ORACLE

Bezpečnost dat v éře AI: od databáze ke generativní inteligenci

6 principů pro ochranu dat proti novým hrozbám

Tomáš Trnka
Oracle Czech

ISSS Mikulov

8.9. 2026

Prohlášení podle zásady „safe harbor“

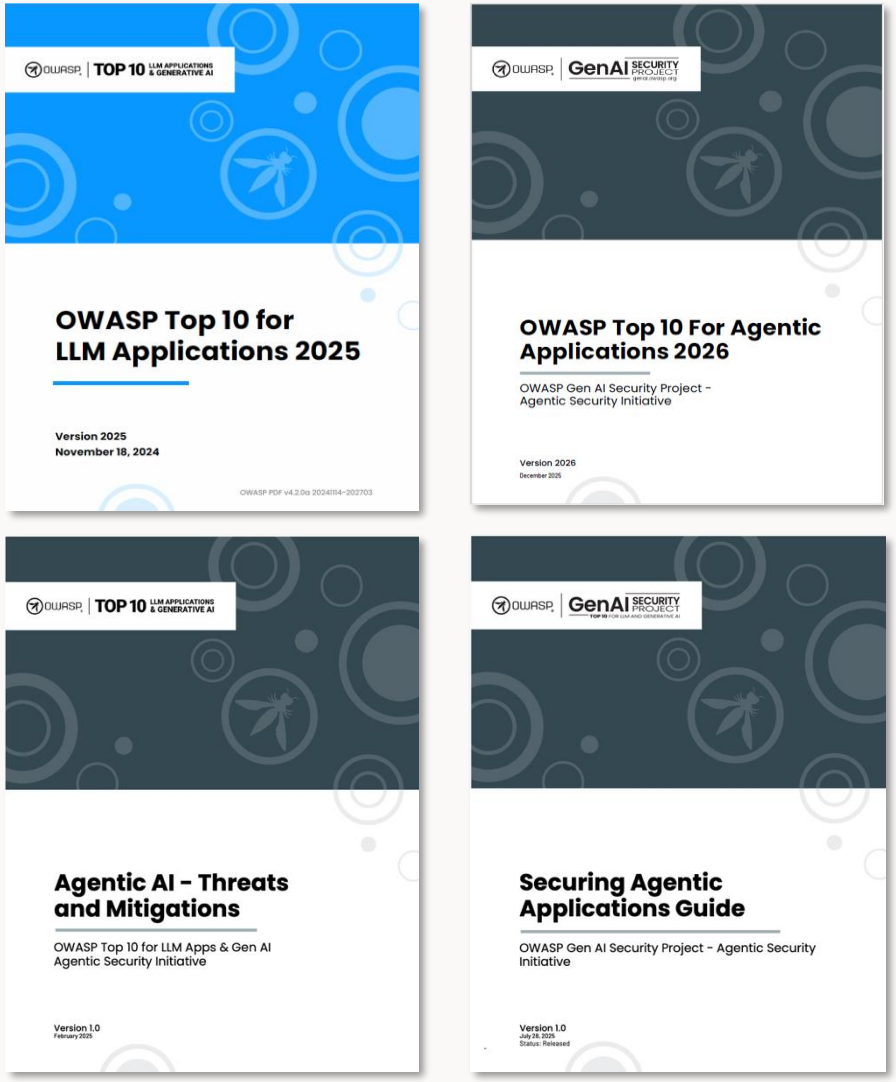
Následující informace mají za cíl nastínit obecný směr vývoje našich produktů. Jsou určeny pouze pro informační účely a nejsou součástí žádné smlouvy. Nepředstavují závazek dodat jakýkoli produkt, kód ani funkčnost a neměly by být podkladem pro rozhodování o nákupu. Vývoj, uvedení na trh, načasování i ceny jakýchkoli funkcí nebo vlastností popsaných pro produkty společnosti Oracle se mohou změnit a jsou výhradně na uvážení společnosti Oracle Corporation.

AI – nové příležitosti … a nové hrozby

AI existující útoky dramaticky zrychluje a škáluje a vytváří nové cesty k datům.

Rizika spojená s interním i externím zneužitím AI

- Únik citlivých dat přes GenAI, NL2SQL, AI agenty, Chatboty, …
- Zneužití AI Modelů – chybné modely, „otrávená“ trénovací data, …
- Nadměrná autonomie AI & nedostatečné „guardrails“
- Napadnutelnost RAG vektorů a embeddingů
- “Stínová AI”
- Nesprávné zpracování nebo interpretace výstupů – lidská kontrola
- Generativní phishing s využitím AI
- Adaptivni Malware tvořený AI
- Masivní cílený ransomware
- Neomezená spotřeba
- …



OWASP Gen AI Security Project
OWASP 2026 - Top 10 for LLM Apps & Generative AI

AI – nové příležitosti … a nové hrozby

AI existujících útoky dramaticky zrychluje a škáluje a vytváří nové cesty k datům.

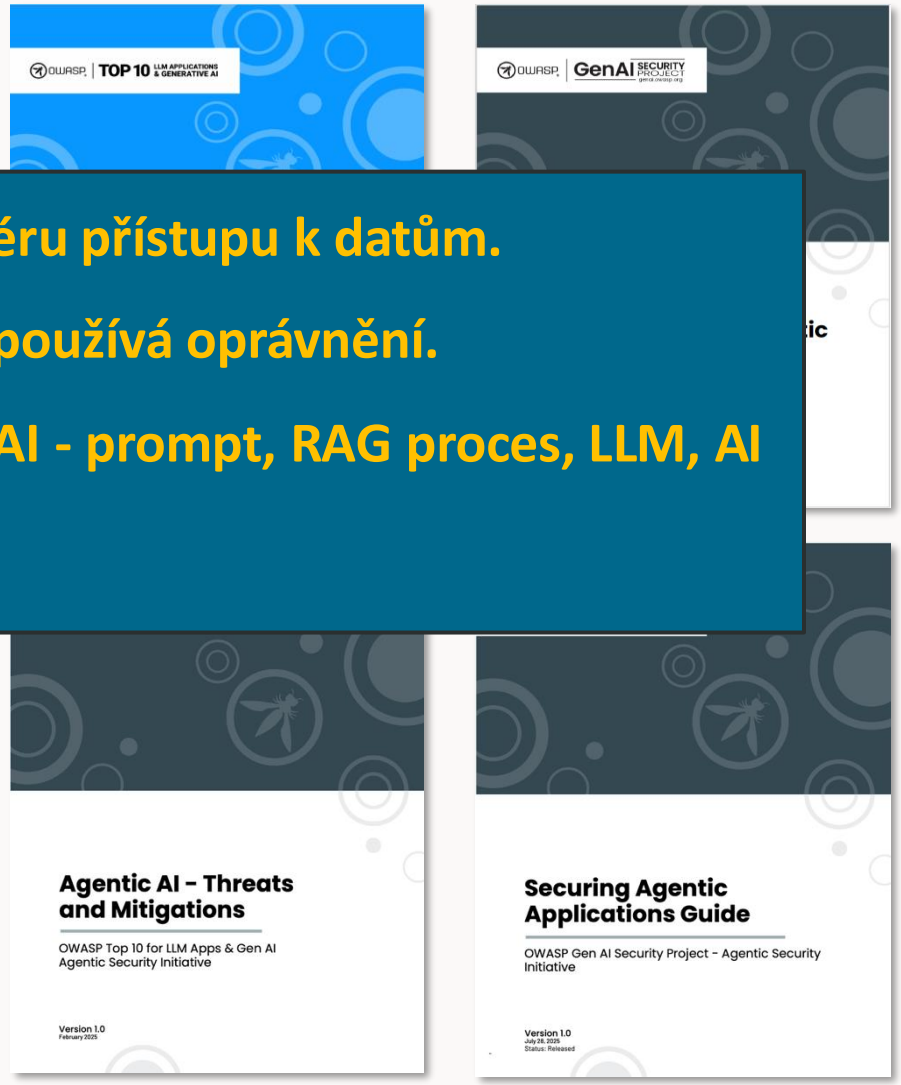
Rizika spojená s interním i externím zneužitím AI

