ISACA KONFERENCIA 2026

Hargitai Zsolt

Szuverén AI

Adatvédelem és kontroll
a generatív modellek korában

2026.06.02.

SUSE

ISACA
Budapest Chapter

A SUSE-ról

1992
Founded in Nuremberg

HQ
Luxembourg

40
Offices

2,600
Employee

$700M+
Revenue

10,000+
Enterprise Customers

90%+
Of the world's leading companies rely on SUSE [6]

10/10
of the largest **Automotive** companies

13/15
of the largest **Pharmaceutical** companies

14/15
of the largest **Aerospace** companies

13/15
of the largest **FinServ** companies

Common Criteria SLSA

Top Supply Chain Security Certifications [3]

Developer contributions measured every day →

Publicly ranked alongside the largest technology companies

Consistently

Top 5 OSSRANK

Top 8 CLOUD NATIVE COMPUTING FOUNDATION

Top 12 OSCI

Recognized leader in Container Management & Virtualization → [2]

Gartner IDC OMDIA

United Nations Global Compact

17% emissions reduction since 2022 [4]

World-class ecosystem of partners

5 years in a row [5]

THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE WINNER 2024

SUSE

[1] SUSE Company Data [2] Gartner Magic Quadrant + Omdia [3] Common Criteria, SLSA [4] The UN Global Compact [5] suse.com/partners [6] SUSE Customer Data

Válaszok az informatika legfontosabb kihívásaira

Költségek optimalizálása heterogén környezetben

Modernizálás alkalmazás és infrastruktúra

Biztonság a modern rendszerekben is

A mesterséges intelligencia biztonságos használata

SUSE

ISACA Budapest Chapter

Válaszok az informatika legfontosabb kihívásaira

Költségek optimalizálása heterogén környezetben

Modernizálás alkalmazás és infrastruktúra

Biztonság a modern rendszerekben is

A mesterséges intelligencia biztonságos használata

SUSE

ISACA Budapest Chapter

A "Black Box" kockázatai

Miért veszélyes a publikus felhős AI a vállalatoknak?

- Shadow AI
  - A kontrollálatlan lakossági eszközök térnyerése a céges hálózatban.
- Adatszivárgás
  - Mi történik a promptokba írt üzleti titkokkal?
- Compliance rések
  - GDPR, EU AI Act stb.
- Függőség
  - A "Vendor Lock-in" veszélyei zárt modellek esetén.

