.

A frissítés nem csak a Windowsról szól

A teljes alkalmazási környezetet kell kezelni.

OPERÁCIÓS RENDSZER

Windows, Linux és macOS biztonsági, minőségi és funkciófrissítései. A kritikus javításokat tesztcsoport után gyorsított ütemben kell teríteni.

KÜLSŐ ALKALMAZÁSOK

Böngészők, PDF-eszközök, Java, VPN-, távoli elérési és kommunikációs kliensek. A 3rd-party szoftverek külön patch-folyamatot igényelnek.

FOLYAMAT

Eszközleltár, kockázati prioritás, tesztelés, ütemezés, telepítés, újraindítás, hibakezelés és végrehajtási riport.

Amit nem tartunk nyilván, azt nem tudjuk következetesen frissíteni.

Heimdal Patch & Asset Management

Központi láthatóság és automatizált javítás.

LÁTHATÓSÁG

Eszköz- és szoftverleltár, verziók, hiányzó javítások, sérülékenységi kitettség és a támogatásból kifutott alkalmazások azonosítása.

AUTOMATIZÁLÁS

Ütemezett OS- és támogatott 3rd-party frissítés, pilot és éles gyűrűk, karbantartási ablakok, újraindítási szabályok és sikertelen telepítések újrapróbálása.

ELLENŐRZÉS

Végrehajtási riportok, megfelelőségi arány, kritikus hiányok, kivételek és kockázatos végpontok. Vezetői cél: csökkenő javítási idő és kitettségi ablak.

Rövidebb kitettségi ablak és kiszámíthatóbb üzemeltetés.

4. Az AI-használat új kockázati dimenziója

Nem az a kérdés, használják-e. Az a kérdés, látjuk-e és kontrolláljuk-e.

KIINDULÓPONT

A magyar vállalatok AI-használata gyorsan nő, miközben a jóváhagyott eszközök, adatkezelési szabályok és technikai kontrollok gyakran lemaradnak.



A produktivitást meg kell őrizni, a kontrollálatlan adatáramlást meg kell állítani.

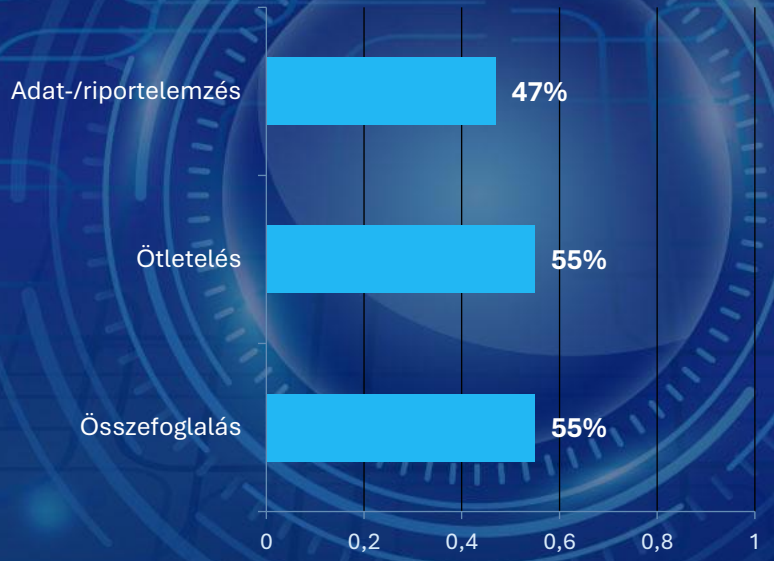
Shadow AI: személyes fiókok a munkahelyen

Nem magyarországi adat, hanem 2025-ös nemzetközi vállalati felmérések eredménye.