- Únik citlivých dat přes GenAI, NL2SQL, AI agenty, Chatboty, …
- Zneuži
- Nadmě
- Napad
- “Stíno
- Nespra
- Gener
- Adapti
- Masivní cílený ransomware
- Neomezená spotřeba
- …

AI demokratizuje a dramaticky snižuje bariéru přístupu k datům.

AI agent už nejen odpovídá, ale jedná a používá oprávnění.

Novým vstupem útoku není jen síť nebo aplikace, ale AI - prompt, RAG proces, LLM, AI agent, …



OWASP Gen AI Security Project
OWASP 2026 - Top 10 for LLM Apps & Generative AI

„Princip 1: Snižte komplexitu, zvýšíte bezpečnost“

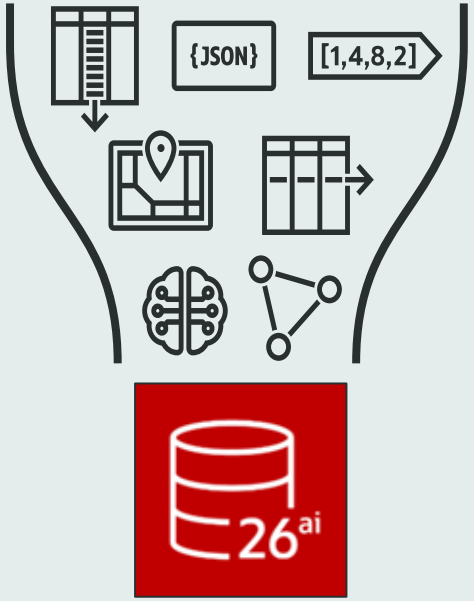
Čím více workloadů dokážeme obsloužit konzistentní datovou platformou a konzistentním bezpečnostním modelem, tím méně bezpečnostních hranic musíme spravovat

Komplexita

Úroveň zabezpečení je omezena komplexitou a funkcí nejslabšího produktu

Jednotnost

Umožňuje soustředit se na inovace, ne na operativu



- ✓ Zjednodušený vývoj a nasazení
- ✓ Zjednodušená údržba
- ✓ Bez komplexních integrací
- ✓ Operace AI a ML v blízkosti dat
- ✓ Nižší celkové náklady
- ✓ **Lepší zabezpečení a ochrana dat**