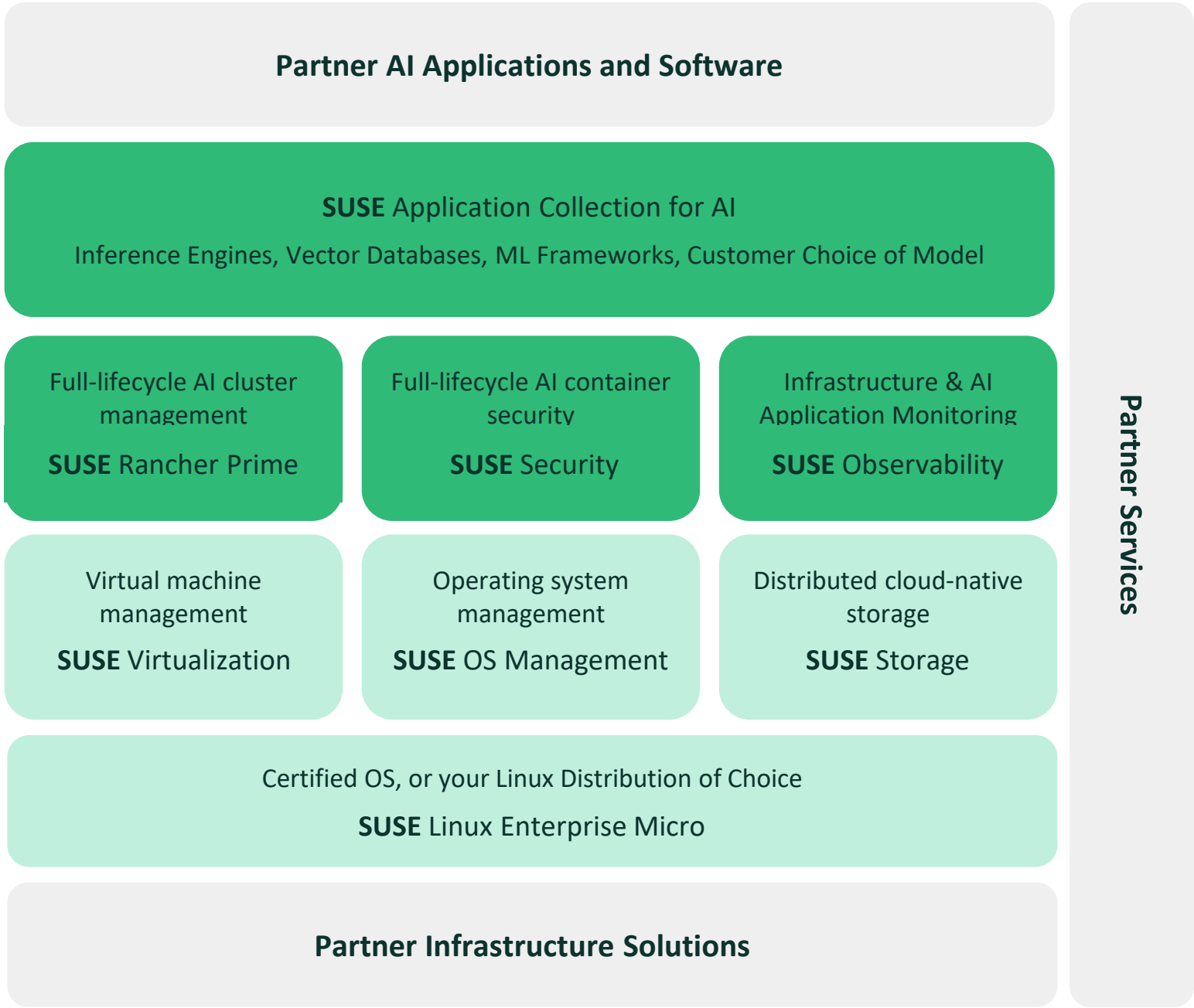
Szuverén AI

Definíció és elvárások:

- Helyi futtatás (On-prem/Private Cloud):
  - Az adatok soha nem hagyják el az adatközpontot.
- Auditálhatóság:
  - Nyílt forráskódú modellek és transzparens infrastruktúra.
- Kontroll:
  - Teljes felügyelet a tanítóadatok és a modell kimenete felett.
- Fenntarthatóság:
  - Hosszú távú stratégia, amely nem egyetlen szolgáltatótól függ.

SUSE AI

Egy integrált, felhőalapú platform ellenőrzött komponensekkel



SUSE AI – biztonsági szolgáltatások

- Auditálható keretrendszer
  - a szabályozási követelmények teljesítéséhez
- Nulla bizalom elv alkalmazása
  - „Soha ne bízz; mindig ellenőrizz”
- Átfogó konténerbiztonság
  - Hálózati szegmentálás
  - Sebezhetőségi vizsgálat
  - Futás idejű biztonság
  - Szabályzat betartatása
- „Upstream” komponensek biztonsága
  - A biztonsági helyzet folyamatos nyomon követése

SUSE

ISACA Budapest Chapter

SUSE AI Universal Proxy

AI ügynökök biztonságos használata

- MCP proxy szolgáltatás
  - Teljes funkcionalitású HTTP proxy MCP szerverekhez fejlett munkamenet-kezeléssel, hitelesítéssel és protokollfordítással.
- Hálózatfelderítés
  - Automatizált hálózati szkennelés az MCP szerverek felderítéséhez, a hitelesítési típusok észleléséhez és az esetleges biztonsági rések felméréséhez.
- Szervernyilvántartás
  - MCP szerverek nyilvántartása, beleértve a GitHub, SUSE MCP, Atlassian, Gitea és több mint 20 más népszerű szolgáltatást.
- Bővítménykezelés
  - Dinamikus bővítményrendszer a funkcionalitás bővítéséhez szolgáltatásregisztrációval, állapotfigyeléssel és képesség-útválasztással.

SUSE

ISACA Budapest Chapter

Miért a SUSE a jó választás?

- Nincs Vendor Lock-in:
  - Bármikor váltható a modell vagy az infrastruktúra.
- Költséghatékony:
  - Nincs rejtett API költség; fix, tervezhető licenszelés.
- Közösségi erő:
  - A nyílt forráskód - gyors biztonsági frissítések.
- Összetett védelem:
  - Az OS-től az AI-ig egy kézben a biztonsági támogatás.

SUSE

ISACA Budapest Chapter

Hargitai Zsolt
zsolt.hargitai@suse.com