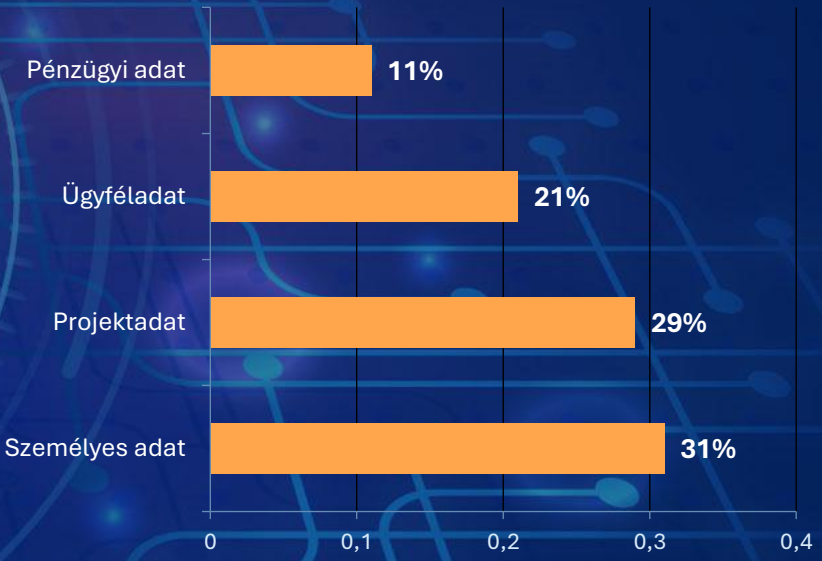
68% személyes fiók



Mire használják?



Milyen adat kerül be?



A személyes fiók gyors és kényelmes, de kívül esik a vállalati SSO, naplózás, megőrzés és kiléptetési kontroll hatókörén.

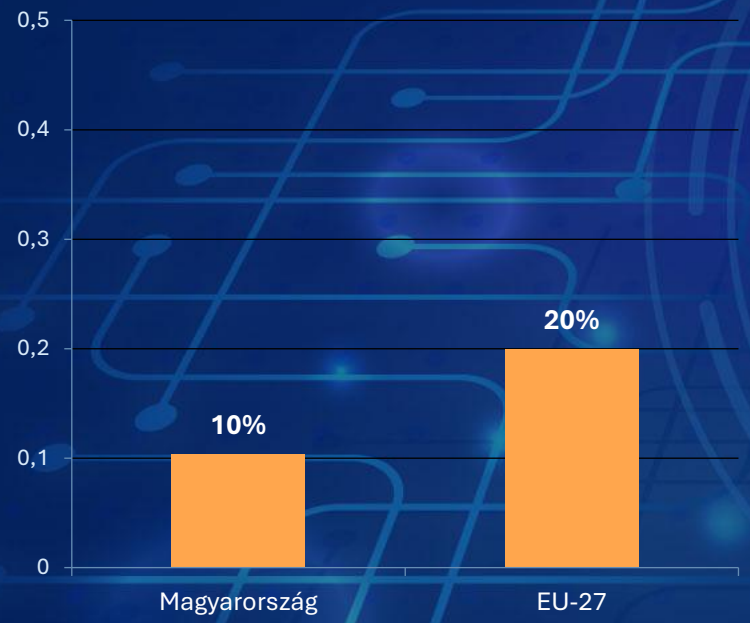
CYBERSECURITY maxvalor
Heimdal's Leading CEE Distributor

Heimdal®

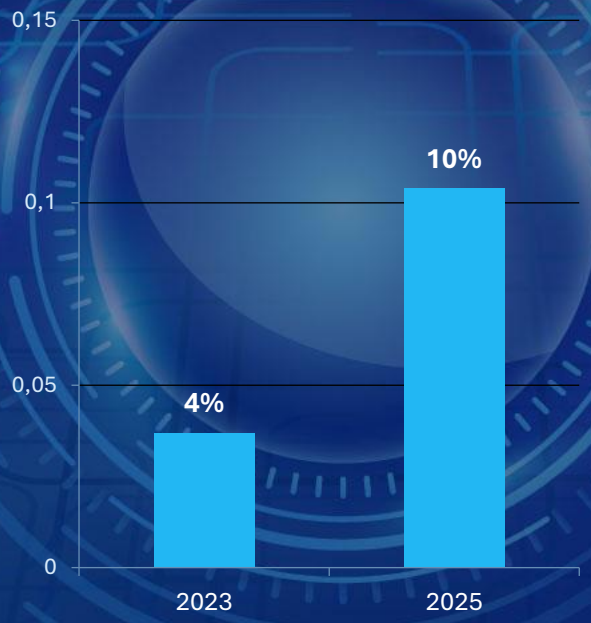
AI-használat Magyarországon és az EU-ban