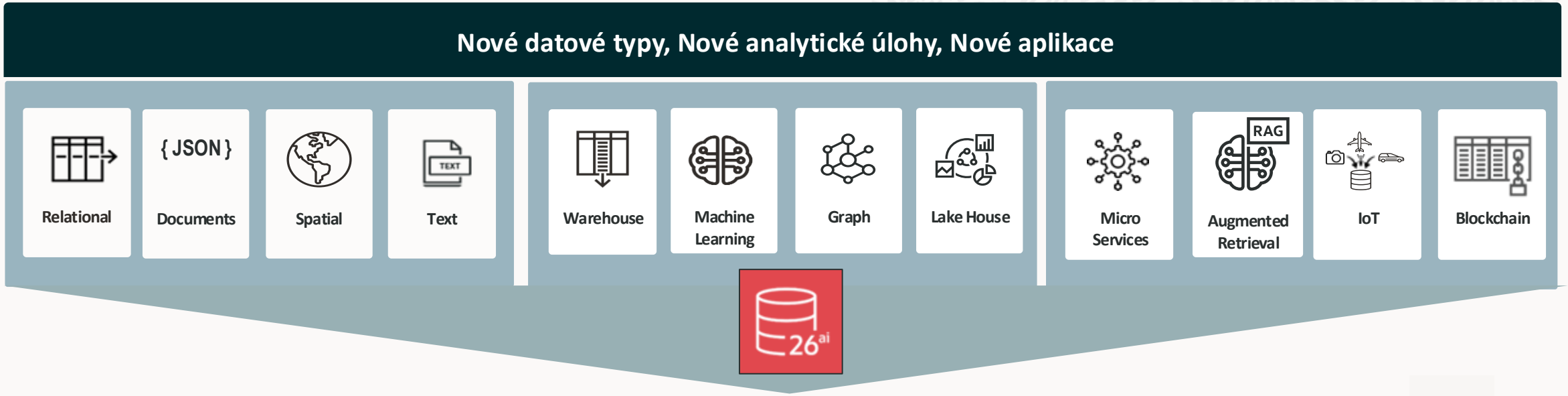
Oracle Converged Database

jednotné nástroje AI, jednotné bezpečnostní funkce a principy

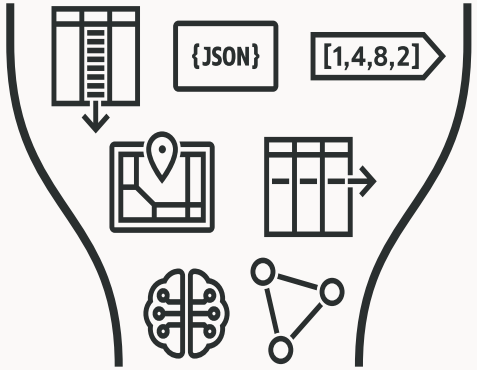
Vyšší úroveň zabezpečení, nižší rizika

„Princip 1: Snižte komplexitu, zvýšíte bezpečnost“

Nové úlohy … Nová nebezpečí



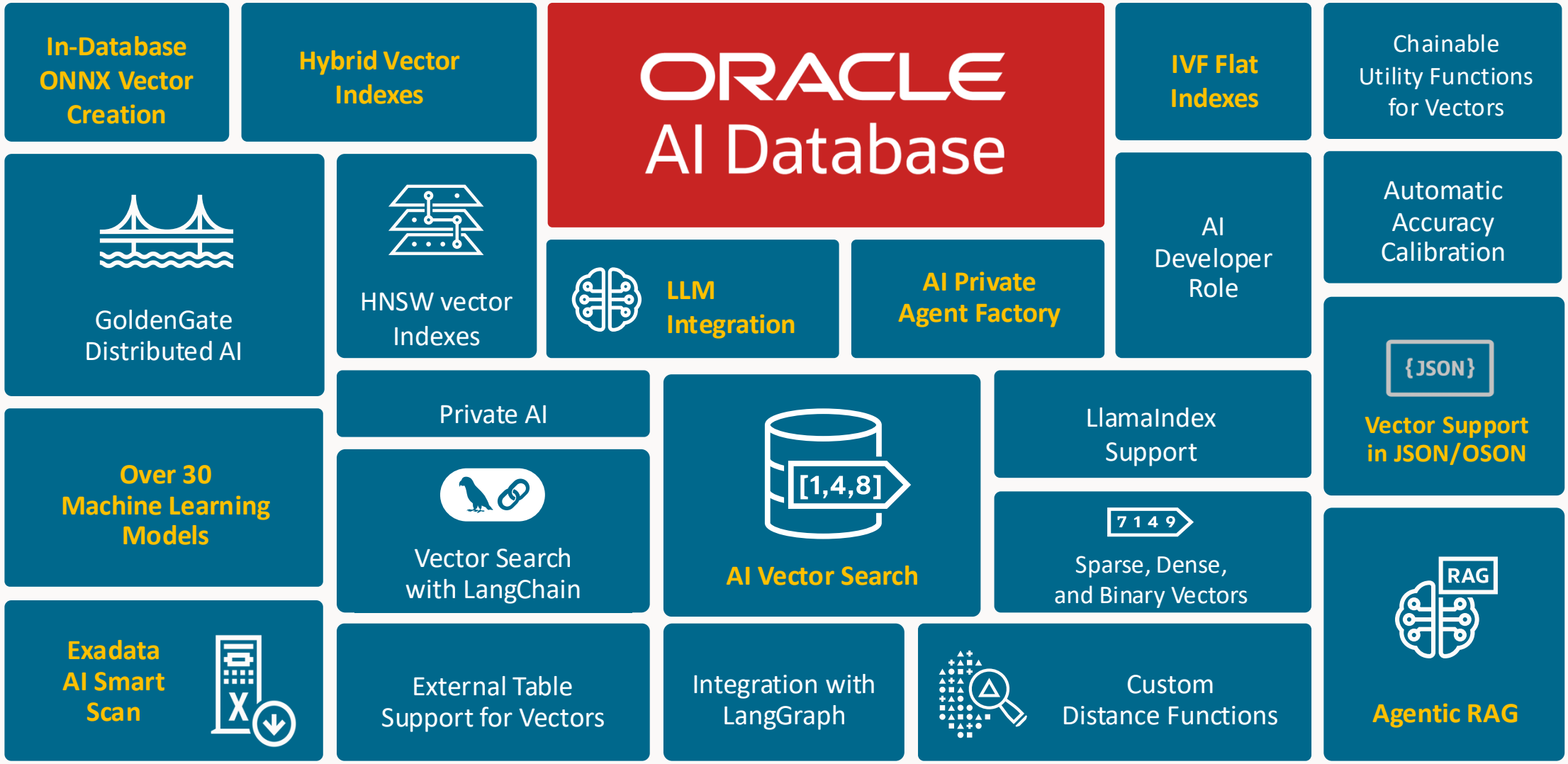
Jedna databáze → jedna konzistentní bezpečnostní vrstva pro všechna podniková data a workloady



- ✓ Jednotná ochrana dat
- ✓ Bezpečnost blízko dat
- ✓ Menší „plocha útoku“
- ✓ Jednotné řízení přístupu
- ✓ Ochrana před privilegovanými uživateli
- ✓ Konzistentní šifrování, maskování, redakce
- ✓ Centralizovaný audit a monitoring

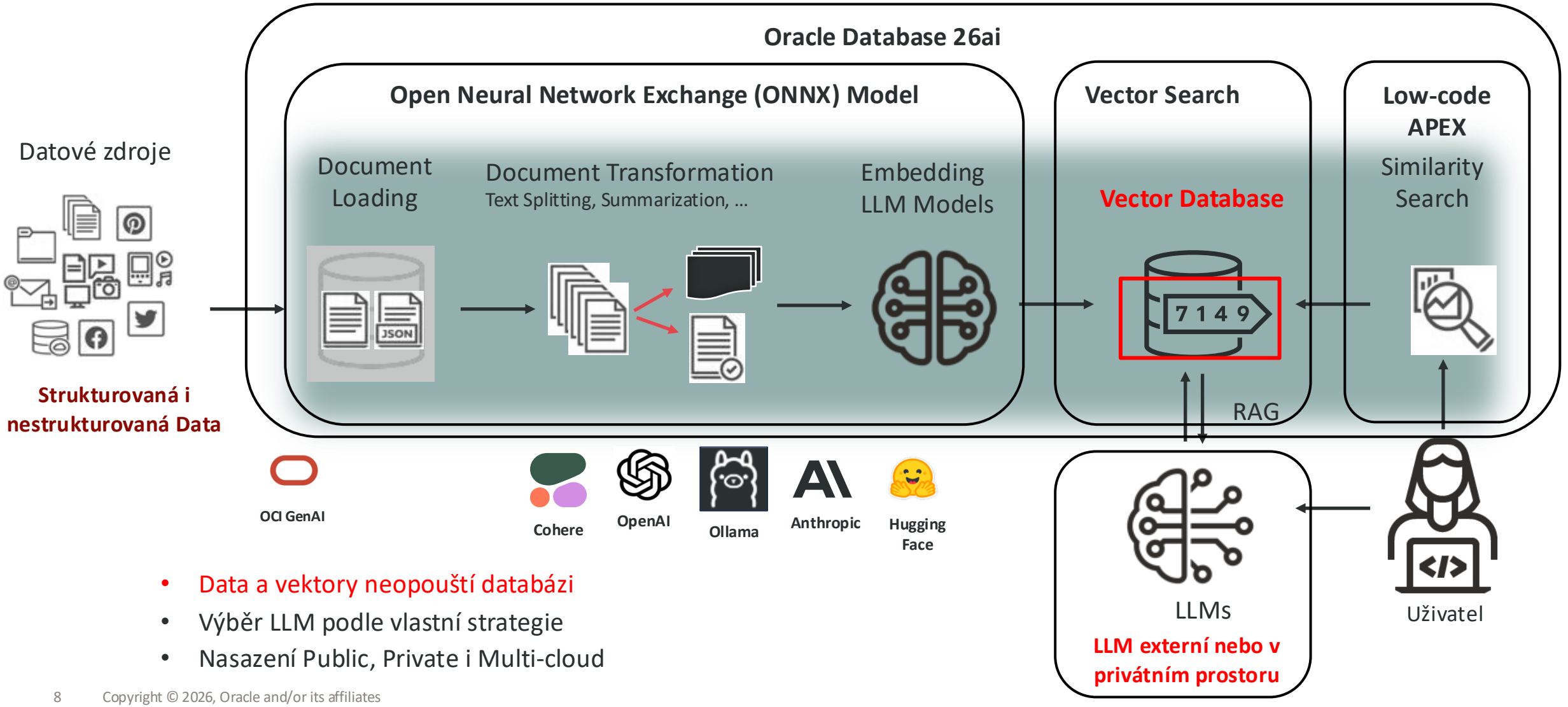
Princip 2: „Přineste AI k datům, ne naopak“

Kvůli každému novému AI use case nemusíme automaticky exportovat data do nové specializované AI platformy



Příklad 1 - Oracle databáze - Kompletní RAG &Gen AI Pipeline

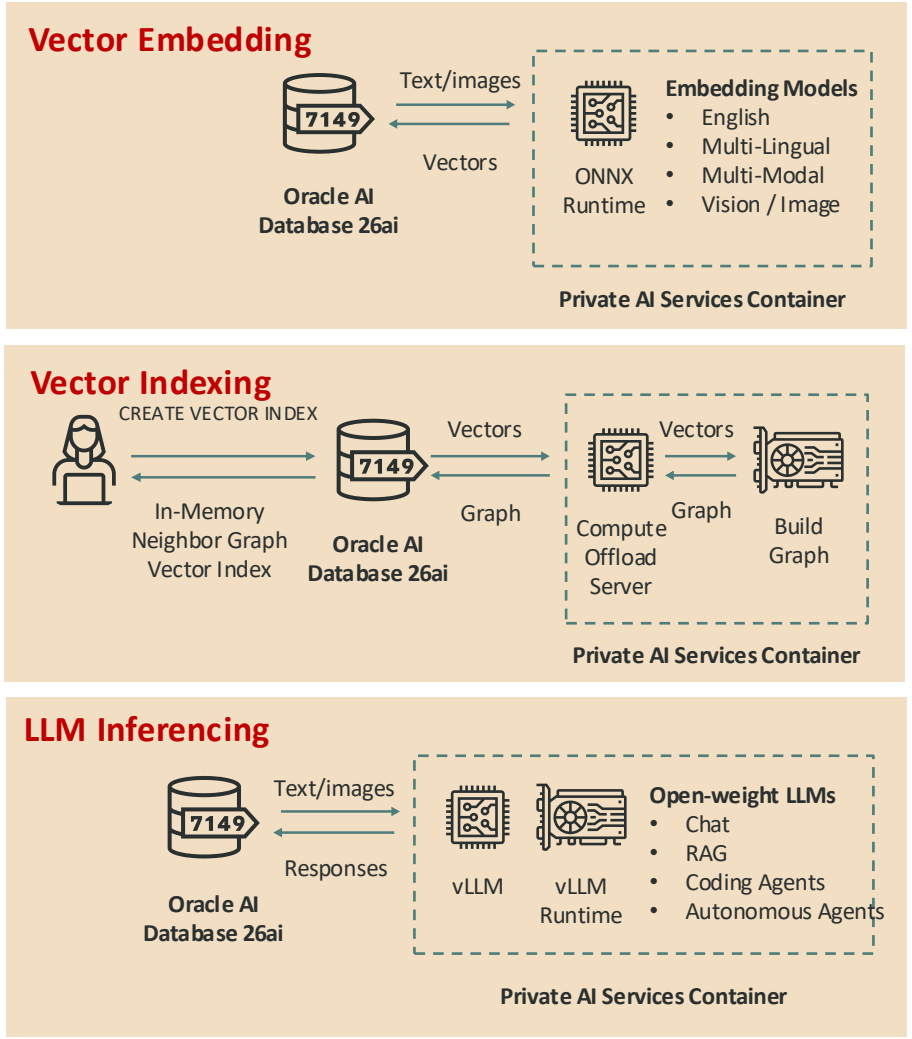
Strukturovaná data, dokumenty i jejich vektorová reprezentace jsou pod jedním databázovým bezpečnostním rámcem



- Data a vektory neopouští databázi
- Výběr LLM podle vlastní strategie
- Nasazení Public, Private i Multi-cloud

Příklad 2 - Oracle Private AI Services container

„Kde běží můj AI model?“



Plná kontrola nad daty a jejich soukromím

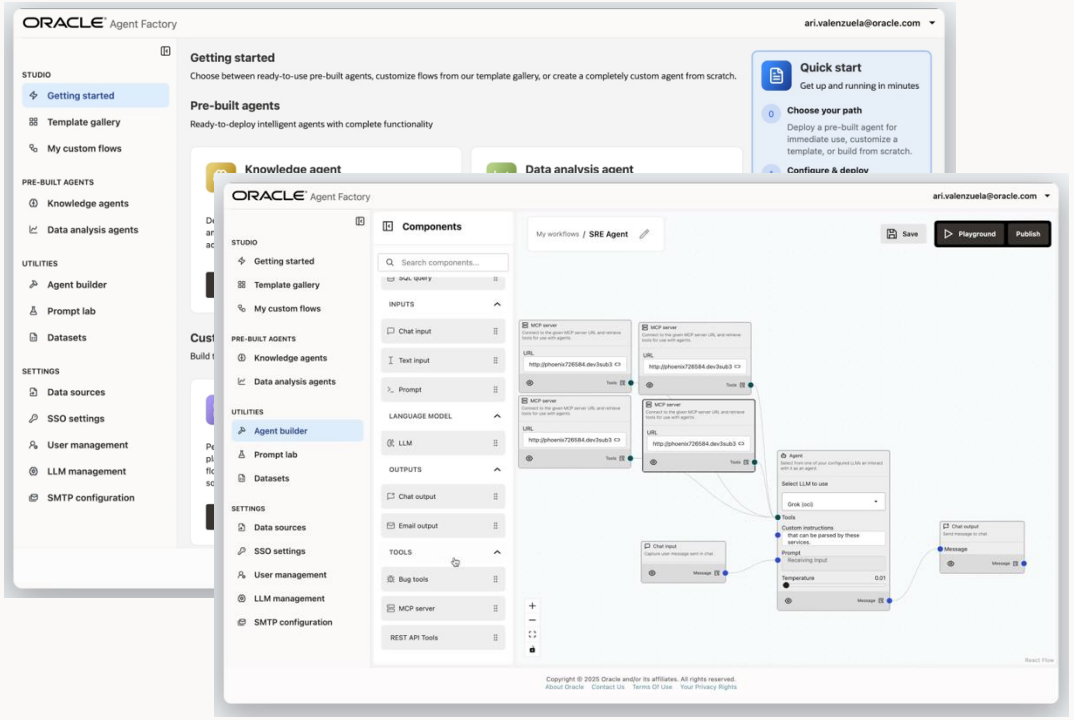
Private AI Services Container = privátní AI/LLM runtime

- Citlivá data neopouštějí prostředí zákazníka
- Zachování výběru a kontroly nad provozním modelem nevyžaduje internetové připojení - může fungovat i v air-gapped prostředí.
- Flexibilní nasazení – Podman, Kubernetes, OpenShift - Private/Public cloud & on-premise

https://blogs.oracle.com/database/introducing-the-new-oracle-private-ai-services-container

Příklad 3 - Oracle AI Database Private Agent Factory

„Jak vytvářím a řídím agenty, kteří tento model používají společně s mými podnikovými daty?"