Eurostat, 2025: legalább 10 főt foglalkoztató vállalatok

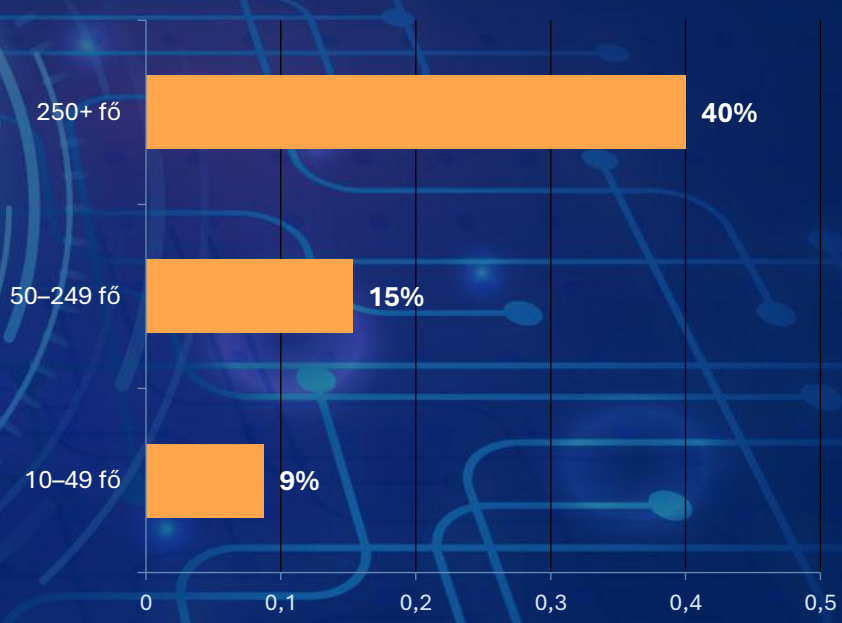
AI-t használó vállalatok, 2025



Növekedés Magyarországon



Magyar vállalatméret szerint



A gyors növekedés miatt a szabályozásnak, oktatásnak és technikai kontrollnak együtt kell fejlődnie.

CYBERSECURITY maxvalor
Heimdal's Leading CEE Distributor
Heimdal®

Vezetői AI-governance: mit kell eldönteni?

Nem az AI betiltása, hanem az engedélyezett használat kijelölése.

ENGEDÉLYEZETT ESZKÖZÖK

Mely szolgáltatások, vállalati csomagok és fióktípusok használhatók?

ENGEDÉLYEZETT ADATOK

Milyen adat tölthető fel, és mely adat soha nem kerülhet nyilvános AI-ba?

EMBERI ELLENŐRZÉS

Mely döntésnél, kommunikációnál vagy automatizmusnál kötelező a felülvizsgálat?

A biztonságos AI-használat üzleti szabály, technikai kontrollokkal kikényszerítve.

Heimdal AI Containment: réteges kontrollmodell

Láthatóság, hozzáférés, futtatás, izoláció és jogosultságkezelés.

NÉGY KONTROLLRÉTEG

CASB és DNS Security: felderítés és webes hozzáférés
Application Control: futtatás
AppFencing: hálózati izoláció
PEDM: jogosultságemelés kontrollja



Nem egyetlen blokkolás, hanem több, egymást kiegészítő kontrollréteg.

DNS Security: webes AI-hozzáférés kontrollja

Naplózás, engedélyezés és blokkolás DNS-szinten.

GYAKORLATI MODELL

AI-kategória és domainek megfigyelése. Nem jóváhagyott szolgáltatások blokkolása. Jóváhagyott vállalati szolgáltatás allowlistre helyezése. Végponti vagy hálózati alkalmazás.