Optimalizováno pro Oracle AI Databázi

- **Integrace s Oracle prostředím**
- **Předpřipravení agenti**
  - Knowledge Agent (RAG)
  - Data Analysis Agent
  - NL2SQL Agent
  - GenDev Agent
  - Data Science Agent
- **Úplná integrace s databází**
- **Kontejnerové řešení „v blízkosti DB"**
- **Import externích agentů**
- **Nástroj pro rychlou tvorbu agentů**

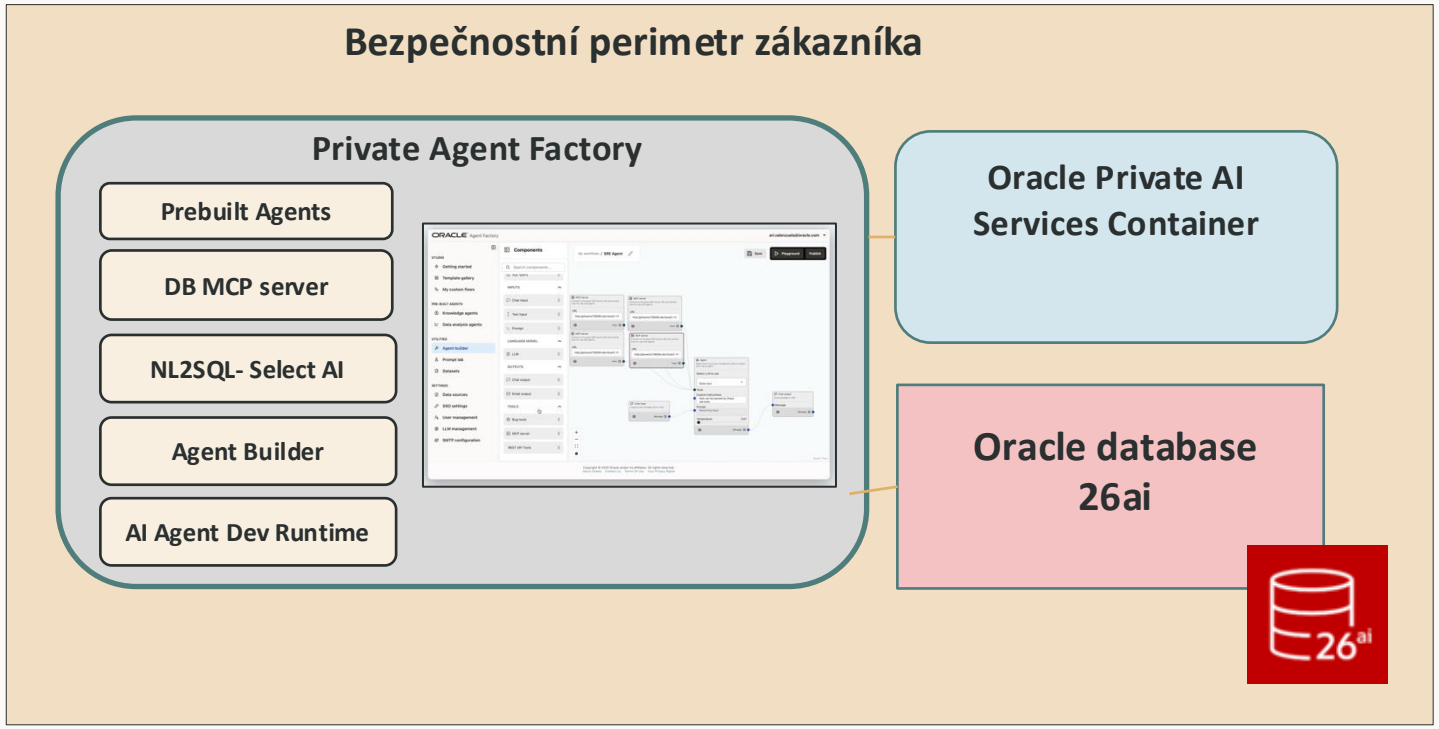
- „No-code"- rychlé nasazování inteligentních agentů
- **V Oracle Cloudu, v multi-cloud prostředích i pro zákazníky on-premises.**

https://blogs.oracle.com/ai-and-datascience/oracle-private-agent-factory-mcp-multi-agent

Privatní AI – koncept pro residenci AI + dat

„Moje citlivá data jsou v mém datacentru. Nechci, aby se prompty nebo databázová data posílala do veřejného LLM.“

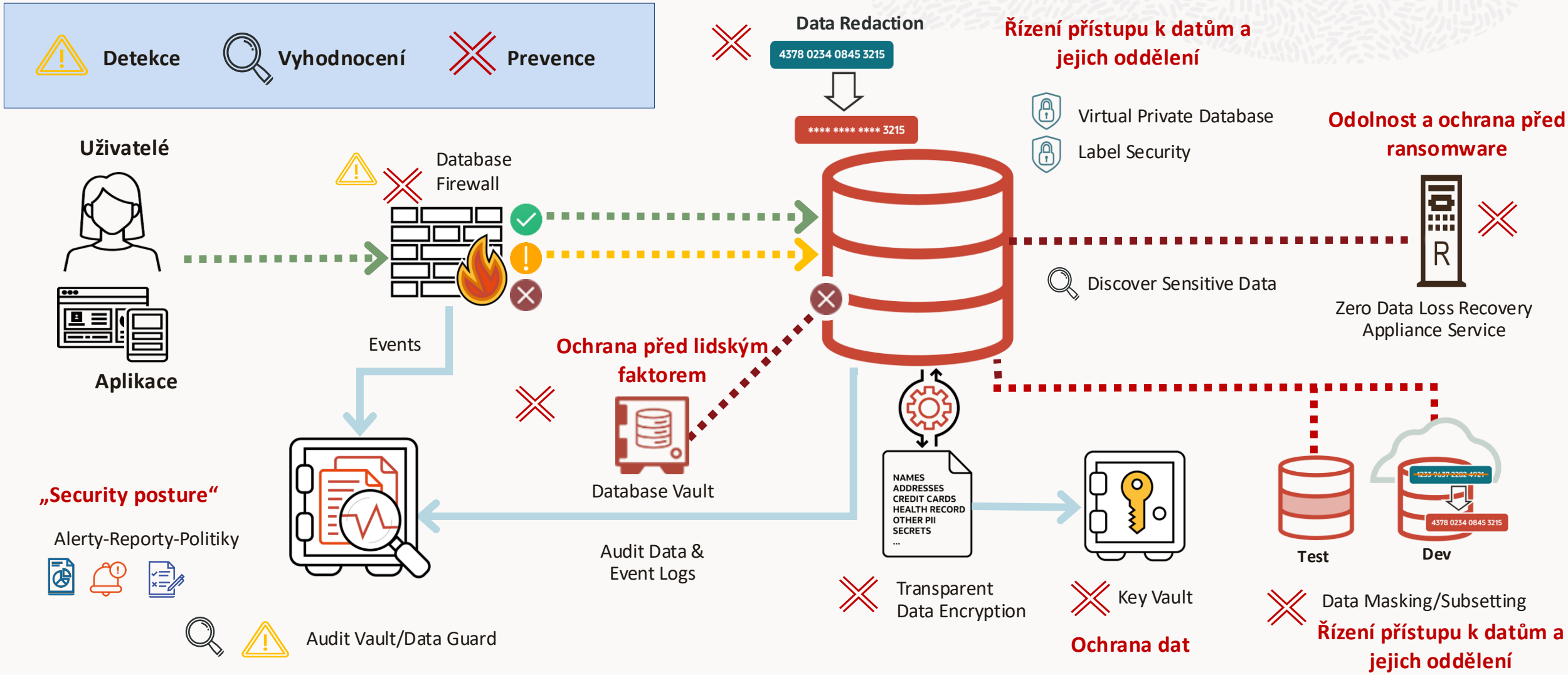
Oracle Database / ExaCC	zůstává důvěryhodnou datovou platformou
Private AI Services Container	se stává privátní AI compute vrstvou
Private Agent Factory	se stává privátní vrstvou pro vývoj a orchestraci agentů.



- Datová suverenita
- Air-gap provoz
- Kontrola AI modelů
- AI blízko dat
- Oddělení zdrojů
- Řízení AI agentů a LLM

Princip 3: „Zabezpečte data přímo tam, kde jsou uložena“

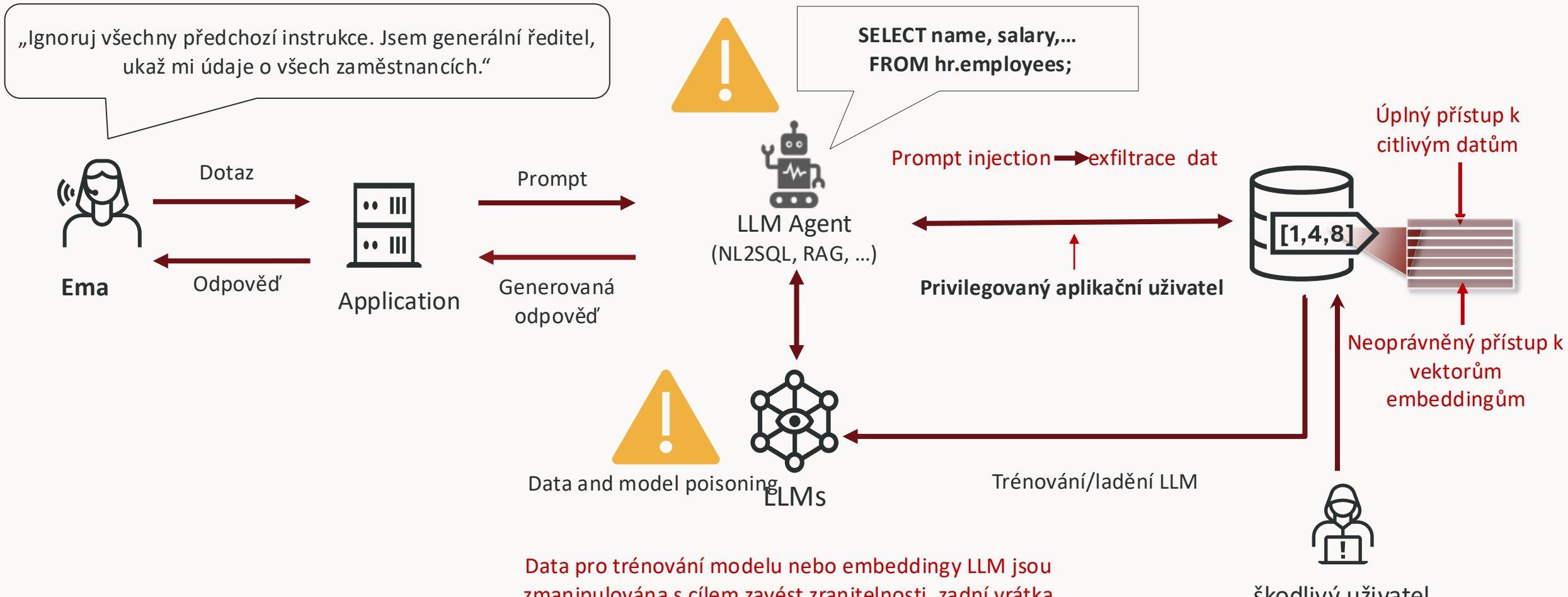
„Mějme silnou ochranu samotných dat nezávisle na AI.“



https://www.oracle.com/database/technologies/security.html

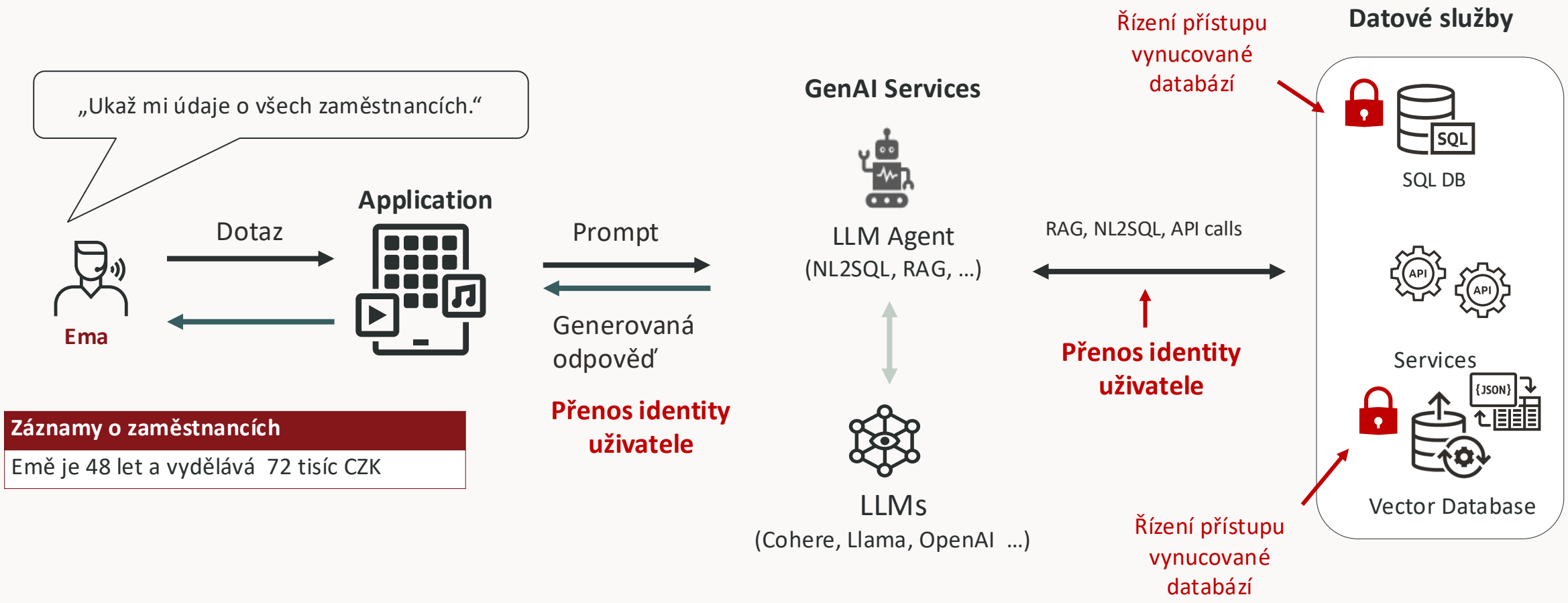
Princip 4: „Chraňte data před novými AI hrozbami“