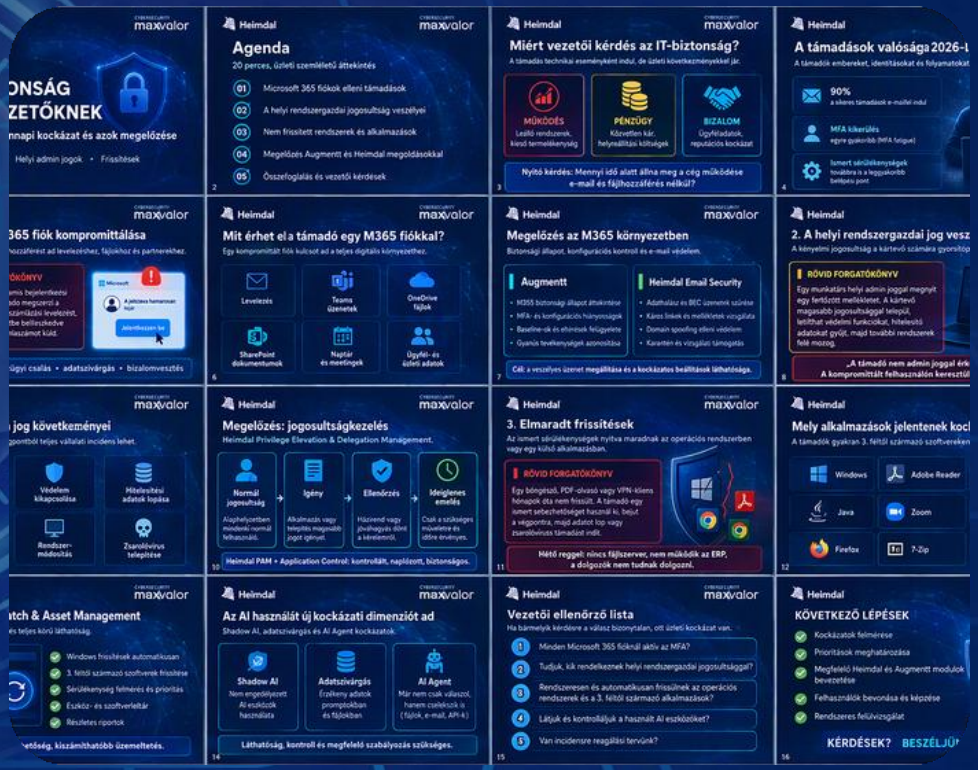
Példa: vállalati Copilot engedélyezhető, más nyilvános AI-szolgáltatások tiltva maradhatnak.

AppFencing + PEDM: műveleti határok

Az AI futhat, de ne kommunikáljon és ne emeljen jogosultságot korlátlanul.

KÉT FÉK

AppFencing: helyi futás internet- vagy célzott hálózati elérés nélkül. PEDM: az AI vagy az általa indított folyamat ne kapjon észrevétlenül magasabb jogosultságot.



Cél: az AI végrehajtási láncának megszakítása.

CYBERSECURITY maxvalor
Heimdal's Leading CEE Distributor

Heimdal®

Biztonságos AI-használat: javasolt működési modell

Fokozatos bevezetés monitor módból célzott enforcement felé.

1	**FELMÉRÉS**	30 napos használati kép
2	**DÖNTÉS**	Jóváhagyott eszközök és adatok
3	**KONTROLL**	DNS, CASB, App Control, AppFencing, PEDM
4	**OKTATÁS**	Konkrét tiltott és engedett példák
5	**FELÜLVIZSGÁLAT**	Havi riport és kivételkezelés

Monitor mód → célzott szabályok → mérhető vezetői kontroll.

Milyen mutatókat lásson a vezetőség?

A technikai eseményeket üzleti kockázati mutatókká kell fordítani.

IDENTITÁS ÉS JOGOSULTSÁG

MFA-lefedettség • admin joggal rendelkező végpontok • Jogosultság emelések

FRISSÍTÉSI ÁLLAPOT

Kritikus hiányzó javítások • javítási idő • alkalmazáslefedettség

AI-HASZNÁLAT

Felderített AI-szolgáltatások • tiltott elérések • kivételek

A dashboard a kockázat trendjét és a döntések hatását mutassa.

90 napos vezetői cselekvési terv

Konkrét, mérhető és fokozatos kockázatcsökkentés.

0–30. NAP

M365, admin jog, patch és AI-használat felmérése. Felelősök kijelölése.

31–60. NAP

Jóváhagyott AI-lista, policy-k, pilot csoport és oktatás.

61–90. NAP

Célzott blokkolás és izoláció, KPI-riport, kivételkezelés és gyakorlat.

A cél a kontrollálatlan kockázat folyamatos csökkentése.

Öt vezetői kérdés

Ha bármelyik válasz bizonytalan, ott kezelendő kockázat van.

1. **Minden M365 fióknál megfelelő az MFA és a konfiguráció?**
2. **Pontosan kik rendelkeznek helyi admin joggal?**
3. **Rendszeresen frissül az OS és a külső alkalmazások köre?**
4. **Látjuk, milyen AI-eszközöket használnak a munkatársak?**
5. **Van AI-policy, oktatás és incidensreakció?**

Nem az a kérdés, hogy lesz-e támadás. Az a kérdés, mennyire vagyunk felkészülve.

CYBERSECURITY
maxvalor
Heimdal's Leading CEE Distributor

Heimdal®



KÖSZÖNÖM A FIGYELMET

Kérdések és válaszok

Bardócz Gyula | MaxValor CEE Kft.

Heimdal®

AUGMENTT

Pentest Tools