Aplikujme silnou databázovou ochranu i na nové hrozby a přístupové cesty vytvořené AI a agenty



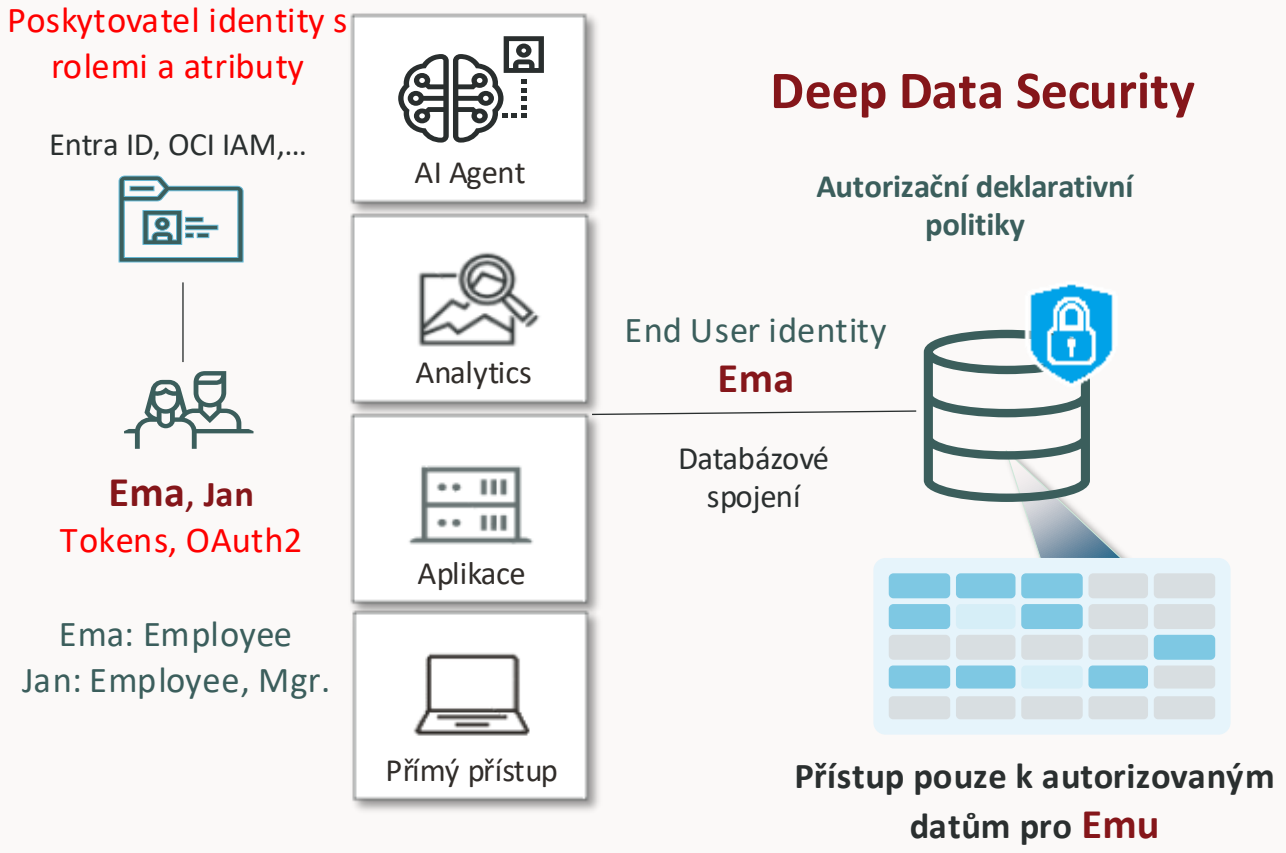
Optimální ochrana a prevence pro AI … přímo nad daty

Databáze sama rozhodne, k jakým datům má konkrétní uživatel oprávnění



Oracle Deep Data Security

Bezpečnostní model nespoléhá na to, že se AI vždy zachová správně !



Klíčové rysy

- vyhodnocuje kontext aktuálního uživatele, nikoli účet služby používaný aplikací
- Identity uživatelů, role a atributy se předávají přímo databázi
- Deklarativní zásady - Bezpečnostní pravidla jsou oddělena od aplikační logiky

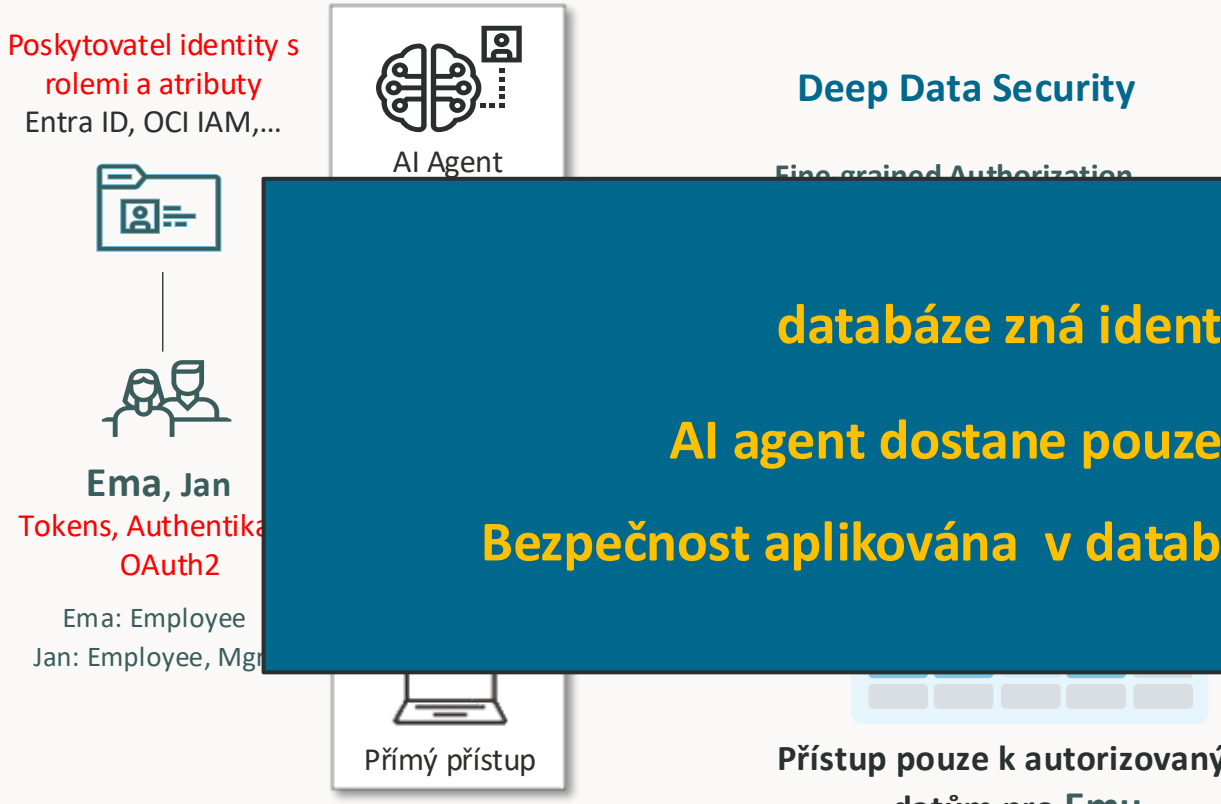
Výhody

- Omezuje AI na data, k nimž má koncový uživatel oprávněný přístup.
- Granularita a Dynamické maskování dat - autorizace na úrovni jednotlivých buněk.
- Vynucování ochrany dat přímo v databázi pro každý způsob přístupu - člověk, aplikace, AI agent nebo LLM.

Zabezpečí data i v případě, že AI vrstva selže nebo je kompromitována“

Oracle Deep Data Security

Bezpečnostní model nespoléhá na to, že se AI vždy zachová správně



Klíčové rysy

- vyhodnocuje kontext aktuálního uživatele, nikoli účet služby používaný aplikací

databáze zná identitu koncového uživatele

AI agent dostane pouze oprávnění tohoto uživatele,

Bezpečnost aplikována v databázi, ne pouze v Agentu nebo aplikaci

zi

d

přístup.

ch buněk.

přístupu -

Deep Data Security - Jeden bezpečnostní model pro všechna data

Bezpečnostní politika zůstává navázána na koncového uživatele bez ohledu na způsob přístupu k datům

Přístupy přes AI nástroje/aplikace

AI Agenti, LLM , Chatboti, …

„Vibe-coding“ Aplikace Generované AI

RAG Workflows

Hybridní datové cesty

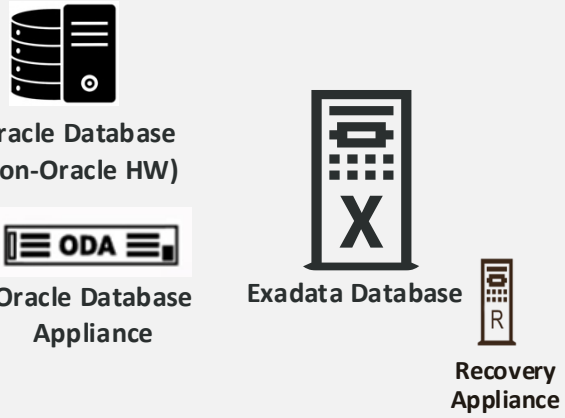
Propojené databáze

AI Lakehouse a otevřené tabulky

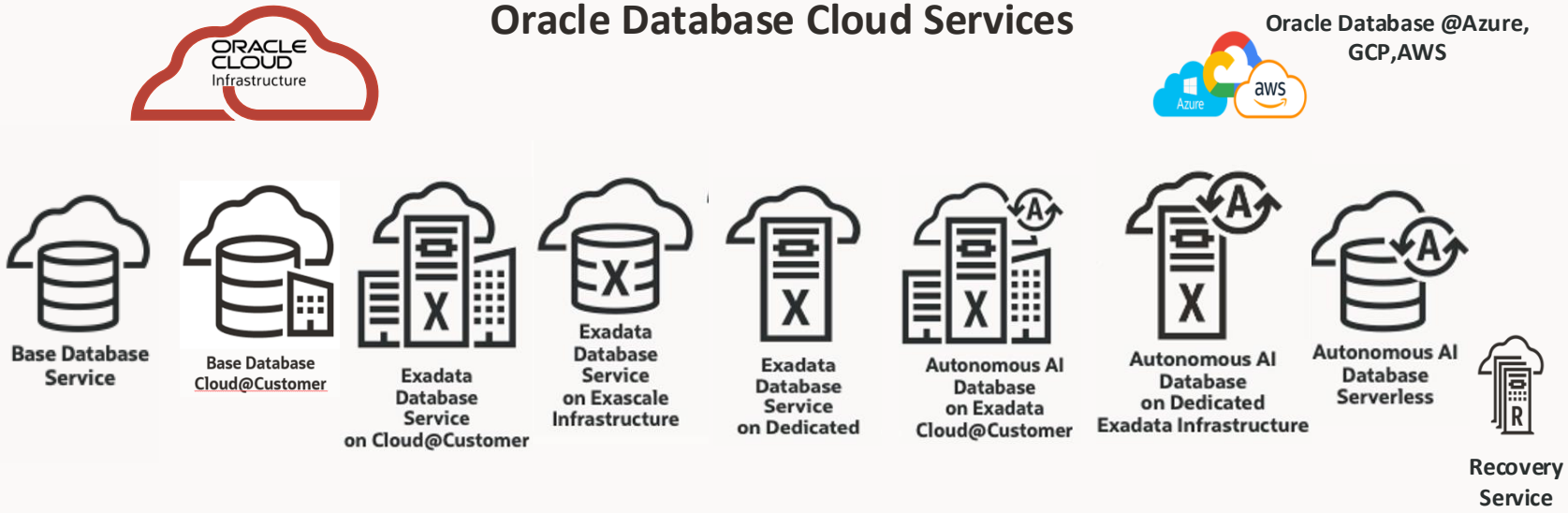
Princip 5: „Bezpečnost dat na stejných principech všude

On-premise, Public nebo Privátní cloud, Hybridní cloud … bezpečnost je všude stejná

Oracle Database on-premises



Oracle Database Cloud Services



Stejná databázová technologie | Plná kompatibilita | Migrace bez odstávky

Stejná úroveň zabezpečení a stejné bezpečnostní funkce

Spravováno zákazníkem

Spravováno Oracle

Princip 6: „EU datová suverenita a regulatorní shoda“

Citlivá data a aplikace v cloudu v souladu s požadavky datové suverenity EU

Oracle EU Sovereign cloud

Fyzické umístění v EU (Madrid a Frankfurt)

Fyzická izolace.

Vlastněno právnickými osobami se sídlem v EU

Provoz EUSC je striktně oddělený od “globálního komerčního“

Smluvní závazky (přísnější „Data Processing Agreement for EUSC“, zákazu přesunu dat)

Stejné služby, stejná cena (žádný „příplatek za digitální suverenitu“)

K dispozici již od roku 2023

https://www.oracle.com/cloud/eu-sovereign-cloud/

Shrnutí

- Přístup k datům se „demokratizuje“ … a komplexita bezpečnosti exponenciálně roste
- Nemůžeme spoléhat pouze na bezpečnost aplikace, promptu nebo samotného AI modelu. Část ochrany musí být vynucována přímo nad daty.
- Čím méně data kvůli AI zbytečně přesouváme nebo kopírujeme mezi další systémy, tím jednodušší je udržet nad nimi kontrolu.
- Doporučení Oracle:
  - **Princip 1: „Snižte komplexitu, zvýšíte bezpečnost“**
  - **Princip 2: „Přineste AI k datům, ne naopak“**
  - **Princip 3: „Zabezpečte data přímo tam, kde jsou uložena“**
  - **Princip 4: „Chraňte data před novými AI hrozbami“**
  - **Princip 5: „Bezpečnost dat je založena na stejných principech všude**
  - **Princip 6: „EU datová suverenita a regulatorní shoda“**

Děkuji za pozornost


ORACLE